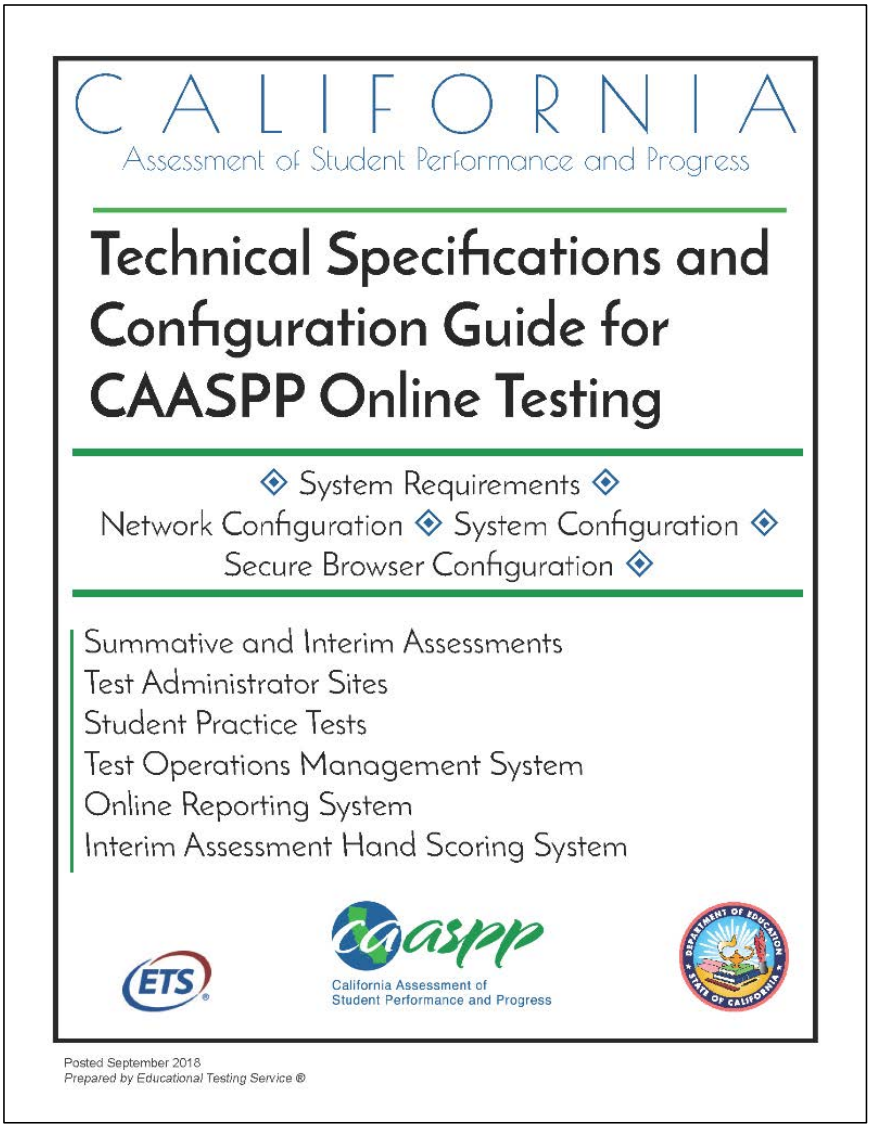
Chapter 4. Secure Browser Configuration



Overview of Secure Browsers

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

This section includes the following topics:

About the Secure Browser

All devices that students will use to access online assessments must have a secure browser installed on that device. The secure browser prevents students from accessing other computer or internet applications or copying test information. **All devices that will be used for testing must have the correct secure browser installed.**

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

While the secure browser is an integral component of test security, test administrators and test examiners perform an equally important role in preserving test integrity. Test administrators and test examiners should be aware of the following requirements and employ the necessary precautions while administering online assessments:

Close External User Applications

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

The secure browser will not work if the device detects that a forbidden application is running. For more information, see the "Forbidden Application Detection" subsection.

Turn Off Background Jobs

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

Warning: Scheduling Background Jobs

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

Warning: Disabling Auto Update

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

Testing on Computers with Dual Monitors

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

However, in extremely rare circumstances, a test administrator or test examiner is administering a test via read-aloud and wants to have a duplicate screen to view exactly what the student is viewing for ease of reading aloud. In these rare cases where a dual monitor **is allowed**, **monitors should be set up to "mirror" each other.** School technology coordinators can assist test administrators in setting up the two monitors to ensure they mirror each other rather than operate as independent monitors.

In these cases, all security procedures must be followed and the test administered in a secure environment to prevent others from hearing the questions or viewing the student or test administrator screens.

Secure Browser Versions for Online Testing

Table 14 lists the secure browsers for each operating system. A secure browser must be downloaded and installed on each device used for student testing. **LEAs that installed a secure browser with a version older than the versions listed in Table 14 must uninstall it before installing the secure browser for the 2018–19 school year.**

Table 14. Secure Browsers by Operating System

Operating Systems	Secure Browser
Windows 7 SP1 (Professional and Enterprise)	10.3
Windows 8.0 (Professional and Enterprise)	10.3
Windows 8.1 (Professional and Enterprise)	10.3
Windows 10 and 10 in S mode (Professional, Educational, and Enterprise) • Versions 1507–1803 • Version 1809 (upon acceptance)	10.3
Windows Server • 2008 • 2012 • 2016 (thin client)	10.3
Mac OS X • Versions 10.9–10.14	10.3
Linux Fedora 25–26 LTS (Gnome)	10.3
Linux Ubuntu LTS (Gnome) • Version 14.04 • Version 16.04 • Version 18.04	10.3
iOS (iPads) • Version 10.3 • Version 11.4 • Version 12	AIRSecureTest Mobile Secure Browser 5
Android • Version 7.1 • Version 8.1 • Version 9	AIRSecureTest Mobile Secure Browser 5
Chrome OS 67+ and above	AIRSecureTest kiosk application 5

Forbidden Application Detection

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

Warning: Forbidden Applications and Testing

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

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

Secure Browser Error Messages

Secure Browser Not Detected

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

Unable to Establish a Connection with the Test Delivery System

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

Installing the Secure Browser on Desktops and Laptops

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

Installing the Secure Browser on Windows

Additional Resources:

- California Assessment of Student Performance and Progress (CAASPP) Portal website—http://www.caaspp.org/
- CAASPP Secure Browsers website—http://ca.browsers.airast.org/
- Microsoft Windows IT Pro Center | Take tests in Windows 10 web page—https://docs.microsoft.com/en-us/education/windows/take-tests-in-windows-10

This subsection provides instructions for installing the secure browser on computers running on versions 7 SP1, 8.0, 8.1, 10, and 10 in S mode. (The secure browser does not run on other versions of Windows.)

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

Installing the Secure Browser on an Individual Computer

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

Installing the Secure Browser via Windows

In this scenario, a user with administrator rights installs the secure browser using standard Windows. (If you do not have administrator rights, refer to the subsection "Installing the Secure Browser Without Administrator Rights.")

1. If you installed a previous version of the secure browser in a location other than a default location—`C:\Program Files (x86)\CASecureBrowser\` (64 bit) or `C:\Program Files)\CASecureBrowser\` (32 bit)—manually uninstall the secure browser and its associated desktop shortcut. (If you installed in the default location, the installation package automatically removes it.) See the instructions in the subsection "Uninstalling the Secure Browser on Windows."
2. Navigate to the CAASPP Secure Browsers web page by going to the CAASPP Portal website and selecting the [**Secure Browsers**] button.

3. Scroll down the CAASPP Secure Browsers web page to the "Download Secure Browsers" section.
4. Select the [**Windows**] tab and then select the [**Download Browser**] button (shown as highlighted in Figure 60). A dialog box opens.

Figure 60. [Download Browser] button

5. Take one of the following steps; this step may vary depending on the web browser you are using:
   a. If presented with a choice to run or save the file, select [**Run**]. This opens the Secure Browser Setup wizard.
   b. If presented only with the option to save, save the file to a convenient location. After saving the file, double-click the installation file `CASecureBrowser-Win.msi` to open the setup wizard.
6. Follow the instructions in the setup wizard. When prompted for setup type, select [**Install**].
7. Select [**Finish**] to exit the setup wizard. The following items are installed:
   - The secure browser to the default location `C:\Program Files (x86)\CASecureBrowser\` (64 bit) or `C:\Program Files\CASecureBrowser\` (32 bit)
   - A shortcut `CASecureBrowser` to the desktop (shown in Figure 61).

Figure 61. [CASecureBrowser] shortcut icon

8. Ensure all background jobs, such as virus scans or software updates, are scheduled outside of test windows. For example, if your testing takes place between 8 a.m. and 3 p.m., schedule background jobs outside of these hours.
9. *Optional:* Apply proxy settings by taking the following steps:
   a. Right-click the [**CASecureBrowser**] shortcut icon on the desktop and select "Properties."
   b. Under the [**Shortcut**] tab, in the *Target* field, modify the command to specify the proxy. See Table 15 for available forms of this command.
   c. Select [**OK**] to close the *Properties* dialog box.

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

10. Run the secure browser by double-clicking the [**CASecureBrowser**] shortcut icon on the desktop (shown in Figure 61). The secure browser opens displaying the student logon screen. The secure browser fills the entire screen and hides the task bar.
11. To exit the secure browser, select [**CLOSE SECURE BROWSER**] in the upper-right corner of the screen.

Installing the Secure Browser via the Command Line

In this scenario, a user with administrator rights installs the secure browser from the command line. If you do not have administrator rights, refer to the subsection "Installing the Secure Browser Without Administrator Rights."

1. If you installed a previous version of the secure browser in a location other than `C:\Program Files (x86)\` (64 bit) or `C:\Program Files\` (32 bit), manually uninstall the secure browser. (If you installed in `C:\Program Files (x86)\`, the installation package automatically removes it.) See the instructions in the subsection "Uninstalling the Secure Browser on Windows."
2. Navigate to the CAASPP Secure Browsers web page by going to the CAASPP Portal website and selecting the [**Secure Browsers**] button.
3. Scroll down the CAASPP Secure Browsers web page to the "Download Secure Browsers" section.
4. Select the [**Windows**] tab and then select the [**Download Browser**] button (shown in Figure 62). A dialog box opens.

Figure 62. [Download Browser] button

5. Save the file on the computer (this step may vary depending on the web browser you are using):
   a. If presented with a choice to run or save the file, select [**Save**] and save the file to a convenient location.
   b. If presented only with the option to save, save the file to a convenient location.
6. Note the full path and file name of the downloaded file, such as `c:\temp\CASecureBrowser-Win.msi`.
7. Open a command prompt.
8. Run the command `msiexec /I <Source> [/quiet] [INSTALLDIR=<Target>]`

`<Source>` Path to the installation file, such as `C:\temp\CASecureBrowser-Win.msi`

`<Target>` Path to the location where you want to install the secure browser. If absent, it installs to the directory described in step 10; the installation program creates the directory if it does not exist

`/I` Perform an install

`[/quiet]` Quiet mode, no interaction

For example, the command

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

installs the secure browser from the installation package at `C:\temp\CASecureBrowser-Win.msi` into the directory `C:\AssessmentTesting\BrowserInstallDirectory` using quiet mode.

9. Follow the instructions in the setup wizard. When prompted for setup type, select [**Install**].
10. Select [**Finish**] to exit the setup wizard. The following items are installed:
    - The secure browser to the default location `C:\Program Files (x86)\CASecureBrowser\` (64 bit) or `C:\Program Files\CASecureBrowser\` (32 bit).
    - A shortcut `CASecureBrowser` to the desktop.
11. Ensure all background jobs, such as virus scans or software updates, are scheduled outside of test windows. For example, if your testing takes place between 8 a.m. and 3 p.m., schedule background jobs outside of these hours.
12. Run the secure browser by double-clicking the [**CASecureBrowser**] shortcut icon on the desktop (shown in Figure 63). The secure browser opens, displaying the student logon screen. The secure browser fills the entire screen and hides the task bar.

Figure 63. [CASecureBrowser] shortcut icon

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

Sharing the Secure Browser over a Network

Warning: Testing Quality over a Network

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

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

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

Figure 64. [CASecureBrowser] shortcut icon

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

Copying the Secure Browser Installation Directory to Testing Computers

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

1. On the machine from where you will copy the installation directory, install the secure browser following the directions in the subsection "Installing the Secure Browser on an Individual Computer." Note the path of the installation directory, such as `C:\Program Files (x86)\CASecureBrowser`.
2. Identify the directory on the local testing computers to which you will copy the secure browser file (it should be the same directory on all computers). For example, you may want to copy the directory to `c:\AssesssmentTesting\`. Ensure you select a directory in which the students can run executables.
3. On each local testing computer, do the following:
   a. Ensure all background jobs, such as virus scans or software updates, are scheduled outside of test windows. For example, if your testing takes place between 8 a.m. and 3 p.m., schedule background jobs outside of these hours.
   b. Copy the installation directory used in step 1 from the remote machine to the directory you selected in step 1. For example, if the target directory is `c:\AssesssmentTesting\`, you are creating a new folder `c:\AssesssmentTesting\CASecureBrowser`.
   c. Copy the shortcut `c:\AssesssmentTesting\CASecureBrowser\CASecureBrowser.exe – Shortcut.lnk` to the desktop.
   d. Run the secure browser by double-clicking the `CASecureBrowser` shortcut on the desktop. The secure browser opens, displaying the student logon screen. The secure browser fills the entire screen and hides the task bar.
   e. To exit the secure browser, select [**CLOSE SECURE BROWSER**] in the upper-right corner of the screen.

Installing the Secure Browser for Use with an NComputing Terminal

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

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

For a listing of supported terminals and servers for this scenario, see Chapter 1, System Requirements.

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

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

   If you used a different installation path on the Windows server, use that in the previous command.
4. Save the file to the desktop as `logon.bat`.
5. Create a group policy object that runs the file `logon.bat` each time a user logs on. For details, see Appendix E, Creating Group Policy Objects to Assign Logon ScriptsAppendixE.
6. On each NComputing console, create a new [**CASecureBrowser**] desktop shortcut by taking the following steps. This subprocess is necessary because the default shortcut created by the installation program has an incorrect target.
   a. Connect to the NComputing terminal.
   b. Log on to the Windows server with administrator privileges.
   c. Delete the secure browser's shortcut currently appearing on the desktop.
   d. Navigate to the secure browser's installation directory, usually `C:\Program Files (x86)\CASecureBrowser\`.
   e. Right-click the file `CASecureBrowser.exe` and select *Send To* → *Desktop (create shortcut)*.
   f. On the desktop, right-click the new shortcut and select *Properties*. The *Shortcut Properties* dialog box appears.
   g. Under the [**Shortcut**] tab, in the *Target* field, type the following command:

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

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

Installing the Secure Browser on a Terminal Server or Windows Server

In this scenario, a network administrator installs the secure browser on a server—either a terminal server or a Windows server. Testing machines then connect to the server's desktop and run the secure browser remotely. This scenario is supported on Windows server 2008.

Warning: Testing Quality with Servers

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

Local educational agency CAASPP coordinators should contact the California Technical Assistance Center for instructions and technical support before the secure browser is installed using this scenario.

Installing the Secure Browser Without Administrator Rights

In this scenario, you copy the secure browser from one machine where it is installed onto another machine on which you do not have administrator rights.

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

Uninstalling the Secure Browser on Windows

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

Uninstalling via the User Interface

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

1. Navigate to *Settings* → *System* → *Apps & features* (Windows 10) or *Control Panel* → *Add or Remove Programs* or *Uninstall a Program* (previous versions of Windows).
2. Select the secure browser program `CASecureBrowser` and select [**Remove**] or [**Uninstall**].
3. Follow the instructions in the uninstall wizard.

Uninstalling via the Command Line

1. Open a command prompt.
2. Run the command `msiexec /X <Source> /quiet`

`<Source>`	Path to the executable file, such as `C:\MSI\CASecureBrowser.exe`.
`/X`	Perform an uninstall.
`[/quiet]`	Quiet mode, no interaction.

For example, the command

```
msiexec /X C:\AssessmentTesting\CASecureBrowser.exe
/quiet
```

uninstalls the secure browser installed at `C:\AssessmentTesting\` using quiet mode.

Secure Browser for Windows and the Microsoft Take a Test App

Windows 10 comes with Microsoft's Take a Test app, which enforces a locked-down, secure testing environment identical to AIR's secure browser. Users of the Take a Test app do not need to install the AIR secure browser on the testing machine.

Creating a Dedicated Test Account for Non-permissive Mode Users

Users not using permissive mode should create a dedicated test account for the Take a Test app; permissive mode features will not available when using this method. To access permissive mode features, see the next subsection, "Creating Desktop Shortcuts for Permissive Mode Users".

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

Take the following steps to created a dedicated test account:

1. Sign into the device with an administrator account.
2. Go to *Settings* > *Accounts* > *Work or school Access* > *Set up an account for taking tests*.
3. Select an existing account to use as the dedicated testing account.

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

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

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

Creating Desktop Shortcuts for Permissive Mode Users

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

1. Log on to Windows as the user taking a test.
2. Right-click on the Desktop and select *New* > *Shortcut*. The Create Shortcut dialog box appears (Figure 65. *Create Shortcut* dialog box).

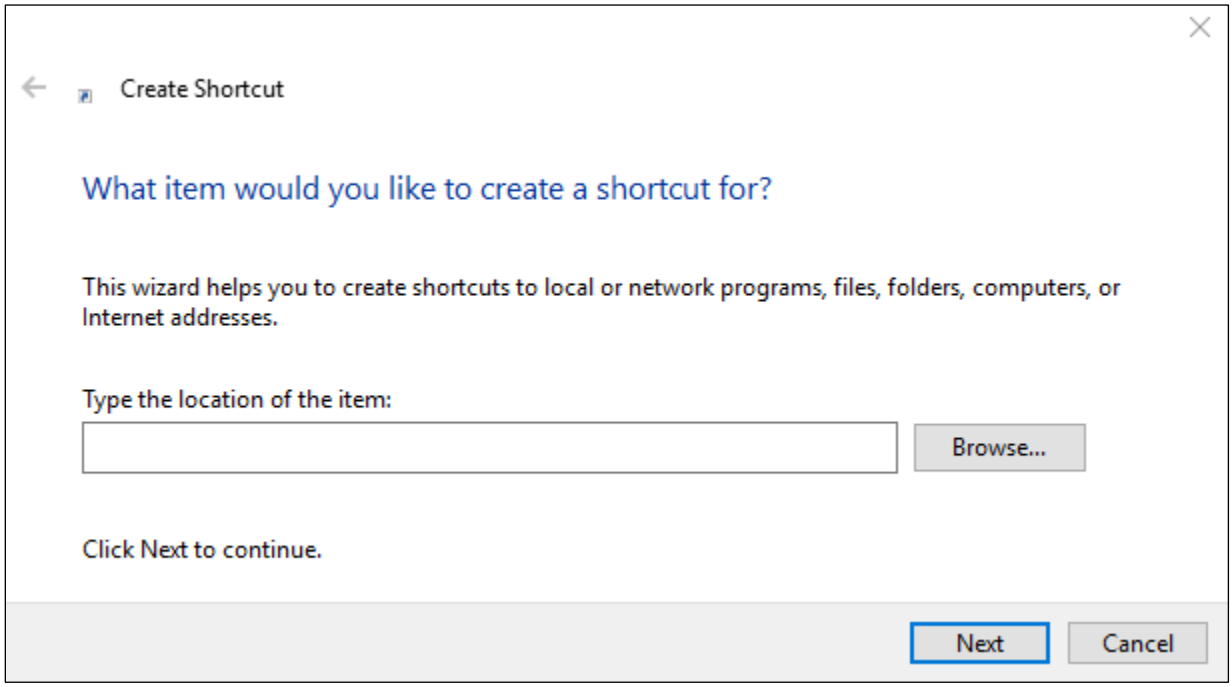


Figure 65. *Create Shortcut* dialog box

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

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

Installing the Secure Browser on Mac OS X

Additional Resources:

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

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

Installing the Secure Browser on an Individual Apple Computer

In this scenario, a user installs the secure browser on Apple desktop and laptop computers running Mac OS X 10.9 through 10.14. The steps in this procedure may vary depending on your version of Mac OS X and your web browser.

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

Figure 66. [Download Browser] button

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

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

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

7. **If you are running Mac OS X 10.11**, follow these additional steps to temporarily allow installation from any source. Otherwise, proceed to step 8.
   a. Open System Preferences (*Apple* → *System Preferences*).
   b. Select the [**Security and Privacy**] icon.
   c. In the [**General**] tab, select the lock in the bottom-left corner of the screen (indicated in Figure 68) and then type your password to enable changes.

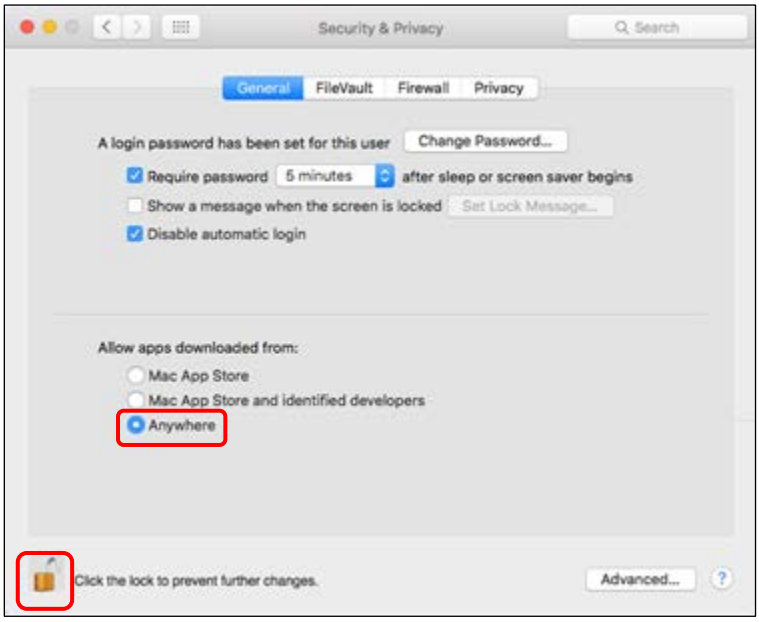


Figure 68. *Security & Privacy* screen for Mac OS X 10.11

d. In the "Allow apps downloaded from" section, first note which radio button is highlighted, and then select the *Anywhere* radio button (also indicated in Figure 68).

e. Select [**Allow From Anywhere**] in the confirmation message.

8. Drag the **[CASecureBrowser]** icon to the folder. This installs the secure browser into Applications.

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

10. Disable Mission Control/Spaces. Instructions for disabling Spaces are in Chapter 3, Hardware Configuration.

11. In Finder, navigate to *Go* → *Applications*, and then double-click `CASecureBrowser` to launch the secure browser. (You must launch the secure browser to complete the installation.) The secure browser opens displaying the student logon screen. The secure browser fills the entire screen and hides the dock.

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

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

13. To create a desktop shortcut, from the Applications folder, drag `CASecureBrowser` to the desktop.

14. **Mac OS X 10.11 only:** Restore security settings by reversing the process in step 7 and resetting the **"Allow apps downloaded from" setting to what it had been previously.**

Cloning the Secure Browser Installation to Other Macs

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

To clone the secure browser installation to other Macs:

1. On the Mac from where you will clone the installation, do the following:

   a. Install the secure browser following the directions in the subsection "Installing the Secure Browser on an Individual Apple Computer." Be sure to run and then close the secure browser after the installation.

   b. In Finder, display the `Library` folder.

   c. Open the `Application Support` folder. The *Application Support* configuration interface opens.

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

e. Delete the `Mozilla` folder (also indicated in Figure 69).

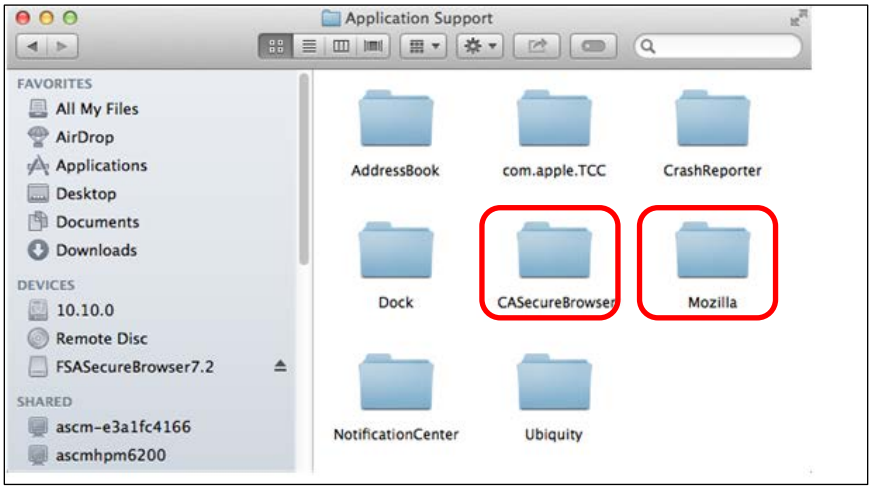


Figure 69. Apple *Application Support* configuration interface

2. Create a shell script that creates a new secure browser profile when a user logs in. The basic command to create a profile is `<install_directory>/Contents/MacOS/CASecureBrowser--CreateProfile profile_name`, where `profile_name` is unique among all testing computers.
3. Clone the OS X image.
4. Deploy the image to the target Macs.

Uninstalling the Secure Browser on OS X

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

Installing the Secure Browser on Linux

Additional Resources:

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

This subsection provides instructions for installing the secure browser on computers running a supported Linux distribution. For additional information about Linux requirements, refer to the subsection "Configuring Linux for Online Testing with the Secure Browser."

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

The instructions in this subsection are for installing the Linux secure browser onto 32- or 64-bit versions of Linux systems. These instructions may vary for your individual Linux distribution.

1. Uninstall any previous versions of the secure browser by deleting the directory containing it.
2. Obtain the root or superuser password for the computer on which you are installing the secure browser.
3. Navigate to the CAASPP Secure Browsers web page by going to the CAASPP Portal website and selecting the [**Secure Browsers**] button.
4. Scroll down the CAASPP Secure Browsers web page to the "Download Secure Browsers" section.
5. Select the [**Linux**] tab and then select the [**Download Browser**] button (shown as highlighted in Figure 70).

Figure 70. [Download Browser] button

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

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

Figure 71. [CASecureBrowser] shortcut icon

12. Enter the password. The script installs all dependent libraries and supported voice packs, and creates a [**CASecureBrowser**] icon on the desktop.
13. Ensure all background jobs, such as virus scans or software updates, are scheduled outside of test windows. For example, if your testing takes place between 8 a.m. and 3 p.m., schedule background jobs outside of these hours.
14. If text-to-speech testing is performed on this computer, reboot it.
15. From the desktop, double-click the [**CASecureBrowser**] icon to launch the secure browser. The student logon screen appears. The secure browser fills the entire screen and hides any panels or launchers.
16. To exit the secure browser, select [**CLOSE SECURE BROWSER**] in the upper-right corner of the screen.

Extracting the Secure Browser TAR File

Users attempting to install the secure browser on Fedora 27–28 or Ubuntu 18.04 may encounter an issue where the secure browser extracts to the `Home` folder and not the `Desktop` folder. This is a feature in these operating systems and *not* an error in the secure browser. The following procedure explains how to extract the secure browser TAR file manually using terminal commands.

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

Creating a Shortcut to Secure Browser 10

Installation of secure browser version 10 on machines running Fedora or Ubuntu Linux will not automatically install a shortcut to the browser. Users must manually create a shortcut. The following procedure explains how to complete this process.

1. Open Terminal.

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

Uninstalling the Secure Browser on Linux

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

Installing the Secure Browser on Mobile Devices

This section contains information about installing AIRSecureTest, the secure browser app for iOS, Android, and Chrome OS. For information about configuring supported tablets and Chromebooks to work with the secure browser, refer to Chapter 3, Hardware Configuration.

Installing the Secure Browser on iOS

Additional Resources:

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

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

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

Instructions for Installation

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

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

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

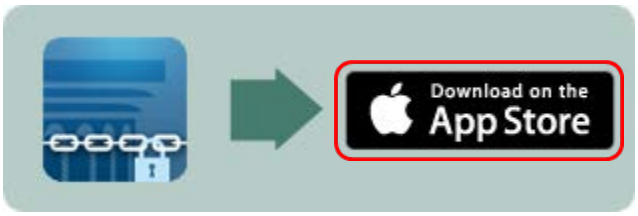


Figure 72. [Download on the App Store] button

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

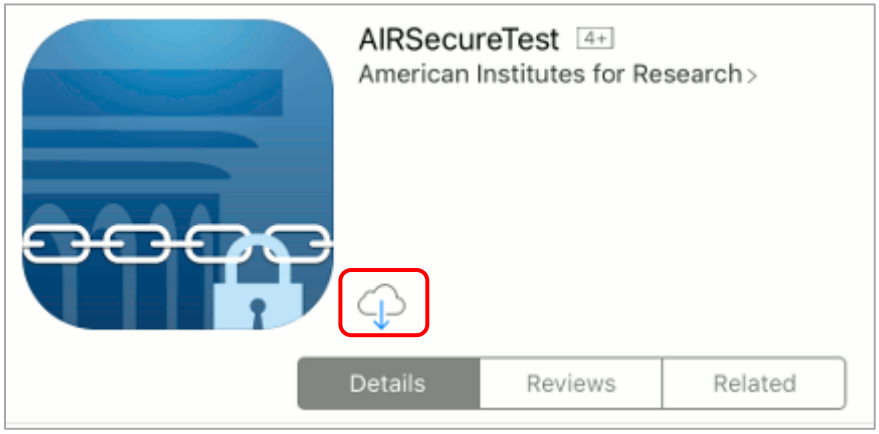


Figure 73. AIRSecureTest App Store download web page

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

Figure 74. [AirSecureTest] icon, iOS

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

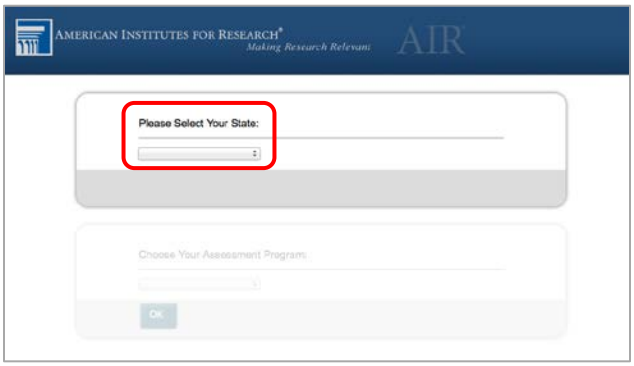


Figure 75. Select the state from the Launchpad

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

Figure 76. Select the assessment from the Launchpad

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

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

Guidance on iOS Classroom and Summative Testing

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

Using MDM to Disable Classroom Observation

You can use the Boolean key `allowScreenShot` to disable access to the Classroom observation feature on student devices. This key is defined as part of the Restrictions profile payload. See the Apple Configuration Profile Reference web page for instructions and more information about using this key.

Installing AIRSecureTest on Android

Additional Resources:

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

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

Downloading and Installing the Android AIRSecureTest Mobile Secure Browser

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

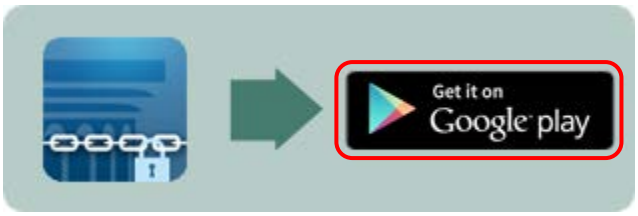


Figure 77. [Get it on Google play] button

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

Figure 78. AIRSecureTest Google Play download web page

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

Figure 79. [AIRSecureTest] icon, Android

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

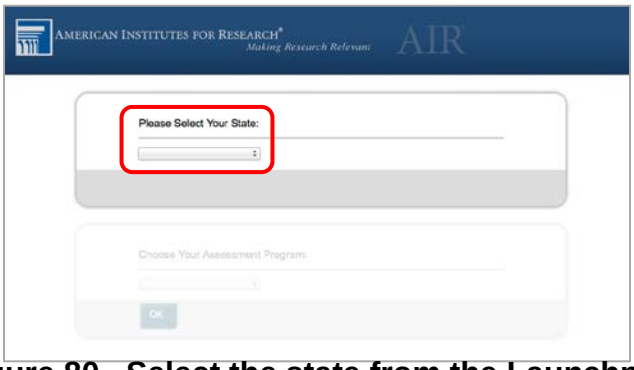


Figure 80. Select the state from the Launchpad

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

Figure 81. Select the assessment from the Launchpad

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

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

Caution:

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

Chrome OS AIRSecureTest Kiosk App

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

Caution: Due to recent changes by Google, users with Chromebooks manufactured in 2017 or later who do not have an Enterprise or Education license will not be able to use those machines for assessments. Google no longer allows users without these licenses to set up kiosk mode, which is necessary to run the AIR Secure Browser. (This change restricting kiosk mode does not affect the Chrome operating system. You can still use any version of the Chrome OS on hardware manufactured in 2016 or earlier.)

Installing the AIRSecureTest Kiosk App on Standalone Chromebooks

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

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

1. Obtain the following from your network administrator:
   - The wireless network to which the Chromebook connects. This typically includes the network's service set identifier, password, and other access credentials.
   - An email address and password for logging on to Gmail.
2. Power off and then power on your Chromebook.
3. If the `OS verification is Off` message appears, take the following steps; otherwise, skip to step 4.
   a. Press the [Spacebar]. In the confirmation screen, press [Enter]. The Chromebook reboots.
   b. In the *Welcome* screen shown in Figure 82, select your language, keyboard, and the wireless network information you acquired from the network administrator, and then select [**Continue**].

Figure 82. Chromebook *Welcome* screen

c. In the *Google Chrome OS Terms* screen, select [**Accept and continue**].

4. When the *Sign in* screen appears, wipe data from the Chromebook by taking the following steps:

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

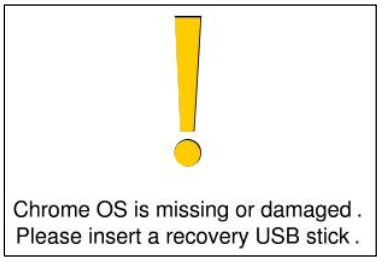


Figure 83. Chrome OS *Missing* message

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

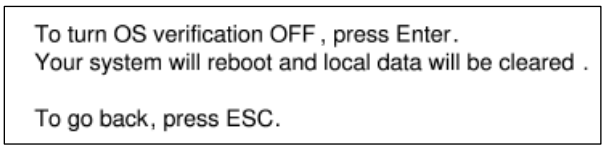


Figure 84. Turn OS Verification Off message

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

Figure 85. OS Verification Is Off message

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

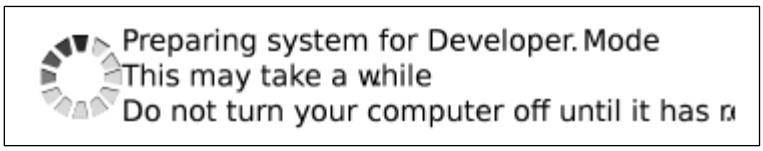


Figure 86. Preparing for Developer Mode message

e. After the Chromebook reboots, the `OS verification is Off` message (Figure 85) appears again.

f. Press the [Spacebar] and then press [Enter]. The Chromebook reboots, and the *Welcome* screen appears (Figure 82).

5. In the *Welcome* screen, select your language, keyboard, and a network. The *Join WiFi Network* screen appears (Figure 87).

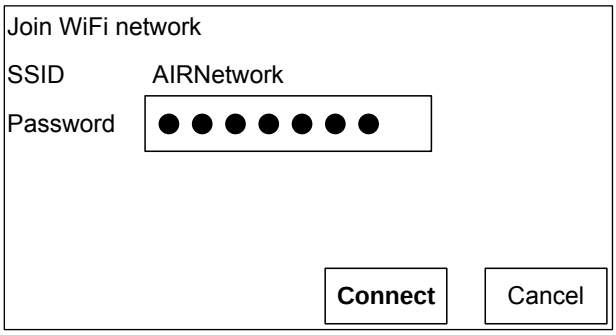


Figure 87. *Join WiFi Network* screen

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

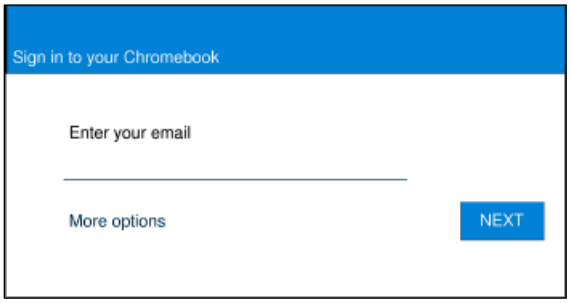


Figure 88. Chromebook *Sign in* screen

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

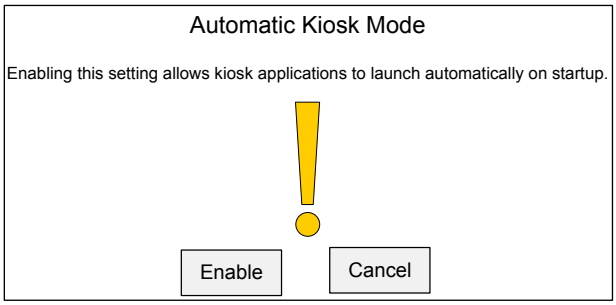


Figure 89. Automatic Kiosk Mode message

10. Select [**Enable**] and then select [**OK**] to open the *Sign in* screen (Figure 88).
11. In the *Sign in* screen, enter your email address, select [**Next**], enter the password, and then select [**Next**] again.
12. When the desktop opens, select the [**Chrome**] icon [ ] to open Chrome.
13. In the URL bar, enter `chrome://extensions` to open the *Extensions* screen (Figure 90).

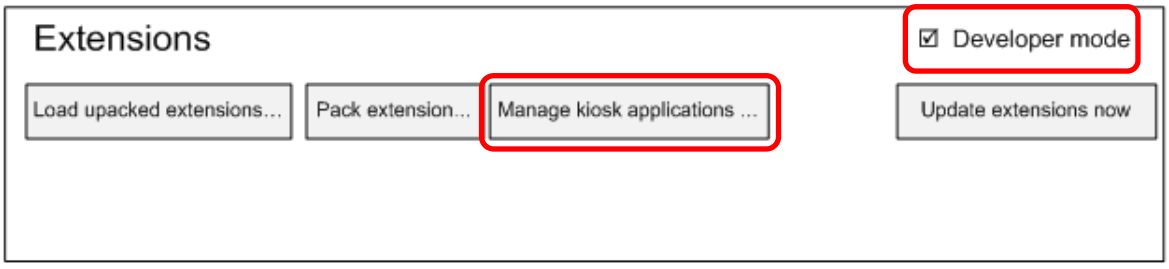


Figure 90. *Extensions* screen

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

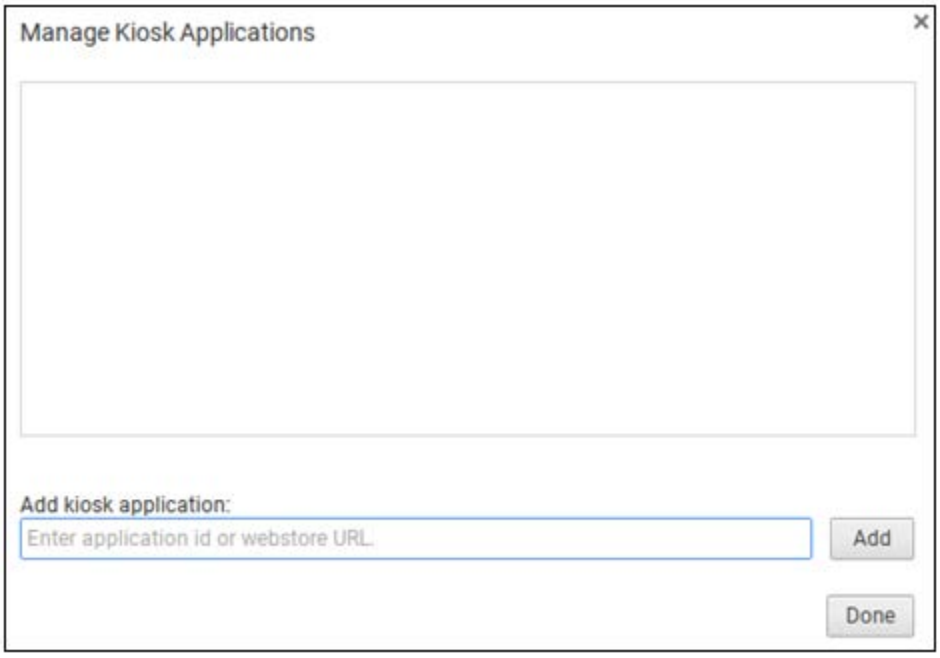


Figure 91. *Manage Kiosk Applications* screen

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

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

    You need to re-install the app in kiosk mode by following the procedure in this subsection.
20. Configure the test administration by following the procedure in the subsection "Opening the AIRSecureTest Kiosk App and Selecting the Assessment Program."

Installing the AIRSecureTest Kiosk App on Managed Chromebooks

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

Caution: AIRSecureTest is not compatible with public sessions.

1. Set up your free Google Apps for Education account and enroll all managed Chromebooks.
2. As the Chromebook administrator, access the Sign in web page to log on to your Admin console using your Google Apps for Education account.
3. Select [**Device management**] (indicated in Figure 92).

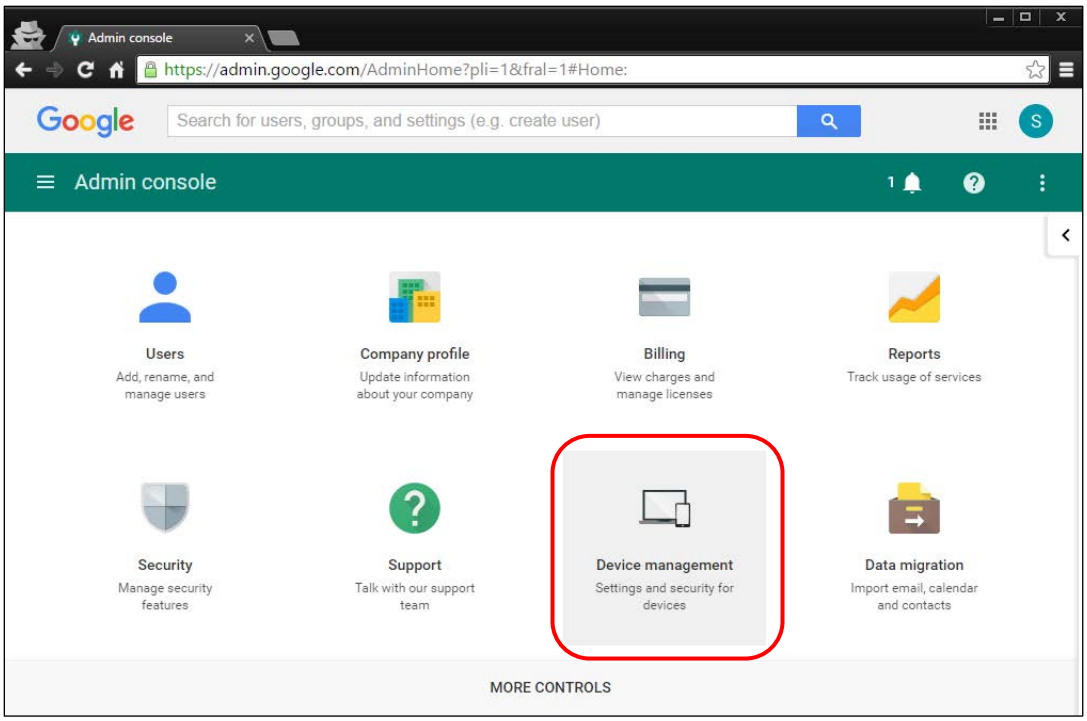


Figure 92. Chrome *Admin console* screen

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

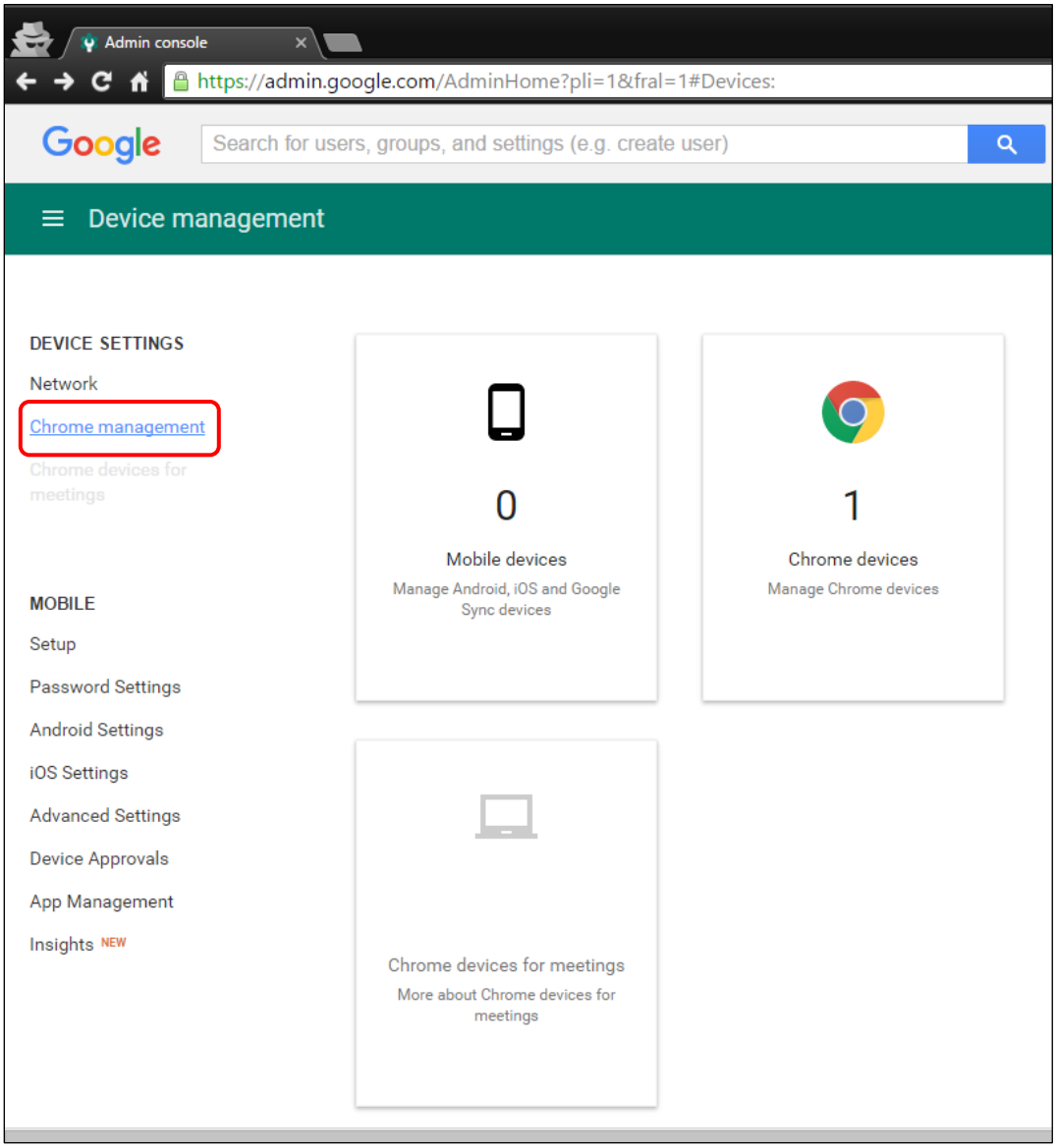


Figure 93. Chrome *Device management* screen

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

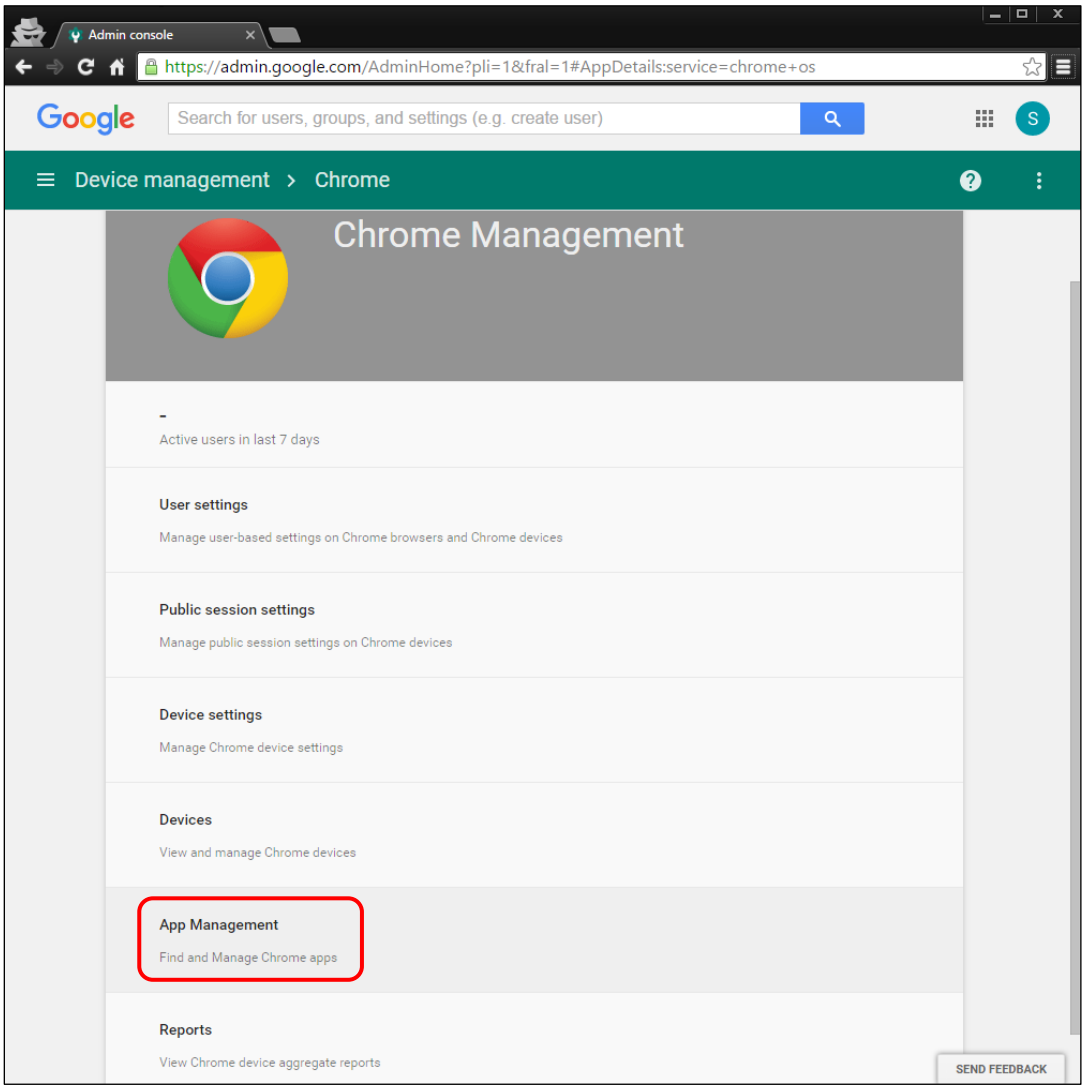


Figure 94. *Chrome Management* screen

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

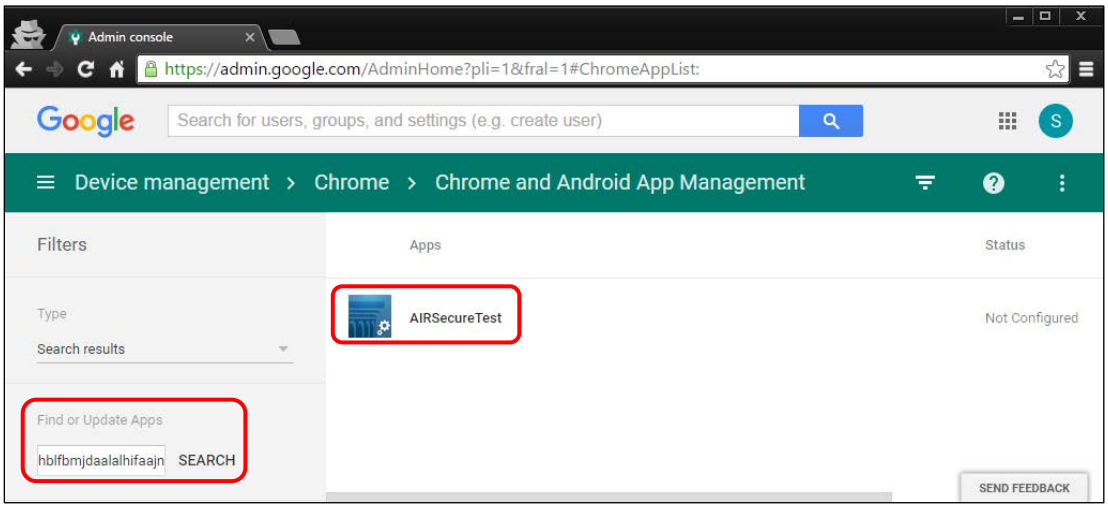


Figure 95. Chrome *App Management* screen

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

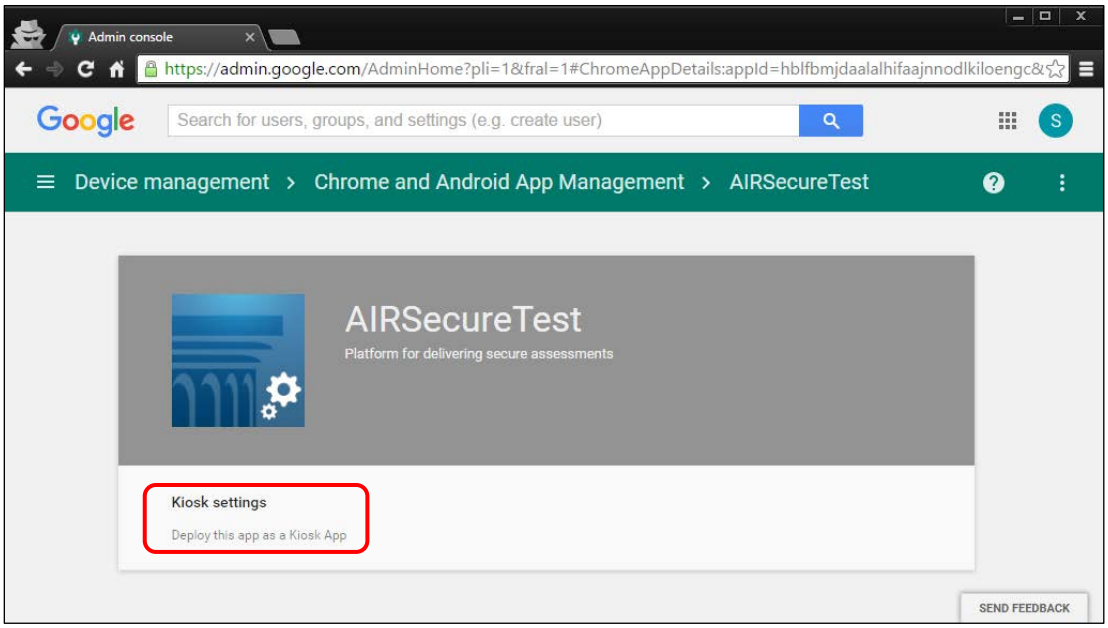


Figure 96. Select [Kiosk settings]

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

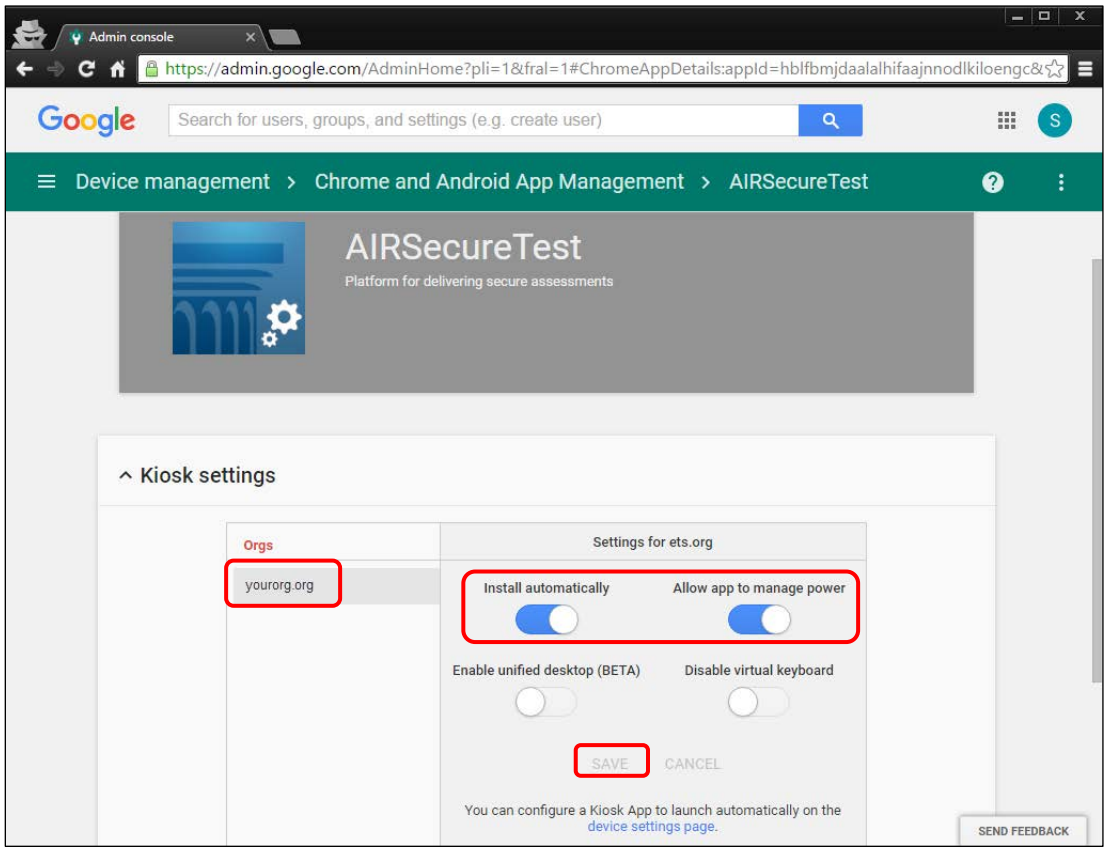


Figure 97. Chrome *Kiosk settings* screen

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

Notes:

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

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

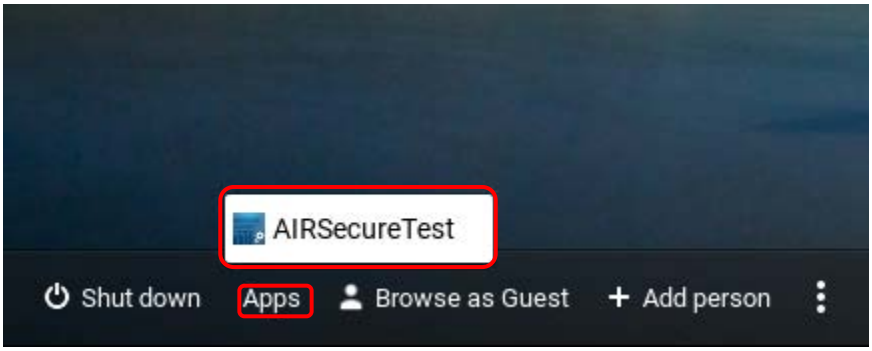


Figure 98. Chromebook logon screen

Opening the AIRSecureTest Kiosk App and Selecting the Assessment Program

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

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

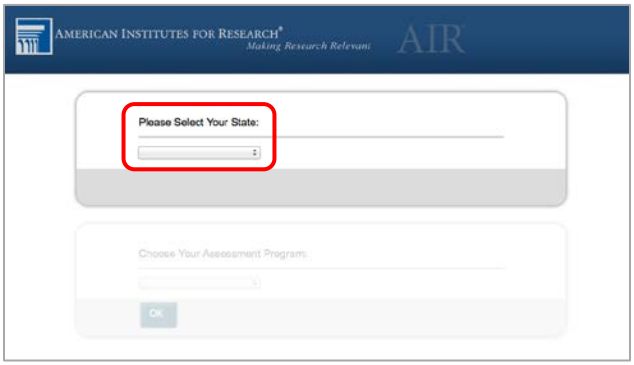


Figure 99. Select the state from the Launchpad

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

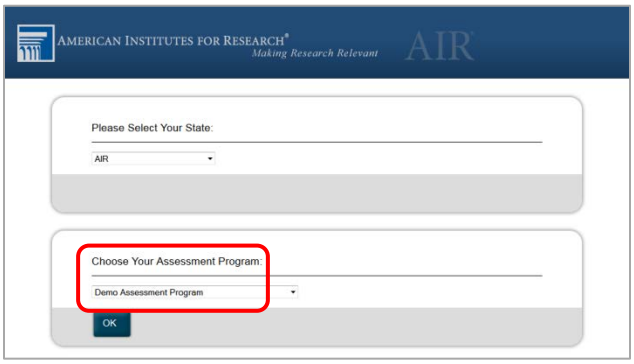


Figure 100. Select the assessment from the Launchpad

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

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

Installing the Secure Browser on Windows Mobile Devices

The procedure for installing the secure browser on Windows mobile devices is the same for installing it on desktops. See the subsection "Installing the Secure Browser via Windows" for details.

Proxy Settings for Desktop Secure Browsers

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

Specifying a Proxy Server to Use with the Secure Browser

By default, the secure browser attempts to detect the settings for your network's web proxy server. Users of web proxies should execute a proxy command once from the command prompt; this command does not need to be added to the secure browser shortcut. Table 15 lists the form of the command for different settings and operating systems. To execute these commands from the command line, change to the directory containing the secure browser's executable file.

Note: The commands in Table 15 uses the domain `fake-url.com`. When configuring for a proxy server, use your actual testing domain names as listed in Appendix B, URLs for Testing Systems.

Table 15. Specifying Proxy Settings Using a Shortcut or the Command Line

Description	System	Command
Use the secure browser without any proxy	Windows	`CASecureBrowser.exe -proxy 0 aHR0cHM6Ly9jYS50ZHMuYWlyYXN0Lm9yZy9zdHVkZW50`
Use the secure browser without any proxy	Mac 10.9–10.14	`./CASecureBrowser -proxy 0 aHR0cHM6Ly9jYS50ZHMuYWlyYXN0Lm9yZy9zdHVkZW50`
Use the secure browser without any proxy	Linux	`./CASecureBrowser.sh -proxy 0 aHR0cHM6Ly9jYS50ZHMuYWlyYXN0Lm9yZy9zdHVkZW50`
Set the proxy for HTTP requests only	Windows	`CASecureBrowser.exe -proxy 1:http:fake-url.com:80 aHR0cHM6Ly9jYS50ZHMuYWlyYXN0Lm9yZy9zdHVkZW50`
Set the proxy for HTTP requests only	Mac 10.9–10.14	`./CASecureBrowser -proxy 1:http:fake-url.com:80 aHR0cHM6Ly9jYS50ZHMuYWlyYXN0Lm9yZy9zdHVkZW50`

Description	System	Command
Set the proxy for HTTP requests only	Linux	`./CASecureBrowser.sh -proxy 1:http:fake-url.com:80 aHR0cHM6Ly9jYS50ZHMuYWlyYXN0Lm9yZy9zdHVkZW50`
Set the proxy for all protocols to mimic the "Use this proxy server for all protocols" of Firefox	Windows	`CASecureBrowser.exe -proxy 1:*:fake-url.com:80 aHR0cHM6Ly9jYS50ZHMuYWlyYXN0Lm9yZy9zdHVkZW50`
Set the proxy for all protocols to mimic the "Use this proxy server for all protocols" of Firefox	Mac 10.9–10.14	`./CASecureBrowser -proxy 1:*:fake-url.com:80 aHR0cHM6Ly9jYS50ZHMuYWlyYXN0Lm9yZy9zdHVkZW50`
Set the proxy for all protocols to mimic the "Use this proxy server for all protocols" of Firefox	Linux	`./CASecureBrowser.sh -proxy 1:*:fake-url.com:80 aHR0cHM6Ly9jYS50ZHMuYWlyYXN0Lm9yZy9zdHVkZW50`
Specify the URL of the PAC file	Windows	`CASecureBrowser.exe -proxy 2:fake-url.com aHR0cHM6Ly9jYS50ZHMuYWlyYXN0Lm9yZy9zdHVkZW50`
Specify the URL of the PAC file	Mac 10.9–10.14	`./CASecureBrowser -proxy 2:fake-url.com aHR0cHM6Ly9jYS50ZHMuYWlyYXN0Lm9yZy9zdHVkZW50`
Specify the URL of the PAC file	Linux	`./CASecureBrowser.sh -proxy 2:fake-url.com aHR0cHM6Ly9jYS50ZHMuYWlyYXN0Lm9yZy9zdHVkZW50`
Auto detect proxy settings	Windows	`CASecureBrowser.exe -proxy 4 aHR0cHM6Ly9jYS50ZHMuYWlyYXN0Lm9yZy9zdHVkZW50`
Auto detect proxy settings	Mac 10.9–10.14	`./CASecureBrowser -proxy 4 aHR0cHM6Ly9jYS50ZHMuYWlyYXN0Lm9yZy9zdHVkZW50`

Description	System	Command
Auto detect proxy settings	Linux	`./CASecureBrowser.sh -proxy 4 aHR0cHM6Ly9jYS50ZHMuYWlyYXN0Lm9yZy9zdHVkZW50`
Use the system proxy setting (default)	Windows	`CASecureBrowser.exe -proxy 5 aHR0cHM6Ly9jYS50ZHMuYWlyYXN0Lm9yZy9zdHVkZW50`
Use the system proxy setting (default)	Mac 10.9–10.14	`./CASecureBrowser -proxy 5 aHR0cHM6Ly9jYS50ZHMuYWlyYXN0Lm9yZy9zdHVkZW50`
Use the system proxy setting (default)	Linux	`./CASecureBrowser.sh -proxy 5 aHR0cHM6Ly9jYS50ZHMuYWlyYXN0Lm9yZy9zdHVkZW50`

Modifying Desktop Shortcuts to Include Proxy Settings

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

Modifying Desktop Shortcuts on Microsoft Windows

1. Right-click the desktop shortcut for the secure browser and select *Properties* from the shortcut menu.
2. Select the [**Shortcut**] tab.
3. If the *Target* field is disabled, do the following (otherwise, skip to step 4):
   a. Close the *Properties* dialog box and delete the desktop shortcut for the secure browser.
   b. **If you have a `/Program Files (x86)` subdirectory:** Create a new desktop shortcut in Windows Explorer by navigating to your relevant 32-bit subdirectory, `C:\Program Files (x86)\`. Right-click the file `CASecureBrowser.exe` and then select *Send To* → *Desktop (create shortcut)*.
   c. **If you do not have a `/Program Files (x86)` subdirectory:** Create a new desktop shortcut in Windows Explorer by navigating to `C:\Program Files\CASecureBrowser\`, right-clicking the file `CASecureBrowser.exe`, and then selecting *Send To* → *Desktop (create shortcut)*.
   d. Right-click the desktop shortcut for the secure browser and select *Properties*.
   e. Select the [**Shortcut**] tab.

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

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

5. Select [**OK**].

Modifying Desktop Shortcuts on Mac OS X

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

   ```
   cd ~/Desktop
   ```

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

   ```
   pico securebrowser.command.
   ```

4. Copy or type the following lines:

   ```
   #!/bin/sh
   ```

   ```
   /Applications/CASecureBrowser.app/Contents/MacOS/./
   CASecureBrowser -proxy 1:http:fake-url.com:80 &
   aHR0cHM6Ly9jYS50ZHMuYWlyYXN0Lm9yZy9zdHVkZW50
   ```

5. Be sure to specify the complete path to the secure browser and the desired proxy option. Ensure the command ends with an ampersand (`&`).Save the file and exit the editor by pressing [Ctrl] + [O], [Enter], and then [Ctrl] + [X].
6. Apply execute permission to the file. In Terminal, type

   ```
   chmod a+x securebrowser.command
   ```

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

This page is left blank intentionally.