Chapter 3. System Configuration
Hardware Configuration

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

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

Connections Between Printers and Testing Devices

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

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

The following are the most commonly deployed wireless networking standards:
- 802.11ac has a theoretical throughput of up to 1G bits per second.
- 802.11n has a theoretical throughput of up to 300M bits per second.
- 802.11g has a theoretical throughput of up to 54M bits per second.
- 802.11b has a theoretical throughput of 11M bits per second.

The recommended number of devices supported by a single wireless connection depends on the standard used for the connection. The two most common networking standards are 802.11g (54 megabits per second [Mbps]) and 802.11n (300Mbps). Table 12 lists recommendations for network topology in which the wireless access point (WAP) provides 802.11g and the testing devices provide 802.11g, 802.11n, or a mixture of the two. Note that
there currently are no recommendations for 802.11ac routers. Refer to your WAP documentation for specific recommendations and guidelines for these or other standards.

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

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

**Hardware for Braille Testing**

For information about braille hardware and software requirements, refer to the Accessibility Guide for CAASPP Online Testing, which will be available on the CAASPP Student Accessibility Resources and Test Settings Web page.
Software Configuration

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

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

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

Optimal Installation Scenario for Secure Browsers
Chapter 4, Secure Browser Configuration, describes several scenarios for installing the secure browser. However, it is strongly recommended that the secure browser be installed locally on each students’ testing device rather than on a shared network drive from which students would run the secure browser as this will compromise the stability and performance of the secure browser, especially during peak testing times. Running the secure browser creates competition among the students’ clients for two resources: local area network bandwidth and shared disk drive input/output. This performance impact can be avoided by installing the secure browser locally on each device. Additionally, running the secure browser from a shared location also creates security risks.

Warning: Testing Quality With Servers
Launching a secure browser from a terminal or Windows server typically does not create a secure test environment because students can use their local devices to search for answers. Therefore, this installation scenario is not recommended for testing.
Configuring Commercially Available Web Browsers

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

Enabling Pop-Up Windows

Systems used to support student California Assessment of Student Performance and Progress (CAASPP) testing provide informational messages or warnings using pop-up windows. Therefore, you must enable pop-up windows on those Web browsers used in support of CAASPP testing systems, such as the Test Operations Management System and the Test Administrator Interface.

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

**Enabling Pop-Up Windows for All Domains**

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

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

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

You can allow pop-up windows only from domains involved in CAASPP testing. The following list describes how to enable domain-specific pop-up windows on many browsers. If your browser is not on this list, consult its user documentation. The list of domains to use in these instructions appears in Appendix B, URLs for Testing Systems.

- **Firefox:** Tools → Options → Content → select Exceptions. Enter domain names and select [Allow] for each.
- **Chrome:** Menu → Settings → Show advanced settings (at the bottom of the screen) → Privacy → Content Settings → Pop-ups → select Manage Exceptions. Enter the domain names and select [Allow] for each.
- **Internet Explorer:** [Internet Options Privacy] tab → Settings. Enter the domain names and select [Add] for each.
• Safari and iOS Safari: N/A
• Chrome on Android tablets: N/A

Preventing Auto Update on Device Operating Systems Used for Test Operations

Additional Resources:

**Warning: Disabling Auto Update**

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

**Delaying Firefox Web Browser Updates**

Quality assurance tests are conducted on the most recent Firefox Web browser versions for each system except the student testing site, which requires the secure browser. You should wait before installing new versions of Firefox, which could impact system performance.

Delaying updates allows time to review changes and verify each system works correctly with the new version.

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

**Enabling Web Fonts in Internet Explorer 11**

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

*To enable Web fonts in Internet Explorer:*

1. In Internet Explorer, open the **Tools** menu and then select **Internet Options**. The **Internet Options** dialog box opens.
2. Select the **[Security]** tab (Figure 3).
3. Select the [Custom Level] button. The Security Settings dialog box opens (Figure 4).

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

Keyboard Navigation to Tool Menu Using a Safari Browser

Unlike other browsers, students cannot use Safari to navigate to the Tool menu using standard methods on practice and training tests. To enable access the Tool menu using Safari, check the Press Tab to highlight each item on a webpage box in the “Accessibility” section of the Safari Advanced preferences, as shown in Figure 5.

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

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

Configuring Windows for Online Testing with the Secure Browser

This subsection describes how to configure Windows for online testing.

Disabling Fast User Switching in Windows

Microsoft Windows (7, 8.0, 8.1, and 10) has a “Fast User Switching” feature that allows more than one user to be logged on at the same time. This is a security risk because students can potentially start a new Windows session during the test and use that session to search the Internet for answers. The following subsections describe how to disable Fast User Switching for different versions of Windows. (There is no need to manually disable Fast User Switching on Windows 10.)
Disabling Fast User Switching in Windows 7

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

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

![Figure 6. Windows Search box](image)

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

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

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

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

6. Close the Local Group Policy Editor screen.
Disabling Fast User Switching in Windows 8.0 and 8.1

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

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

2. Select the `[gpedit]` icon in the Apps pane. The Local Group Policy Editor screen opens.
4. In the Setting pane, double-click `Hide entry points for Fast User Switching` (Figure 10).

5. Select the `Enabled` radio button, and then select `[OK]`. Both are indicated in Figure 11.
6. In the Search charm, type run.
7. Select the [Run] icon in the Apps pane. The Run dialog box opens.
8. Enter the command `gpupdate /force` into the Run dialog box and then select [OK] (Figure 12). (Note the space before the forward slash.)

![Figure 12. Windows Run dialog box](image)

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

![Figure 13. Notification in the Windows Command window](image)

### Setting Touch Input

**Blocking Device Touch Input Using the Group Policy Editor**

Some tablets and devices have touch features that may need to be disabled before testing. The following procedure describes how to disable the touch features on these devices using the Group Policy Editor to edit policy settings.

1. Type `gpedit.msc` in the Search box on the Start menu and then select the link. The Local Group Policy Editor window, shown in Figure 14, appears.
1. In the left pane, navigate to Computer Configuration → Administrative Templates → Windows Components (indicated in Figure 14).

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

4. In the Input Panel group, select a policy setting to view its description or double-click it to change its state; current policy settings are shown in the State column, indicated in (Figure 17).

5. To enable an item, double-click on that item in the Setting column to open the Disable [policy setting] dialog box, which is shown in Figure 18 for the setting “Disable text prediction.” The following settings should be enabled:
a. Turn off AutoComplete integration with Input Panel
b. Prevent Input Panel tab from appearing
c. For tablet pen input, don’t show the Input Panel icon
d. For touch input, don’t show the Input Panel icon
e. Disable text prediction

Figure 18. Disable text prediction dialog box

6. To enable the setting, select the Enabled radio button, and then select [OK]. This dialog box also gives you the option to disable the setting. Select [Apply] and then the [Next Setting] or [Previous Setting] button to move to the next or previous item displayed in the “Settings” list.

7. Close the Local Group Policy Editor window.

Configuring the Touch Keyboard on Microsoft Surface Pro 3 Tablet

Some students using Surface Pro 3 tables and accessing the touch keyboard may see the touch keyboard disappear when they select outside a text box while testing or when they type an answer into a text box and then select [Next]. Then, the touch keyboard fails to reappear when they select inside the next text box. To avoid this issue, the student’s touch keyboard must be set to show up automatically.

Take these steps to set the touch keyboard to show up automatically:

1. Access the device’s Settings (which can be done on devices using Windows 8.1 and above by using the keyboard shortcut [Windows] + [I]).
2. Select [Devices] (indicated in Figure 19) and then Typing from the left pane (shown in Figure 20).

3. Scroll down and toggle on *Automatically show the touch keyboard in windowed apps when there's no keyboard attached to your device*, which is indicated in Figure 20.
Disabling the Two-finger Scrolling Feature in HP Stream Notebooks with Synaptics TouchPad

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

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

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

![Mouse Properties dialog box](image)

4. From the Devices list, select “Synaptics LuxPad V7.5,” and then select [Settings...] (indicated in Figure 21).
5. Uncheck the Two-Finger Scrolling box, which is indicated in Figure 22.
Figure 22. Properties for Synaptics TouchPad V7.5 on PS/2 Port dialog box

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

Installing Windows Media Pack for Windows 8.1 N and 8.1 KN

**Additional Resources:**

Some versions of Windows 7, 8.1, and 10 are not shipped with media software installed. As a result, you may need to install software to enable students to listen to and record audio as well as watch videos.

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

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

You are encouraged to download this software and ensure it works with sample Web sites and video and audio files prior to installing the Windows secure browser. Installation instructions are provided on Microsoft’s download page.
Microsoft Resources:
- Media Feature Pack for Windows 8.1 N and Windows 8.1 KN Editions
  - About
  - Download

Configuring Mac OS X for Online Testing with the Secure Browser

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

Disabling Exposé or Spaces

Mac OS X versions 10.7 through 10.11 include an Exposé or Spaces feature that allows running more than one desktop session. This is a security risk because students can potentially start a new desktop session during the test and use that session to search the Internet for answers. The following procedure explains how to disable Exposé or Spaces on those versions of OS X. (You can disable Spaces quickly from the command line; see Disabling Spaces and Application Launches from the Command Line for details.)

To disable Spaces:

1. Choose the Apple menu → System Preferences (Figure 23).

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

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

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

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

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

4. In the left panel of the screen, select [Mission Control]. The right panel lists all Mission Control options (Figure 26).
To re-enable Exposé or Spaces, follow steps 1–5, this time marking the boxes for spaces.

Disabling Application Launches from Function Keys

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

Starting with OS X versions 10.7 and later, some Mac devices are factory configured to launch iTunes and other applications by pressing the function keys (e.g., [F8]) on the keyboard. If a student accidentally presses the function key, the secure browser assumes that a forbidden application is running and pauses the student's test. To avoid this scenario, disable the use of function keys to launch applications.

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

To disable application launches from function keys:

1. Choose the Apple menu → System Preferences.
2. In System Preferences, select the [Keyboard] icon (Figure 27). The Keyboard screen opens.
3. In the Keyboard screen, check the Use all F1, F2, etc. keys as standard function keys box (Figure 28).
If you need to launch iTunes or another application, press the [Fn] key and then press the desired function key. This combination will launch the application. (Doing so while taking a test causes the secure browser to pause the test.)

**Disabling Updates to Third-Party Apps**

Updates to third-party apps may include components that compromise the testing environment. This subsection describes how to disable updates to third-party apps. The following instructions are based on OS X 10.11; similar instructions apply for other versions of OS X.

To disable updates to third-party apps:
1. Log on to the student’s account.
2. Choose the Apple menu \(\rightarrow\) System Preferences. The System Preferences dialog box opens (Figure 27).
3. Select the [App Store] icon. The App Store screen opens (Figure 29).
4. Check the Automatically check for updates box.
5. Clear the Download newly available updates in the background check box.
6. Clear the Install app updates check box.
7. Check the Install system data files and security updates box.
Disabling Updates to iTunes

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

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

To disable updates to iTunes:
1. Log on to the student’s account.
2. Start iTunes.
3. Select **iTunes → Preferences**.
4. Under the [Advanced] tab, clear the **Check for new software updates automatically** check box (Figure 30).

![Advanced Preferences options](image)

5. Select [OK].

Disabling Look-Up Gesture

OS X versions 10.7 and later include a look-up gesture function, which permits users to highlight a word and then, after tapping with three fingers on the trackpad, to access a dictionary for the highlighted word. This feature can compromise testing security. This subsection describes how to disable the look-up gesture.

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

To disable updates to third-party apps:
1. Choose the **Apple menu → System Preferences**.
2. Select [Trackpad]. The **Trackpad Preferences** dialog box opens.
3. Select the [Point and Click] tab (Figure 31).
4. Clear the Look up check box.

Disabling Display of Notification Center

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

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

To disable the gesture for displaying the Notification Center:

1. Choose the Apple menu → System Preferences.
2. Select [Trackpad]. The Trackpad Preferences dialog box opens.
4. Select the Notification Center check box, which is highlighted in Figure 32.

Disabling Spaces and Application Launches from the Command Line

The subsections “Disabling Exposé or Spaces” and “Disabling Application Launches from Function Keys” describe how to configure OS X through the desktop. This subsection describes how to perform those configurations from the command line, which may take less time than working through the desktop. To perform this task, you need to be familiar with logging on to OS X devices through Terminal or other terminal emulator.
To disable Spaces and application launches from the command line:

1. Log on to the device as the user that runs the secure browser.

2. Enter the following commands to modify the file 
   `~/Library/Preferences/com.apple.symbolichotkeys.plist`

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

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

3. If you logged on to a device running OS X 10.8.5 or later, log off and then log back on.

4. If you need to restore Spaces and the default application launchers, repeat steps 1–3. In step 2, change `enabled = 0` to `enabled = 1`.

**Disabling Spaces and Application Launches on Remote Devices**

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

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

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

When students speak into an OS X device, utilizing the Dictation feature that suggests words or spellings, they may compromise testing security or violate the construct of the assessment. Take these steps to disable Dictation in an OS X device:

1. Access System Preferences.
2. Select the [Keyboard] option (indicated in Figure 33) and then Dictation.

![Figure 33. [Keyboard] button in OS X System Preferences](image)

3. Select the Off radio button to turn the Dictation option off (Figure 34).

![Figure 34. Dictation system preferences options in OS X](image)

Disabling Siri

Take these steps to disable the Siri feature:

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

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

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

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

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

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

**Caution:** On Linux systems, all keyboard shortcuts are disabled while taking an assessment with the secure browser. In the event of an abnormal browser exit, those shortcuts will be reset to the default state they were in before the exit.

This subsection describes how to configure Linux for online testing.
Adding the Verdana Font

Additional Resources:
- SourceForge: An easy way to install Microsoft’s TrueType core fonts on linux Web page—http://corefonts.sourceforge.net/

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

- Fedora and Red Hat—Follow the steps in the “How to Install” section of the instructions on the An easy way to install Microsoft’s TrueType core fonts on linux Web page.
- Ubuntu—In a terminal window, enter the following command to install the msttcorefonts package:
  
  `sudo apt-get install msttcorefonts`

Configuring Apple Mobile Devices for Online Testing with the Secure Browser

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

Using Autonomous Single App Mode (ASAM)

If you have iOS tablets running version 8.0 or higher and if you have a device running iOS version 10.10 or higher, then you can use Autonomous Single App Mode (ASAM) to quickly create a secure testing environment on all iPads used for testing. There is no need to activate ASAM on each iPad before each test session.

**TIP:** If you are using iPads with iOS 9.3.2 or later, you can use the automatic assessment configuration that comes with the AIRSecureTest app to save time with automatic assessment configuration. For details, see the instructions for Using Automatic Assessment Configuration.

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

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

After completing these steps, each time a student starts a test, the iPad enters ASAM and the test environment is secure.
Step 1. Create a mobile device management profile.

Additional Resources:


The first step in provisioning iPads with ASAM is to create a mobile device management (MDM) profile. Any profile with default settings is compatible with the secure browser. However, you may wish to restrict certain features in devices with iOS 9.2 or later (see the next step for instructions). Deploy the profile to a host that the iPads can access.

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

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

Step 2. (Optional) Restrict Features in iOS 9.2 or later.

You can restrict features in supervised devices with iOS 9.2 or later that may give students an unfair testing advantage, including the dictionary, predictive keyboard, spell check, and auto correction. If you wish to restrict any of these features, you may do so when creating the MDM profile for these devices.

Note: The current version of Apple Configurator does not allow you to restrict these features. If you wish to restrict these features when configuring the MDM profile, you must use a third-party MDM solution.

To restrict features in iOS 9.2 or later:

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

<table>
<thead>
<tr>
<th>Feature</th>
<th>Profile Key</th>
<th>Recommended Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dictionary, Share Selected Text</td>
<td>&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>
<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 screen appears (Figure 37).
3. Select + below the Profiles list (Figure 37) and select [Create New Profile…]. The configuration screen shown in Figure 38 appears.
4. In the “General” section, enter a name for the profile in the Name field.

5. In the “Restrictions” section, select [Configure]. A list of restrictions appears.
   a. Make any required changes to the restrictions, or retain the default settings.
   b. Select [Save]. You return to the [Settings] tab, and the profile appears in the Profiles list.

6. Select the [Export] right-arrow icon to export the profile to the Mac.

Creation of the supervisory profile is complete.

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

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

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

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

1. On the Mac where you performed **Step 3. Create a supervisory profile**, open the Apple Configurator.

2. From the Apple Configurator menu, select Preferences. The Preferences screen opens (Figure 39).

![Figure 39. Preferences options](image)

3. In the [General] tab, clear the Automatically refresh and Remove apps and profiles Configurator did not install check boxes.

4. Close the Preferences screen.

5. Back in the Apple Configurator, select [Prepare] and then [Settings]. The Settings screen appears (see Figure 37).
6. In the Name field, enter a name to apply to the iPads.

7. Optional: Mark the Number sequentially starting at 1 check box. This adds a number to each iPad’s name. For example, if the Name field says Garden Elementary School, and if three iPads are connected, each device receives a name like Garden Elementary School 1, Garden Elementary School 2, and Garden Elementary School 3.

8. Set Supervision to [On].

9. Select [Organization Info…]. The Organization Info screen appears (Figure 40).

![Organization Info screen](image)

**Figure 40. Organization Info screen**

10. In the Name field, enter [Local Educational Agency Name or Test Site Name] and then select Done. The Organization Info screen closes.

11. If the profile you created in Step 3. Create a supervisory profile does not appear in the Profiles list, import it by taking the following steps:
   a. Select + below the Profiles list and select Import Profile….
   b. Navigate to the profile you saved as a result of this process, and then select [Open].

12. Check the box for the profile you want to prepare onto the iPads (see Figure 37).

13. Connect each iPad to the Mac via a USB cable or USB hub.

14. On each connected iPad, uninstall any existing versions of the secure browser.

15. In the Apple Configurator, under the [Prepare] tab, select the [Prepare] icon at the bottom of the screen. A confirmation message appears.

16. Select [Apply] in the confirmation message. Preparation starts and may take several minutes, after which the iPad restarts. The Apple Configurator displays progress messages during the prepare process (Figure 41).
Figure 41. Apple Configurator screen

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

17. After the iPad restarts, follow the prompts on the iPad to configure it until the home screen appears.

18. **Optional:** Confirm the supervisory profile is installed on the iPad. Go to Settings → General → Profiles. The profile name you used in Step 4. Place iPads in Autonomous Single App Mode appears under Configuration Profiles.

19. On the iPad, download and install the MDM profile you created in Step 1. Create a mobile device management profile.

20. After the MDM profile installation completes, install the secure browser onto the iPad. You can download the secure browser for iOS from the CAASPP Secure Browsers Web site. (Detailed instructions for installing the secure browser are in the subsection “Installing the Secure Browser on iOS” of Chapter 4, Secure Browser Configuration.)

21. **Optional:** To confirm installation, attempt to open the secure browser on the testing device. If it opens and the student is able to access a practice or training test, installation was successful. If it does not, then repeat this process.

22. Repeat steps 13–21 to prepare additional iPads.

23. In the Apple Configurator, select [Stop] and close the Apple Configurator.

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

**Using Automatic Assessment Configuration**

**Caution:** MDM profiles for managed iPads override the automatic assessment configuration. If you want to use automatic assessment configuration, delete any existing MDM profiles from the Apple Configurator.

If students are using iPads with iOS 9.3.2 or later, you can use Automatic Assessment Configuration. This configuration includes a preset profile in the AIRSecureTest app that automatically suppresses the features listed in Table 6.
When a student taps [**Begin Test Now**] on an iPad with Automatic Assessment Configuration, a message similar to that in Figure 42 appears.

![Confirm App Self-Lock](image)

**Figure 42. Notification when starting test with automatic assessment configuration**

**Removing the Emoji Keyboard from an iOS Device**

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

IOS has an Emoji keyboard that contains emoticons (Figure 43). This keyboard, if activated, can be confusing for test takers or scorers. Use the following procedure to remove the Emoji keyboard from an iOS device.

To remove the Emoji keyboard:

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

![Emoji keyboard for iOS](image)

**Figure 43. Emoji keyboard for iOS**

![Keyboards configuration interface](image)

**Figure 44. [Settings] icon**

**Figure 45. Keyboards configuration interface**
Disabling Dictation

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

Take these steps to disable Dictation in an OS X device:

1. Tap the [Settings] icon.
2. Navigate to General → Keyboard.
3. Move the slider to turn off Enable Dictation (Figure 46).

![Figure 46. Disabled dictation](image)

Disabling Keyboard Functions

Disable keyboard functions by taking the following steps:

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

![Figure 47. Keyboard Settings for iOS 9.3 (other versions of iOS are similar)](image)

Configuring Android for Online Testing with the Secure Browser

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

The default keyboard for the Android allows predictive text, which may provide students with hints for answers to tests. For this reason, the secure browser for Android requires that a mobile secure browser keyboard be configured for the secure browser itself. The secure browser keyboard is a basic keyboard, with no row for predictive text functionality.
The first time you open the mobile secure browser on an Android tablet, you will be prompted to select the secure browser keyboard.

**Note about the Secure Browser Keyboard and General Settings:**
Once the secure browser keyboard is set, it becomes the default keyboard for all Android tablet applications, not just for the secure browser. If you want to return to the default Android keyboard after using the secure browser, you will need to navigate to *Settings → Language & Input* and uncheck the secure browser keyboard.

If you change back to the default Android keyboard, you will be prompted to select the secure browser keyboard the next time you open the secure browser. The secure browser will not allow you to access the student logon page until the secure browser keyboard has been selected.

The following procedure describes how to enable the secure browser keyboard. The screenshots were taken with a Samsung Galaxy Tab 2; other Android versions may vary.

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

![Figure 48. [Secure Browser] icon](image)

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

![Figure 49. Change Keyboard for the secure browser keyboard pop-up message](image)

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

5. You will be prompted to acknowledge that this selection is okay. Select [OK] to continue.

   *Note:* This action allows the mobile secure browser to use the secure browser keyboard.

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

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

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

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

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

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

13. Select [OK] (Figure 56).
Disabling the Multi Window on Samsung Tablets

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

The following instructions are based on Android 4.4 on a Samsung tablet; similar instructions apply for other versions of Android on Samsung tablets.

To disable the Multi window:
1. Tap [Settings].
2. Navigate to Device → Sound and display.
3. Turn off the Multi window using the slider (Figure 57).

Disabling the Stylus on Samsung Galaxy Note

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

To disable the stylus:
1. Tap [Settings].
2. Navigate to Controls → Voice and input methods.
3. Tap S Pen.
4. Disable all of the available features (Figure 58).
Figure 58. Disable the Samsung stylus

Configuring Chromebook Mobile Devices for Online Testing with the Secure Browser

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

Disabling Auto Updates for Chrome OS

Additional Resources:

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

You may want to disable auto updates during your LEA’s or test site’s selected testing window to avoid unknown issues that may be introduced by future operating system updates (although versions of Chrome are presumed to be supported). For example, if AIR supports up to Chrome OS version 58, and version 58 is installed on your students’ Chromebooks, you can prevent auto updates to any later version. (Alternatively, you can allow auto updates to a specific version supported by AIR; for details, see the next subsection “Limiting Chrome OS Updates to a Specific Version for Managed Chrome Devices.”)

To disable auto updates for Chrome OS:

1. Display the Device Settings page by following the procedure in the Manage Chrome device settings Web page. The steps in that procedure assume that the Chromebooks are managed through the admin console.

2. From the Auto Update list, select Stop auto-updates.

3. From the Restrict Google Chrome version to at most list, select the required version.

4. Select [Save].
Limiting Chrome OS Updates to a Specific Version for Managed Chrome Devices

AIR has tested CAASPP operational software (such as the Test Administrator Interface) and the practice and training tests up to version 51 of the Chrome OS; you may want to prevent your Chromebooks from auto-updating beyond that version. (Alternatively, you can disable auto updates entirely; for details, see the subsection “Installing the AIRSecureTest Kiosk App on Managed Chromebooks.”)

To limit Chrome OS updates to a specific version:

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

Securing Chrome OS for High-Stakes Assessments

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

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

Turning ChromeVOX Off

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

To disable ChromeVOX before launching the secure browser:

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

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

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

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

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

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

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

Installing CloudReady on PCs and Macs

Additional Resources:
- Google Chrome Web Store—https://chrome.google.com/webstore/
- Neverware Web site—https://www.neverware.com/
- Neverware Certified Model Finder Web page—https://guide.neverware.com/supported-devices/

CloudReady is a reduced-feature operating system, built on the same technology as Chrome OS, that runs on devices with limited resources. If your school or local educational agency has older devices that do not run newer versions of Windows or OS X, consider installing CloudReady on those devices. This installation can postpone or prevent a costly hardware upgrade.

Warning: Process Erases All Data

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

Take these steps to install CloudReady:

1. Ensure the device on which you are installing CloudReady meets the following requirements:
- is **supported for use with CloudReady**;
- has a USB port; and
- can boot from a USB drive.

2. Visit the Neverware Web site to purchase a CloudReady license for the device. (Bulk licenses may be available.)

3. If you received a USB drive from Neverware with the CloudReady image, proceed to step 18. Otherwise, prepare a bootable image by following steps 4 through 17. Ideally, perform these steps on a device on which the Google Chrome Web browser is already installed.

4. Obtain a blank 8 GB USB drive.

5. Install Google Chrome if it is not already installed.

6. In a Web browser, go to the URL for the image file provided to you by Neverware. This URL downloads a file with a name similar to `cloudready_site646.bin`. Note the location of the file on your device.

7. Insert the USB drive into the device.

8. Start Chrome, and then navigate to the Chrome Web Store.

9. Search for the app **Chromebook Recovery Utility** (Figure 64).

![Figure 64. Chromebook Recovery Utility](image)

10. Select `[ADD TO CHROME]`; and in the confirmation prompt, select `[Add app]`.

11. After installation has completed, select `[Launch App]`.

12. Select the gear `[⚙️]` icon in the top-right corner and then select **Use local image** (Figure 65).

![Figure 65. Selecting the CloudReady image](image)


14. At the prompt (Figure 66), select the USB drive you inserted in step 7.
15. Select [Continue].

16. In the next screen, select [Create Now]. The recovery utility creates a bootable image of CloudReady onto the USB drive. This operation takes 15–30 minutes.

17. When copying is complete, eject the USB drive from the device.

18. On the device where you are installing CloudReady, do the following:
   a. Back up all files you want to save. The installation procedure erases all data on the device.
   b. Boot the device from the USB drive. Booting and installation take 10–15 minutes, depending on the device. When the installation is complete, your device turns off.
   c. Remove the USB drive and power on the device.
   d. Install the AIRSecureTest Kiosk App; see Chapter 4, Secure Browser Configuration for details.

Configurations for Testing Students Using Accessibility Supports

Additional Resources:

• CAASPP Student Accessibility Resources and Test Settings Web page—
  http://www.caaspp.org/administration/accessibility/

For information about configuring operating systems and software for testing with accessibility supports, including braille, text-to-speech and the NeoSpeech voice pack, and permissive mode, refer to the Accessibility Guide for CAASPP Online Testing, which will be available on the CAASPP Student Accessibility Resources and Test Settings Web page.
This page is left blank intentionally.