Oregon Statewide Assessment System

Secure Browser Installation Manual

For Technology Coordinators

2018-2019

Published November 13, 2018

Prepared by the American Institutes for Research®

Table of Contents

Table of Figures

Table of Tables

Section I. Introduction to the Secure Browser Manual

The Secure Browser is a web browser for taking online assessments. The Secure Browser prevents students from accessing other computer or Internet applications and from copying test information. It also occupies the entire computer screen.

Major Changes

The list below details major changes to the document for the 2018-2019 school year.

- Update Take a Test app instructions

Scope

This manual provides instructions for installing the Secure Browsers on computers and devices used for online assessments.

System Requirements

For the Secure Browser to work correctly, the computer on which you install it must have a supported operating system. For a list of supported operating systems, see the *Technical Specifications Manual for Online Testing* available from the Oregon Statewide Assessment System portal at oaksportal.org.

Manual Content

This manual is organized as follows:

- Section I, Introduction to the Secure Browser Manual (this section), describes this guide.
- Section II, Installing the Secure Browser on Desktops and Laptops, includes instructions for installing the Secure Browser onto supported Windows and Mac platforms.
- Section III, Installing the Secure Browser on Mobile Devices, includes instructions for installing the mobile Secure Browser onto supported iOS and Chrome OS platforms.
- Section IV, Proxy Settings for Desktop Secure Browsers, provides commands for specifying proxy servers that the Secure Browser should use.
- Appendix A, Creating Group Policy Objects, describes how to create scripts that launch when a user logs into a Windows computer.
- Appendix B, Resetting Secure Browser Profiles, provides instructions for resetting Secure Browser profiles.

- Appendix C, User Support, provides Help Desk information.

Intended Audience

This installation guide is intended for the following audiences:

- Technology coordinators familiar with downloading installation packages from the Internet or from a network location and installing software onto Windows or Mac operating systems or Chromebook or iPad devices.
- Network administrators familiar with mapping or mounting network drives, and creating and running scripts at the user and host level.
- If you install and run the Secure Browser from an NComputing server, you should be familiar with operating that software and related hardware.

Document Conventions

Table 1 lists typographical conventions and key symbols.

Table 1. Document conventions

Element	Description
	**Warning:** This symbol accompanies important information regarding actions that may cause fatal errors.
	**Alert:** This symbol accompanies important information regarding a task that may cause minor errors.
	**Tip:** This symbol accompanies useful information on how to perform a task.
`filename`	Monospaced text indicates a directory, filename, or something you enter in a field.
text	Bold text indicates a link or button that is clickable.

Other Resources

- For information about securing a computer before a test session, see the *Test Administrator User Guide*.
- For information about supported operating systems and web browsers, network and Internet requirements, general peripheral and software requirements, and configuring text-to-speech settings, see the *Technical Specifications Manual for Online Testing*.

- For information about supported hardware and software for Braille testing as well as information about configuring JAWS, see the *Braille Requirements and Testing Manual.*

These documents are available at oaksportal.org.

Section II. Installing the Secure Browser on Desktops and Laptops

This section contains installation instructions for Windows and Mac under a variety of deployment scenarios. Some scenarios describe installing the Secure Browser on a shared network drive, from which students would then run the Browser. However, there are significant drawbacks in this method. Running the Secure Browser from a shared network drive creates contention among the students' client machines for two resources: LAN bandwidth and shared drive I/O. This performance impact can be avoided by installing the Secure Browser locally on each machine. **AIR strongly discourages the use of network shared drive installation for the Secure Browser, as this setup can compromise the stability and performance of the browser, especially during peak testing times.**

Installing the Secure Browser on Windows

This section provides instructions for installing the Secure Browser on computers running supported versions of Windows.

The instructions in this section assume machines 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\`.

TIP. If you are testing on Windows 10, consider using the Take a Test app. See the section "Microsoft Take a Test App" for details.

Installing the Secure Browser on an Individual Computer

This section 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 section Installing the Secure Browser Without Administrator Rights.)

1. If you installed a previous version of the Secure Browser by copying its directory from one computer to another, manually uninstall the Secure Browser by deleting the installation folder and the desktop shortcut. (If you installed the Secure Browser using the Windows installation program, the installation package automatically removes it.) See the instructions in the section Uninstalling the Secure Browser on Windows.

2. Navigate to the **Secure Browsers** page of the Oregon Statewide Assessment System portal at oaksportal.org. Click the **Windows** tab, then click **Download Browser**. A dialog window opens.

3. Do one of the following (this step may vary depending on the browser you are using):

   - If presented with a choice to **Run** or **Save** the file, click **Run**. This opens the Secure Browser Setup wizard.

   - If presented only with the option to **Save**, save the file to a convenient location. After saving the file, double-click the installation file `OAKSSecureBrowser-Win.msi` to open the setup wizard.

4. Follow the instructions in the setup wizard. When prompted for setup type, click **Install**.

5. Click **Finish** to exit the setup wizard. The following items are installed:

   - The Secure Browser to the default location `C:\Program Files (x86)\OAKSSecureBrowser\` (64-bit) or `C:\Program Files)\OAKSSecureBrowser\` (32-bit).

   - A shortcut `OAKSSecureBrowser` to the desktop.

6. 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 8:00 a.m. and 3:00 p.m., schedule background jobs outside of these hours.

7. *Optional:* Apply proxy settings by doing the following:

   a. Right-click the shortcut `OAKSSecureBrowser` on the desktop, and select **Properties**.

   b. Under the **Shortcut** tab, in the **Target** field, modify the command to specify the proxy. See Table 2 for available forms of this command.

   c. Click **OK** to close the Properties dialog box.

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

8. Run the browser by double-clicking the `OAKSSecureBrowser` shortcut on the desktop. The Secure Browser opens displaying the student login screen. The browser fills the entire screen and hides the task bar.

9. To exit the browser, click **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 section Installing the Secure Browser Without Administrator Rights.

1. If you are not signed on to the computer as an administrator, obtain the administrator password.

2. If you installed a previous version of the Secure Browser by copying its directory from one computer to another, manually uninstall the Secure Browser by deleting the installation folder and the desktop shortcut. (If you installed the Secure Browser using the Windows installation program, the installation package automatically removes it.) See the instructions in the section Uninstalling the Secure Browser on Windows.

3. Navigate to the **Secure Browsers** page of the Oregon Statewide Assessment System portal at oaksportal.org. Click the **Windows** tab, then click **Download Browser**. A dialog window opens.

4. Save the file on the computer (this step may vary depending on the browser you are using):

    - If presented with a choice to **Run** or **Save** the file, click **Save**, and save the file to a convenient location.

    - If presented only with the option to **Save**, save the file to a convenient location.

5. Note the full path and filename of the downloaded file, such as `c:\temp\OAKSSecureBrowser-Win.msi`.

6. Open a command prompt as the administrator by doing the following:

    a. Click **Start**, and locate the Command Prompt application. (In some versions of Windows the application is under **All Programs > Accessories > Command Prompt**.)

    b. Right-click **Command Prompt**, and select **Run as Administrator**.

    c. As necessary, type the administrator password for the computer. The command prompt opens.

    (You need to do step 6 only once for the current login. The next time you open the command prompt, Windows retains the administrator role.)

7. Run the command `msiexec /I <Source> [/quiet] [INSTALLDIR=<Target>]`

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

   `<Target>` Path to the location where you want to install the Secure Browser. If absent, installs to the directory described in step 9. 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\OAKSSecureBrowser-Win.msi /quiet
   INSTALLDIR=C:\AssessmentTesting\BrowserInstallDirectory
   ```

   installs the Secure Browser from the installation package at `C:\temp\OAKSSecureBrowser-Win.msi` into the directory `C:\AssessmentTesting\BrowserInstallDirectory` using quiet mode.

8. Follow the instructions in the setup wizard. When prompted for setup type, click **Install**.

9. Click **Finish** to exit the setup wizard. The following items are installed:

   - The Secure Browser to the default location `C:\Program Files (x86)\OAKSSecureBrowser\` (64-bit) or `C:\Program Files\OAKSSecureBrowser\` (32-bit).

   - A shortcut `OAKSSecureBrowser` to the desktop.

10. 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 8:00 a.m. and 3:00 p.m., schedule background jobs outside of these hours.

11. Run the browser by double-clicking the `OAKSSecureBrowser` shortcut on the desktop. The Secure Browser opens displaying the student login screen. The browser fills the entire screen and hides the task bar.

12. To exit the browser, click **CLOSE SECURE BROWSER** in the upper-right corner of the screen.

Sharing the Secure Browser over a Network

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. As stated above, **AIR strongly discourages the use of network shared drive installation for the Secure Browser, as this setup**

can compromise the stability and performance of the browser, especially during peak testing times.

1. On the remote computer from which the students run the Secure Browser, install the Secure Browser following the directions in the section Installing the Secure Browser on an Individual Computer.

2. On each testing machine, sign in and 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 8:00 a.m. and 3:00 p.m., schedule background jobs outside of these hours.

    b. Copy the desktop shortcut `OAKSSecureBrowser` from the remote machine to the directory `C:\Users\Public\Public Desktop`.

    c. Run the browser by double-clicking the `OAKSSecureBrowser` shortcut on the desktop. The Secure Browser opens displaying the student login screen. The browser fills the entire screen and hides the task bar.

    d. To exit the browser, click **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 computer from where you will copy the installation directory, install the Secure Browser following the directions in the section Installing the Secure Browser on an Individual Computer. Note the path of the installation directory, such as `C:\Program Files (x86)\OAKSSecureBrowser`.

2. Identify the directory on the local testing computers to which you will copy the 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 8:00 a.m. and 3:00 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 2. For example, if the target directory is `c:\AssesssmentTesting\`, you are creating a new folder `c:\AssesssmentTesting\OAKSSecureBrowser`.

c. Copy the shortcut `c:\AssesssmentTesting\OAKSSecureBrowser\OAKSSecureBrowser.exe - Shortcut.lnk` to the desktop.

d. Run the browser by double-clicking the `OAKSSecureBrowser` shortcut on the desktop. The Secure Browser opens displaying the student login screen. The browser fills the entire screen and hides the task bar.

e. To exit the browser, click **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 testing coordinator connects consoles to the NComputing terminal, logs in from each to the Windows server, and starts the Secure Browser so that 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 *Technical Specifications Manual for Online Testing* available from the Oregon Statewide Assessment System portal (oaksportal.org).

1. Log in to the machine running the Windows server.

2. Install the Secure Browser following the directions in the section Installing the Secure Browser on an Individual Computer.

3. Open Notepad and type the following command (no line breaks):

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

   If you used a different installation path on the Windows server, use that in the above 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 in. For details, see Appendix A, Creating Group Policy Objects.

6. On each NComputing console, create a new `OAKSSecureBrowser` desktop shortcut by doing the following (this step is necessary because the default shortcut created by the installation program has an incorrect target):

   a. Connect to the NComputing terminal.

   b. Log in to the Windows server with administrator privileges.

   c. Delete the Secure Browser's shortcut appearing on the desktop.

   d. Navigate to the Secure Browser's installation directory, usually `C:\Program Files (x86)\OAKSSecureBrowser\`.

   e. Right-click the file `OAKSSecureBrowser.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)\OAKSSecureBrowser\
      OAKSSecureBrowser.exe" -P%SESSIONNAME%
      ```

      If you used a different installation path on the Windows server, use that in the above command.

   h. Click **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 R2, 2012 R2, and 2016 R2.

Ima 

CAUTION: Testing Quality with Servers Launching a Secure Browser from a terminal or Windows server is typically not a secure test environment, because students can use their local machines to search for answers. Therefore, AIR does not recommend this installation scenario for testing.

1. Log in to the server, and install the Secure Browser by following the directions in the section Installing the Secure Browser on an Individual Computer. Note the path of the installation directory.

2. Copy and paste the line below into Notepad (no line breaks):

   ```
   "C:\Program Files (x86)\OAKSSecureBrowser\OAKSSecureBrowser" -CreateProfile
   %SESSIONNAME%
   ```

   If you used a different installation path, use that in the above command.

3. Save the file to the desktop as `logon.bat`.

4. Create a group policy object that runs the file `logon.bat` each time a user connects to the server's desktop. For details, see Appendix A, Creating Group Policy Objects.

5. On each client, create a new `OAKSSecureBrowser` desktop shortcut by doing the following (this step is necessary because the default shortcut created by the installation program has an incorrect target):

   a. Connect from the client to the server.

   b. On the desktop provided by the server, delete the Secure Browser's shortcut.

   c. Navigate to the Secure Browser's installation directory, usually `C:\Program Files (x86)\OAKSSecureBrowser\`.

   d. Right-click the file `OAKSSecureBrowser.exe` and select **Send To > Desktop (create shortcut)**.

   e. On the desktop, right-click the new shortcut and select **Properties**. The Shortcut Properties dialog box appears.

   f. Under the **Shortcut** tab, in the **Target** field, type the following command:

      ```
      "C:\Program Files(X86)\OAKSSecureBrowser\
      OAKSSecureBrowser.exe" -P%SESSIONNAME%
      ```

      If you used a different installation path on the server, use that in the above command.

   g. Click **OK** to close the Properties dialog box.

6. Verify the installation by double-clicking the shortcut to start the Secure Browser.

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 machine on which the Secure Browser is installed.
2. Copy the entire folder where the browser was installed (usually `C:\Program Files (x86)\OAKSSecureBrowser`) 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 `OAKSSecureBrowser.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 8:00 a.m. and 3:00 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 sections 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 `OAKSSecureBrowser` and click **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\OAKSSecureBrowser.exe`.

   `/X` Perform an uninstall.

   `[/quiet]` Quiet mode, no interaction.

For example, the command

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

uninstalls the Secure Browser installed at `C:\AssessmentTesting\` using quiet mode.

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. For more information about configuring Take a Test, see https://docs.microsoft.com/en-us/education/windows/take-tests-in-windows-10. (ELPA21 does not support the Take a Test app. If you are administering ELPA21 tests, you must install the AIR Secure Browser on testing machines.)

Creating a Dedicated Test Account for Non-permissive Mode Users

Non-permissive mode users 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, please see 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 don't start these apps, which causes the Take a Test app to log a user out of their account. (For more information, see https://support.microsoft.com/en-us/help/4338725/k-12-assessment-unexpected-reports-apps-running-background-windows-10) Because of this, AIR has disabled the forbidden app check when using the Take a Test app through a dedicated test account.

To create a dedicated test account:

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

Note: If you don't 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://oaks.tds.airast.org/student
5. Click **Save**.

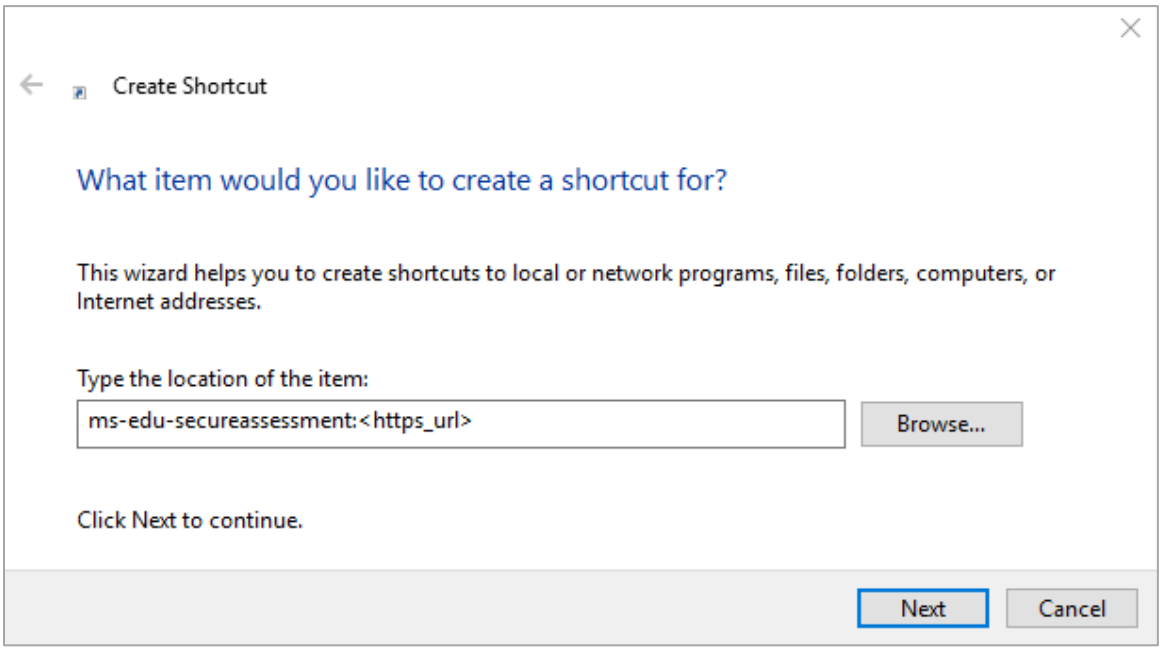
The student can now sign in to the dedicated account to take the specified test.

Creating Desktop Shortcuts for Permissive Mode Users

Permissive mode users should create a desktop shortcut for the Take a Test app.

To create a desktop shortcut for Take a Test:

1. Log in to Windows as the user taking a test.
2. Right-click on the desktop and select **New > Shortcut**. The Create Shortcut dialog box appears.



3. In the *Type the location of the item* field, enter

   `ms-edu-secureassessment:https://oaks.tds.airast.org`/student

4. Click **Next**.
5. In the next dialog box, type a name for the shortcut.
6. Click **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+Atl+Del**.

Installing the Secure Browser on Mac

This section provides instructions for installing the secure browsers on Mac desktop and laptop computers.

Installing the Secure Browser on an Individual Mac

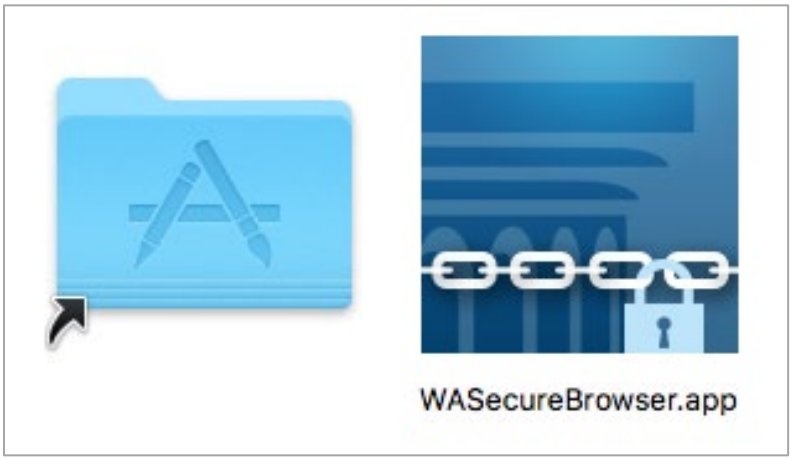
In this scenario, a user installs the Secure Browser on desktop or laptop computers running Mac OS. The steps in this procedure may vary depending on your version of Mac OS and your web browser.

1. Remove any previous versions of the Secure Browser by dragging its folder to the Trash.

2. Navigate to the **Secure Browser** page of the Oregon Statewide Assessment System portal at oaksportal.org. Click the **Mac** tab, then click **Download Browser**. If prompted for a download location, select your downloads folder.

3. Open Downloads from the Dock, and click `OAKSSecureBrowser-OSX.dmg` to display its contents (see Figure 1).

Figure 1. Contents of OAKSSecureBrowser-OSX.dmg



4. Drag the `OAKSSecureBrowser` icon to the folder. This installs the Secure Browser into Applications.

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 8:00 a.m. and 3:00 p.m., schedule background jobs outside of these hours.

6. Disable Mission Control/Spaces. Instructions for disabling Spaces are in the *Technical Specifications Manual for Online Testing*, available from the Oregon Statewide Assessment System portal (oaksportal.org).

7. In Finder, navigate to **Go > Applications**, and double-click **OAKSSecureBrowser** to launch the Secure Browser. (You must launch the Secure Browser to complete the installation.) The Secure Browser opens displaying the student login screen. The browser fills the entire screen and hides the dock.

8. To exit the browser, click **CLOSE SECURE BROWSER** in the upper-right corner of the screen.

9. Create a desktop shortcut; from the **Applications** folder, drag `OAKSSecureBrowser` to the desktop.

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 copy the image to other Macs.

To clone the Secure Browser installation to other computers:

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

    a. Install the Secure Browser following the directions in the section Installing the Secure Browser on an Individual Mac. 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. See Figure 18.

    d. Delete the folder containing the Secure Browser.

    e. Delete the `Mozilla` folder.

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/OAKSSecureBrowser --CreateProfile profile_name`, where `profile_name` is unique among all testing computers.

3. Clone the image.

4. Deploy the image to the target Macs.

Uninstalling the Secure Browser on Mac

To uninstall a Mac Secure Browser, drag its folder to the Trash.

Section III. Installing the Secure Browser on Mobile Devices

This section contains information about installing AIRSecureTest, the Secure Browser app for iOS and Chrome OS. For information about configuring supported tablets and Chromebooks to work with the Secure Browser, refer to the *Technical Specifications Manual for Online Testing*, available from the Oregon Statewide Assessment System portal (oaksportal.org).

Installing the Secure Browser on iOS

This section 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. (To install the Secure Browser on many iOS devices simultaneously, consider using Autonomous Single App Mode. For details, see the section "Configuring Using Autonomous Single App Mode" in *Technical Specifications Manual for Online Testing*.) (To run the Secure Browser or classroom app in iOS, you must first disable Speech to Text.)

1. On your iPad, navigate to the **Secure Browser** page of the Oregon Statewide Assessment System portal at oaksportal.org, and click the iOS tab. Click **Download on the App Store**. (You can also search for `AIRSecureTest` in the App Store to find the Secure Browser app.) The AIRSecureTest download page opens (see Figure 2).

Figure 2. AIRSecureTest Download Page on the Apple Store

2. Tap . The iPad downloads and installs the Secure Browser, and the button changes to **Open**. After installation, an AIRSecureTest icon appears on the iPad's home screen.

3. Configure the test administration by following the procedure in the section Configuring Your State and Assessment Program on Mobile Devices.

Guidance on iOS Classroom App 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 un-installing the Classroom app, or by turning off Bluetooth on the teacher iPad during testing windows.

Using MDM to Disable Classroom Observation

You can use the following key value to disable access to the Classroom observation feature on student devices. This key is defined as part of the Restrictions profile payload and is documented in the Configuration Profile Reference.

allowScreenShot	Boolean	If set to false, users can't save a screenshot of the display and are prevented from capturing a screen recording; it also prevents the Classroom app from observing remote screens. Defaults to true.

Installing AirSecureTest on Chrome OS

This section contains instructions for installing AIRSecureTest, the Secure Browser app for Chrome OS, as a kiosk application.

Chromebooks Manufactured in 2017 or later

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 Chrome OS on hardware manufactured in 2016 or earlier.

Installing AIRSecureTest as a Kiosk App on Standalone Chromebooks

These instructions are for installing the AIRSecureTest Secure Browser as a kiosk app on standalone Chromebook devices.

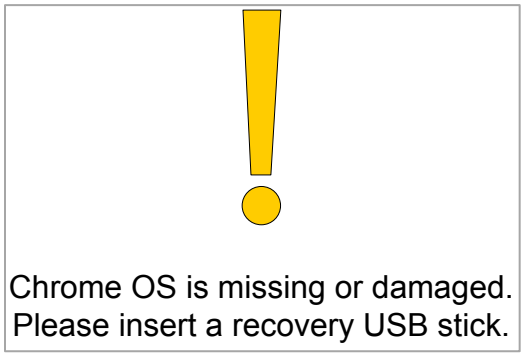
Warning Step 5 of this procedure erases all data on the Chromebook. Before wiping, be sure to back up any data.

1. From your network administrator, obtain the following:
    - The wireless network to which the Chromebook connects. This typically includes the network's SSID, password, and other access credentials.
    - An email and password for logging in to Gmail.
2. Power off, then power on your Chromebook.
3. If the `OS verification is Off` message appears (similar to Figure 5), do the following (otherwise skip to step 4):
    a. Press **Space**. In the confirmation screen, press **Enter**. The Chromebook reboots.
    b. In the Welcome screen (see Figure 7), select your language, keyboard, and enter the network name and password you obtained in step 1. Back in the Welcome screen, click **Continue**.
    c. In the Google Chrome OS Terms screen, click **Accept and continue**. The Sign in screen appears.
4. If this Chromebook was already wiped and configured for a wireless network, skip to step 10; otherwise, continue with step 5.

5. In the Sign in screen, wipe the Chromebook by doing the following:

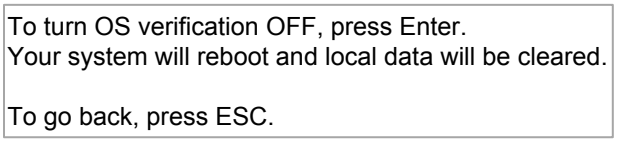
   a. Press **Esc** + ↻ + ⏻. A yellow exclamation mark appears similar to that in Figure 3.

Figure 3. Chrome OS Missing Message



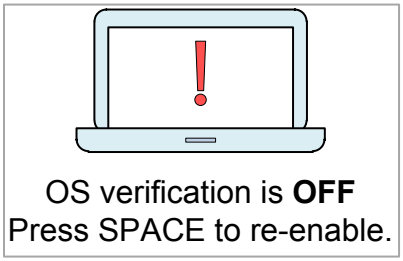
   b. Press **Ctrl + D**. The message in Figure 4 appears.

Figure 4. Turn OS Verification Off Message



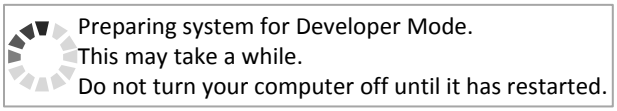
   c. Press **Enter**. A message similar to that in Figure 5 appears.

Figure 5. OS Verification Off Message



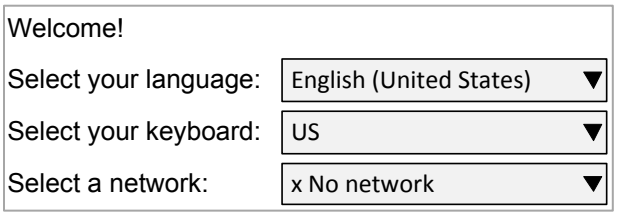
d. Press **Ctrl + D**. The Chromebook indicates it is transitioning to developer mode (see Figure 6). The transition takes approximately 10 minutes, after which the Chromebook reboots.

Figure 6. Preparing for Developer Mode Message



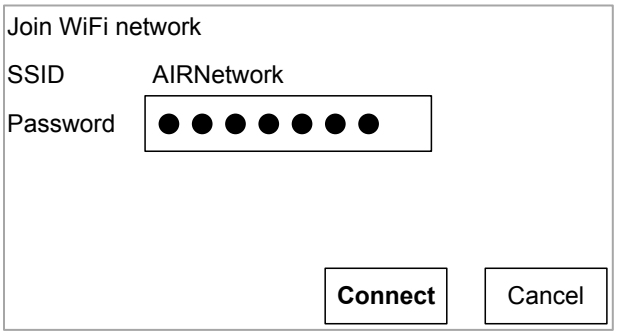
e. After the Chromebook reboots, the `OS verification is Off` message appears again (see Figure 5). Press **Space**, then press **Enter**. The Chromebook reboots, and the Welcome screen appears (see Figure 7).

Figure 7. Welcome Screen



6. In the Welcome screen, select your language, keyboard, and network. The Join WiFi network screen appears (see Figure 8).

Figure 8. Join WiFi Network Screen

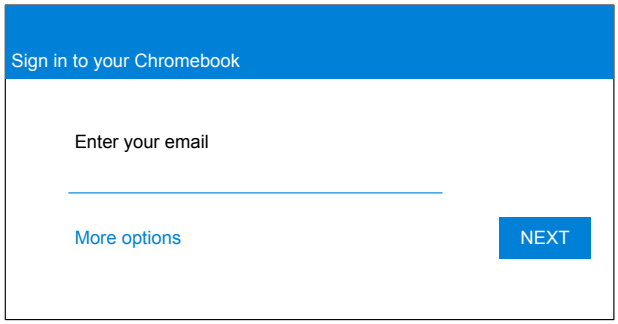


7. Enter the network's password you obtained in step 1.

8. Click **Connect**, and back in the Welcome screen click **Continue**.

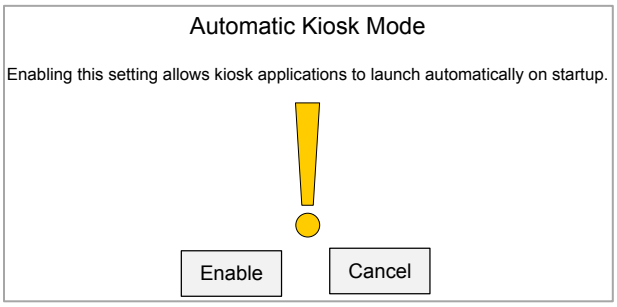
9. In the Google Chrome OS Terms screen, click **Accept and continue**. The Sign in screen appears (see Figure 9).

Figure 9. Sign in Screen



10. In the Sign in screen, press **Ctrl** + **Alt** + **K**. The Automatic Kiosk Mode screen appears (see Figure 10).

Figure 10. Automatic Kiosk Mode Message



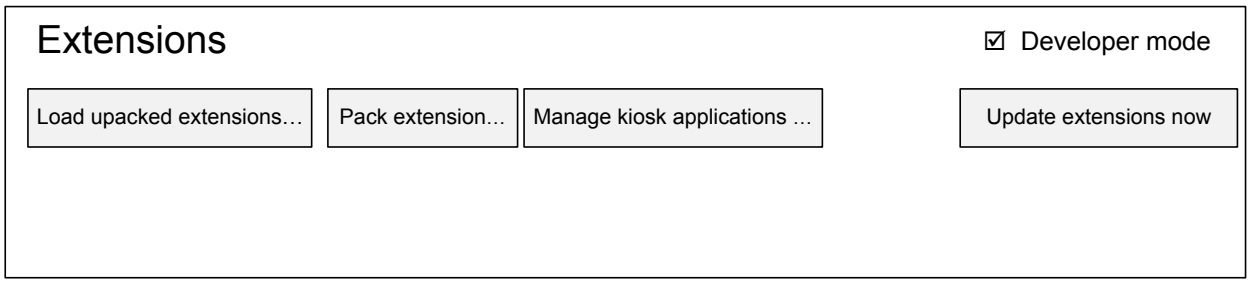
11. Click **Enable**, then click **OK**. The Sign in screen appears (see Figure 9).

12. In the Sign in screen, enter the Gmail address you obtained in step 1, click **Next**, enter the password, and click **Next** again.

13. When you get to the desktop, click the Chrome icon ( ) to open Chrome.

14. In the URL bar, enter `chrome://extensions`. The Extensions screen appears (see Figure 11).

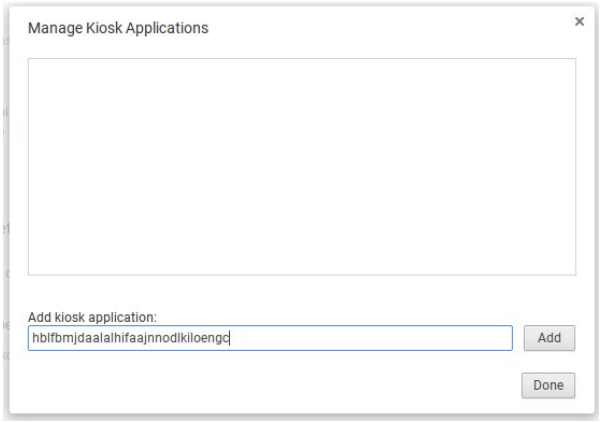
Figure 11. Extensions Screen



15. Mark the checkbox for **Developer Mode**.

16. Click **Manage kiosk applications** located at the top of the screen. The Manage Kiosk Applications screen appears (see Figure 12).

Figure 12. Manage Kiosk Applications Screen



17. Do the following in the Manage Kiosk Applications screen:

    a. Enter the following into the **Add kiosk application** field:
    `hblfbmjdaalalhifaajnnodlkiloengc`

    b. Click **Add**. The `AIRSecureTest` application appears in the Manage Kiosk Applications list.

    c. Click **Done**.

18. Click your avatar in the lower-right corner, and then click **Sign Out**.

19. Back at the desktop, click **Apps** at the bottom of the screen, then click **AIRSecureTest**. The Secure Browser launches.

20. 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 restarting this procedure.

21. Configure the test administration by following the procedure in the section Configuring Your State and Assessment Program on Mobile Devices.

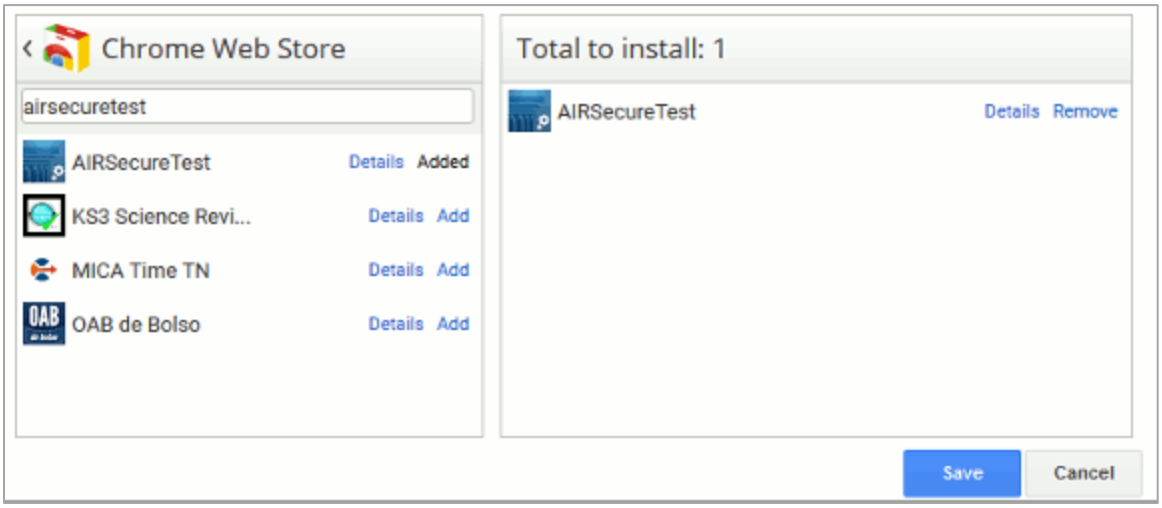
Installing AIRSecureTest as a Kiosk App on Managed Chromebooks

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.

AIRSecureTest is not compatible with public sessions.

1. As the Chromebook administrator, log in to your admin console (https://admin.google.com).
2. Click **Device management**. The Device management page appears.
3. In the left side of the page, click **Chrome management**, and in the next page click **Device settings**.
4. In the ***Device settings*** page, scroll down to the *Kiosk Settings* section.
5. Click **Manage Kiosk Applications**. The ***Kiosk Apps*** window appears (see Figure 13).

Figure 13. Kiosk Apps Window



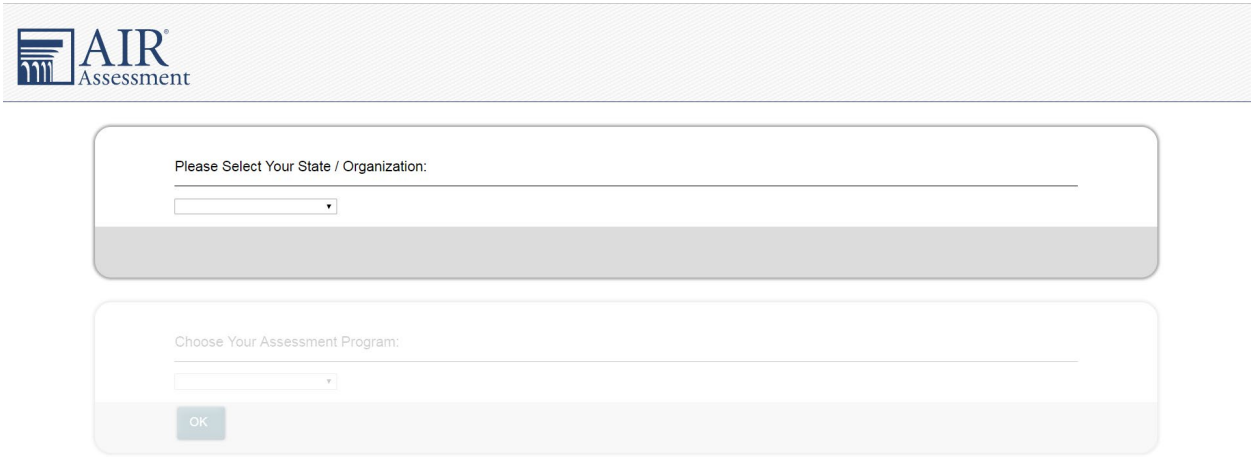
6. If any AIRSecureTest apps appear in the right column, remove them by clicking **Remove**.
7. Add the AIRSecureTest app by doing the following:
   a. Click **Manage Kiosk Applications**. The ***Kiosk Apps*** window appears.
   b. Click **Chrome Web Store**.
   c. In the search box, enter `AIRSecureTest` and press **Enter**. The AIRSecureTest app appears.
   d. Click **Add**. The app appears in the *Total to install* section.
   e. Click **Save**. The AIRSecureTest application appears on all managed Chromebook devices.

Configuring Your State and Assessment Program on Mobile Devices

The first time you open the AIRSecureTest app, a launchpad appears. This launchpad establishes the test administration to which your students will log in.

1. Under **Please Select Your State**, select **Oregon** from the drop-down list (see Figure 14).

Figure 14. AIRSecureTest Launchpad



2. Under **Choose Your Assessment Program**, the Oregon Statewide Assessment System should already be selected.

3. Tap or select **OK**. The student login page will load. The Secure Browser is now ready for students to use.

The launchpad appears only once. The student login 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 section Installing the Secure Browser via Windows for details.

Section IV. 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. However, 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 2 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: Domain names in commands The commands in Table 2 use the domains foo.com and proxy.com. When configuring for a proxy server, use your actual testing domain names as listed in the section "URLs for Testing Sites" in the *Technical Specifications Manual for Online Testing*.

Table 2. Specifying proxy settings using the command line

Description	System	Command
Use the browser without any proxy	Windows	`OAKSSecureBrowser.exe -proxy 0 https://oaks.tds.airast.org/student`
	Mac	`./OAKSSecureBrowser -proxy 0 https://oaks.tds.airast.org/student`
Set the proxy for HTTP requests only	Windows	`OAKSSecureBrowser.exe -proxy 1:http:foo.com:80 https://oaks.tds.airast.org/student`
	Mac	`./OAKSSecureBrowser -proxy 1:http:foo.com:80 https://oaks.tds.airast.org/student`
Set the proxy for all protocols to mimic the “Use this proxy server for all protocols” of Firefox	Windows	`OAKSSecureBrowser.exe -proxy 1:*:foo.com:80 https://oaks.tds.airast.org/student`
	Mac	`./OAKSSecureBrowser -proxy 1:*:foo.com:80 https://oaks.tds.airast.org/student`
Specify the URL of the PAC file	Windows	`OAKSSecureBrowser.exe -proxy 2:proxy.com https://oaks.tds.airast.org/student`
	Mac	`./OAKSSecureBrowser -proxy 2:proxy.com https://oaks.tds.airast.org/student`
Auto-detect proxy settings	Windows	`OAKSSecureBrowser.exe -proxy 4 https://oaks.tds.airast.org/student`
	Mac	`./OAKSSecureBrowser -proxy 4 https://oaks.tds.airast.org/student`
Use the system proxy setting (default)	Windows	`OAKSSecureBrowser.exe -proxy 5 https://oaks.tds.airast.org/student`
	Mac	`./OAKSSecureBrowser -proxy 5 https://oaks.tds.airast.org/student`

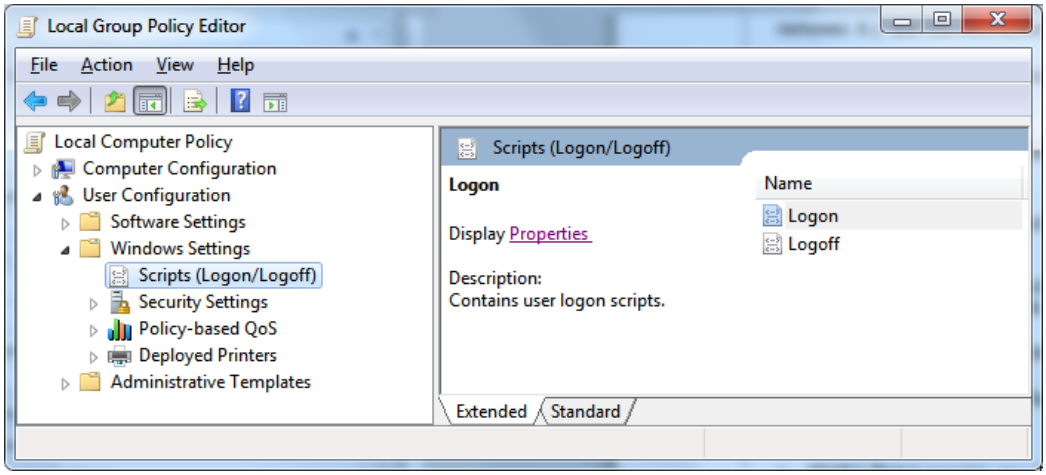
Appendix A. Creating Group Policy Objects

Many of the procedures in the section Installing the Secure Browser on Windows refer to creating a group policy object. These are objects that Windows executes upon certain events. The following procedure explains how to create a group policy object that runs a script when a user logs in. The script itself is saved in a file `logon.bat`.

For additional information about creating group policy objects, see https://technet.microsoft.com/en-us/library/cc754740(v=ws.11).aspx.

1. In the task bar (Windows 10), or in **Start > Run** (previous versions of Windows), enter `gpedit.msc`. The Local Group Policy Editor appears (see Figure 15).

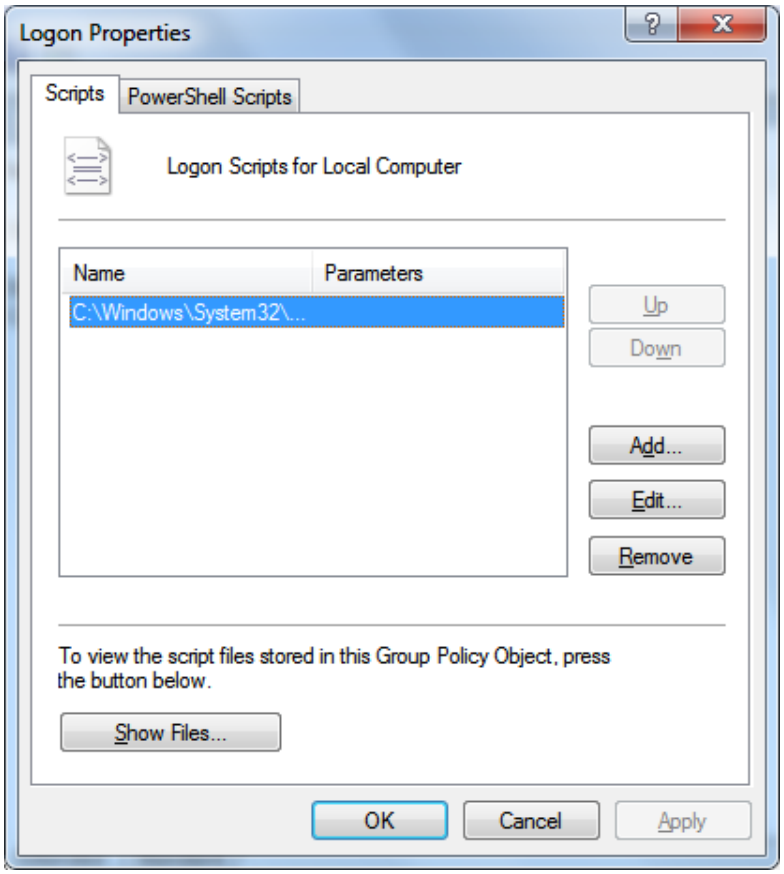
Figure 15. Local Group Policy Editor



2. Expand **Local Computer Policy > User Configuration > Windows Settings > Scripts (Logon/Logoff)**.

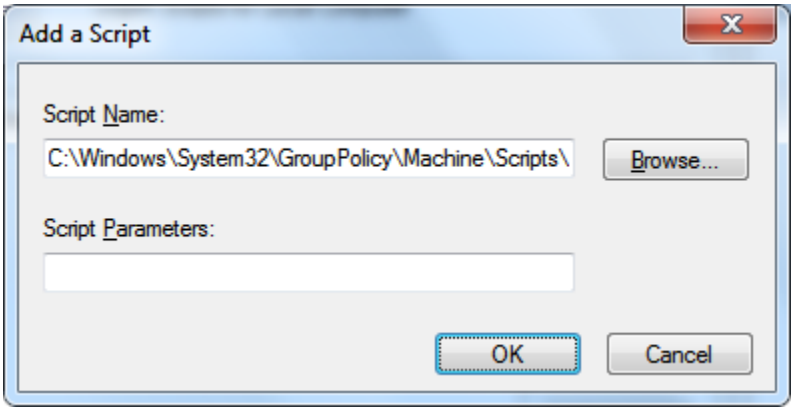
3. Select **Logon** and click **Properties**. The Logon Properties dialog box appears (see Figure 16).

Figure 16. Logon Properties Dialog Box



4. Click **Add**. The Add a Script dialog box appears (Figure 17).

Figure 17. Add a Script Dialog Box



5. Click **Browse…**, and navigate to the `logon.bat` you want to run.

6. Click **OK**. You return to the Logon Properties dialog box.

7. Click **OK**. You return to the Local Group Policy Editor.
8. Close the Local Group Policy Editor.

Appendix B. Resetting Secure Browser Profiles

If the Help Desk advises you to reset the Secure Browser profile, use the instructions in this section.

Resetting Secure Browser Profiles on Windows

The following procedure applies to Windows 7 and later.

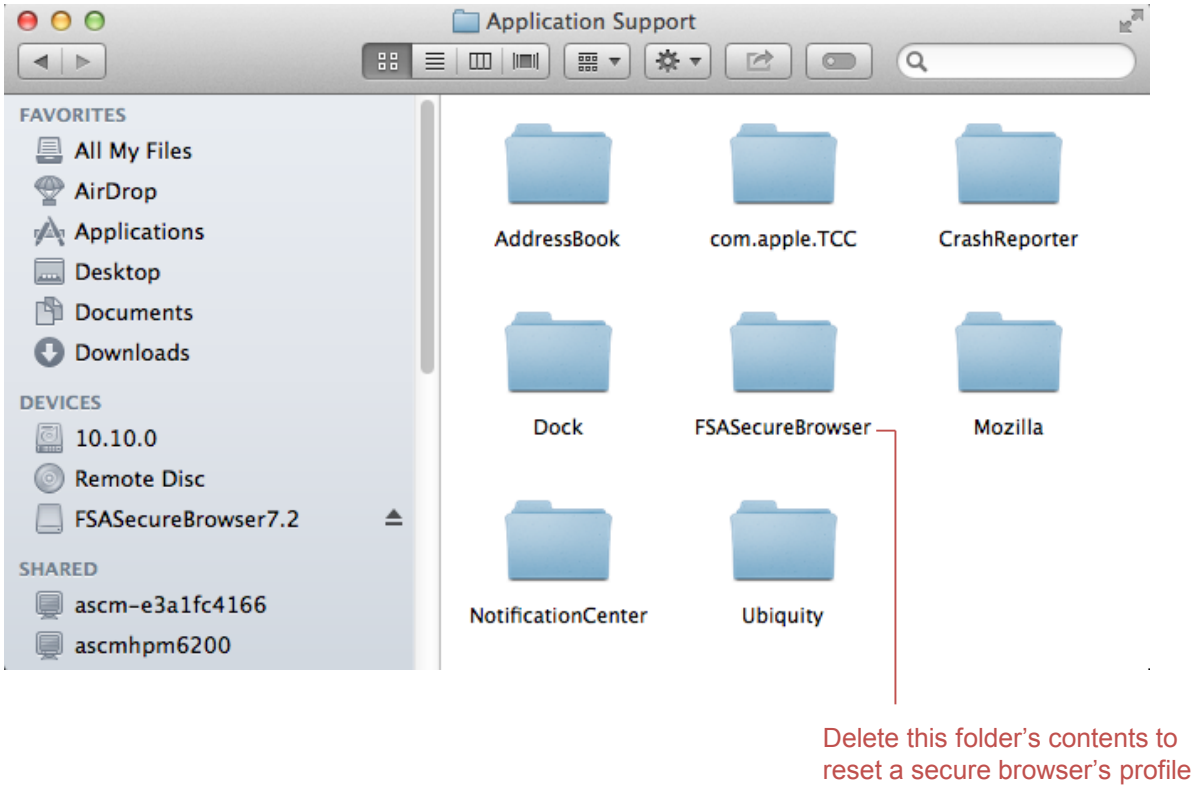
1. Log on as an admin user or as the user who installed the Secure Browser, and close any open Secure Browsers.
2. Delete the contents of the following folders:
   - `C:\Users\username\AppData\Local\AIR\`
   - `C:\Users\username\AppData\Roaming\AIR\`

   where `username` is the Windows user account where the Secure Browser is installed. (Keep the `AIR\` folders, just delete their contents.)
3. Start the Secure Browser.

Resetting Secure Browser Profiles on Mac

1. Log on as an admin user or as the user who installed the Secure Browser, and close any open Secure Browsers.
2. Start Finder.
3. While pressing **Option**, select **Go > Library**. The contents of the Library folder appear. See Figure 18.
4. Open the **Application Support** folder, and delete the folder containing the Secure Browser.
5. Returning to the Library, open the **Caches** folder, and delete the Secure Browser's folder.
6. Restart the Secure Browser.

Figure 18. Cleaning Secure Browser on Mac



Appendix C. User Support

If this document does not answer your questions, please contact the Oregon Statewide Assessment System Help Desk.

The Help Desk is open Monday-Friday from 7:00 a.m. to 5:00 p.m. Pacific Time (except holidays).

Oregon Statewide Assessment System Help Desk

Toll-Free Phone Support: 1-866-509-6257

Email Support: osashelpdesk@air.org

Chat Support: https://oaksportal.org/chat.stml

If you contact the Help Desk, you will be asked to provide as much detail as possible about the issues you encountered.

Include the following information:

- Test Administrator name and IT/network contact person and contact information
- SSIDs of affected students
- Results ID for the affected student tests
- Operating system and browser version information
- Any error messages and codes that appeared, if applicable
- Information about your network configuration:
    - Secure Browser installation (to individual machines or network)
    - Wired or wireless Internet network setup

Appendix D. Change Log

Change	Date
Updated Help Desk email address and chat support URL in “Appendix C. User Support” (pg. 33)	7/23/18
Corrected label name of the Secure Browsers page on the OSAS portal in “Section II. Installing the Secure Browser on Desktops and Laptops” (pg. 4 and pg. 6)	11/13/18