Technical Specifications for Online Testing Manual

2015-16 Administration

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

Section I. Introduction to the Technical Specifications for Online Testing Manual ..............................................1
What’s New in 2015-16 ......................................................................................................................................1
Manual Content ...............................................................................................................................................2
Document Conventions .................................................................................................................................2
Intended Audience .........................................................................................................................................2
Other Resources .............................................................................................................................................3

Section II. Network Configuration and Testing .................................................................................................4
Network Configuration .....................................................................................................................................4
Guidance for Determining Required Bandwidth .............................................................................................4
Required Ports and Protocols .........................................................................................................................5
Configuration for Domain Name Resolution .................................................................................................5
Configuring Session Timeouts .......................................................................................................................5
Data Caching .................................................................................................................................................5
Configuring Quality of Service and Traffic Shaping .....................................................................................6
Configuring for Certificate Revocations ....................................................................................................6
Network Diagnostic Tools ...............................................................................................................................6
American Institutes for Research’s (AIR’s) Network/Bandwidth Diagnostic Tool ........................................6
Windows-Specific Tools ................................................................................................................................8
OS X-Specific Tools .....................................................................................................................................8
Multi-Platform Tools ...................................................................................................................................8

Section III. Hardware Configuration ................................................................................................................9
Connections between Printers and Testing Devices .......................................................................................9
Wireless Networking and Determining the Number of Wireless Access Points ........................................9
Hardware for Braille Testing ..........................................................................................................................9

Section IV. Software Configuration ................................................................................................................10
Configuring Commercially Available Browsers ............................................................................................10
Enabling Pop-Up Windows .............................................................................................................................10
Requirements for Flash ..................................................................................................................................11
Optimal Installation Scenario for Secure Browsers .......................................................................................11
Configuring Windows for Online Testing ......................................................................................................11
Disabling Fast User Switching .......................................................................................................................11
Enabling Web Fonts in Internet Explorer 10 and 11 ..................................................................................16
Installing Windows Media Pack for Windows 8.1 N and KN ....................................................................17
Configuring Mac OS X for Online Testing .....................................................................................................18
Disabling Exposé or Spaces ...........................................................................................................................18
Disabling Application Launches from Function Keys ..................................................................................19
Disabling Updates to Third-Party Apps .........................................................................................................20
Disabling Updates to iTunes .........................................................................................................................20
Disabling Spaces and Application Launches from the Command Line ......................................................21
Disabling Spaces and Application Launches on Remote Devices ................................................................22
Configuring Linux for Online Testing ........................................................................................................22
Adding the Verdana Font ...............................................................................................................................22
Adding Flash ..................................................................................................................................................22
Configuring Mobile Devices ..........................................................................................................................22
Configuring for Guided Access on iOS ........................................................................................................22
Configuring Using Autonomous Single App Mode ....................................................................................24
Removing the Emoji Keyboard from an iOS Device ....................................................................................29
Enabling the Secure Browser Keyboard on Android ..................................................................................30
Installing CloudReady on PCs and Macs ......................................................................................................33
Configurations for Braille Requirements .....................................................................................................34

Section V. Text-to-Speech Requirements .........................................................................................................35
Overview of Text-to-Speech ...........................................................................................................................35
Using Text-to-Speech .....................................................................................................................................35
How the Secure Browser Selects Voice Packs .............................................................................................35
About NeoSpeech Voice Packs for Windows ...............................................................................................35
Configuring Windows Text-to-Speech Settings ..........................................................................................36
Configuring OS X Text-to-Speech Settings ..................................................................................................38
Configuring Linux Text-to-Speech Settings ..................................................................................................40

Appendix A. URLs for Testing Systems ........................................................................................................41
URLs for Nontesting Sites ..............................................................................................................................41
URLs for Testing Sites ....................................................................................................................................41
Test Administrator and Student Testing Web Sites ......................................................................................41
List of Tables
Table 1. Document Conventions ......................................................................................... 2
Table 2. Average Bandwidth Used by Secure Browser for Testing ........................................ 5
Table 3. Ports and Protocols for the TDS ........................................................................... 5
Table 4. Domain Names for OCSP ...................................................................................... 6
Table 5. Recommended Ratios of Devices to Wireless Access Points ................................. 9
Table 6. Flash Requirements ............................................................................................... 11
Table 7. Profile Keys for Features in iOS 8.1.3 or Later ...................................................... 24
Table 8. Voice Packs on Mobile Versions of the Secure Browser ........................................ 35
Table 9. Voice Packs Recognized by Secure Browsers—Windows ........................................ 36
Table 10. Voice Packs Recognized by Secure Browsers—OS X ......................................... 38
Table 11. Packages that Include Supported Voice Packs on Linux Distributions ................ 40
Table 12. URLs for Nontesting Sites ..................................................................................... 41
Table 13. URLs for Testing Web Sites .................................................................................. 41
Table 14. URLs for Online Dictionaries and Thesauruses .................................................... 42

List of Figures
Figure 1. Sign In Web page for the training test .................................................................... 7
Figure 2. Run the diagnostics test ....................................................................................... 7
Figure 3. Windows XP [User Accounts] icon .................................................................... 12
Figure 4. Windows XP User Accounts dialog box ............................................................... 12
Figure 5. Windows Search box ........................................................................................... 12
Figure 6. Local Policy Editor window options ................................................................. 13
Figure 7. Finish in the Windows Local Group Policy Editor window ................................... 13
Figure 8. Windows Search box ........................................................................................... 13
Figure 9. Windows Registry Editor options .................................................................... 13
Figure 10. Windows Registry Editor entry ........................................................................ 14
Figure 11. Windows Search charm ................................................................................... 14
Figure 12. Windows Local Group Policy Editor options .................................................... 14
Figure 13. Windows Local Group Policy Editor selection .................................................. 15
Figure 14. Windows Run dialog box ................................................................................. 15
Figure 15. Notification in the Windows Command window ................................................ 15
Figure 16. Internet Explorer Internet Options dialog box .................................................. 16
Figure 17. Internet Explorer Security Settings dialog box .................................................. 17
Figure 18. Select OS X System Preferences .................................................................... 18
Figure 19. [Keyboard] icon ............................................................................................. 18
Figure 20. [Keyboard Shortcuts] tab ................................................................................ 18
Figure 21. OS X Exposé panel .......................................................................................... 18
Figure 22. OS X Mission Control options .................................................................... 19
Figure 23. Apple System Preferences window ................................................................... 19
Figure 24. Keyboard options .......................................................................................... 20
Figure 25. App Store window .......................................................................................... 20
Figure 26. Advanced Preferences dialog box .................................................................... 21
Figure 27. [Settings] icon ............................................................................................. 23
Figure 28. Guided Access options .................................................................................. 23
Figure 29. Keyboard Settings for iOS 8.1 (other versions of iOS are similar) ....................... 23
Figure 30. Settings window in Apple Configurator ............................................................. 26
Figure 31. Create New Profile configuration window ....................................................... 26
Figure 32. Preferences window ....................................................................................... 27
Figure 33. Organization Info window .............................................................................. 28
Figure 34. Apple Configurator window ........................................................................... 28
Figure 35. Emoji keyboard for iOS ............................................................................... 29
Figure 36. [Settings] icon ............................................................................................. 29
CAASPP System

Figure 37. Keyboards configuration interface
Figure 38. [Secure Browser] icon
Figure 39. Change Keyboard for the secure browser keyboard pop-up message
Figure 40. Choose input method dialog box
Figure 41. Language and input settings options
Figure 42. Change Keyboard for the secure browser keyboard pop-up message
Figure 43. Choose input method dialog box
Figure 44. Continue the application launch
Figure 45. Complete the application launch
Figure 46. Clear default settings pop-up message
Figure 47. Chromebook Recovery Utility
Figure 48. Selecting the CloudReady image
Figure 49. CloudReady media insertion prompt
Figure 50. Windows Control Panel window
Figure 51. Speech Recognition configuration options in Windows
Figure 52. Default text-to-speech preferences in Windows
Figure 53. Select OS X System Preferences
Figure 54. OS X System Preferences
Figure 55. OS X Dictation & Speech options

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

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</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>CAAs</td>
<td>California Alternate Assessments</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>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>ISP</td>
<td>Internet service provider</td>
</tr>
<tr>
<td>LEA</td>
<td>local educational agencies</td>
</tr>
<tr>
<td>Mbps</td>
<td>megabits per second</td>
</tr>
<tr>
<td>MDM</td>
<td>mobile device management</td>
</tr>
<tr>
<td>OCSP</td>
<td>Online Certificate Status Protocol</td>
</tr>
<tr>
<td>ORS</td>
<td>Online Reporting System</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of Service</td>
</tr>
<tr>
<td>SoX</td>
<td>Sound eXchange</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>WAP</td>
<td>wireless access points</td>
</tr>
</tbody>
</table>
Section I. Introduction to the Technical Specifications for Online Testing Manual

This manual provides information about device hardware, software, and network configurations for running various testing applications used in California Assessment of Student Performance and Progress testing.

The System Requirements for Online Testing lists the minimum hardware and software requirements for online testing. Ensure your device hardware complies with those requirements before undertaking the tasks described in this manual.

What’s New in 2015–16

<table>
<thead>
<tr>
<th>Feature</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration of the California Alternate Assessments (CAAs) Online Assessments requires secure browser</td>
<td>In addition to being used to take the Smarter Balanced Online Summative and Interim Assessments, the secure browser must also be used to take the CAA operational tests.</td>
</tr>
<tr>
<td>System requirements as a separate manual</td>
<td>System requirements have been moved from the Secure Browser Installation Manual to a separate manual, the System Requirements Manual, which will be posted to the California Assessment of Student Performance and Progress (CAASPP) Instructions and Manuals Web page at <a href="http://www.caaspp.org/administration/instructions/">http://www.caaspp.org/administration/instructions/</a>.</td>
</tr>
</tbody>
</table>
| Updated desktop secure browsers                                        | The secure browser for all platforms except for Mac OSX 10.5 has been updated to version 8.x. Please note the following about the updated secure browsers:  
  • Secure browsers do not require uninstallation.  
  • Secure browsers now have auto update capability.  
  • Icons for version 8.x of the secure browser no longer include version numbers on them (except for the secure browser for Mac OSX 10.5, which is still version 10.5).  
  • The secure browser for Mac OSX 10.5 is version 6.5; it does not require updating for the 2015–16 CAASPP administration. |
| Supported operating systems                                            | The list of supported operating systems, included in the System Requirements Manual, has been updated. |
| Updated functionality for the current secure browser                  | The secure browser no longer requires separate installation of the Active X controls to ensure secure browser security. (Does not apply to version 6.5.) |
| Auto update                                                            | The secure browser now has auto update capability. |
| NeoSpeech Voice Packs                                                  | The NeoSpeech Voice Packs are available for use with the secure browser for the 2015–16 test administration. These voice packs are available for download through the Test Operations Management System (TOMS). See the NeoSpeech Installation Guide that accompany the NeoSpeech Voice Packs in TOMS for instructions on downloading and installing them. You must have a user role assignment that grants you access to TOMS to download this software. |
Manual Content

This guide contains the following sections:

- **Section II, Network Configuration and Testing**, provides information about configuring networks and lists helpful networking diagnostic tools.

- **Section III, Hardware Configuration**, provides guidance regarding the proper infrastructure for printers and wireless access points.

- **Section IV, Software Configuration**, outlines configurations for operating systems (desktop, laptop, and mobile).

- **Section V, Text-to-Speech Requirements**, outlines configurations for enabling text-to-speech settings on desktop operating systems. This section also lists the voice packs recognized by the secure browser on those operating systems.

- **Appendix A, URLs for Testing Sites**, lists URLs that should be whitelisted in your firewalls.

- **Appendix B, Technology Coordinator Checklist**, lists the activities required to prepare a facility for online testing.

- **Appendix C, Scheduling Online Testing**, provides a worksheet for estimating the required time to administer an online test.

- **Appendix D, California Technical Assistance Center for LEA CAASPP Coordinators**, provides Help Desk information.

Document Conventions

Table 1 describes the conventions appearing in this user guide.

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Warning" /></td>
<td><strong>Warning:</strong> This symbol accompanies important information regarding actions that may cause fatal errors.</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="Tip" /></td>
<td><strong>Tip:</strong> This symbol accompanies useful information on how to perform a task.</td>
</tr>
<tr>
<td><code>filename</code></td>
<td>Monospaced text indicates a directory, filename, or something you enter in a field.</td>
</tr>
<tr>
<td><code>[text]</code></td>
<td>Bold text in brackets is used to indicate a link or button that is selectable.</td>
</tr>
</tbody>
</table>

Intended Audience

This publication is intended for technology coordinators responsible for configuring the hardware, software, and network in a school’s online testing environment. You 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

- Configuring Web browsers—Settings in Chrome, Safari, Firefox, and Internet Explorer
Other Resources

- For information about supported operating systems, see the System Requirements for Online Testing at http://www.caaspp.org/rsc/pdfs/CAASPP.system-requirements-manual.2016.pdf.


- For information about supported hardware and software for Braille testing as well as information about configuring Job Access with Speech®, see the Braille Requirements and Testing Manual at http://www.caaspp.org/rsc/pdfs/CAASPP.braille-requirements.2016.pdf.

These resources, as well as test administration manuals, are available on the California Assessment of Student Performance and Progress Instructions and Manuals Web page at http://www.caaspp.org/administration/instructions/.
Section II. 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 sections provide guidance on properly configuring your network, and lists popular tools for diagnosing network bottlenecks.

Network Configuration

This section 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 or simulations 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 2 displays the estimated average bandwidth used by the secure browser for testing. When designing your network for online testing, ensure that the available bandwidth can support these values.

<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&lt;sup&gt;a&lt;/sup&gt;</th>
<th>Average Estimated Bandwidth Consumed During Testing&lt;sup&gt;b&lt;/sup&gt;</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>

<sup>a</sup> 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.

<sup>b</sup> The values in this column are based on averages from tests in a variety of subjects.

### Required Ports and Protocols

Table 3 lists the ports and protocols used by the TDS. Ensure that all content filters, firewalls, and proxy servers are open accordingly.

<table>
<thead>
<tr>
<th>Port/Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>80/Transfer Control Protocol (TCP)</td>
<td>HTTP (initial connection only)</td>
</tr>
<tr>
<td>443/TCP</td>
<td>HTTPS (secure connection)</td>
</tr>
</tbody>
</table>

### Configuration for Domain Name Resolution

Appendix A, URLs for Testing Sites, lists the domain names for California Assessment of Student Performance and Progress testing and nontesting applications. Ensure the testing devices have access to a 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 (QoS), ensure the URLs in Appendix A, URLs for Testing Sites, have high priority.

Configuring for Certificate Revocations

Testing servers present certificates to the clients. The following sections 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/.

Online Certificate Status Protocol

To use the Online Certificate Status Protocol (OCSP), ensure your firewalls allow the domain names listed in Table 4. The values in the Patterned column are preferred because they are more robust.

<table>
<thead>
<tr>
<th>Patterned</th>
<th>Fully Qualified</th>
</tr>
</thead>
<tbody>
<tr>
<td>*.thawte.com</td>
<td>oscp.thawte.com</td>
</tr>
<tr>
<td>*.geotrust.com</td>
<td>oscp.geotrust.com</td>
</tr>
<tr>
<td>*.ws.symantec.com</td>
<td>oscp.ws.symantec.com</td>
</tr>
</tbody>
</table>

If your firewall is configured to check only Internet protocol (IP) addresses, do the following:

2. Add the retrieved IP addresses to your firewall’s whitelist. Do not replace any existing IP addresses.

Network Diagnostic Tools

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

AIR provides a diagnostic tool that can be directly accessed from the student sample test logon page or in the “Additional Resources” box on most caaspp.org Web pages.

1. On the sample test logon page (accessed by selecting the [Student Interface Practice and Training Tests] button on the Online Practice and Training Tests Web page at http://www.caaspp.org/practice-and-training/index.html), select the [Run Diagnostics] link in the lower-left corner of the sign-in page (Figure 1) to open the Diagnostic Screen Web page.
2. In the **Network Diagnostics** section, select a test.
3. Select the approximate number of students who may take that test **at one time**.
4. Select **[Run Network Diagnostics Tests]**.

   **Figure 2. Run the diagnostics test**
Network Configuration and Testing | Network Diagnostic Tools

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

**PRTG Traffic Grapher**


**NTttcp**

NTttcp ([www.microsoft.com/whdc/device/network/TCP_tool.mspx](http://www.microsoft.com/whdc/device/network/TCP_tool.mspx)) 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 over a time period.

OS X-Specific Tools

**Network Utility.app**

This tool is built into OS X.

Multi-Platform Tools

**Wireshark**

Wireshark ([www.wireshark.org](http://www.wireshark.org)) is a network protocol analyzer. It has a large feature set and runs on most platforms including Windows, OS X, and Linux.

**TCPDump**

TCPDump ([http://sourceforge.net/projects/tcpdump](http://sourceforge.net/projects/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 ([www.winpcap.org/windump/](http://www.winpcap.org/windump/)).

**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 ([http://sourceforge.net/projects/iperf/](http://sourceforge.net/projects/iperf/)) measures maximum TCP bandwidth, allowing the tuning of various parameters and User Datagram Protocol characteristics. Iperf reports bandwidth, delay jitter, and datagram loss.
Section III. Hardware Configuration

This section provides topology guidance for printers and wireless access points (WAPs). It also provides a reference for hardware configurations that support braille testing.

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-request 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

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 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 5 lists recommendations for network topology in which the WAP provides 802.11g and the testing devices provide 802.11g, 802.11n, or a mixture of the two. Refer to your WAP documentation for specific recommendations and guidelines for these or other standards.

<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>

Recommendations for 802.11ac routers are under investigation.

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

Hardware for Braille Testing

For information about braille hardware and software requirements, refer to the Braille Requirements manual linked at http://www.caaspp.org/rsc/pdfs/CAASPP_braille-requirements_2016.pdf.
Section IV. Software Configuration

This section describes how to configure the operating systems and Web browsers for online testing.

Configuring Commercially Available Browsers

This section describes how to configure commercially available browsers (Chrome, Safari, Firefox, and Internet Explorer) for online testing.

Enabling Pop-Up Windows

Systems used in California Assessment of Student Performance and Progress (CAASPP) testing provide informational messages or warnings using pop-up windows. Therefore, enable pop-up windows on those Web browsers using CAASPP testing systems.

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 CAASPP testing, use the instructions in 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 checkbox.
- 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 A, URLs for Testing Sites.

- 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
Requirements for Flash

Some test items require Flash. Table 6 lists the requirements for installing Flash on testing devices.

<table>
<thead>
<tr>
<th>Browser</th>
<th>Flash Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure browser 8.0 and later</td>
<td>Flash included in the browser. In addition, consider installing your operating system’s version of Flash to increase reliability. Flash is available from <a href="https://get.adobe.com/flashplayer/">https://get.adobe.com/flashplayer/</a>.</td>
</tr>
<tr>
<td>Secure browser 7.0</td>
<td>Install Flash for your operating system, or install the Flash plug-in for the browser.</td>
</tr>
<tr>
<td>Secure browser 6.5</td>
<td>Flash bundled in the secure browser installation pack.</td>
</tr>
<tr>
<td>Commercial Web browser* with HTML5</td>
<td>Flash included in the browser, no need for additional installation.</td>
</tr>
<tr>
<td>Commercial Web browser* before HTML5</td>
<td>Install Flash for your operating system, or install the Flash plug-in for the browser.</td>
</tr>
</tbody>
</table>

*Commercial Web browsers—the versions of Internet Explorer, Firefox, Chrome, Safari, and mobile Web browsers listed in the Online System Requirements

Optimal Installation Scenario for Secure Browsers

The Secure Browser Installation Manual at [http://www.caaspp.org/rsc/pdfs/CAASPP_secure-browser-manual.2016.pdf](http://www.caaspp.org/rsc/pdfs/CAASPP_secure-browser-manual.2016.pdf) 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. Running the secure browser creates competition among the students' clients for two resources: local area network bandwidth and shared disk drive. This performance impact can be avoided by installing the secure browser locally on each device. 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 Windows for Online Testing

This section describes how to configure Windows for online testing.

Disabling Fast User Switching

Microsoft Windows (XP, Vista, 7, 8.0, 8.1, and 10) has a “Fast User Switching” feature that allows more than one user to be logged in 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 sections describe how to disable Fast User Switching for different versions of Windows.
Disabling Fast User Switching in Windows XP

This subsection describes how to disable Fast User Switching under Windows XP. This configuration is not necessary if the testing device is joined to a domain, because Fast User Switching is not available in that scenario.

1. Open the Control Panel and switch to classic view.
2. Select the [User Accounts] icon (Figure 3).
3. Select [Change the Way Users Log On or Off].
4. Mark the Use the Welcome Screen checkbox.
5. Clear the Use Fast User Switching checkbox (Figure 4).
6. Select [Apply Options].

Figure 3. Windows XP [User Accounts] icon

Figure 4. Windows XP User Accounts dialog box

Disabling Fast User Switching in Windows Vista and 7

This subsection describes how to disable Fast User Switching under Windows Vista and Windows 7. The process is similar for later versions of Windows.

Option A: Access the Group Policy Editor

The following procedure describes how to disable Fast User Switching using the Group Policy Editor. Some editions of Windows Vista do not support this configuration through the Group Policy Editor; in such cases, configure Fast User Switching through the registry. See Option B for instructions.

1. Select [Start].
2. Type gedit.msc in the Search programs and files field (Figure 5) and then press the [Enter] key. The Local Group Policy Editor window appears.

Figure 5. Windows Search box
3. Navigate to Local Computer Policy → Computer Configuration → Administrative Templates → System → Logon (Figure 6).

4. Double-click **Hide entry points for Fast User Switching**.

5. Select the *Enabled* radio button (Figure 7), and then select **[OK]**.

6. Close the Local Group Policy Editor window.

---

**Option B: Access the Registry**

The following procedure describes how to disable Fast User Switching using the Windows registry.

1. Select **[Start]**.

2. Type `regedit.exe` in the *Search programs and files* field (Figure 8), and then press the **[Enter]** key.


4. Right-click the *System* folder.

5. Select **New → DWORD (32-bit) value** (Figure 9).

6. Type `HideFastUserSwitching` and press **[Enter]**.

8. In the Value data field, enter 1 (Figure 10).

9. Select [OK].

10. Close the Registry Editor.

**Disabling Fast User Switching in Windows 8.0, 8.1, and 10**

The following procedure describes how to disable Fast User Switching under Windows 8.0, 8.1, and 10. The process is similar for other versions of Windows.

1. In the Search charm, type `gpedit.msc` (Figure 11).

2. Double-click the gpedit icon in the Apps pane. The Local Group Policy Editor window opens.


4. In the Setting pane, double-click [Hide entry points for Fast User Switching] in the Setting column (Figure 12).
5. Select the Enabled radio button, and then select [OK].

![Figure 13. Windows Local Group Policy Editor selection](image)

6. In the Search charm, type **run**. The Run dialog box opens (Figure 14).

7. Enter the command `gpupdate /force` into the text box and then select [OK]. (Note the space before the backslash.)

![Figure 14. Windows Run dialog box](image)

8. The Command window opens (Figure 15). The message **Computer Policy update has completed successfully** is your notification that Windows has successfully disabled Fast User Switching.

![Figure 15. Notification in the Windows Command window](image)
Enabling Web Fonts in Internet Explorer 10 and 11

Some applications, such as sample tests or Teacher Hand Scoring System, display test items that may require Web fonts. The following procedure describes how to enable Web fonts in Internet Explorer 10 or 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 16).

Figure 16. Internet Explorer Internet Options dialog box
4. Scroll to Font download and select the Enable radio button (Figure 17).

5. Select [OK]. The Security Settings dialog box closes.

6. Select [OK]. The Internet Options dialog box closes.

![Figure 17. Internet Explorer Security Settings dialog box](image)

Installing Windows Media Pack for Windows 8.1 N and KN

Some versions of Windows 8.1 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:

  ([http://support.microsoft.com/kb/2929699/en-us](http://support.microsoft.com/kb/2929699/en-us))

- Download Media Feature Pack for N and KN Versions of Windows 8.1
Configuring Mac OS X for Online Testing

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

Disabling Exposé or Spaces

Mac OS X 10.6 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 Exposé or Spaces:

1. Choose the Apple menu → System Preferences (Figure 18).

   ![Figure 18. Select OS X System Preferences](image)

2. Select the [Keyboard] icon (Figure 19). The Keyboard window opens.

   ![Figure 19. [Keyboard] icon](image)

3. Select the [Keyboard Shortcuts] or [Shortcuts] tab (Figure 20).

   ![Figure 20. [Keyboard Shortcuts] tab](image)

4. Take the following steps for OS X 10.6; otherwise, skip to step 5:
   a. In the left panel, select [Exposé & Spaces]. The right panel lists the Exposé options (Figure 21).
   b. In the right panel, clear all the checkboxes.

   ![Figure 21. OS X Exposé panel](image)
5. For OS X 10.7 and later, take the following steps:
   a. In the left panel, select [Mission Control]. The right panel lists all Mission Control options (Figure 22).
   b. In the right panel, clear the following checkboxes:
      c. Move left a space
      d. Move right a space
      e. 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 10.6 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 10.9; 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 23). The Keyboard window opens.
3. In the Keyboard window, check the Use all F1, F2, etc. keys as standard function keys box (Figure 24).

   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.)

   ![Figure 24. Keyboard options](image)

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 10.9; 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 23).
3. Select the [App Store] icon. The App Store window opens (Figure 25).
4. Check the Automatically check for updates box.
5. Clear the Download newly available updates in the background checkbox.
6. Clear the Install app updates checkbox.
7. Check the Install system data files and security updates box.

   ![Figure 25. App Store window](image)

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 10.9; 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 checkbox (Figure 26).
5. Select [OK].

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 in 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.
   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 sections 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:

- File Distributor
- Apple’s Active Directory Client and Directory Utility
- Apple’s Open Directory and Profile Manager
- Centrify & PowerBrokers Identity Enterprise
- Apple Remote Desktop

Configuring Linux for Online Testing

This section describes how to configure Linux for online testing.

Adding the Verdana Font

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, Red Hat, and openSUSE—Follow the steps in the “How to Install” section of the following website: http://corefonts.sourceforge.net/
- Ubuntu—In a terminal window, enter the following command to install the msttcorefonts package:

  sudo apt-get install msttcorefonts

Adding Flash

If your distribution or Web browser does not come with Flash, you need to install it. See your distribution’s documentation for details.

Configuring Mobile Devices

This section describes how to configure mobile devices for online testing.

Configuring for Guided Access on iOS

Guided Access restricts the iOS to a single application and prevents taking screenshots. This ensures a secure test environment. (You may want to use Single App mode, which is easier to enable and activate than Guided Access; for more details about this configuration, see Configuring Using Autonomous Single App Mode.)

To configure for Guided Access:

1. Tap the [Settings] icon (Figure 27).

2. Navigate to General → Accessibility → Learning, and turn on Guided Access (Figure 28).

3. Set the passcode for Guided Access. (Test administrators use this passcode to deactivate Guided Access after a test.)
   a. Tap Set Passcode.
   b. Enter a passcode.
   c. Confirm the passcode.
   d. Save the passcode in a safe place. There is no ability to retrieve a forgotten passcode.

4. On devices with iOS 7 or later, disable keyboard functions by taking the following steps:
   a. Under Settings, tap General → Keyboard.
   b. Turn off all settings (Figure 29).
Configuring Using Autonomous Single App Mode

If you have iOS tablets running version 7.1 or higher and if you have a Mac running 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. (Tablets running a version earlier than 7.1 require Guided Access; for details about this configuration, see Configuring for Guided Access on iOS.) Compared to Guided Access, ASAM requires less time to prepare for test sessions; there is no need to activate Guided Access on each iPad before each test session.

Overview of Autonomous Single App Mode and the Secure Testing Environment

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 8.1.3 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.

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 8.1.3 or later (see (Optional) Restrict Features in iOS 8.1.3 or later). 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:


Step 2. (Optional) Restrict Features in iOS 8.1.3 or later.

You can restrict features in supervised devices with iOS 8.1.3 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 8.1.3 or later:

1. In the Custom Settings section of the MDM solution, insert the profile key for each feature you wish to restrict. Table 7 provides a list of the relevant profile keys.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Profile Key</th>
<th>Recommended Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dictionary</td>
<td>&lt;key&gt;allowDefinitionLookup&lt;/key&gt;</td>
<td>False</td>
</tr>
<tr>
<td>Predictive Keyboard</td>
<td>&lt;key&gt;allowPredictiveKeyboard&lt;/key&gt;</td>
<td>False</td>
</tr>
<tr>
<td>Spell Check</td>
<td>&lt;key&gt;allowSpellCheck&lt;/key&gt;</td>
<td>False</td>
</tr>
</tbody>
</table>

Table 7. Profile Keys for Features in iOS 8.1.3 or Later
<table>
<thead>
<tr>
<th>Feature</th>
<th>Profile Key</th>
<th>Recommended Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto Correction</td>
<td>&lt;key&gt;allowAutoCorrection&lt;/key&gt;</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 window appears (Figure 30).
3. Select + below the Profiles list (Figure 31) and select [Create New Profile…]. A configuration window 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 [Ctrl] icon to export the profile to the Mac.

7. Creation of the supervisory profile is complete.

**Step 4. Placing iPads in Autonomous Single App Mode.**

**TIP:** Installing on multiple iPads at once—Before starting this procedure, connect the iPads to the Mac through a USB hub. That way you can perform the installation on many of them at one time.

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

1. On the Mac where you performed Create a supervisory profile, open the Apple Configurator.
2. From the Apple Configurator menu, select Preferences. The Preferences window opens (Figure 32).

![Figure 32. Preferences window](image)

3. In the [General] tab, clear the Automatically refresh and Remove apps and profiles Configurator did not install checkboxes.
4. Close the Preferences window.
5. Back in the Apple Configurator, select [Prepare] and then [Settings]. The Settings window appears (see Figure 30).
6. In the Name field, enter a name to apply to the iPads.
7. Optional: Mark the Number sequentially starting at 1 checkbox. This adds a number to each iPad’s name. For example, if the Name field is 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 window appears (Figure 33).
10. In the Name field, enter [LEA Name or Test Site Name] and then select Done. The Organization Info window 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 in step 6 on page 27, and then select [Open].

12. Check the box for the profile you want to prepare onto the iPads (see Figure 30).
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 window. 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 34).
Note: iOS Upgrade—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 on page 26 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 California Assessment of Student Performance and Progress Web site at http://ca.browsers.airast.org/. (Detailed instructions for installing the secure browser are in the section “Installing the Secure Browser on iOS” of the Secure Browser Installation Manual at http://www.caaspp.org/rsc/pdfs/CAASPP.secure-browser-manual.2016.pdf.)

21. Optional: After installation completes, test it by taking the following steps:
   a. Open the secure browser.
   b. Open the Test Administrator Interface.
   c. Log on to a test site.
   d. Select a test; have the test administrator approve the test.
   e. Start the test. The iPad enters the test.

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.

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

To remove the Emoji keyboard:

1. Tap the Settings icon (Figure 36).
2. Navigate to General → Keyboard.
3. Tap the [Keyboards] icon.
4. Delete *Emoji* from the list by sliding it to the left (Figure 37).

![Figure 37. Keyboards configuration interface](image)

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

1. Select the **[Secure Browser]** icon on the Home screen (Figure 38).

![Figure 38. [Secure Browser] icon](image)
2. A Change Keyboard message appears; tap [Close] (Figure 39).

![Figure 39. Change Keyboard for the secure browser keyboard pop-up message](image)

3. Tap [Set up input methods] (Figure 40). The Language and Input settings screen opens.

![Figure 40. Choose input method dialog box](image)

4. Select the checkbox next to AIRSecureTest so that a checkmark appears (Figure 41).

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.

![Figure 41. Language and input settings options](image)

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 42).

![Figure 42. Change Keyboard for the secure browser keyboard pop-up message](image)
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 43).

![Figure 43. Choose input method dialog box](image)

10. Select [Continue] (Figure 44). You will be prompted to complete the application launch using the preferred method.

![Figure 44. Continue the application launch](image)

11. Select AIRSecureTest (ensure it is shaded and highlighted blue, as it is in Figure 45) 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.)

![Figure 45. Complete the application launch](image)

13. Select [OK].

![Figure 46. Clear default settings pop-up message](image)
Installing CloudReady on PCs and Macs

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: Loss of data—The procedure described in this section erases all data on the device on which you are installing CloudReady. Be sure to back up all necessary data before starting this procedure.

To install CloudReady:

1. Ensure the device on which you are installing CloudReady meets the following requirements:
   • is one of the supported models listed in https://docs.google.com/document/d/1yPxKAmNFaJwk0kwikF5iROFMOxinmkW_9Ke1u5jVo/edit?pli=1;
   • has a USB port; and
   • can boot from a USB drive.

2. Purchase a Neverware license for the device. Licenses are available from http://www.neverware.com/. (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 at https://chrome.google.com/webstore/.

9. Search for the app Chromebook Recovery Utility (Figure 47).

![Figure 47. Chromebook Recovery Utility](image)

10. Select [ADD TO CHROME]; and in the conformation 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 48).

14. At the prompt (Figure 49), 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.

**Configurations for Braille Requirements**

For information about configuring operating systems and software for braille testing, see the Braille Requirements guide, which is available at http://www.caaspp.org/rsc/pdfs/CAASPP_braille-requirements.2016.pdf.


## Section V. Text-to-Speech Requirements

This section contains information about text-to-speech requirements.

### Overview of Text-to-Speech

Using text-to-speech requires at least one voice pack to be installed on testing devices. A number of voice packs are available for testing devices, and all voice packs are researched and tested for compatibility with the secure browsers. Additionally, not all voice packs that come pre-installed with operating systems are approved for use with online testing. The voice packs listed in the operating system subsections have been tested and are whitelisted by the secure browser.

### Using Text-to-Speech

Students using text-to-speech for the practice tests must log on using a supported secure browser. Students can also verify that text-to-speech works on their devices by logging in to a practice test session and selecting a test for which text-to-speech is available.

**Note:** Test sites are strongly encouraged to test the text-to-speech settings before students take operational tests. You can check these settings through the diagnostic page. From the student sample test logon screen, select the **Run Diagnostics** link, and then select the **Text-to-Speech Check** button.

### How the Secure Browser Selects Voice Packs

This subsection describes how the secure browsers select which voice pack to use.

#### Voice Pack Selection on Desktop Versions of Secure Browsers

When a student who is using text-to-speech starts a test, the secure browser looks for voice packs on the student’s device. Upon recognizing an approved voice pack, the secure browser uses the one with the highest priority.

If any of the approved voice packs has also been set as the default voice on the device, then that voice pack will always get the highest priority.

#### Voice Pack Selection on Mobile Versions of Secure Browsers

The mobile secure browser uses either the device’s native voice pack or a voice pack embedded in the secure browser. Additional voice packs downloaded to a mobile device are not recognized by the mobile secure browser. Table 8 lists the voice packs used by mobile versions of the secure browser.

<table>
<thead>
<tr>
<th>Platform</th>
<th>Voice Pack Used by Secure Browser</th>
</tr>
</thead>
<tbody>
<tr>
<td>iOS 7.0–8.2</td>
<td>Native iOS voice pack.</td>
</tr>
<tr>
<td>Android</td>
<td>Native Android voice pack.</td>
</tr>
<tr>
<td>Chrome OS</td>
<td>Native Chromebook voice pack.</td>
</tr>
</tbody>
</table>

### About NeoSpeech Voice Packs for Windows

Pursuant to an agreement between NeoSpeech and the American Institutes for Research (the subcontractor providing the online testing systems), authorized users may download and install specific licensed NeoSpeech voice packs for use on supported Windows devices (Windows XP Service Pack 3, Vista, 7, 8.0, 8.1, and 10).
Text-to-Speech Requirements | Configuring Windows Text-to-Speech Settings

These voice packs can be used instead of the default Windows voice packs for English and the commercial Spanish voice packs from Cepstral. (The default Windows voice packs as well as the Cepstral voice packs for Windows may still be used for text-to-speech, if desired.)

- The Julie voice pack is for English text-to-speech users.
- The Violeta voice pack is for Spanish text-to-speech users.

The NeoSpeech voice pack is to be used only in conjunction with, and not separate from, the online assessments provided by the test delivery system. The NeoSpeech voice packs and the NeoSpeech Voice Packs Installation Guide can be downloaded from the Test Operations Management System (TOMS).

Note: You must have a user role assignment that grants you access to TOMS to download this software.

Configuring Windows Text-to-Speech Settings

This section explains how to configure Windows for using text-to-speech with the secure browser. The text-to-speech feature is available on Windows versions as listed in the System Requirements document. Using Table 9 as a reference, install voice packs from the indicated packages—these are the supported voice packs.

Windows devices are typically shipped with at least one default voice pack. Many of these default voice packs are recognized by the secure browser.

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Voice Pack</th>
<th>Language</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows (pre-installed)</td>
<td>Julie</td>
<td>English</td>
</tr>
<tr>
<td>Windows (pre-installed)</td>
<td>Kate</td>
<td>English</td>
</tr>
<tr>
<td>Windows (pre-installed)</td>
<td>Michael</td>
<td>English</td>
</tr>
<tr>
<td>Windows (pre-installed)</td>
<td>Michelle</td>
<td>English</td>
</tr>
<tr>
<td>Windows (pre-installed)</td>
<td>MSAnna</td>
<td>English</td>
</tr>
<tr>
<td>Windows (pre-installed)</td>
<td>MS_EN-GB_HAZEL</td>
<td>English</td>
</tr>
<tr>
<td>Windows (pre-installed)</td>
<td>MS_EN-US_DAVID</td>
<td>English</td>
</tr>
<tr>
<td>Windows (pre-installed)</td>
<td>MS_EN-US_ZIRA</td>
<td>English</td>
</tr>
<tr>
<td>Windows (pre-installed)</td>
<td>MSMary</td>
<td>English</td>
</tr>
<tr>
<td>Windows (pre-installed)</td>
<td>MSMike</td>
<td>English</td>
</tr>
<tr>
<td>Windows (pre-installed)</td>
<td>MSSam</td>
<td>English</td>
</tr>
<tr>
<td>Windows (pre-installed)</td>
<td>Paul</td>
<td>English</td>
</tr>
<tr>
<td>Windows (pre-installed)</td>
<td>Violeta</td>
<td>Spanish</td>
</tr>
<tr>
<td>Cepstral (commercial)</td>
<td>Cepstral_David</td>
<td>English</td>
</tr>
<tr>
<td>Cepstral (commercial)</td>
<td>Cepstral_Marta</td>
<td>Spanish</td>
</tr>
<tr>
<td>Cepstral (commercial)</td>
<td>Cepstral_Miguel</td>
<td>Spanish</td>
</tr>
<tr>
<td>NeoSpeech (commercial)</td>
<td>VW Julie</td>
<td>English</td>
</tr>
<tr>
<td>NeoSpeech (commercial)</td>
<td>VW Violeta</td>
<td>Spanish</td>
</tr>
</tbody>
</table>
Text-to-Speech Requirements | Configuring Windows Text-to-Speech Settings

The instructions in this section are for Windows 7. The process is similar for other versions of Windows.

1. Open the Control Panel, and then select [Speech Recognition] (Figure 50).

   ![Figure 50. Windows Control Panel window](image)

2. In the Speech Recognition configuration options window, select [Text to Speech] (Figure 51).

   ![Figure 51. Speech Recognition configuration options in Windows](image)

3. Select the [Text to Speech] tab to configure default text-to-speech preferences (Figure 52).

   a. Voice selection: If multiple voice packs are available, select the default voice.

   b. Select [Preview Voice] to hear a sample of the voice and determine whether the selected voice requires a rate adjustment.

   c. Voice speed: If necessary, adjust the voice speed. Drag the slider to make the voice speak slower or faster. To listen to the rate, select [Audio Output].

4. When you are finished selecting options, select [OK] to save your settings and close the Speech Properties window.

   ![Figure 52. Default text-to-speech preferences in Windows](image)
Text-to-Speech Requirements | Configuring OS X Text-to-Speech Settings

Configuring OS X Text-to-Speech Settings

This section explains how to configure Mac OS X for using text-to-speech with the secure browser. The text-to-speech feature is available on OS X versions as listed in the System Requirements document. Using Table 10 as a reference, install voice packs from the indicated packages—these are the supported voice packs.

Mac OS X devices are typically shipped with at least one default voice pack. Many of these default voice packs are recognized by the secure browser.

Table 10. Voice Packs Recognized by Secure Browsers—OS X

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Voice Pack</th>
<th>Language</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mac (pre-installed)</td>
<td>Agnes</td>
<td>English</td>
</tr>
<tr>
<td>Mac (pre-installed)</td>
<td>Alex</td>
<td>English</td>
</tr>
<tr>
<td>Mac (pre-installed)</td>
<td>Bruce</td>
<td>English</td>
</tr>
<tr>
<td>Mac (pre-installed)</td>
<td>Callie</td>
<td>English</td>
</tr>
<tr>
<td>Mac (pre-installed)</td>
<td>David</td>
<td>English</td>
</tr>
<tr>
<td>Mac (pre-installed)</td>
<td>Fred</td>
<td>English</td>
</tr>
<tr>
<td>Mac (pre-installed)</td>
<td>Jill</td>
<td>English</td>
</tr>
<tr>
<td>Mac (pre-installed)</td>
<td>Junior</td>
<td>English</td>
</tr>
<tr>
<td>Mac (pre-installed)</td>
<td>Kathy</td>
<td>English</td>
</tr>
<tr>
<td>Mac (pre-installed)</td>
<td>Princess</td>
<td>English</td>
</tr>
<tr>
<td>Mac (pre-installed)</td>
<td>Ralph</td>
<td>English</td>
</tr>
<tr>
<td>Mac (pre-installed)</td>
<td>Samantha</td>
<td>English</td>
</tr>
<tr>
<td>Mac (pre-installed)</td>
<td>Tom</td>
<td>Spanish</td>
</tr>
<tr>
<td>Mac (pre-installed)</td>
<td>Vicki</td>
<td>English</td>
</tr>
<tr>
<td>Mac (pre-installed)</td>
<td>Victoria</td>
<td>English</td>
</tr>
<tr>
<td>Mac (pre-installed)</td>
<td>Diego</td>
<td>Spanish</td>
</tr>
<tr>
<td>Mac (pre-installed)</td>
<td>Javier</td>
<td>Spanish</td>
</tr>
<tr>
<td>Mac (pre-installed)</td>
<td>Marta</td>
<td>Spanish</td>
</tr>
<tr>
<td>Mac (pre-installed)</td>
<td>Monica</td>
<td>Spanish</td>
</tr>
<tr>
<td>Mac (pre-installed)</td>
<td>Paulina</td>
<td>Spanish</td>
</tr>
<tr>
<td>Infovox (commercial)</td>
<td>Heather Infovox iVox HQ</td>
<td>English</td>
</tr>
<tr>
<td>Infovox (commercial)</td>
<td>Rosa Infovox iVox HQ</td>
<td>Spanish</td>
</tr>
</tbody>
</table>

The instructions in this section are for OS X 10.9. The process is similar for other versions of OS X.

1. Choose the Apple menu → System Preferences (Figure 53).
2. Select the [Dictation & Speech] icon (Figure 55).

3. In the **Text to Speech** section of the **Dictation & Speech** configuration window (Figure 55), set your default text-to-speech preferences.
   
   a. **System Voice**: If multiple voice packs are available, select the default voice.
   
   b. Select **[Play]** to hear a sample of the voice and determine whether the selected voice requires a rate adjustment.
   
   c. **Speaking Rate**: If necessary, adjust the voice speed. Drag the slider to make the voice speak slower (left) or faster (right). To listen to the rate, select **[Play]**.
   
   d. When you are done, select the red X or bubble in the upper-left corner to save your settings and close the Dictation & Speech window.
**Configuring Linux Text-to-Speech Settings**

This section explains how to install voice packs on the supported Linux distributions. Using Table 11 as a reference, install voice packs from the indicated packages—these are the supported voice packs.

| Table 11. Packages that Include Supported Voice Packs on Linux Distributions |
|---------------------------------|---------------------------------|
| **Distribution/Voice Pack** | **Available in Package** |
| Ubuntu | | |
| kal_diphone (Kevin American English male) | festvox-kallpc16k, festvox-kallpc8k |
| ked_diphone (Kurt American English male) | festvox-kdlpc16k, festvox-kdlpc8k |
| el_diphone (Castilian Spanish male) | festvox-ellpc11k |
| openSuse | | |
| kal_diphone (Kevin American English male) | (included in festival) |
| Fedora, RedHat | | |
| cmu_us_awb_arctic_hts (Scottish English male) | festvox-awb-arctic-hts |
| cmu_us_bdl_arctic_hts (American English male) | festvox-bdl-arctic-hts |
| cmu_us_jmk_arctic_hts (Canadian English male) | festvox-jmk-arctic-hts |
| kal_diphone (Kevin American English male) | festvox-kal-diphone |
| ked_diphone (Kurt American English male) | festvox-ked-diphone |

1. Install Festival for text-to-speech:
   - **Ubuntu**: `sudo apt-get install festival`
   - **Fedora, RedHat**: `yum install festival`
   - **openSUSE**: `zypper install festival`

2. Install Sound eXchange (SoX) for text-to-speech:
   - **Ubuntu**: `sudo apt-get install sox`
   - **Fedora, RedHat**: `yum install sox`
   - **openSUSE**: `zypper install festival`
Appendix A. 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 Non testing Sites

Table 12 lists URLs for non testing sites, such as Test Information Distribution Engine (TIDE), Online Reporting System (ORS), and Learning Point Navigator.

<table>
<thead>
<tr>
<th>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):</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Test Operations Management System (TOMS)</td>
</tr>
<tr>
<td>• ORS</td>
</tr>
<tr>
<td>• Test Administrator Interface</td>
</tr>
<tr>
<td>• TIDE (used to file appeals)</td>
</tr>
<tr>
<td>• Interim Assessment Hand Scoring System (for interim assessments)</td>
</tr>
</tbody>
</table>

Table 12. URLs for Non testing Sites

<table>
<thead>
<tr>
<th>System</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAASPP Portal</td>
<td><a href="http://www.caaspp.org">http://www.caaspp.org</a></td>
</tr>
<tr>
<td>Secure browser installation files</td>
<td><a href="http://ca.browsers.airast.org/">http://ca.browsers.airast.org/</a></td>
</tr>
<tr>
<td>TOMS</td>
<td><a href="https://caaspp.ets.org">https://caaspp.ets.org</a></td>
</tr>
<tr>
<td>Single Sign On System</td>
<td>(The full URL varies by system such as TOMS or the Test Administrator Interface.)</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 13. URLs for Testing Web Sites

<table>
<thead>
<tr>
<th>System</th>
<th>URL</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>
</tbody>
</table>
Online Dictionary and Thesaurus

Some online assessments contain an embedded dictionary and thesaurus provided by Merriam-Webster. The Merriam-Webster URLs listed in Table 14 should also 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 B. Technology Coordinator Checklist

This checklist can be printed out 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>System Requirements Guide <a href="http://www.caaspp.org/rsc/pdfs/CAASPP_system-requirements-manual.2016.pdf">http://www.caaspp.org/rsc/pdfs/CAASPP_system-requirements-manual.2016.pdf</a></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>Network Configuration and Testing</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>Secure Browser Installation Manual <a href="http://www.caaspp.org/rsc/pdfs/CAASPP_secure-browser-manual.2016.pdf">http://www.caaspp.org/rsc/pdfs/CAASPP_secure-browser-manual.2016.pdf</a></td>
</tr>
<tr>
<td>Enable pop-up windows and 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>Software Configuration</td>
</tr>
<tr>
<td>On <strong>Windows</strong> 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</td>
</tr>
<tr>
<td>On <strong>Mac 10.7–10.11</strong>, disable Spaces 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>Install any required text-to-speech software on devices that will be used for testing and verify that installation.</td>
<td>5–10 hours</td>
<td>1–2 weeks before testing begins in your school</td>
<td>Text-to-Speech Requirements</td>
</tr>
<tr>
<td>On <strong>iPads</strong>, ensure that Guided Access or Autonomous Single App Mode is enabled and that test administrators know how to activate Guided Access.</td>
<td>5–10 hours</td>
<td>1–2 weeks before testing begins in your school</td>
<td>Configuring for Guided Access on iOS</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>Enabling the Secure Browser Keyboard on Android</td>
</tr>
</tbody>
</table>
Appendix C. 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 below 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. You may want to work with the California Assessment of Student Performance and Progress test site coordinator to adapt this worksheet as necessary so you do not risk overloading your 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>
</tbody>
</table>

Estimated number of hours needed per student to complete the test. This estimate should include approximately 15 minutes for students to get set up and logged in as well as the average estimated time to complete the test.

Number of hours that must be scheduled to administer the test:

(students + test administrators) x hours ÷ devices =

Example:

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

| 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/ |

If you must contact CalTAC, you will be asked to provide as much detail as possible about the issue(s) you encountered. **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 tests
- Operating system and secure browser version information (test delivery system)
- Operating system and Web browser version information (Test Administrator Interface)
- 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.