Appendix O

Additional Configurations and Troubleshooting Guide for Windows, Mac, Chrome OS, and Linux

Configurations, Troubleshooting, and Advanced Secure Browser Installation Guide for Windows

For Technology Coordinators

2020-2021

Updated July 14, 2020

Prepared by Cambium Assessment, Inc.

Table of Contents

Configurations, Troubleshooting, and Advanced Secure Browser Installation for Windows

This document contains configurations, troubleshooting, and advanced Secure Browser installation instructions for your network and Windows workstations.

How to Configure Networks for Online Testing

This section contains additional configurations for your network.

Which Resources to Add to your Allowlist for Online Testing

This section presents information about the URLs that Cambuim Assessment, Inc. (CAI) provides. Ensure your network's firewalls are open for these URLs. If your testing network includes devices that perform traffic shaping, packet prioritization, or Quality of Service, ensure these URLs have high priority.

Which URLs for Non-Testing Sites to Add to your Allowlist

Table 1 lists URLs for non-testing sites, such as Test Information Distribution Engine (TIDE) and Online Reporting System (ORS).

Table 1. CAI URLs for Non-Testing Sites

System	URL
Indiana Assessment Portal and Secure Browser installation files	https://indiana.portal.cambiumast.com
Single Sign-On System	https://sso1.cambiumast.com/auth/realms/indiana/account
Test Information Distribution Engine	https://in.tide.cambiumast.com/
Online Reporting System	https://in.reports.cambiumast.com/

Which URLs for TA and Student Testing Sites to Add to your Allowlist

Testing servers and satellites may be added or modified during the school year to ensure an optimal testing experience. As a result, CAI strongly encourages you to add these URLs to your allowlist at the root level. This requires using a wildcard.

Table 2. CAI and AIR URLs for Testing Sites

System	URL
TA and Student Testing Sites Assessment Viewing Application For 2020-2021, users should add both CAI and AIR URLs listed to their allowlist	*.cambiumast.com *.tds.cambiumast.com *.cloud1.tds.cambiumast.com *.cloud2.tds.cambiumast.com *.airast.org *.tds.airast.org

	*.cloud1.tds.airast.org *.cloud2.tds.airast.org

Which URLs for Online Dictionary and Thesaurus to Add to your Allowlist

Some online assessments contain an embedded dictionary and thesaurus provided by Merriam-Webster. The Merriam-Webster URLs listed in Table 3 should be added to your allowlist to ensure that students can use them during testing.

Table 3. CAI URLs for Online Dictionaries and Thesauruses

Domain Name	IP Address
media.merriam-webster.com	64.124.231.250
www.dictionaryapi.com	64.124.231.250

Which Ports and Protocols are Required for Online Testing

Table 4 lists the ports and protocols used by the Test Delivery System. Ensure that all content filters, firewalls, and proxy servers are open accordingly.

Table 4. Ports and Protocols for Test Delivery System

Port/Protocol	Purpose
80/TCP	HTTP (initial connection only)
443/TCP	HTTPS (secure connection)

How to Configure Filtering Systems

If the school's filtering system has both internal and external filtering, the URLs for the testing sites (see Table 2) must be added to allowlists in both filters. Please see your vendor's documentation for specific instructions. Also, be sure to add these URLs to your allowlist in any multilayer filtering system (such as local and global layers).

How to Configure for Domain Name Resolution

Table 1 and Table 2 list the domain names for CAI's testing and non-testing applications. Ensure the testing machines have access to a server that can resolve those names.

How to Configure Network Settings for Online Testing

Local Area Network (LAN) settings on testing machines should be set to automatically detect network settings.

1. Open Control Panel.
2. Open Internet Options.

3. Open Connections tab.
4. Open LAN Settings.
5. Mark the Automatically detect settings checkbox.
6. Click OK to close the Local Area Network (LAN) Settings window.
7. Click **OK** to close the ***Internet Properties*** window.
8. Click **X** to close the **Control Panel**.

How to Configure the Secure Browser for Proxy Servers

By default, the Secure Browser attempts to detect the settings for your network's web proxy server. However, users of web proxies should execute a proxy command once from the command prompt. This command does not need to be added to the Secure Browser shortcut. Table 5 lists the form of the command for different settings and operating systems. To execute these commands from the command line, change to the directory containing the Secure Browser's executable file.

Note: Domain names in commands The commands in Table 5 use the domains foo.com and proxy.com. When configuring for a proxy server, use your actual testing domain names as listed in the section Which Resources to Add to your Allowlist for Online Testing.

Table 5. Specifying proxy settings using the command line

Description	System	Command
Use the browser without any proxy	Windows	IndianaSecureBrowser.exe -proxy 0 aHR0cHM6Ly9pbi50ZHMuY2FtYml1bWFzdC5jb20vc3R1ZGVudA==
Set the proxy for HTTP requests only	Windows	IndianaSecureBrowser.exe -proxy 1:http:foo.com:80 aHR0cHM6Ly9pbi50ZHMuY2FtYml1bWFzdC5jb20vc3R1ZGVudA==
Set the proxy for all protocols to mimic the "Use this proxy server for all protocols" of Firefox	Windows	IndianaSecureBrowser.exe -proxy 1:*:foo.com:80 aHR0cHM6Ly9pbi50ZHMuY2FtYml1bWFzdC5jb20vc3R1ZGVudA==
Specify the URL of the PAC file	Windows	IndianaSecureBrowser.exe -proxy 2:proxy.com aHR0cHM6Ly9pbi50ZHMuY2FtYml1bWFzdC5jb20vc3R1ZGVudA==

Auto-detect proxy settings	Windows	IndianaSecureBrowser.exe -proxy 4 aHR0cHM6Ly9pbi50ZHMuY2FtYml1bWFzdC5jb20vc3R1ZGVudA==
Use the system proxy setting (default)	Windows	IndianaSecureBrowser.exe -proxy 5 aHR0cHM6Ly9pbi50ZHMuY2FtYml1bWFzdC5jb20vc3R1ZGVudA==

How to Install the Secure Browser for Windows Using Advanced Methods

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

How to Install 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 How to Install the Secure Browser Without Administrator Rights.

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

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

1. Navigate to the **Download Secure Browsers** page of the Indiana Assessment Portal: https://indiana.portal.cambiumast.com/securebrowsers.stml. Click the **Windows** tab, then click **Download Browser**. A dialog window opens.
2. Save the file on the computer (this step may vary depending on the browser you are using):
3. If presented with a choice to **Run** or **Save** the file, click **Save**, and save the file to a convenient location.
4. If presented only with the option to **Save**, save the file to a convenient location.
5. Note the full path and filename of the downloaded file, such as c:\temp\IndianaSecureBrowser-Win.msi.
6. Open a command prompt as the administrator by doing the following:
    a. Click **Start**, and locate the Command Prompt application. (In some versions of Windows the application is under **All Programs > Accessories > Command Prompt**.)
    b. Right-click Command Prompt, and select Run as Administrator.
    c. As necessary, type the administrator password for the computer. The command prompt opens.

7. (You need to do step 4 only once for the current login. The next time you open the command prompt, Windows retains the administrator role.)
8. Run the command msiexec /I <Source> [/quiet] [INSTALLDIR=<Target>]
9. <Source> Path to the installation file, such as C:\temp\IndianaSecureBrowser-Win.msi.
10. <Target> Path to the location where you want to install the Secure Browser. If absent, installs to the directory described in step 7. The installation program creates the directory if it does not exist.
11. /I Perform an install.
12. [/quiet] Quiet mode, no interaction.
13. For example, the command
14. msiexec /I c:\temp\IndianaSecureBrowser-Win.msi /quiet INSTALLDIR=C:\AssessmentTesting\BrowserInstallDirectory
15. installs the Secure Browser from the installation package at C:\temp\ IndianaSecureBrowser-Win.msi into the directory C:\AssessmentTesting\BrowserInstallDirectory using quiet mode.
16. Follow the instructions in the setup wizard. When prompted for setup type, click **Install**.
17. Click **Finish** to exit the setup wizard. The following items are installed:
    d. The Secure Browser to the default location C:\Program Files (x86)\ IndianaSecureBrowser\ (64-bit) or C:\Program Files\ IndianaSecureBrowser\ (32-bit).
    e. A shortcut IndianaSecureBrowser to the desktop.
18. 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.
19. Run the browser by double-clicking the IndianaSecureBrowser shortcut on the desktop. The Secure Browser opens displaying the student login screen. The browser fills the entirescreen and hides the task bar.
20. To exit the browser, click **CLOSE SECURE BROWSER** in the upper-right corner of the screen.

How to Copy 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 on the Indiana Assessment Portal. Note the path of the installation directory, such as C:\Program Files (x86)\IndianaSecureBrowser.

2. Identify the directory on the local testing computers to which you will copy the browser file (it should be the same directory on all computers). For example, you may want to copy the directory to c:\AssesssmentTesting\. Ensure you select a directory in which the students can run executables.

3. On each local testing computer, do the following:

   a. Ensure all background jobs, such as virus scans or software updates, are scheduled outside of test windows. For example, if your testing takes place between 8:00 a.m. and 3:00 p.m., schedule background jobs outside of these hours.

   b. Copy the installation directory used in step 1 from the remote machine to the directory you selected in step 2. For example, if the target directory is c:\AssesssmentTesting\, you are creating a new folder c:\AssesssmentTesting\IndianaSecureBrowser.

   c. Copy the shortcut c:\AssesssmentTesting\IndianaSecureBrowser\IndianaSecureBrowserSecureBro wser.exe - Shortcut.lnk to the desktop.

   d. Run the browser by double-clicking the IndianaSecureBrowser shortcut on thedesktop. 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.

How to Install 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.

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

2. Install the Secure Browser following the directions on the Indiana Assessment Portal.

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

4. "C:\Program Files (x86)\IndianaSecureBrowser\ IndianaSecureBrowser.exe" -CreateProfile %SESSIONNAME%

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

6. Save the file to the desktop as logon.bat.

7. Create a group policy object that runs the file logon.bat each time a user logs in. For details, see How to Create Group Policy Objects.

8. On each NComputing console, create a new IndianaSecureBrowser 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)\IndianaSecureBrowser\.
    e. Right-click the file IndianaSecureBrowser.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:
9. "C:\Program Files(X86)\IndianaSecureBrowser\IndianaSecureBrowser.exe" -P %SESSIONNAME%
10. If you used a different installation path on the Windows server, use that in the above command.
    a. Click **OK** to close the Properties dialog box.
11. Verify the installation by double-clicking the shortcut to start the Secure Browser.

How to Install 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 2012 R2 and 2016 R2.

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, CAI does not recommend this installation scenario for testing.

1. Log in to the server, and install the Secure Browser by following the directions on the Indiana Assessment Portal. Note the path of the installation directory.
2. Copy and paste the line below into Notepad (no line breaks):
3. "C:\Program Files (x86)\IndianaSecureBrowser\IndianaSecureBrowser" -CreateProfile %SESSIONNAME%
4. If you used a different installation path, use that in the above command.

5. Save the file to the desktop as logon.bat.

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

7. On each client, create a new IndianaSecureBrowser desktop shortcut by doing thefollowing (this step is necessary because the default shortcut created by the installation programhas 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)\ IndianaSecureBrowser\.

   d. Right-click the file IndianaSecureBrowser.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:

8. "C:\Program Files(X86)\IndianaSecureBrowser\ IndianaSecureBrowser.exe" -P %SESSIONNAME%

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

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

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

How to Install 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)\ IndianaSecureBrowser) 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 IndianaSecureBrowser.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.

About Sharing the Secure Browser over a Network

While the Secure Browser can be installed on a server's shared drive and then shared to each testing computer's desktop via a shortcut, CAI strongly discourages this setup as it can compromise the stability and performance of the browser, especially during peak testing times.

How to Uninstall the Secure Browser on Windows

The following sections describe how to uninstall the Secure Browser from Windows or from the command line. Older versions of the Secure Browser will be automatically uninstalled during the installation of a new version.

How to Uninstall the Secure Browser via the User Interface

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

1. Navigate to Settings > System > Apps & features (Windows 10) or Control Panel > Add or Remove Programs or Uninstall a Program (previous versions of Windows).
2. Select the Secure Browser program IndianaSecureBrowser and click **Remove** or **Uninstall**.
3. Follow the instructions in the uninstall wizard.

How to Uninstall the Secure Browser via the Command Line

1. Open a command prompt.
2. Run the command msiexec /X <Source> /quiet
3. <Source> Path to the executable file, such as C:\MSI\IndianaSecureBrowser.exe.
4. /X Perform an uninstall.
5. [/quiet] Quiet mode, no interaction.
6. For example, the command
7. msiexec /X C:\AssessmentTesting\IndianaSecureBrowser.exe /quiet
8. uninstalls the Secure Browser installed at C:\AssessmentTesting\ using quiet mode.

How to Install 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 Indiana Assessment Portal for details.

How to Create Group Policy Objects

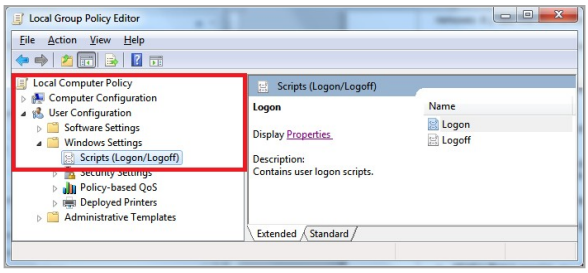
Many of the procedures listed above refer to creating a group policy object. These are objects that Windows executes upon certain events. The following procedure explains how to create a

group policy object that runs a script when a user logs in. The script itself is saved in a file logon.bat.

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

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

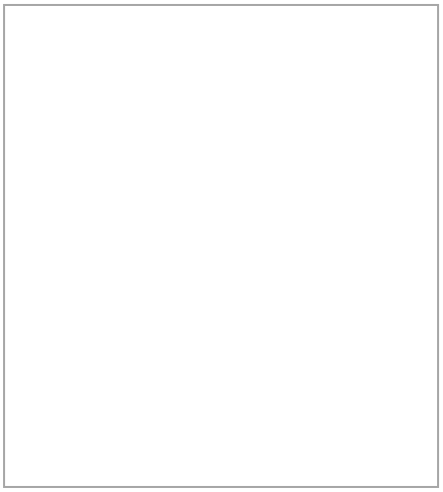
Figure 1. Local Group Policy Editor



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

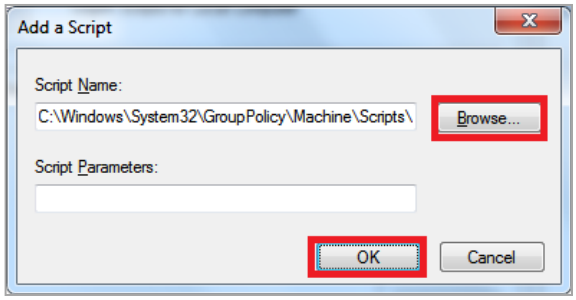
3. Select **Logon** and click **Properties**. The ***Logon Properties*** dialog box appears.

Figure 2. Logon Properties



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

Figure 3. Add a Script



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.

How to Configure Windows Workstations for Online Testing

This section contains additional configurations for Windows.

How to Disable Fast User Switching

Fast User Switching is a feature in Windows 8, 8.1, and 10 that allows for more than one user to be logged in at the same time. If Fast User Switching is not disabled and students try to access it during a test, the Secure Browser will pause the test. The following sections describe how to disable Fast User Switching for different versions of Windows.

How to Disable Fast User Switching in Windows 8 and 8.1

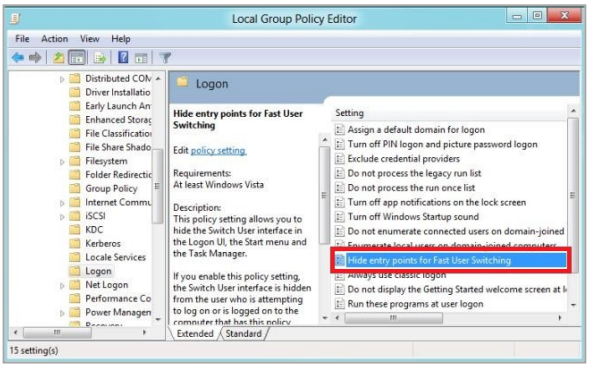
The following procedure describes how to disable Fast User Switching under Windows 8 and 8.1.

1. In the Search charm, type gpedit.msc. Double-click the gpedit icon in the Apps pane. The Local Group Policy Editor window opens.

Figure 4. Search Charm

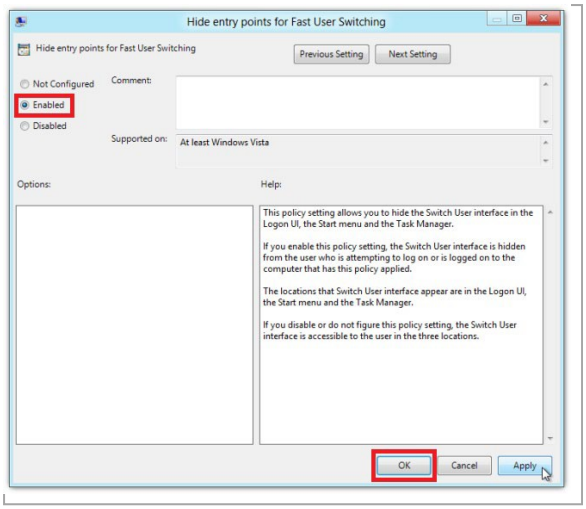
2. Navigate to Computer Configuration > Administrative Templates > System > Logon.
3. In the Setting pane, double-click Hide entry points for Fast User Switching.

Figure 5. Local Group Policy Editor



4. Select **Enabled** and then click **OK**.

Figure 6. Hide entry points for Fast User Switching

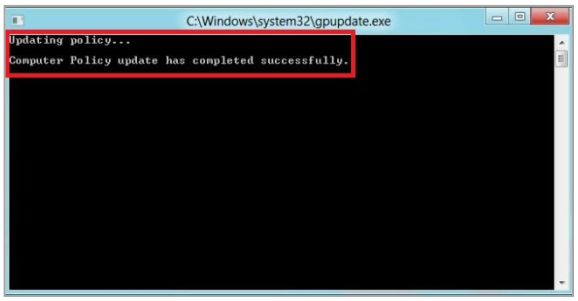


5. In the Search charm, type **run**. The ***Run*** dialog box opens.
6. Enter the command gpupdate /force into the text box and then click **OK**. (Note the space before the forward slash.)

Figure 7. Run

7. The command window opens. When you see the message Computer Policy update has completed successfully, this will be your notification that Windows has successfully disabled Fast User Switching.

Figure 8. Command Window



How to Troubleshoot Windows Workstations

This section contains troubleshooting tips for Windows.

How to Reset Secure Browser Profiles on Windows

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

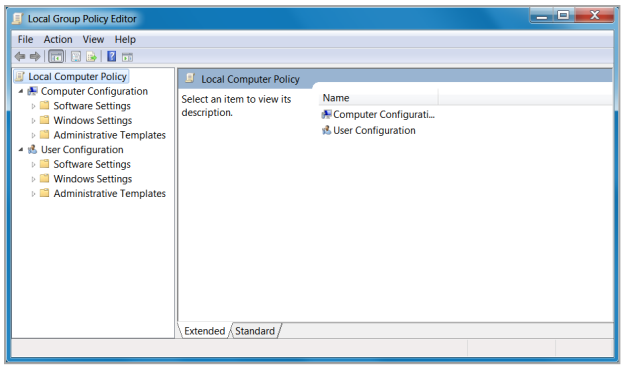
1. Log on as an admin user or as the user who installed the Secure Browser, and close any open Secure Browsers.
2. Delete the contents of the following folders:
3. C:\Users\username\AppData\Local\CAI\
4. C:\Users\username\AppData\Roaming\CAI\
5. where username is the Windows user account where the Secure Browser is installed. (Keep the CAI\ folders, just delete their contents.)
6. Start the Secure Browser.

How to Block Device Touch Input Using the Group Policy Editor

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

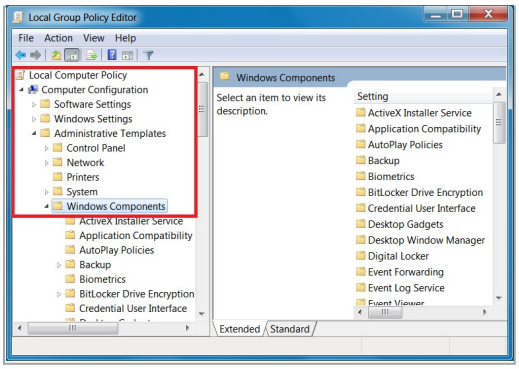
1. Type gpedit.msc in the *Search* box on the **Start** menu. The ***Local Group Policy Editor*** window appears.
2. Navigate to Computer Configuration\Administrator Templates\Windows Components.

Figure 9. Local Group Policy Editor



3. Navigate to Computer Configuration\Administrator Templates\Windows Components.

Figure 10. Windows Components



4. Scroll down to the **Tablet PC** folder, then select **Input Panel**. The following screen displays.

Figure 11. Input Panel

5. Enable the following items in the *Setting* column:

a. Turn off AutoComplete integration with Input Panel

b. Prevent Input Panel tab from appearing

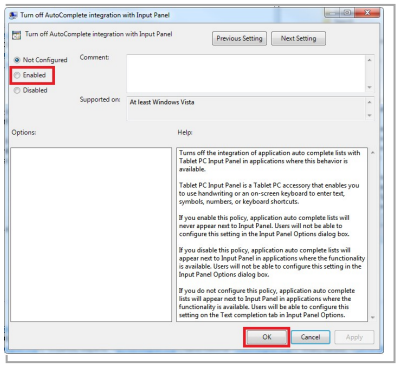
c. For tablet pen input, don't show the Input Panel icon

d. For touch input, don't show the Input Panel icon

e. Disable text prediction

6. To enable an item in the *Setting* column, double-click on that item. The following screen will display that will allow you to enable or disable your selected item as required.

Figure 12. Turn off AutoComplete integration with Input Panel



7. Select **Enabled**, and click **OK**.

8. Close the Local Group Policy Editor window.

How to Install Windows Media Pack for Windows 8.1 N and KN

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

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

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

CAI encourages downloading this software and ensuring it works with sample websites and video and audio files prior to installing the Windows Secure Browser. Installation instructions are provided on Microsoft's download page.

Microsoft Resources:

- About the Media Feature Pack for Windows 8.1 N and Windows 8.1 KN Editions: April 2014 (http://support.microsoft.com/kb/2929699/en-us)
- Download Media Feature Pack for N and KN Versions of Windows 8.1 (http://www.microsoft.com/en-us/download/details.aspx?id=42503)

How to Configure ZoomText to Recognize the Secure Browser

When displaying a test with a print-size accommodation above 4× magnification, the Secure Browser automatically enters streamlined mode. If you want to retain the standard layout of a test but display it with a print magnification above 4×, then consider using ZoomText—a magnification and screen-reading software that you can use with the Secure Browser. Use the following procedure to ensure ZoomText recognizes the Secure Browser.

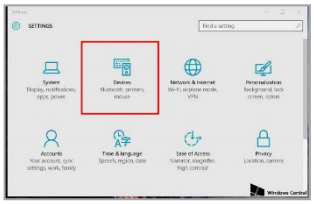
1. If ZoomText is running, close it.
2. In the Windows Explorer, go to the installation directory for your version of ZoomText. For example, if you have ZoomText version 10.1:
3. Go to C:\Program Files (x86)\ZoomText 10.1\ (Windows 64-bit)
4. Go to C:\Program Files\ZoomText 10.1\ (Windows 32-bit).
5. In a text editor, open the file ZoomTextConfig.xml.
6. Search for line containing the D2DPatch property, similar to the following:
7. <Property name="D2DPatch" value ="*,~dwm,~firefox,~thunderbird"/>
8. In the value attribute, add the prefix for your state's Secure Browser:
9. <Property name="D2DPatch" value ="*,~dwm,~firefox,~ IndianaSecureBrowser,~thunderbird"/>
10. Save the file, and restart ZoomText.

How to Set the Touch Keyboard on Microsoft Surface Pro Tablet to Appear

Some Surface Pro users accessing the touch keyboard are seeing the touch keyboard disappear when they click outside a text box or when they type an answer into a text box and then click next. The keyboard fails to reappear when users click back inside the next text box. To avoid these issues, users must set the touch keyboard to automatically show up.

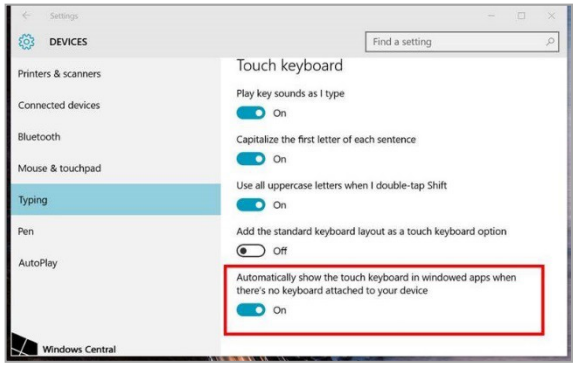
1. Go to **Settings** (keyboard shortcut: **Windows + I**)

Figure 13. Settings



2. Go to Devices > Typing.
3. Scroll down and toggle on: Automatically show the touch keyboard in windowed apps when there's no keyboard attached to your device.

Figure 14. Typing

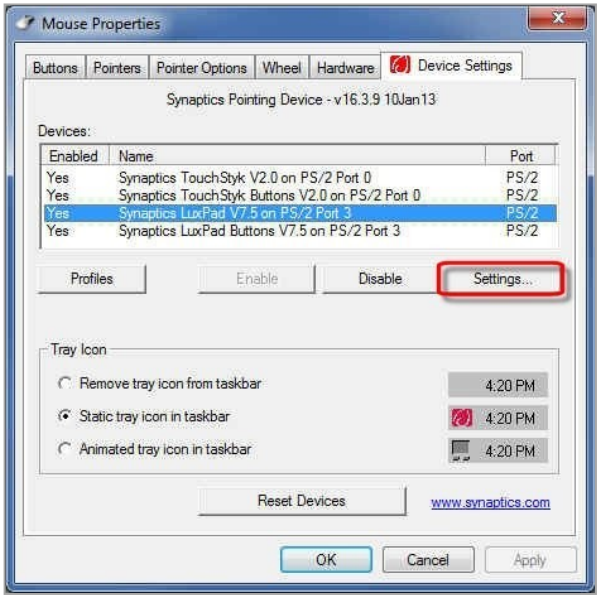


How to Disable Two-finger Scrolling in HP Notebooks with Synaptics TouchPad

The trackpad software on the HP stream notebooks can cause the Secure Browser to close and display an “environment not secure” error. This can occur when a student tries to use the advanced trackpad features such as scrolling gesture with the trackpad. The Synaptics Touchpad driver is the driver that allows full use of all features of the trackpad. To avoid this error and the closing of the Secure Browser, disable the TouchPad two-finger scrolling Feature.

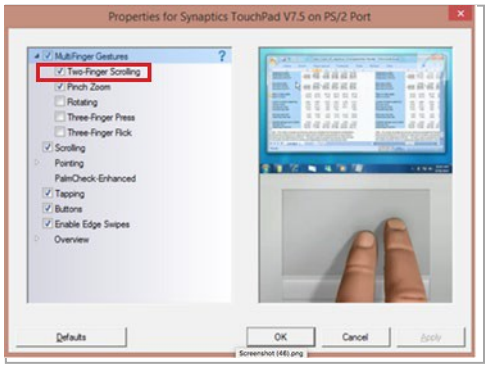
1. Click the **Start** menu (), and then type mouse in the search field.
2. Select **Mouse** from the list of options.
3. Click the **Device Settings** tab.
4. From the **Devices** list, select **Synaptics LuxPad V7.5**, and then click **Settings...**.

Figure 15. Mouse Properties



5. Uncheck Two-Finger Scrolling.

Figure 16. Properties for Synaptics TouchPad



6. Click **Close**, and then click **OK**.

7. In the **Mouse Properties** window, click **Apply**.

How to Disable Automatic Volume Reduction

A feature in Windows automatically lowers or mutes the volume of some apps if Windows detects audio recording. This section describes how to disable automatic volume reduction.

1. Open the **Start Menu**.

2. Open the Control Panel.

3. Select **Sound**. The **Sound** window will open.

4. Select the **Communications** tab.

5. By default, the option to "Reduce the volume of other sounds by 80%" is selected. Change this to **Do nothing**.

6. Select **OK**.

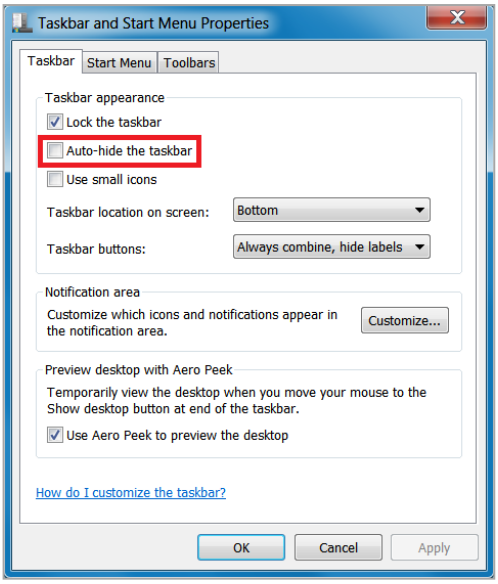
How to View the Windows Taskbar in Permissive Mode

In Permissive Mode, the Windows taskbar should appear when a user hovers their mouse pointer near the bottom of the screen. In Windows 8, 8.1, and 10, the taskbar does not appear as intended. The following sections describe how to view the Windows taskbar in Permissive Mode by turning off the auto-hide feature in the Taskbar Properties. These instructions differ slightly depending on your version of Windows. This procedure must be completed before the Secure Browser is launched on the student workstation.

How to View the Taskbar in Permissive on Windows 8, and 8.1

1. Right-click on the taskbar.
2. Click **Properties**. The ***Taskbar and Start Menu Properties*** window appears. (See Figure 17.)
3. Uncheck the **Auto-hide the taskbar** checkbox.
4. Click **OK**.

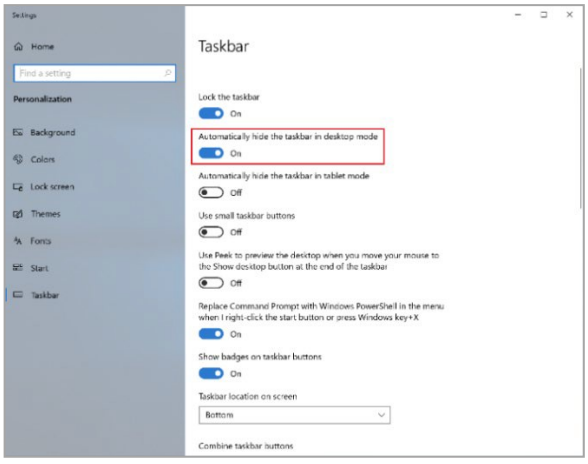
Figure 17. Taskbar and Start Menu Properties



How to View the Taskbar in Permissive Mode on Windows 10

1. Right-click on the taskbar.
2. Click **Properties**. The ***Taskbar*** window appears. (See Figure 18.)
3. Toggle Automatically hide the taskbar in desktop mode to Off.
4. Close the ***Taskbar*** window.

Figure 18. Taskbar



Appendix. Change Log

Changes made after August 2, 2019 are noted.

Location	Description of Change
Throughout	CAI replaced a reference to AIR within text, URLs, or email address.
How to Configure Networks for Online Testing	Changed all references of “whitelist” to “allowlist” or “add to your allowlist”.
Cover Page	Updated dates from 2019-2020 to 2020-2021.
Configurations, Troubleshooting, and Advanced Secure Browser Installation for Windows – Table 2	Added note: For 2020-2021, users should add both CAI and AIR URLs listed to their allowlist.
How to Configure Networks for Online Testing	Removed next section “Configuring for Certificate Revocations”. Our Secure Browser no longer uses the Online Certificate Status Protocol to check certificates. We now validate our certificates in our custom code.
How to Configure Windows Workstations for Online Testing	2020-2021 Update – Remove section on Disabling Fast User Switching in Windows 7.
How to Configure Windows Workstations for Online Testing	2020-2021 Update – Remove language referencing Windows 7.
How to Troubleshoot Windows Workstations	Removed section *How to Run NVDA Screen Reader 2018.1.1 with Take a Test App*. Not supported for IN.
Throughout	Corrected typo “SecureBrowserSecureBrowser” to “SecureBrowser”.

Configurations, Troubleshooting, and Advanced Secure Browser Installation Guide for Mac

For Technology Coordinators

2020-2021

Published March 29, 2020

Prepared by Cambium Assessment, Inc.

Table of Contents

Configurations, Troubleshooting, and Advanced Secure Browser Installation for Mac

This document contains configurations, troubleshooting, and advanced Secure Browser installation instructions for your network and Mac workstations.

How to Configure Networks for Online Testing

This section contains additional configurations for your network.

Which Resources to Add to you Allowlist for Online Testing

This section presents information about the URLs that Cambium Assessment, Inc. (CAI) provides. Ensure your network's firewalls are open for these URLs. If your testing network includes devices that perform traffic shaping, packet prioritization, or Quality of Service, ensure these URLs have high priority.

Which URLs for Non-Testing Sites to Add to you Allowlist

Table 1 lists URLs for non-testing sites, such as Test Information Distribution Engine (TIDE) and Online Reporting System (ORS).

Table 1. CAI URLs for Non-Testing Sites

System	URL
Indiana Assessment Portal and Secure Browser installation files	https://indiana.portal.cambiumast.com
Single Sign-On System	https://sso1.cambiumast.com/auth/realms/indiana/account
Test Information Distribution Engine	https://in.tide.cambiumast.com/
Online Reporting System	https://in.reports.cambiumast.com/

Which URLs for TA and Student Testing Sites to Add to your Allowlist

Testing servers and satellites may be added or modified during the school year to ensure an optimal testing experience. As a result, CAI strongly encourages you to add these URLs to your allowlist at the root level. This requires using a wildcard.

Table 2. CAI and AIR URLs for Testing Sites

System	URL
TA and Student Testing Sites Assessment Viewing Application For 2020-2021, users should add both CAI and AIR URLs listed in this table to their allowlist.	*.cambiumast.com *.tds.cambiumast.com *.cloud1.tds.cambiumast.com *.cloud2.tds.cambiumast.com *.airast.org *.tds.airast.org *.cloud1.tds.airast.org

	*.cloud2.tds.airast.org

Which URLs for Online Dictionary and Thesaurus to Add to your Allowlist

Some online assessments contain an embedded dictionary and thesaurus provided by Merriam-Webster. The Merriam-Webster URLs listed in Table 3 should be added to your allowlist to ensure that students can use them during testing.

Table 3. CAI URLs for Online Dictionaries and Thesauruses

Domain Name	IP Address
media.merriam-webster.com	64.124.231.250
www.dictionaryapi.com	64.124.231.250

Which Ports and Protocols are Required for Online Testing

Table 4 lists the ports and protocols used by the Test Delivery System. Ensure that all content filters, firewalls, and proxy servers are open accordingly.

Table 4. Ports and Protocols for Test Delivery System

Port/Protocol	Purpose
80/TCP	HTTP (initial connection only)
443/TCP	HTTPS (secure connection)

How to Configure Filtering Systems

If the school's filtering system has both internal and external filtering, the URLs for the testing sites (see Table 2) must be added to your allowlist in both filters. Please see your vendor's documentation for specific instructions. Also, be sure to add these URLs to your allowlist in any multilayer filtering system (such as local and global layers).

How to Configure for Domain Name Resolution

Table 1 and Table 2 list the domain names for CAI's testing and non-testing applications. Ensure the testing machines have access to a server that can resolve those names.

How to Configure Network Settings for Online Testing

Local Area Network (LAN) settings on testing machines should be set to automatically detect network settings.

1. Open System Preferences.
2. Open Network.
3. Select **Ethernet** for wired connections or **WiFi** for wireless connections.

4. Click Advanced.
5. Click **Proxies** tab.
6. Click Auto Proxy Discovery checkbox.
7. Click **OK** to close window.
8. Click **Apply** to close **Network** window.
9. Close System Preferences.

How to Configure the Secure Browser for Proxy Servers

By default, the Secure Browser attempts to detect the settings for your network's web proxy server. However, users of web proxies should execute a proxy command once from the command prompt. This command does not need to be added to the Secure Browser shortcut. Table 5 lists the form of the command for different settings and operating systems. To execute these commands from the command line, change to the directory containing the Secure Browser's executable file.

Note: Domain names in commands The commands in Table 5 use the domains foo.com and proxy.com. When configuring for a proxy server, use your actual testing domain names as listed in the section Which Resources to Add to your Allowlist for Online Testing.

Table 5. Specifying proxy settings using the command line

Description	System	Command
Use the browser without any proxy	Mac	./IndianaSecureBrowser -proxy 0 aHR0cHM6Ly9pbi50ZHMuY2FtYmlI1bWFzdC5jb20vc3R1ZGVudA==
Set the proxy for HTTP requests only	Mac	./IndianaSecureBrowser -proxy 1:http:foo.com:80 aHR0cHM6Ly9pbi50ZHMuY2FtYmlI1bWFzdC5jb20vc3R1ZGVudA==
Set the proxy for all protocols to mimic the "Use this proxy server for all protocols" of Firefox	Mac	./IndianaSecureBrowser -proxy 1:*:foo.com:80 aHR0cHM6Ly9pbi50ZHMuY2FtYmlI1bWFzdC5jb20vc3R1ZGVudA==
Specify the URL of the PAC file	Mac	./IndianaSecureBrowser -proxy 2:proxy.com aHR0cHM6Ly9pbi50ZHMuY2FtYmlI1bWFzdC5jb20vc3R1ZGVudA==

Auto-detect proxy settings	Mac	./IndianaSecureBrowser -proxy 4 aHR0cHM6Ly9pbi50ZHMuY2FtYmlI1bWFzdC5jb20vc3R1ZGVudA==
Use the system proxy setting (default)	Mac	./IndianaSecureBrowser -proxy 5 aHR0cHM6Ly9pbi50ZHMuY2FtYmlI1bWFzdC5jb20vc3R1ZGVudA==

How to Install the Secure Browser for Mac using Advanced Methods

This section contains additional instructions for installing the Secure Browser for Mac.

How to Clone 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.

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

   Install the Secure Browser following the directions on the Indiana Assessment Portal. Be sure to run and then close the Secure Browser after the installation.

2. Clone the image.

3. Deploy the image to the target Macs.

How to Uninstall the Secure Browser on Mac

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

How to Configure Mac Workstations for Online Testing

This section contains additional configurations for Mac.

Several features on Mac workstations must be disabled before testing begins. Installing the Mac Secure Profile disables the hot keys for enabling Dictation, Mission Control, and Spaces and the trackpad gestures for accessing Lookup, Space Switching, Expose, and Notification Center. It also sets function keys to standard functions for all users of the Mac for which it is deployed. If you do not install the Secure Profile, these settings and the other settings listed below must be disabled manually. Even if you do install the Secure Profile, the other settings listed below must still be disabled manually.

CAI recommends installing the Mac Secure Profile, as it reduces the number of steps needed to set up Mac devices for online testing; however, the Mac Secure Profile is not required for online testing. Apple provided an updated Mac Secure Profile (now available on CAI's Indiana Assessment Portal) in October 2019 to disable the keyboard shortcuts for screenshots. Devices that had the Secure Profile installed before October 2019 will need to follow the steps below to manually disable keyboard shortcuts for screenshots or install the updated Mac Secure Profile by repeating the installation steps (below). If repeating the Secure Profile installation steps, the former Secure Profile does not need to be deleted. As noted above, there are other Mac device settings listed below that must be manually disabled, despite using the Mac Secure Profile.

How to Install the Mac Secure Profile

The Secure Profile is a configuration profile that can be used to configure Mac workstations for online testing. It can be downloaded from the Indiana Assessment Portal's Secure Browser page and must be installed, along with the Secure Browser, before testing begins.

The Secure Profile disables the hot keys for enabling Mission Control, Spaces, Screenshots, and Dictation and the trackpad gestures for accessing Lookup, App Exposé, Launchpad, and Show Desktop. It also sets function keys to standard functions for all users of the Mac to which it is deployed, disables Voice Control, and disables the menu pop-up that appears when triple-tapping the power button on Touch Bar-enabled devices. It also prevents the device from receiving files via AirDrop and the ability to have your Mac identify items under the pointer. If you do not install the Secure Profile, the features listed in this paragraph must be disabled manually. Even if you do install the Secure Profile, the features listed in the bullet points above must still be disabled manually.

Because the Secure Profile configures the operating system regardless of the operating system's current settings, there is no way for CAI to create a configuration profile to roll back the changes. Before you install the Secure Profile, you should back up your device profile's preferences and settings. Once the device is no longer used for testing, the profile can be removed, and your original settings can be reapplied.

To revert configurations made by the Secure Profile if you did not create a backup of your device profile's preferences and settings prior to installation, the features listed in the paragraph above must be re-enabled manually. These features can be re-enabled through System Preferences. If you need assistance, including reapplying settings to multiple devices at once, contact the Helpdesk.

2020-2021 Update: The Secure Profile has been updated for 2020-2021 to disable Voice Control and the menu pop-up that appears when triple-tapping the power button on Touch Bar-enabled devices. If you have previously installed an older version of the Secure Profile, you must download and install the new version from the link the Indiana Assessment Portal.

Spring 2021 Update: The Secure Profile has been updated for Spring 2021 to prevent the device from receiving files via AirDrop and the ability to have your Mac identify items under the pointer.

1. Click the **Download the Secure Profile** link on the Mac tab of the Indiana Assessments Portal's Secure Browser's page to download the Mac Secure Profile.

Figure 1. Download Mac Secure Profile

2. Run the Mac Secure Profile installer.
3. Upon installation, restart your computer.

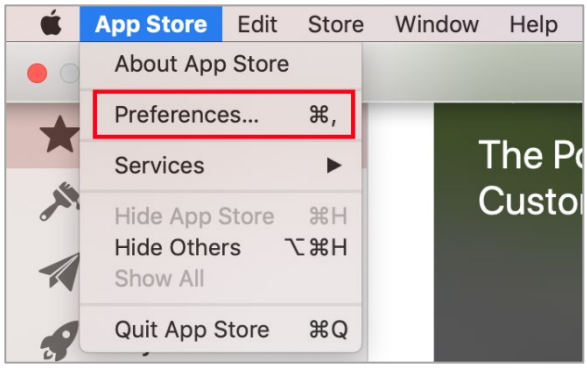
How to Disable Updates to Third-Party Apps

Updates to third-party apps may include components that compromise the testing environment. This section describes how to disable updates to third-party apps.

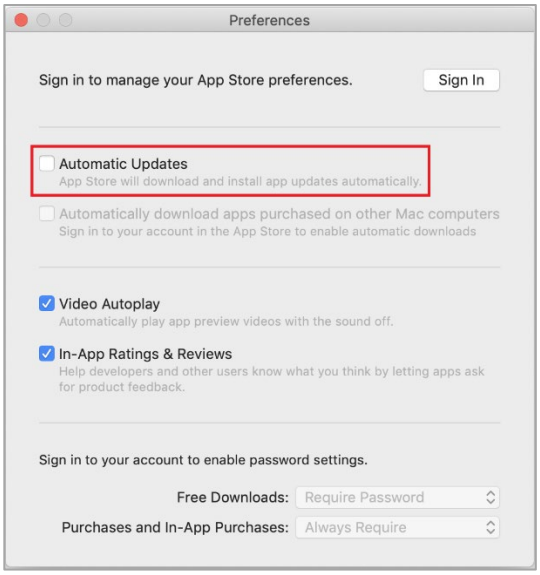
The following instructions are based on macOS 10.14; similar instructions apply for other versions of Mac OS.

1. Log in to the student's account.
2. Open **App Store**. The ***App Store*** window opens.
3. From the menu bar, select **App Store**.

Figure 2. App Store Window



4. Select **Preferences**. The ***Preferences*** window opens.
5. Clear the ***Automatic Updates*** checkbox.
6. Close the ***Preferences*** and ***App Store*** windows.

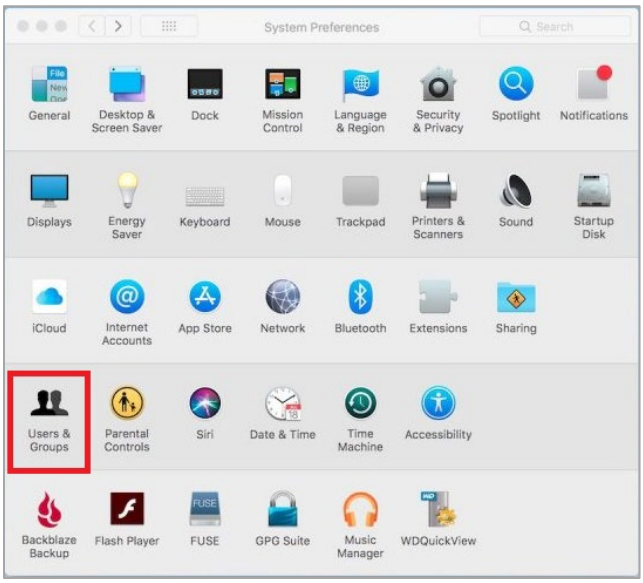


How to Disable Fast User Switching

Fast User Switching is a feature in Mac OS X 10.11 and higher that allows for more than one user to be logged in at the same time. If Fast User Switching is not disabled and students try to access it during a test, the Secure Browser will pause the test. The following instructions describe how to disable Fast User Switching.

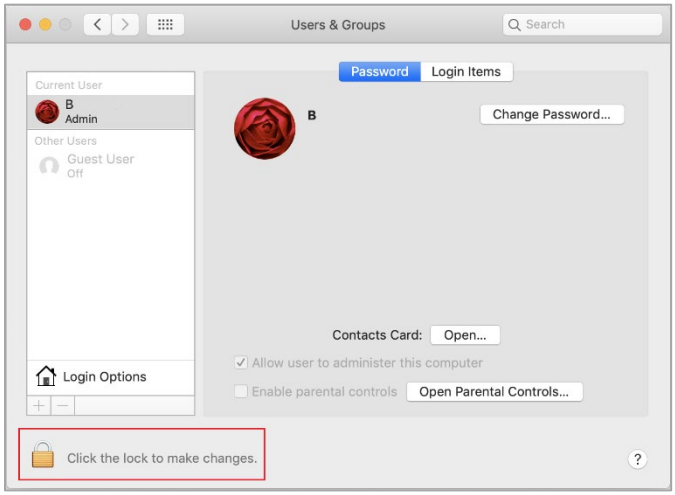
1. Open **System Preferences**. The ***System Preferences*** window opens.

Figure 4. System Preferences > Users & Groups



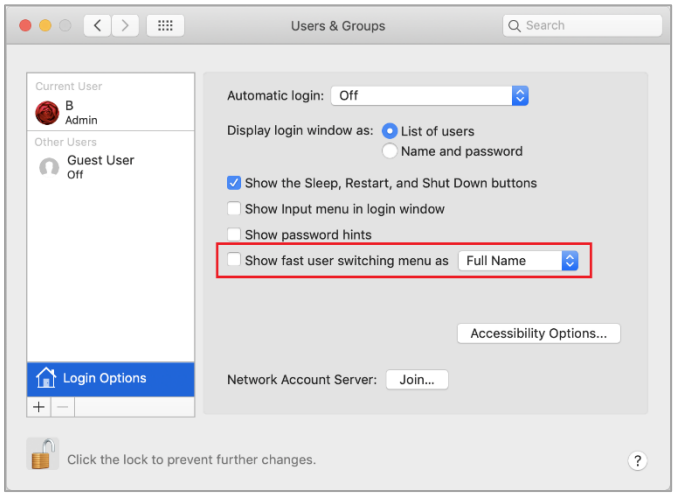
2. Select **Users & Groups**. The ***Users & Groups*** window opens.
3. If the padlock in the lower left corner is locked, click it and authenticate with administrator credentials.

Figure 5. Users & Groups



4. Select **Login Options**. The ***Login Options*** window opens.
5. Clear the ***Show fast user switching menu as*** checkbox

Figure 6. Login Options



How to Disable Sleep Mode on macOS 11

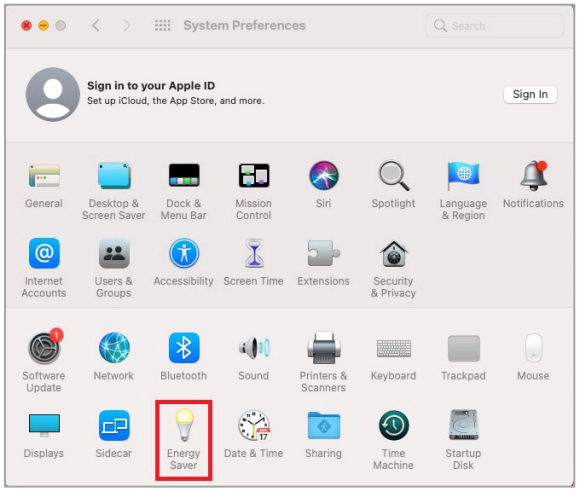
Sleep mode should be disabled on macOS 11 devices prior to testing. If sleep mode is not disabled and the device enters sleep mode while the student is testing, the student's testing experience may be disrupted. The following instructions differ slightly if you are using a desktop or laptop computer.

How to Disable Sleep Mode on macOS 11 Desktops

The following instruction describe how to disable sleep mode on macOS 11 desktop computers.

6. Open System Preferences. The *System Preferences* window opens.

Figure 7. System Preferences > Energy Saver



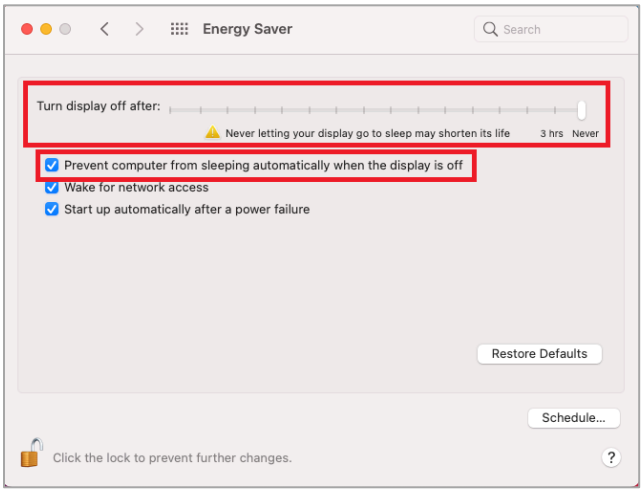
7. Open **Energy Saver** settings. The ***Energy Saver*** setting window opens.

8. If the padlock in the lower left corner is locked, click it and authenticate with administrator settings.

9. Drag the ***Turn display off after*** slider to **Never**.

10. If the ***Prevent computer from sleeping automatically when the display if off*** checkbox is cleared, mark it.

Figure 8. macOS 11 Energy Saver Settings

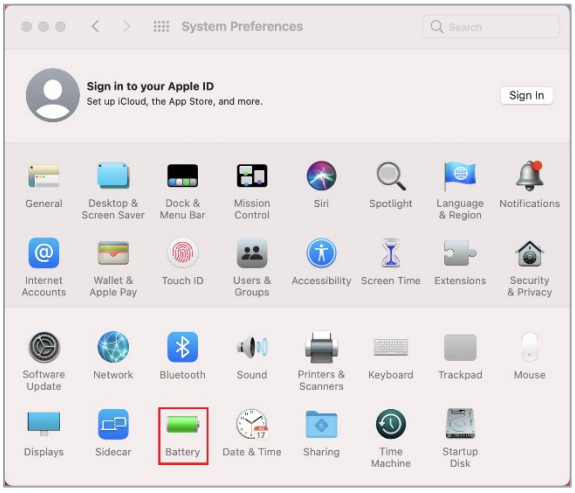


How to Disable Sleep Mode on macOS 11 Laptops

The following instruction describe how to disable sleep mode on macOS 11 laptops computers.

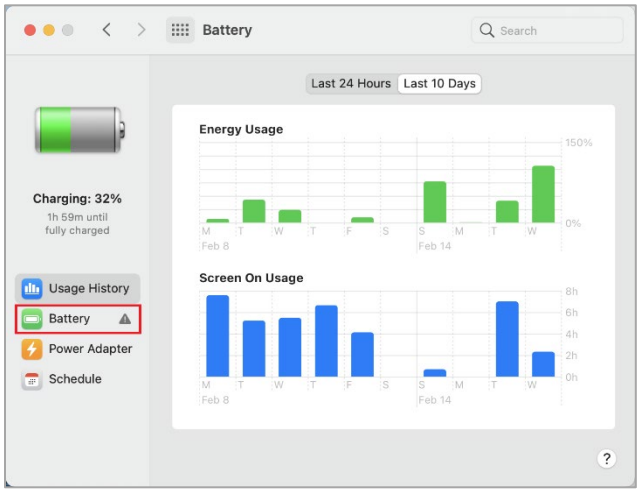
11. Open System Preferences. The *System Preferences* window opens.

Figure 9. System Preferences > Battery



12. Open **Battery** settings. The ***Battery*** setting window opens, displaying the ***Usage History*** tab.

Figure 10. Battery Settings – Usage History Tab

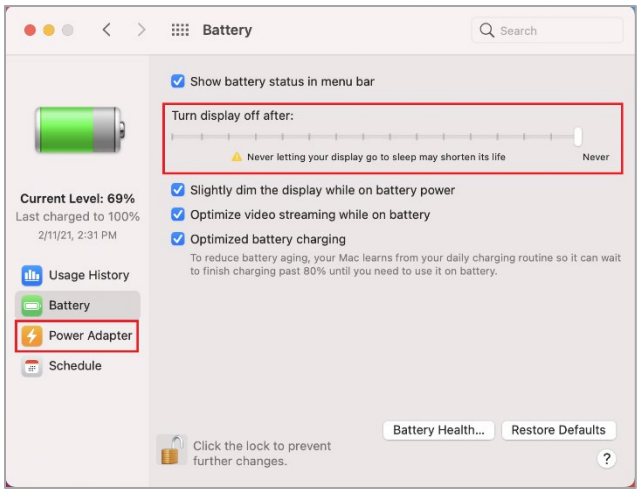


13. Select the **Battery** settings tab. The ***Battery*** settings tab opens.

14. If the padlock in the lower left corner is locked, click it and authenticate with administrator settings.

15. Drag the ***Turn display off after*** slider to **Never**.

Figure 11. Battery Settings – Battery Tab



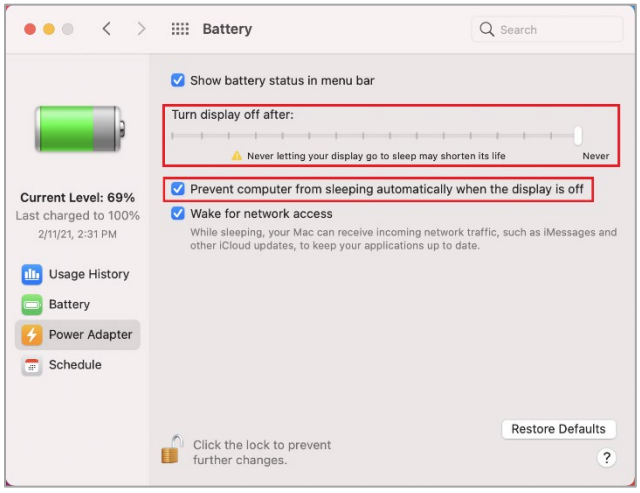
16. Open **Power Adapter** settings tab. The ***Power Adapter*** settings tab window opens.

17. If the padlock in the lower left corner is locked, click it and authenticate with administrator settings.

18. Drag the ***Turn display off after*** slider to **Never**.

19. If the ***Prevent computer from sleeping automatically when the display if off*** checkbox is cleared, mark it.

Figure 12. Battery Settings – Power Adapter Tab



How to Install Rosetta 2

If you are running the Secure Browser on Apple silicon devices, you must first install Rosetta 2.

Rosetta 2 may already be installed on your Apple silicon device if you needed it to run another Intel-based application. If it not already installed, a prompt to install it will appear the first time you launch the Secure Browser.

Rosetta 2 can also be deployed to multiple devices at once through scripting or mobile device management (MDM).

For more information about Rosetta 2, including instructions to install it, please see https://support.apple.com/en-us/HT211861.

How to Troubleshoot Mac Workstations

This section contains troubleshooting tips for Mac.

How to Reset Secure Browser Profiles on Mac

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

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

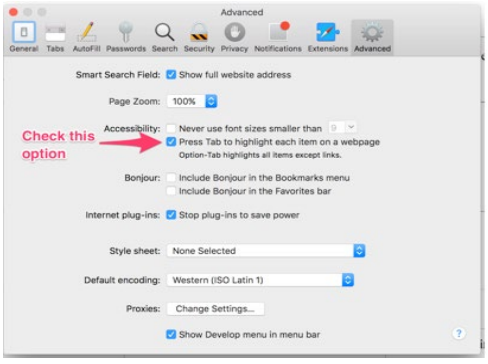
How to Navigate to Tool Menu with the Keyboard Using a Safari Browser

Students can use any supported public browser for the Released Item Repository (RIR), and navigate to the Tool menu using standard methods, with the exception of Safari. To access the Tool menu using Safari, enable the "Press tab to highlight each item on a webpage" option in Safari Preferences, as shown below.

NOTE: Students who have the text-to-speech (TTS) accommodation enabled for the RIR will need to use the Secure Browser.

1. Open Safari, and from the Safari menu, click **Preferences**.
2. Click Advanced.
3. Mark the checkbox Press tab to highlight each item on a webpage.

Figure 8. Advanced Safari Preferences



How to Disable Text-to-Speech Keyboard Shortcut

A feature in macOS 10.12 and later allows users to have any text on the screen read aloud by selecting the text and hitting a preset key or set of keys on the keyboard. By default, this feature is disabled and must remain disabled so as not to compromise test security. This section describes how to toggle this feature.

1. From the Apple menu, select **System Preferences**.
2. Select Accessibility.
3. Select **Speech**.
4. To enable this feature, check the **Speak selected text when the key is pressed** checkbox. To disable, deselect the checkbox.

Appendix. Change Log

Changes to this guide after August 2, 2019 are noted.

Section	Description of Change
How to Configure Mac Workstations for Online Testing	Added information on disabling keyboard shortcuts for screenshots on Mac OS.
How to Configure Mac Workstations for Online Testing	Added updated guidance on Mac Secure Profile.
Throughout	CAI replaced a reference to AIR within text, URLs, or email address.
How to Download and Install the Mac Secure Profile	Added Voice Control to the list of features disabled by the Secure Profile and added note describing updates to the Secure Profile for 2020-2021.
How to Configure Networks for Online Testing	Changed all references of “whitelist” to “allowlist” or “add to your allowlist”.
Configurations, Troubleshooting, and Advanced Secure Browser Installation for Windows – Table 2	Added note: For 2020-2021, users should add both Cambium and AIR URLs listed to their allowlist.
How to Configure Networks for Online Testing	Removed next section “Configuring for Certificate Revocations”. Our Secure Browser no longer uses the Online Certificate Status Protocol to check certificates. We now validate our certificates in our custom code.
How to Install the Mac Secure Profile	2020-2021 update – revised language throughout section.
How to Configure Mac Workstations for Online Testing	Removed sections *How to Disable Siri.* The secure browser now handles this configuration.
How to Configure Mac Workstations for Online Testing	Removed section *How to Disable Keyboard Shortcuts for Screenshots*. Secure browser has been updated to handle this.
How to Download and Install the Mac Secure Profile	Added features added to Profile for Spring 2021.
How to Download and Install the Mac Secure Profile	Added the following sentence: If you need assistance, including reapplying settings to multiple devices at once, contact the Helpdesk.

How to Disable Updates to Third-Party Apps	Updated instructions and screenshots throughout topic. Old instructions and screenshots were from OS X 10.9.
How to Disable Updates to iTunes	Removed topic. This configuration is no longer necessary.
How to Disable Fast User Switching	Updated instructions and screenshots throughout topic. Old instructions and screenshots were outdated.
How to Disable Sleep Mode on macOS 11	Added new topic with subtopics How to Disable Sleep Mode on macOS 11 Desktops and How to Disable Sleep Mode on macOS 11 Laptops.
How to Install Rosetta 2	Added new topic.

Configurations, Troubleshooting, and Advanced Secure Browser Installation Guide for Chrome OS

For Technology Coordinators

2020-2021

Updated August 10, 2020

Prepared by Cambium Assessment, Inc.

Table of Contents

Configurations, Troubleshooting, and Advanced Secure Browser Installation for Chrome OS

This document contains configurations, troubleshooting, and advanced Secure Browser installation instructions for your network and Chrome OS workstations.

How to Configure Networks for Online Testing

This section contains additional configurations for your network.

Which Resources to Add to your Allowlist for Online Testing

This section presents information about the URLs that Cambium Assessment, Inc. (CAI) provides. Ensure your network's firewalls are open for these URLs. If your testing network includes devices that perform traffic shaping, packet prioritization, or Quality of Service, ensure these URLs have high priority.

Which URLs for Non-Testing Sites to Add to your Allowlist

Table 1 lists URLs for non-testing sites, such as Test Information Distribution Engine (TIDE) and Online Reporting System (ORS).

Table 1. CAI URLs for Non-Testing Sites

System	URL
Portal and Secure Browser installation files	https://indiana.portal.cambiumast.com/
Single Sign-On System	https://sso1.cambiumast.com/auth/realms/indiana/account
Test Information Distribution Engine	https://in.tide.cambiumast.com/
Online Reporting System	https://in.reports.cambiumast.com/

Which URLs for TA and Student Testing Sites to Add to your Allowlist

Testing servers and satellites may be added or modified during the school year to ensure an optimal testing experience. As a result, CAI strongly encourages you to add these URLs to your allowlist at the root level. This requires using a wildcard.

Table 2. CAI and AIR URLs for Testing Sites

System	URL
TA and Student Testing Sites Assessment Viewing Application For 2020-2021, users should add both CAI and AIR URLs listed in this table to their allowlist.	*.cambiumast.com *.tds.cambiumast.com *.cloud1.tds.cambiumast.com *.cloud2.tds.cambiumast.com *.airast.org *.tds.airast.org *.cloud1.tds.airast.org

	*.cloud2.tds.airast.org

Which URLs for Online Dictionary and Thesaurus to Add to your Allowlist

Some online assessments contain an embedded dictionary and thesaurus provided by Merriam-Webster. The Merriam-Webster URLs listed in Table 3 should be added to your allowlist to ensure that students can use them during testing.

Table 3. CAI URLs for Online Dictionaries and Thesauruses

Domain Name	IP Address
media.merriam-webster.com	64.124.231.250
www.dictionaryapi.com	64.124.231.250

Which Ports and Protocols are Required for Online Testing

Table 4 lists the ports and protocols used by the Test Delivery System (TDS). Ensure that all content filters, firewalls, and proxy servers are open accordingly.

Table 4. Ports and Protocols for Test Delivery System

Port/Protocol	Purpose
80/TCP	HTTP (initial connection only)
443/TCP	HTTPS (secure connection)

How to Configure Filtering Systems

If the school's filtering system has both internal and external filtering, the URLs for the testing sites (see Table 1) must be added to your allowlist in both filters. Please see your vendor's documentation for specific instructions. Also, be sure to add these URLs to your allowlist in any multilayer filtering system (such as local and global layers). Ensure all items that handle traffic to *.tds.cambiumast.com and *.tds.airast.org have the entire certificate chain and are using the latest TLS 1.2 protocol.

How to Configure for Domain Name Resolution

Table 1 and Table 2 list the domain names for CAI's testing and non-testing applications. Ensure the testing machines have access to a server that can resolve those names.

How to Install the Secure Browser for Chrome OS using Advanced Methods

This document contains additional installation instructions for installing the Secure Browser for Chrome OS.

Note: Chromebooks manufactured in 2017 or later must have an Enterprise or Education license to run in kiosk mode, which is necessary to run the Secure Browser.

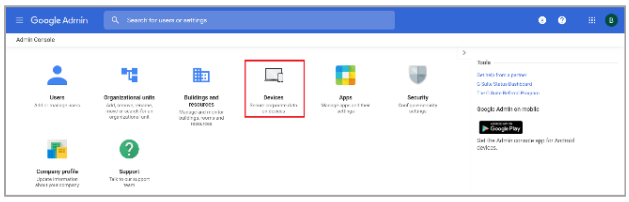
How to Install SecureTestBrowser (formerly AIRSecureTest) as a Kiosk App on Managed Chromebooks

These instructions are for installing the SecureTestBrowser (formerly AIRSecureTest) Secure Browser as a kiosk app on domain-managed Chromebook devices. The steps in this procedure assume that your Chromebooks are already managed through the admin console.

SecureTestBrowser is not compatible with public sessions.

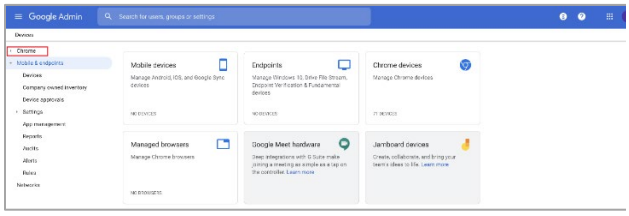
1. As the Chromebook administrator, log in to your admin console (https://admin.google.com)

Figure 1. Google Admin Console



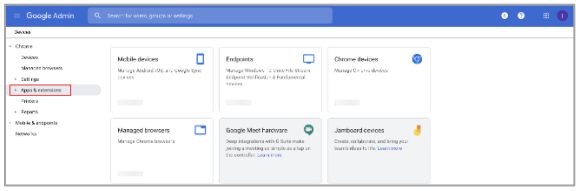
2. Click **Devices**. The ***Device*** page appears.

Figure 2. Device Page



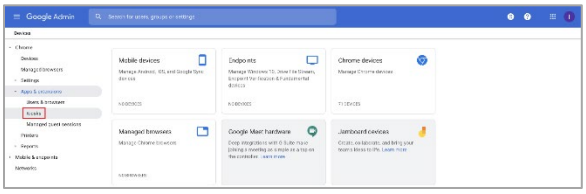
3. Select **Chrome**. The *Chrome* drop-down list appears.

Figure 3. Chrome Drop-down List



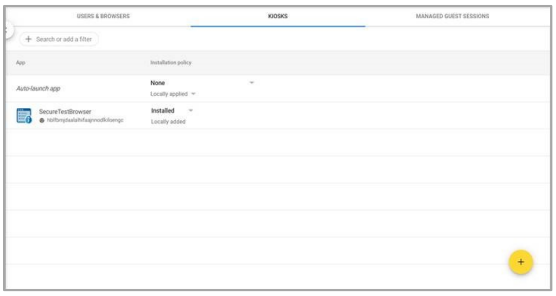
4. From the *Chrome* drop-down list, select **Apps & extensions**. The *Apps & extensions* drop-down list appears.

Figure 4. Apps & extensions Drop-down List



5. From the *Apps & extensions* drop-down list, select **Kiosks**. The *Apps & Extensions* page appears, displaying the *Kiosks* tab.

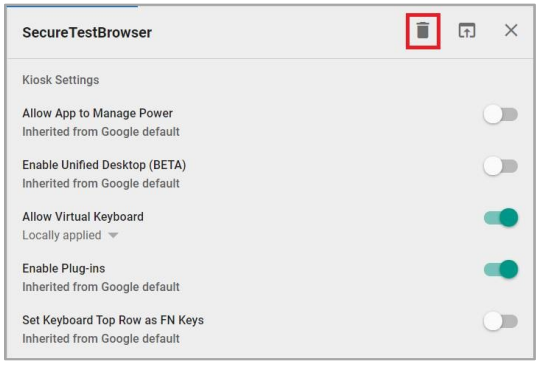
Figure 5. Apps & extensions page – Kiosks tab



6. Remove any previous versions of the apps that appear by selecting the app name to display the app settings and then selecting  . These may appear as SecureTestBrowser or AIRSecureTest.

7. Click X to close app settings.

Figure 6. App Settings



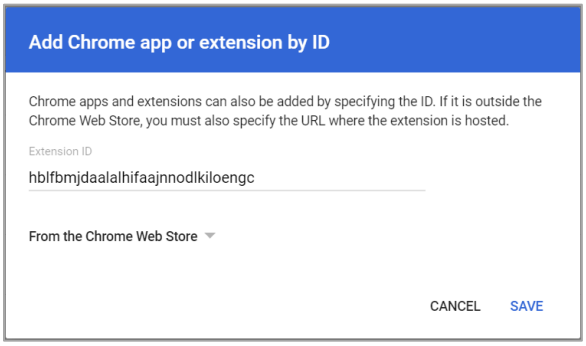
8. Hover over  to display options to add a new app.

9. Click  to add a Chrome app or extension by ID. The ***Add Chrome app or extension by ID*** window appears.

10. Enter hblfbmjdaalalhifaajnnodlkiloengc in the *Extension ID* field.

11. Ensure **From the Chrome Web Store** is selected from the drop-down list.

Figure 7. Add Chrome app or extension by ID



12. Click **Save**. The SecureTestBrowser app appears in the app list.

13. Ensure **Installed** is selected from the *Installation Policy* drop-down list.

The SecureTestBrowser app will be installed on all managed devices the next time each managed device is turned on.

How to Configure Chrome OS Workstations for Online Testing

This section contains additional configurations for Chrome OS.

How to Manage Chrome OS Auto-Updates

This section describes how to manage Chrome OS auto-updates. CAI recommends disabling Chrome OS auto-updates or limiting updates to a specific version used successfully before summative testing begins.

How to Disable Auto-Updates for Chrome OS

This section describes how to disable auto-updates for Chrome OS.

1. Display the Device Settings page by following the procedure in ***Manage device settings***, https://support.google.com/chrome/a/answer/1375678. The steps in that procedure assume that your Chromebooks are managed through the admin console.
2. From the *Auto Update* list, select **Stop auto-updates**.
3. Click **Save**.

How to Limit Chrome OS Updates to a Specific Version

This section describes how to limit Chrome OS updates to a specific version.

1. Display the Device Settings page by following the procedure in ***Manage device settings***, https://support.google.com/chrome/a/answer/1375678. The steps in that procedure assume that your Chromebooks are managed through the admin console.
2. From the *Auto Update* list, select **Allow auto-updates**.
3. From the *Restrict Google Chrome version to at most* list, select the required version.
4. Click **Save**.

Appendix. Change Log

Changes made after August 2, 2019 are noted.

Location	Description
Pgs. 6-8	Added updated steps for accessing the Secure Test (formerly AIRSecureTest) app through kiosk mode.
Throughout	CAI replaced a reference to AIR within text, URLs, or email address.
Throughout	Replaced whitelist with allowlist
How to Install the Secure Browser for Chrome OS Using Advanced Methods	2020-2021 Update – Updated to reflect both app names.
How to Install the Secure Browser for Chrome OS Using Advanced Methods	2020-2021 Update – Updates throughout to rebrand AIRSecureTest as SecureTestBrowser and to reflect changes to Google Admin Console user interface.
Configuring for Certificate Revocations	Removed section “Configuring for Certificate Revocations”

Configurations and Troubleshooting for Linux

For Technology Coordinators

2020-2021

Published July 14, 2020

Prepared by Cambium Assessment, Inc.

Table of Contents

Configurations and Troubleshooting for Linux

This document contains configurations and troubleshooting for your network and Linux workstations.

How to Configure Networks for Online Testing

This section contains additional configurations for your network.

Which Resources to Add to your Allowlist for Online Testing

This section presents information about the URLs that Cambium Assessment, Inc. (CAI) provides. Ensure your network's firewalls are open for these URLs. If your testing network includes devices that perform traffic shaping, packet prioritization, or Quality of Service, ensure these URLs have high priority.

Which URLs for Non-Testing Sites to Add to your Allowlist

Table 1 lists URLs for non-testing sites, such as Test Information Distribution Engine (TIDE) and Online Reporting System (ORS).

Table 1. CAI URLs for Non-Testing Sites

System	URL
Indiana Assessment Portal and Secure Browser installation files	https://indiana.portal.cambiumast.com
Single Sign-On System	https://sso1.cambiumast.com/auth/realms/indiana/account
Test Information Distribution Engine	https://in.tide.cambiumast.com/
Online Reporting System	https://in.reports.cambiumast.com/

Which URLs for TA and Student Testing Sites to Add to your Allowlist

Testing servers and satellites may be added or modified during the school year to ensure an optimal testing experience. As a result, CAI strongly encourages you to add these URLs to your allowlist at the root level. This requires using a wildcard.

Table 2. CAI and AIR URLs for Testing Sites

System	URL
TA and Student Testing Sites Assessment Viewing Application For 2020-2021, users should add both CAI and AIR URLs listed in this table to their allowlist.	*.cambiumast.com *.tds.cambiumast.com *.cloud1.tds.cambiumast.com *.cloud2.tds.cambiumast.com *.airast.org *.tds.airast.org *.cloud1.tds.airast.org *.cloud2.tds.airast.org

Which URLs for Online Dictionary and Thesaurus to Add to your Allowlist

Some online assessments contain an embedded dictionary and thesaurus provided by Merriam-Webster. The Merriam-Webster URLs listed in Table 3 should be added to your allowlist to ensure that students can use them during testing.

Table 3. CAI URLs for Online Dictionaries and Thesauruses

Domain Name	IP Address
media.merriam-webster.com	64.124.231.250
www.dictionaryapi.com	64.124.231.250

Which Ports and Protocols are Required for Online Testing

Table 4 lists the ports and protocols used by the Test Delivery System. Ensure that all content filters, firewalls, and proxy servers are open accordingly.

Table 4. Ports and Protocols for Test Delivery System

Port/Protocol	Purpose
80/TCP	HTTP (initial connection only)
443/TCP	HTTPS (secure connection)

How to Configure Filtering Systems

If the school's filtering system has both internal and external filtering, the URLs for the testing sites (see Table 1) must be added to your allowlist in both filters. Please see your vendor's documentation for specific instructions. Also, be sure to add these URLs to your allowlist in any multilayer filtering system (such as local and global layers).

How to Configure for Domain Name Resolution

Table 1 and Table 2 list the domain names for CAI's testing and non-testing applications. Ensure the testing machines have access to a server that can resolve those names.

How to Configure Network Settings for Online Testing

Local Area Network (LAN) settings on testing machines should be set to automatically detect network settings.

To set LAN settings to auto-detect on Linux machines:

1. Open **System Settings**.
2. Open **Network**.
3. Select **Network Proxy**.
4. From the **Method** dropdown, select **None**.

5. Click **X** to close **Network** window.

How to Configure the Secure Browser for Proxy Servers

By default, the Secure Browser attempts to detect the settings for your network's web proxy server. However, users of web proxies should execute a proxy command once from the command prompt. This command does not need to be added to the Secure Browser shortcut. Table 5 lists the form of the command for different settings and operating systems. To execute these commands from the command line, change to the directory containing the Secure Browser's executable file.

Note: Domain names in commands The commands in Table 5 use the domains foo.com and proxy.com. When configuring for a proxy server, use your actual testing domain names as listed in the section Which Resources Add to your Allowlist for Online Testing.

Table 5. Specifying proxy settings using the command line

Description	System	Command
Use the browser without any proxy	Linux	./IndianaSecureBrowser.sh -proxy 0 aHR0cHM6Ly9pbi50ZHMuY2FtYml1bWFzdC5jb20vc3R1ZGVudA==
Set the proxy for HTTP requests only	Linux	./IndianaSecureBrowser.sh -proxy 1:http:foo.com:80 aHR0cHM6Ly9pbi50ZHMuY2FtYml1bWFzdC5jb20vc3R1ZGVudA==
Set the proxy for all protocols to mimic the "Use this proxy server for all protocols" of Firefox	Linux	./IndianaSecureBrowser.sh -proxy 1:*:foo.com:80 aHR0cHM6Ly9pbi50ZHMuY2FtYml1bWFzdC5jb20vc3R1ZGVudA==
Specify the URL of the PAC file	Linux	./IndianaSecureBrowser.sh -proxy 2:proxy.com aHR0cHM6Ly9pbi50ZHMuY2FtYml1bWFzdC5jb20vc3R1ZGVudA==
Auto-detect proxy settings	Linux	./IndianaSecureBrowser.sh -proxy 4 aHR0cHM6Ly9pbi50ZHMuY2FtYml1bWFzdC5jb20vc3R1ZGVudA==
Use the system proxy setting (default)	Linux	./IndianaSecureBrowser.sh -proxy 5 aHR0cHM6Ly9pbi50ZHMuY2FtYml1bWFzdC5jb20vc3R1ZGVudA==

How to Uninstall the Secure Browser on Linux

This section contains instructions to uninstall the Secure Browser for Linux

How to Uninstall the Secure Browser on Linux

To uninstall a Secure Browser, delete the folder from the installation directory.

How to Configure Linux Workstations for Online Testing

This section contains additional configurations for Linux.

Which Libraries and Packages Are Required

The following libraries and packages are required to be installed on all 32-bit and 64-bit Linux workstations:

- GTK+ 2.18 or higher
- GLib 2.22 or higher
- Pango 1.14 or higher
- X.Org 1.0 or higher (1.7+ recommended)
- libstdc++ 4.3 or higher
- libreadline6:i386 (required for Ubuntu only)
- GNOME 2.16 or higher

The following libraries and packages are recommended to be installed on all 32-bit and 64-bit Linux workstations:

- NetworkManager 0.7 or higher
- DBus 1.0 or higher
- HAL 0.5.8 or higher

The following libraries and packages are required to be installed on all 64-bit Linux workstations:

- Sox
- Net-tools

How to Add Verdana Font

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

- Fedora—Follow the steps in the “How to Install” section of the following website: http://corefonts.sourceforge.net/.
- Ubuntu—In a terminal window, enter the following command to install the msttcorefonts package:
    - sudo apt-get install msttcorefonts

How to Disable the On-Screen Keyboard

Fedora and Ubuntu feature an on-screen keyboard that should be disabled before online testing. This section describes how to disable the on-screen keyboard.

To disable the on-screen keyboard:

1. Open **System Settings**.
2. Select **Universal Access**.
3. In the ***Typing*** section, toggle **Screen Keyboard** to **Off**.

How to Troubleshoot Linux Workstations

This section contains troubleshooting tips for Linux.

How to Reset Secure Browser Profiles on Linux

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

1. Log on as a superuser or 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 directories:

/home/username/.cai

3. /home/username/.cache/cai
4. where username is the user account where the Secure Browser is installed. (Keep the directories, just delete their contents.)
5. Restart the Secure Browser.

Appendix. Change Log

Changes made after August 2, 2019 are noted.

Location	Description of Change
Throughout	CAI replaced a reference to AIR within text, URLs, or email address.
How to Configure Networks for Online Testing	Changed all references of “whitelist” to “allowlist” or “add to your allowlist”.
How to Troubleshoot Linux Workstations	Updated AIR to CAI language.
How to Configure Networks for Online Testing	Removed section “*Configuring for Certificate Revocations.* CAI’s Secure Browser no longer uses the Online Certificate Status Protocol to check certificates. We now validate our certificates in our custom code.
How to Configure the Secure Browser for Proxy Servers	Corrected typo “IndianaSecureBrowserSecureBrowser.sh” to “IndianaSecureBrowser.sh”