



Setup & Installation Guide

Nextera®

New York State Testing Program 2026-2027 Grades 3–8
ELA, Math, and Grades 5 & 8 Science
Computer-Based Tests

©2024 NWEA. Nextera is a registered trademark of NWEA in the US and in other countries. All trademarks, product names, and logos are the property of their respective owners. All Rights Reserved. Windows® is a registered trademark of Microsoft®. Google Chrome™ and Chromebook™ are trademarks of Google®. Casper Suite® is a registered trademark of JAMF Software, LLC. iPad® and Mac® are registered trademarks of Apple®. Clean Slate® is a registered trademark of Fortres Grand. Deep Freeze™ is a trademark of Faronics. All trademarks, product names, and logos are the property of their respective owners. All Rights Reserved.

Contents

Introduction to the Deployment and Installation of the Nextera [®] Assessment System	5
Overview.....	5
Security and the Student Experience	6
Preparing your Site - General	6
Checklist of Preparation Activities	6
Preparing your Site – Step by Step.....	8
Perform Site Setup – System Scan	8
Perform Site Setup – Test Readiness	11
Network Considerations and Setup.....	16
Proxy Servers / Firewalls / Web Content Filters	16
Nextera Test Delivery System Installation	18
Windows Installation	18
MacOS Installation.....	24
Apple iPad Installation.....	28
Chromebooks Installation	32
Accessibility Settings.....	38
Text-To-Speech	38
Speech-To-Text	38
Additional Settings	39
Disable Sticky Keys and Filter Keys: Windows	39
Disable Fast User Switching: Windows.....	41
Disable Handoff on iPad Devices	42
Disable Siri: iPadOS	43
Disable Scribble: iPadOS	44
Disable Select to Speak: Chromebooks.....	44
Disable Dictation: Chromebooks.....	45
Disable All Apps: Windows and MacOS	45
Disable Startup Applications.....	56
Disable AssistiveTouch: iPad Pro	58
Disable App Power Management: Chromebook.....	61
Disable Predictive Text	62
Disable Predictive Math.....	63
Approved Questar Secure Browser Block List.....	64
Sample Test Login.....	66
Appendix A – Student Response Flowcharts	67
Student Response Flow	67

Appendix B – System Requirements	70
General System Requirements:	70
OS Specific System Requirements:	70
System Requirements continued	71
Appendix C – Frequently Asked Questions (FAQ)	72
Appendix D – Troubleshooting Tips	73
Issues Loading Test	73
Response Recovery When Internet is Disconnected Prior to Test Session Submission	73
-118 Error Code/Unable to access https://nextera.questarai.com	74
Issues Editing Constructed Responses.....	74
Troubleshooting Error Messages Students May Encounter Prior to and During Testing	75
Possible Error Messages When Logging In.....	75
Possible Error Messages During Testing	79
Possible Questar Secure Browser Errors.....	85

Introduction to the Deployment and Installation of the Nextera® Assessment System

Overview

The Nextera Assessment System is a suite of software applications used for conducting standardized assessments. This *Setup and Installation Guide* provides the following information regarding the Nextera Assessment System:

- A high-level overview
- Guidelines for deployment and implementation
- Troubleshooting Tips

This document is designed for technology coordinators responsible for the installation, administration, and configuration of the Nextera Assessment System. Successfully deploying the client software requires a solid understanding of the environment, requirements, and specific testing needs. Since each device platform has different installation steps, client deployment methodologies, and system requirements, this guide includes detailed installation instructions for the commonly used platforms (e.g., Windows). The Nextera Assessment System is comprised of two primary applications:

- **Nextera Admin** is a web-based application for loading and managing district, school, class, teacher, and student information. The Help Tab contains links and downloads, including the Questar Secure Browser.
- **Nextera Test Delivery System (TDS)** is a software application for administering student assessments delivered through the **Questar Secure Browser**.
 - The **Questar Secure Browser** allows students to take the test on the Nextera Test Delivery System. It is downloaded and installed on student workstations and will prevent access to other applications, computer functions, or network access, until the student exits the testing mode.
 - **Important Note:** This year there is a new Secure Browser release. Schools must install the new Browser for the 2026-2027 school year following the instructions in this guide.

The technology coordinator should have received an email with a **URL, username, and password to access Nextera Admin**. If this information has not been received, or has been misplaced, please contact **Customer Support** by calling **866-997-0695** or emailing NYTesting@nwea.org.

Security and the Student Experience

As a technology coordinator you may be asked about test security, recommendations, and the student experience. The Nextera Test Delivery System (TDS) is designed to prevent a student from navigating away from the Questar Secure Browser while testing. Therefore, many keyboard shortcuts are disabled. For example, if a student testing with a Windows PC attempts to use **Alt+Tab**, the student will be logged out of the test and returned to the login screen.

Technology evolves constantly. Every effort to engage security measures does not replace the important role of proctors and their oversight of students while testing.

Please refer to [Appendix A](#) for information on student testing during the loss of internet connectivity during testing.

Preparing your Site - General

Preparedness is the first step toward a successful assessment administration. Use the following checklist as a guideline for your preparation. Following the checklist, see the instructions to evaluate your site using the Readiness tools available on the Test Readiness website at <https://www.nwea.org/nextera/readiness/>. Using workstations representative of your testing environment, perform the *System Scan* and *Test Readiness* checks to validate that your devices and network are ready for student testing.

Checklist of Preparation Activities

- ❑ Perform Site Setup – System Scan
 - For detailed instructions, select the following link: [Perform Site Setup – System Scan](#)
 - At a minimum, each device type being used for testing should be scanned.
- ❑ Perform Site Setup – Test Readiness
 - For detailed instructions, select the following link: [Perform Site Setup – Test Readiness](#)
 - If using Wireless Networks, ensure there is ample coverage and capacity to support testing.
- ❑ **Verify that all student devices being used for testing in 2027 are running the latest supported version of the Secure Browser.**

Mac	iPad	Chrome	Windows
5.2	2.2	1.0	5.2

- **Download and install the secure browser from the Help > Downloads page in Nextera Admin.**
- ❑ Ensure device [Accessibility Settings](#) and [Additional Settings](#) are set appropriately as outlined in this guide.

- ❑ Log into the Practice Test using the Questar Secure Browser. For additional information and Practice Test logins, please view the article on CBT Support: [NWEA Secure Browser Practice Test Logins](#)
- ❑ Ensure Test Administrators are aware of district policies, expectations, and processes for troubleshooting issues. Please see the [Proctor Training](#) for more information.
- ❑ Before testing begins, disable and close all applications before students launch the Questar Secure Browser on devices being used for testing. The Questar Secure Browser cannot open until all applications are closed.
- ❑ Prior to testing, confirm that devices display the correct date and time for the location that testing is occurring to ensure proper functionality of Text-to-Speech and accessibility to the assessment.
- ❑ During testing, limit network activity that may impact bandwidth, such as streaming music and video.

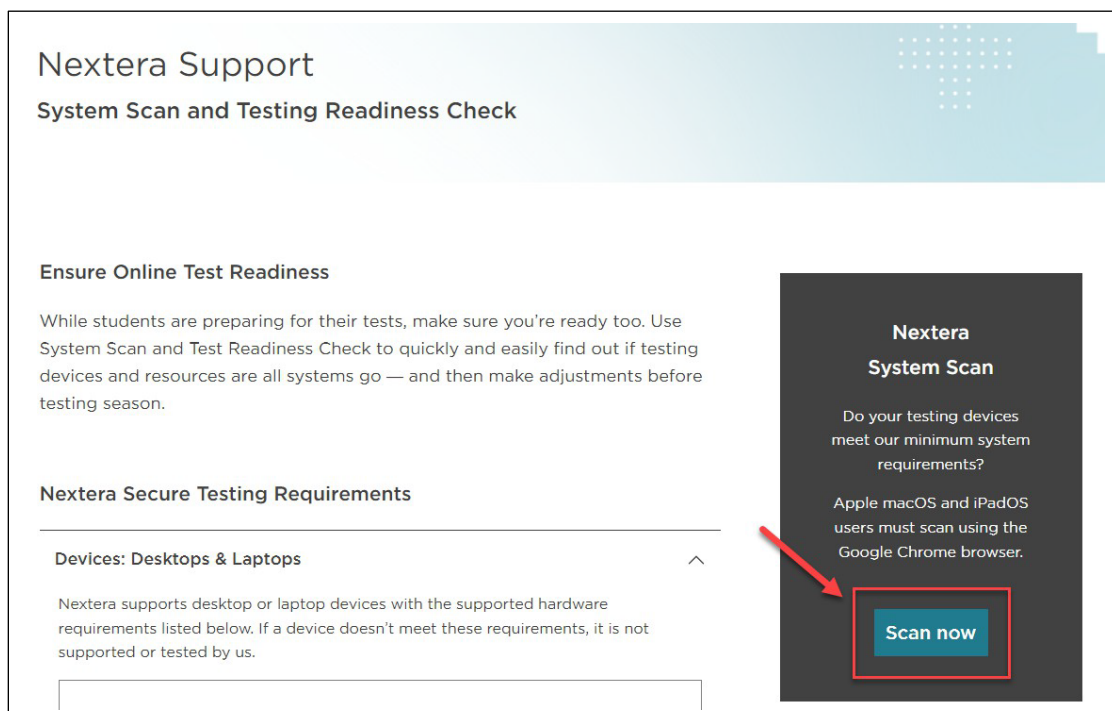
IMPORTANT: If a new operating system becomes available and it is not listed on the Test Readiness website at <https://www.nwea.org/nextera/readiness/> or addressed in a subsequent release note by NWEA, it may not be supported. Please do not upgrade to new operating systems on devices that will be used to administer online assessments without verifying that the new operating system is supported.

Preparing your Site – Step by Step

Perform Site Setup – System Scan

Please note: The System Scan is designed to validate Desktop Device configurations. See the system requirements for additional detail about Tablet devices and Chromebooks.

- 1) Open a Web browser and access <https://www.nwea.org/nextera/readiness/>.
- 2) Locate the *System Scan* message and select **Scan Now**.



Select **Scan Now**.

Do your testing devices meet our minimum system requirements for Nextera?

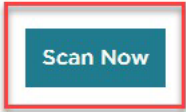
System Scan takes a deep dive and then surfaces with details about how your device's browsers, operating systems, device specs and more comply with our general [system requirements](#).

The System Scan is designed to validate Desktop and Laptop device configurations. See the [system requirements](#) for additional detail about Chromebook and Tablet devices.

During testing, students will need to use Nextera's secure testing browser to access the testing material. The browser portion of this scan applies only to Nextera testing administration sites and not to the actual tests themselves.

System Scan

Apple macOS and iPadOS users must scan using the Google Chrome browser.



Scan Now

The scan results display below. If a warning message displays, verify the workstation has the minimum system requirements specified for that type of device. Visit the Test Readiness website at <https://www.nwea.org/nextera/readiness/> for System Requirements listed under Questar Secure Testing Requirements.

Device Information	Browser Information
Applies to both the Nextera administrative portal and the student testing experience.	Only applies to the Nextera administration portal
 SYSTEM TYPE Desktop Computer	 BROWSER Google Chrome
 OPERATING SYSTEM Microsoft Windows	 VERSION 127.0.0.0
 OPERATING SYSTEM VERSION Supported	 ACCEPTING COOKIES? Yes
 SCREEN RESOLUTION 1920 x 1080 pixels	

Perform Site Setup – Test Readiness

- 1) Open a Web browser and visit the [Test Readiness webpage](https://www.nwea.org/nextera/readiness/) (<https://www.nwea.org/nextera/readiness/>).
- 2) Locate *Test Readiness*, then select **Test Now**.

Nextera Support

System Scan and Testing Readiness Check

Ensure Online Test Readiness

While students are preparing for their tests, make sure you're ready too. Use System Scan and Test Readiness Check to quickly and easily find out if testing devices and resources are all systems go — and then make adjustments before testing season.

Nextera Secure Testing Requirements

Devices: Desktops & Laptops

Nextera supports desktop or laptop devices with the supported hardware requirements listed below. If a device doesn't meet these requirements, it is not supported or tested by us.

	Chromebook	Windows	Apple
Minimum Screen Size	11.6"+	11.6"+	11.6"+
Minimum Resolution	1024×768	1024×768	1024×768
Minimum Processor	Intel Core 2 equivalent or higher CPU	Intel Core 2 equivalent or higher CPU	Intel Core 2 equivalent or higher CPU
Minimum System Memory	1GB minimum 2GB recommended	1GB minimum 2GB recommended	1GB minimum 2GB recommended
Free Storage	1GB	1GB	1GB
Additional Notes	- Chromebooks must be supported by Google auto-updates. - Dual-mode Chromebooks with laptop/tablet modes must be run in laptop mode (tablet mode is not supported).		

Devices: Tablets & Touchscreen

Nextera System Scan

Do your testing devices meet our minimum system requirements?

Apple macOS and iPadOS users must scan using the Google Chrome browser.

Scan now

Nextera Test Readiness

Do your classrooms and schools have the right resources to testing online?

Test now

- 3) Select the link <http://www.speedtest.net/> to determine your download and upload speeds. This will open the *SPEEDTEST* website in a new internet browser tab or window.

Do your classrooms and schools have the right resources to test online?

The Nextera Test Readiness Check takes a quick tour of your system and comes back with a readiness assessment based on how much testing you plan to do, the number of devices present and available bandwidth. We suggest that you run this test when your system bandwidth most closely reflects what it will be on test day.

Visit www.speedtest.net (opens in new tab) to determine your download and upload speeds. Input the results from the speed test in the first two fields of the form below.

Download Speed*

Enter speed from test.
Mbps

Upload Speed*

Enter speed from test.
Mbps

Individual Student Testing Time*

hours

Hours Available for Testing*

hours

Total Number of Students Testing*

students

Number of Devices*

devices

Testing Window*

Number of days

days

Test Now

Results

To estimate the number of tests that can be administered at the same time, Test Readiness Check assumes 100 percent bandwidth availability. If you use your network for other tasks during testing, the number of tests you can administer may decrease.

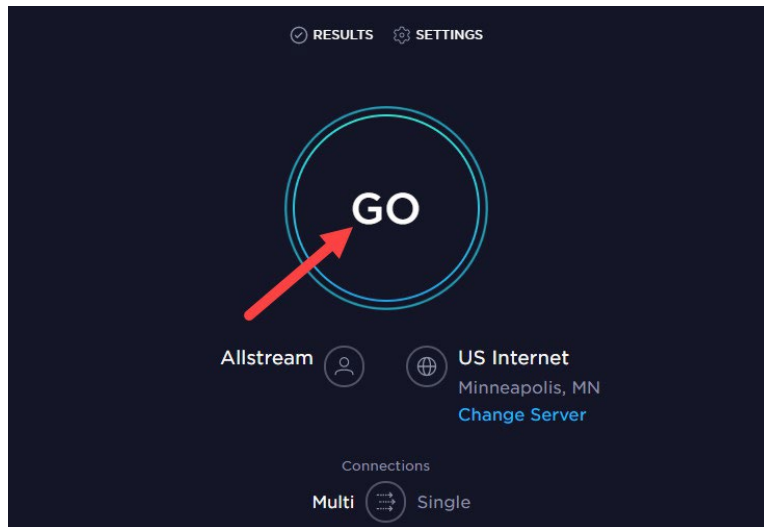
Need support?

Mississippi: 1-800-644-4054

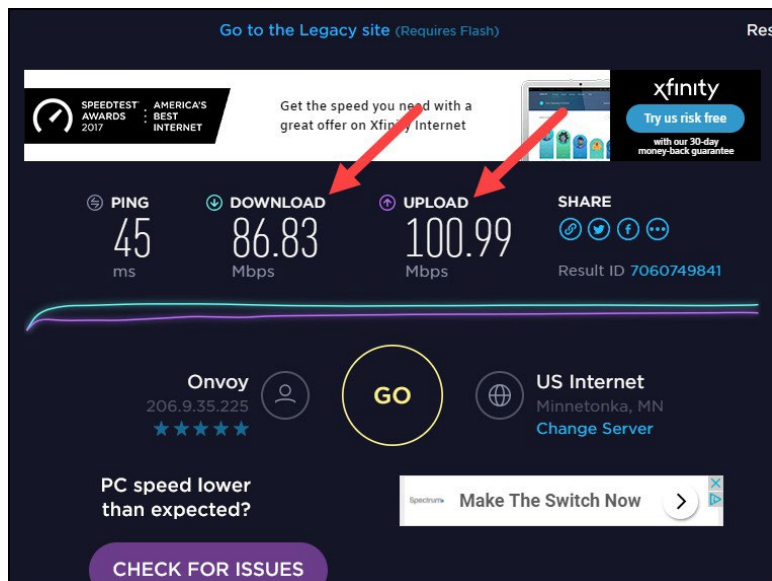
New York: 1-866-997-0695

Missouri: 1-800-571-2545

- 4) Select **Go**. The test process may take a few minutes to complete. It is recommended that you run this test at the same time of day you will be testing.



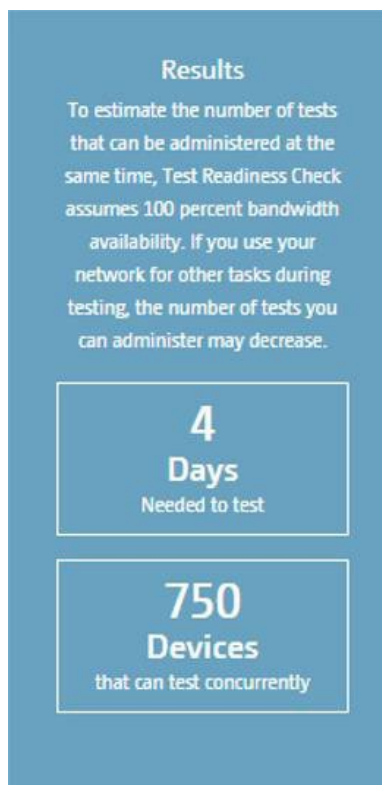
- 5) The results display.



- 6) To estimate the number of tests that can be administered at the same time, copy the download and upload speeds from step 5, then close the browser window/tab to return to the *Test Readiness* page. Input the data in the fields provided and select **Test Now**.

Download Speed*	Upload Speed*
Enter speed from test. Mbps	Enter speed from test. Mbps
Individual Student Testing Time*	
hours	
Hours Available for Testing*	
hours	
Total Number of Students Testing*	
students	
Number of Devices*	
devices	
Testing Window*	
Number of days days	
	
Test Now	

7) The Test Readiness Check results appear.



- Wireless connections can impact testing performance due to access contention, interference, or design. **A wired LAN connection will always outperform a wireless connection.**
- Results from this test vary from site to site and may not accurately reflect the maximum total bandwidth of your connection.
- If you have concerns regarding your system readiness or want assistance interpreting the results of the compatibility check or network bandwidth test, contact **Customer Support** by calling: 866-997-0695 or emailing NYTesting@nwea.org. For more information on NWEA'S Customer Support team and hours please visit this article on [CBT Support](#).

Network Considerations and Setup

Once you have used the Site Setup tools to determine there is adequate available bandwidth, ensure readiness regarding other upstream network devices (e.g., firewalls, proxy servers, Internet content filters). Given the wide variety of devices in the market, and their overlapping feature sets, this guide does not provide specific device-level settings for each possible configuration; however, since most of these devices perform the same basic functions, the following guidelines will help you configure your network devices for the Nextera Assessment System.

Proxy Servers / Firewalls / Web Content Filters

A proxy server typically sits between the students' workstations and the Internet. Proxy servers are commonly used for caching, filtering, and authentication.

- **Caching** accelerates Web page request/load time by retrieving content saved from a previous request by the same user or other users.
- **Filtering** applies policies to specific networks, protocols, and content; blocks undesired websites and/or content.

Note: Cisco Umbrella is incompatible with Nextera.

- **Authentication** controls which users and resources can access the Internet.

Nextera Test Delivery System uses the same protocols to communicate on the Internet as standard Web browsers, so it is critical that proxy servers be configured to **allow all HTTP traffic between the Nextera Test Delivery System and the Internet on ports 80, 443, and 8443**. The following domains should be whitelisted at the firewall, authenticating proxy server, or content filtering server:

NY.nextera.questarai.com

***questarai.com**

***nwea.org**

***transcribestreaming.us-west-2.amazonaws.com AND cognito-identity.us-west-2.amazonaws.com (for Speech-to-Text troubleshooting)**

mobileapp.questarai.com (for Apple iPad devices)

To avoid possible domain name server problems, ensure the following URLs will pass through your proxy server, firewall, and Web content filter:

URL: https://NY.nextera.questarai.com **PORT:** 443

URL: https://NY.nextera.questarai.com **PORT:** 80

URL: https://NY.nextera.questarai.com **PORT:** 8443

If you need to whitelist by IP address, the IP's for ny.nextera.questarai.com are currently 104.17.137.108 and 104.17.138.108. Please verify with "nslookup ny.nextera.questarai.com" prior to testing.

- To ensure a stable testing environment with minimal issues, observe these guidelines during student testing:
 - **Minimize network traffic load** on the network servers.
 - **Avoid** performing client software updates, patching, and data backups.
 - **Remove bandwidth throttling** on ports **80, 443 and 8443**.
 - **Minimize or turn off network bandwidth intensive programs** (e.g., streaming music and video).
- Certain firewalls may present a **false positive warning** if they incorrectly recognize the bit sequence of a particular file as malware or a virus.

If you have difficulty accessing the Nextera Test Delivery System, please contact our Customer Support team at 866-997-0695 or [email \(NYTesting@nwea.org\)](mailto:NYTesting@nwea.org).

Nextera Test Delivery System Installation

The Nextera TDS is available for many types of devices using a variety of software formats, such as:

- *Questar Secure Browser* – for Windows OS and MacOS
- **Mobile App** – for Apple iPadOS Devices
- *Questar Secure Browser* – for Google Chromebooks

The Questar Secure Browser for each platform is available on Nextera Admin and the system requirements for each operating system are listed on the Test Readiness website at <https://www.nwea.org/nextera/readiness/>.

Detailed installation instructions at the device level and the managed level for each device are provided in the following sections:

[Windows Installation](#) (see below)

[MacOS Installation](#)

[Apple iPad Installation](#)

[Chromebooks Installation](#)

Windows Installation

Windows provides several installation types to support nearly every possible configuration scenario. These include local workstation installations and mass deployment push. File server installations are not supported.

For each Windows installation type, each student must have access to the cache location that contains the encrypted student responses, which is used to protect the student's test responses if network connectivity is lost. For instructions on changing the default location of the cache files select the following link: [Cache Location](#). It is recommended that this be a local device location since the device will not be able to cache responses to a server if the network connection is lost.

Each Windows installation scenario makes use of the appropriate *.msi* file from Nextera Admin. The following sections describe the steps necessary to perform each of the typical Windows installation scenarios:

[Basic Installation –Individual Device](#)

[Push Installation](#)

Uninstall

If a previous version of the Questar Secure Browser is available on the device, uninstall the previous version before installing the updated version. If a previous version of the Questar Secure Browser is launched on MacOS or Windows devices, a message will display as a reminder to update the Questar Secure Browser to the most recent version. If you are uncertain whether or not there is a previous version of the Questar Secure Browser on the device, follow steps 1 through 3 below to verify a previous version exists.

- 1) From the *Start menu*, select **Windows System -> Control Panel**.
- 2) Select **Programs and Features**.
- 3) Locate the previous Questar Secure Browser.
- 4) Select the **Questar Secure Browser** icon using the secondary mouse button (commonly configured as a “right-click”).
- 5) In the drop-down menu that appears, select **Uninstall**.
- 6) A pop-up window asks you to confirm that you wish to uninstall. Select **Yes**.

Basic Installation - Individual Device

- 1) Access Nextera Admin online using the URL, User ID, and Password provided by your District Test Coordinator.
- 2) Under the *Help* tab select **Downloads**. Then select **Download** in the Microsoft Windows row.
- 3) Select **Next** to begin the installation wizard.
- 4) Select **Install** to start the installation process.
- 5) Select **Finish** to complete the installation wizard.
- 6) Verify the installation is complete by launching the *Questar Secure Browser* icon from your Desktop.
- 7) Follow the Sample Test Login steps.

Creating and Sharing a Shortcut

- 1) Select the **QuestarStudent.exe** file created from your File Server installation using the secondary mouse button, pasting the new shortcut to your file share location.
- 2) Distribute the shortcut to students' accounts using your preferred distribution method.

Push Installation

Because of their powerful automation capabilities, software packaging and distribution tools have become a popular way to manage the delivery of software applications. Many of these tools leverage the Windows Installer and its related MSI files. The Questar Secure Browser is provided in this standard format to allow administrators and technology coordinators to automate the installation process. If you need assistance completing the steps for a push installation, please contact Customer Support for the software company used for the push notification. If additional assistance is needed, please contact NWEA Customer Support team by calling 866-997-0695 or emailing NYTesting@nwea.org.

Basic Install:

- `msiexec /i QuestarStudent-(product).msi`

Silent Install:

- `msiexec /i QuestarStudent-(product).msi /quiet`
or
- `msiexec /i QuestarStudent-(product).msi /qn`

Silent Install to a Specified Directory:

- `msiexec /i QuestarStudent-(product).msi`
- `APPLICATIONFOLDER="\\server\share\path\QuestarStudent-(product)" /quiet`

Uninstall:

The syntax below requires the msi file to be in the current directory.

- `msiexec /x QuestarStudent-(product).msi /quiet`
or
- `msiexec /x {Product Code} /quiet`

Cache Location

When deploying the Questar Secure Browser in your environment, **it is crucial to protect the location of the cached student responses**. This file location contains the encrypted responses for each student. Therefore, it is important to understand where these files are located for each possible installation scenario and how it can be changed to suit your environment.

On *Windows*, the cache location is:

%allusersprofile%\QuestarStudent\%username%

(Normally C:\ProgramData\QuestarStudent\%username%)

When the student launches the Questar Secure Browser to begin testing, the folder structure is created and populated with testing materials. The student's encrypted responses are also stored in this location; therefore, the student account used for testing must have permissions to write into this location. For the normal Windows User profile, these rights are granted by default; however, when using other deployment methods, **it is essential to grant the appropriate rights for the accounts used for testing**.

To accommodate the variety of installation and deployment methods, **a command line switch can be used to change the default location of the Questar Secure Browser cache**. The following example shows the format of this switch and how it can be used to change the location of the cache.

For example, the Windows shortcut can be modified by adding the command line switch in the Target field (--cache-path="C:\temp\%COMPUTERNAME%\cachefolder").

Regardless of the deployment method, this command line switch can be used in a variety of ways, on the condition that the account used for conducting the assessment has sufficient rights to the location indicated and unique paths are provided for each student.

For example, consider the following scenario where the technology coordinator wants to perform a network installation with the cache location stored on a network location. Using a network location for the cache location should be done with caution since the responses will not be stored if the device loses connection to the network.

- Installation is performed according to the *File Server Installation* instructions provided in this guide.
- A shortcut is created and distributed to all student workstations using a Windows Group Policy. With the additional command line switch added to change the cache location to a network share, follow the instructions in this guide at this link: [Creating and Sharing a Shortcut](#).
- In this case, the following cache path was used in the Windows shortcut being distributed: --cache-path=\\Server\share\%USERNAME%\cache

Immutable shortcut target issue:

These shortcuts in which the target is not editable are shortcuts to PIDs rather than files:

<https://docs.microsoft.com/en-us/windows/win32/shell/namespace-intro?redirectedfrom=MSDN#pids>

To fix this we need to replace the shortcut with a standard shortcut with an editable target:

- **Method 1:** Open the current shortcut's properties and copy the "Start in" directory to the clipboard. Open that directory in Windows Explorer and locate the QuestarStudent-?.exe file. Copy that file onto the clipboard. On the desktop or wherever you would like the shortcut, using the secondary mouse button select **Paste shortcut**.
- **Method 2:** Use the secondary mouse button on the desktop or wherever you would like the shortcut and select **New -> Shortcut**. Browse to the location of the QuestarStudent-?.exe file as above and select it. Verify the name of the shortcut and select Finish.

Either method will produce a shortcut with a Target field that is editable.

Workstation Lockout Applications (DeepFreeze or CleanSlate)

If you **do not** use the default location and you have any scripts or applications, such as DeepFreeze™ or CleanSlate™ that clear out student profiles, complete one of the following actions:

- Disable the workstation lockout application, or
- Configure the workstation lockout application to exclude the cache location, or
- Use the command line switch described above to change the location where the encrypted response files are saved. As long as there is a network connection to this folder, and the account being used has proper rights, Nextera will use this alternate location to save the encrypted response file.

Common Practices to Follow and Background Processes to Disable

Please follow the steps in the table below during device set up in order to avoid possible interruptions during student testing.

Table 1 - Windows Machines

Common Background Processes to Disable	Common Practices to Follow
- Fast User Switching on Windows and Mac - Sticky keys and Filter Keys on Windows - Malware Software - Adobe Background Processes - Disable workstation lockout application	- Disable keyboard shortcuts - Avoid software updates, patching and data backups - Remove bandwidth throttling on ports 80/443 - Minimize and turn off network bandwidth intensive programs - Plug headsets in prior to launching TDS (for Text-to-Speech students only)

MacOS Installation

Note: Mac installations do not require changing student cache settings.

Automatic Assessment Configuration (AAC) should be used for the installation and configuration of MacOS. Using AAC, necessary restrictions will be automatically set using the installation instructions below.

Uninstall

If a previous version of the Questar Secure Browser is available on the device, uninstall the previous version before installing the updated version.

- 1) If there is a shortcut on the desktop, drag it to the trash or use the secondary mouse button and select **Move to Trash**.
- 2) Open Finder.
- 3) On the left side, select **Applications**.
- 4) Locate **Questar Secure Browser**.
- 5) Drag the application to the trash or use the secondary mouse button and select **Move to Trash**.

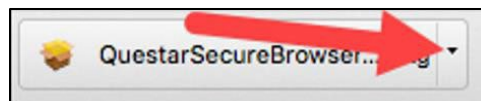
Install

The Questar Secure Browser application can be distributed using administrative tools such as the Casper Suite from JAMF Software. The following steps demonstrate how to **manually** install the MacOS client.

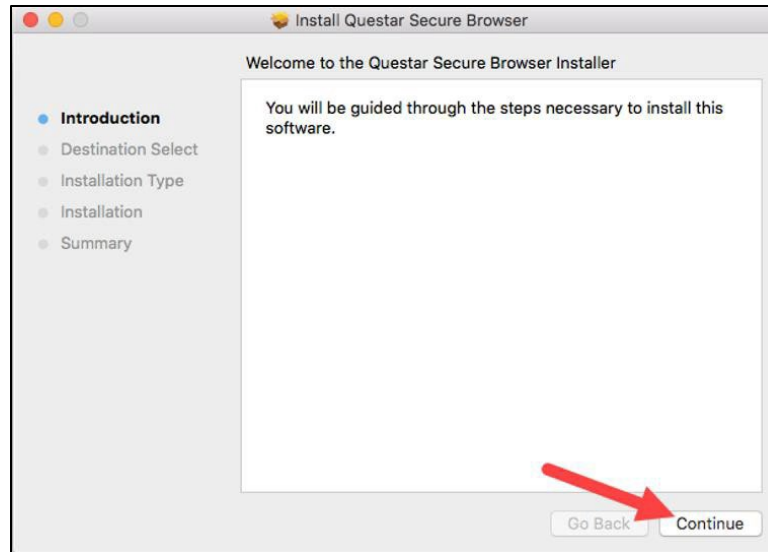
- 1) Access Nextera Admin online using the URL, User ID, and Password provided by your District Test Coordinator.
- 2) Under the *Help* tab, select *Downloads*, then select **Download** in the MacOS row, and download the .pkg package.
- 3) The download starts. If using Chrome, the following image appears in the lower left corner of the screen.



- 4) After the download is complete, select the arrow to open the file.

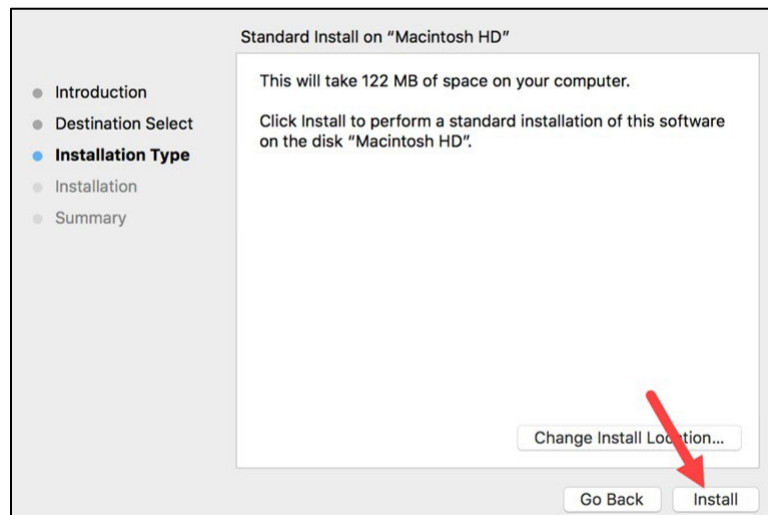


5) After you select the arrow to open the file, you will see the following:

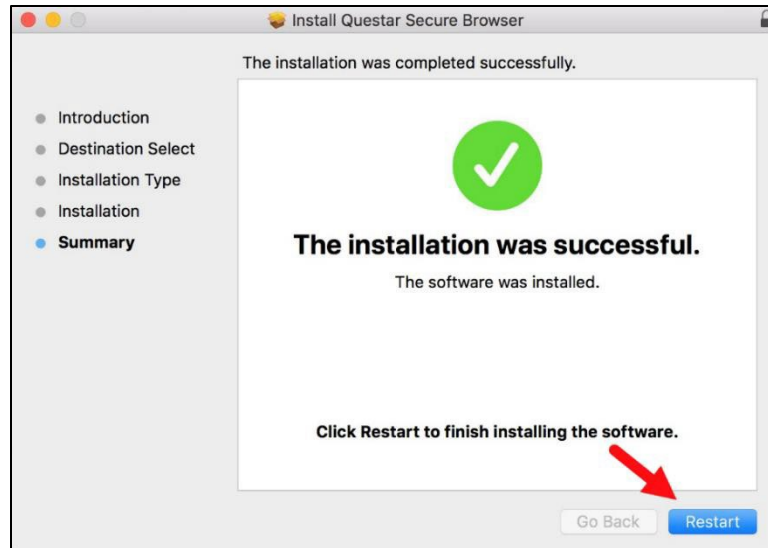


6) Select **Continue**.

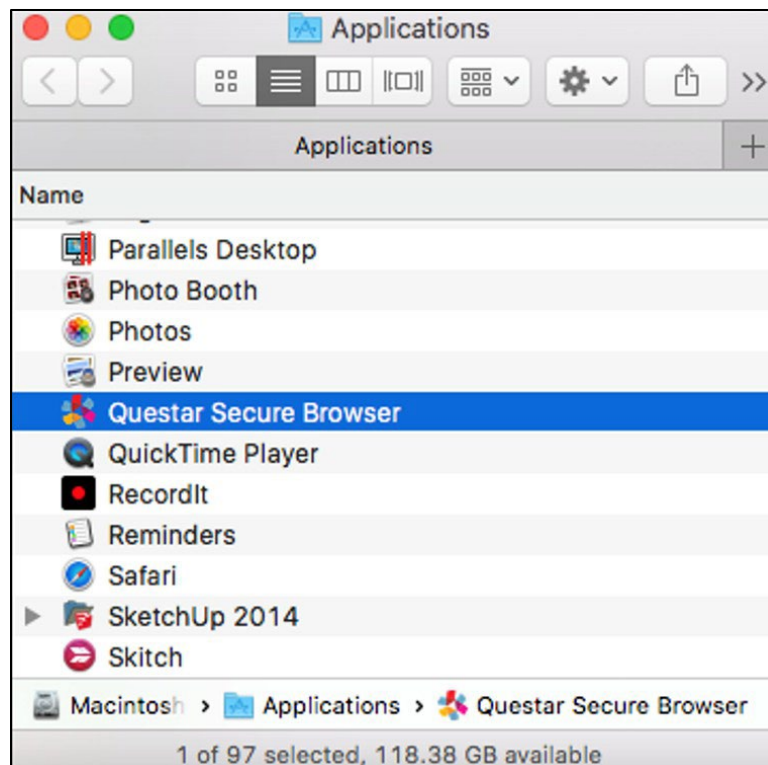
7) Select **Install**.



- 8) The browser will install and display this summary page. Select **Restart**.



- 9) After the machine restarts, log back into your user account and verify that the Questar Secure Browser is in your *Applications* folder. You can also search for this application through Spotlight Search.



User Switching:

Avoid user switching. While it is possible in macOS to switch from one logged-in user to another without logging out, it is best practice for only one user to be logged in at a time.

Common Practices to Follow and Background Processes to Disable

Please follow the steps in the table below during device set up.

Table 2 - MacOS Machines

Common Background Processes to Disable	Common Practices to Follow
• Siri • Handoff on Mac Devices • Fast User Switching on Windows and Mac • Sticky keys and Filter keys on Windows • Malware Software • Adobe Background Processes • Disable workstation lockout application	• Disable keyboard shortcuts • Avoid software updates, patching and data backups • Remove bandwidth throttling on ports 80/443 • Minimize and turn off network bandwidth intensive programs • Plug headsets in prior to launching TDS (for Text-to-Speech students only)

Apple iPad Installation

Automatic Assessment Configuration (AAC) should be used for the installation and configuration of iPads. Using AAC, necessary restrictions will be automatically set using the instructions below.

Automatic Assessment Configuration

AAC is recommended for secure testing in the **Questar Assessment for Students** app. AAC will automatically be enabled when launching the app.

Use the following steps as a guide for configuring devices using AAC.

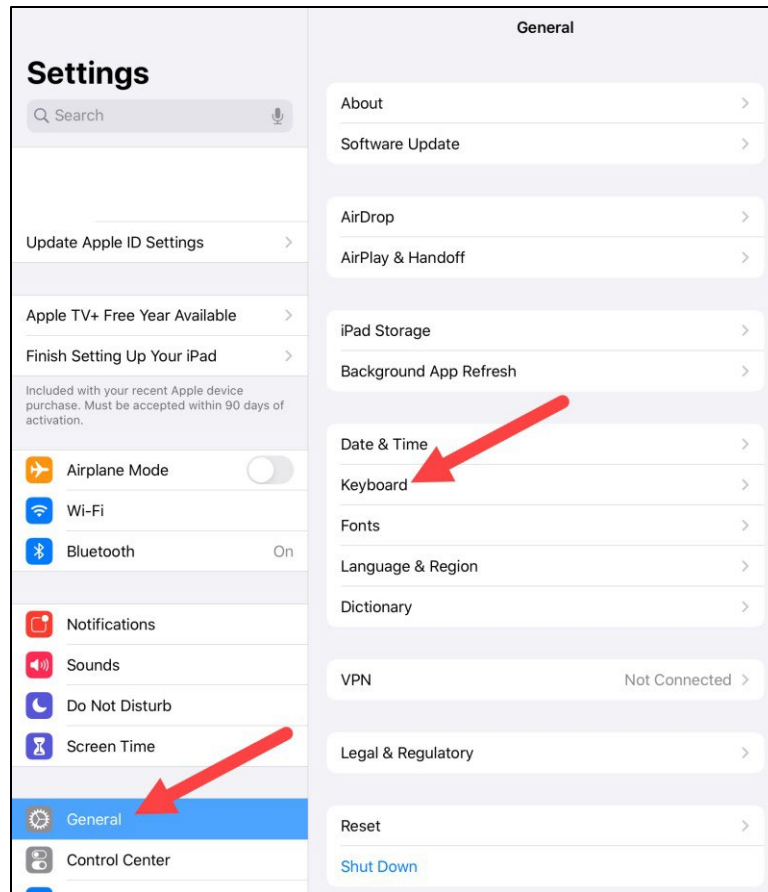
- 1) Download and install the free *Questar Assessments for Students* app from the App store.
- 2) When using AAC, the standard Apple QWERTY on-screen keyboard must be installed and enabled. If a third-party on-screen keyboard is installed, students may not have a keyboard that will be able to be used for testing.

Use the following steps to choose the standard Apple QWERTY keyboard:

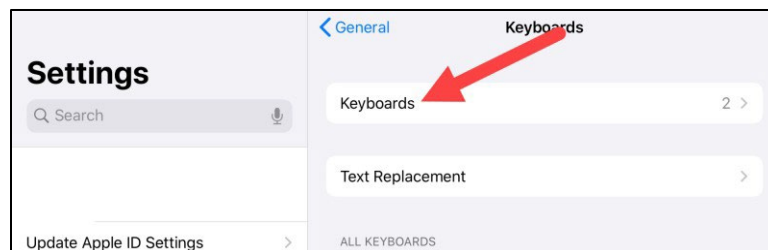
- a) From the iPadOS home page select **Settings**.



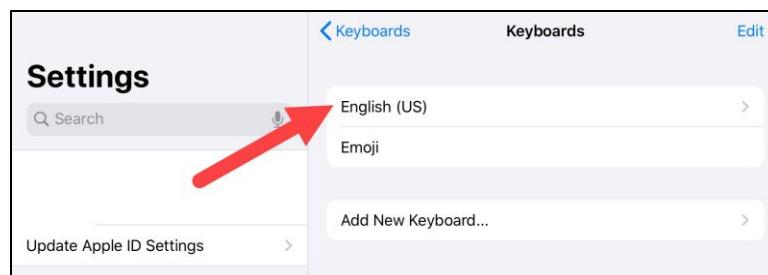
b) From the *Settings* menu, select **General**, then select **Keyboard**.



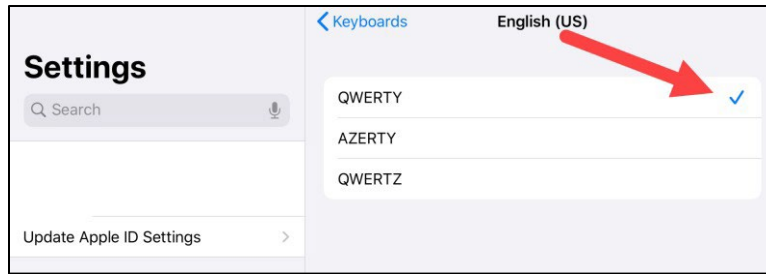
c) Select Keyboards.



d) Select English (US).

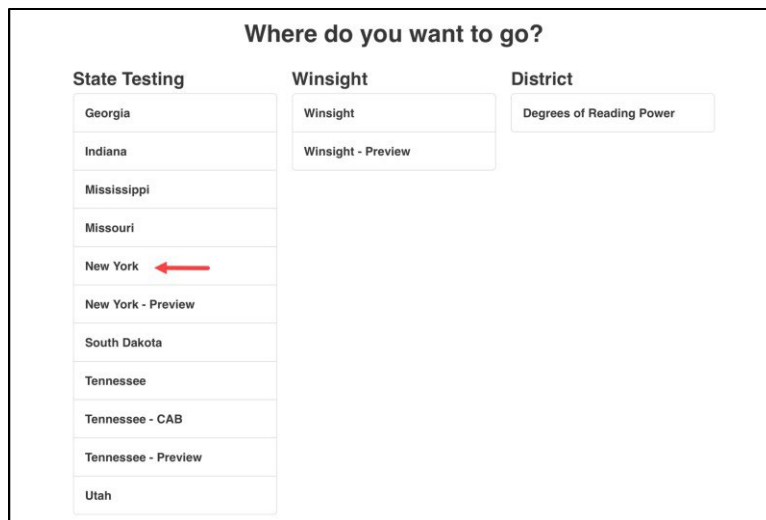


- e) Ensure **QWERTY** is selected from the available options.



AAC will automatically set other necessary restrictions.

- 3) After launching the app, select **New York** from the “Where do you want to go?” page.



- 4) The Log in page displays.



The image shows a login screen for the New York Statewide Assessment. At the top, the text "New York Statewide Assessment" is displayed in a large, dark font. Below it, in a smaller, lighter blue font, is "Powered by Nextera™". The login fields are centered and include a "NYSSIS ID" label above a text input field containing the placeholder "NYSSIS ID". Below this is a "Password" label above a password input field containing the placeholder "Password" and a toggle icon (an eye). There are two blue buttons: "Sign In" and "Exit". At the bottom center is the Questar logo, which consists of a colorful geometric design above the word "Questar®".

Additional Resources

For further information about iPad assessment configuration options, contact your MDM vendor or refer to [Apple Support \(https://support.apple.com/en-us/HT204775\)](https://support.apple.com/en-us/HT204775).

For more information about using iPads for assessments, contact NWEA Customer Support.

Chromebooks Installation

End of support for Chrome apps:

For the 2026-27 administration, the Chromebook Secure Browser has been updated from a Chrome App to a Progressive Web App (PWA) due to Google's deprecation of Chrome Apps.

The new Secure Browser will be installed through the Google Admin Console on managed devices. Testing Coordinators will install the application and accompanying extension. The app will then be managed through kiosk mode. Coordinators should remove the legacy Chrome App.

Testing Coordinators are advised to make the transition to modern web technologies.

For additional information please visit:

<https://support.google.com/chrome/a/answer/15950395?hl=en>.

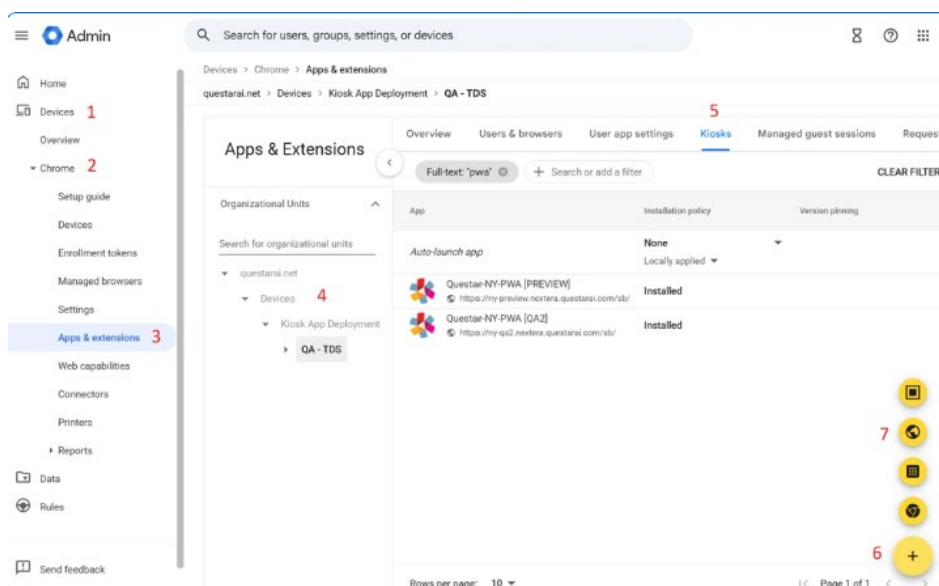
More information can be found below and on Nextera Admin under the Help Downloads tab.

Install Questar PWA Secure Browser and Supporting Extension of Chromebooks

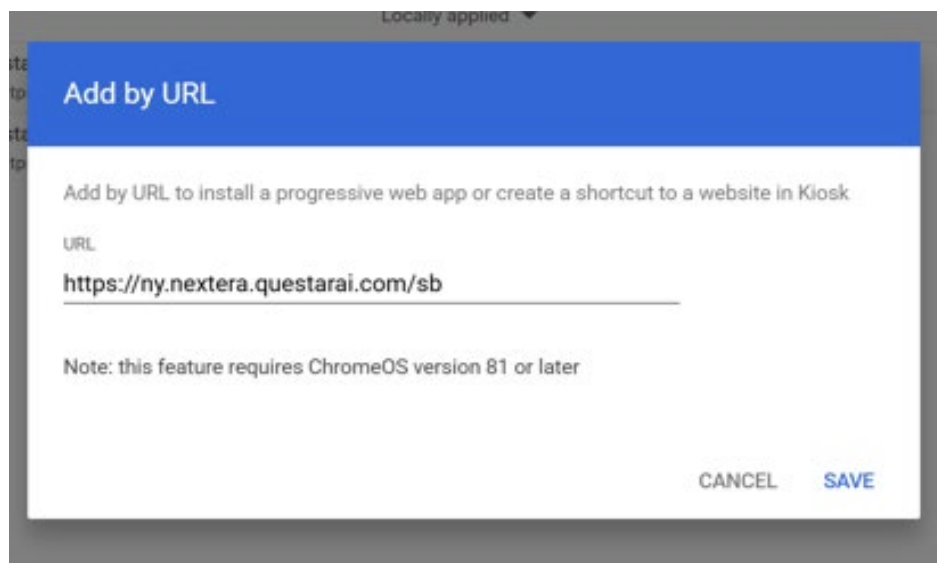
Use this procedure to install the Questar-NY-PWA Secure Browser and its supporting Chrome extension for a Chromebook organizational unit.

1. In the Google Admin console, go to **Devices** → **Chrome** → **Apps & Extensions** → **Kiosks**.

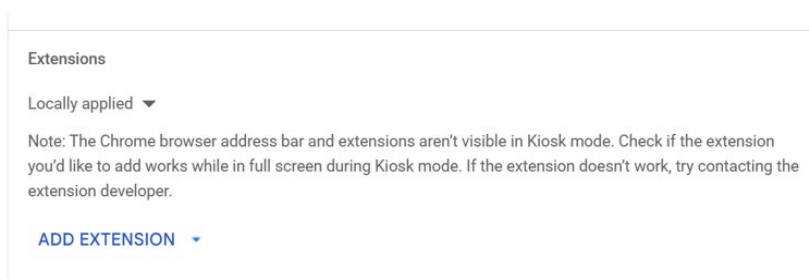
Select the organizational unit where the PWA will be installed, select the + button, and choose **Add by URL**.



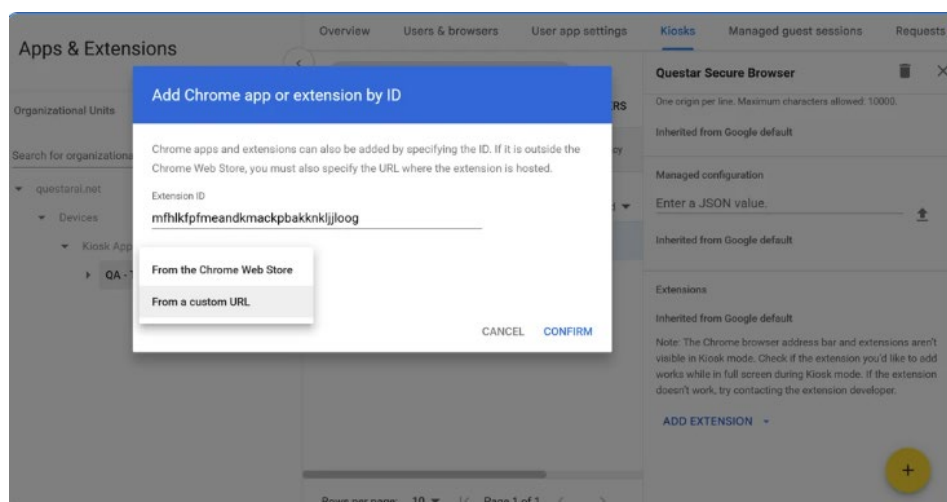
2. In the **Add by URL** window, enter the following URL and select **Save**:
<https://ny.nextera.questarai.com/sb>



3. Select **Agree** to grant the permissions required by the PWA.
4. After the PWA is added, select **Add Extension** → **Add from a custom URL**.



5. In the **Add Chrome app or extension by ID** window, open the drop-down menu and select **From a custom URL**.



6. Enter the following information, then select **Confirm**:

- o **Extension ID:** mfhlkfpfmeandkmackpbakknkljjloog
- o **URL:** <https://ny.nextera.questarai.com/sbext/update.xml>

Add Chrome app or extension by ID

Chrome apps and extensions can also be added by specifying the ID. If it is outside the Chrome Web Store, you must also specify the URL where the extension is hosted.

Extension ID

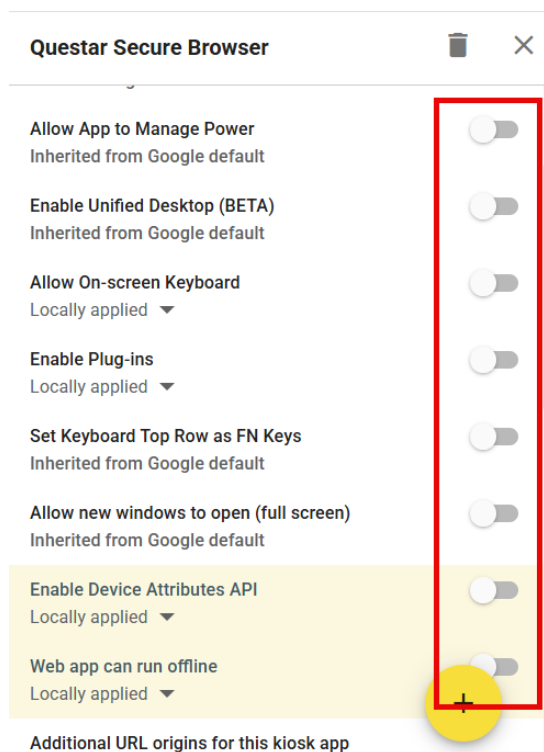
mfhlkfpfmeandkmackpbakknkljjloog

From a custom URL

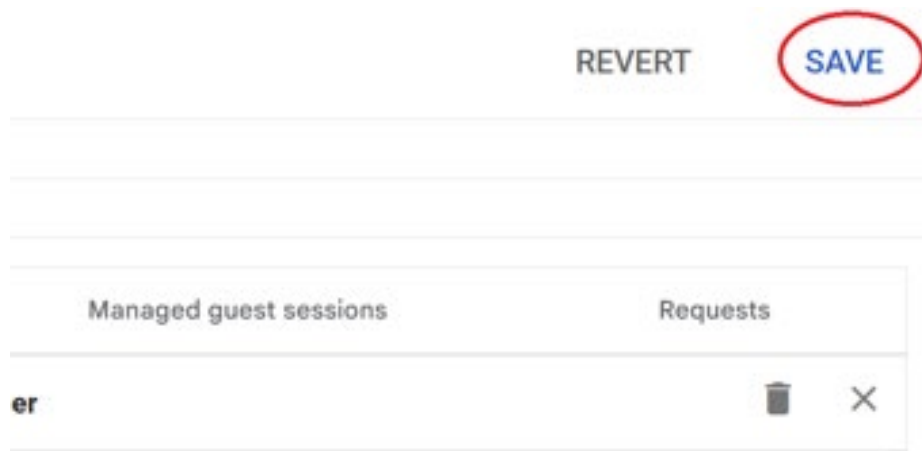
URL

<https://ny.nextera.questarai.com/sbext/update.xml>

CANCEL CONFIRM



7. After the extension is added, select **Save** (upper right corner).



After the configuration is complete, verify that **Questar Secure Browser** appears in the Chromebook kiosk apps list.

Note: Before saving, ensure nothing is toggled ON.

Note: The name of the app will change to Questar-NY-PWA after first load.

Verification checklist

- The PWA URL was added to the correct organizational unit.
- Required PWA permissions were accepted.
- The supporting extension was added from the custom update URL.
- Questar-NY-PWA (or Questar Secure Browser) appears in the kiosk apps list.

IMPORTANT: Google does not support the Questar Secure Browser being used in un-managed kiosk mode. Chromebooks must be managed by Google Admin Console to install and use the Questar Secure Browser.

If installation is attempted on an un-managed device, you may receive an error stating “App with ‘kiosk only’ manifest attribute must be installed in Chrome OS kiosk mode”.

First, you must sign in to your Google Admin console as an Administrator. Please use the app ID in conjunction with the following scenarios:

App ID: gdehbmmmjkddebbonbmknngoigkleicpec

Assessments can be delivered on Chromebooks as a Kiosk app. Instructions for installation via Google Support can be found below in the Kiosk App Installation link. We recommend installing the Kiosk App with Auto-Launch not configured if students will be using devices outside of testing:

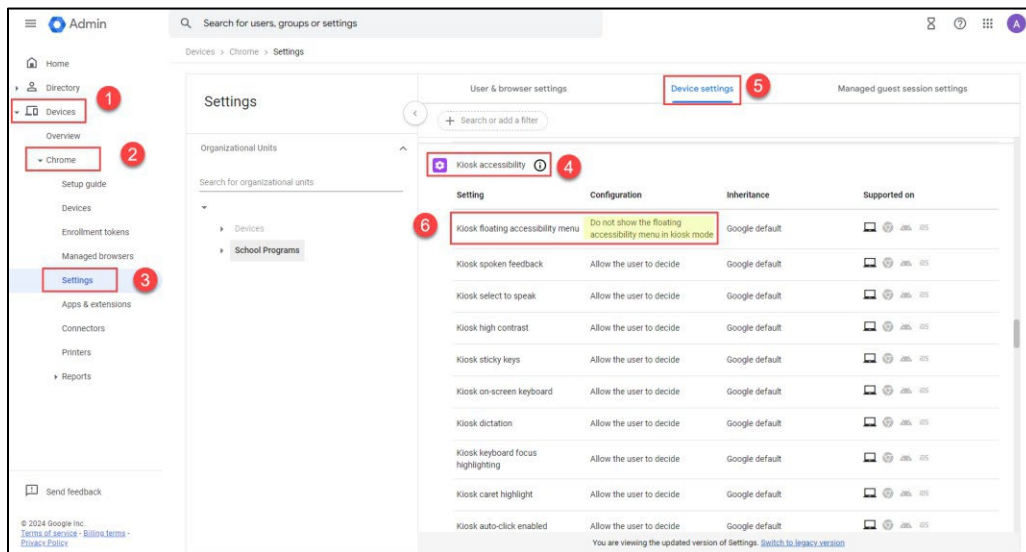
- [Kiosk App Installation](#): The exam is delivered on Chromebooks set up as a "Single App Kiosk". In this method, the testing provider creates the exam as a Chrome kiosk app, and this exam app runs in a full screen mode.

Preparing Chromebooks

If you are using the downloaded app, the Kiosk app is available as soon as the Chromebook is turned on. Access the app from the lower left corner of the screen.

Note: Prior to the test administration window opening, ensure “Do not erase local user data” is set under the Google Admin Console. This setting is located at Devices, Settings, Device; scroll down to Sign In Settings and look for User Data.

Note: Prior to the test administration window opening, ensure “Do not show the floating accessibility menu in Kiosk mode” is set. Please follow these steps in Google Admin: Devices > Chrome > Settings > Kiosk accessibility > Device Settings > Kiosk floating accessibility menu



Please follow these steps in Google Admin: Devices > Chrome > Settings > Device Settings > Kiosk Select to Speak > Select “Disable select to speak”.

Accessibility Settings

Text-To-Speech

Text-to-Speech uses Amazon Polly and requires an Internet connection. Technology Coordinators will not need to install any additional programs for Text-to-Speech functionality.

Note: Text-to-Speech (TTS) requires an Internet connection. TTS will be unavailable until the Internet connection is restored. When the Internet connection is restored, the student with the TTS accommodation will be able to select play and TTS will load again.

Speech-To-Text

The Speech to Text accommodation has been made available in the Test Delivery System through AWS' transcription service (Standard Streaming only). This accommodation will be available on all ELA constructed-response items. The accommodation allows a student to transcribe their spoken response to text. Once transcribed to text the student can further edit their extended text response. Currently this accommodation is available on ELA constructed-response items only.

Use of the feature requires the student be set up with the Speech to Text accommodation for ELA in the Nextera Admin. Students who are assigned in Nextera admin with the speech to text accommodation will see a new microphone icon in the Extend Text Entry tool bar.

Once you have used the Site Setup tools to determine there is adequate available bandwidth, ensure readiness regarding other upstream network devices (e.g., firewalls, proxy servers, Internet content filters).

Required to use:

- Speech-to-Text requires a stable internet connection.
- The student's device must be set to allow access to the microphone, and the device should be set to a suitable volume level.
- The student's device time (clock) must be set to the correct time zone and accurate.
- Confirm all devices are updated with the most recent Secure Browser.

Note: An Error Message could display during the microphone test if you have not whitelisted the following addresses:

- transcribestreaming.us-west-2.amazonaws.com
- cognito-identity.us-west-2.amazonaws.com

For additional guidance, please reference the Speech-to-Text QRG:

https://cbtsupport.nysed.gov/hc/en-us/article_attachments/30592587618189

If after troubleshooting as well as clearing cache, checking bandwidth, and trying a new device there are still issues, have the student pause testing, gather the details below and contact NWEA Customer Service at 1-866-997-0695. Remind schools to have the device information as well as the OS version ready to share.

Additional Settings

Please follow the steps below to ensure devices have all necessary safeguards in place.

Disable Sticky Keys and Filter Keys: Windows

Disable Sticky Keys

Sticky Keys enables users to enter key combinations in sequence one at a time instead of simultaneously. This feature is available on Windows machines. Please disable Sticky Keys using the process below.

- 1) Open the **Control Panel**.
- 2) Open the **Ease of Access Center**.
- 3) Select **Make the keyboard easier to use**.
- 4) Uncheck the **Turn on Sticky Keys** check box.
- 5) Select **Set up Sticky Keys**.
- 6) Uncheck **Turn on Sticky Keys when SHIFT is pressed five times**.
- 7) Select **select**.

Disable Filter Keys

Filter Keys tell the keyboard to ignore brief or repeated keystrokes. This feature is available on Windows machines. Please disable Filter Keys using the process below.

- 1) Open the **Control Panel**.
- 2) Open the **Ease of Access Center**.
- 3) Select **Make the keyboard easier to use**.
- 4) Uncheck the **Turn on Filter Keys** check box.
- 5) Select **Set up Filter Keys**.
- 6) Uncheck **Turn on Filter Keys when right SHIFT is pressed for 8 seconds** check box.
- 7) Select **OK**.

Disable Alexa/Cortana: Windows

Disable Alexa

If you have downloaded Alexa, uninstall the Alexa application using the following steps:

- 1) Type “uninstall” in the **Windows** search box and select **Add or remove programs** from the search results.
- 2) Locate and select **Amazon Alexa** and select **Uninstall**
- 3) Follow the on-screen instructions to uninstall the Amazon Alexa application.

Disable Cortana

- 1) From **Start**, type **gpedit.msc**.
- 2) Select **Apps** from the sidebar on the right.
- 3) Select **gpedit.msc** in the main window.
- 4) In the left side of the *Local Group Policy Editor* window, expand the following options: **Local Computer Policy -> Computer Configuration -> Administrative Templates -> Windows Components** > then locate and select **Search**.
- 5) On the right, use the secondary mouse button to select **Allow Cortana**.
- 6) In the Allow Cortana dialogue box, select “**Disabled**” and then select **OK**.
- 7) Close the *Local Group Policy Editor* and open the Run dialog box (**Windows + R**). Enter **gpupdate/force** and select **OK**.

Configuring USB Mouse with iPad

- 1) Select the **Gear** icon to access **Settings**.
- 2) Select **Accessibility**.
- 3) Select **Touch** from the *Accessibility* menu.
- 4) Select **Assistive Touch**.
- 5) Scroll down to the *Pointer Devices* section.
- 6) Select **Devices**.
- 7) Select device name (e.g., USB Optical Mouse).
- 8) Select **Button 1**.
- 9) Select **Long Select**.

Disable Fast User Switching: Windows

Fast User Switching allows multiple users to be logged into one device and switch between the user profiles quickly. This feature is available on Windows and Mac machines. Please disable Fast User Switching using one of the processes below.

Windows

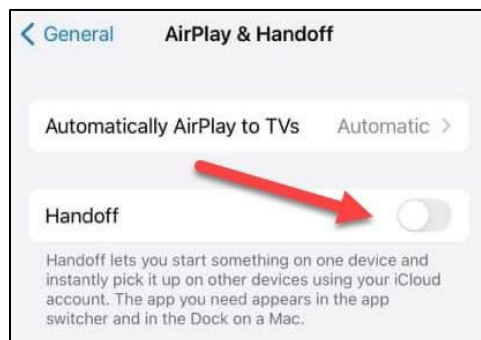
- 1) From **Start**, type **gpedit.msc**.
- 2) Select **Apps** from the sidebar on the right.
- 3) Select **gpedit.msc** in the main window.
- 4) In the left side of the *Local Group Policy Editor* window, expand the following options: **Local Computer Policy -> Computer Configuration -> Administrative Templates -> System**, then locate and select **Logon**.
- 5) On the right, double-select **Hide entry points for Fast User Switching**.
- 6) In the *Hide entry points for Fast User Switching* dialogue box, select **Enabled** and select **OK**.
- 7) Close the *Local Group Policy Editor* and open the Run dialog box (Windows + R). Enter **gpupdate/force** and select **OK**.

Disable Handoff on iPad Devices

When your iPadOS devices are within Bluetooth range of each other, they can automatically “hand off” what you are doing from one device to another. On newer versions of iPadOS, this feature includes something called the Universal Clipboard that allows one Apple device to copy and paste to a different Apple device using Handoff.

iPadOS

- 1) Navigate to **Settings**.
- 2) Choose **General**.
- 3) Choose **AirPlay & Handoff**.
- 4) Ensure **Handoff** is turned off. (The pill switch will turn grey/white when turned off and is green when turned on.)



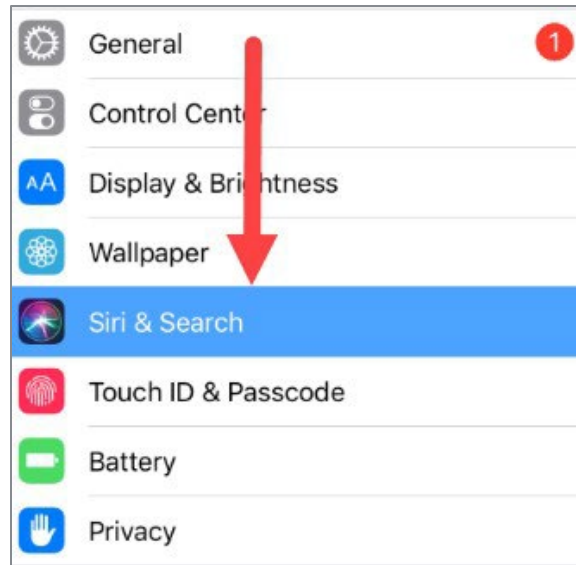
Note: The emoji keyboard is not compatible with the assessments on iPads and should be removed. Remove the keyboard under **Settings -> General -> Keyboards -> Keyboards** (inside the keyboards option). Select **Edit** in the top right corner and then select the  symbol next to the Emoji Keyboard. Select **Delete** after it opens.

Disable Siri: iPadOS

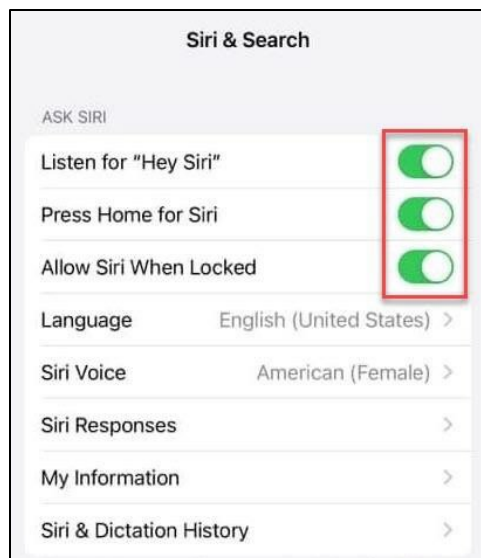
- 1) Select **Settings**.



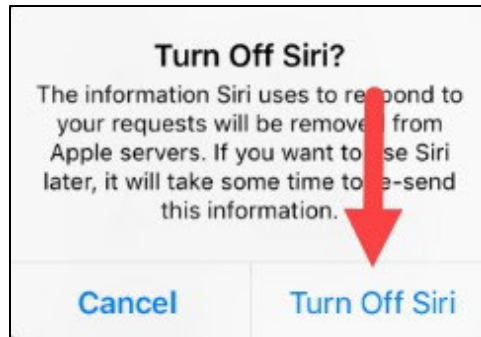
- 2) Select **Siri & Search**.



- 3) Slide off all pill boxes for **Listen for “Hey Siri”**, **Press Home for Siri**, and **Allow Siri when Locked**. The pill boxes will turn grey/white when off (previously green).



- 4) A pop-up message displays. Select **Turn Off Siri**.



Disable Scribble: iPadOS

Scribble should be disabled. New York only supports the use of basic styluses during testing, and digital pens like the Apple Pencil introduce capabilities that go beyond the functionality of an average stylus.

To disable Scribble on iPadOS using MDM, you can deploy a configuration profile that turns off this feature. This prevents handwriting-to-text conversion when an Apple Pencil is used.

Steps to Disable Scribble via MDM:

- 1) Open your MDM solution: Log in to your MDM provider's console (e.g., Jamf, Kandji, Intune).
- 2) Create or edit a configuration profile: Select iOS/iPadOS and create a new Device Configuration Profile.
- 3) Configure Restrictions: Navigate to the *Restrictions* payload.
- 4) Disable Scribble: Locate the Apple Pencil settings and toggle off Allow Scribble.
- 5) Deploy: Save and assign the profile to the appropriate devices.

Once deployed, the Scribble setting will be grayed out or removed, ensuring users cannot enable it.

If adjustments need to be made directly on a device, Scribble can be turned off manually by going to Settings > Apple Pencil and switching off Scribble.

Disable Select to Speak: Chromebooks

The select to speak feature on the Chromebook needs to be turned off. On a Chromebook, a user can use ESC + Search + S and highlight certain text to allow speech to play. This feature is not allowed during testing.

Please follow these steps to turn off this feature:

Navigate to Google Admin: Devices > Chrome > Settings > Device Settings > Kiosk Select to Speak > Select "Disable select to speak".

Disable Dictation: Chromebooks

The dictation feature on the Chromebook needs to be turned off. On a Chromebook, a user can use the shortcut Search + D or Launcher + D to activate the microphone. This feature is not allowed during testing.

Please follow these steps to turn off this feature:

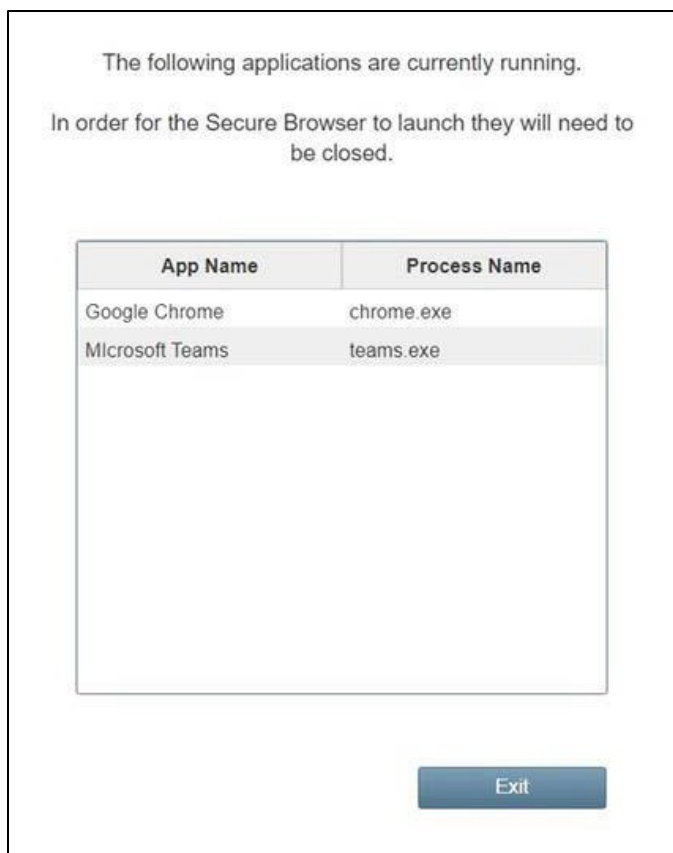
Navigate to Google Admin: Devices > Chrome > Settings> Device Settings > Kiosk Dictation > Select “Disable Dictation”.

Disable All Apps: Windows and MacOS

All applications must be disabled prior to testing. The Questar Secure Browser cannot open until all apps (e.g., meeting apps, classroom apps, browsers, email, etc.) are closed.

Note: You may need to disable multiple apps before the Questar Secure Browser can be launched.

If an app has not been disabled, students cannot access the Questar Secure Browser and the below message will display. It is best to close all apps prior to accessing the Questar Secure Browser.



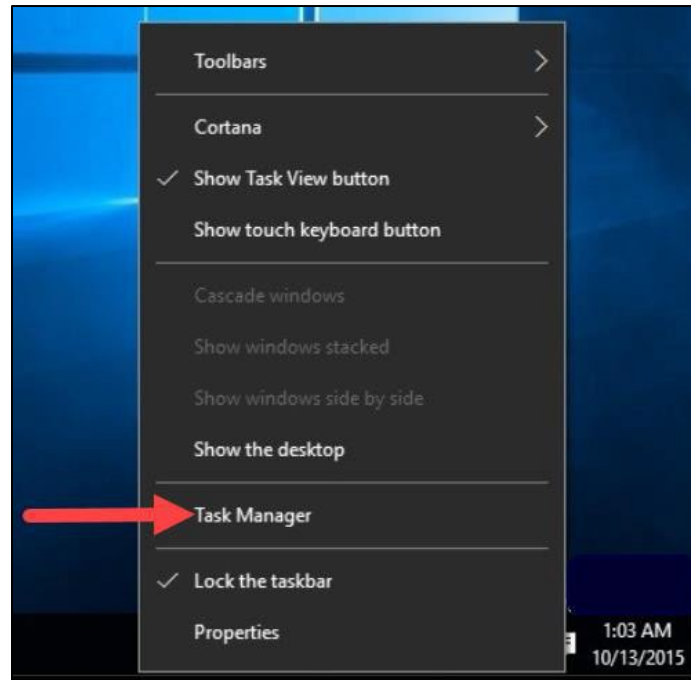
Note: If you do not have access to the **Task Manager** using Windows or Activity Monitor using Mac devices, contact your technology coordinator to complete the steps outlined within this document.

Windows: Opening Task Manager

To use *Task Manager* to view and close processes, you first need to know how to open the tool. There are different ways to access *Task Manager*. Each numbered example below is a different option to access Task Manager on Windows devices:

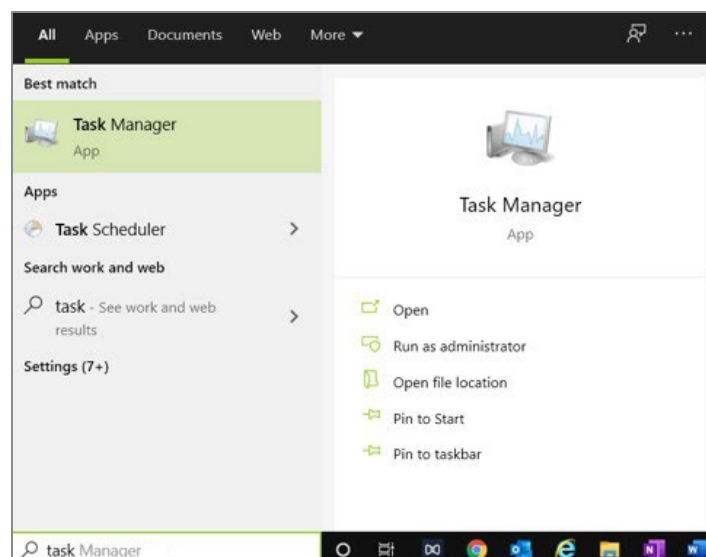
Option 1

- 1) Select the **clock** in the bottom right corner of the screen using the secondary mouse button and select **Task Manager**.



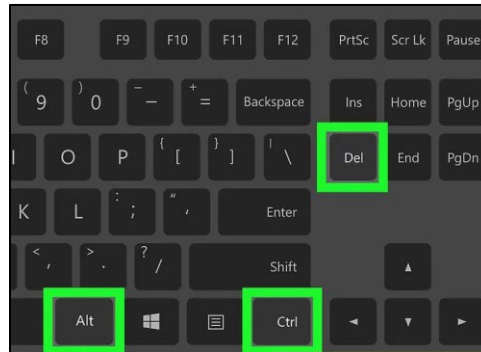
Option 2

- 1) Open **Start**, complete a search for **Task Manager**, then select the result.



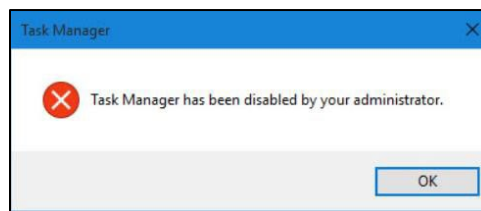
Option 3

- 1) Use the **Ctrl + Alt + Del** keyboard shortcut and select **Task Manager**.



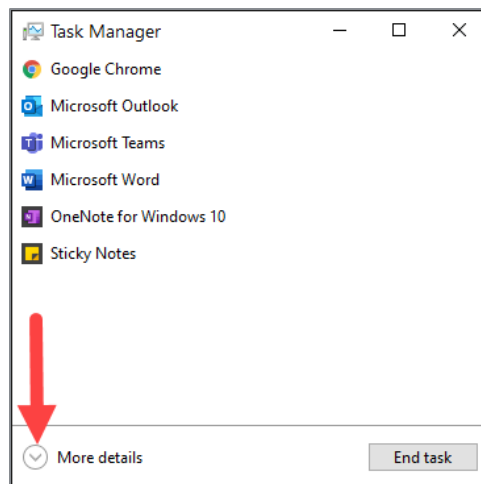
Task Manager Possible Solutions

The device you are on may have security settings that will not allow anyone to access *Task Manager* without Administrator rights. If *Task Manager* will not open, or you receive the error message below, contact your IT administrator.

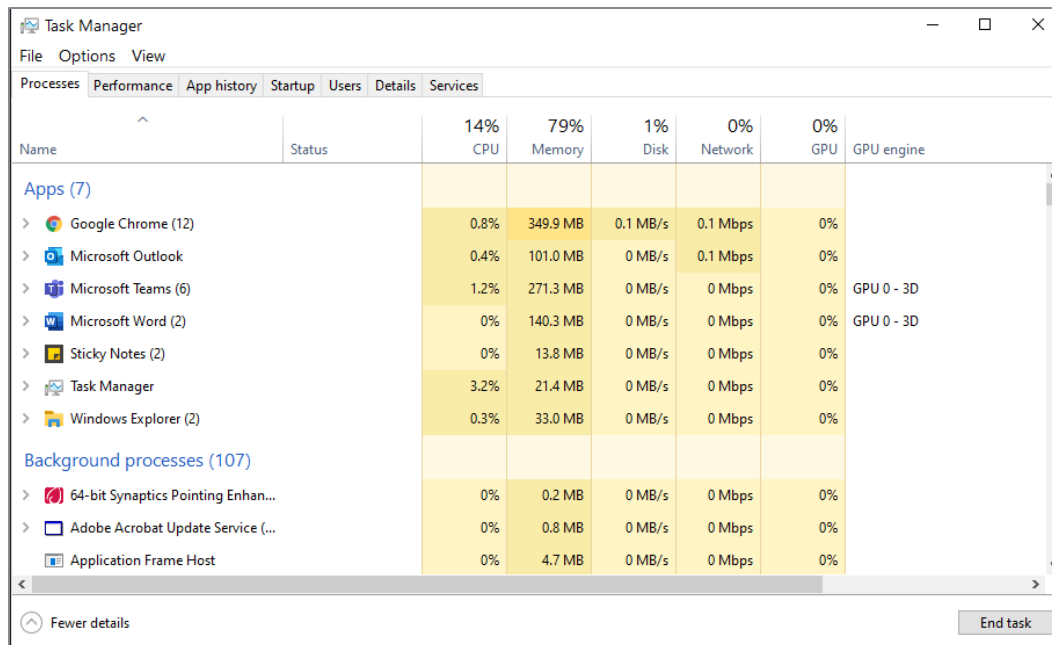


If this is your first time opening *Task Manager*, the tool may open in compact mode, which only lists running applications.

Select **More details** to access *Task Manager* in advanced mode.

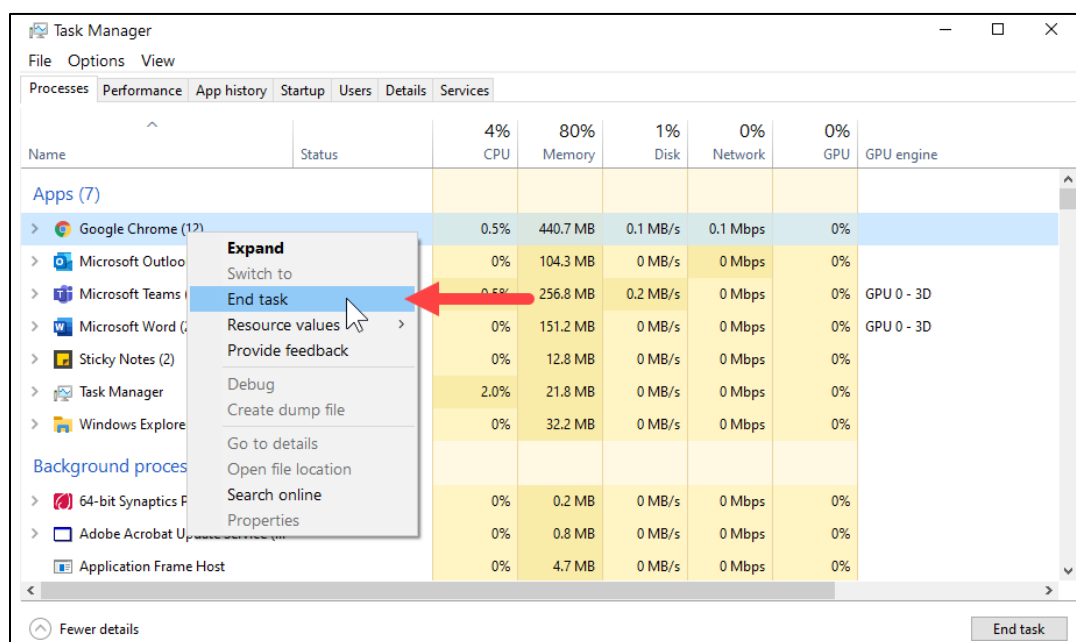


Task Manager opens in advanced mode.



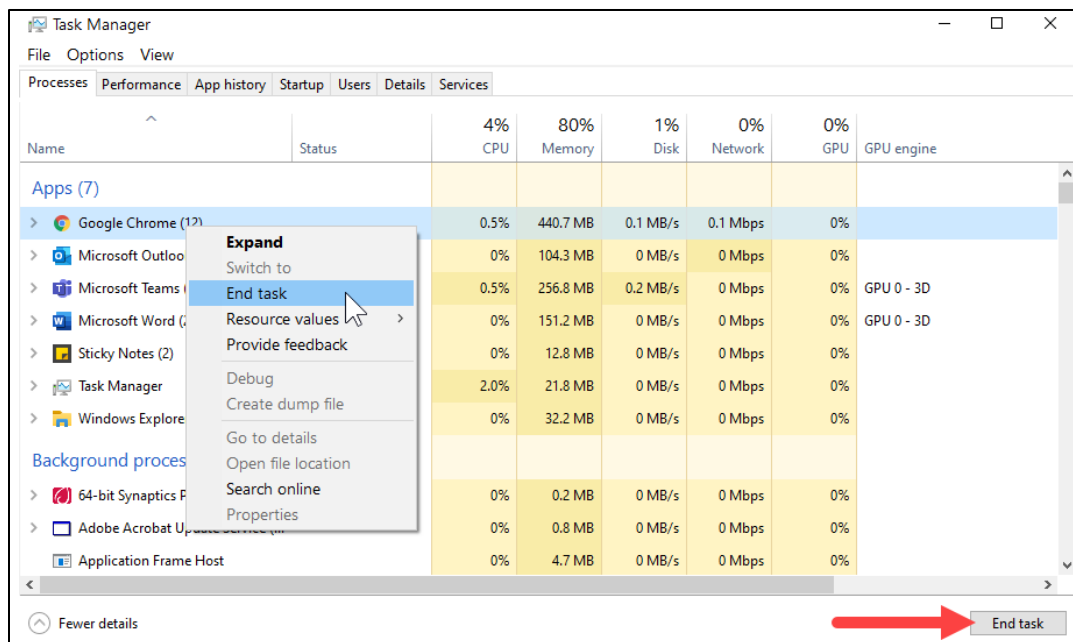
Windows: How to Close Applications or Processes Using Task Manager

- 1) Locate the application or process that displays in the error message provided by the Questar Secure Browser.
- 2) After you identify the application or process you would like to close, select the application or process using the secondary mouse button, then select **End task** to close it.

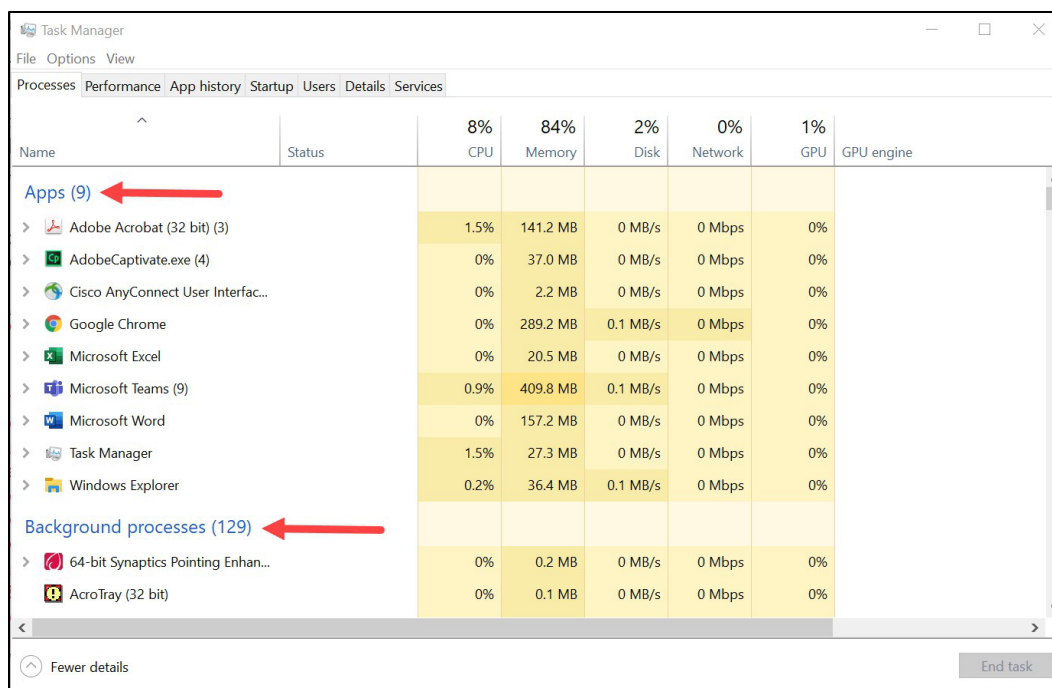


Note: While closing an application or process using the Task Manager, you could lose any unsaved data. It is recommended to save your data before closing an application or process, if possible.

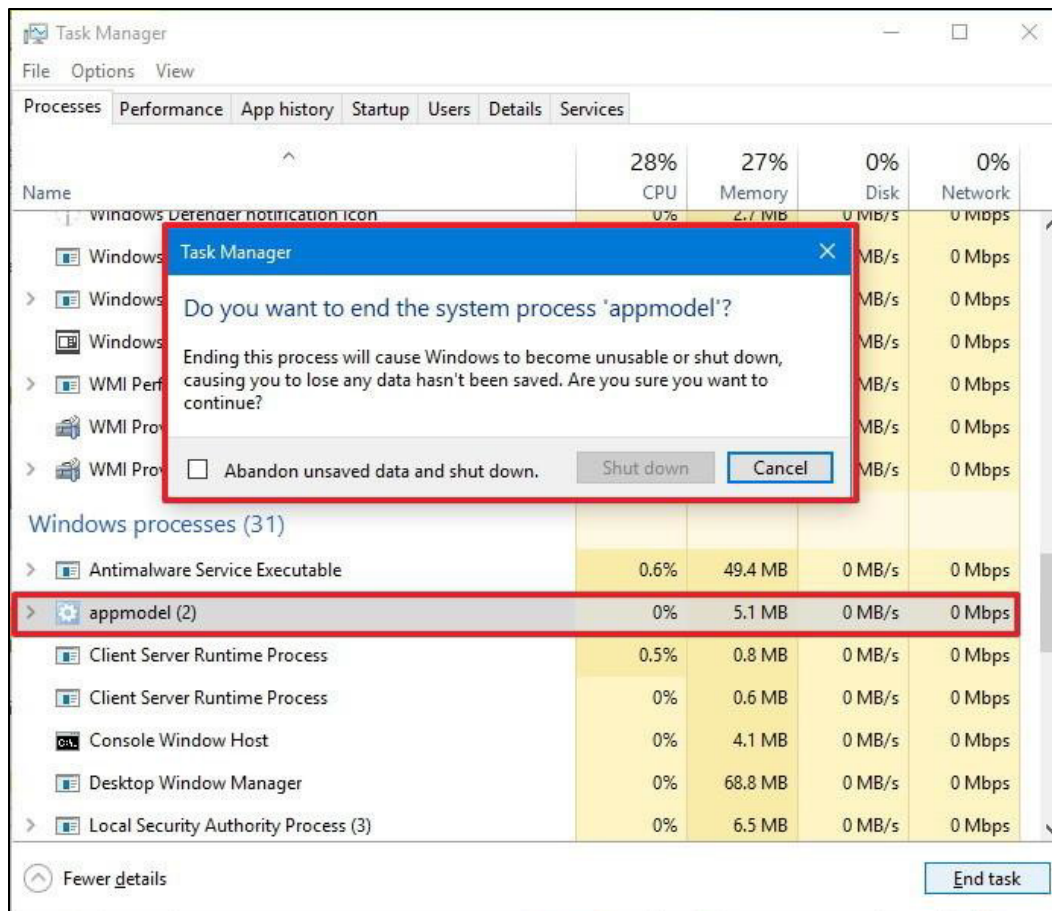
Alternatively, you can simply select the item and select **End task** in the bottom-right corner.



Note: You may have to close both the application and background process to fully close the program that is running and blocking the launch of the Questar Secure Browser.



- 1) If you need to close a process rather than an application, and you attempt to close an essential system process that should not be closed, you will get a Warning message from Windows.



- 2) After closing the application or process that was not allowing the Questar Secure Browser to launch, you may close task manager. Now, launch the Questar Secure Browser. If you receive additional notifications to close background apps or processes, repeat the previous steps. When conflicting apps and processes have been closed, the Questar Secure Browser will launch, and the student will be able to enter their login information.

Microsoft Teams

As a first step to disable the Microsoft Teams application, users need to follow the steps below:

- 1) Open **Microsoft Teams** and sign-in.
- 2) Select the **Teams** icon in the system tray using the secondary mouse button and select **Quit**.
- 3) Attempt to launch the Questar Secure Browser.

If still unable to access the Questar Secure Browser, then follow the steps below:

- 1) Open **Task Manager**. (CTRL + ALT + DELETE)
- 2) Go to the **Details** tab.
- 3) Select the **Teams app**.
- 4) Select **End Task**.
- 5) Try launching the Questar Secure Browser again.

If still unable to access the Questar Secure Browser, then restart your computer and attempt to launch the Questar Secure Browser.

Additionally, Microsoft Teams is associated with Office 365 and OneDrive. It may be possible to receive a warning about Teams being open even after closing and disabling Teams. In this situation, you will also want to close and disable Office 365 and OneDrive. To close and disable these programs, follow the steps outlined in the section [Windows: How to Close Applications or Processes using Task Manager](#) and select **Office 365** and/or **OneDrive**.

MacOS: How to Close Applications or Processes Using the Activity Monitor

Option 1

- 1) Select these three keys together: **Option**, **Command**, and **Esc** (Escape). (This is similar to pressing **Control-Alt-Delete** on a PC.)



- 2) Select the app in the Force Quit Applications window and select **Force Quit**.

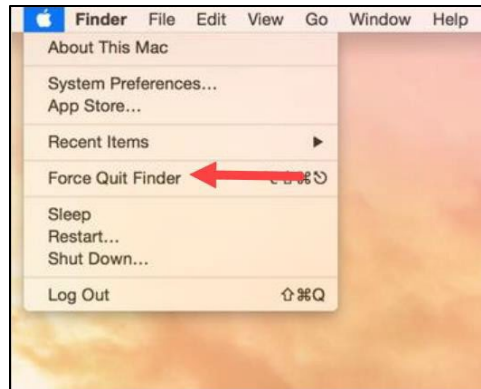


Option 2

- 1) Select the **Apple** menu  in the upper-left corner of your screen.



2) Select **Force Quit Finder** from the menu.



3) Select **Force Quit**.



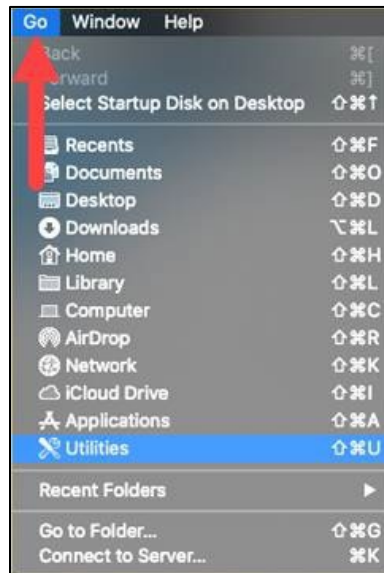
Using Activity Monitor

The following link shows a different way to close an application or process depending on version of MacOS using Activity Monitor.

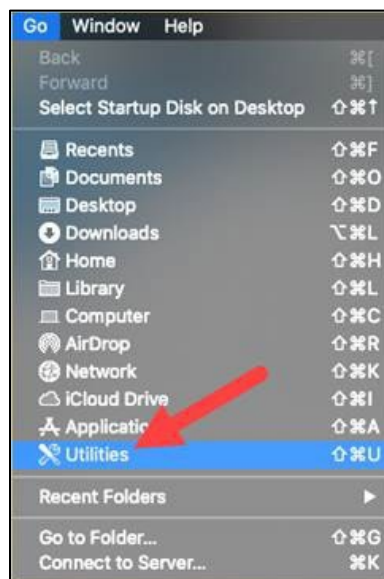
<https://support.apple.com/guide/activity-monitor/quit-a-process-actmntr1002/mac>

Access Activity Monitor by going to the **Utilities** folder and launching the **Activity Monitor** app.

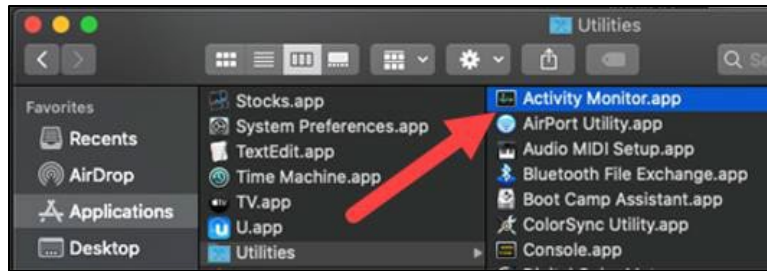
- 1) Select the **Go** menu.



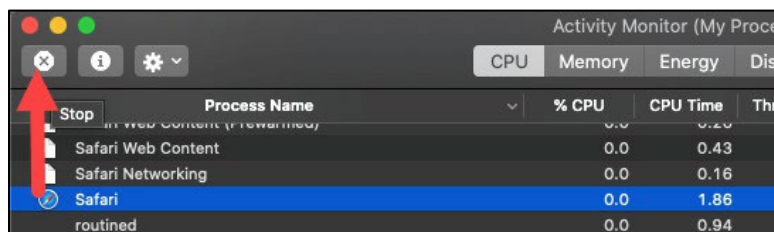
- 2) Select Utilities.



- 3) Select **Activity Monitor.app**.



- 4) Select the application or process shown from the message and select the **stop button** (⏏) to close the selected application or process.



Disable Startup Applications

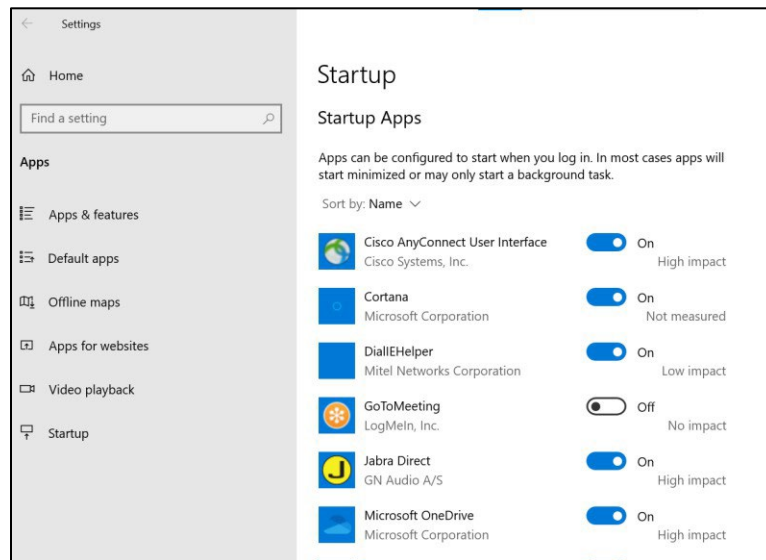
If an application that is on the blocked list is launching on Startup, you may want to disable the application from doing so.

Note: If you find at any point in the steps below that you do not have access, you will need to contact your Technology Coordinator.

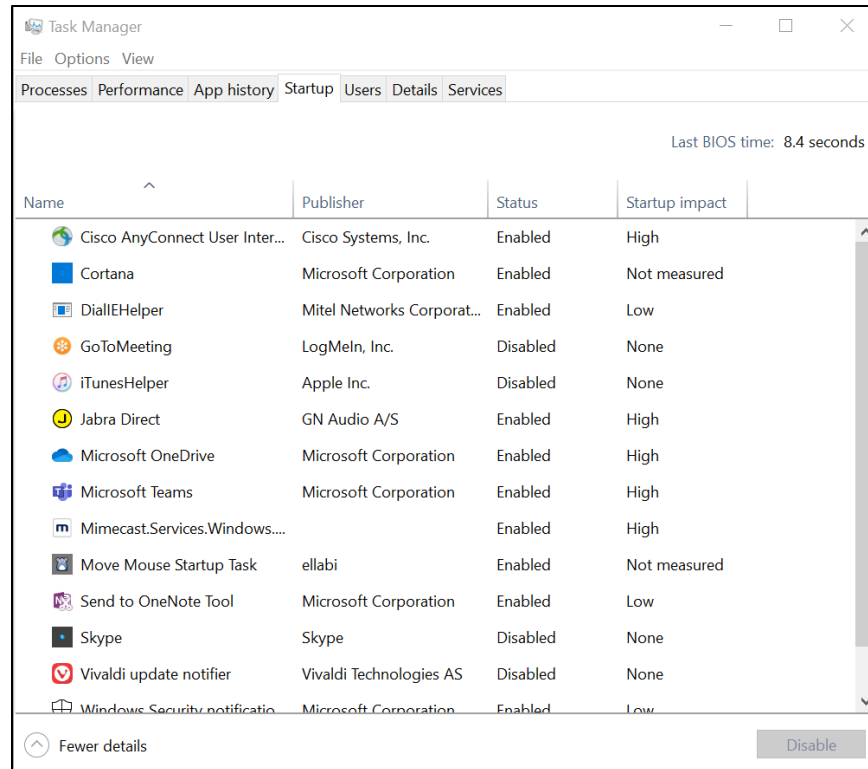
Windows

There are two ways you can change which apps will automatically run at startup in Windows:

- 1) Select the **Start**  button, then select **Settings** () > **Apps** > **Startup**. Make sure any app you want to disable from launching at startup is turned **Off**.



- 2) If you don't see the **Startup** option in Settings, select the **Start** button using the secondary mouse button, select **Task Manager**, then select the **Startup** tab. (If you don't see the Startup tab, select *More details*.) Select the app you want to change, then select **Disable** so it doesn't run.



For further information about how to change which apps run automatically at startup in Windows, refer to [Microsoft Support](https://support.microsoft.com/en-us/windows/change-which-apps-run-automatically-at-startup-in-windows-10-9115d841-735e-488d-e749-9ba301d441e6).

<https://support.microsoft.com/en-us/windows/change-which-apps-run-automatically-at-startup-in-windows-10-9115d841-735e-488d-e749-9ba301d441e6>

MacOS

To remove items that open automatically whenever you log in:

- 1) On your Mac, select **Apple** menu  > **System Preferences**, then select **Users & Groups**.
- 2) Select your user account, then select **Login Items** at the top of the window.

Complete any of the following options:

Remove a login item

- 1) Select the name of the item you want to prevent from opening automatically, then select the **Remove** button below the list.



Temporarily prevent items from opening automatically when you log in

- 1) If you see the login window, select the **Shift** key while you select the **Log In** button, then release the **Shift** key when you see the **Dock**.
- 2) If you don't see the login window, restart your Mac, select and hold the **Shift** key when you see the progress bar in the startup window, then release the **Shift** key after the desktop appears.

For further information about how to remove items automatically when you log in, refer to [Apple Support](https://support.apple.com/guide/mac-help/open-items-automatically-when-you-log-in-mh15189/11.0/mac/11.0) (<https://support.apple.com/guide/mac-help/open-items-automatically-when-you-log-in-mh15189/11.0/mac/11.0>).

Disable AssistiveTouch: iPad Pro

If you have one of the models below, then you will need to disable AssistiveTouch.

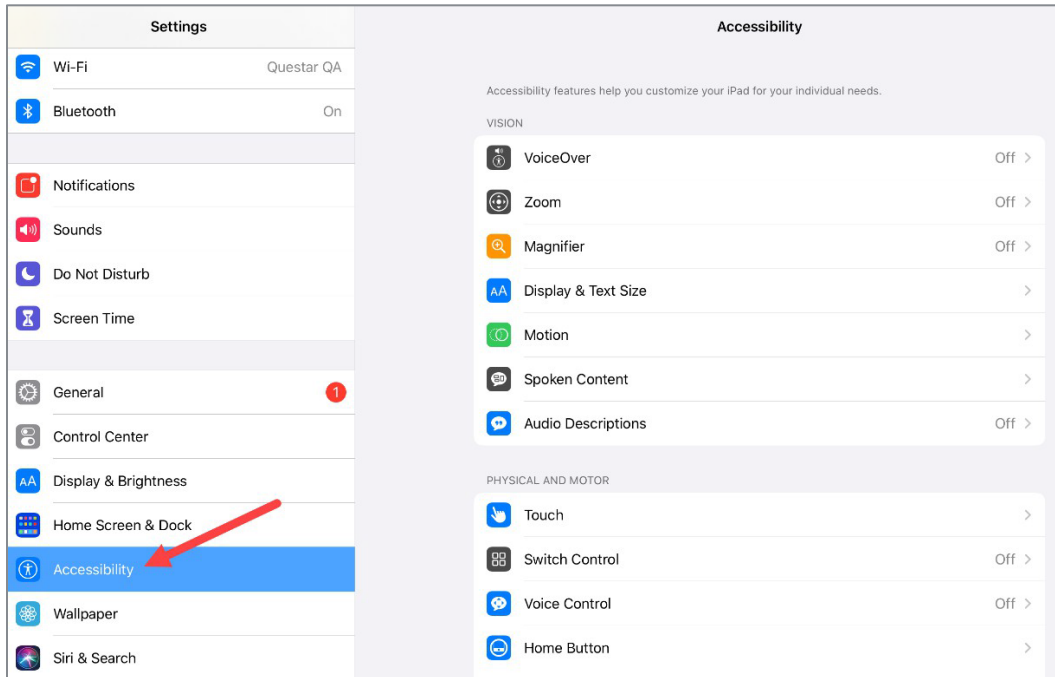
- A1876
- A2014
- A1980
- A2013

Steps for Disabling

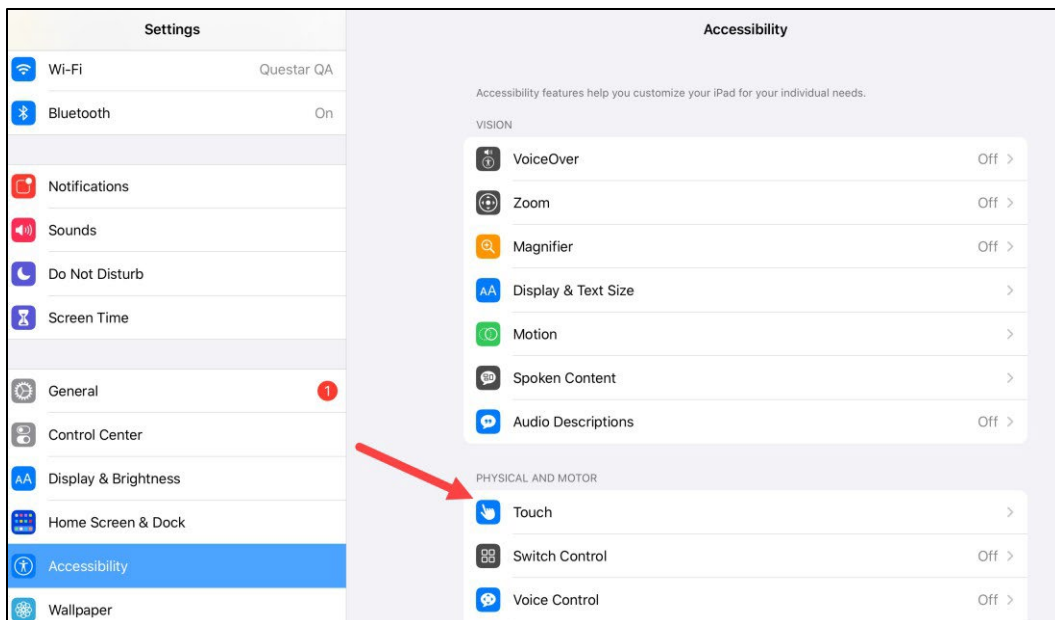
- 1) Select **Settings**.



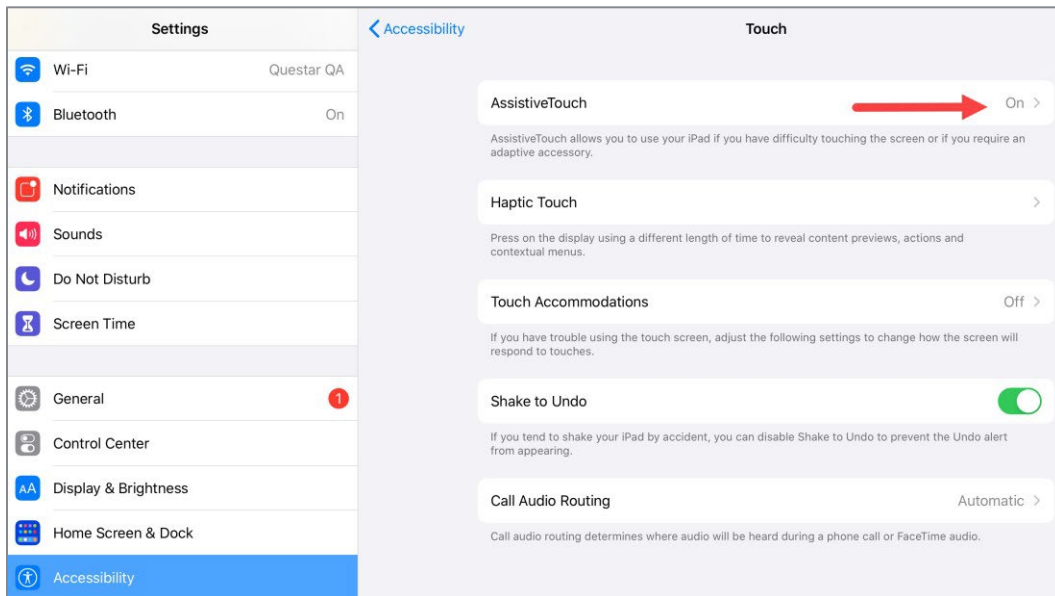
2) Select **Accessibility**.



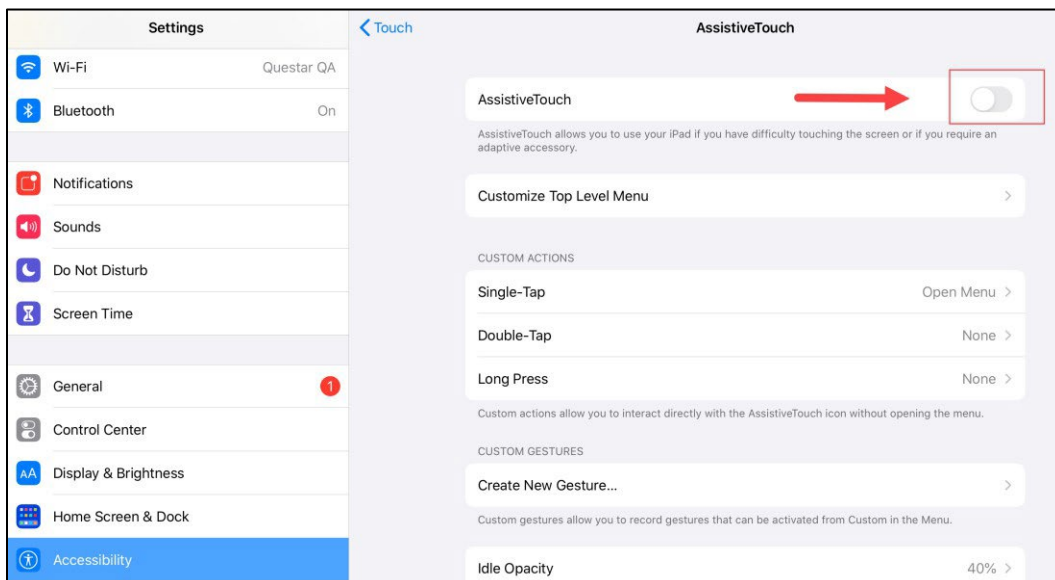
3) Select **Touch**.



4) Select **AssistiveTouch**.



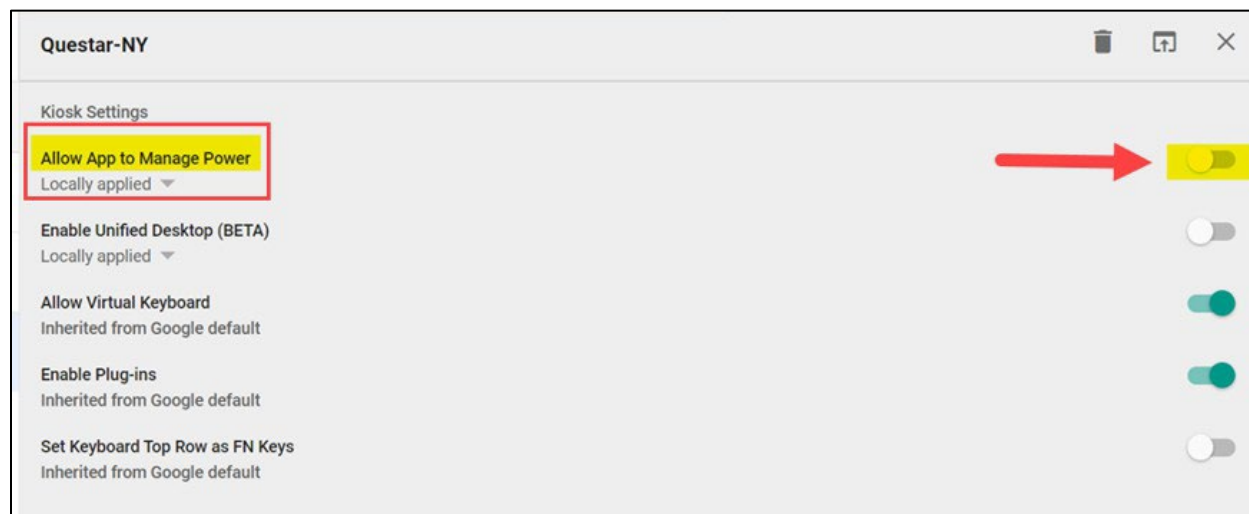
5) Slide to the off position (it will turn grey).



Disable App Power Management: Chromebook

This feature will need to be disabled through your Google Admin Management Console for Chromebook testing devices prior to testing.

- 1) Login to your Google Admin Console.
- 2) Select **Devices** from the Home Screen.
- 3) Select **Chrome** from the left pane.
- 4) Select **Apps & Extensions** from the left pane.
- 5) Select **Kiosks** from the left pane.
- 6) Choose your OU from the left pane.
- 7) Select **Kiosks** on the upper right pane.
- 8) Select the Questar Secure Browser application.
- 9) Set **Allow App to Manage Power** to Off
- 10) Select **Save** on the upper right of the page.

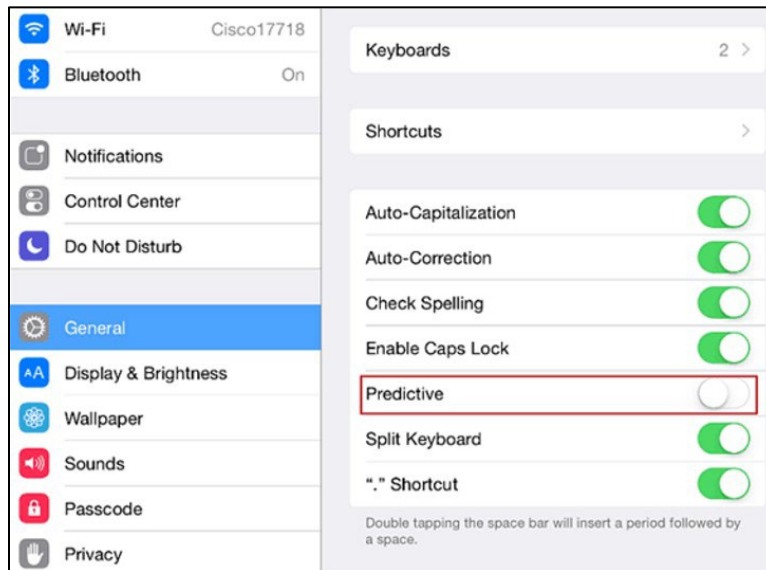


Disable Predictive Text

Predictive text will need to be disabled on student devices prior to the beginning of testing.

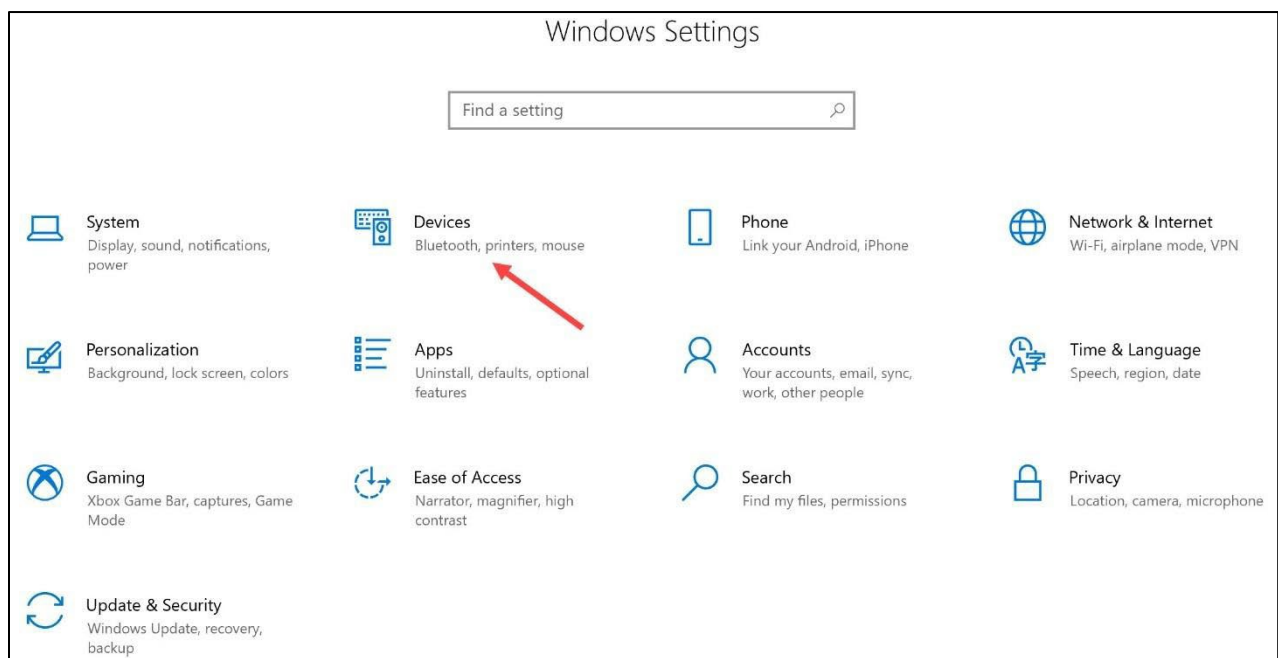
iPad

- 1) Select **Settings**, then **General**.
- 2) Select **Keyboards**.
- 3) Locate the *Predictive* pill-switch and toggle the pill-switch from **Enabled** to **Disabled**.

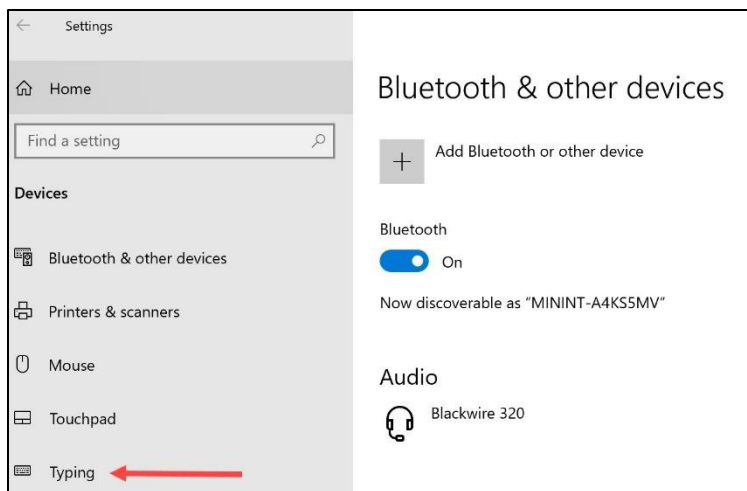


Windows

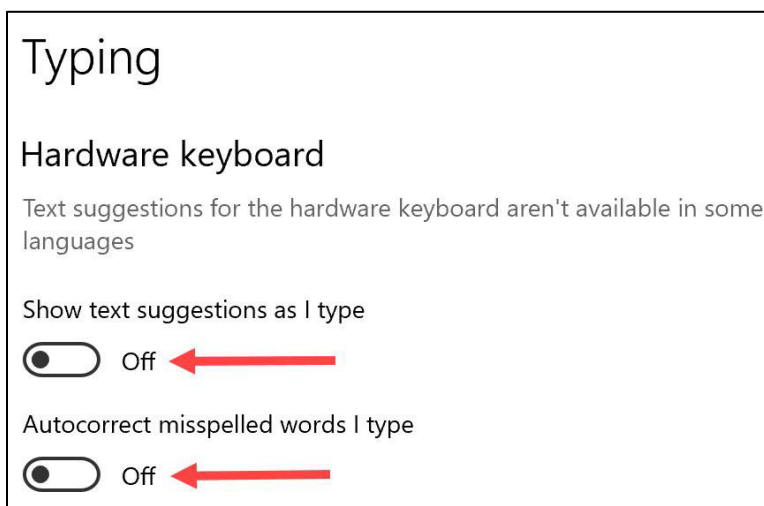
- 1) Select **Settings**, then **Devices**.



2) Select **Typing**.



3) Locate *Hardware keyboard* and toggle the pill-switches to **off**.



Disable Predictive Math

Predictive text will need to be disabled on student devices prior to the beginning of testing. Predictive math is a feature that provides suggestions or solutions to math problems and is available on iPads running iPadOS 18 or later.

You can disable it through Settings > General > Keyboard > Find the “Show Math Results” toggle and toggle the switch to off.

This feature is also accessible in the Calculator app’s Math Notes. The Calculator app’s Math Notes is where a user can solve various math problems and/or variables.

Approved Questar Secure Browser Block List

The following applications will be blocked by adding the process names listed to the config.json. If the process is running when a user launches the Questar Secure Browser, they will receive a message that they must close the application. The name listed in the Display Name column will be displayed as part of the error message.

Application Type	Application	Win App Process Name	Mac App Process Name	Display Name
Browser	Google Chrome	chrome.exe	Google Chrome	Google Chrome
Browser	Internet Explorer	iexplore.exe	N/A	Internet Explorer
Browser	Microsoft Edge (2020 new)	msedge.exe	Microsoft Edge	Microsoft Edge (2020 new)
Browser	Microsoft Edge (Legacy)	MicrosoftEdge.exe MicrosoftEdgeCP.exe MicrosoftEdgeSH.exe	N/A	Microsoft Edge (Legacy)
Browser	Mozilla Firefox	firefox.exe	Firefox	Mozilla Firefox
Browser	Opera	Opera.exe	Opera	Opera
Browser	Safari	N/A	Safari	Safari
LMS	Moodle	Moodle Desktop.exe	Moodle4Mac	Moodle
Videoconferencing	FaceTime	N/A	FaceTime	FaceTime
Videoconferencing	GoToMeeting	G2mstart.exe	GoToMeeting	GoToMeeting
Videoconferencing	Skype	Skype.exe	Skype	Skype
Videoconferencing	U Meeting	U.exe	U	U Meeting
Videoconferencing	WebEx	ptoneclk.exe atmgr.exe CiscoWebExStart.exe webexmta.exe	Cisco Webex Meetings webexmta	WebEx
Videoconferencing	WhatsApp	WhatsApp.exe	WhatsApp	WhatsApp
Videoconferencing	Zoom	zoom.exe	zoom.us	Zoom
Videoconferencing / LMS	Teams	teams.exe	Teams	Teams
Writing Assistant	Grammarly	grammarly.desktop.exe	Grammarly Desktop	Grammarly

The below applications are not online and are accessed by a web browser, therefore there is no specific configuration for these applications to block them. As long as all applicable web browsers are blocked, these applications will not be able to be run.

Application Type	Application	Win App Process Name	Mac App Process Name	Display Name
LMS	Blackboard	NA, Online/Web only	NA, Online/Web only	NA
LMS	Buzz (Agilix)	NA, Online/Web only	NA, Online/Web only	NA
LMS	Canvas	NA, Online/Web only	NA, Online/Web only	NA
LMS	Edmodo	NA, Online/Web only	NA, Online/Web only	NA
LMS	Google Classroom (GSuite)	NA, Online/Web only	NA, Online/Web only	NA
LMS	Schoology	NA, Online/Web only	NA, Online/Web only	NA
Videoconferencing	Google Hangout/Meet	NA, Online/Web only	NA, Online/Web only	NA

Please note: Microsoft Boost is Microsoft Edge, so this needs to be disabled.

Sample Test Login

Once the Questar Secure Browser is available on the student devices, log in to the Sample Test to ensure the download was successful and the test is available and functioning on the device.

1) Launch the Questar Secure Browser from the desktop of student device(s).

2) Enter:

User ID: practice Password: practice

3) Navigate through the sample test to ensure:

- ☐ The test loads at an acceptable speed (See Appendix B: General System Requirements for details.)
- ☐ Items render correctly and can be answered (items/answers do not bleed off the screen, etc.)
- ☐ Available tools work appropriately
- ☐ The test can be submitted upon completion via the Review screen

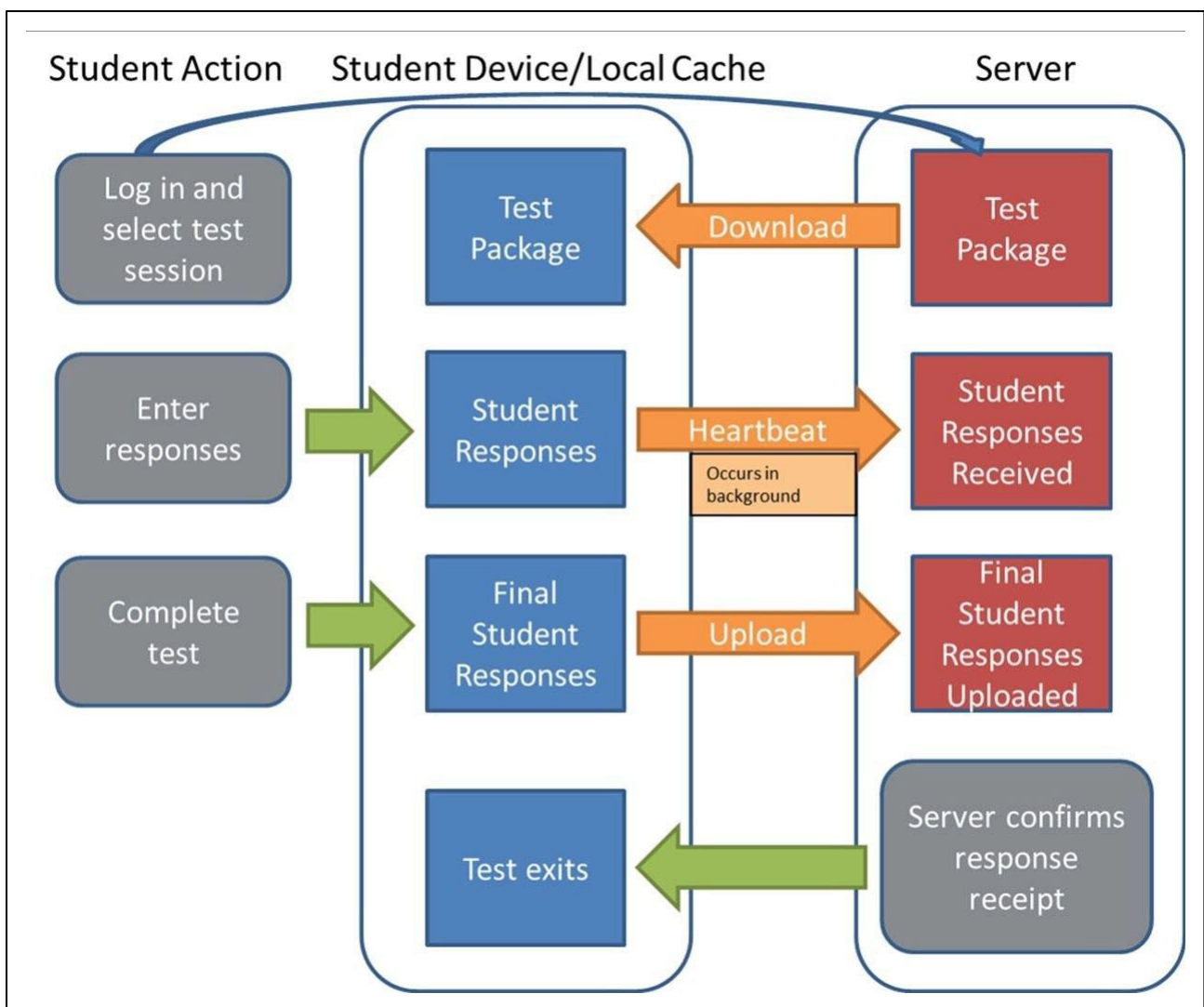
Appendix A – Student Response Flowcharts

Student Response Flow

After a student logs in and selects a test, the complete test package is downloaded to an encrypted file on the student's device. The student's responses are saved to an encrypted local cache on the device.

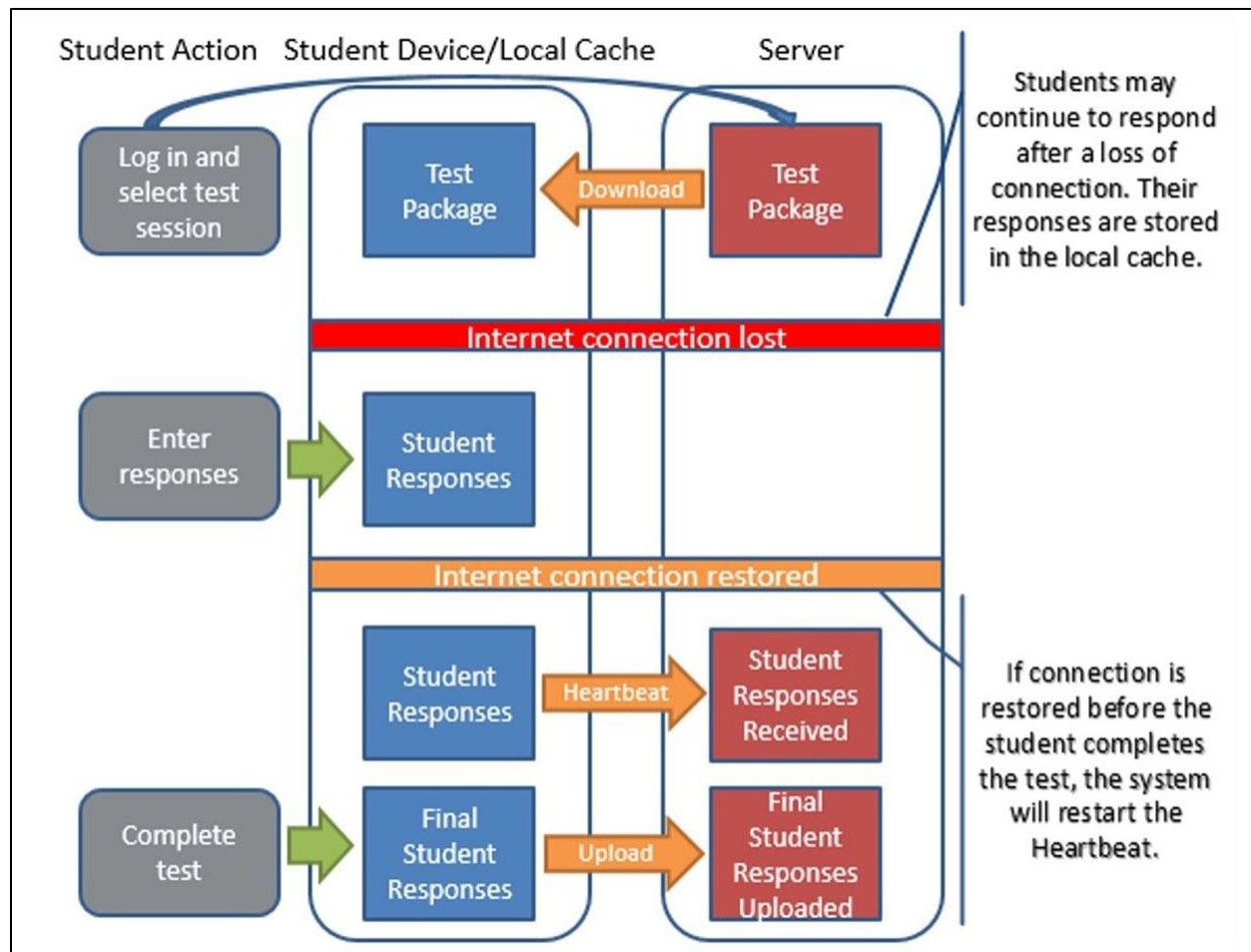
Continuous Internet Connection

Optimally, the student's device will have continuous Internet connection during testing. The student's responses are sent to the NWEA Server in the background. This is referred to as a "heartbeat." This heartbeat is a configured time interval. When the student completes testing, the final responses are uploaded to the NWEA Server. The NWEA Server confirms response receipt and the Questar Secure Browser will exit on the student's device.



Internet Connection Lost and Restored During Testing

If Internet connection is lost, the student continues responding to test questions without interruption. The **student should not move to another device** as their responses are stored on their local device until connectivity is re-established. The testing system continuously attempts to re-establish connection with the NWEA Server. When the Internet connection is restored, the responses are automatically sent to the NWEA Server. When the student completes testing, the final responses are uploaded to the NWEA Server. The NWEA Server confirms response receipt and the test will exit on the student's device.

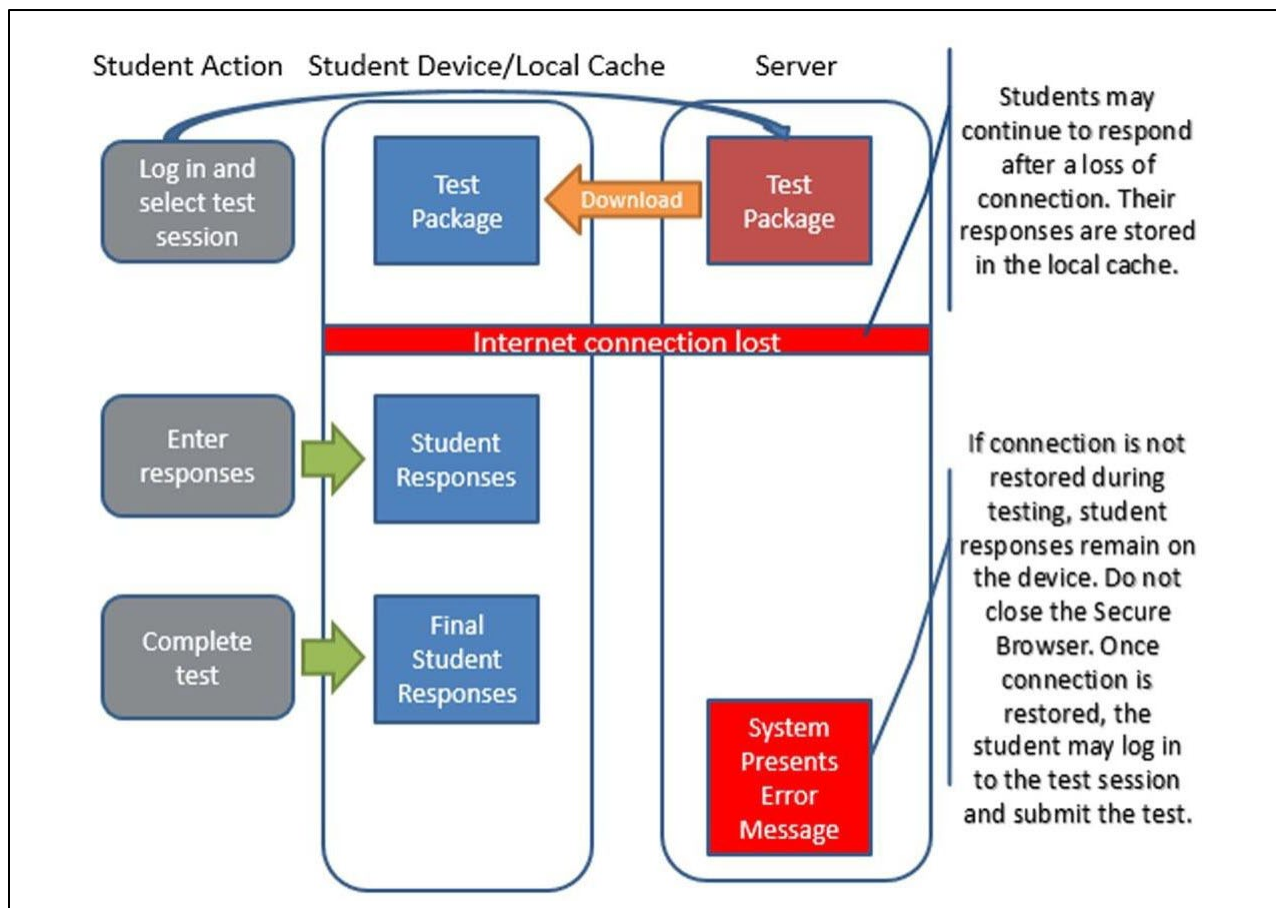


Note: Text-to-Speech (TTS) and Speech-to-Text (STT) require an Internet connection. TTS and STT will be unavailable until the Internet connection is restored. When the Internet connection is restored, the student with the TTS accommodation will be able to select play and TTS will load again, or the student with the STT accommodation will be able to use the microphone again.

Internet Connection Lost

If Internet connection is lost, the student continues responding to test questions without interruption. The **student should not move to another device** as their responses are stored on their local device until connectivity is re-established. If the student completes testing and the Internet connection has not been restored, the following process occurs:

- The system will present an error message directing the student to alert the test administrator.
- The student's responses remain on the device. **The device should not be used by another student before the following steps are completed by the technology coordinator or test administrator:**
 - 1) Restore Internet connection to the device.
 - 2) If the student has logged out, direct them to log in again.
 - 3) Submit the test.
- The NWEA Server confirms response receipt and the test will exit on the student's device.
- Another student can now use the device.



Appendix B – System Requirements

General System Requirements:

- System Memory/Hard Disk Space
 - Minimum 512MB Free RAM
 - Recommended 2GB Free Storage Space
 - Minimum 1GB Free Storage Space
- LAN Network
 - Recommended available LAN bandwidth at each workstation 2Mbps
- Internet Speed
 - Minimum per device: 150Kbps
 - Recommended: 300Kbps

Note: All OS support is for released versions only; we do not support BETA releases at this time.

OS Specific System Requirements:

For details on specific supported devices, operating systems, and specifications, please visit the *Test Readiness* page at the following link: <https://www.nwea.org/nextera/readiness/>.

System Requirements continued

Topic	Notes
Touchscreen input	- NWEA supports touchscreen input for Chrome, Windows, and iPad operating systems (OS) that meet the specifications above. Any other system that has a touchscreen input would require the use of a mouse or keyboard touchpad to support mouse interactions. - Dual mode Chromebook devices offering a laptop and tablet mode must be used in laptop mode (tablet mode is not supported). - Touchscreen devices are supported; however, this is specific to student testing devices that are using touchscreens as "standard" laptop screens. There are some new devices on the market, such as those offered by Lenovo and Dell, that allow the computer screen to be "flipped" to become/function like a tablet device instead of a standard laptop device. These devices are also referred to as 2:1 devices. Students may not use the devices in flipped-screen tablet mode for the operational CBT exams.
External keyboards and mice	- An external keyboard must be provided and available for all students testing on computer. - All devices must have a mouse, touchpad, or touchscreen to assist students with responding to different item types.
Dual monitors	NWEA does not support dual monitors for student testing.
Stylus use	- Most compatible stylus devices will work with tablets — electro-magnetic resonance (EMR) digital pens are not supported, including Microsoft Surface stylus. - A stylus for touch-screen displays is allowed on the computer-based tests for Grades 3-8 ELA and math and Grades 5 & 8 science if students in the school are using a stylus as part of daily instruction. - If a school wishes to allow students to use a stylus for the CBT administration, the school must provide a stylus to any student who wants to use a stylus for touchscreen displays responding to CBT items on a touch-screen device.
Energy Saver	NWEA recommends that devices are fully charged or plugged in, and low power modes are turned off. Please disable any sleep settings to prevent devices from going to sleep during testing.

Appendix C – Frequently Asked Questions (FAQ)

Can a student restart a paused or terminated test session on the same platform but another device?

All efforts should be made to have the student resume a test on the same device they began testing with. Only if the device is permanently incapacitated or the student cannot be held any longer should another device be used. In this case, the student should be made aware that unsaved or partially saved responses may have to be re-entered before submitting the test.

Partially saved responses would occur due to connection loss between heartbeat intervals. The heartbeat intervals are estimated to transmit student responses to NWEA every 120 seconds under optimal internet connectivity.

Can a student needing accommodations use the native accessibility features of an iPad or Chromebook?

No. iPad and Chromebook devices must be locked down to only access Nextera TDS during testing.

Do I need to turn off auto-capitalization on an iPad?

No, this is not required but when a student begins typing their username, the first letter is automatically capitalized unless this is disabled or if a student turns off the capitalization arrow before typing. Auto-capitalization can be turned off in the Settings menu of the iPad.

Does the Nextera Test Delivery System include spell-checking software?

No, the Nextera Test Delivery System does not include spell-checking software as a student testing accommodation. We want to make sure that our operational CBT schools understand that spell-checking software is not an available testing accommodation in the Nextera Test Delivery System. The use of a spell-checking device/software is an allowable testing accommodation on the Grades 3–8 ELA and Mathematics and Grades 5 & 8 Science Tests if specified in the student's IEP or 504 plans.

How do I contact NWEA?

You can contact NWEA Customer Support for any questions on the Grades 3–8 ELA and Math and Grades 5 & 8 Science Computer-Based Tests by calling: 866-997-0695; emailing [NWEA Customer Support Email](mailto:NYTesting@nwea.org) (NYTesting@nwea.org); and by going to the Test Readiness website (<https://www.nwea.org/nextera/readiness/>).

Appendix D – Troubleshooting Tips

Issues Loading Test

If you experience latency while the test is loading, review the following list of possible solutions presented in order of most likely to resolve the issue:

- Confirm the network bandwidth is flowing without impediment.
 - Try opening a website on another device on your network. If you experience latency accessing the Internet on another device, you may be experiencing a broader network issue.
- Confirm the Questar and NWEA domain names (*.questarai.com and *.nwea.org) are whitelisted in your firewall. If your firewall or Web content filter supports SSL inspection, ensure that function is turned off in the firewall and/or content filter.
- If the error occurs intermittently, it may be that the firewall or Web content filter is prioritizing traffic and causing some requests to fail. If the firewall or Web content filter allows it, add a rule to allow traffic to the Questar domain *.questarai.com and the NWEA domain *.nwea.org to be top priority in the firewall or content filter.
- Add *.questarai.com and/or *.nwea.org to the ignore list/blanket bypass if one is in use.
- Use the secondary mouse button, select quit Questar Secure Browser, and log in again. This issue may be a result of firewall or content filter inspecting the connection; this resolution may create a new connection that is unlocked.
- If using an iPad, close out of the Questar Secure Browser then turn on and off Airplane mode under Settings. This will reset all radios, allowing the device to create a clean network connection.

Response Recovery When Internet is Disconnected Prior to Test Session Submission

If Internet connectivity is lost for any reason prior to the submission of a test session, the device cache stores the responses locally until connectivity is restored. The following indicators are visible when Internet connectivity is lost:

- The connection indicator in the upper left corner of the Nextera Test Delivery System changes from green to red.



A checkmark means you are currently online.

- If connectivity is lost for 45 seconds or more, a “Lost Connection” message displays.



An “x” means you are working offline. Don’t worry, your answers are still being saved. You will have to reconnect before submitting your test.

- If the network connection is restored, the responses will automatically submit and the display will return to the Nextera TDS login screen. It is strongly recommended the device be left in this state until the network connection is restored.
- **Note:** Text-to-Speech (TTS) and Speech-to-Text (STT) require an Internet connection. TTS and STT will be unavailable until the Internet connection is restored. When the Internet connection is restored, the student with the TTS accommodation will be able to select play and TTS will load again, or the student with the STT accommodation will be able to use the microphone again.

Once connectivity is restored, the stored responses need to be submitted to the NWEA server. From the device that lost connectivity, follow the steps below to upload the stored responses:

- Refer to the State Education Department for the state policy regarding teachers or test administrators logging in with student credentials to submit a student test. If permitted, complete the following steps.
- Log in to the Nextera Test Delivery System with the user’s login username and password, select the session that lost connectivity, and enter the session access code.
- After the “Preparing Your Test” message disappears, select “Begin.” The stored responses are now synced between the device and the NWEA server, and the responses are viewed within the Test Delivery System. The user may resume completing and/or submitting the test.

-118 Error Code/Unable to access <https://nextera.questarai.com>

The workstation is unable to access the site.

- If the error occurs routinely, the site is being blocked by a firewall or content filter. Ensure *.questarai.com is whitelisted in the firewall. If the firewall and/or content filter brand supports SSL inspection, ensure that function is turned off in the firewall and/or content filter.
- If the error occurs intermittently, the firewall or content filter is prioritizing traffic and causing some requests to fail. If possible, add a rule to allow *.questarai.com to be top priority in the firewall or content filter.

Issues Editing Constructed Responses

Select the Insert key to ensure the keyboard is in insert mode rather than overwrite mode. When a keyboard is in overwrite mode, existing text is deleted as new text is written. Selecting the Insert key again changes back to insert mode. Also ensure that there are no testing tools enabled in the Nextera Test Delivery system. Testing tools must be disabled before editing text in a constructed response box.

Troubleshooting Error Messages Students May Encounter Prior to and During Testing

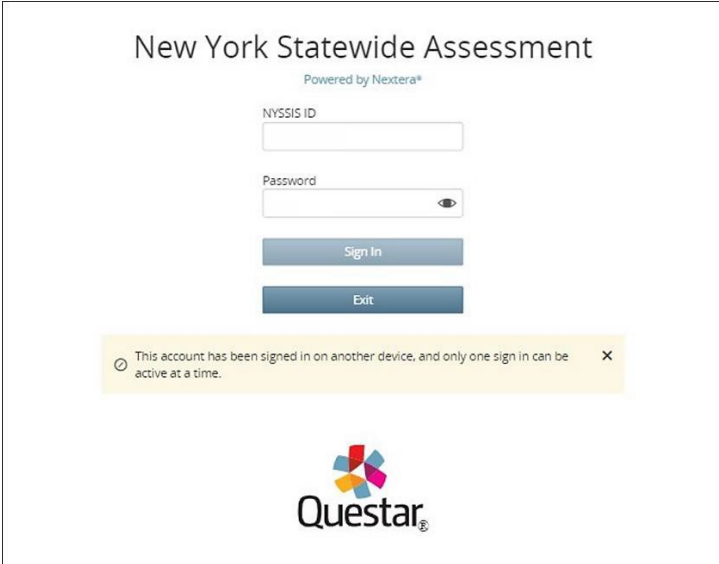
Possible Error Messages When Logging In

The following table will review possible error messages students may encounter before they begin testing, the potential causes for the error message, and actions to take to correct the error.

Name of Error	Error Message	Potential Cause(s)	Corrective Action(s)
Sign-in error	New York Statewide Assessment Powered by Nextera® NYSSIS ID NYSSIS ID Password Password Sign in We couldn't verify your account using those credentials. ✕ Please check them and try again. Questar®	User enters the wrong User ID and/or Password on the Nextera TDS sign- in screen.	Confirm correct user ID/password and try again. Check to ensure Caps Lock is not on.

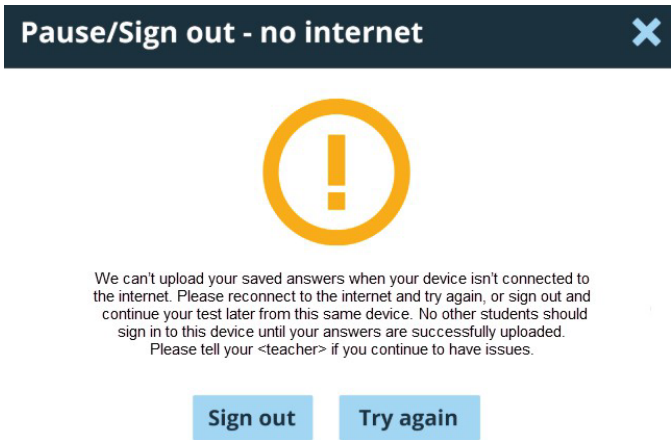
Name of Error	Error Message	Potential Cause(s)	Corrective Action(s)
Choose Test Outside of Window	Choose your test English 1 Session 1 Grade 8 <i>This test will be available on 3/24/2021 at 8:00am</i> English 1 Session 2 Grade 8	User is outside of the assigned test window. NOTE: This date is simply for reference.	1) Begin test within the testing window. 2) Check testing device time/date to confirm it is set correctly for current time/date EST.
Access Code Incorrect	Access code needed  Please enter the access code that your teacher gives you. 4384 Something isn't right. Please check your code and try again. Exit Continue	User enters the wrong access code for the class test session.	Confirm the four-digit access code and try again. 1) Confirm you have the correct testing class access code. 2) Confirm you have the correct test session access code. 3) Confirm you are not using the Proctor PIN instead of the access code.

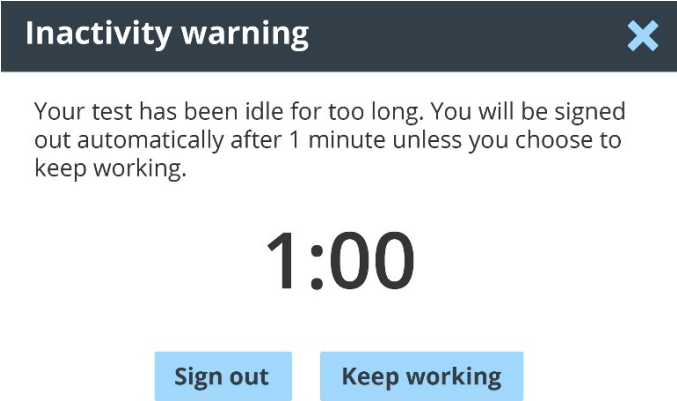
Name of Error	Error Message	Potential Cause(s)	Corrective Action(s)
Proctor PIN Incorrect	Proctor PIN needed  You need a Proctor PIN to start or continue this test. Something isn't right. Please check your code and try again. Cancel Continue	User enters the wrong Proctor PIN.	Confirm the eight-digit Proctor PIN and try again. 1) Confirm you are not using the four-digit access code in the Proctor PIN box. 2) Confirm with your Principal that the Proctor PIN has not been changed.

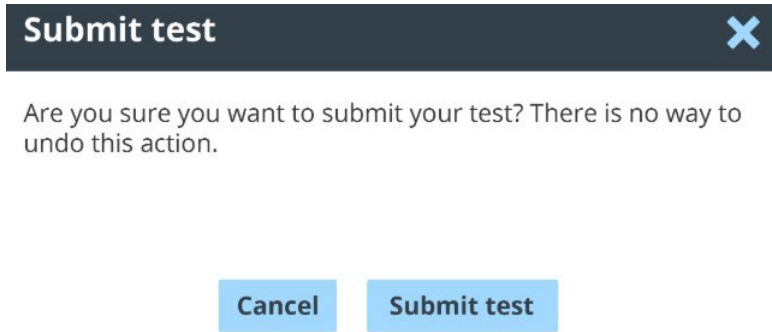
Name of Error	Error Message	Potential Cause(s)	Corrective Action(s)
Concurrent Login	 The screenshot shows the 'New York Statewide Assessment' login page. It includes fields for 'NYSSIS ID' and 'Password', 'Sign in' and 'Exit' buttons, and a yellow error message at the bottom: 'This account has been signed in on another device, and only one sign in can be active at a time.' The Questar logo is at the bottom.	User enters credentials that have already been used to sign in on another device. This may be due to a device having lost power while the student is testing and attempts login on a second device, or two students having been given the same login credentials.	Confirm correct user ID/password and try again. If error persists, contact the principal, BLU, DTC, STC, DLU or RIC to unlock the credentials or, in the case of two students being given the same login credentials, to locate the other user. For any additional needed follow-up, contact NYSED or NWEA customer support.

Possible Error Messages During Testing

The following table will review possible error message students may encounter during testing, the potential causes for the error message, and actions to take to correct the error.

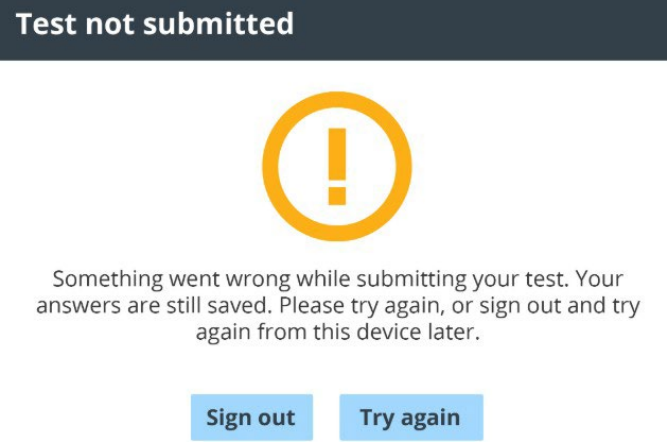
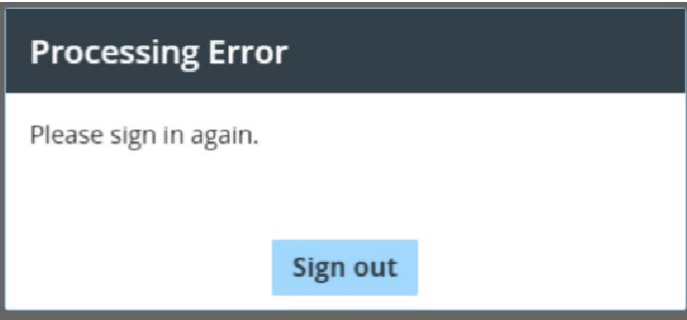
Name of Error	Error Message	Potential Cause(s)	Corrective Action(s)
Signing Out/Pausing — No Internet Connection	 Pause/Sign out - no internet We can't upload your saved answers when your device isn't connected to the internet. Please reconnect to the internet and try again, or sign out and continue your test later from this same device. No other students should sign in to this device until your answers are successfully uploaded. Please tell your <teacher> if you continue to have issues. Sign out Try again	A user pauses/signs out in the middle of a test session without being connected to the internet.	Reconnect to the internet and select Try again or Sign out and continue the test session later from the same device. Selecting Sign out will save the student responses locally. No other users should sign into this device until the user's responses are successfully uploaded. The device should be quarantined until the internet connection is restored and the responses can be uploaded to NWEA.

Name of Error	Error Message	Potential Cause(s)	Corrective Action(s)
Inactivity warning – the test has been idle for too long. Sign out or Keep working.	 Inactivity warning Your test has been idle for too long. You will be signed out automatically after 1 minute unless you choose to keep working. 1:00 Sign out Keep working	A user has been inactive and without any keystrokes, mouse movements, touch- pad, or touchscreen activity for 120 minutes. At this point in time, an inactivity warning will display.	By continuing the inactivity, students will be automatically logged out at the end of a one minute count down. When the inactivity warning displays, students may select Sign out to be signed out of the Test Delivery System. By selecting Keep working, students may continue testing. The Inactivity warning may be avoided by students continuing to make keystrokes, mouse movements, or interact with their touch-pad or touchscreen. Note: If the student device falls asleep due to a sleep timer set at the OS level prior to 120 minutes of inactivity, they will not receive the Inactivity message.

Name of Error	Error Message	Potential Cause(s)	Corrective Action(s)
Test Submission — Confirmation Messaging with all questions answered		Confirmation message for when a student submits their test through the review screen. This one indicates the student has answered all the test questions.	Student can choose to submit the test by selecting Submit test or they can select Cancel. Selecting Submit test submits the test. There is no returning to the active test session once selected. Selecting Cancel returns the student to the active test session.

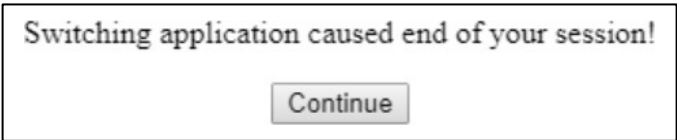
Name of Error	Error Message	Potential Cause(s)	Corrective Action(s)
Test Submission — Confirmation Messaging with unanswered questions	You have unanswered questions You have unanswered question(s) on your test. Are you sure that you want to submit your test? There is no way to undo this action. Cancel Submit test	Confirmation message for when a student submits their test through the review screen. This message indicates the student has unanswered questions in the test session.	Student can choose to submit the test with unanswered questions by selecting Submit test or they can select Cancel. Selecting Submit test submits the test with unanswered questions. Selecting Cancel returns the student to the active test session.

Name of Error	Error Message	Potential Cause(s)	Corrective Action(s)
Test Not Submitted — No Internet	Test not submitted - no internet  We can't submit your test without being connected to the internet. Please reconnect to the internet and try again, or sign out and continue your test later from this same device. No other students should sign into this device until your answers are successfully submitted. Please tell your <teacher> if you continue having issues. Sign out Try again	Message appears if a user tries to submit a test when they are not connected to the internet.	Reconnect to the internet and select Try again or select Sign out and continue the test later from the same device. Selecting Sign out will save the student responses locally on the device. No other users should sign into this device until the user's responses are successfully submitted. The device should be quarantined until the internet connection is restored and the responses can be uploaded to NWEA.

Name of Error	Error Message	Potential Cause(s)	Corrective Action(s)
Test Not Submitted — Other Error		Message appears if any error occurs on NWEA's end or at the device level while submitting a test.	User should select Try again or select Sign out and try again from the same device later. Selecting Sign out will save the student responses locally on the device. No other students should sign into this device until the user's responses are successfully uploaded. This device should be quarantined until the internet connection is restored and the responses can be uploaded to NWEA.
Processing Error-Unexpected Error Message		In the exceedingly rare event when a new student session cannot be established, or if there is a disruption when reloading prior responses, a student will not be allowed to continue.	Exit the test and sign in again.

Possible Questar Secure Browser Errors

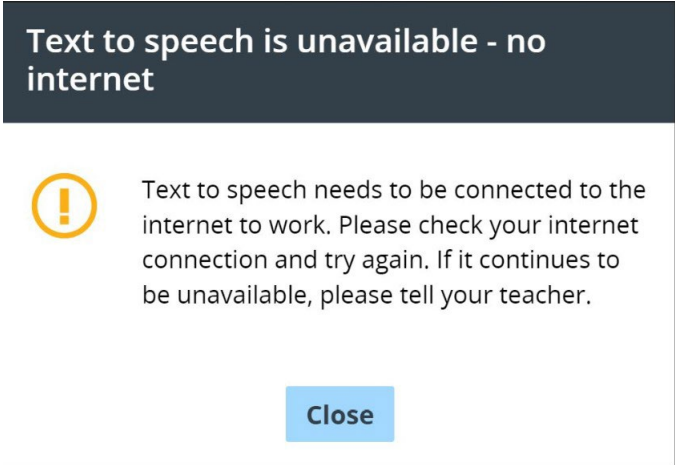
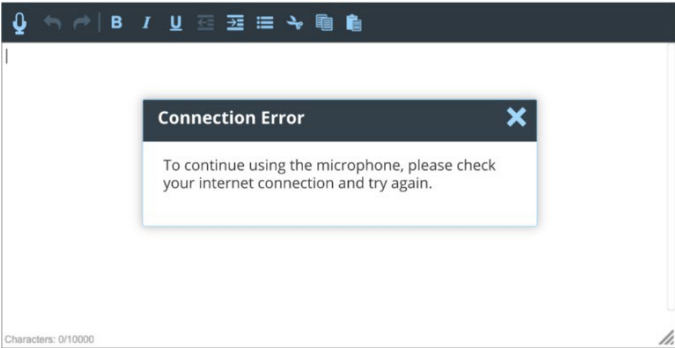
The following table will review possible error messages that may occur involving the operation or interruption of the Questar Secure Browser, potential causes for the errors, and actions to take to correct the error.

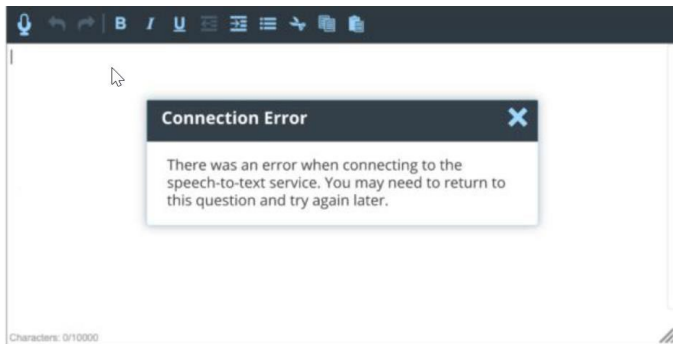
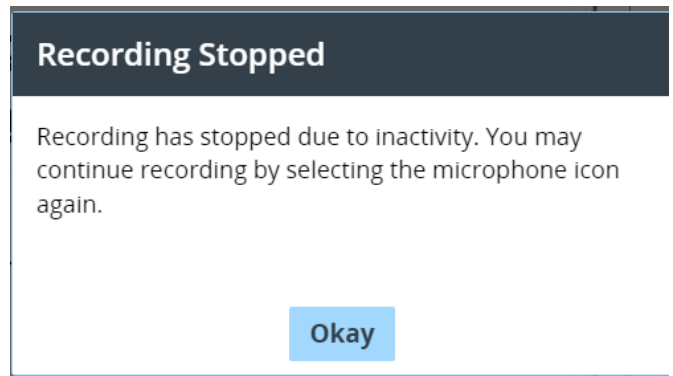
Name of Error	Error Message	Potential Cause(s)	Corrective Action(s)
Loss of Focus/ Switching Application		Another application can gain the focus away from the Questar Secure Browser. There are three possible reasons for this error: 1) A pop-up is generated by the device's operating system, or another application is asking for permission to do something. 2) An application is activated that has an overlay (Example: OS accessibility features like Windows Sticky Keys, Virtual Keyboard, etc.). 3) The operating system login screen displayed and then the user logged back into the operating system (Example: The user types the Windows key + L shortcut. This will bring up the Windows login screen.).	Attempt to identify and disable or prevent whatever program or student behavior caused the loss of focus, and then have the student log back in to continue testing.

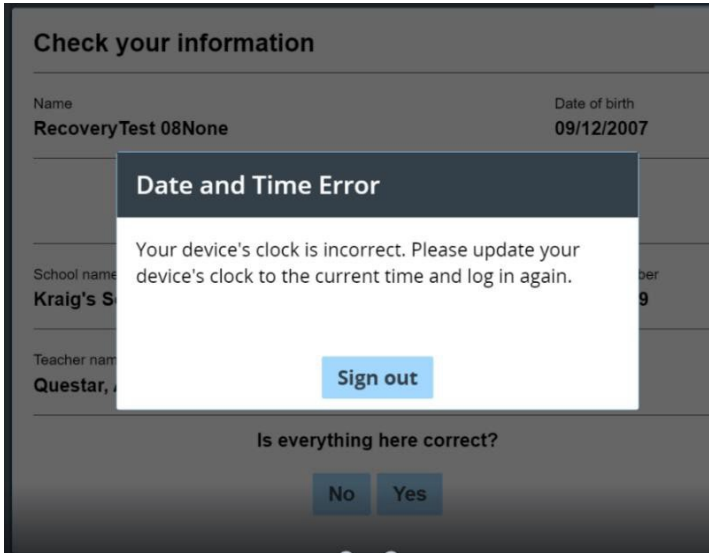
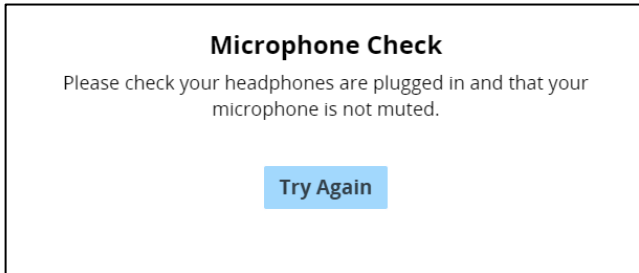
Name of Error	Error Message	Potential Cause(s)	Corrective Action(s)
		4) The user selected the Questar Secure Browser's icon too many times, resulting in the secure browser launching multiple times.	
Siri is Enabled on Apple devices	Please disable Siri and try again. Exit	1) When Siri hasn't been disabled for the given user/system. 2) If there is a Siri service still running somewhere in the background.	Siri must be disabled. Open System Preferences , select Siri , and deselect Enable Siri .
Alexa is Enabled	Please disable Alexa and try again. Exit	3) When Alexa hasn't been disabled for the given user/system. 4) If there is an Alexa service still running somewhere in the background	Alexa must be disabled. Uninstall Alexa and disable Cortana. For step by step instructions see Additional Settings: Disable Alexa/Cortana Windows on page 32 of this document

Name of Error	Error Message	Potential Cause(s)	Corrective Action(s)						
Other Apps Enabled on Windows and Mac OS	The following applications are currently running. In order for the Secure Browser to launch they will need to be closed. <table><thead><tr><th>App Name</th><th>Process Name</th></tr></thead><tbody><tr><td>Google Chrome</td><td>chrome.exe</td></tr><tr><td>Microsoft Teams</td><td>teams.exe</td></tr></tbody></table> Exit	App Name	Process Name	Google Chrome	chrome.exe	Microsoft Teams	teams.exe	1) When an app (e.g., meeting apps, classroom apps, browsers, email, etc.) has not been disabled for the given user/system. 2) If there is an app still running somewhere in the background.	All other apps must be disabled. Disable all running apps prior to testing and before the Questar Secure Browser is launched.
App Name	Process Name								
Google Chrome	chrome.exe								
Microsoft Teams	teams.exe								

Name of Error	Error Message	Potential Cause(s)	Corrective Action(s)
We Can't Connect	 Questar™ We can't connect. Please tell your teacher. For the teacher: There seems to be an issue in connecting with Questar. Please check the internet connection and try again.	When the Test Delivery System (TDS) application is not available for the moment. (Or the internet or connection to the application was aborted for some reason.) The causes for a loss of connection can happen at any level in the connection process that prevents access at the local school through the TDS application. This could refer to a local machine, school connectivity issues, or local internet provider issues.	Check the internet connection and try again.

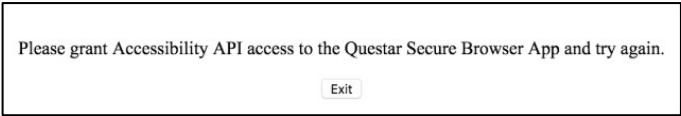
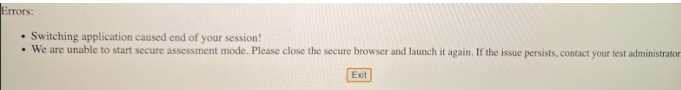
Name of Error	Error Message	Potential Cause(s)	Corrective Action(s)
Text to speech is unavailable – no internet		Message appears if a user tries to access TTS while offline.	Check the internet connection and try again.
Speech to Text is unavailable – no internet		Message appears if a user tries to access STT while offline.	Check the internet connection and try again.

Name of Error	Error Message	Potential Cause(s)	Corrective Action(s)
Connection Error		Message appears if there is a connection error with the Speech-to-Text (STT) service. Note: this is in reference to the service <i>AWS Transcribe</i> which STT uses. It does not refer to internet connectivity.	Return to the question and try again later. This error message could display during the microphone test if you have not whitelisted the addresses listed on page 15 under Network Considerations and Setup.
Inactivity Message		When using STT, if no spoken language is detected for 5 seconds, the student will receive a 5 second count down warning. After 10 seconds of inactivity the recording will stop.	To continue recording, select the microphone icon again.

Name of Error	Error Message	Potential Cause(s)	Corrective Action(s)
Date and Time Error Message		This error message will display if the device's clock is off by more than 5 minutes. This message only displays if the student is assigned the STT accommodation.	Update the device's clock to the correct time. Log in again.
Microphone Check Error Message		Message appears if a student attempts to use the STT accommodation and a microphone is not detected by the device.	Check that headphones are plugged in and the microphone is not muted.

Name of Error	Error Message	Potential Cause(s)	Corrective Action(s)
Outdated Secure Browser	The screenshot shows a white background with the text 'New York Statewide Assessment' at the top, followed by 'powered by Nextera'. Below this is the message 'Your secure browser is out of date and needs to be updated.' in a grey box. At the bottom is the Questar logo and copyright information: '© 2014 Questar Assessment', 'Questar is a registered trademark of Questar Assessment, Inc.', and 'Version 79.0'.	An old version of the Questar Secure Browser is installed on the testing device.	Download the new Questar Secure Browser available on the Downloads page from the HELP tab in Nextera Admin.
No Kiosk Mode Session	The screenshot shows the Questar logo at the top, followed by the text 'Can't launch app' in a bold font. Below this is the message 'This application can only run on a Chromebook in Kiosk Mode. Please tell your teacher.' in a smaller font.	If the user is trying to run the Questar Secure Browser Chromebook app on a Windows or MacOS machine through the Chrome Browser: 1) Some of the previous versions of the Questar Secure Browser Chromebook apps can be added to the Chrome Browser as an extension. 2) These apps will appear as "Not Compatible" when opened on a Chrome Browser.	The Questar Secure Browser Chromebook app can only be run in a Kiosk mode on a Chromebook. For additional information on Chromebooks and Kiosk mode see the Chromebook Installation section on page 33 of this document. Uninstall and reinstall with the latest version of the Questar Secure Browser to the correct associated device.

Name of Error	Error Message	Potential Cause(s)	Corrective Action(s)
App Self-Lock (iPadOS Popup)	Confirm App Self-Lock Questar wants to start Single App Mode. You will be unable to use other apps on iPad until Questar ends Single App Mode. Do you want to allow this? No Yes	The “Confirm App Self-Lock” message may appear for iPadOS users, after the user enters their login credentials, as a confirmation to enter into single app mode to begin their secure test. 1) The user enters their login credentials. 2) The “Confirm App Self-Lock” message appears.	If No is selected, TDS won’t open and the student will not be able to begin the test. By selecting Yes, the device will start Single App Mode and the secure test will be launched.
Guided Access and Self-Lock (iPadOS Popup)	Turn off Guided Access and Confirm Self-Lock to Proceed. Cancel	The Questar Secure Browsers utilize AAC Mode (Automatic Assessment Configuration) for securing the device and it cannot work while Guided Access Mode is turned on. Therefore, this message displays when Guided Access Mode (Accessibility feature) is turned on before logging into the Questar Secure Browser.	This can be turned off by selecting the Home button 3 times.

Name of Error	Error Message	Potential Cause(s)	Corrective Action(s)
Accessibility API Access (MacOS)		The Questar Secure Browser was not given Accessibility API access.	Go to Settings and give access to the Questar Secure Browser on individual machines, or in bulk for the MacOS versions that use mobilconfig in Multiple Device Management (MDM).
AAC Failure (MacOS)		A verification checks to ensure AAC mode starts successfully on Mac computers is added. If AAC mode fails to start, a message will be presented to the user, preventing the test from starting without AAC mode.	Contact test coordinator to ensure AAC mode is on.