Secure Browser Installation Manual

2014–2015

Published February 23, 2015

Prepared by the American Institutes for Research®

|  |  |
| --- | --- |
|  | [http://www.ode.state.oh.us/gd/templates/images/ODE/ohio_logo.gif](http://ohio.gov/) |

Table of Contents

[Section I. Introduction to the Secure Browser Manual 1](#_Toc412472772)

[Scope 1](#_Toc412472773)

[System Requirements 1](#_Toc412472774)

[Manual Content 1](#_Toc412472775)

[Intended Audience 2](#_Toc412472776)

[Document Conventions 2](#_Toc412472777)

[Other Resources 2](#_Toc412472778)

[Section II. Installing the Secure Browser on Desktop and Laptops 3](#_Toc412472779)

[Installing the Secure Browser on Windows 3](#_Toc412472780)

[Installing the Secure Browser on an Individual Computer 3](#_Toc412472781)

[Installing the Secure Browser via Windows 3](#_Toc412472782)

[Installing the Secure Browser via the Command Line 5](#_Toc412472783)

[Sharing the Secure Browser over a Network 6](#_Toc412472784)

[Copying the Secure Browser Installation Directory to Testing Computers 7](#_Toc412472785)

[Installing the Secure Browser on an NComputing Server 8](#_Toc412472786)

[Terminal Server Installation 9](#_Toc412472787)

[Installing the Secure Browser Without Administrator Rights 10](#_Toc412472788)

[Uninstalling the Secure Browser on Windows 10](#_Toc412472789)

[Uninstalling via the User Interface 10](#_Toc412472790)

[Uninstalling via the Command Line 11](#_Toc412472791)

[Installing the Secure Browser on Mac OS X 11](#_Toc412472792)

[Installing Secure Browser 7.2 11](#_Toc412472793)

[Installing Secure Browser 6.5 12](#_Toc412472794)

[Uninstalling the Secure Browser on OS X 13](#_Toc412472795)

[Installing the Secure Browser on Linux 14](#_Toc412472796)

[Installing the Secure Browser on 32-Bit Distributions 14](#_Toc412472797)

[Installing the Secure Browser on 64-Bit Distributions 15](#_Toc412472798)

[Linux Secure Browser: Uninstallation 15](#_Toc412472799)

[Section III. Installing the Secure Browser on Mobile Devices 16](#_Toc412472800)

[Installing the Secure Browser on iOS 16](#_Toc412472801)

[Installing AIRSecureTest on iOS 16](#_Toc412472802)

[Activating Guided Access Before a Test Session Begins 18](#_Toc412472803)

[Deactivating Guided Access After a Test Session Ends 19](#_Toc412472804)

[Closing AIRSecureTest 20](#_Toc412472805)

[Closing AIRSecureTest under iOS 6.0–6.1 20](#_Toc412472806)

[Closing AIRSecureTest under iOS 7.0–7.1 20](#_Toc412472807)

[Installing AIRSecureTest on Android 20](#_Toc412472808)

[Downloading and Installing the Android AIRSecureTest Mobile Secure Browser 20](#_Toc412472809)

[Opening the AIRSecureTest Browser and Selecting the Assessment Program 21](#_Toc412472810)

[Closing the AIRSecureTest Mobile Secure Browser 22](#_Toc412472811)

[Chrome OS AIRSecureTest Kiosk App 22](#_Toc412472812)

[Installing the AIRSecureTest Kiosk App on Standalone Chromebooks 23](#_Toc412472813)

[Installing the AIRSecureTest Kiosk App on Managed Chromebooks 24](#_Toc412472814)

[Opening the AIRSecureTest Kiosk App and Selecting the Assessment Program 25](#_Toc412472815)

[Section IV. Proxy Settings for Desktop Secure Browsers 27](#_Toc412472816)

[Specifying a Proxy Server to Use with the Secure Browser 27](#_Toc412472817)

[Modifying Desktop Shortcuts to Include Proxy Settings 28](#_Toc412472818)

[Microsoft Windows 28](#_Toc412472819)

[Mac OS X 28](#_Toc412472820)

[Appendix A. Creating Group Policy Objects 30](#_Toc412472821)

[Appendix B. Resetting Secure Browser Profiles 32](#_Toc412472822)

[Resetting Secure Browser Profiles on Windows 32](#_Toc412472823)

[Resetting Secure Browser Profiles on OS X 10.6 or Later 33](#_Toc412472824)

[Resetting Secure Browser Profiles on OS X 10.5 33](#_Toc412472825)

[Resetting Secure Browser Profiles on Linux 34](#_Toc412472826)

[Appendix C. User Support 35](#_Toc412472827)

List of Tables

[Table 1. Document conventions 2](#_Toc405371522)

[Table 2. Commands for installing 32-bit compatibility libraries 15](#_Toc405371523)

[Table 3. Specifying proxy settings using a shortcut or the command line 26](#_Toc405371524)

# Introduction to the Secure Browser Manual

The AIR 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.

## 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 Online System Requirements available from the OCBA (Ohio Computer Based Assessments) portal at .

## 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 Desktop and Laptops, includes instructions for installing the secure browser onto supported Windows, Mac, and Linux platforms.
* Section III, Installing the Secure Browser on Mobile Devices, includes instructions for installing the mobile secure browser onto supported iOS, Android, 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, 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, Mac OS X, or Linux operating systems or Chromebook, iPad, or Android devices.
* Network administrators familiar with mapping or mounting network drives, and creating and running scripts at the user and host level.

## 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. |
|  | **Note:** This symbol accompanies additional information that may be of interest. |
| 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 technical specifications and related requirements, including supported hardware, software, and text-to-speech, refer to the System Requirements for Online Testing.
* For information about steps to take on test day, see the Test Administrator User Guide.

These documents are available at .

# Installing the Secure Browser on Desktop and Laptops

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

## Installing the Secure Browser on Windows

This section provides instructions for installing the secure browser on computers running on Windows XP, Vista, 7, and 8. (The secure browser does not run on other 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\.

### 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 in a location other than C:\Program Files (x86)\, manually uninstall the secure browser. (If you installed in C:\Program Files (x86)\, 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 Ohio Online portal at . Under **Download Secure Browsers**, 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 OHSecureBrowser7.2-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)\‌OHSecureBrowser7.2.
   * A shortcut OHSecureBrowser7.2 to the desktop.
6. If you are running Windows 8.0 or later do the following (otherwise skip to step 7):
   1. The Test Policy for AIR setup wizard starts. Click **Continue**.
   2. Follow the setup wizard, and click **Finish** to exit.

This wizard installs and starts a service Test Policy Standalone Service for Student.

1. 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.
2. Optional: Apply proxy settings by doing the following:
   1. Right-click the shortcut OHSecureBrowser7.2 on the desktop, and select **Properties**.
   2. Under the **Shortcut** tab, in the **Target** field, modify the command to specify the proxy. See Table 3 for available forms of this command.
   3. Click **OK** to close the Properties dialog box.

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

1. Run the browser by double-clicking the OHSecureBrowser7.2 shortcut on the desktop. The secure browser opens displaying the student login screen. The browser fills the entire screen and hides the task bar.
2. To exit the browser, click  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 installed a previous version of the secure browser in a location other than C:\Program Files (x86)\, manually uninstall the secure browser. (If you installed in C:\Program Files (x86)\, 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 Ohio Online portal at . Under **Download Secure Browsers**, click the **Windows** tab, then click **Download Browser**. A dialog window opens.
3. 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.
4. Note the full path and filename of the downloaded file, such as c:\temp\OHSecureBrowser7.2-Win.msi.
5. Open a command prompt.
6. Run the command msiexec /I <Source> [/quiet] [INSTALLDIR=<Target>]

|  |  |
| --- | --- |
| <Source> | Path to the installation file, such as C:\temp\OHSecureBrowser7.2.msi. |
| <Target> | Path to the location where you want to install the secure browser. If absent, install to C:\Program Files (x86)\OHSecureBrowser7.2. 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\OHSecureBrowser7.2-Win.msi /quiet INSTALLDIR=C:\AssessmentTesting\BrowserInstallDirectory

installs the secure browser from the installation package at C:\temp\‌OHSecureBrowser7.2-Win.msi into the directory C:\AssessmentTesting\BrowserInstallDirectory using quiet mode.

1. Follow the instructions in the setup wizard. When prompted for setup type, click **Install**.
2. Click **Finish** to exit the setup wizard. The following items are installed:
   * The secure browser to the default location C:\Program Files (x86)\‌OHSecureBrowser7.2.
   * A shortcut OHSecureBrowser7.2 to the desktop.
3. If you are running Windows 8.0 or later do the following (otherwise skip to step 10):
   1. The Test Policy for AIR setup wizard starts. Click **Continue**.
   2. Follow the setup wizard, and click **Finish** to exit.

This wizard installs and starts a service Test Policy Standalone Service for Student.

1. 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.
2. Run the browser by double-clicking the OHSecureBrowser7.2 shortcut on the desktop. The secure browser opens displaying the student login screen. The browser fills the entire screen and hides the task bar.
3. To exit the browser, click  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.

|  |  |
| --- | --- |
|  | **WARNING Unsupported Installation for Windows 8.x** This installation scenario is not supported on test computers running Windows 8.x, and the secure browser does not run. Test computers running Windows 8.x must have local installations as described in Installing the Secure Browser on an Individual Computer. |

1. On the remote computer from where 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:
   1. 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.
   2. Copy the desktop shortcut OHSecureBrowser7.2 from the remote machine to the directory C:\Users\Public\Public Desktop.
   3. Run the browser by double-clicking the OHSecureBrowser7.2 shortcut on the desktop. The secure browser opens displaying the student login screen. The browser fills the entire screen and hides the task bar.
   4. To exit the browser, click  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)\OHSecureBrowser7.2.
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:
   1. 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.
   2. Copy the installation directory C:\Program Files (x86)\OHSecureBrowser7.2 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\OHSecureBrowser7.2.
   3. Copy the shortcut c:\AssesssmentTesting\OHSecureBrowser7.2\OHSecureBrowser7.2.exe - Shortcut.lnk to the desktop.
   4. Run the browser by double-clicking the OHSecureBrowser7.2 shortcut on the desktop. The secure browser opens displaying the student login screen. The browser fills the entire screen and hides the task bar.
   5. To exit the browser, click  in the upper-right corner of the screen.

### Installing the Secure Browser on an NComputing Server

In this scenario, a network administrator installs the secure browser on an NComputing server. If you install and run the secure browser from an NComputing server, you should be familiar with operating that software and related hardware. On testing day, the testing coordinator logs in to the NComputing server from each client and starts the secure browser so that it is ready for the students.

For a listing of supported terminals and servers for this scenario, see the Technical Specifications Manual for Online Testing, available from the Ohio Online portal (), **Secure Browsers** page.

1. Log in to the machine running the NComputing 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 or paste the following command:

"C:\Program Files (x86)\OHSecureBrowser7.2\‌OHSecureBrowser7.2.exe" ‑CreateProfile %SESSIONNAME%

1. Save the file as C:\Windows\‌System32\‌GroupPolicy\‌Machine\‌Scripts\‌Startup\‌logon.bat.
2. 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.
3. Test the installation from a client by doing the following:
   1. Connect the NComputing server to a terminal, and connect a keyboard and monitor to the same terminal.
   2. Turn on the monitor, select the NComputing server, and log in. The secure browser’s shortcut appears on the desktop.
   3. Double-click the shortcut to run the secure browser.

### Terminal Server Installation

In this scenario, a network administrator installs the secure browser on a terminal server. Testing machines then log in to the terminal server and run the secure browser remotely. This scenario is supported on Windows server 2003 and 2008.

|  |  |
| --- | --- |
|  | **CAUTION: Testing Quality With Terminal Servers** Launching a secure browser from a terminal 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 terminal server, and 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.
2. Copy and paste the line below into Notepad:

"C:\Program Files (x86)\OHSecureBrowser7.2\‌OHSecureBrowser7.2" -CreateProfile %SESSIONNAME%

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

1. Save the file as C:\Windows\‌System32\‌GroupPolicy\‌Machine\‌Scripts\‌Startup\‌logon.bat.
2. 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.
3. Modify the OHSecureBrowser7.2 desktop shortcut by doing the following:
   1. Right-click the shortcut and select **Properties**. The Properties dialog box appears.
   2. Under the **Shortcut** tab, in the **Target** field, type or copy/paste the following command:

"C:\Program Files(X86)\OHSecureBrowser7.2\‌OHSecureBrowser7.2.exe" ‑P "%SESSIONNAME%"

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

1. From a different computer, do the following:
   1. Connect to the terminal server.
   2. Double-click the desktop shortcut to run 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.

|  |  |
| --- | --- |
|  | **WARNING Unsupported Installation for Windows 8.x** This installation scenario is not supported on test computers running Windows 8.x, and the secure browser does not run. Test computers running Windows 8.x must have local installations as described in Installing the Secure Browser on an Individual Computer. |

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)\‌OHSecureBrowser7.2) 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 OHSecureBrowser7.2.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. Open the Control Panel.
2. Select **Add or Remove Programs** or **Uninstall a Program**.
3. Select the secure browser program OHSecureBrowser7.2 and click **Remove** or **Uninstall**.
4. 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 installation file, such as C:\MSI\OHSecureBrowser7.2-Win.msi. |
| /X | Perform an uninstall. |
| /quiet | Quiet mode, no interaction. |

For example, the command

msiexec /X C:\AssessmentTesting\‌OHSecureBrowser7.2.exe /quiet

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

## Installing the Secure Browser on Mac OS X

This section provides instructions for installing the secure browsers on Macintosh desktop computers.

### Installing Secure Browser 7.2

In this scenario, a user installs the secure browser on desktop computers running Mac OS X 10.6–10.10. The steps in this procedure may vary depending on your version of Mac OS X 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 Ohio Online portal at . Click the **Mac OS X 10.6–10.10** tab, then click **Download Browser**. If prompted for a download location, select your downloads folder.
3. Open Downloads from the Dock, and click OHSecureBrowser7.2-OSX.dmg to display its contents.
4. Drag the OHSecureBrowser7.2 icon to the desktop.
5. Disable fast user switching by doing the following:
   1. Select **Apple menu** > **System Preferences** > **Users & Groups**.
   2. Click the lock icon to unlock it, and then enter an administrator name and password.
   3. Click **Login Options**.
   4. Clear the **Show fast user switching menu as** checkbox.
6. Disable the Launchpad by doing the following:
   1. In Users & Groups, click **Show All**.
   2. Click **Keyboard**, then click **Shortcuts**.
   3. Click **Launchpad & Dock**, and clear the **Show Launchpad** checkbox
   4. Close System Preferences.
7. 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.
8. For Mac OS 10.7–10.10, disable Mission Control/Spaces. Instructions for disabling Spaces are in the Technical Specifications Manual for Online Testing, available from the Ohio Online portal (), Secure Browsers page.
9. Double-click the OHSecureBrowser7.2 icon on the desktop 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.

Mac OS 10.6: The secure browser disables Exposé (hot corner) settings if they are set, and the settings remain disabled after the browser is closed.

1. To exit the browser, click **Close** in the upper-right corner of the screen.

### Installing Secure Browser 6.5

In this scenario, you install the secure browser on desktop computers running Mac OS 10.5 with an Intel processor.

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 Ohio Online portal at . Click the **Mac OS X 10.5** tab, then click **Download Browser**. A dialog window opens. If prompted for a download location, select the desktop.
3. Open Downloads from the Dock, and click OHSecureBrowser6.5‑OSX.dmg to display its contents.
4. Drag the OHSecureBrowser6.5 icon to the desktop.
5. Disable fast user switching by doing the following:
   1. Select **Apple menu** > **System Preferences** > **Users & Groups**.
   2. Click the lock icon to unlock it, and then enter an administrator name and password.
   3. Click **Login Options**.
   4. Clear the **Show fast user switching menu as** checkbox.
6. Disable the Launchpad by doing the following:
   1. In Users & Groups, click **Show All**.
   2. Click **Keyboard**, then click **Shortcuts**.
   3. Click **Launchpad & Dock**, and clear the **Show Launchpad** checkbox
   4. Close System Preferences.
7. 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.
8. Double-click the OHSecureBrowser6.5 icon on the desktop 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.

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

1. To exit the browser, click **Close** in the upper-right corner of the screen.

### 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

This section provides instructions for installing the secure browser on computers running a supported Linux distribution. For more information about Linux requirements, refer to the Technical Specifications Manual for Online Testing, available from the Ohio Online portal (), Secure Browsers page.

### Installing the Secure Browser on 32-Bit Distributions

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

1. Navigate to the **Secure Browser** page of the Ohio Online portal at . Click the **Linux** tab, then click **Download Browser**. Save the file to the desktop.
2. Right-click the downloaded file OHSecureBrowser6.5-Linux.tar.bz2, and select **Extract Here** to expand the file. This creates the OHSecureBrowser6.5 folder on the desktop.
3. In a file manager, open the OHSecureBrowser6.5 folder.
4. Double-click the file install-icon.sh and select **Run** from the prompt. The installation program runs and creates a OHSecureBrowser6.5 icon on the desktop.
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. If text-to-speech testing is performed on this computer, reboot it.
7. From the desktop, double-click the OHSecureBrowser6.5 icon to launch the browser. The student login screen appears. The browser fills the entire screen and hides any panels or launchers.
8. To exit the browser, click  in the upper-right corner of the screen.

### Installing the Secure Browser on 64-Bit Distributions

Use the following procedure to install the secure browser on 64‑bit machines.

1. Using Table 2 as a guide, install the 32‑bit compatibility libraries for your distribution. If your distribution does not appear in Table 2, consult its documentation for 32-bit compatibility.
2. Install the secure browser by following the procedure in the section Installing the Secure Browser on 32-Bit Distributions.

Table 2 lists the commands for installing 32-bit compatibility libraries for popular Linux distributions.

Table 2. Commands for installing 32-bit compatibility libraries

| Distribution | Command |
| --- | --- |
| Fedora 16–20 | sudo yum install glibc.i686 nspr.i686 gtk2.i686 xulrunner.i686 |
| openSUSE 13.1 | zypper install glibc-32bit |
| Red Hat Enterprise Linux 6.5 | sudo yum install xulrunner.i686 libgtk-x11-2.0.50.0 libxcom.so glibc.i686 |
| Ubuntu (LTS) 10.04, 12.04, 14.04 | sudo apt-get install libgtk2.0.0:i386 libstdc++6:i386 libasound2:i386 libasound2-plugins:i386 libdbus-glib-1-2:i386 libXt6:i386 |

### Linux Secure Browser: Uninstallation

Before installing a new Linux secure browser, you will need to uninstall the previous version, if you have one. 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 the Technical Specifications Manual for Online Testing, available from the Ohio Online portal (), Secure Browsers page.

## Installing the Secure Browser on iOS

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

### Installing AIRSecureTest on iOS

|  |  |
| --- | --- |
| 1. On your iPad, navigate to the **Secure Browser** page of the Ohio Online portal at , and click the iOS tab. Click **Download**. (You can also search for **AIRSecureTest** in the App store to find the secure browser app.) 2. The AIRSecureTest application download page opens. |  |
| 1. Tap **Free**. The button changes to **Install App**. |  |
| 1. Tap **Install App**. 2. Enter your Apple ID password. |  |
| The AIRSecureTest mobile secure browser downloads and installs onto your iPad. Look for the AIRSecureTest icon. |  |
| The first time you open AIRSecureTest, a Launchpad appears. The Launchpad establishes the test administration for your students. |  |
| 1. Under **Please Select Your State**, select **Ohio** from the drop-down list. |  |
| 1. Under **Choose Your Assessment Program**, select **Ohio Science and Social Studies Tests**. 2. Tap or click **OK**. The student login page opens. The secure browser is now ready for students to use.   The Launchpad screen appears only once. The student login page appears automatically the next time the secure browser is launched. |  |

### Activating Guided Access Before a Test Session Begins

Guided Access must already be enabled via iOS Settings prior to completing these steps. More information about Guided Access and how to enable it is located in the Technical Specifications Manual for Online Testing, available from the Ohio Online portal (), Secure Browsers page.

If students are using iPads with iOS 7, the volume buttons should be enabled prior to starting Guided Access.

|  |  |
| --- | --- |
| 1. Open the AIRSecureTest secure browser app. The student login page appears. |  |
| 1. Triple-click (press) the Home button on the iPad. The Guided Access options appear at the bottom of the screen. |  |
| 1. For iOS 7.0 and later:    1. Tap **Options** under **Hardware Buttons**. A pop-up menu appears.    2. Tap **Volume Buttons** so that it is enabled. This allows students to adjust volume during the test. 2. Tap **Start** in the upper-right corner. A confirmation message appears. |  |

|  |  |
| --- | --- |
|  | **Notes:**   * Guided Access is not the same as Single App Mode. It cannot be enabled or activated via a Mobile Device Management program. * When Guided Access is activated, students cannot switch to other applications or take screenshots. * If you are using iOS 6, the Hardware Buttons are completely disabled and cannot be enabled. |

### Deactivating Guided Access After a Test Session Ends

|  |  |
| --- | --- |
| 1. Triple-click (press) the Home button on the iPad. |  |
| 1. Enter the Guided Access passcode. This must be the same passcode used when Guided Access was enabled. |  |
| 1. Tap **End** in the upper-left corner. A pop-up message appears saying **Guided Access ended**. |  |

### Closing AIRSecureTest

Closing the AIRSecureTest browser is the same as closing any other iOS application.

#### Closing AIRSecureTest under iOS 6.0–6.1

1. Double-tap the Home button. The multitasking bar appears.
2. Press the **AIRSecureTest** icon until it wiggles and the red minus sign appears.
3. Tap the red minus sign and then press the Home button.

#### Closing AIRSecureTest under iOS 7.0–7.1

1. Double-tap the Home button. The multitasking bar appears.
2. Locate the **AIRSecureTest** app preview and slide it upwards.

## Installing AIRSecureTest on Android

You can download AIRSecureTest from the Ohio Online portal or from the Google Play store. The process for installing the secure browser is the same as for any other Android application.

This section contains instructions for downloading and installing AIRSecureTest and selecting your state and assessment program.

### Downloading and Installing the Android AIRSecureTest Mobile Secure Browser

|  |  |
| --- | --- |
| 1. On your Android tablet, navigate to the **Secure Browser** page of the Ohio Online portal at and tap the Android tab. Click **Download Browser**. (You can also search for “AIRSecureTest” in the Google Play store to find the secure browser app.) 2. The AIRSecureTest application download page appears. |  |
| 1. Tap **Install**. |  |
| 1. The AIRSecureTest mobile secure browser downloads and installs onto your tablet. Look for the AIRSecureTest icon. (The name may be truncated.) 2. Configure the test administration by following the procedure in the section Opening the AIRSecureTest Browser and Selecting the Assessment Program. |  |

|  |  |
| --- | --- |
|  | **Android Secure Browser Keyboard**  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 the Technical Specifications Manual for Online Testing, available from the Ohio Online portal (), Secure Browsers page. |

### Opening the AIRSecureTest Browser and Selecting the Assessment Program

The first time you open the AIRSecureTest mobile secure browser, the **Launchpad** screen appears. The Launchpad establishes the test administration for your students.

|  |  |
| --- | --- |
| 1. Under **Please Select Your State**, select Ohio from the drop-down list. |  |
| 1. Under **Choose Your Assessment Program**, select **Ohio Science and Social Studies Tests**. 2. Tap **OK**. The student login page appears. The secure browser is now ready for students to use.   The Launchpad screen appears only once. The student login page appears the next time the secure browser is launched. |  |

### Closing the AIRSecureTest Mobile Secure Browser

Closing the AIRSecureTest browser is the same as closing any other Android application.

1. Tap the Menu icon  in the upper-right corner.
2. Tap **Exit**. A confirmation message appears.
3. Tap **Exit**.

## Chrome OS AIRSecureTest Kiosk App

The AIRSecureTest kiosk application can be installed onto managed Chromebooks via the Google Admin Console. Information about this method can be found in Google’s online documentation for using Chromebooks for student assessments at <https://support.google.com/chrome/a/answer/3273084>. Refer to “Scenario 1: School sets up Chromebook to run as a Single App Kiosk running the exam app.” Do NOT follow the instructions for Scenarios 2 and 3.

The app can also be downloaded and installed on non-managed Chromebooks from the Chrome Web store.

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

### Installing the AIRSecureTest Kiosk App on Standalone Chromebooks

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

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, do the following (otherwise skip to step 4):
   1. Press the spacebar. In the confirmation screen, press Enter. The Chromebook reboots.
   2. In the Welcome screen, select your language, keyboard, and the wireless network information you acquired from the network administrator. Back in the Welcome screen, click **Continue**.
   3. In the Google Chrome OS Terms screen, click **Accept and continue**.
4. When the Sign In screen appears, wipe the Chromebook by doing the following:
   1. Press Esc + Samsung Chromebook Refresh key + Power. The screen displays a yellow exclamation point (!).
   2. Press Ctrl + D to begin developer mode, then press Enter. The screen displays a red exclamation point.
   3. Press Ctrl + D, then press Enter. The Chromebook indicates it is transitioning to developer mode. The transition takes approximately 10 minutes, after which the Chromebook reboots.
   4. After the Chromebook reboots, the OS verification is Off message appears. Press the spacebar, then press Enter. The Chromebook reboots, and the Welcome screen appears.
5. In the Welcome screen, select your language, keyboard, and a network. Back in the Welcome screen, click **Continue**.
6. In the Google Chrome OS Terms screen, click **Accept and continue**. The Sign in screen appears.
7. In the Sign In screen, press Ctrl + Alt + K. The Automatic Kiosk Mode screen appears with a yellow exclamation mark.
8. Click **Enable**, then click **OK**. The Sign in screen appears.
9. In the Sign in screen, enter your email and password, then click **Sign in**.
10. Set your Chromebook preferences as desired.
11. When you get to the desktop, click the Chrome icon () to open Chrome.
12. In the URL bar, enter chrome://extensions. The Extensions screen appears.
13. Mark the checkbox for **Developer Mode**.
14. Click **Manage kiosk applications** located at the top of the screen. The Manage Kiosk Applications screen appears.
15. Do the following in the Manage Kiosk Applications screen:
    1. Enter the following into the **Add kiosk application** field: ondcgjblmdblfnmdeoeebaemlckomedj
    2. Click **Add**. The **AIRSecureTest** application appears in the Manage Kiosk Applications list.
    3. Click **Done**. You return to the **Extensions** screen.
16. Click your icon in the lower-right corner and select **Sign Out**.
17. Back at the desktop, click **Apps** at the bottom of the screen, then click **AIRSecureTest**. The secure browser launches.
18. 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 section.

1. Configure the test administration by following the procedure in the section 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 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. Navigate to **Device management** > **Chrome management** > **Device settings**.
3. On the Device settings page, scroll down to the Kiosk Settings section.
4. Set Single App Kiosk to **Allow Single App Kiosk**.
5. Click **Manage Kiosk Applications**. The Kiosk Apps window appears.
6. Add the AIRSecureTest app by doing the following:
   1. Click **Chrome Web Store**.
   2. In the search box, enter AIRSecureTest and press **Enter**. The AIRSecureTest app appears.
   3. Click **Add**. The app appears in the Total to install section.
   4. Click **Save**. The AIRSecureTest application appears on all managed Chromebook devices.

### Opening the AIRSecureTest Kiosk App and Selecting the Assessment Program

The first time you open the AIRSecureTest kiosk app a **Launchpad** screen appears. This Launchpad establishes the test administration to which your students will log in.

|  |  |
| --- | --- |
| 1. Under **Please Select Your State**, select from the drop-down list. |  |
| 1. Under **Choose Your Assessment Program**, the Ohio Science and Social Studies Tests should already be selected. 2. Tap or select **OK**. The student login page will load. The secure browser is now ready for students to use.   The Launchpad screen appears only once. The student login page appears the next time the secure browser is launched. |  |

# Proxy Settings for Desktop Secure Browsers

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

## Specifying a Proxy Server to Use with the Secure Browser

By default, the secure browser attempts to detect the settings for your network’s web proxy server. You can optionally force the secure browser to use specific proxy settings by passing them through the command line. Table 3 lists the form of the command for different settings and operating systems.

Table 3. Specifying proxy settings using a shortcut or the command line

| Description | System | Command |
| --- | --- | --- |
| Run the browser without any proxy | Windows | AIRSecureBrowser7.2.exe -proxy 0 |
| Mac 10.5 (Intel) | arch -i386 ./AIRSecureBrowser6.5 -proxy 0 |
| Mac 10.6–10.10 | ./AIRSecureBrowser7.2 -proxy 0 |
| Linux | ./AIRSecureBrowser6.5 -proxy 0 |
| Set the proxy for HTTP requests only | Windows | AIRSecureBrowser7.2.exe -proxy 1:http:foo.com:80 |
| Mac 10.5 (Intel) | arch -i386 ./AIRSecureBrowser6.5 -proxy 1:http:foo.com:80 |
| Mac 10.6–10.10 | ./AIRSecureBrowser7.2 -proxy 1:http:foo.com:80 |
| Linux | ./AIRSecureBrowser6.5.sh -proxy 1:http:foo.com:80 |
| Set the proxy for all protocols to mimic the “Use this proxy server for all protocols” of Firefox | Windows | AIRSecureBrowser7.2.exe -proxy 1:\*:foo.com:80 |
| Mac 10.5 (Intel) | arch -i386 ./AIRSecureBrowser6.5 -proxy 1:\*:foo.com:80 |
| Mac 10.6–10.10 | ./AIRSecureBrowser7.2 -proxy 1:\*:foo.com:80 |
| Linux | ./AIRSecureBrowser6.5.sh -proxy 1:\*:foo.com:80 |
| Specify the URL of the PAC file | Windows | AIRSecureBrowser7.2.exe -proxy 2:proxy.com |
| Mac 10.5 (Intel) | arch -i386 ./AIRSecureBrowser6.5 -proxy 2:proxy.com |
| Mac 10.6–10.10 | ./AIRSecureBrowser7.2 -proxy 2:proxy.com |
| Linux | ./AIRSecureBrowser6.5.sh -proxy 2:proxy.com |
| Auto-detect proxy settings | Windows | AIRSecureBrowser7.2.exe -proxy 4 |
| Mac 10.5 (Intel) | arch -i386 ./AIRSecureBrowser6.5 -proxy 4 |
| Mac 10.6–10.10 | ./AIRSecureBrowser7.2 -proxy 4 |
| Linux | ./AIRSecureBrowser6.5.sh -proxy 4 |
| Use the system proxy setting (default) | Windows | AIRSecureBrowser7.2.exe -proxy 5 |
| Mac 10.5 (Intel) | arch -i386 ./AIRSecureBrowser6.5 -proxy 5 |
| Mac 10.6–10.10 | ./AIRSecureBrowser7.2 -proxy 5 |
| Linux | ./AIRSecureBrowser6.5.sh -proxy 5 |

## Modifying Desktop Shortcuts to Include Proxy Settings

This section provides guidelines for passing a proxy setting to the secure browser. All commands in this section are examples only, with the assumption that you have a shortcut for the secure browser on your desktop.

### Microsoft Windows

1. Right-click the desktop shortcut for the secure browser, and select **Properties**.
2. Under the Shortcut tab, in the **Target** field, modify the command as specified in Table 3. For example:

"C:\Program Files (x86)\AIRSecureBrowser7.2\AIRSecureBrowser7.2.exe" ‑proxy 1:http:foo.com:80

1. Click **OK**.

### Mac OS X

The steps in this section require you to use Terminal and a text editor.

1. Open the terminal by selecting **Applications > Utilities > Terminal**.
2. Change to the desktop directory

cd Desktop

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

pico securebrowser.command.

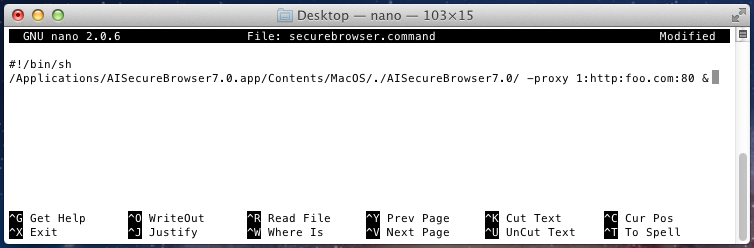
1. Copy or type the following the lines:

#!/bin/sh

/Applications/AIRSecureBrowser7.2.app/Contents/MacOS/./ AIRSecureBrowser7.2 ‑proxy 1:http:foo.com:80 &

Be sure to specify the complete path to the secure browser and the desired proxy option. Ensure the command ends with an ampersand &. For example, for Mac 10.6–10.10:

Figure 1. Sample Mac 10.7.5 Command



1. Save the file and exit the editor by pressing **Ctrl-O**, **Enter** and **Ctrl-X**.
2. Apply execute permission to the file. In Terminal, type

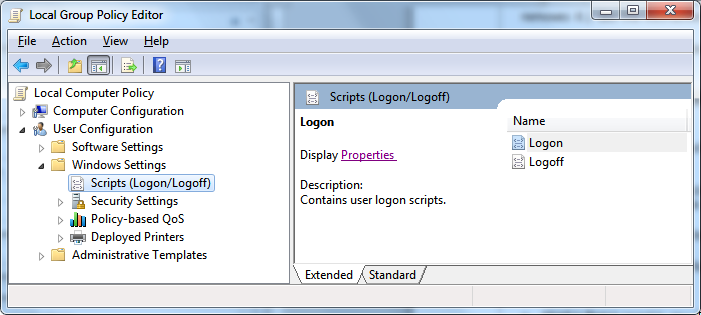
chmod a+x securebrowser.command

1. Close Terminal.
2. Click the securebrowser.command icon on the desktop. The secure browser opens with the proxy setting you configured.
3. Creating Group Policy Objects

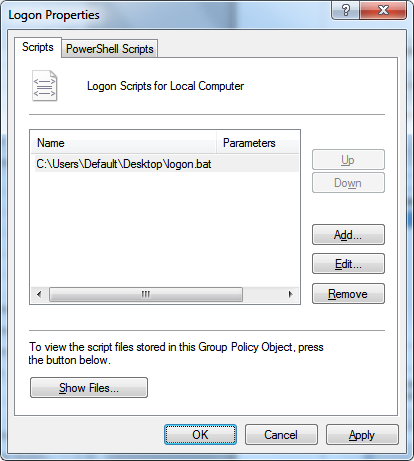
Many of the procedures in the section Installing the Secure Browser on Windows refer to creating a group policy object. These are objects that Windows executes upon certain events. The following procedure explains how to create a group policy object that runs a script when a user logs in. The script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

For additional information about creating group policy objects, see “Assign user logon scripts” at <http://technet.microsoft.com/en-us/library/cc781361%28v=ws.10%29.aspx>.

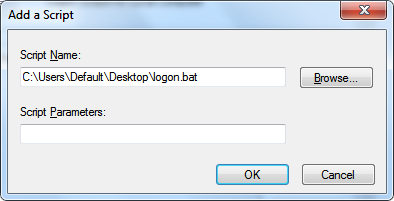
1. **Start > Run >** gpedit.msc. The Local Group Policy Editor appears.



1. Expand **Local** **Computer Policy > User Configuration > Windows Settings > Scripts (Logon/Logoff)**.
2. Select **Logon** and click **Properties**. The Logon Properties dialog box appears.



1. Click **Add**. The Add a Script dialog box appears.



1. Click **Browse…**, and navigate to the logon.bat you want to run.
2. Click **OK**. You return to the Logon Properties dialog box.
3. Click **OK**. You return to the Local Group Policy Editor.
4. Close the Local Group Policy Editor.
5. Resetting Secure Browser Profiles

If the Help Desk advises you to reset the secure browser profile, please consult the instructions in this section.

## Resetting Secure Browser Profiles on Windows

Resetting profiles for 64-bit versions of Windows

1. Log on as the user who installed the secure browser, and close any open secure browsers.
2. Delete the contents of the following folders:
   * C:\Users\username\AppData\Local\AIR\
   * C:\Users\username\AppData\Roaming\AIR\

where username is the Windows user account where the secure browser is installed. (Keep the AIR\ directories, just delete their contents.)

1. Start the secure browser.

Resetting profiles for 32-bit versions of Windows

1. Log on as the user who installed the secure browser, and close any open secure browsers.
2. Delete the contents of the following folders:
   * C:\Documents and Settings\username\Local Settings\Application Data\AIR\
   * C:\Documents and Settings\username\Application Data\AIR\

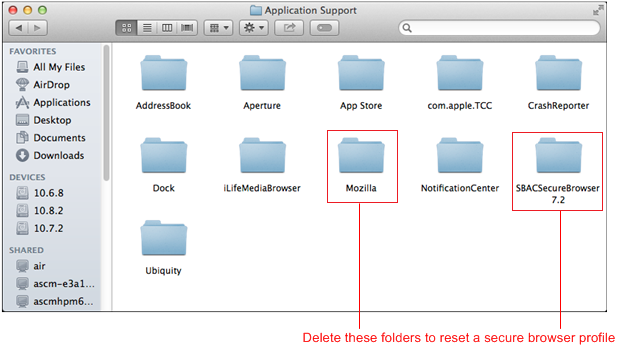
where username is the Windows user account where the secure browser is installed. (Keep the AIR\ directories, just delete their contents.)

1. Start the secure browser.

## Resetting Secure Browser Profiles on OS X 10.6 or Later

1. Log on 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 2.
4. Open the **Application Support** folder.
5. Delete the folder containing the secure browser.
6. Delete the Mozilla folder.
7. Restart the secure browser.

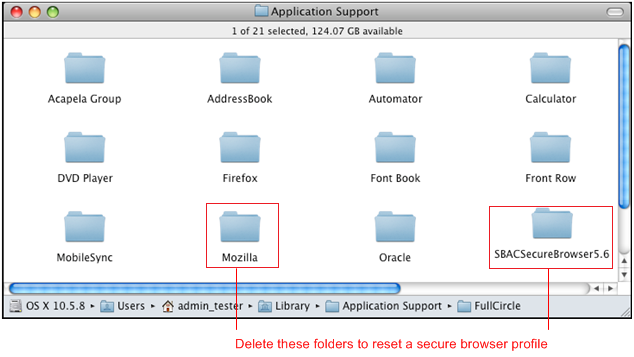
Figure 2. Cleaning Secure Browser on OS X 10.6 or Later



## Resetting Secure Browser Profiles on OS X 10.5

1. Log on as the user who installed the secure browser, and close any open secure browsers.
2. Start Finder.
3. Select **Go > Home**.
4. Open **Library > Application Support**. The contents of the Library folder appear. See Figure 3.
5. Delete the folder containing the secure browser.
6. Delete the Mozilla folder.
7. Restart the secure browser.

Figure 3. Cleaning Secure Browser on OS X 10.5



## Resetting Secure Browser Profiles on Linux

1. Log on as the user who installed the secure browser, and close any open secure browsers.
2. Open a terminal, and delete the contents of the following folders:
   * /home/username/.air
   * /home/username/.mozilla

where username is the user account where the secure browser is installed. (Keep the .air/ and .mozilla/ directories, just delete their contents.)

1. Restart the secure browser.
2. User Support

If this document does not answer your questions, please contact the Help Desk.

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

|  |
| --- |
| **Ohio Help Desk**  Toll-Free Phone Support:  Email Support: |

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