Secure Browser Installation Manual
For Technology Coordinators

2015-2016

Published April 13, 2016

Prepared by the American Institutes for Research®

Descriptions of the operation of the Test Information Distribution Engine, Test Delivery System, and related systems are property of the American Institutes for Research (AIR) and are used with the permission of AIR.
# Table of Contents

**Section I. Introduction to the Secure Browser Manual** ................................................................. 1  
  Scope .................................................................................................................................................. 1  
  Connecticut Comprehensive Assessments ......................................................................................... 1  
  System Requirements ....................................................................................................................... 1  
  Manual Content ............................................................................................................................... 2  
  Intended Audience ........................................................................................................................... 2  
  Document Conventions ..................................................................................................................... 3  
  Other Resources ............................................................................................................................... 3  

**Section II. Installing the Secure Browser on Desktops and Laptops** .............................................. 4  
  Installing the Secure Browser on Windows ....................................................................................... 4  
    Installing the Secure Browser on an Individual Computer .......................................................... 4  
      Installing the Secure Browser via Windows ............................................................................... 4  
        Installing the Secure Browser via the Command Line ......................................................... 5  
  Sharing the Secure Browser over a Network ................................................................................. 7  
  Copying the Secure Browser Installation Directory to Testing Computers .................................... 8  
  Installing the Secure Browser for Use with an NComputing Terminal ......................................... 8  
  Installing the Secure Browser on a Terminal Server or Windows Server .................................... 10  
  Installing the Secure Browser Without Administrator Rights ...................................................... 11  
  Uninstalling the Secure Browser on Windows ............................................................................. 11  
    Uninstalling via the User Interface ............................................................................................. 11  
    Uninstalling via the Command Line ........................................................................................... 12  
  Installing the Secure Browser on Mac OS X .................................................................................. 12  
  Installing the Secure Browser ......................................................................................................... 12  
  Installing Secure Browser 6.5 .......................................................................................................... 14  
  Cloning the Secure Browser Installation to Other Macs ............................................................... 15  
  Uninstalling the Secure Browser on OS X ..................................................................................... 15  

**Section III. Installing the Secure Browser on Mobile Devices** .................................................... 20
Secure Browser Installation Manual

Installing the Secure Browser on iOS .................................................................................. 20
Installing AIRSecureTest on Android .................................................................................. 21
Chrome OS AIRSecureTest Kiosk App .................................................................................. 22
  Installing the AIRSecureTest Kiosk App on Standalone Chromebooks ......................... 22
  Installing the AIRSecureTest Kiosk App on Managed Chromebooks ......................... 28
Configuring Your State and Assessment Program on Mobile Devices ............................... 29
Installing the Secure Browser on Windows Mobile Devices ................................................. 29

Section IV. Proxy Settings for Desktop Secure Browsers .................................................... 30
Specifying a Proxy Server to Use with the Secure Browser ................................................. 30
Modifying Desktop Shortcuts to Include Proxy Settings .................................................... 31
  Modifying Desktop Shortcuts on Microsoft Windows .................................................... 31
  Modifying Desktop Shortcuts on Mac OS X .................................................................. 32

Appendix A. Creating Group Policy Objects ....................................................................... 33

Appendix B. Resetting Secure Browser Profiles ................................................................. 35
  Resetting Secure Browser Profiles on Windows ............................................................. 35
  Resetting Profiles on Windows Vista and Later ............................................................. 35
  Resetting Profiles on Windows XP .............................................................................. 35
  Resetting Secure Browser Profiles on OS X 10.6 or Later ............................................ 36
  Resetting Secure Browser Profiles on Linux ................................................................. 37

Appendix C. User Support .................................................................................................... 38

Appendix D. Change Log ..................................................................................................... 39
List of Tables

Table 1. Document conventions ........................................................................................................................................... 3
Table 2. Commands for installing 32-bit compatibility libraries ............................................................................................. 17
Table 3. Specifying proxy settings using a shortcut or the command line .............................................................................. 30
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.

Scope

This manual provides instructions for installing the secure browsers on computers and devices used for online assessments.

Connecticut Comprehensive Assessments

The secure browser should be downloaded for the following online test administrations:

- CMT/CAPT Science (online)
- Smarter Balanced English Language Arts/Literacy
- Smarter Balanced Mathematics

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 System Requirements for Online Testing available from the Connecticut Comprehensive Assessment Program portal at http://CT.portal.airast.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, 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, 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, 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.

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

Other Resources

- For information about supported operating systems and web browsers, see the *System Requirements for Online Testing*.

- For information about securing a computer before a test session, see the *Test Administrator User Guide*.

- For information about 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 [http://CT.portal.airast.org](http://CT.portal.airast.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.

Installing the Secure Browser on Windows

This section provides instructions for installing the secure browser on computers running on Windows XP, Vista, 7, 8.0, 8.1, and 10. (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)\CTSecureBrowser\` (64 bit) or `C:\Program Files\CTSecureBrowser\` (32 bit), manually uninstall the secure browser. (If you installed in the default location, the installation package automatically removes it.) See the instructions in the section Uninstalling the Secure Browser on Windows.


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 `CTSecureBrowser-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)\CTSecureBrowser\(64 bit) or C:\Program Files)\CTSecureBrowser\(32 bit).
   - A shortcut CTSecureBrowser 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 CTSecureBrowser on the desktop, and select **Properties**.
   b. Under the **Shortcut** tab, in the **Target** field, modify the command to specify the proxy. See **Table 3** 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. **Optional:** Disable auto-update by following the procedure in the section **Disabling Auto-Update**.

9. Run the browser by double-clicking the CTSecureBrowser shortcut on the desktop. The secure browser opens displaying the student login screen. The browser fills the entire screen and hides the task bar.

10. 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 installed a previous version of the secure browser in a location other than C:\Program Files \(x86)\(64 bit) or C:\Program Files\(32 bit), manually uninstall the secure browser. (If you installed in C:\Program Files \(x86)\, the installation package automatically removes it.) See the instructions in the section **Uninstalling the Secure Browser on Windows**.
Secure Browser Installation Manual


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\CTSecureBrowser-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\CTSecureBrowser-Win.msi.
   - <Target> Path to the location where you want to install the secure browser. If absent, installs to the directory described in step 8. 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\CTSecureBrowser-Win.msi /quiet
   INSTALLDIR=C:\AssessmentTesting\BrowserInstallDirectory
   ```
   installs the secure browser from the installation package at C:\temp\CTSecureBrowser-Win.msi into the directory C:\AssessmentTesting\BrowserInstallDirectory using quiet mode.

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

8. Click Finish to exit the setup wizard. The following items are installed:
   - The secure browser to the default location C:\Program Files (x86)\CTSecureBrowser\ (64 bit) or C:\Program Files\CTSecureBrowser\ (32 bit).
   - A shortcut CTSecureBrowser to the desktop.
9. Ensure all background jobs, such as virus scans or software updates, are scheduled outside of test windows. For example, if your testing takes place between 8:00 a.m. and 3:00 p.m., schedule background jobs outside of these hours.

10. Optional: Disable auto-update by following the procedure in the section Disabling Auto-Update.

11. Run the browser by double-clicking the CTSecureBrowser 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.

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:
   
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 CTSecureBrowser from the remote machine to the directory C:\Users\Public\Public Desktop.

c. Run the browser by double-clicking the CTSecureBrowser 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)\CTSecureBrowser.

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:\AssessmentTesting\. 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:\AssessmentTesting\, you are creating a new folder c:\AssessmentTesting\CTSecureBrowser.

c. Copy the shortcut c:\AssessmentTesting\CTSecureBrowser\CTSecureBrowser.exe -shortcut.lnk to the desktop.

d. Run the browser by double-clicking the CTSecureBrowser 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.
Secure Browser Installation Manual

For a listing of supported terminals and servers for this scenario, see System Requirements for Online Testing, available from the Connecticut Comprehensive Assessment Program portal (http://CT.portal.airast.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)\CTSecureBrowser\CTSecureBrowser.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 CTSecureBrowser 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)\CTSecureBrowser\.
   e. Right-click the file CTSecureBrowser.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)\CTSecureBrowser\CTSecureBrowser.exe" -P%SESSIONNAME%

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

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 2003 and 2008.

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)\CTSecureBrowser\CTSecureBrowser" -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 CTSecureBrowser 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)\CTSecureBrowser\.

   d. Right-click the file CTSecureBrowser.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)\CTSecureBrowser\CTSecureBrowser.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)\CTSecureBrowser`) 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 `CTSecureBrowser.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).
Secure Browser Installation Manual

2. Select the secure browser program CTSecureBrowser 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\CTSecureBrowser.exe.

   /X Perform an uninstall.

   [/quiet] Quiet mode, no interaction.

For example, the command

   msiexec /X C:\AssessmentTesting\CTSecureBrowser.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 the Secure Browser

In this scenario, a user installs the secure browser on desktop computers running Mac OS X 10.6 through 10.11. (If you are installing the secure browser on Mac OS X 10.5 with an Intel processor, see the procedure in the section Installing Secure Browser 6.5.) 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 Connecticut Comprehensive Assessment Program portal at http://CT.portal.airast.org. Click the Mac OS X 10.6–10.11 tab, then click Download Browser. If prompted for a download location, select your downloads folder.
3. Open Downloads from the Dock, and click CTSecureBrowser-OSX.dmg to display its contents.

4. Drag the CTSecureBrowser 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.


7. Optional: Disable auto-update by following the procedure in the section Disabling Auto-Update.

8. In Finder, navigate to Go > Applications, and double-click CTSecureBrowser 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.

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

10. Create a desktop shortcut; from the Applications folder, drag CTSecureBrowser to the desktop.
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. (If you are installing the secure browser on Mac OS X 10.6 or later, see the procedure in the section Installing the Secure 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 Connecticut Comprehensive Assessment Program portal at http://CT.portal.airast.org. 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 CTSecureBrowser6.5.OSX.dmg to display its contents.

4. Drag the CTSecureBrowser6.5 icon to 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. Double-click the CTSecureBrowser6.5 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.

7. To exit the browser, click Close in the upper-right corner of the screen.
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. 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 19.

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

3. Clone the OS X image.

4. Deploy the image to the target Macs.

Uninstalling the Secure Browser on OS X

To uninstall an OS X secure browser, drag its folder to the Trash.
Installing the Secure Browser on Linux

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 Connecticut Comprehensive Assessment Program portal (http://CT.portal.airast.org).

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

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

1. Uninstall any previous versions of the secure browser by deleting the directory containing it.

2. If you are installing Linux secure browser version 8.0 or earlier: 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.


4. Right-click the downloaded file CTSecureBrowser-Linux.tar.bz2, and select Extract Here to expand the file. This creates the CTSecureBrowser folder on the desktop.

5. In a file manager, open the CTSecureBrowser folder.

6. Right-click the file install-icon.sh and select Open. At the next dialog box, click Run in Terminal. The installation program installs all dependent libraries and supported voice packs, and creates a CTSecureBrowser icon on the desktop.

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. Optional: Disable auto-update by following the procedure in the section Disabling Auto-Update.

9. If text-to-speech testing is performed on this computer, reboot it.

10. From the desktop, double-click the CTSecureBrowser icon to launch the browser. The student login screen appears. The browser fills the entire screen and hides any panels or launchers.

11. To exit the browser, click CLOSE SECURE BROWSER in the upper-right corner of the screen.
Table 2 lists the commands for installing 32-bit compatibility libraries for popular Linux distributions.

Table 2. Commands for installing 32-bit compatibility libraries

<table>
<thead>
<tr>
<th>Distribution</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fedora 19–22</td>
<td>sudo yum install glibc.i686 nspr.i686 gtk2.i686 xulrunner.i686</td>
</tr>
<tr>
<td>openSUSE 13.1</td>
<td>zypper install glibc-32bit</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 6.5</td>
<td>sudo yum install xulrunner.i686 libgtk-x11-2.0.50.0 libxcom.so glibc.i686</td>
</tr>
<tr>
<td>Ubuntu (LTS) 12.04, 14.04</td>
<td>sudo apt-get install libgtk2.0.0:i386 libstdc++6:i386 libasound2:i386</td>
</tr>
<tr>
<td></td>
<td>libasound2-plugins:i386 libdbus-glib-1-2:i386 libXt6:i386 libreadline6:i386</td>
</tr>
</tbody>
</table>

Uninstalling the Secure Browser on Linux

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

Disabling and Enabling Auto-Update

Starting with version 8, the secure browser automatically checks for and installs updates—if TDS is configured to support auto-update. You can disable this feature on a per-browser level.

Understanding Auto-Update

AIR publishes updates to the secure browser as necessary, usually to provide enhancements, compatibility with operating systems, or to resolve identified security issues. Starting with version 8, the secure browser can automatically install these updates, similar to a web browser.

The secure browser checks for updates under the following conditions:

- The secure browser is running and its login page is visible. If the secure browser is closed, or if a student is taking a test, it does not check for updates.

- No other application is running on the computer. If another application is running, the secure browser does not check for updates.

If all of the above conditions are satisfied, the secure browser checks for an update. If an update is available, the secure browser asks if you want to download and install it. After installation, the secure browser restarts.
Secure Browser Installation Manual

On days when you want to check for an update, keep the computer on and ensure the secure browser is open to the login page. AIR announces release dates on the portal, so you may want to keep the secure browser running on those release dates.

If the secure browser is not running the night an auto-update is published, it continues checking on subsequent nights until the update can be installed. Some updates are optional, and others are required. If an update is required, you will be informed of the time by which the update must be installed. If a required update is not installed during that time, students will not be able to log in and test using the secure browser.

The auto-update feature is not available if the secure browser is installed in a non-standard location such as on a network drive or on a computer that uses a thin-client configuration.

Auto-update is available starting with version 8 of the secure browser. If you have an earlier version, you must manually install version 8 or a later version to take advantage of auto-update. You can download the installation files for the secure browser from the Connecticut Comprehensive Assessment Program portal at http://CT.portal.airast.org.

Auto-update is enabled by default when you install the secure browser. To disable auto-update, follow the procedure in the section Disabling Auto-Update.

Disabling Auto-Update

To disable auto-update:

1. Close the secure browser.

2. In a text editor create a file with a single line containing the word OFF—all upper case. Ensure this is the first and only line in the file.

3. Save the file with the name AUTOUPDATE.txt (upper-case filename, lower-case extension) in the secure browser’s installation directory:

   - Windows (64 bit): C:\Program Files (x86)\CTSecureBrowser\n   - Windows (32 bit): C:\Program Files\CTSecureBrowser\n   - OS X: /Applications/CTSecureBrowser.app/Contents/MacOS/
   - Linux: ~/Desktop/CTSecureBrowser/

4. Start the secure browser.

   **TIP**: **Disabling auto-update on multiple computers** With appropriate network permissions, you can push the file AUTOUPDATE.txt to the directory in step 3 on other computers running the secure browser. Be sure to restart the secure browser on each target machine.
Enabling Auto-Update

You can resume the secure browser’s auto-update feature—if TDS is configured to support auto-update.

To enable auto-update:

1. Navigate to the file where the secure browser is installed.
   - a. Windows (64 bit): C:\Program Files (x86)\CTSecureBrowser\n   - b. Windows (32 bit): C:\Program Files\CTSecureBrowser\n   - c. OS X: /Applications/CTSecureBrowser.app/Contents/MacOS/
   - d. Linux: ~/Desktop/CTSecureBrowser/

2. Delete the file AUTOUPDATE.txt.
Section III. 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 Connecticut Comprehensive Assessment Program portal (http://CT.portal.airast.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.)

1. On your iPad, navigate to the Secure Browser page of the Connecticut Comprehensive Assessment Program portal at http://CT.portal.airast.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 1).

![Figure 1. AIRSecureTest Download Page on the Apple Store](image)

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.
Installing AIRSecureTest on Android

You can download AIRSecureTest from the Connecticut Comprehensive Assessment Program 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.

1. On your Android tablet, navigate to the Secure Browser page of the Connecticut Comprehensive Assessment Program portal at http://CT.portal.airast.org and tap the Android tab. Tap Get it on Google play. (You can also search for AIRSecureTest in the Google Play store to find the secure browser app.) The AIRSecureTest download page appears.

   Figure 2. AIRSecureTest Download Page on Google Play

2. Tap Install, and then tap Accept. The tablet downloads and installs the secure browser.

3. Tap Open. (After installation, an AIRSecureTest icon appears on the tablet’s home page.)

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

   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 Connecticut Comprehensive Assessment Program portal (http://CT.portal.airast.org), Download Secure Browsers page.
Secure Browser Installation Manual

Chrome OS AIRSecureTest Kiosk App

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 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:
   
   o The wireless network to which the Chromebook connects. This typically includes the network’s SSID, password, and other access credentials.
   
   o 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 + Ctrl + D. A yellow exclamation mark appears similar to that in Figure 3.

      ![Figure 3. Chrome OS Missing Message](image)
      Chrome OS is missing or damaged. Please insert a recovery USB stick.

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

      ![Figure 4. Turn OS Verification Off Message](image)
      To turn OS verification OFF, press Enter. Your system will reboot and local data will be cleared.
      To go back, press ESC.

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

      ![Figure 5. OS Verification Off Message](image)
      OS verification is OFF
      Press SPACE to re-enable.
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

Preparing system for Developer Mode.
This may take a while.
Do not turn your computer off until it has restarted.

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

Welcome!
Select your language: English (United States)
Select your keyboard: US
Select a network: x No network

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

Join WiFi network
SSID AIRNetwork
Password

Connect Cancel

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](image)

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](image)

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 (chrome icon) to open Chrome.

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

![Figure 11. Extensions Screen](image)
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: hblfbmjdaalhifaajnnodlkiloengc

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

   c. If you want to run the secure browser as a dedicated kiosk application, do the following:

      i. Point the mouse over AIRSecureTest, and click **Set to auto-launch**.

      ii. Mark the **Permanently keep this device in kiosk mode** checkbox (see Figure 13).
iii. Click Yes to confirm.

d. Click Done. You return to the Extensions screen.

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 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. 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 14).

   Figure 14. 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 Connecticut from the drop-down list (see **Figure 15**).

   ![Figure 15. AIRSecureTest Launchpad](image)

   **Figure 15. AIRSecureTest Launchpad**

   2. Under **Choose Your Assessment Program**, the Connecticut Comprehensive Assessment Program 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. 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. To execute these commands from the command line, change to the directory containing the secure browser’s executable file.

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

<table>
<thead>
<tr>
<th>Description</th>
<th>System</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run the browser without any proxy</td>
<td>Windows</td>
<td>CTSecureBrowser.exe -proxy 0</td>
</tr>
<tr>
<td></td>
<td>Mac 10.5 (Intel)</td>
<td>arch -i386 ./CTSecureBrowser6.5 -proxy 0</td>
</tr>
<tr>
<td></td>
<td>Mac 10.6–10.11</td>
<td>./CTSecureBrowser -proxy 0</td>
</tr>
<tr>
<td></td>
<td>Linux</td>
<td>./CTSecureBrowser.sh -proxy 0</td>
</tr>
<tr>
<td>Set the proxy for HTTP requests only</td>
<td>Windows</td>
<td>CTSecureBrowser.exe -proxy 1:http:foo.com:80</td>
</tr>
<tr>
<td></td>
<td>Mac 10.5 (Intel)</td>
<td>arch -i386 ./CTSecureBrowser6.5 -proxy 1:http:foo.com:80</td>
</tr>
<tr>
<td></td>
<td>Mac 10.6–10.11</td>
<td>./CTSecureBrowser -proxy 1:http:foo.com:80</td>
</tr>
<tr>
<td></td>
<td>Linux</td>
<td>./CTSecureBrowser.sh -proxy 1:http:foo.com:80</td>
</tr>
<tr>
<td>Set the proxy for all protocols to mimic the “Use this proxy server for all protocols” of Firefox</td>
<td>Windows</td>
<td>CTSecureBrowser.exe -proxy 1:*:foo.com:80</td>
</tr>
<tr>
<td></td>
<td>Mac 10.5 (Intel)</td>
<td>arch -i386 ./CTSecureBrowser6.5 -proxy 1:*:foo.com:80</td>
</tr>
<tr>
<td></td>
<td>Mac 10.6–10.11</td>
<td>./CTSecureBrowser -proxy 1:*:foo.com:80</td>
</tr>
<tr>
<td></td>
<td>Linux</td>
<td>./CTSecureBrowser.sh -proxy 1:*:foo.com:80</td>
</tr>
</tbody>
</table>
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.

Modifying Desktop Shortcuts on Microsoft Windows

1. Right-click the desktop shortcut for the secure browser, and select Properties.

2. Click the Shortcut tab.

3. If the Target field is disabled, do the following (otherwise skip to step 4):
   a. Close the Properties dialog box, and delete the desktop shortcut for the secure browser.
   b. Create a new desktop shortcut. In the Windows Explorer, navigate to C:\Program Files (x86) \ (64 bit) or C:\Program Files \CTSecureBrowser\ (32 bit). Right-click the file CTSecureBrowser.exe, and select Send To \ Desktop (create shortcut).
Secure Browser Installation Manual

c. Right-click the desktop shortcut for the secure browser, and select **Properties**.

d. Click the **Shortcut** tab.

4. In the **Target** field, modify the command as specified in **Table 3**. For example:

   "C:\Program Files (x86)\CTSecureBrowser\CTSecureBrowser.exe" -proxy 1:http:foo.com:80

5. Click **OK**.

**Modifying Desktop Shortcuts on Mac OS X**

1. In Finder, navigate to Applications > Utilities, and open **Terminal**.

2. Change to the desktop directory.

   ```
   cd ~/Desktop
   ```

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

   ```
   pico securebrowser.command
   ```

4. Copy or type the following the lines:

   ```
   #!/bin/sh
   /Applications/CTSecureBrowser.app/Contents/MacOS./CTSecureBrowser -proxy 1:http:foo.com:80 &
   ```

5. Be sure to specify the complete path to the secure browser and the desired proxy option. Ensure the command ends with an ampersand &. Save the file and exit the editor by pressing **Ctrl-O, Enter** and **Ctrl-X**.

6. Apply execute permission to the file. In Terminal, type

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

7. Close Terminal.

8. Click the **securebrowser.command** icon on the desktop. The secure browser opens with the proxy setting you configured.
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 “Assign user logon scripts” at http://technet.microsoft.com/en-us/library/cc781361(v=ws.10).aspx.

1. In the task bar (Windows 10), or in Start > Run, (previous versions of Windows), enter > gedit.msc. The Local Group Policy Editor appears.

   ![Local Group Policy Editor](image)

   Figure 16. Local Group Policy Editor

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

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

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

Resetting Profiles on Windows Vista and Later
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\n   - C:\Users\username\AppData\Roaming\AIR\n   - C:\Users\username\AppData\Local\Mozilla\n   - C:\Users\username\AppData\Roaming\Mozilla\n
   where username is the Windows user account where the secure browser is installed. (Keep the AIR\ and Mozilla\ directories, just delete their contents.)

3. Start the secure browser.

Resetting Profiles on Windows XP
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\n   - C:\Documents and Settings\username\Application Data\AIR\n   - C:\Documents and Settings\username\Local Settings\Application Data\Mozilla\n   - C:\Documents and Settings\username\Application Data\Mozilla\n
   where username is the Windows user account where the secure browser is installed. (Keep the AIR\ and Mozilla\ directories, just delete their contents.)

3. 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 19.

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 19. Cleaning Secure Browser on OS X 10.6 or Later
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.)

3. Restart the secure browser.
Appendix C. User Support

If this document does not answer your questions, please contact the Connecticut Comprehensive Assessment Program Help Desk.

The Help Desk is open Monday–Friday from 7:00 a.m. to 7:00 p.m. Eastern Time (except holidays) during the testing window. During these hours, staff will respond promptly to calls. Outside of the testing window, the Help Desk is open Monday–Friday from 7:00 am to 4:00 pm Eastern Time.

Connecticut Comprehensive Assessment Program Help Desk

Toll-Free Phone Support: 1-844-202-7583
Email Support: CThelpdesk@air.org

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

<table>
<thead>
<tr>
<th>Location</th>
<th>Change</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document Preparation</td>
<td></td>
<td>08/14/15</td>
</tr>
<tr>
<td><strong>Connecticut Comprehensive Assessments</strong></td>
<td>Listed all relevant online assessments</td>
<td>08/25/15</td>
</tr>
<tr>
<td><strong>Installing the Secure Browser via Windows</strong></td>
<td>Updated to support Windows 10</td>
<td>09/22/15</td>
</tr>
<tr>
<td><strong>Uninstalling the Secure Browser on Windows</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Modifying Desktop Shortcuts on Microsoft Windows</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Installing the AIRSecureTest Kiosk App on Standalone Chromebooks</strong></td>
<td>Updated Kiosk Application installation process</td>
<td>01/07/16</td>
</tr>
<tr>
<td><strong>Configuring Your State and Assessment Program on Mobile Devices</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Installing the Secure Browser on 32- or 64-Bit Distributions</strong></td>
<td>Updated Linux 32- and 64-Bit instructions</td>
<td>01/07/16</td>
</tr>
<tr>
<td><strong>Configuring Your State and Assessment Program on Mobile Devices</strong></td>
<td>Renamed section for both Chrome and iOS</td>
<td>1/28/16</td>
</tr>
<tr>
<td><strong>Installing the Secure Browser on Mobile Devices</strong></td>
<td>Updated the processes for Chromebooks and Android</td>
<td>3/9/16</td>
</tr>
<tr>
<td><strong>Resetting Secure Browser Profiles on Windows</strong></td>
<td>Added additional directories to empty; clarified versions of Windows</td>
<td>3/9/16</td>
</tr>
</tbody>
</table>