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
# Table of Contents

**Introduction** ........................................................................................................................................... 1  
Manual Content .......................................................................................................................................... 2  
What’s New in 2017–18 ............................................................................................................................... 2  
Sections ..................................................................................................................................................... 5  
Document Conventions ............................................................................................................................... 5  
Intended Audience ..................................................................................................................................... 6  

**Chapter 1. System Requirements** ........................................................................................................ 7  
Supported Operating Systems for Student Testing .................................................................................. 8  
Desktops and Laptops ................................................................................................................................. 8  
Tablets ...................................................................................................................................................... 9  
Chromebooks and Chromebases .............................................................................................................. 9  
Thin Clients: NComputing and Terminal Servers for Windows ............................................................... 10  
Supported Web Browsers for Online Systems Associated with Testing ................................................ 12  
Supported Web Browsers by Operating System .................................................................................... 12  
Available Audio Settings by Web Browser ............................................................................................. 14  
Requirements for Peripheral Equipment ................................................................................................. 15  
Monitors and Screen Display Requirements ......................................................................................... 15  
Keyboards .............................................................................................................................................. 15  
Headsets and Headphones ..................................................................................................................... 16  
Mice .......................................................................................................................................................... 17  

**Chapter 2. Network Configuration** ..................................................................................................... 19  
Network Configuration and Testing ......................................................................................................... 20  
Network Configuration ............................................................................................................................. 20  
Network Diagnostic Tools ....................................................................................................................... 23  

**Chapter 3. System Configuration** ....................................................................................................... 26  
Hardware Configuration ............................................................................................................................. 27  
Connections Between Printers and Testing Devices .............................................................................. 27  
Wireless Networking and Determining the Number of Wireless Access Points (WAPs) ....................... 27  
Hardware for Braille Testing .................................................................................................................... 28  
Software Configuration ............................................................................................................................ 29  
Optimal Installation Scenario for Secure Browsers .................................................................................. 29  
Configuring Commercially Available Web Browsers ............................................................................. 30  
Configuring Windows for Online Testing with the Secure Browser ..................................................... 33  
Configuring Mac OS X for Online Testing with the Secure Browser .................................................... 43  
Configuring Linux for Online Testing with the Secure Browser ............................................................ 50  
Configuring Apple Mobile Devices for Online Testing with the Secure Browser .................................. 51  
Configuring Android for Online Testing with the Secure Browser ....................................................... 59  
Configuring Chromebook Mobile Devices for Online Testing with the Secure Browser ..................... 64  
Installing CloudReady on PCs and Macs ................................................................................................. 67  
Configurations for Testing Students Using Accessibility Supports .................................................... 69  

**Chapter 4. Secure Browser Configuration** ........................................................................................ 71  
Overview of Secure Browsers .................................................................................................................. 72  
About the Secure Browser ......................................................................................................................... 72  
Secure Browser Versions for Online Testing ............................................................................................ 73  
Forbidden Application Detection ............................................................................................................. 74  
Secure Browser Error Messages .............................................................................................................. 75  
Installing the Secure Browser on Desktops and Laptops ...................................................................... 76  
Installing the Secure Browser on Windows ............................................................................................. 76  
Installing the Secure Browser on Mac OS X ............................................................................................ 83  
Installing the Secure Browser on Linux .................................................................................................... 86
Installing the Secure Browser on Mobile Devices ................................................................. 88
Installing the Secure Browser on iOS .................................................................................... 88
Installing AIRSecureTest on Android .................................................................................... 91
Chrome OS AIRSecureTest Kiosk App .................................................................................. 93
Installing the Secure Browser on Windows Mobile Devices ................................................ 102
Proxy Settings for Desktop Secure Browsers .......................................................................... 103
   Specifying a Proxy Server to Use with the Secure Browser .................................................. 103
   Modifying Desktop Shortcuts to Include Proxy Settings ....................................................... 104
Appendixes .......................................................................................................................... 107
      Timing of Secure Browser Updates .................................................................................... 108
      Support Plan for Operating Systems ................................................................................ 109
   Appendix B. URLs for Testing Systems ................................................................................ 111
      URLs for Nontesting Sites ............................................................................................... 111
      URLs for Testing Sites ..................................................................................................... 112
   Appendix C. Technology Coordinator Checklist .................................................................... 113
   Appendix D. Scheduling Online Testing ................................................................................ 115
      Number of Devices and Hours Required to Complete Online Tests .................................. 115
      Sample Test Scheduling Worksheet .................................................................................. 115
   Appendix E. Creating Group Policy Objects to Assign Logon Scripts ............................... 116
   Appendix F. Resetting Secure Browser Profiles .................................................................... 118
      Resetting Secure Browser Profiles on Windows ................................................................. 118
      Resetting Secure Browser Profiles on OS X 10.7 or Later ................................................ 118
      Resetting Secure Browser Profiles on Linux ...................................................................... 119
   Appendix G. User Support ..................................................................................................... 120
      California Technical Assistance Center for LEA CAASPP Coordinators .......................... 120

List of Tables

Table 1. Key Symbols and Document Conventions ................................................................. 5
Table 2. Supported Desktop Operating Systems ................................................................. 8
Table 3. Supported Tablets and Operating Systems ............................................................... 9
Table 4. Supported Chromebooks .......................................................................................... 10
Table 5. Supported NComputing Solutions ........................................................................... 10
Table 6. Supported Terminal Servers .................................................................................... 10
Table 7. Supported Web Browsers by Test Administration Web Site ................................... 12
Table 8. Available Audio Settings by Browser ....................................................................... 14
Table 9. Supported Headphones and Headsets .................................................................... 17
Table 10. Average Bandwidth Used by Secure Browser for Testing .................................. 21
Table 11. Ports and Protocols for the TDS .......................................................................... 21
Table 12. Recommended Ratios of Devices to Wireless Access Points .............................. 28
Table 13. Profile Keys for Features in iOS 9.2 or Later ........................................................ 52
Table 14. Secure Browsers by Operating System .................................................................. 73
Table 15. Specifying Proxy Settings Using a Shortcut or the Command Line .................... 103
Table 16. Supported Operating Systems ............................................................................... 109
Table 17. URLs for Nontesting Sites ..................................................................................... 111
Table 18. URLs for Testing Web Sites .................................................................................... 112
Table 19. URLs for Online Dictionary and Thesaurus .......................................................... 112
List of Figures

Figure 1. Sign-In Web page for the training test ................................................................. 23
Figure 2. Run the diagnostics test .................................................................................... 24
Figure 3. Internet Explorer Internet Options dialog box ................................................... 32
Figure 4. Internet Explorer Security Settings dialog box .................................................. 32
Figure 5. Safari Advanced preferences ............................................................................. 33
Figure 6. Windows Search box .......................................................................................... 34
Figure 7. Local Group Policy Editor screen options .......................................................... 34
Figure 8. Finish in the Windows Local Group Policy Editor screen .................................... 34
Figure 9. Windows Search charm ...................................................................................... 35
Figure 10. Windows Local Group Policy Editor options .................................................... 35
Figure 11. Windows Local Group Policy Editor selection ................................................... 35
Figure 12. Windows Run dialog box .................................................................................. 36
Figure 13. Notification in the Windows Command window ................................................. 36
Figure 14. Local Group Policy Editor .................................................................................. 37
Figure 15. Windows Components in the Local Group Policy Editor .................................. 37
Figure 16. Input Panel in the Local Group Policy Editor ..................................................... 38
Figure 17. Disable text prediction selection ...................................................................... 38
Figure 18. Disable text prediction dialog box ................................................................... 39
Figure 19. Surface Pro 3 Settings interface ....................................................................... 40
Figure 20. Touch keyboard settings interface .................................................................... 40
Figure 21. Mouse Properties dialog box ............................................................................ 41
Figure 22. Properties for Synaptics TouchPad V7.5 on PS/2 Port dialog box ..................... 42
Figure 23. Select OS X System Preferences ...................................................................... 43
Figure 24. [Keyboard] icon ............................................................................................... 43
Figure 25. [Keyboard Shortcuts] tab .................................................................................. 43
Figure 26. OS X Mission Control options ......................................................................... 44
Figure 27. Apple System Preferences screen .................................................................... 44
Figure 28. Keyboard options ............................................................................................. 45
Figure 29. App Store screen .............................................................................................. 45
Figure 30. Advanced Preferences options ......................................................................... 46
Figure 31. Trackpad Preferences options, [Point & Click] tab ............................................. 47
Figure 32. Trackpad Preferences options, [More Gestures] tab ........................................... 47
Figure 33. [Keyboard] button in OS X System Preferences .................................................. 49
Figure 34. Dictation system preferences options in OS X .................................................... 49
Figure 35. [Siri] button in OS X System Preferences ............................................................ 50
Figure 36. Siri system preferences options in OS X ............................................................ 50
Figure 37. Settings options in Apple Configurator .............................................................. 54
Figure 38. Create New Profile configuration options .......................................................... 54
Figure 39. Preferences options .......................................................................................... 55
Figure 40. Organization Info screen .................................................................................. 56
Figure 41. Apple Configurator screen ............................................................................... 57
Figure 42. Notification when starting test with automatic assessment configuration .......... 58
Figure 43. Emoji keyboard for iOS .................................................................................. 58
Figure 44. [Settings] icon ................................................................................................. 58
Figure 45. Keyboards configuration interface ..................................................................... 58
Figure 46. Disabled dictation .............................................................................................. 59
Figure 47. Keyboard Settings for iOS 9.3 (other versions of iOS are similar) ....................... 59
Figure 97. Manage Kiosk Applications screen ................................................................. 96
Figure 98. Chrome Admin console screen .......................................................................... 97
Figure 99. Chrome Device management screen ............................................................... 98
Figure 100. Chrome Management screen ................................................................................. 99
Figure 101. Chrome App Management screen ....................................................................... 100
Figure 102. Select [Kiosk settings] ...................................................................................... 100
Figure 103. Chrome Kiosk settings screen ........................................................................... 101
Figure 104. Chromebook logon screen .................................................................................. 101
Figure 105. Select the state from the Launchpad ................................................................. 102
Figure 106. Select the assessment from the Launchpad ....................................................... 102
Figure 107. The Local Group Policy Editor window .......................................................... 116
Figure 108. The Logon Properties dialog box ....................................................................... 117
Figure 109. The Add a Script dialog box ............................................................................ 117
Figure 110. Resetting the secure browser on OS X 10.7 or later ........................................ 119

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

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIR</td>
<td>American Institutes for Research</td>
</tr>
<tr>
<td>ASAM</td>
<td>Autonomous Single App Mode</td>
</tr>
<tr>
<td>CAASPP</td>
<td>California Assessment of Student Performance and Progress</td>
</tr>
<tr>
<td>CalTAC</td>
<td>California Technical Assistance Center</td>
</tr>
<tr>
<td>CAST</td>
<td>California Science Test</td>
</tr>
<tr>
<td>CDE</td>
<td>California Department of Education</td>
</tr>
<tr>
<td>CSA</td>
<td>California Spanish Assessment</td>
</tr>
<tr>
<td>DEI</td>
<td>Data Entry Interface</td>
</tr>
<tr>
<td>IAHSS</td>
<td>Interim Assessment Hand Scoring System</td>
</tr>
<tr>
<td>ISP</td>
<td>Internet service provider</td>
</tr>
<tr>
<td>LEA</td>
<td>local educational agency</td>
</tr>
<tr>
<td>Mbps</td>
<td>megabits per second</td>
</tr>
<tr>
<td>MDM</td>
<td>mobile device management</td>
</tr>
<tr>
<td>ORS</td>
<td>Online Reporting System</td>
</tr>
<tr>
<td>STS</td>
<td>Standards-based Tests in Spanish</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>TDS</td>
<td>test delivery system</td>
</tr>
<tr>
<td>TIDE</td>
<td>Test Information Distribution Engine</td>
</tr>
<tr>
<td>TOMS</td>
<td>Test Operations Management System</td>
</tr>
<tr>
<td>TTS</td>
<td>text-to-speech</td>
</tr>
<tr>
<td>WAP</td>
<td>wireless access point</td>
</tr>
</tbody>
</table>
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 2017–18

<table>
<thead>
<tr>
<th>Feature</th>
<th>Change</th>
</tr>
</thead>
</table>
| Support for the California Spanish Assessment (CSA) pilot | • Unless specifically noted, all technical requirements and specifications described in this manual apply also to the 2017–18 CSA pilot.  
• When additional bandwidth data are available, the CSA will be added as an option to the Network/Bandwidth Diagnostic Tool. |
| Support for the California Science Test (CAST) field test | • Unless specifically noted, all technical requirements and specifications described in this manual apply also to the 2017–18 CAST field test.  
• When additional bandwidth data are available, the CAST will be added as an option to the Network/Bandwidth Diagnostic Tool. |
| Support for the Standards-based Tests in Spanish (STS) online | The STS, which is the optional primary language assessment for reading/language arts, will be administered online. Student test registration and other management activities will occur using the Administration and Registration Tools. |
| Updated secure browser for desktop and laptop machines | The updated secure browser for desktop and laptop operating systems (Windows and Mac iOS versions 10.9–10.12), version 10, currently is available and will be the only secure browser version that can be used on Windows, iOS versions 10.9–10.12, and Linux desktop and laptop machines after December 31, 2017. Version 9.5 will be supported on iOS versions 10.7–10.8 only. |
| Supported browser version changes | **Browser** | **Supported Version** | **Support Ended** |
| | Chrome | • 60+ (upon release) | • 51–59 |
| | Firefox | • 52+ | • 45–51* |
| | Safari | • 11 (upon release) | • N/A |
| *Note that Firefox 45–51 may be used only on devices with Mac OS X versions 10.7–10.8 using version 9.5 of the secure browser. |
| Operating system additions | **Operating System** | **Version Addition** |
| | Windows | • (no additions) |
| | Mac OS X (Intel) | • OS 10.13 |
| | Linux | • Fedora 26 |
| | iOS | • iOS 11.0 |
| | Android | • Android 7.0 (Nougat) |
| | Chrome OS | • Chrome 60  
• Any OS Google supports with auto update |
### Feature | Change
---|---
**Operating system deletions** (See page 8.) | **Operating System** | **Version Deletion**
Windows | • Vista
Mac OS X | • (no deletions)
Linux | • Fedora 23–24
• openSUSE 13.1, 13.2
• Ubuntu 12.04
iOS | • iOS 8.0–8.2
Android | • Android 4.4
Chrome OS | • Chrome 59 and below

**Windows Thin Client Host Additions** (See page 10.)

<table>
<thead>
<tr>
<th>Server Host</th>
<th>Server Software/Terminal</th>
</tr>
</thead>
<tbody>
<tr>
<td>NComputing</td>
<td></td>
</tr>
<tr>
<td>Server 2008 R2</td>
<td>• vSpace Server 8.4 (replaces v8.3)</td>
</tr>
<tr>
<td>Windows Server 2012, 2016 R2</td>
<td>• vSpace PRO 10</td>
</tr>
<tr>
<td>Windows 10</td>
<td>• vSpace PRO 10</td>
</tr>
<tr>
<td><strong>Terminal Server</strong></td>
<td></td>
</tr>
<tr>
<td>Windows Server 2016</td>
<td>• (no change)</td>
</tr>
</tbody>
</table>

**Minimum desktop system requirement additions** (See page 10.)

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Requirement Addition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>• 1.1 GHZ processor</td>
</tr>
<tr>
<td>Mac OS X</td>
<td>• 1.1 GHZ processor</td>
</tr>
<tr>
<td>Linux</td>
<td>• 1.1 GHZ processor</td>
</tr>
</tbody>
</table>

**Minimum desktop system requirement deletions** (See page 8.)

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Requirement Deletion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>• Pentium 4 or new processor</td>
</tr>
<tr>
<td>Mac OS X</td>
<td>• Intel x86 processor</td>
</tr>
<tr>
<td>Linux</td>
<td>• Intel x86 processor</td>
</tr>
</tbody>
</table>

**Minimum desktop system recommended specifications additions** (See page 8.)

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Recommended Specification Addition</th>
</tr>
</thead>
</table>
| Windows | • 1.4 GHZ processor
• 16 or more GB hard drive space |
| Mac OS X | • 1.4 GHZ processor
• 16 or more GB hard drive space |
| Linux | • 1.4 GHZ processor
• 16 or more GB hard drive space |

**Minimum desktop system recommended specifications deletions** (See page 8.)

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Recommended Specification Deletion</th>
</tr>
</thead>
</table>
| Windows | • Pentium 4 or new processor
• 80 GB+ hard drive |
| Mac OS X | • Pentium 4 or new processor
• 80 GB+ hard drive |
| Linux | • Pentium 4 or new processor
• 80 GB+ hard drive |

**Tablet additions** (See page 9.)

<table>
<thead>
<tr>
<th>Type</th>
<th>Supported Tablet</th>
</tr>
</thead>
<tbody>
<tr>
<td>iPad</td>
<td>• 5th Generation (Retina Display)</td>
</tr>
</tbody>
</table>
| Android | • Asus Transformer Pad
• Asus Memo Pad
• Dell Venue 10
• HP Pro Slate 10 |
<table>
<thead>
<tr>
<th>Feature</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Tablet deletions</strong> (See page 9.)</td>
<td><strong>Operating System</strong></td>
</tr>
</tbody>
</table>
| | Android | • Motorola Xoom  
• Samsung Galaxy Note (2014 edition)  
• Samsung Galaxy Tab 3  
• LearnPad Quarto |
| **Update to the mouse policy** (See page 17.) | Mice equipped with a “browser back” button that could potentially kick users out of a test should not be used. |
| **New instructions** | Instructions on the following topics have been added to this manual:  
• Configuring Commercially Available Web Browsers | Keyboard Navigation to Tool Menu Using a Safari Browser  
• Configuring Windows for Online Testing with the Secure Browser | Setting Touch Input  
• Configuring Mac OS X for Online Testing with the Secure Browser | Disabling Look-Up Gesture  
• Configuring Mac OS X for Online Testing with the Secure Browser | Disabling Dictation  
• Configuring Mac OS X for Online Testing with the Secure Browser | Disabling Siri  
• Configuring Chromebook Mobile Devices for Online Testing with the Secure Browser | Securing Chrome OS for High-stakes Assessments  
• Configuring Chromebook Mobile Devices for Online Testing with the Secure Browser | Turning ChromeVOX Off  
• Configuring Apple Mobile Devices for Online Testing with the Secure Browser | Using Automatic Assessment Configuration  
• Installing the Secure Browser on Desktops and Laptops | Installing the Secure Browser on Mac OS | Cloning the Secure Browser Installation to Other Macs  
• Installing the Secure Browser on Mobile Devices | Installing the Secure Browser on iOS | Guidance on iOS Classroom App and Summative Testing |
| **Updated instructions** (The sections in this list contain substantial edits to existing instructions.) | • Added recommendation for disabling Exposé with Spaces.  
• For all secure browser installation, added a step recommending that all background jobs be scheduled outside of potential testing times (8 a.m. to 3 p.m.).  
• Updated instructions for installing AIR SecureTest Kiosk app on standalone Chromebooks.  
• Reduced the number of folders that must be deleted when resetting a secure browser user profile. |
| **Deleted instructions** | The following instructions have been deleted:  
• Configuring Apple Mobile Devices for Online Testing with the Secure Browser | Configuring for Guided Access |
Sections

This document contains the technology requirements for online CAASPP testing for the 2017–18 test administration. This document 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>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>⚠️</td>
<td><strong>Warning:</strong> This symbol accompanies important information regarding actions that may cause fatal errors.</td>
</tr>
<tr>
<td>🚫</td>
<td><strong>Caution:</strong> This symbol accompanies important information regarding a task that may cause minor errors.</td>
</tr>
<tr>
<td>Element</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td><img src="image" alt="Note" /></td>
<td><strong>Note:</strong> This symbol accompanies additional information that may be of interest.</td>
</tr>
<tr>
<td><img src="image" alt="Additional Resources" /></td>
<td><strong>Additional Resources:</strong> This symbol accompanies a list of URLs for Web pages and/or Web documents that provide additional information.</td>
</tr>
<tr>
<td><img src="image" alt="Tip" /></td>
<td><strong>Tip:</strong> This symbol accompanies useful information on how to perform a task.</td>
</tr>
<tr>
<td><img src="image" alt="file name" /></td>
<td>Monospaced text indicates a directory, file name, or something you enter in a field.</td>
</tr>
<tr>
<td><img src="image" alt="text" /></td>
<td>Bold text in brackets is used to indicate a link or button that is selectable.</td>
</tr>
</tbody>
</table>

## 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, Firefox, and Internet Explorer
- 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 Desktop Operating Systems

Operating systems that become available but do not appear in the following tables are not supported. Do not upgrade to new operating systems on devices that will be used to administer online assessments without ensuring the updates meet the required specifications. The exceptions to this rule are versions of Google Chrome OS for which there is presumed support—updates to Google Chrome OS are presumed to be compatible with CAASPP systems and may be used. See Appendix A for the operating system support plan.

Desktops and Laptops

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>
<thead>
<tr>
<th>Supported Operating Systems</th>
<th>Minimum Requirements</th>
<th>Recommended Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Windows</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 7, 8.0, 8.1 (Professional and Enterprise)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 10 (Professional, Educational, and Enterprise)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Server 2008, 2012, 2016 (thin client)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 1.1 GHZ processor</td>
<td></td>
<td>• 1.4 GHZ processor</td>
</tr>
<tr>
<td>• 512 MB of RAM</td>
<td></td>
<td>• 2 or more GB RAM</td>
</tr>
<tr>
<td>• 200 MB hard drive space</td>
<td></td>
<td>• 16 or more GB hard drive space</td>
</tr>
</tbody>
</table>

**Mac OS X**

• 10.7–10.12 (Support for this version is anticipated upon completion of testing following its release.)
• 10.13 (Support for this version is anticipated upon completion of testing following its release.)

• 1.1 GHZ processor
• 512 MB of RAM
• 200 MB hard drive space

• 1.4 GHZ processor
• 2 or more GB RAM
• 16 or more GB hard drive space
### Supported Operating Systems

<table>
<thead>
<tr>
<th>Supported Operating Systems</th>
<th>Minimum Requirements</th>
<th>Recommended Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux</td>
<td>1.1 GHZ processor</td>
<td>1.4 GHZ processor</td>
</tr>
<tr>
<td></td>
<td>512 MB of RAM</td>
<td>2 or more GB RAM</td>
</tr>
<tr>
<td></td>
<td>200 MB hard drive space</td>
<td>16 or more GB hard drive space</td>
</tr>
<tr>
<td></td>
<td>Required libraries/packages:</td>
<td>Recommended libraries/packages:</td>
</tr>
<tr>
<td></td>
<td>– GTK+ 2.18 or higher</td>
<td>– NetworkManager 0.7 or higher</td>
</tr>
<tr>
<td></td>
<td>– GLib 2.22 or higher</td>
<td>– DBus 1.0 or higher</td>
</tr>
<tr>
<td></td>
<td>– Pango 1.14 or higher</td>
<td>– HAL 0.5.8 or higher</td>
</tr>
<tr>
<td></td>
<td>– X.Org 1.0 or higher (1.7+ recommended)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>– libstdc++ 4.3 or higher</td>
<td></td>
</tr>
<tr>
<td></td>
<td>– libreadline6:i386 (required for Ubuntu only)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>– GNOME 2.16 or higher</td>
<td></td>
</tr>
</tbody>
</table>

**Linux**
- Fedora 25 LTS (Gnome)
- Fedora 26 LTS (Gnome) (Support for this version will begin upon its release.)
- Red Hat Enterprise 6.5
- Ubuntu 14.04, 16.04 LTS (Gnome)

**Minimum Requirements**
- 1.1 GHZ processor
- 512 MB of RAM
- 200 MB hard drive space

**Recommended Specifications**
- 1.4 GHZ processor
- 2 or more GB RAM
- 16 or more GB hard drive space

**Required libraries/packages:**
- 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

### Tablets

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

<table>
<thead>
<tr>
<th>Supported Operating Systems</th>
<th>Supported Tablets</th>
</tr>
</thead>
<tbody>
<tr>
<td>iOS (iPads)</td>
<td>iPad 2, iPad 3, 4th generation (retina display), 5th generation (retina display), iPad Air, iPad Air 2</td>
</tr>
<tr>
<td>9.2, 9.3, 10.0</td>
<td></td>
</tr>
<tr>
<td>11 (Support for this version is anticipated upon completion of testing following its release.)</td>
<td></td>
</tr>
<tr>
<td>Android</td>
<td>Google Nexus 10, Asus Transformer Pad, Asus Memo Pad, Dell Venue 10, HP Pro Slate 10, Samsung Galaxy Tab 4 Education</td>
</tr>
<tr>
<td>5.0, 5.1, 6.0, 7.0 (Nougat)</td>
<td></td>
</tr>
<tr>
<td>Windows</td>
<td>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.</td>
</tr>
<tr>
<td>8.0 (Professional)</td>
<td></td>
</tr>
<tr>
<td>8.1 (Professional and Enterprise)</td>
<td></td>
</tr>
<tr>
<td>10 (Professional, Educational, and Enterprise)</td>
<td></td>
</tr>
</tbody>
</table>

### Chromebooks and Chromebases

**Additional Resources:**

Table 4 lists the supported operating systems for Chromebooks and Chromebases. The American Institutes for Research (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.

**Note:** 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.

### Table 4. Supported Chromebooks

<table>
<thead>
<tr>
<th>Supported Operating Systems</th>
<th>Related Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chrome OS</td>
<td>See Chapter 4, Secure Browser Configuration, for information about installing the secure browser in kiosk mode, a requirement for online testing.</td>
</tr>
<tr>
<td>• 60 (Support for this version will begin upon its release.)</td>
<td></td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Supported Server Host</th>
<th>Supported Server Software</th>
<th>Supported Terminals</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Windows Server 2008 R2</td>
<td>• vSpace Server 8.4</td>
<td>L300, firmware version 1.11.xx</td>
</tr>
<tr>
<td>• Windows Server 2012 R2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Windows Server 2016 R2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Windows 10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• vSpace PRO 10</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Terminal Servers

Table 6 lists the supported terminal servers for use with a thin client device.

### Table 6. Supported Terminal Servers

<table>
<thead>
<tr>
<th>Supported Terminal Servers</th>
<th>Supported Thin Client</th>
</tr>
</thead>
</table>
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 2017–18 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 9.2–9.3 requires Safari 9.

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Accepted Web Browser</th>
<th>TA Sites (inc. DEI)</th>
<th>Student Practice Test</th>
<th>TOMS</th>
<th>ORS</th>
<th>TIDE</th>
<th>IAHSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7 (Professional and Enterprise)</td>
<td>Chrome 60+ (upon release)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Firefox 52+</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Internet Explorer 11</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>8.0 RT</td>
<td>Internet Explorer 11</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>8.0 (Professional and Enterprise)</td>
<td>Chrome 60+ (upon release)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>8.1 (Professional and Enterprise)</td>
<td>Firefox 52+</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Internet Explorer 11</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>10 (Professional, Educational, and Enterprise)</td>
<td>Chrome 60+ (upon release)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Firefox 52+</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Internet Explorer 11</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Edge</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>10 RT</td>
<td>Chrome 60+ (upon release)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Firefox 52+</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Internet Explorer 11</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

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”

Table 7: Supported Web Browsers by Test Administration Web Site

This table provides the supported Web browsers for online systems associated with testing. The only type of browser students use to take online assessments is the secure browser.
### System Requirements

- **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”
  
  TIDE comprises of Completion Status, Roster Management, and Appeals

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Accepted Web Browser</th>
<th>TA Sites (inc. DEI)</th>
<th>Student Practice Test</th>
<th>TOMS</th>
<th>ORS</th>
<th>TIDE</th>
<th>IAHSS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mac OS X</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.7–10.8</td>
<td>Chrome 60+ (upon release)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Firefox 45+</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Safari 7+</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>10.10</td>
<td>Chrome 60+ (upon release)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>10.11</td>
<td>Firefox 52+</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>10.12 (upon release)</td>
<td>Safari 7+</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Linux</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fedora LTS (Gnome)</td>
<td>Chrome 60+ (upon release)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>25–26 (upon release)</td>
<td>Firefox 52+</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Red Hat Enterprise 6.5</td>
<td>Chrome 60+ (upon release)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Firefox 52+</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Ubuntu (LTS) (Gnome)</td>
<td>Chrome 60+ (upon release)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>14.04, 16.04</td>
<td>Firefox 52+</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>iOS</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9.2–9.3</td>
<td>Safari 9</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>10.0, 10.2</td>
<td>Safari 10</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>11.0 (upon release)</td>
<td>Safari 11 (upon release)</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td><strong>Android</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.0, 5.1, 6.0, 7.0 (Nougat)</td>
<td>Chrome 60+ (upon release)</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td><strong>Chrome OS</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>60 (upon release)</td>
<td>Chrome 60+ (upon release)</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>
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.) Use Table 8 to ensure that you deploy a browser with the required capability.

Table 8. Available Audio Settings by Browser

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Browser</th>
<th>System Volume</th>
<th>TTS Volume</th>
<th>TTS Pitch</th>
<th>TTS Rate</th>
<th>Pause</th>
<th>Resume</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>Secure browser</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>Internet Explorer 11 Web browser</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td></td>
<td>Edge Web browser</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td></td>
<td>Chrome Web browsera</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td></td>
<td>Firefox Web browser</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>OS X</td>
<td>Secure browser</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>Safari Web browser</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td></td>
<td>Chrome Web browsera</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Linux</td>
<td>Secure browser</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>Firefox Web browser</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td></td>
<td>Chrome Web browsera</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>iOS</td>
<td>Mobile secure browser</td>
<td>N</td>
<td>Yb</td>
<td>Yb</td>
<td>Yb</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td></td>
<td>Safari Web browser</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Android</td>
<td>Mobile secure browser</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td></td>
<td>Chrome Web browsera</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Chromebook</td>
<td>Secure browser</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td></td>
<td>Chrome Web browsera</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
</tbody>
</table>

a TTS features for practice tests are available on Chrome if explicitly enabled.

b Available for mobile secure browser version 3.1 or later.
Requirements for Peripheral Equipment

Additional Resources:


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, manual, and Bluetooth-based keyboards. 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.
Wireless Keyboards

While wireless keyboards are permissible, local educational agencies should be aware that high-density deployments of wireless keyboards and mice might interfere with each other or with the wireless network. Therefore, they should test the room configuration before the examination date and consider wired alternatives.

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.

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.

• 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 enhanced accessibility accommodation 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

<table>
<thead>
<tr>
<th>Model</th>
<th>Connector</th>
<th>Microphone Included</th>
<th>Hardware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logitech 390</td>
<td>USB (wired)</td>
<td>Yes</td>
<td>All supported desktops, laptops, and Chromebases with USB port</td>
</tr>
<tr>
<td>Panasonic RP-HT21</td>
<td>XBS</td>
<td>No</td>
<td>All supported desktops, laptops, and Chromebases with XBS port</td>
</tr>
<tr>
<td>Logitech analog</td>
<td>3.5 mm</td>
<td>No</td>
<td>iOS, Android tablets with 3.5 mm port</td>
</tr>
<tr>
<td>Plantronics 326</td>
<td>3.5 mm</td>
<td>Yes</td>
<td>All supported desktops, laptops, and Chromebases with 3.5 mm port—except NComputing terminals</td>
</tr>
<tr>
<td>Sennheiser PC 151</td>
<td>3.5 mm</td>
<td>Yes</td>
<td>All supported desktops, laptops, and Chromebases with 3.5 mm port—except NComputing terminals</td>
</tr>
<tr>
<td>Plantronics 355</td>
<td>3.5 mm</td>
<td>Yes</td>
<td>All supported desktops, laptops, and Chromebases with 3.5 mm port—except NComputing terminals</td>
</tr>
<tr>
<td>Generic headphones</td>
<td>3.5 mm</td>
<td>No</td>
<td>All supported desktops, laptops, and Chromebases with 3.5 mm port—except NComputing terminals</td>
</tr>
<tr>
<td>Generic headphones</td>
<td>USB (wired)</td>
<td>No</td>
<td>All supported desktops, laptops, and Chromebases with USB port</td>
</tr>
</tbody>
</table>

**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.
This page is left blank intentionally.
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 following subsections provide guidance on properly configuring your network and lists 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 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.

  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.

- **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**

<table>
<thead>
<tr>
<th>Number of Students Testing Concurrently in School or Building</th>
<th>Average Estimated Bandwidth Consumed During Subsequent Startup of Secure Browser</th>
<th>Average Estimated Bandwidth Consumed During Testing</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>8K bits/second</td>
<td>5–15K bits/second</td>
</tr>
<tr>
<td>50</td>
<td>400K bits/second</td>
<td>250–750K bits/second (0.25–0.75M bits/second)</td>
</tr>
<tr>
<td>100</td>
<td>800K bits/second</td>
<td>500–1500K bits/second (0.5–1.5M bits/second)</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Port/Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>80/Transmission Control Protocol (TCP)</td>
<td>HTTP (initial connection only)</td>
</tr>
<tr>
<td>443/TCP</td>
<td>HTTPS (secure connection)</td>
</tr>
</tbody>
</table>
Whitelisting Test Site URLs
If the school’s filtering system has both internal and external filtering, the URLs for the testing sites (See URLs for Testing Sites) must be whitelisted in both filters. 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. The following subsections discuss the methods used to check those certificates for revocation.

Certificate Revocation List
To use a certificate revocation list, ensure your firewalls allow the URL http://crl.verisign.com/.
Network Diagnostic Tools

**Additional Resources:**

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.

![Figure 1. Sign-in Web page for the training test](image-url)
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: IE v11
Secure Browser: false

Network Diagnostics:
Select Test: Smarter Balanced ELA
Enter the total number of students you would like to test at one time: 200
Run Network Diagnostics Tests

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
- 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

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

<table>
<thead>
<tr>
<th>Testing Device</th>
<th>Ratio of Devices to 802.11g WAP</th>
<th>Ratio of Devices to 802.11n WAP</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11g</td>
<td>20</td>
<td>40</td>
</tr>
<tr>
<td>802.11n</td>
<td>20</td>
<td>40</td>
</tr>
<tr>
<td>Mix of 802.11g and 802.11n</td>
<td>20</td>
<td>40–50 (depending on the mix of wireless cards used)</td>
</tr>
</tbody>
</table>

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. 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, Firefox, and Internet Explorer) 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 on this page, “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:**

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

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.

![Figure 5. Safari Advanced preferences](image)

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

**Configuring Windows for Online Testing with the Secure Browser**

This subsection describes how to configure Windows for online testing.

**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](image)

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

   ![Figure 7. Local Group Policy Editor screen options](image)

5. Select the `Enabled` radio button (Figure 8), and then select [OK].

   ![Figure 8. Finish in the Windows Local Group Policy Editor screen](image)

6. Close the Local Group Policy Editor screen.
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](image)

2. Select the [gpedit] icon in the Apps pane. The Local Group Policy Editor screen opens.


4. In the Setting pane, double-click `Hide entry points for Fast User Switching` (Figure 10).

![Figure 10. Windows Local Group Policy Editor options](image)

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

![Figure 11. Windows Local Group Policy Editor selection](image)
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](image)

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](image)

**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 14, appears.
1. In the left pane, navigate to **Computer Configuration** → **Administrative Templates** → **Windows Components** (indicated in Figure 14).

2. In the Windows Components group in the right pane, scroll down to the [**Tablet PC**] folder icon—indicated in Figure 15—and double-click it.
3. Double-click to select the [Input Panel] icon, which is indicated in Figure 16.

4. 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 17.

5. 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 18 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

![Disable text prediction dialog box](image)

**Figure 18. Disable text prediction dialog box**

6. 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.

7. Close the *Local Group Policy Editor* window.

**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]).
2. Select [Devices] (indicated in Figure 19) and then Typing from the left pane (shown in Figure 20).

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 20.
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 [Start] and then type mouse in the Search programs and files field.
2. Select Mouse from the list of options to open the Mouse Properties dialog box (Figure 21).

![Figure 21. Mouse Properties dialog box](image)

4. From the Devices list, select “Synaptics LuxPad V7.5,” and then select [Settings...] (indicated in Figure 21).
5. Uncheck the Two-Finger Scrolling box, which is indicated in Figure 22.
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:**

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 Web sites 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

Configuring Mac OS X for Online Testing with the Secure Browser

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

Disabling Exposé or Spaces

Mac OS X versions 10.7 through 10.11 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 23).

   ![Figure 23. Select OS X System Preferences](image)

2. Select the [Keyboard] icon (Figure 24). The Keyboard screen opens.

   ![Figure 24. [Keyboard] icon](image)

3. Select the [Keyboard Shortcuts] or [Shortcuts] tab (Figure 25).

   ![Figure 25. [Keyboard Shortcuts] tab](image)

4. In the left panel of the screen, select [Mission Control]. The right panel lists all Mission Control options (Figure 26).
5. In the right panel, clear the following check boxes:
   - **Move left a space**
   - **Move right a space**
   - **Switch to Desktop 1**

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 10.7 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 27). The **Keyboard** screen opens.

   ![Figure 27. Apple System Preferences screen](#)

3. In the **Keyboard** screen, check the **Use all F1, F2, etc. keys as standard function keys** box (Figure 28).
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 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 27).
3. Select the [App Store] icon. The App Store screen opens (Figure 29).

   ![Figure 29. App Store screen](image)

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 30).

![Advanced Preferences options](image)

5. Select [OK].

Disabling Look-Up Gesture

OS X versions 10.7 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 31).
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.
4. Select the Notification Center check box, which is highlighted in Figure 32.

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 10.8.5 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
- Centrify & 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. Access System Preferences.
2. Select the [Keyboard] option (indicated in Figure 33) and then Dictation.
3. Select the Off radio button to turn the Dictation option off (Figure 34).

Disabling Siri

Take these steps to disable the Siri feature:

1. Access the System Preferences.
2. Select [Siri] from the System Preferences options (Figure 35).

![Figure 35. [Siri] button in OS X System Preferences](image)

3. Uncheck the Enable Siri box (indicated in Figure 36).

![Figure 36. Siri system preferences options in OS X](image)

With Siri disabled, the menu bar icon is removed, the [Dock] icon is hidden, the [Tool Bar] icon is removed (if applicable to the student’s Mac), and the Siri service is completely turned off and unable to activate for any reason.

**Configuring Linux for Online Testing with the Secure Browser**

**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 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/](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 and Red Hat—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](http://corefonts.sourceforge.net/) Web page.
- Ubuntu—In a terminal window, enter the following command to install the msttcorefonts package:

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

Configuring Apple Mobile Devices for Online Testing with the Secure Browser

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

**Using Autonomous Single App Mode (ASAM)**

If you have iOS tablets running version 8.0 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.

**TIP:** If you are using iPads with iOS 9.3.2 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:

1. Create a mobile device management profile.
2. (Optional) Restrict features in iOS 9.2 or later.
3. Create a supervisory profile.

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:

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 9.2 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 9.2 or later.

You can restrict features in supervised devices with iOS 9.2 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. If you wish to restrict these features when configuring the MDM profile, you must use a third-party MDM solution.

To restrict features in iOS 9.2 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>
<thead>
<tr>
<th>Feature</th>
<th>Profile Key</th>
<th>Recommended Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dictionary, Share Selected Text</td>
<td><code>&lt;key&gt;allowDefinitionLookup&lt;/key&gt;</code></td>
<td>False</td>
</tr>
<tr>
<td>Predictive Keyboard</td>
<td><code>&lt;key&gt;allowPredictiveKeyboard&lt;/key&gt;</code></td>
<td>False</td>
</tr>
<tr>
<td>Spell Check</td>
<td><code>&lt;key&gt;allowSpellCheck&lt;/key&gt;</code></td>
<td>False</td>
</tr>
<tr>
<td>Auto Correction</td>
<td><code>&lt;key&gt;allowAutoCorrection&lt;/key&gt;</code></td>
<td>False</td>
</tr>
</tbody>
</table>
2. The following snippet turns off the iPad's auto correction feature. The snippets for dictionary, predictive keyboard, and spell check are similar.

```xml
<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 above, 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 37).
3. Select + below the Profiles list (Figure 37) and select [Create New Profile…]. The configuration screen shown in Figure 38 appears.
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 Web site—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.

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 39).

   ![Figure 39. Preferences options](image)

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 37).
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 40).

![Image of Organization Info screen]

**Figure 40. 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 37).

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 41).
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 Web site. (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: MDM profiles for managed iPads override the automatic assessment configuration. If you want to use automatic assessment configuration, delete any existing MDM profiles from the Apple Configurator.

If students are using iPads with iOS 9.3.2 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 42 appears.

![Confirm App Self-Lock](image)

**Figure 42. 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 43). 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.

To remove the Emoji keyboard:

1. Tap the [Settings] icon (Figure 44).
2. Navigate to General → Keyboard.
3. Tap the [Keyboards] icon.
4. Delete *Emoji* from the list by sliding it to the left (Figure 45).

![Emoji keyboard for iOS](image)

**Figure 43. Emoji keyboard for iOS**

**Figure 44. [Settings] icon**

**Figure 45. 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 46).

Disabling Keyboard Functions

Disable keyboard functions by taking the following steps:

1. Under Settings, tap General → Keyboard.
2. Turn off all settings (Figure 47)

Configuring Android for Online Testing with the Secure Browser

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.
The first time you open the mobile secure browser on an Android tablet, you will be prompted to select the secure browser keyboard.

**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. The screenshots were taken with a Samsung Galaxy Tab 2; other Android versions may vary.

1. Select the [Secure Browser] icon on the Home screen (Figure 48).

2. A Change Keyboard message appears; tap [Close] (Figure 49).

3. Tap [Set up input methods] (Figure 50). The Language and Input settings screen opens.
4. Select the check box next to **AIRSecureTest** so that a checkmark appears (Figure 51).

5. You will be prompted to acknowledge that this selection is okay. Select [OK] to continue.
   
   **Note:** This action allows the mobile secure browser to use the secure browser keyboard.

6. Navigate to the secure browser to open it. (You can use the application switcher or go back to Home and select the [Secure Browser] icon.)

7. You will be prompted to change the keyboard. Select [Close] (Figure 52).

8. The Android tablet’s default keyboard will still be selected.

9. Select the checkmark or radio button for the **AIRSecureTest** keyboard (similar to the input methods shown in Figure 53).
10. Select [Continue] (Figure 54). You will be prompted to complete the application launch using the preferred method.

11. Select [AIRSecureTest] (ensure it is shaded and highlighted blue, as it is in Figure 55) and then select [Always].

12. You will need to acknowledge that the secure browser's default settings have changed. (This is a result of selecting the secure browser keyboard.)

13. Select [OK] (Figure 56).
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 4.4 on a Samsung tablet; 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 (Figure 57).

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 58).
Figure 58. Disable the Samsung stylus

Configuring Chromebook Mobile Devices for Online Testing with the Secure Browser

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 58, and version 58 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.
3. From the Restrict Google Chrome version to at most list, select the required version.
4. Select [Save].

![Disabling Auto Updates for Chrome OS](image)
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

2. Select the Do not allow any user to sign-in option from the Restrict sign-in list (Figure 59).

![Figure 59. Chrome Sign-in Settings options](image)

Turning ChromeVOX Off

ChromeVOX may read the nontest elements of the secure browser and the test itself, which poses a construct violation. ChromeVOX should be manually disabled before starting to test. (Future versions of the Mobile Secure Browser will auto disable ChromeVOX.)

To disable ChromeVOX before launching the secure browser:

1. Sign in to the Chromebook.
2. Select the status area, where the account picture appears (Figure 60), or press [Alt] + [Shift] + [S] on the keyboard.

![Figure 60. Chromebook status area](image)

3. Select the [Settings] button, which is shown in Figure 61.

![Figure 61. Chromebook [Settings] button](image)

4. Select the [Show advanced settings] link at the bottom of the Settings screen (Figure 62).

![Figure 62. Chromebook [Show advanced settings] link](image)

5. In the “Accessibility” section, uncheck the Enable Chromevox (Spoken feedback) box indicated in Figure 62.
3. If the secure browser has already been launched, disable ChromeVOX with the keyboard command [Ctrl] + [Alt] + [Z].

Installing CloudReady on PCs and Macs

Additional Resources:
• Google Chrome Web Store—https://chrome.google.com/webstore/
• Neverware Web site—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:
is supported for use with CloudReady;
• has a USB port; and
• can boot from a USB drive.

2. Visit the Neverware Web site 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 64).

![Chromebook Recovery Utility](image)

**Figure 64. 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 65).

![Selecting the CloudReady image](image)

**Figure 65. Selecting the CloudReady image**


14. At the prompt (Figure 66), select the USB drive you inserted in step 7.
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.
This page is left blank intentionally.
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 Smarter Balanced assessments.

However, in extremely rare circumstances, a test administrator 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, Smarter Balanced requires that the monitors 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 2017–18 school year.

<table>
<thead>
<tr>
<th>Operating Systems</th>
<th>Secure Browser</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td></td>
</tr>
<tr>
<td>7 (Professional and Enterprise)</td>
<td>10</td>
</tr>
<tr>
<td>8.0 (Professional and Enterprise)</td>
<td>10</td>
</tr>
<tr>
<td>8.1 (Professional and Enterprise)</td>
<td>10</td>
</tr>
<tr>
<td>10 (Professional, Educational, and Enterprise)</td>
<td>10</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Operating Systems</th>
<th>Secure Browser</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mac OS X</strong></td>
<td></td>
</tr>
<tr>
<td>10.7–10.8</td>
<td>9.5</td>
</tr>
<tr>
<td>10.9–10.12 (upon release)</td>
<td>10</td>
</tr>
<tr>
<td><strong>Linux</strong></td>
<td></td>
</tr>
<tr>
<td>Fedora 25–26 (upon release) LTS (Gnome)</td>
<td>10</td>
</tr>
<tr>
<td>Red Hat Enterprise 6.5</td>
<td>10</td>
</tr>
<tr>
<td>Ubuntu 14.04, 16.04 LTS (Gnome)</td>
<td>10</td>
</tr>
<tr>
<td><strong>iOS (iPads)</strong></td>
<td></td>
</tr>
<tr>
<td>9.2–9.3</td>
<td>AIRSecureTest Mobile Secure Browser</td>
</tr>
<tr>
<td>10.0, 10.2</td>
<td>AIRSecureTest Mobile Secure Browser</td>
</tr>
<tr>
<td>11 (upon release)</td>
<td>AIRSecureTest Mobile Secure Browser</td>
</tr>
<tr>
<td><strong>Android</strong></td>
<td></td>
</tr>
<tr>
<td>5.0, 5.1, 6.0, 7.0 (Nougat)</td>
<td>AIRSecureTest Mobile Secure Browser</td>
</tr>
<tr>
<td><strong>Chrome OS</strong></td>
<td></td>
</tr>
<tr>
<td>60 (upon release)</td>
<td>AIRSecureTest kiosk application</td>
</tr>
</tbody>
</table>

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:**

- CAASPP Secure Browsers Web site—http://ca.browsers.airast.org/

This subsection provides instructions for installing the secure browser on computers running on versions 7, 8.0, 8.1, and 10. (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 Web site and selecting the [Secure Browsers] button.


4. Select the [Windows] tab and then select the [Download Browser] button (shown as highlighted in Figure 67). A dialog box opens.

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 68).

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.

   For more information about proxy settings, see Proxy Settings for Desktop Secure Browsers.

10. Run the secure browser by double-clicking the [CASecureBrowser] shortcut icon on the desktop (shown in Figure 68). 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 Web site and selecting the [Secure Browsers] button.

4. Select the [Windows] tab and then select the [Download Browser] button (shown in Figure 69). A dialog box opens.

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 70). The secure browser opens, displaying the student logon screen. The secure browser fills the entire screen and hides the task bar.

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**

The use of this scenario is strongly discouraged because sharing the secure browser on a network drive installation can compromise the stability and performance of the browser, especially during peak testing times. 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 71). The secure browser opens, displaying the student logon screen. The secure browser fills the entire screen and hides the task bar.
   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:\AssesssmentTesting\. 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:\AssesssmentTesting\, you are creating a new folder c:\AssesssmentTesting\CASecureBrowser.
   c. Copy the shortcut c:\AssesssmentTesting\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.

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 Scripts.
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 machines to search for answers. 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.
Perform an uninstall.

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.

## Installing the Secure Browser on Mac OS X

**Additional Resources:**

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

### Installing the Secure Browser on an Individual Apple Computer

In this scenario, a user installs the secure browser on Apple desktop and laptop computers running Mac OS X 10.7 through 10.12. 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 Web site and selecting the [Secure Browsers] button.


4. Select the [Mac OS X 10.7–10.12] tab and then select the [Download Browser] button (shown as highlighted in Figure 72). A dialog box opens.

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

6. Open Downloads from the dock, and then select CASecureBrowser-OSX.dmg to display its contents (Figure 73).

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 74) and then type your password to enable changes.

![Figure 74. Security & Privacy screen for Mac OS X 10.11](image)

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 74).

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.

   ![Application Support Interface](image)

   **Figure 75. Apple Application Support configuration interface**

   d. Delete the CASecureBrowser folder containing the secure browser (indicated in Figure 75).
   e. Delete the Mozilla folder (also indicated in Figure 75).

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:
- CAASPP Secure Browsers Web site—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 Web site 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 76).
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].
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 [CASecureBrowser] icon on the desktop (shown in Figure 77). The installation script prompts you for the root or superuser password you obtained in step 2.

12. Enter the password. The script installs all dependent libraries and supported voice packs, and creates a [CASecureBrowser] 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 [CASecureBrowser] 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.

**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
- CAASPP Secure Browsers Web site—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 Web site 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 78. (You also can search for AIRSecureTest in the App Store to find the secure browser app.)
5. The AIRSecureTest download Web page, shown in Figure 79, opens.

6. Tap the [Download] cloud [ ] icon, indicated in Figure 79. 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 80 appears on the iPad’s home screen.

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 81), select California.
10. In the Choose Your Assessment Program drop-down list (indicated in Figure 82), select California Assessment System.

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:
- CAASPP Secure Browsers Web site—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 Web site 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 83. (You can also search for AIRSecureTest in the Google Play store to find the secure browser app.)

5. The AIRSecureTest download Web page appears (Figure 84).

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. After installation, an [AIRSecureTest] icon like the one shown in Figure 85 appears on the tablet’s home page.

![AIRSecureTest icon, Android](image)

Figure 85. [AIRSecureTest] icon, Android

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 86), select California.

![Select the state from the Launchpad](image)

Figure 86. Select the state from the Launchpad

10. In the Choose Your Assessment Program drop-down list (shown in Figure 87), select California Assessment of Student Performance and Progress.

![Select the assessment from the Launchpad](image)

Figure 87. Select the assessment from the Launchpad

11. 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.

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 e-mail 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 88, select your language, keyboard, and the wireless network information you acquired from the network administrator, and then select [Continue].

   ![Figure 88. Chromebook Welcome screen](image)

   c. In the Google Chrome OS Terms screen, select [Accept].
4. When the **Sign in** screen appears, wipe data from the Chromebook by taking the following steps:

   a. Press `[Esc] + [Enter] + [Power]`. The screen displays a yellow exclamation point (!) similar to that in Figure 89.

   ![Chrome OS Missing message]

   **Figure 89. Chrome OS Missing message**

   b. Press `[Ctrl] + [D]` to begin developer mode. A message similar to that in Figure 90 will appear.

   ![Turn OS Verification Off message]

   **Figure 90. Turn OS Verification Off message**

   c. Press `[Enter]`. A message similar to that in Figure 91 will appear.

   ![OS Verification Is Off message]

   **Figure 91. OS Verification Is Off message**

   d. Press `[Ctrl] + [D]`. The Chromebook indicates it is transitioning to developer mode (Figure 92). The transition takes approximately 10 minutes, after which the Chromebook reboots.

   ![Preparing for Developer Mode message]

   **Figure 92. Preparing for Developer Mode message**

   e. After the Chromebook reboots, the **OS verification is Off** message (Figure 91) appears again.

   f. Press the [Spacebar] and then press [Enter]. The Chromebook reboots, and the **Welcome** screen appears (Figure 88).
5. In the *Welcome* screen, select your language, keyboard, and a network. The *Join WiFi Network* screen appears (Figure 93).

![Figure 93. Join WiFi Network screen](image)

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 94) appears.

![Figure 94. Chromebook Sign in screen](image)

9. In the *Sign in* screen, press [Ctrl] + [Alt] + [K] to open the *Automatic Kiosk Mode* screen (Figure 95).

![Figure 95. Automatic Kiosk Mode message](image)

10. Select [Enable] and then select [OK] to open the *Sign in* screen (Figure 94).

11. In the *Sign in* screen, enter your e-mail address, select [Next], enter the password, and then select [Next] again.

12. When the desktop opens, select the [Chrome] icon [()] to open Chrome.
13. In the URL bar, enter `chrome://extensions` to open the *Extensions* screen (Figure 96).

![Extensions screen](image)

**Figure 96. Extensions screen**

14. Mark the check box for *Developer Mode* (indicated in Figure 96).

15. Select the [Manage kiosk applications] button—also indicated in Figure 96—to open the *Manage Kiosk Applications* screen (Figure 97).

![Manage Kiosk Applications screen](image)

**Figure 97. 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]. The AIRSecureTest application appears in the Manage Kiosk Applications list.

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 98).

![Figure 98. Chrome Admin console screen](image-url)
4. When the *Device management* screen appears, select the [Chrome Management] link (indicated in Figure 99).

![Chrome Device management screen](image)

**Figure 99. Chrome Device management screen**

5. In the *Chrome Management* screen, select [App Management] (indicated in Figure 100).
6. In the left column of the App Management screen, enter AIRSecureTest or hblfbmjdaalalhifaaajnnodlkiloengc in the Find or Update Apps field (indicated in Figure 101).
7. Select the [Kiosk settings | Deploy this app as a Kiosk App] link (indicated in Figure 102).

8. Select your organization in the Org column on the right (indicated in Figure 103).
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 103).

**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 104).
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 105), select California.

![Figure 105. Select the state from the Launchpad](image)

2. In the Choose Your Assessment Program drop-down list (indicated in Figure 106), the option California Assessment of Student Performance and Progress should already be selected.

![Figure 106. Select the assessment from the Launchpad](image)

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. You can optionally force the secure browser to use specific proxy settings by passing them through the command line. 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 use the domains foo.com and proxy.com. When configuring for a proxy server, use your actual testing domain names as listed in Appendix B, URLs for Testing Systems.

<table>
<thead>
<tr>
<th>Description</th>
<th>System</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run the secure browser without any proxy</td>
<td>Windows</td>
<td>CASecureBrowser.exe -proxy 0 aHR0cHM6Ly9jYS50ZHMuYWlyYXN0Lm9yZy9zdHVkZW50</td>
</tr>
<tr>
<td></td>
<td>Mac 10.7–10.12</td>
<td>./CASecureBrowser -proxy 0 aHR0cHM6Ly9jYS50ZHMuYWlyYXN0Lm9yZy9zdHVkZW50</td>
</tr>
<tr>
<td></td>
<td>Linux</td>
<td>./CASecureBrowser.sh -proxy 0 aHR0cHM6Ly9jYS50ZHMuYWlyYXN0Lm9yZy9zdHVkZW50</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> The commands in Table 15 use the domains foo.com and proxy.com. When configuring for a proxy server, use your actual testing domain names as listed in Appendix B, URLs for Testing Systems.</td>
</tr>
<tr>
<td>Set the proxy for HTTP requests only</td>
<td>Windows</td>
<td>CASecureBrowser.exe -proxy 1:http:foo.com:80 aHR0cHM6Ly9jYS50ZHMuYWlyYXN0Lm9yZy9zdHVkZW50</td>
</tr>
<tr>
<td></td>
<td>Mac 10.7–10.12</td>
<td>./CASecureBrowser -proxy 1:http:foo.com:80 aHR0cHM6Ly9jYS50ZHMuYWlyYXN0Lm9yZy9zdHVkZW50</td>
</tr>
<tr>
<td></td>
<td>Linux</td>
<td>./CASecureBrowser.sh -proxy 1:http:foo.com:80 aHR0cHM6Ly9jYS50ZHMuYWlyYXN0Lm9yZy9zdHVkZW50</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> The commands in Table 15 use the domains foo.com and proxy.com. When configuring for a proxy server, use your actual testing domain names as listed in Appendix B, URLs for Testing Systems.</td>
</tr>
<tr>
<td>Set the proxy for all protocols to mimic the “Use this proxy server for all protocols&quot; of Firefox</td>
<td>Windows</td>
<td>CASecureBrowser.exe -proxy 1:*:foo.com:80 aHR0cHM6Ly9jYS50ZHMuYWlyYXN0Lm9yZy9zdHVkZW50</td>
</tr>
<tr>
<td></td>
<td>Mac 10.7–10.12</td>
<td>./CASecureBrowser -proxy 1:*:foo.com:80 aHR0cHM6Ly9jYS50ZHMuYWlyYXN0Lm9yZy9zdHVkZW50</td>
</tr>
<tr>
<td></td>
<td>Linux</td>
<td>./CASecureBrowser.sh -proxy 1:*:foo.com:80 aHR0cHM6Ly9jYS50ZHMuYWlyYXN0Lm9yZy9zdHVkZW50</td>
</tr>
</tbody>
</table>
### Proxy Settings for Desktop Secure Browsers

#### Description

<table>
<thead>
<tr>
<th>Description</th>
<th>System</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Specify the URL of the PAC file</strong></td>
<td>Windows</td>
<td>C ASecureBrowser.exe -proxy 2:proxy.com aHR0cHM6Ly9jYS50ZHSuYWlyYWZ0ZS50ZHMuYWlyYWZ0ZS50ZHSuYWlyYWZ0ZS50ZHMuYWlyYWZ0ZS</td>
</tr>
<tr>
<td></td>
<td>Mac 10.7–10.12</td>
<td>./C ASecureBrowser -proxy 2:proxy.com aHR0cHM6Ly9jYS50ZHSuYWlyYWZ0ZS50ZHMuYWlyYWZ0ZS50ZHSuYWlyYWZ0ZS</td>
</tr>
<tr>
<td></td>
<td>Linux</td>
<td>./C ASecureBrowser.sh -proxy 2:proxy.com aHR0cHM6Ly9jYS50ZHSuYWlyYWZ0ZS50ZHMuYWlyYWZ0ZS50ZHSuYWlyYWZ0ZS</td>
</tr>
<tr>
<td><strong>Auto detect proxy settings</strong></td>
<td>Windows</td>
<td>C ASecureBrowser.exe -proxy 4 aHR0cHM6Ly9jYS50ZHSuYWlyYWZ0ZS50ZHMuYWlyYWZ0ZS50ZHSuYWlyYWZ0ZS</td>
</tr>
<tr>
<td></td>
<td>Mac 10.7–10.12</td>
<td>./C ASecureBrowser -proxy 4 aHR0cHM6Ly9jYS50ZHSuYWlyYWZ0ZS50ZHMuYWlyYWZ0ZS50ZHSuYWlyYWZ0ZS</td>
</tr>
<tr>
<td></td>
<td>Linux</td>
<td>./C ASecureBrowser.sh -proxy 4 aHR0cHM6Ly9jYS50ZHSuYWlyYWZ0ZS50ZHMuYWlyYWZ0ZS50ZHSuYWlyYWZ0ZS</td>
</tr>
<tr>
<td><strong>Use the system proxy setting (default)</strong></td>
<td>Windows</td>
<td>C ASecureBrowser.exe -proxy 5 aHR0cHM6Ly9jYS50ZHSuYWlyYWZ0ZS50ZHMuYWlyYWZ0ZS50ZHSuYWlyYWZ0ZS</td>
</tr>
<tr>
<td></td>
<td>Mac 10.7–10.12</td>
<td>./C ASecureBrowser -proxy 5 aHR0cHM6Ly9jYS50ZHSuYWlyYWZ0ZS50ZHMuYWlyYWZ0ZS50ZHSuYWlyYWZ0ZS</td>
</tr>
<tr>
<td></td>
<td>Linux</td>
<td>./C ASecureBrowser.sh -proxy 5 aHR0cHM6Ly9jYS50ZHSuYWlyYWZ0ZS50ZHMuYWlyYWZ0ZS50ZHSuYWlyYWZ0ZS</td>
</tr>
</tbody>
</table>

---

### 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. Create a new desktop shortcut in Windows Explorer by navigating to `C:\Program Files (x86)` (64 bit) or `C:\Program Files\CASecureBrowser` (32 bit), right-clicking the file `CASecureBrowser.exe`, and then selecting *Send To → Desktop (create shortcut)*.
   c. Right-click the desktop shortcut for the secure browser and select *Properties*.
   d. Select the [**Shortcut**] tab.
4. In the Target field, modify the command as specified in Table 15. For example:

```
"C:\Program Files (x86)\CASecureBrowser\CASecureBrowser.exe" -proxy 1:http:foo.com:80 aHR0cHM6Ly9jYS50ZHMuYWlyYXN0Lm9yZy9zdHVkZW50
```

5. Select [OK].

**Modifying Desktop Shortcuts on Mac OS X**

1. In Finder, navigate to Applications → Utilities and open Terminal.
2. Change to the desktop directory.
   ```
   cd ~/Desktop
   ```
3. Create a file `securebrowser.command` on the desktop using a text editor such as pico.
   ```
   pico securebrowser.command.
   ```
4. Copy or type the following lines:
   ```
   #!/bin/sh
   /Applications/CASecureBrowser.app/Contents/MacOS/./
   CASecureBrowser -proxy 1:http:foo.com:80 &
   aHR0cHM6Ly9jYS50ZHMuYWlyYXN0Lm9yZy9zdHVkZW50
   ```
5. Be sure to specify the complete path to the secure browser and the desired proxy option. Ensure the command ends with an ampersand (&). Save the file and exit the editor by pressing [Ctrl] + [O], [Enter], and then [Ctrl] + [X].
6. Apply execute permission to the file. In Terminal, type
   ```
   chmod a+x securebrowser.command
   ```
7. Close Terminal.
8. Select the `securebrowser.command` icon on the desktop. The secure browser opens with the proxy setting you configured.
This page is left blank intentionally.
Appendixes
Appendix A. Operating System Support Plan for the 2017–18 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

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. For major version upgrades to a device operating system released before May 1, AIR will provide a secure browser update for that operating system version for the upcoming school year. For example, if an upgrade is released in April 2018, AIR will provide a secure browser that works on that upgrade for the 2017–18 school year.

For major version upgrades to a device operating system released after May 1, AIR will not provide a secure browser update until the following school year, and the existing secure browser may or may not be compatible with the upgrade. For example, if an upgrade is released in June 2017, AIR will not provide a secure browser that works on that upgrade until the 2018–19 school year. Exceptions may be made on a case-by-case basis.

A “minor version upgrade” is usually denoted by an increase in a number after a decimal point. For example, the upgrade from Mac OS 10.1 to 10.2 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 lists the operating systems and the anticipated end-of-support dates. The shaded cells in Table 16 indicate that AIR ends support for operating systems after the 2018–19 school year.

Table 16. Supported Operating Systems

<table>
<thead>
<tr>
<th>Supported Operating Systems</th>
<th>Release Date</th>
<th>Anticipated End-of-Support Date</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows(^a)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8.0, 8.1</td>
<td>Oct. 2012</td>
<td>End of 2021–22 School Year</td>
<td>AIR’s support for a Windows operating systems 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.</td>
</tr>
<tr>
<td>10</td>
<td>July 2015</td>
<td>End of 2025–26 School Year</td>
<td></td>
</tr>
<tr>
<td>Server 2008</td>
<td>Oct. 2009</td>
<td>End of 2018–19 School Year</td>
<td></td>
</tr>
<tr>
<td>Server 2012</td>
<td>April 2012</td>
<td>End of 2021–22 School Year</td>
<td></td>
</tr>
<tr>
<td>Server 2016</td>
<td>Sept. 2016</td>
<td>End of 2025–26 School Year</td>
<td></td>
</tr>
<tr>
<td>Mac OS X (Intel)(^a)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.7</td>
<td>July 2011</td>
<td>End of 2020–21 School Year</td>
<td>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.</td>
</tr>
<tr>
<td>10.8</td>
<td>July 2012</td>
<td>End of 2021–22 School Year</td>
<td></td>
</tr>
<tr>
<td>10.9</td>
<td>Oct. 2013</td>
<td>End of 2022–23 School Year</td>
<td></td>
</tr>
<tr>
<td>10.10</td>
<td>Oct. 2014</td>
<td>End of 2023–24 School Year</td>
<td></td>
</tr>
<tr>
<td>10.11</td>
<td>Oct. 2015</td>
<td>End of 2024–25 School Year</td>
<td></td>
</tr>
<tr>
<td>10.12(^b)</td>
<td>Sept. 2016</td>
<td>End of 2025–26 School Year</td>
<td></td>
</tr>
<tr>
<td>10.13(^b)</td>
<td>Pending</td>
<td>Pending</td>
<td></td>
</tr>
<tr>
<td>Linux(^c)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fedora 25 LTS (Gnome)</td>
<td>Nov. 2016</td>
<td>End of 2017–28 School Year</td>
<td>Official Fedora support typically ends one to two years after a release.</td>
</tr>
<tr>
<td>Fedora 26 (LTS Gnome)</td>
<td>July 2017</td>
<td>End of the 2018–19 School Year</td>
<td></td>
</tr>
<tr>
<td>Ubuntu 14.04 LTS (Gnome)</td>
<td>April 2014</td>
<td>End of 2018–19 School Year</td>
<td>Ubuntu typically supports long term support (LTS) distributions for five years after a release.</td>
</tr>
<tr>
<td>Ubuntu 16.04 LTS (Gnome)</td>
<td>April 2016</td>
<td>End of 2020–21 School Year</td>
<td></td>
</tr>
<tr>
<td>Supported Operating Systems</td>
<td>Release Date</td>
<td>Anticipated End-of-Support Date</td>
<td>Notes</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------------</td>
<td>---------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td><strong>iOS</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8.0–8.2</td>
<td>Sept. 2014</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.0&lt;sup&gt;b&lt;/sup&gt;</td>
<td>Fall 2016</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Android</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| 5.0 (Lollipop)–6.0 (Marshmallow) | Nov. 2014; rolling | Android operating systems are released on a rolling basis. AIR supports the three most recent minor releases of Android. | Supported tablets:  
- Google Nexus 10  
- Asus Transformer Pad  
- Asus Memo Pad  
- Dell Venue 10  
- HP Pro Slate 10  
- Samsung Galaxy Tab 4 Education |
| 7.0 (Nougat)<sup>d</sup>    | Aug. 2016    |                                 |       |
| **Chrome OS**               |              |                                 |       |
| 60 and up                   | Jan. 2016; rolling | For a given school year, AIR supports the version of Chrome OS available at the start of that school year and any subsequent version. For example if Chrome OS version 51 is available at the start of school year 2017–18, AIR supports that version and any other version released during that school year. | Google releases new versions of Chrome OS every six weeks. Support may require updating the Chrome kiosk application. |

<sup>a</sup> If Microsoft or Apple ends support for an operating system sooner than 10 years after its release, then AIR will stop supporting that system after one full school year.

<sup>b</sup> Support for this version depends on its availability at the start of the school year.

<sup>c</sup> For Linux distributions, AIR will end support at the end of the school year after the official distributor’s announced end-of-life support date.

<sup>d</sup> Android 7.0 has been released but is not yet formally supported, pending its inclusion in the Google for Education program.
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 17 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 user name 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>
<thead>
<tr>
<th>Table 17. URLs for Nontesting Sites</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Destination</strong></td>
</tr>
<tr>
<td>CAASPP Portal</td>
</tr>
<tr>
<td>Secure browser installation files</td>
</tr>
<tr>
<td>TOMS</td>
</tr>
<tr>
<td>Single Sign On System</td>
</tr>
</tbody>
</table>
URLs for Testing Sites

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

Test Administrator and Student Testing Web Sites

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.

<table>
<thead>
<tr>
<th>Systems</th>
<th>URLs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test Administrator and Student Testing Sites</td>
<td>*.airast.org</td>
</tr>
<tr>
<td>Assessment Viewing Application</td>
<td>*.tds.airast.org</td>
</tr>
<tr>
<td></td>
<td>*.cloud1.tds.airast.org</td>
</tr>
<tr>
<td></td>
<td>*.cloud2.tds.airast.org</td>
</tr>
<tr>
<td>Certificate revocation list</td>
<td><a href="http://crl.verisign.com/">http://crl.verisign.com/</a></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>media.merriam-webster.com</td>
<td>64.124.231.250</td>
</tr>
<tr>
<td><a href="http://www.dictionaryapi.com">www.dictionaryapi.com</a></td>
<td>64.124.231.250</td>
</tr>
</tbody>
</table>
# Appendix C. Technology Coordinator Checklist

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

<table>
<thead>
<tr>
<th>Activity</th>
<th>Estimated Time to Complete</th>
<th>Target Completion Date</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that all of your school's devices that will be used for online testing meet the operating system requirements.</td>
<td>5–10 hours</td>
<td>3–4 weeks before testing begins in your school</td>
<td>Chapter 1, System Requirements</td>
</tr>
<tr>
<td>Verify that your school’s network and Internet are properly configured for testing, conduct network diagnostics, and resolve any issues.</td>
<td>5–10 hours</td>
<td>3–4 weeks before testing begins in your school</td>
<td>Chapter 2, Network Configuration</td>
</tr>
<tr>
<td>Confirm that URLs for testing sites and the online dictionary and thesaurus have been whitelisted on your server.</td>
<td>30 minutes</td>
<td>3–4 weeks before testing begins in your school</td>
<td>Appendix B, URLs for Testing Systems</td>
</tr>
<tr>
<td>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.</td>
<td>5–10 hours</td>
<td>3–4 weeks before testing begins in your school</td>
<td>Turn Off Background Jobs</td>
</tr>
<tr>
<td>Install the secure browser on all devices that will be used for testing.</td>
<td>5–10 hours</td>
<td>3–4 weeks before testing begins in your school</td>
<td>Chapter 4, Secure Browser Configuration</td>
</tr>
<tr>
<td>Review software requirements for each operating system.</td>
<td>5–10 hours</td>
<td>1–2 weeks before testing begins in your school</td>
<td>Chapter 3, Software Configuration</td>
</tr>
<tr>
<td>Enable pop-up windows on student devices.</td>
<td>5–10 hours</td>
<td>1–2 weeks before testing begins in your school</td>
<td>Enabling Pop-Up Windows</td>
</tr>
<tr>
<td>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.</td>
<td>5–10 hours</td>
<td>1–2 weeks before testing begins in your school</td>
<td>Disabling Fast User Switching in Windows</td>
</tr>
<tr>
<td>On Mac 10.7–10.12 devices, disable Spaces or Exposé in Mission Control.</td>
<td>5–10 hours</td>
<td>1–2 weeks before testing begins in your school</td>
<td>Disabling Exposé or Spaces</td>
</tr>
<tr>
<td>On iPads, ensure that Autonomous Single App Mode is enabled.</td>
<td>5–10 hours</td>
<td>1–2 weeks before testing begins in your school</td>
<td>Using Autonomous Single App Mode (ASAM)</td>
</tr>
<tr>
<td>Activity</td>
<td>Estimated Time to Complete</td>
<td>Target Completion Date</td>
<td>Reference</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>---------------------------</td>
<td>---------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>On <strong>iOS</strong> devices, ensure that features that might pose a security risk are disabled.</td>
<td>5–10 hours</td>
<td>1–2 weeks before testing begins in your school</td>
<td>Configuring Apple Mobile Devices for Online Testing with the Secure Browser</td>
</tr>
<tr>
<td>On <strong>Android</strong> tablets, ensure that the secure browser keyboard is enabled.</td>
<td>5–10 hours</td>
<td>1–2 weeks before testing begins in your school</td>
<td>Configuring Android for Online Testing with the Secure Browser</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Number of devices available for testing at once:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of students who need to take the test:</td>
</tr>
<tr>
<td>Number of test administrators who need a device:</td>
</tr>
<tr>
<td>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.</td>
</tr>
<tr>
<td>Number of hours that must be scheduled to administer the test: (students + test administrators) x hours ÷ devices =</td>
</tr>
</tbody>
</table>

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 x 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 TechNet Assign User Logon Scripts Web page—

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`.

**TIP:** See the Microsoft TechNet topic Assign User Logon Scripts for additional information about creating a group policy object that executes a logon script.

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 107, appears.

![Figure 107. The Local Group Policy Editor window](image)

2. Expand Local Computer Policy → User Configuration → Windows Settings → Scripts (Logon/Logoff) (indicated in Figure 107).

3. Select **Logon** and then select **Properties**. The Logon Properties dialog box appears.
4. Select [Add] (indicated in Figure 108). The Add a Script dialog box appears.

5. Select [Browse...] (indicated in Figure 109) and navigate to the logon.bat you want to run.

6. Select [OK] (also indicated in Figure 109) 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\n   C:\Users\username\AppData\Roaming\AIR\n   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 10.7 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 110).
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 (CalTAC).

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 CalTAC, you will be asked to provide as much detail as possible about the issue(s) you encountered.

CalTAC
Hours: 7 a.m. to 5 p.m., Monday–Friday
Toll-Free Phone Support: 800-955-2954
E-mail Support: caltac@ets.org
Web site: 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.