Florida
Statewide Assessments

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

2021–2022

Updated 2/1/22

FSA
ELA & Mathematics
Assessments

NGSSS
Science & Social Studies
Assessments

Table of Contents

Configurations, Troubleshooting, and Secure Browser Installation for Windows

This document contains instructions for installing the Secure Browser, as well as configurations, troubleshooting, and advanced Secure Browser installation instructions for your network and Windows devices.

Secure Browser Installation Instructions

Below you will find the installation instructions for the Windows Secure Browser as well as steps to set up Microsoft's Take a Test app for Windows.

Installing Secure Browser for Windows

This procedure installs Secure Browser on all supported versions of Windows.

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

2. Download the Secure Browser on the Windows tab on the Secure Browsers page. A dialog window opens.

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

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

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

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

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

    - The secure browser to the default location `C:\Program Files\FLSecureBrowser`

    - A shortcut **FLSecureBrowser** to the desktop.

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

7. *Optional*: Apply proxy settings, if needed. For more information about proxy settings consult the *Technology Setup for Online Testing* document.

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

9. Run the browser by double-clicking the **FLSecureBrowser** 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 **X** in the upper-right corner of the screen.

Setting up Microsoft's Take a Test app for Windows 10

Windows 10 and 10 in S Mode come with Microsoft's Take a Test app, which enforces a locked-down, secure testing environment identical to CAI's Secure Browser. Users of the Take a Test app do not need to install the Secure Browser on the testing machine. For more information about configuring Take a Test, see https://docs.microsoft.com/en-us/education/windows/take-tests-in-windows-10.

For more information on installing Take a Test on multiple computers, see https://docs.microsoft.com/en-us/education/windows/take-a-test-multiple-pcs.

Creating a Dedicated Account for Take a Test

To set up Take a Test on an individual computer, you will need to create a dedicated local test account. This method should be used for non-permissive mode users only, as permissive mode features will not be accessible in a dedicated test account.

Note: Assessments administered through the Take a Test app will detect some forbidden apps are running in the background even if users don't start these apps, which causes the Take a Test app to log a user out of their account. (For more information, see https://support.microsoft.com/en-us/help/4338725/k-12-assessment-unexpected-reports-apps-running-background-windows-10.) Because of this, CAI has disabled the forbidden app check when using the Take a Test app through a dedicated test account.

To create a dedicated test account:

1. Sign into the device with an administrator account.

2. Go to **Settings** > **Accounts** > **Family & other people** > **Add someone else to this PC** > **I don't have this person's sign-in information** > **Add a user without a Microsoft account**. Fill out the fields and close out of the window.

3. Go to **Settings** > **Accounts** > **Access work or school** > **Set up an account for taking tests**.

4. Select the local account that you created in step 2. This account will be used as the dedicated testing account.

5. In the *Enter the test's web address* field, enter https://fl.tds.cambiumast.com/student/

6. Click **Save**.

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

Additional Instructions for Installing the Secure Browser for Windows

This section 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 to 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.**

Installing the Secure Browser via the Command Line

In this scenario, a user with administrator rights installs the Secure Browser from the command line. If you do not have administrator rights, refer to the section Installing the Secure Browser Without Administrator Rights.

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

Previously installed versions of the Secure Browser must be manually uninstalled before installing the current version.

1. Navigate to the Secure Browsers page of the Florida Statewide Assessments Portal. 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):

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

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

3. Note the full path and filename of the downloaded file, such as `c:\temp\XXSecureBrowser-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\FLSecureBrowser-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\FLSecureBrowserWin.msi /quiet
   INSTALLDIR=C:\AssessmentTesting\BrowserInstallDirectory
   ```

   installs the Secure Browser from the installation package at `C:\temp\XXSecureBrowser-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\FLSecureBrowser\`

   b. A shortcut `FLSecureBrowser` 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 `FLSecureBrowser` 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 **X** in the upper-right corner of the screen.

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.**

Copying the Secure Browser Installation Directory to Testing Computers

In this scenario, a network administrator installs the Secure Browser on one machine and copies the entire installation directory to testing computers.

1. On the computer from where you will copy the installation directory, install the Secure Browser following the directions on your portal. Note the path of the installation directory, such as:

   `C:\Program Files\FLSecureBrowser`.

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\FLSecureBrowser`

   c. Copy the shortcut

```
C:\AssesssmentTesting\FLSecureBrowser\FLSecureBrowser.exe -
Shortcut.lnk
```

to the desktop.

d. Run the browser by double-clicking the `FLSecureBrowser`  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 **X** in the upper-right corner of the screen.

Installing the Secure Browser for Use with an NComputing Terminal

In this scenario, a network administrator installs the Secure Browser on a Windows server accessed through an NComputing terminal. Prior to testing day, the testing coordinator connects consoles to the NComputing terminal, logs in from each to the Windows server, and starts the Secure Browser so that it is ready for the students.

This procedure assumes that you already have a working NComputing topology with consoles able to reach the Windows server.

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

2. Install the Secure Browser following the directions on the Secure Browser page on the portal.

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

```
"C:\Program Files\FLSecureBrowser\FLSecureBrowser.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 Creating Group Policy Objects.

6. On each NComputing console, create a new `FLSecureBrowser`  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 the path listed below:

```
C:\Program Files\FLSecureBrowser\.
```

e. Right-click the file

```
FLSecureBrowser.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\FLSecureBrowser\FLSecureBrowser.exe" -P %SESSIONNAME%
```

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

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

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

Installing the Secure Browser 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\FLSecureBrowser
```

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

```
FLSecureBrowser.exe
```

and select **Send To > Desktop (create shortcut)**.

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

6. Double-click the desktop shortcut  to run the Secure Browser.

Uninstalling the Secure Browser on Windows

The following sections describe how to uninstall the Secure Browser from Windows or from the command line. Previously installed versions of the Secure Browser must be manually uninstalled before installing the current version.

Uninstalling via the User Interface

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

1. Navigate to **Settings** > **System** > **Apps & features** (Windows 10) or **Control Panel** > **Add or Remove Programs** or **Uninstall a Program** (previous versions of Windows).

2. Select the Secure Browser program `FLSecureBrowser` and click **Remove** or **Uninstall**.

3. Follow the instructions in the uninstall wizard.

Uninstalling via the Command Line

1. Open a command prompt.

2. Run the command `msiexec /X <Source> /quiet`

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

   `/X` Perform an uninstall.

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

For example, the command

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

uninstalls the Secure Browser installed at

```
C:\AssessmentTesting\
```

using quiet mode.

Installing the Secure Browser on Windows Tablet Devices

The procedure for installing the Secure Browser on Windows tablet devices is the same for installing it on desktops. See above for details.

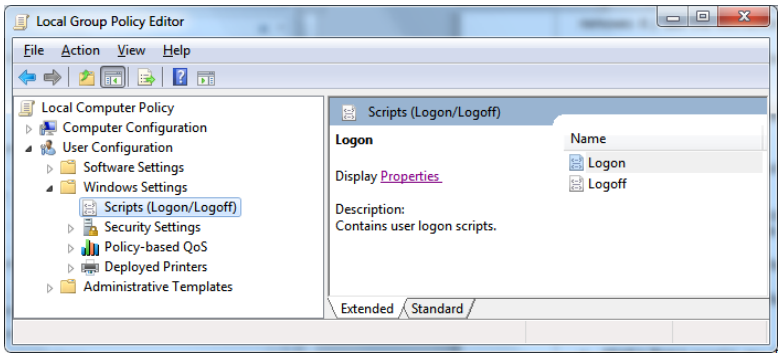
Creating Group Policy Objects

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 the file:

```
logon.bat
```

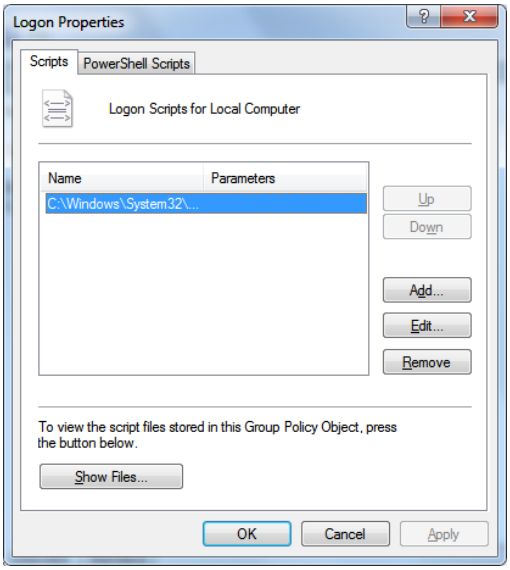
For additional information about creating group policy objects, see https://technet.microsoft.com/en-us/library/cc754740(v=ws.11).aspx.

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

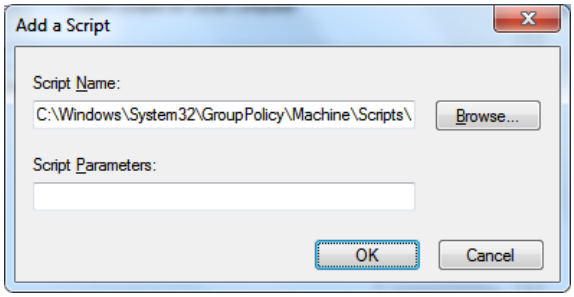


2. Expand **Local Computer Policy** > **User Configuration** > **Windows Settings** > **Scripts (Logon/Logoff)**.

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



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



5. Click **Browse…** and navigate to the `logon.bat` you want to run.
6. Click **OK**. You return to the **Logon Properties** dialog box.
7. Click **OK**. You return to the Local Group Policy Editor.
8. Close the Local Group Policy Editor.

Additional Configurations for Windows

This section contains additional configurations required for setting up Windows devices for testing.

Disabling Fast User Switching

Fast User Switching is a feature in all supported versions of Windows 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 log the student out of the test. The following sections describe how to disable Fast User Switching for different versions of Windows.

If you plan to use the Take a Test app on a dedicated test account on a Windows 10 device, do not disable fast user switching, as it causes the machine to enter an infinite loop when rebooted.

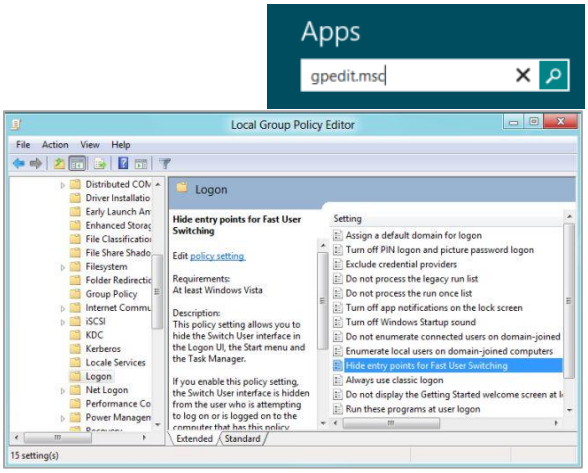
Disabling Fast User Switching in All Supported Versions of Windows

The following procedure describes how to disable Fast User Switching under all supported versions of Windows.

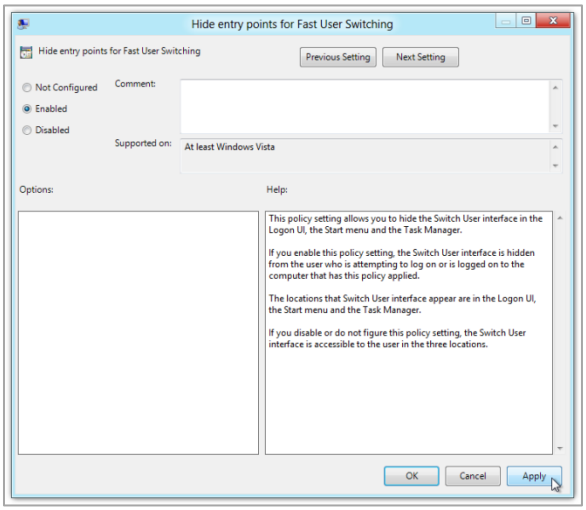
1. In the Search charm, type `gpedit.msc`. Double-click the gpedit icon in the Apps pane. The Local Group Policy Editor window opens.

2. Navigate to `Computer Configuration > Administrative Templates > System > Logon.`

3. In the Setting pane, double-click **Hide entry points for Fast User Switching**.

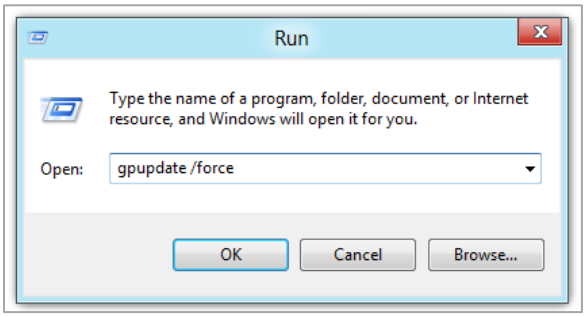


4. Select **Enabled** and then click **OK**.

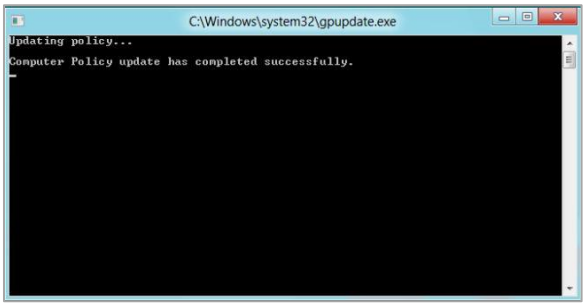


5. In the Search charm, type `run`. The **Run** dialog box opens.

6. Enter the command `gpupdate /force` into the text box and then click **OK**. (Note the space before the forward slash.)



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.



Disabling App Prelaunching for Windows

Application Prelaunch is a feature in Windows 10 that allows Universal Windows Platform apps, such as the Photos app or Edge web browser, to prelaunch and run in the background even if a user didn't open the apps themselves. Users will be unable to start Take a Test with these apps running in the background and will be kicked out of a test if the apps launch while the user is running the Take a Test app. This does not affect users running the Florida Secure Browser.

App pre-launching can be disabled by using a PowerShell command and editing the registry. For instructions on how to disable app pre-launching, see this page from Microsoft's Online Windows Support.

Disabling Screen Edge Swipe on Windows 10 Touchscreen Devices

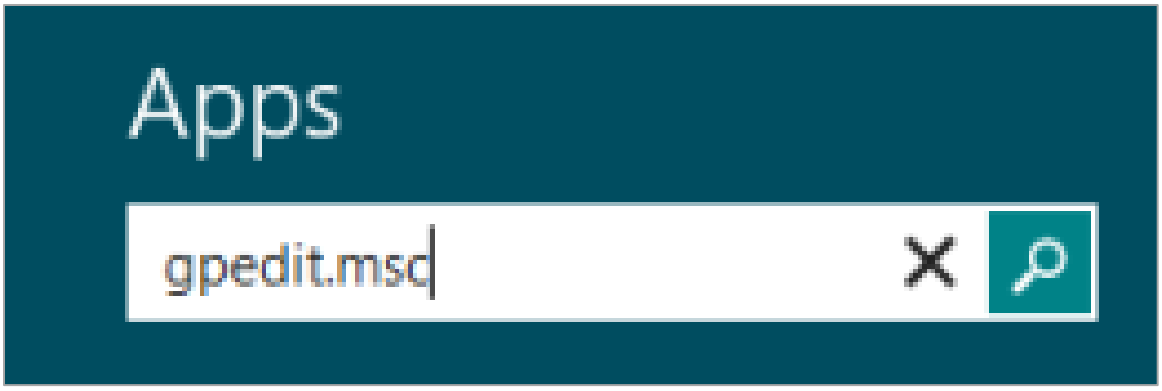
Swiping inward from the edge of the display on Windows 10 touchscreen devices opens the Windows notification center. If this swiping gesture is not disabled and students taking a test in the Secure Browser on a Windows 10 touchscreen devices swipe from the edge of the screen during a test, the notification center will open, displaying any notifications that might appear there and pausing the test. This affects all Windows 10 touchscreen devices. The following section describes how to disable Screen Edge Swipe using the Local Group Policy Editor.

You can also roll this change out to multiple devices at once using the Registry Editor. To make this change via the Registry Editor, you must have administrator privileges on the device.

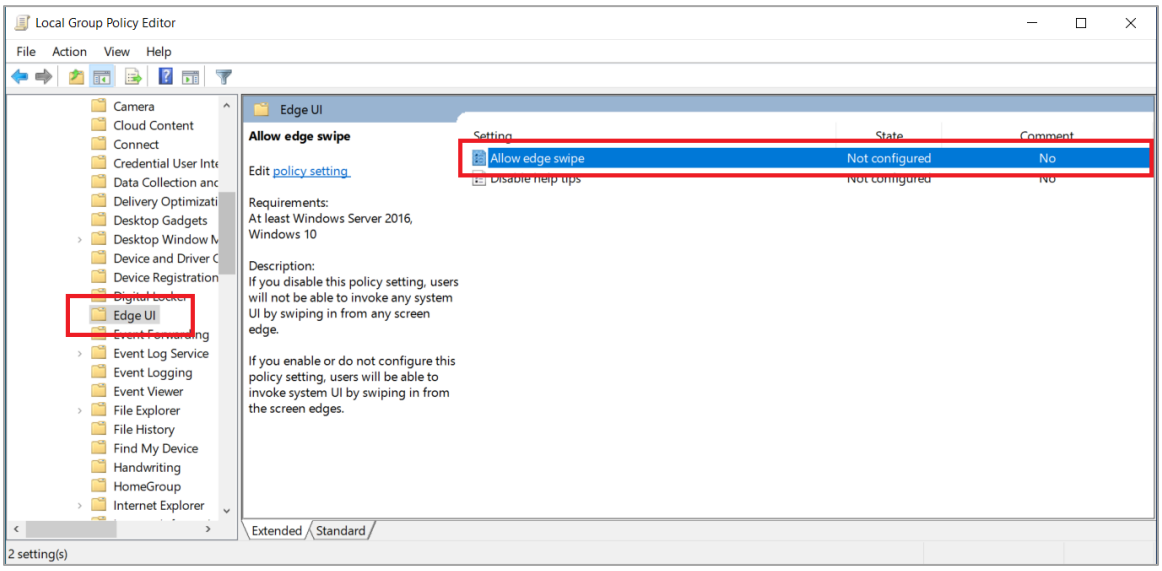
Disabling Screen Edge Swipe Using the Local Group Policy Editor

The following procedure describes how to disable Screen Edge Swipe using the Local Group Policy Editor.

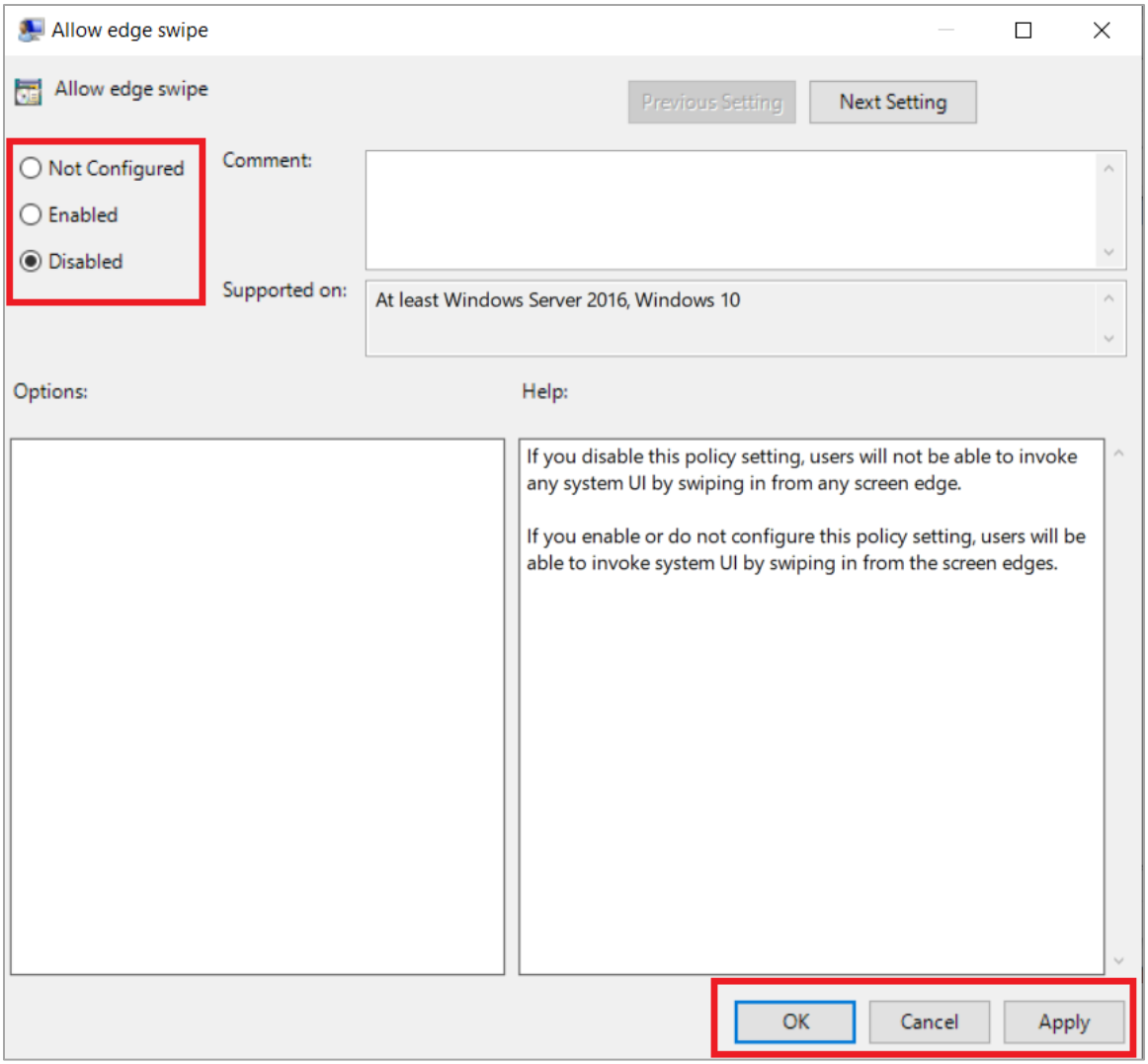
1. In the Search charm, type gpedit.msc. Select the gpedit icon in the Apps pane. The Local Group Policy Editor window opens.



2. Navigate to Computer Configuration > Administrative Templates > Windows Components > Edge UI.



3. In the right pane, double-click/tap **Allow edge swipe**. The ***Allow Edge Swipe*** window opens.



4. Select **Disabled**.
5. Select **Apply**.
6. Select **OK**.
7. Close the ***Local Group Policy Editor*** window.
8. Restart your computer or tablet for the change to take effect.

Troubleshooting for Windows

This section contains troubleshooting tips for Windows.

Resetting Secure Browser Profiles on Windows

If the Florida 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\CAI\`

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

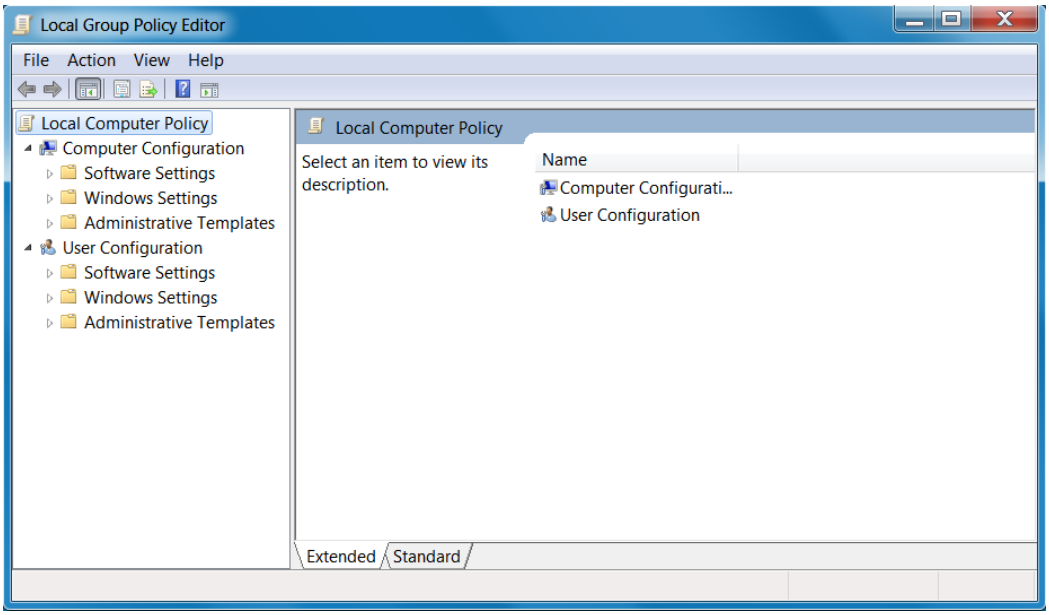
   where `username` is the Windows user account where the Secure Browser is installed. (Keep the `CAI\` folders, just delete their contents.)

3. Start the Secure Browser.

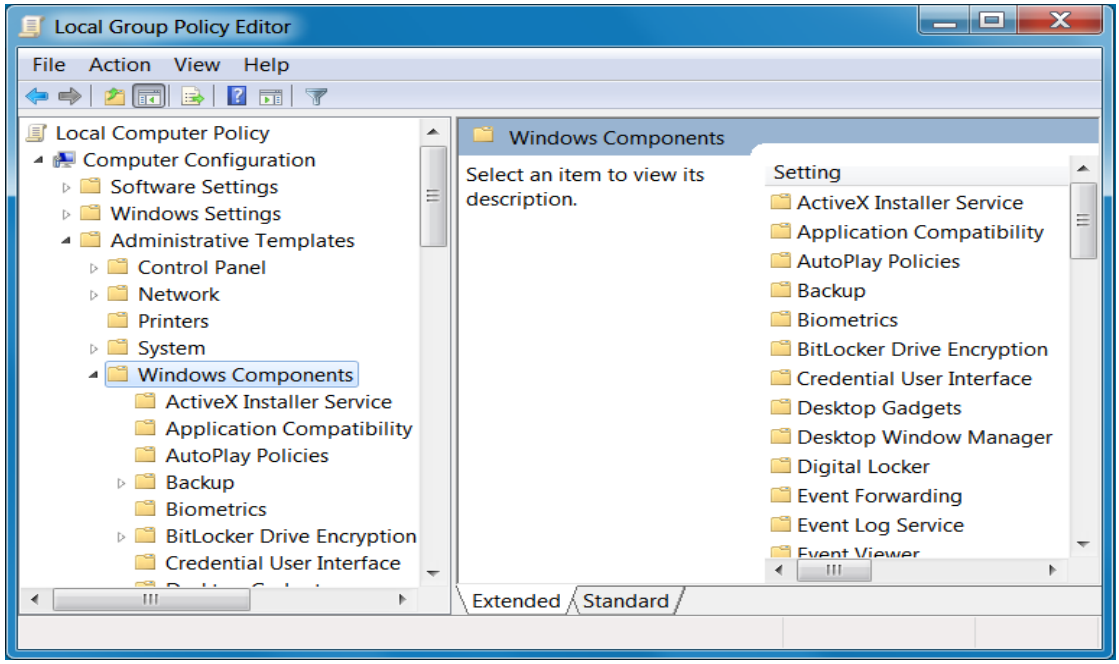
Blocking Device Touch Input Using the Group Policy Editor

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:

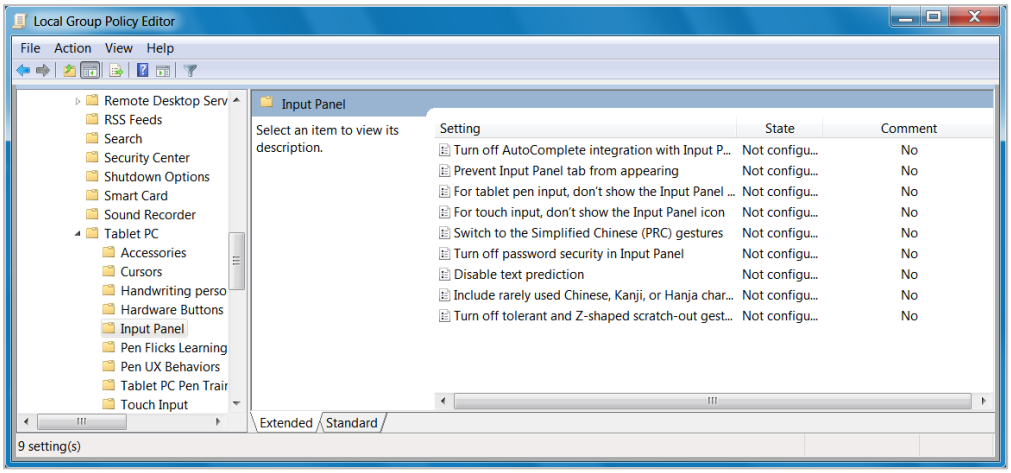
1. Type `gpedit.msc` in the *Search* box on the **Start** menu. The ***Local Group Policy Editor*** window appears.



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



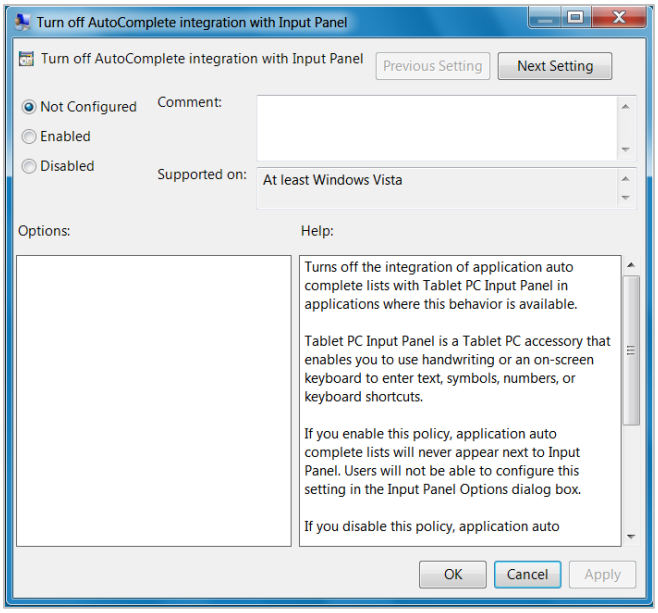
3. Scroll down to the **Tablet PC** folder, then select **Input Panel**. The following screen displays.



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.



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

7. Close the ***Local Group Policy Editor*** window.

Installing 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:

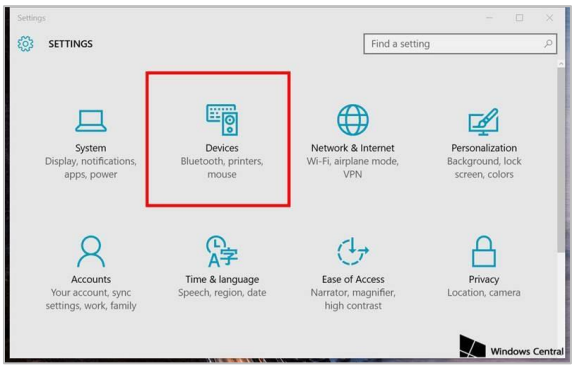
- About the Media Feature Pack for Windows 8.1 N and Windows 8.1 KN Editions: April 2014 (http://support.microsoft.com/kb/2929699/en-us)
- Download Media Feature Pack for N and KN Versions of Windows 8.1 (http://www.microsoft.com/en-us/download/details.aspx?id=42503)

Touch Keyboard on Microsoft Surface Pro Tablet

On some Surface Pro devices, the touch keyboard disappears when the student clicks outside a text box or when the student types an answer into a text box and clicks next. The keyboard fails to reappear when the student clicks back inside the next text box. To avoid these issues, set the touch keyboard to appear each time.

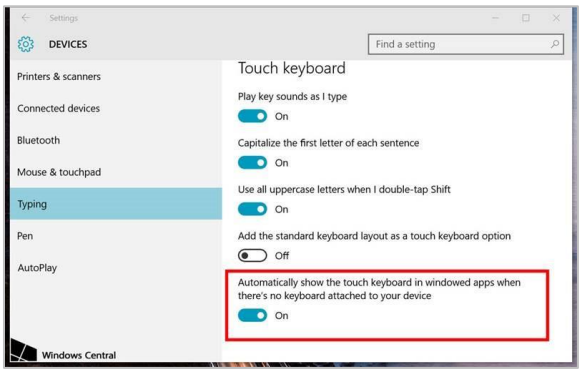
To set the touch keyboard to automatically appear each time:

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



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*.

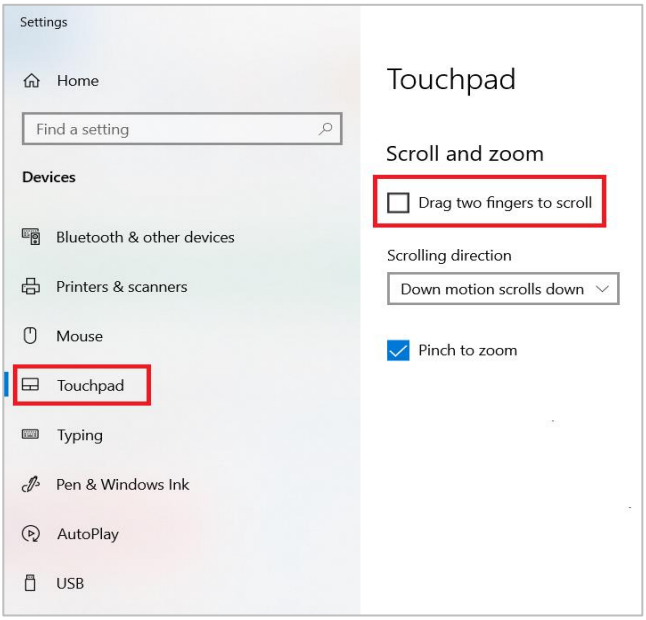


Disabling Two-finger Scrolling Feature in HP Notebooks with Synaptics TouchPad

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.

To disable the TouchPad feature in HP notebooks with Synaptics TouchPad:

1. Click the **Start** menu (), and then type `mouse settings` in the search field.
2. Select **Mouse settings** from the list of options.
3. Select **TouchPad**.
4. In the *Scroll and zoom section*, clear the *Drag two fingers to scroll* checkbox.



Disabling Automatic Volume Reduction

A feature in Windows automatically lowers or mutes the volume of some apps if Windows detects audio recording, even when the user is not actively using audio recording software. This section describes how to disable automatic volume reduction.

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**.

Troubleshooting Text-to-Speech

Using text-to-speech requires at least one voice pack to be installed on testing computers.

A number of voice packs are available for desktop computers, and CAI researches and tests voice packs for compatibility with the Secure Browsers. Additionally, not all voice packs that come pre-installed with operating systems are approved for use with online testing. The voice packs listed at the end of this section have been tested and are allowed by the Secure Browser.

Using Text-to-Speech

Students using text-to-speech for the practice and operational tests must log in using the Secure Browser.

We strongly encourage schools to test the text-to-speech settings before students take operational tests. You can check these settings by running a practice test or the Infrastructure Trial with text-to-speech enabled or through the diagnostic page. From the student practice test login screen, click the **Run Diagnostics** link, and then click the **TTS Check** button.

How the Secure Browser Selects Voice Packs

This section describes how CAI's Secure Browsers select which voice pack to use. It is recommended that students use the same voice pack that the student uses for instruction. Moreover, if students were using NeoSpeech Julie prior to the Summer 2020 administration, a new voice pack must be selected prior to testing to avoid using a 'demo' version of the Julie voice pack.

Voice Pack Selection on Desktop Versions of Secure Browsers

When a student who is using text-to-speech starts a test, the Secure Browser looks for voice packs on the student's machine. Upon recognizing an approved voice pack, the Secure Browser uses the one with the highest priority.

If any of the approved voice packs has also been set as the default voice on the computer, then that voice pack will always get the highest priority. Currently, Microsoft David is one of the Voice Packs used to check for proper pronunciation.

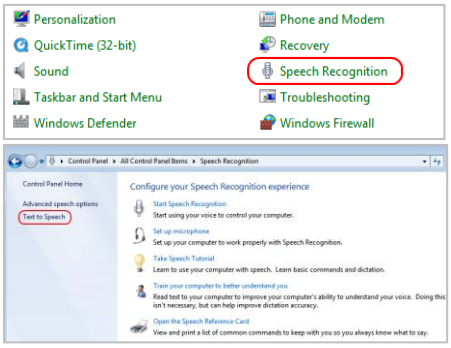
Configuring Windows Text-to-Speech Settings

This section explains how to configure Windows for using text-to-speech with the Secure Browser. The text-to-speech feature is available on Windows versions as listed on the Supported Systems & Requirements page.

The instructions in this section are similar for all versions of Windows.

1. Open the ***Control Panel*** window and select **Speech Recognition**.

2. In the ***Speech Recognition*** window, select **Text to Speech**.



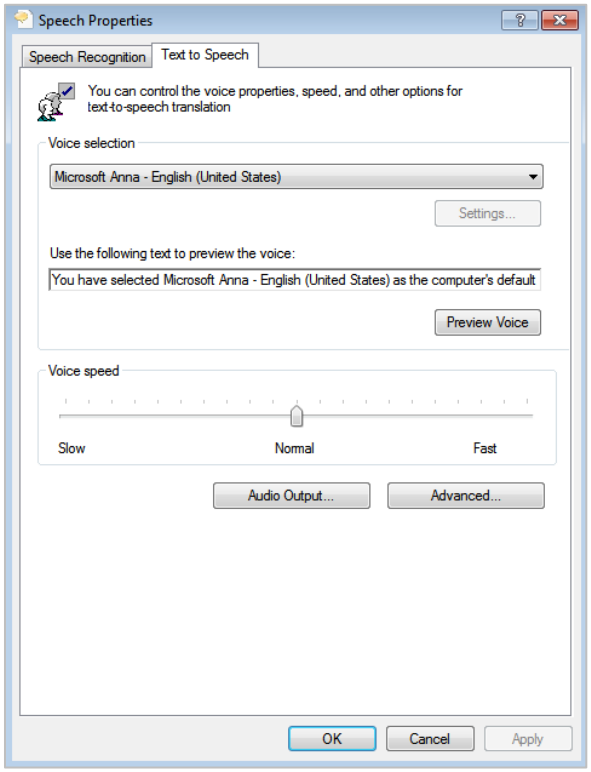
3. Configure default text-to-speech preferences.

   a. *Voice selection:* If multiple voice packs are available, select the default voice.

   b. Select **Preview Voice** to see whether the selected voice requires a rate adjustment.

   c. *Voice speed:* If necessary, adjust the voice speed. Drag the slider to make the voice speak slower or faster. To listen to the rate, select **Audio Output**.

   d. When you are done, click **OK** to save your settings and then close the ***Speech Properties*** window.



Voice Packs Recognized by Desktop Secure Browsers

The tables in this section display the voice packs for Windows that are currently recognized by the Secure Browser.

Voice Packs for Windows

Voice Packs Recognized by Secure Browsers—Windows

Vendor	Voice Pack	Language
Windows (pre-installed)	Kate	English
Windows (pre-installed)	Michael	English
Windows (pre-installed)	Michelle	English
Windows (pre-installed)	MSAnna	English
Windows (pre-installed)	MS_EN-GB_HAZEL	English
Windows (pre-installed)	**MS_EN-US_DAVID**	**English**
Windows (pre-installed)	MS_EN-US_ZIRA	English
Windows (pre-installed)	MSMary	English
Windows (pre-installed)	MSMike	English
Windows (pre-installed)	MSSam	English
Windows (pre-installed)	Paul	English
Cepstral (commercial)	Cepstral_David	English

Windows Technology Coordinator Checklist

This checklist can be printed out and referred to during review of networks and computers used for testing.

	Activity	Target Completion Date	Reference
For all Operating Systems			
☐	Verify that all of your school's computers/devices that will be used for online testing meet the operating system requirements.	3–4 weeks before testing begins in your school	Supported Systems & Requirements
☐	Install the secure browser on all computers/devices that will be used for testing.	3–4 weeks before testing begins in your school	Configurations, Troubleshooting, and Secure Browser Installation for Windows
☐	Verify that your school's network and Internet are properly configured for testing, including Allowlisting procedures, conducting network diagnostics, and resolving any issues.	3–4 weeks before testing begins in your school	Technology Setup for Online Testing
☐	Enable pop-up windows and review configuration requirements for each operating system.	1–2 weeks before testing begins in your school	Configurations, Troubleshooting, and Secure Browser Installation for Windows
For Windows			
☐	Install any required text-to-speech software on computers that will be used for testing with that accommodation and verify the installation.	1–2 weeks before testing begins in your school	Using Text-to-Speech
☐	On computers, complete remainder of additional configurations, including disable Fast User Switching and app prelaunch. If a student can access multiple user accounts on a single computer, you are encouraged to disable the Fast User Switching function.	1–2 weeks before testing begins in your school	Additional Configurations for Windows

Florida Help Desk and User Support

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

The Help Desk is open **Monday–Friday from 7:00 a.m. to 8:30 p.m. Eastern Time** (except holidays or as otherwise indicated on the Florida Statewide Assessments Portal).

Toll-Free Phone Support: 1-866-815-7246

Email Support: FloridaHelpDesk@CambiumAssessment.com

In order to help us effectively assist you with your issue or question, please be ready to provide the Florida Help Desk with detailed information that may include the following:

- Device, 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

Location	Change	Date
Throughout Guide	Updated links to new portal.	9/2/21
Disabling Screen Edge Swipe on Windows 10	Added new section.	9/2/21
Disabling Screen Edge Swipe Using the Local Group Policy Editor	Added new section.	9/2/21
Throughout Guide	Removed references to 32-bit Windows.	9/2/21