Hawai'i Statewide Assessment Program

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

For Technology Coordinators

2019-2020

Published July 18, 2019

Updated June 10, 2020

Prepared by Cambium Assessment, Inc.

Cambium Assessment

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 Whitelist for Online Testing

This section presents information about the URLs that 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 Whitelist

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

Table 1. CAI URLs for Non-Testing Sites

System	URL
Portal and Secure Browser installation files	https://alohahsap.org/
Single Sign-On System	https://sso1.cambiumast.com/auth/realms/hawaii/account
Test Information Distribution Engine	https://www.hitide.org/
Online Reporting System	hsa.reports.cambiumast.com
Centralized Reporting System	hi.reporting.cambiumast.com

Which URLs for TA and Student Testing Sites to Whitelist

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 whitelist 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	*.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 Whitelist

Some online assessments contain an embedded dictionary and thesaurus provided by Merriam-Webster. The Merriam-Webster URLs listed in Table 3 should be whitelisted 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 whitelisted in both filters. Ensure your filtering system is not configured to perform packet inspection on traffic to CAI servers. Please see your vendor's documentation for specific instructions. Also, be sure to whitelist these URLs 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 Configure for Certificate Revocations

CAI's servers present certificates to the clients. The following section discusses the methods used to check those certificates for revocation.

How to Use the Online Certificate Status Protocol

To use the Online Certificate Status Protocol (OCSP), ensure your firewalls allow the domain names listed in Table 5. The values in the Patterned column are preferred because they are more robust.

Table 5. Domain Names for OCSP

Patterned	Fully Qualified
*.thawte.com	ocsp.thawte.com
*.geotrust.com	ocsp.geotrust.com
*.ws.symantec.com	ocsp.ws.symantec.com

If your firewall is configured to check only IP addresses, do the following:

1. Get the current list of OCSP IP addresses from Symantec. The list is available at https://www.symantec.com/content/en/us/enterprise/other_resources/OCSP_Upgrade_-_New_IP_Addresses.txt.
2. Add the retrieved IP addresses to your firewall's whitelist. Do not replace any existing IP addresses.

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 6 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 6 use the domain proxy.com. When configuring for a proxy server, use your actual proxy server hostname.

Table 6. Specifying proxy settings using the command line

Description	System	Command
Use the browser without any proxy	Windows	`HISecureBrowser.exe -proxy 0 aHR0cHM6Ly9oc2EudGRzLmNhbWJpdW1hc3QuY29tL3N0dWRlbnQ=`
Set the proxy for HTTP requests only	Windows	`HISecureBrowser.exe -proxy 1:http:proxy.com:8080 aHR0cHM6Ly9oc2EudGRzLmNhbWJpdW1hc3QuY29tL3N0dWRlbnQ=`
Set the proxy for all protocols to mimic the "Use this proxy server for all protocols" of Firefox	Windows	`HISecureBrowser.exe -proxy 1:*:proxy.com:8080 aHR0cHM6Ly9oc2EudGRzLmNhbWJpdW1hc3QuY29tL3N0dWRlbnQ=`
Specify the URL of the PAC file	Windows	`HISecureBrowser.exe -proxy 2:proxy.com aHR0cHM6Ly9oc2EudGRzLmNhbWJpdW1hc3QuY29tL3N0dWRlbnQ=`
Auto-detect proxy settings	Windows	`HISecureBrowser.exe -proxy 4 aHR0cHM6Ly9oc2EudGRzLmNhbWJpdW1hc3QuY29tL3N0dWRlbnQ=`
Use the system proxy setting (default)	Windows	`HISecureBrowser.exe -proxy 5 aHR0cHM6Ly9oc2EudGRzLmNhbWJpdW1hc3QuY29tL3N0dWRlbnQ=`

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 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 Hawaii Statewide Assessment Program portal at alohahsap.org. 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):
    a. If presented with a choice to **Run** or **Save** the file, click **Save**, and save the file to a convenient location.
    b. If presented only with the option to **Save**, save the file to a convenient location.

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

4. Open a command prompt as the administrator by doing the following:
    a. Click **Start**, and locate the Command Prompt application. (In some versions of Windows the application is under **All Programs > Accessories > Command Prompt**.)
    b. Right-click **Command Prompt**, and select **Run as Administrator**.
    c. As necessary, type the administrator password for the computer. The command prompt opens.

    (You need to do step 4 only once for the current login. The next time you open the command prompt, Windows retains the administrator role.)

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

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

   `<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.

   `/I` Perform an install.

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

   For example, the command

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

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

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

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

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

   b. A shortcut `HISecureBrowser` to the desktop.

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

9. Run the browser by double-clicking the `HISecureBrowser` 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.

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 your portal. Note the path of the installation directory, such as `C:\Program Files (x86)\HISecureBrowser`.

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\HISecureBrowser`.

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

   d. Run the browser by double-clicking the HISecureBrowser 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.

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 your portal.

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

   ```
   "C:\Program Files (x86)\HISecureBrowser\
   HISecureBrowser.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 How to Create Group Policy Objects.

6. On each NComputing console, create a new HISecureBrowser 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)\HISecureBrowser\`.
   e. Right-click the file HISecureBrowser.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)\HISecureBrowser\HISecureBrowser.exe" -P %SESSIONNAME%
      ```

      If you used a different installation path on the Windows server, use that in the above command.
   h. Click **OK** to close the Properties dialog box.
7. Verify the installation by double-clicking the shortcut to start the Secure Browser.

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 your portal. Note the path of the installation directory.
2. Copy and paste the line below into Notepad (no line breaks):

   ```
   "C:\Program Files (x86)\HISecureBrowser\HISecureBrowser" -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 How to Create Group Policy Objects.

5. On each client, create a new HISecureBrowser 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)\HISecureBrowser\`.
   d. Right-click the file HISecureBrowser.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)\HISecureBrowser\HISecureBrowser.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.

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)\HISecureBrowser`) 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 HISecureBrowser.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 HISecureBrowser 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

   `<Source>` Path to the executable file, such as `C:\MSI\HISecureBrowser.exe`.

   `/X` Perform an uninstall.

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

For example, the command

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

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 your portal for details.

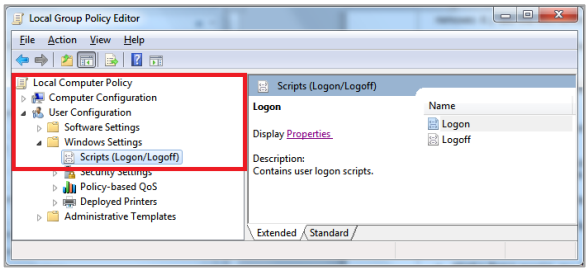
How to Create Group Policy Objects

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.

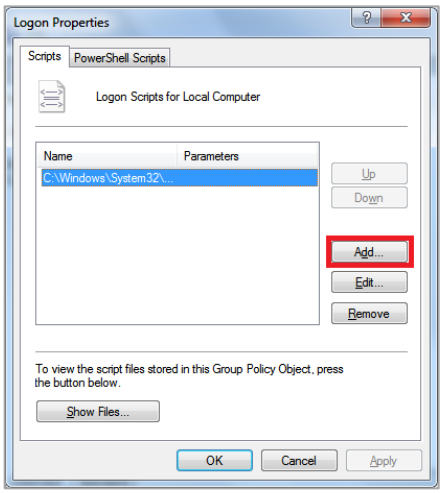
Figure 1. Local Group Policy Editor



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

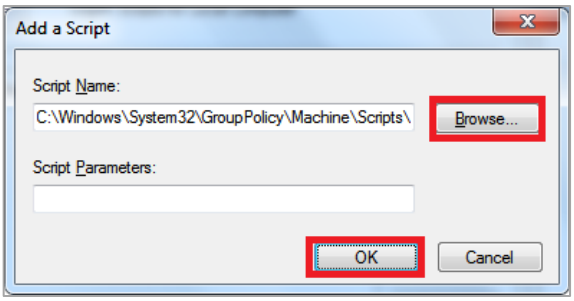
3. Select **Logon** and click **Properties**. The ***Logon Properties*** dialog box appears.

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 7, 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 7

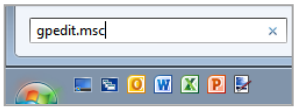
This section describes how to disable Fast User Switching in Windows 7. The process is similar for later versions of Windows.

Option A: Access the Group Policy Editor

The following procedure describes how to disable Fast User Switching using the Group Policy Editor. You can also configure Fast User Switching through the registry. See Option B below for instructions.

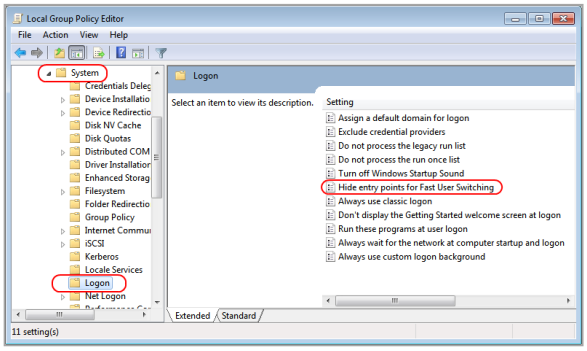
1. Click **Start**, type `gpedit.msc` in the search box. The Local Group Policy Editor window appears.

Figure 4. Start Menu Search Box



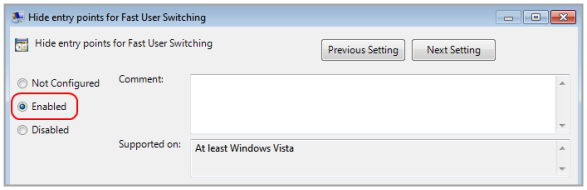
2. Navigate to Local Computer Policy > Computer Configuration > Administrative Templates > System > Logon.
3. Double-click **Hide entry points for Fast User Switching**.

Figure 5. Local Group Policy Editor



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

Figure 6. Hide entry points for Fast User Switching



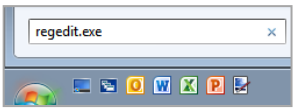
5. Close the Local Group Policy Editor window.

Option B: Access the Registry

The following procedure describes how to disable Fast User Switching using the Windows registry.

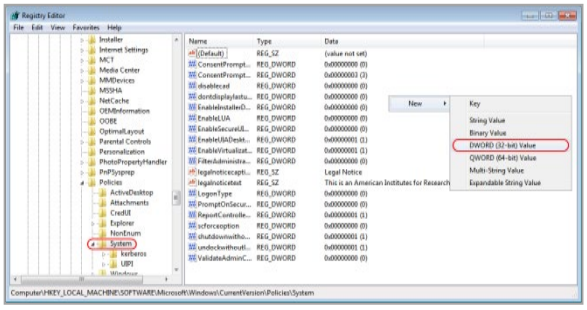
1. Click **Start**, type `regedit.exe` in the **Start Search** dialog box, and press **Enter**.

Figure 7. Start Menu Search Box



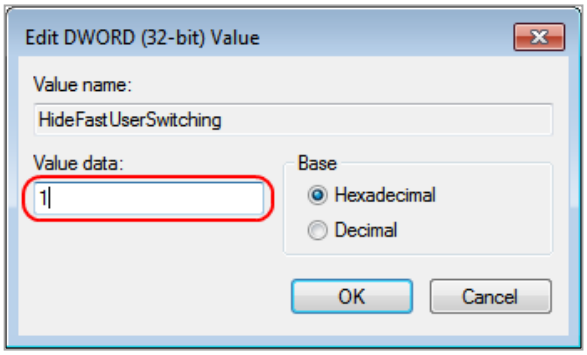
2. Navigate to HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Windows > CurrentVersion > Policies > System.
3. Right-click the **System** folder.
4. Click **New, DWORD (32-bit) value**.
5. Type **HideFastUserSwitching** and press **Enter**.

Figure 8. Registry Editor



6. Double-click the **HideFastUserSwitching** value.
7. In the **Value data** field, enter 1.
8. Click **OK**.

Figure 9. Edit DWORD (32-bit) Value



9. Close the Registry Editor.

How to Disable Fast User Switching in Windows 8 and 8.1

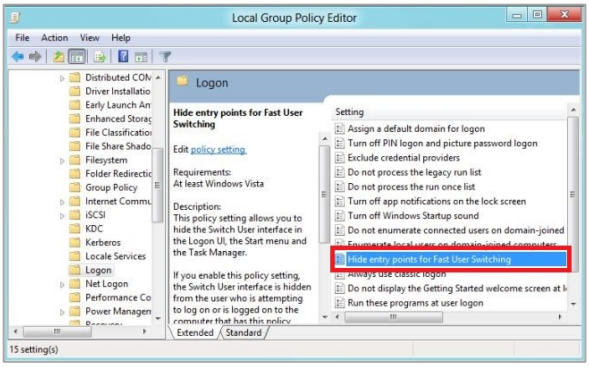
The following procedure describes how to disable Fast User Switching under Windows 8 and 8.1.

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 10. Search Charm

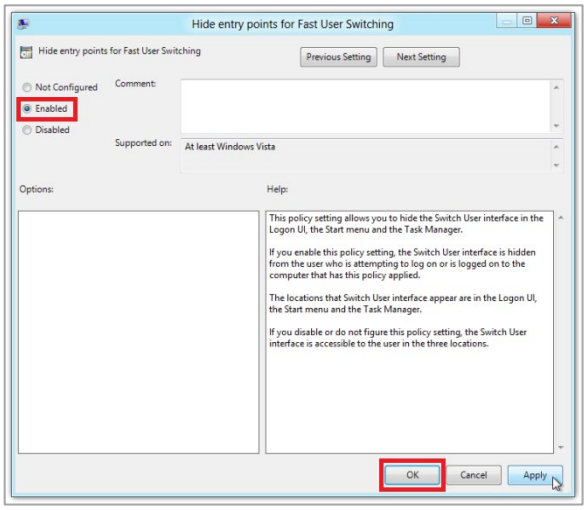
2. Navigate to Computer Configuration > Administrative Templates > System > Logon.
3. In the Setting pane, double-click **Hide entry points for Fast User Switching**.

Figure 11. Local Group Policy Editor



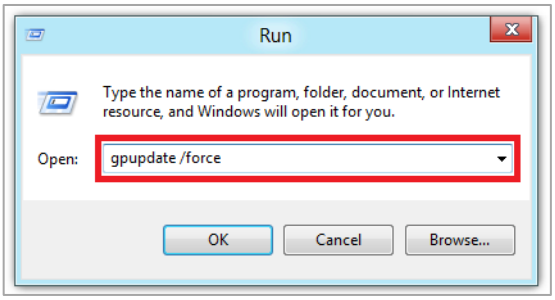
4. Select **Enabled** and then click **OK**.

Figure 12. Hide entry points for Fast User Switching



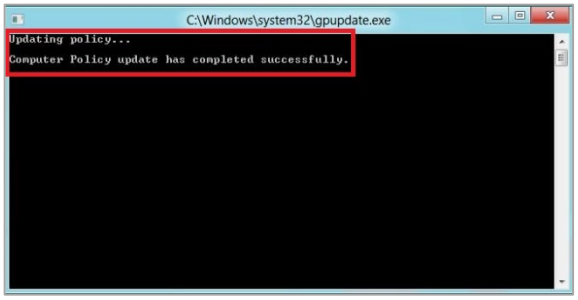
5. In the Search charm, type **run**. The ***Run*** dialog box opens.
6. Enter the command `gpupdate /force` into the text box and then click **OK**. (Note the space before the forward slash.)

Figure 13. 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 14. 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:

   `C:\Users\username\AppData\Local\AIR\`

   `C:\Users\username\AppData\Roaming\AIR\`

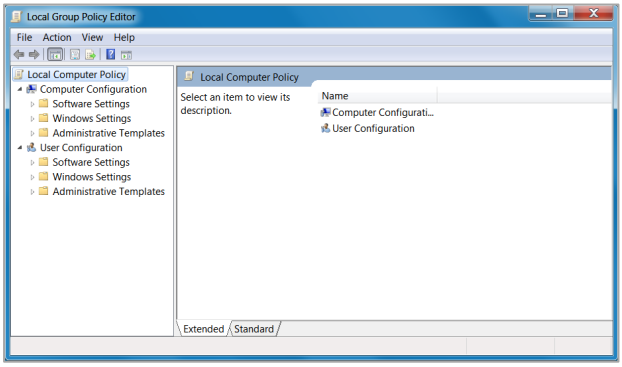
   where username is the Windows user account where the Secure Browser is installed. (Keep the AIR\ folders, just delete their contents.)
3. Start the Secure Browser.

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:

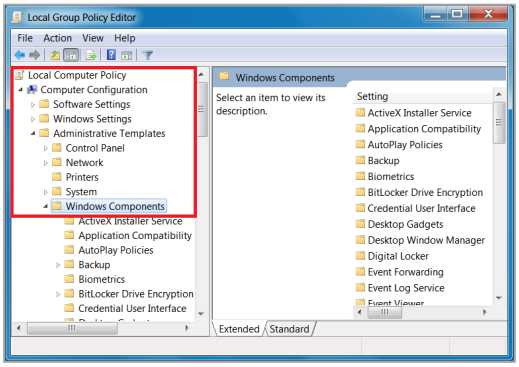
1. Type `gpedit.msc` in the *Search* box on the **Start** menu. The ***Local Group Policy Editor*** window appears.

Figure 15. Local Group Policy Editor



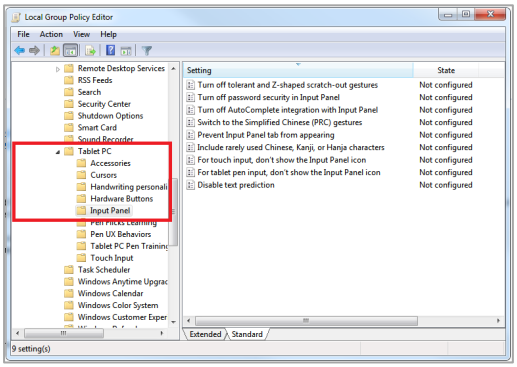
2. Navigate to **Computer Configuration\Administrator Templates\Windows Components.**

Figure 16. Windows Components



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

Figure 17. Input Panel



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

   a. Turn off AutoComplete integration with Input Panel

   b. Prevent Input Panel tab from appearing

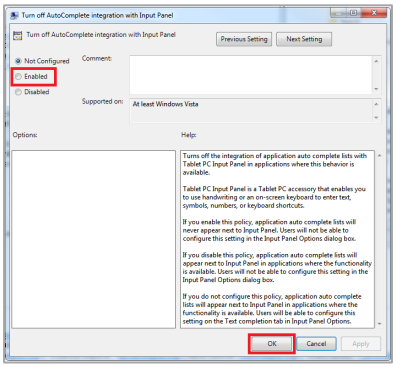
   c. For tablet pen input, don't show the Input Panel icon

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

   e. Disable text prediction

5. 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 18. Turn off AutoComplete integration with Input Panel



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

7. 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:

   Go to `C:\Program Files (x86)\ZoomText 10.1\` (Windows 64-bit)

   Go to `C:\Program Files\ZoomText 10.1\` (Windows 32-bit).
3. In a text editor, open the file ZoomTextConfig.xml.
4. Search for line containing the D2DPatch property, similar to the following:

   <Property name="D2DPatch" value ="*,~dwm,~firefox,~thunderbird"/>
5. In the value attribute, add the prefix for your state's Secure Browser:

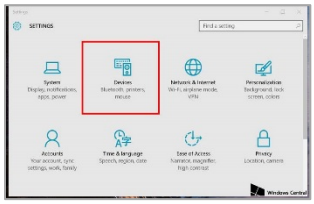
   <Property name="D2DPatch" value ="*,~dwm,~firefox,~ HIsecurebrowser,~thunderbird"/>
6. Save the file, and restart ZoomText.

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.

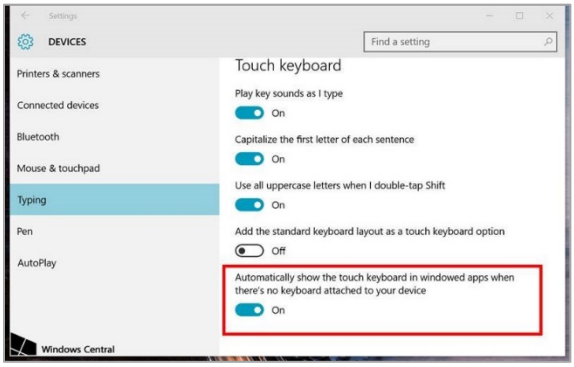
1. Go to **Settings** (keyboard shortcut: **Windows + I**)

Figure 19. 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 20. Typing

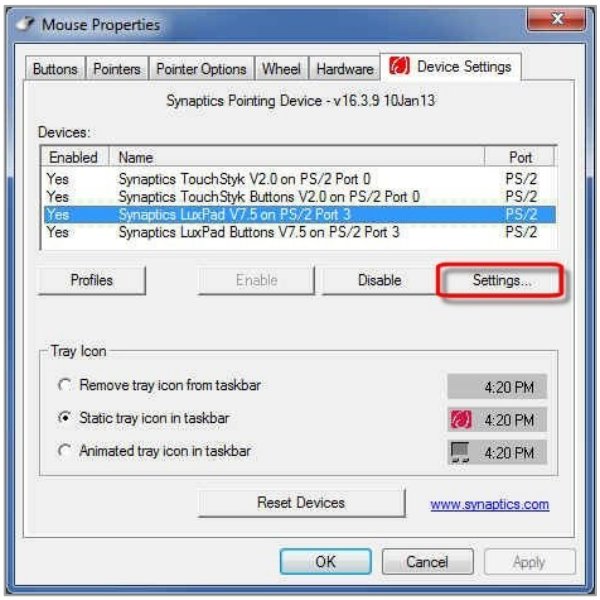


How to Disable Two-finger Scrolling in HP Notebooks with Synaptics TouchPad

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.

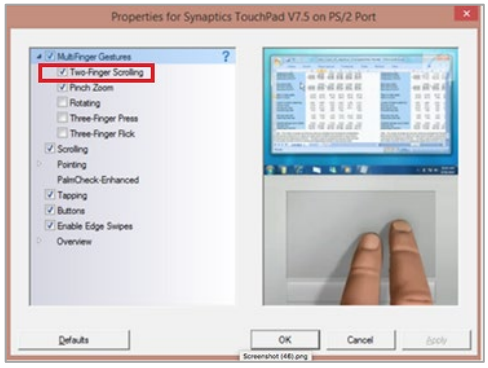
1. Click the **Start** menu (), and then type mouse in the search field.
2. Select **Mouse** from the list of options.
3. Click the **Device Settings** tab.
4. From the **Devices** list, select **Synaptics LuxPad V7.5**, and then click **Settings...**.

Figure 21. Mouse Properties



5. Uncheck **Two-Finger Scrolling**.

Figure 22. 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.

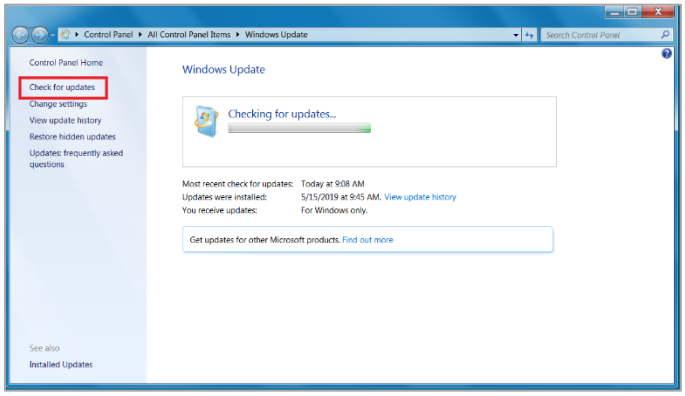
1. Open the **Start Menu**.
2. Open the **Control Panel**.
3. Select **Sound**. The **Sound** window will open.
4. Select the **Communications** tab.
5. By default, the option to “Reduce the volume of other sounds by 80%” is selected. Change this to **Do nothing**.
6. Select **OK**.

How to Run NVDA Screen Reader 2018.1.1 with Take a Test App

Users running the Take a Test app and NVDA screen reader version 2018.1.1 at the same time on Windows 10 and 10 in S Mode with RS v1709 and v1803 are experiencing the Take a Test app crashing before a test is started. To keep the Take a Test app from crashing while running the NVDA screen reader 2018.1.1, you should update Windows 10 and 10 in S Mode to at least RS v1809. Windows Updates can be accessed through the Control Panel.

1. Open the **Start Menu.**
2. Type **Windows Update** in the search charm and hit enter. The ***Windows Update*** window appears.
3. Select **Check for Updates**.
4. Select **Install Updates** to install all available updates.

Figure 23. Windows Update



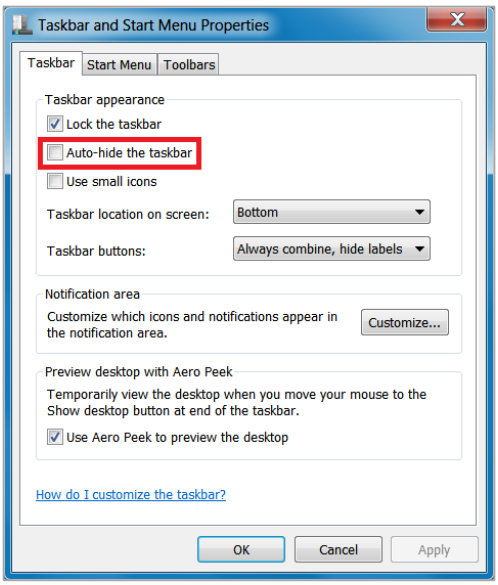
How to View the Windows Taskbar in Permissive Mode

In Permissive Mode, the Windows taskbar should appear when a user hovers their mouse pointer near the bottom of the screen. In Windows 7 SP1, 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 7 SP1, 8, and 8.1

1. Right-click on the taskbar.
2. Click **Properties**. The ***Taskbar and Start Menu Properties*** window appears. (See Figure 24.)
3. Uncheck the **Auto-hide the taskbar** checkbox.
4. Click **OK**.

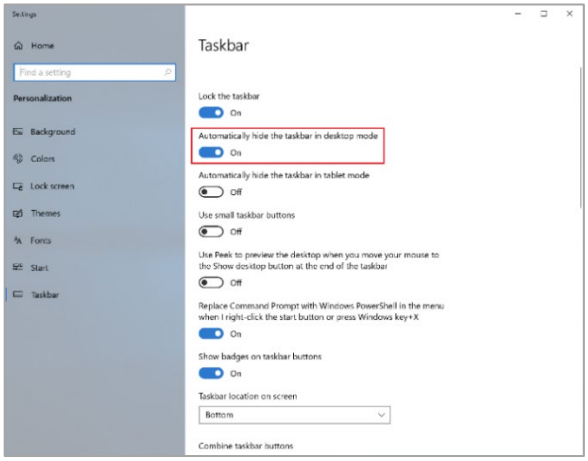
Figure 24. Taskbar and Start Menu Properties



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 25.)
3. Toggle **Automatically hide the taskbar in desktop mode** to **Off**.
4. Close the ***Taskbar*** window.

Figure 25. Taskbar



User Support

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

The Help Desk will be open Monday–Friday from 7:30 a.m. to 4:00 p.m. Hawaiian Standard Time (except holidays).

Hawaii Statewide Assessment Program Help Desk

Toll-Free Phone Support: 1-866-648-3712

Email Support:
hsaphelpdesk@cambiumassessment.com

If you contact the Help Desk, you will be asked to provide as much detail as possible about the issues you encountered. You may choose to use the *Help Desk Intake Form*, available on the https://alohahsap.org/ portal website in the **Resources >> Technology** section.

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

Change Log

This Change Log can be used to identify specific changes that are made to any of the information included in the original document throughout the current school year.

Change	Section	Date
Changed "oscp" to "ocsp" in the Fully Qualified column of Table 5.	Table 5. Domain Names for OCSP	9/25/19
Updated the note and some of the proxy commands.	How to Configure the Secure Browser for Proxy Servers	11/16/19
Updated information throughout the paragraph.	How to Configure Filtering Systems	11/27/19
Changed all references to “American Institutes for Research” and “AIR” to “Cambium Assessment, Inc.” and “CAI” respectively.	Global	6/10/20