Setup & Installation Guide

Nextera®

Mississippi Academic Assessment Program Fall 2023

Contents

Introduction to the Nextera Assessment System

Overview

The Nextera Assessment System is a suite of software applications used for conducting standardized assessments. This *Setup & 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).

Note: A current version of this document will be provided at the start of each administration year. Any updates throughout the administration year will be provided in the form of Release Notes, which will be housed on the *Help* page in Nextera Admin.

The Nextera Assessment System is comprised of two primary applications:

> 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 ask your District Test Coordinator to either create a District Information Technology Coordinator (DITC) account for you or reset your password for an existing account.

- **Nextera Admin** is a web-based application for loading and managing district, school, class, teacher, and student information. The *Downloads* page, located on the **HELP** tab, contains links and downloads, including the *Secure Browser*.
- The **Nextera Test Delivery System (TDS)** is a software application for completion of student assessments delivered through the *Secure Browser*.

Security and the Student Experience

As a Technology Coordinator, you may be asked about test security, recommendations, and the student experience. The Nextera TDS is designed to prevent a student from navigating away from the *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.

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 tools available on the Test Readiness website at http://www.questarai.com/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

4 Weeks Prior to Testing

- ✓ Perform System Scan
- ✓ Perform Test Readiness
  - If using wireless networks, ensure there is ample coverage and capacity to support testing.
- ✓ Download/deploy the *Secure Browser* to all devices being used for student testing.

3 Weeks Prior to Testing

- ✓ Log in to the Sample Test using the *Secure Browser*.
- ✓ Once the *Secure Browser* is installed and tested, you should avoid software updates prior to and during testing.

2 Weeks Prior to Testing

- ✓ Ensure Test Administrators are aware of district policies, expectations, and processes for troubleshooting Internet connectivity issues (select the following link to view this information: Appendix A). It is also recommended that Test Administrators review the *Internet Connectivity Troubleshooting Guide*, available to print from the Nextera Admin *HELP* page, and have this guide readily available during testing.

During Testing

- ✓ Limit network activity that may impact bandwidth, such as streaming music and video.
- ✓ 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.

IMPORTANT: If a new operating system becomes available and it is not listed on the Test Readiness website at http://www.questarai.com/readiness/ or in a subsequent Release Note, it may not be supported. Do not upgrade to new operating systems on devices that will be used to administer online assessments without validating that the new operating system is supported.

Preparing your Site – Step by Step

Perform System Scan

Please note: The System Scan is designed to validate desktop device configurations. Select the following link for additional details about tablet devices and Chromebooks: http://www.questarai.com/readiness/.

1) Open a Web browser and access http://www.questarai.com/readiness/.
2) Locate the *System Scan* box and select **Scan Now**.
3) Select **Scan Now** again on the next page.
4) The scan results display. If a warning message displays, verify the workstation has the minimum system requirements specified for that type of device. The requirements can be found at http://www.questarai.com/readiness/.

Perform Test Readiness

1) Open a web browser and access http://www.questarai.com/readiness/.
2) Locate the *Test Readiness* box and select **Test Now**.
3) Select the link www.speedtest.net to determine your download and upload speeds.
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, return to the *Test Readiness* page, input the data in the fields provided, and select **Test Now**. The download and upload speeds are found in the test results from the prior step.
7) The Test Readiness Check results are calculated and displayed.

- 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 NWEA Customer Support by calling 1-800-644-4054 or emailing mscustomersupport@nwea.org.

Network Considerations and Setup

Once you have used the System Scan and Test Readiness tools to determine there is adequate available bandwidth, ensure readiness regarding other upstream network devices (e.g., firewalls, proxy servers, and 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. Since technology is constantly changing, it is possible that some of the file names outlined here may have updated versions. If you would like assistance at any point, contact NWEA Customer Support by calling 1-800-644-4054 or emailing mscustomersupport@nwea.org.

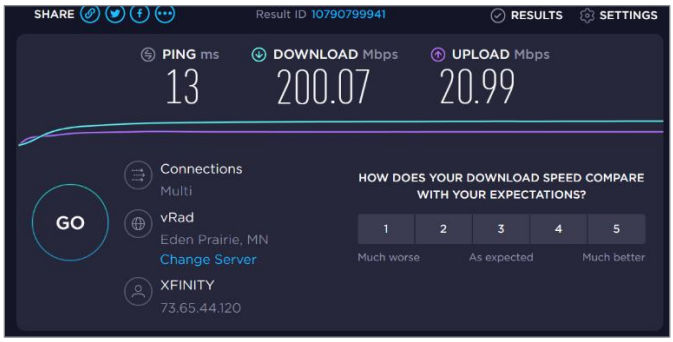
Technical Specifications

There are typically two bands of speed available on a wireless network: 2.4 GHz and 5 GHz. The 2.4 GHz frequency provides a slower connection but has a longer range of connectivity. The 2.4 GHz band can cover 400 feet or more (rated at 380 – 820 feet amplified) with 300 Mbps speed. The 5 GHz frequency is faster but allows a shorter range of reliable connectivity at approximately 200 feet and allows for speeds under 900 Mbps. If your network is designed to provide dual-band support, each band will allow connectivity for up to 100 devices. However, a more realistic number of 30 to 45 connected devices per wireless band will provide optimized testing in the Nextera Test Delivery System.

Newer devices and Wi-Fi access points will usually default to the 5 GHz frequency and this document will focus on this setup. Please make sure your IT department has avoided any overlapping channels on your wireless network as this could causes interference and result in packet loss. Your speed may be different than described in this document, but the same rules will apply for all networks.

Site Survey

Here is a basic computation of a site survey to assess the Wi-Fi capabilities of the expected activity of the Nextera Test Delivery System. First, you will need to evaluate your speed. Using your internet browser, navigate to https://www.speedtest.net and select **Go** (in the center of the page) to obtain your download and upload speeds. In this example, you can see a 200 Mbps download and 20 Mbps upload.



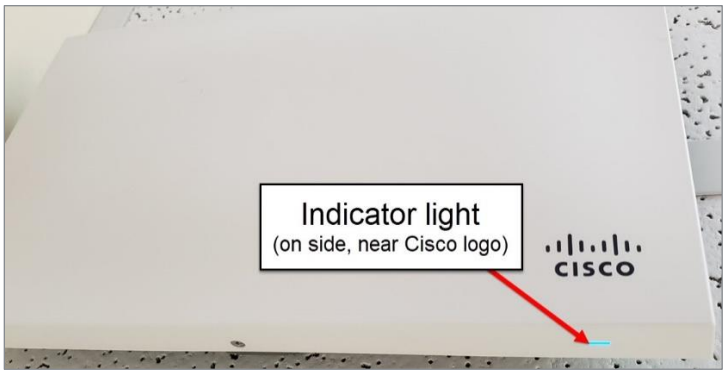
Depending on the type of test, downloading diagrams, graphs, etc., the expected data for a single device is up to 5 Mb. Uploading of a complete test will have an approximate size of 4 Mb per device.

Let us review a scenario with 30 wireless devices testing in a classroom on one 5 Ghz access point (often located in classroom or in the hallway). The desired maximum speed for Nextera at a single time would be 150 Mbps for the 30 devices of payload during downloading the tests. In theory, four classrooms downloading tests at the same time would need 600 Mbps for optimal performance at the time of downloading. Experiencing delayed download of the test (after a student selects **Start Test**) is related to number of connected devices, Wi-Fi access point, or network speed. The heaviest payload is only during the download of the test and minimal during the test. In the previous speed test example of 200 Mbps internet speed, I would have a bottleneck during the download when 40 or more students select **Start Test** at the same time. To correct the issue, limit the number of devices connected to a specified access point (30 to 45). Keep in mind that other devices such as laptops, tablets, or cell phones in the room or the next room may also be connected. Reduce the data download by staggering a comparable number of devices at a time. For example, 30 devices totaling 150 Mb for a 200 Mbps connection at a time as the next group of 30 devices start two to five minutes after. For efficiency, increase the supported bandwidth of 200 Mbps to a higher bandwidth to support more testing devices.

While taking the test, the information will be uploaded periodically in small packets of only a few kilobytes, such as the heartbeat and session state. Because the test is completely downloaded when starting a test, a student may continue taking the test even if the network disconnects. In the top-left corner of the Nextera Test Delivery System, a status indicator shows the active connection with a green checkmark; if the connection is not active it will show a red "X". In the case that the network disconnects, and multiple devices are waiting for the network to re-connect to submit, please follow these guidelines. Each device may have student responses up to 4 Mb of data waiting to submit if there is a loss in connectivity. Going back to the example of 20 Mbps upload speed, there will be a bottleneck if five or more devices (4 Mb each device) are to lose connectivity and reconnect at the same time to submit. You can correct the issue by limiting the number of devices submitting by staggering or increasing the bandwidth and upload speeds.

Checking Wireless Access Point Status

Many devices seen in school networks are the Meraki access points. This is a picture for reference and a quick guide to check the light status, easily seen and identifiable.



If the LED light indicator is green, then the Wi-Fi is working, and is connected to the network. If it is amber, then the access point is trying to get an uplink and attempting to connect to the internet. Visually confirming that the light is amber will tell you that there is no internet for this device. If it is white, the access point is connected and waiting for Wi-Fi devices to connect to it, no communication or data has gone through yet. This quick check can confirm if the access point is working correctly or not.

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 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; filtering also blocks undesired websites and/or content.
- **Authentication** controls which users and resources can access the Internet.

The Nextera TDS 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 TDS and the Internet on ports 80 and 443. The following domains should be whitelisted at the firewall, authenticating proxy server, or content filtering server:

***.questarai.com**

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. Use an NSlookup website to find the exact server address associated with our named addresses:

URL: http://ms.nextera.questarai.com **PORT**: 443

URL: http://ms.nextera.questarai.com **PORT**: 80

If you need to whitelist by IP address, the IPs for ms.nextera.questarai.com are currently 104.17.137.108 and 104.17.138.108. Please verify with "nslookup ms.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 and avoid performing client software updates, patching, and data backups.
  - Remove bandwidth throttling on ports 80 and 443.
  - 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 TDS, please contact NWEA Customer Support at 1-800-644-4054 or mscustomersupport@nwea.org.

Nextera Test Delivery System (TDS) Installation

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

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

The link to download the *Secure Browser* for each platform is available in Nextera Admin. To view the system requirements for each operating system, select the following link: Appendix B.

Select one of the following links for detailed installation instructions at the device level and the managed level for each device:

Windows Installation

macOS Installation

Apple iPad Installation

Chromebook Installation

Windows Installation

Windows provides a number of installation types to support nearly every possible configuration scenario. These include local workstation installations and server-based installations

For each Windows installation type, each student must have access to the cache location that contains the encrypted student responses. 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. Select one of the following links to view the sections that 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 *Secure Browser* is available on the device, uninstall the previous version before installing the updated version.

If you are uncertain if there is a previous version of the *Secure Browser* on the device, follow steps 1 through 3 below to verify a previous version exists. The steps outlined in these processes may vary slightly depending on your device and system setup.

1) From the **Start** menu, select **Control Panel.**
2) Select **Programs and Features.**
3) Locate the previous *Secure Browser*.
4) Use the secondary mouse button (commonly configured as a "right-click") to select the **Secure Browser** icon.
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 using the URL, User ID, and Password provided by your District Test Coordinator.
2) Under the **HELP** tab, select **Downloads.** Then select the file to download.
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 selecting the **Secure Browser** icon from your desktop.
7) Complete a sample test log in. Select the following link to view the steps to complete this task: Sample Test Log In.

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 *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 NWEA Customer Support team by calling 1-800-644-4054 or emailing mscustomersupport@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) APPLICATIONROOTDIRECTORY=”C:\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 *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 10 and later*, the cache location is:

%allusersprofile%\QuestarStudent\%username%

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

When the student launches the *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 Secure Browser cache**. The following example shows the format of a command line 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.

- 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 the following 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 PIDLs rather than files: https://docs.microsoft.com/en-us/windows/win32/shell/namespace-intro?redirectedfrom=MSDN#pidls

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, use the secondary mouse button and 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:

1) Disable the workstation lockout application, or
2) Configure the workstation lockout application to exclude the cache location, or
3) 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.

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

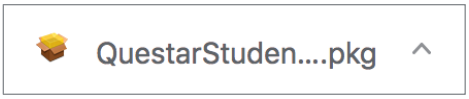
If a previous version of the *QuestarStudent* application is available on the device, uninstall the previous version before installing the updated version.

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 the *QuestarStudent* application**.**
5) Drag the application to the trash or use the secondary mouse button to selct the application and select **Move to Trash**.

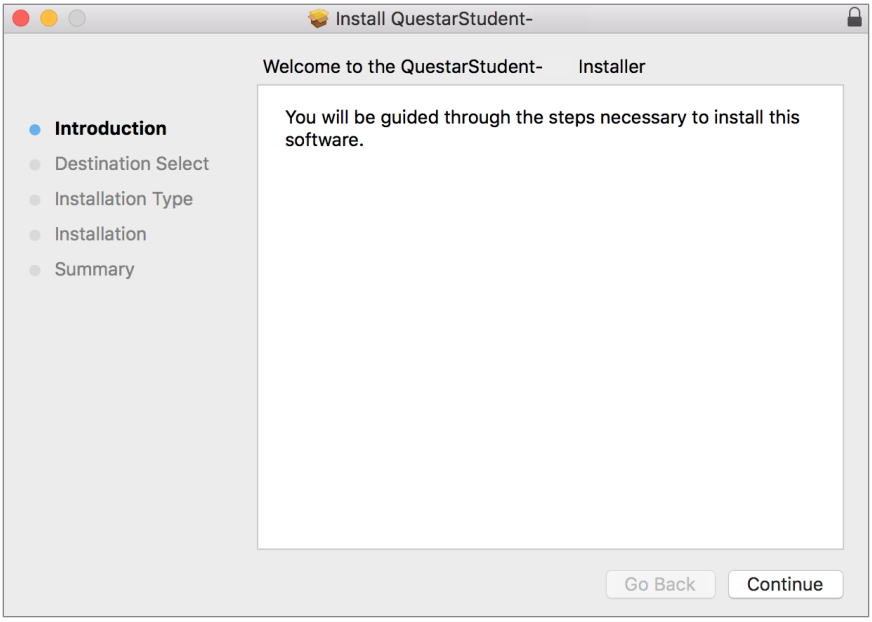
Install

The *Secure Browser* 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 using the URL, User ID, and Password provided by your District Test Coordinator.
2) Under the **HELP** tab, select **Downloads**, and then select the appropriate link for the macOS *Secure Browser,* and download the .pkg package.
3) The download starts. If using Chrome, the following image appears in the lower-left corner of the screen.

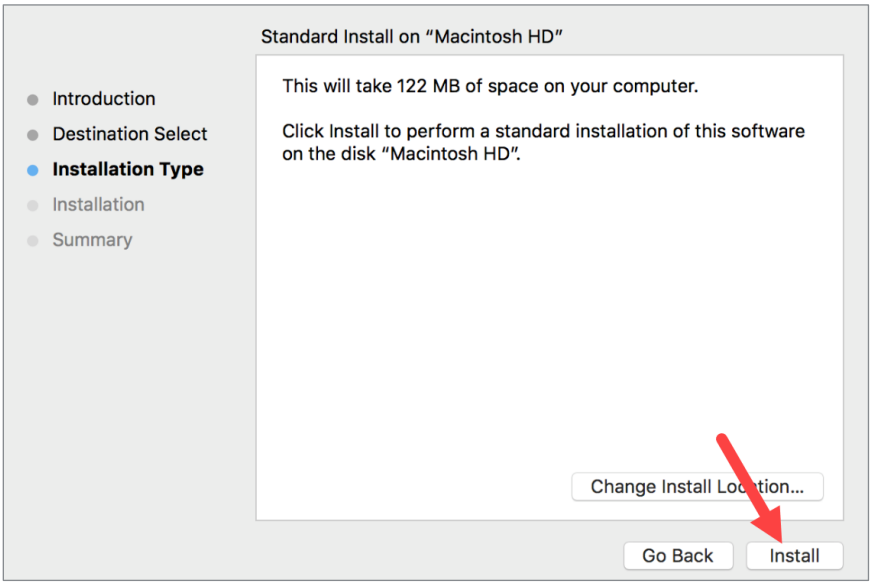


4) After the download is complete, select the up-arrow to open the file. The installation wizard will launch and the following window will display.

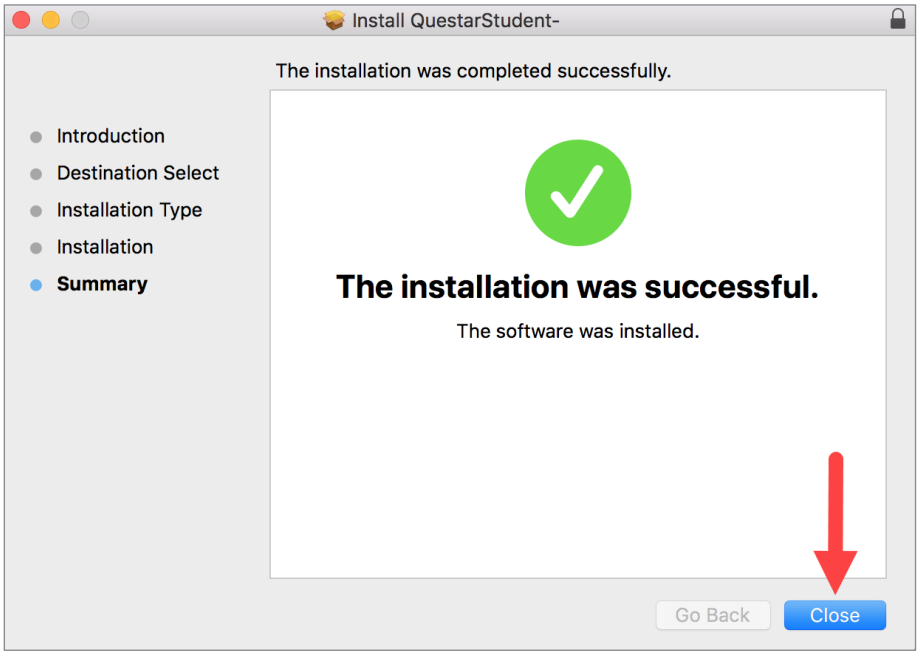


5) Select **Continue.**

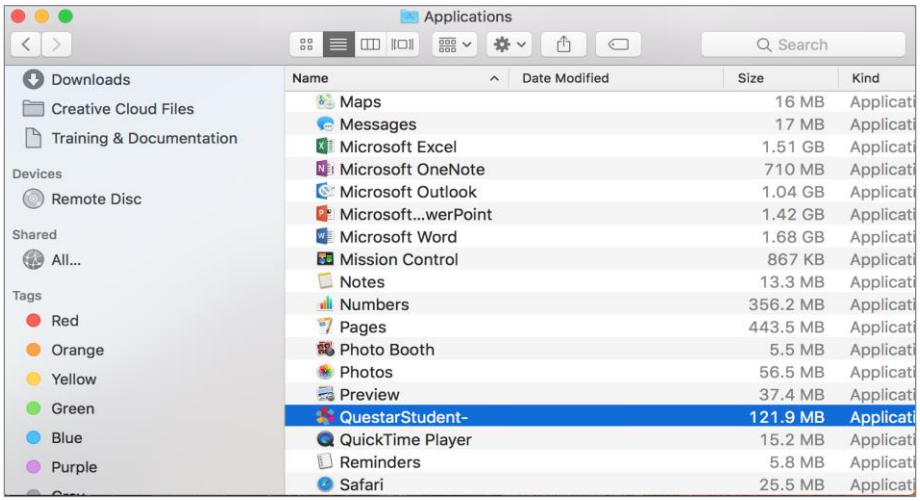
6) Select **Install.**



7) The browser will install and display the summary page below. Select **Close.**



8) Verify that the *QuestarStudent* application 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.

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.

Using Automatic Assessment Configuration (AAC)

AAC is recommended for secure testing in the *Questar Student Assessments* app. Using AAC, necessary restrictions will be automatically set using the instructions below.

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

1) Download and install the free *Questar Student Assessments* app from the Apple AppStore 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 > General > Keyboard > Keyboards > English**.
   b. Select **QWERTY** from the available options.

   AAC will automatically set other necessary restrictions.

After launching the app, select Mississippi from the *"Where do you want to go?"* page.

Additional Resources

For further information about iPad assessment configuration options, refer to Apple Support at the following link: https://support.apple.com/en-us/HT204775.

For more information about using iPads for assessments, contact NWEA Customer Support by calling 1-800-644-4054 or emailing mscustomersupport@nwea.org, or refer to Apple Support at: http://images.apple.com/education/docs/Assessment_with_iPad.pdf.

Chromebook Installation

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

App ID: nanoidlkencgghkphophigbmnohnbbcb

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 use 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.

Critical Note: Prior to test administration window opening, ensure "Do not erase local user data" is set under the Google Admin Console. The setting is located at Devices, Settings, Device; scroll down to Sign In Settings and look for User Data. If this setting is not changed before testing, there will be no data available if a student needs a test recovery. Additionally, this setting can cause concurrent lockout issues. Additionally, you must turn off or disable “Allow app to manage power” prior to testing occurring. If you do not turn off “Allow app to manage power”, the device may go to sleep during testing.

Additional Settings

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

Disable Sticky Keys: Windows

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

To disable Sticky Keys:

1) Open the Control Panel.
2) Select **Ease of Access Center**.
3) Select **Make the keyboard easier to use**.
4) Deselect the **Turn on Sticky Keys** checkbox.
5) Select **OK**.

Disable Alexa/Cortana: Windows

Disable Alexa

If you have downloaded Alexa, uninstall the 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, double-select "Allow **Cortana**".
6) In the Allow Cortana dialogue box, select **Disabled**, then select **OK**.
7) Close the *Local Group Policy Editor* and open the Run dialog box (Windows + R). Enter *gpupdate/force* and select **OK**.

Disable Fast User Switching: Windows

Fast User Switching allows multiple users to be logged in to one device and switch between the user profiles quickly. This feature is available on Windows machines. 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**.

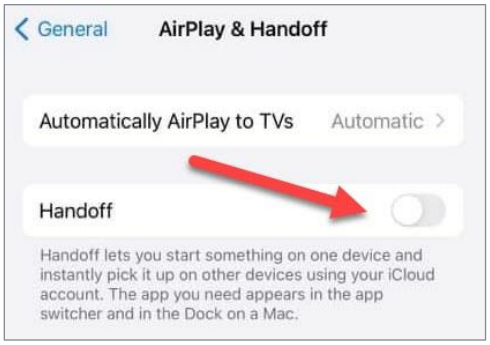
Disable Handoff on iOS

When your iPadOS devices are within Bluetooth range of each other, they can automatically "hand off" what you're 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.

This feature will need to be disabled through your MDM platform or individually on iPadOS devices prior to testing.

iPadOS

1) Navigate to *Settings*.
2) Select **General**.
3) Select **AirPlay & Handoff**.
4) Ensure *Handoff* is deselected.



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 minus symbol next to the Emoji Keyboard. Select **Done** after it opens.

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.

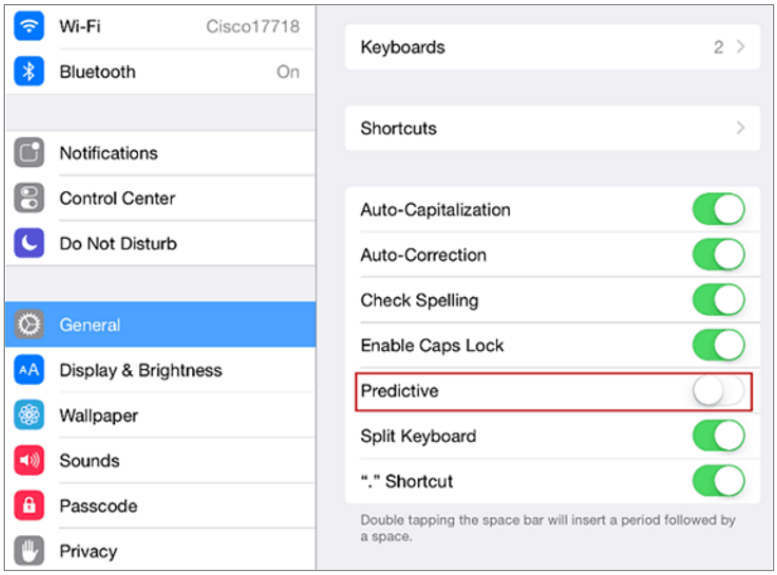
1) Login to your Google Admin Console.
2) Select **Devices** from the Home Screen.
3) Select **Chrome** from the left pane.
4) Select **Apps & Extensions** from the left pane.
5) Select **Kiosks** from the left pane.
6) Choose your OU from the left pane.
7) Select **Kiosks** on the upper right pane.
8) Select the 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.

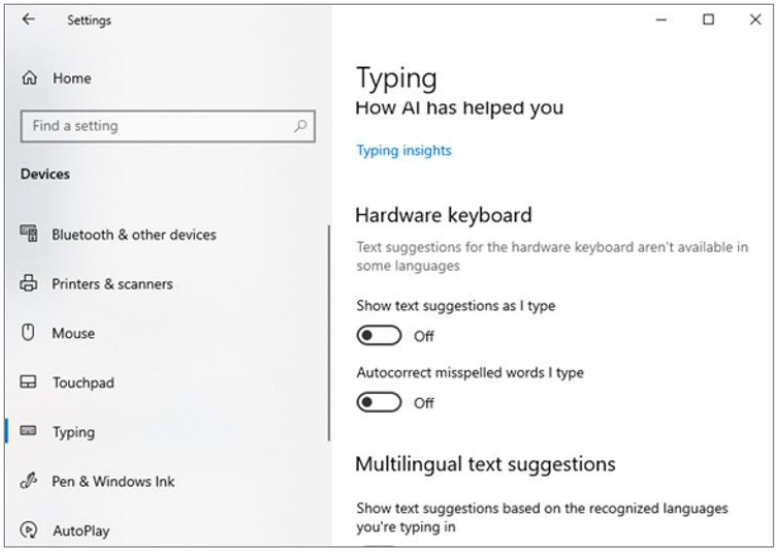
iPad

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



Windows 10

1) Select **Settings**, then **Devices**.
2) Select **Typing**.
3) Locate *Hardware keyboard* and toggle the pill-switch to **off**.



Approved 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 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

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	Goggle 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 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 *Secure Browser* from the desktop of student device(s).
2) Enter

   User ID: practice
   Password: practice

3) Navigate through the sample test to ensure:
   c. The test loads at an acceptable speed (select the following link to see details: Perform Test Readiness)
   d. Items render correctly and can be answered (items/answers don't bleed off the screen, etc.)
   e. Available tools work appropriately
   f. The test can be submitted upon completion via the Review screen

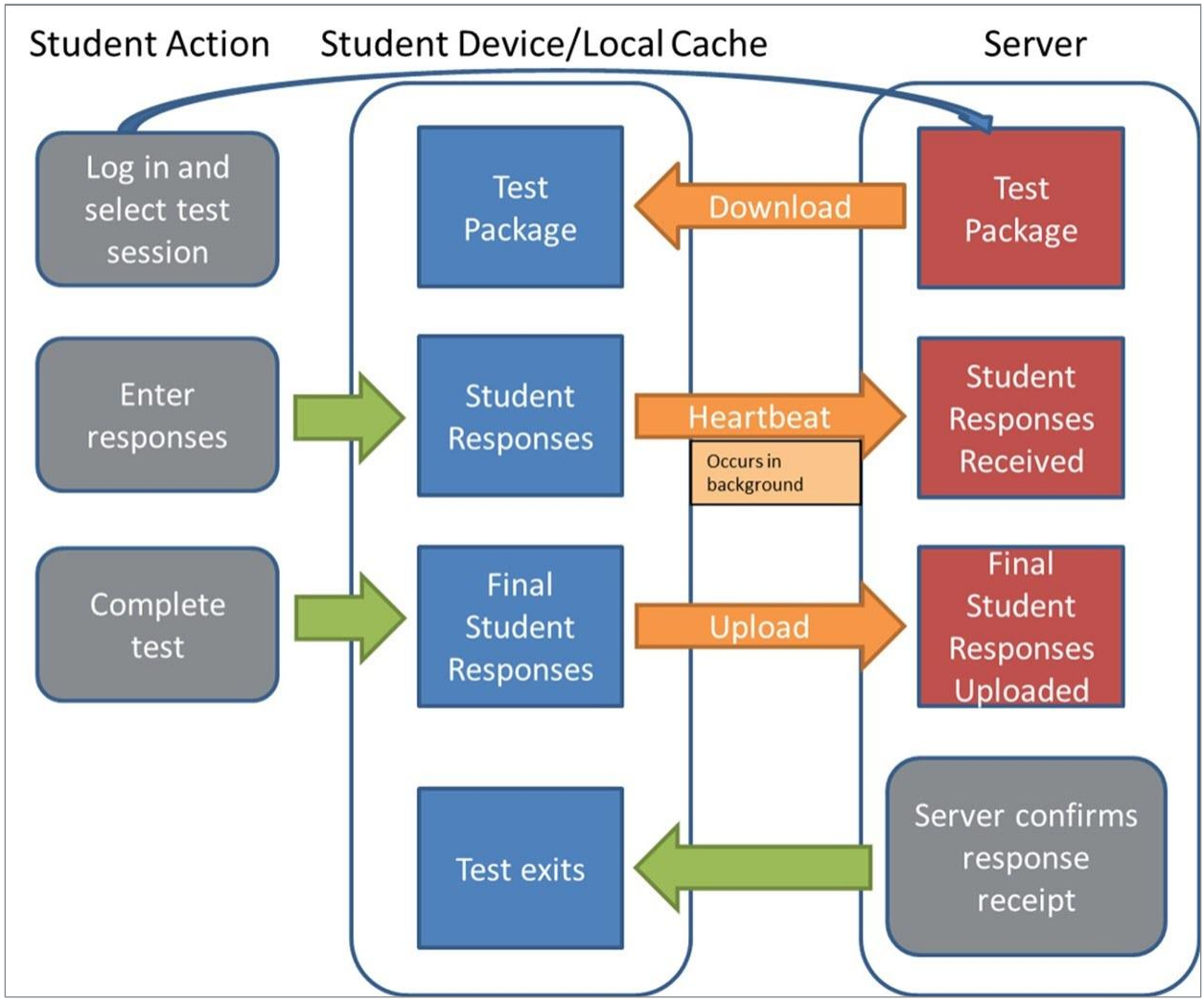
Appendix A – Student Response Flowcharts

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.

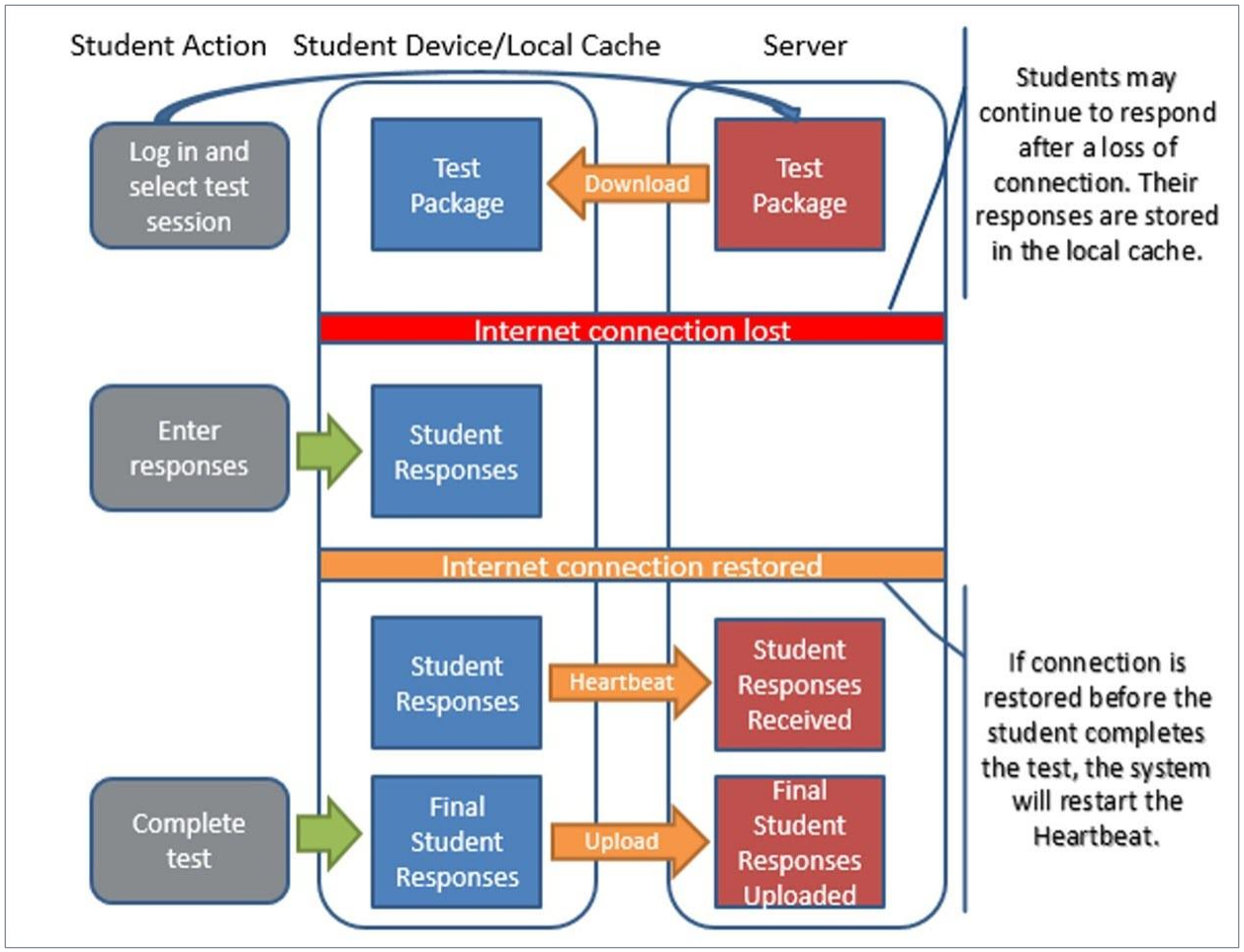
Continuous Internet Connection

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 test will exit on the student's device.



Internet Connection Lost and Restored During Testing

If the 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.

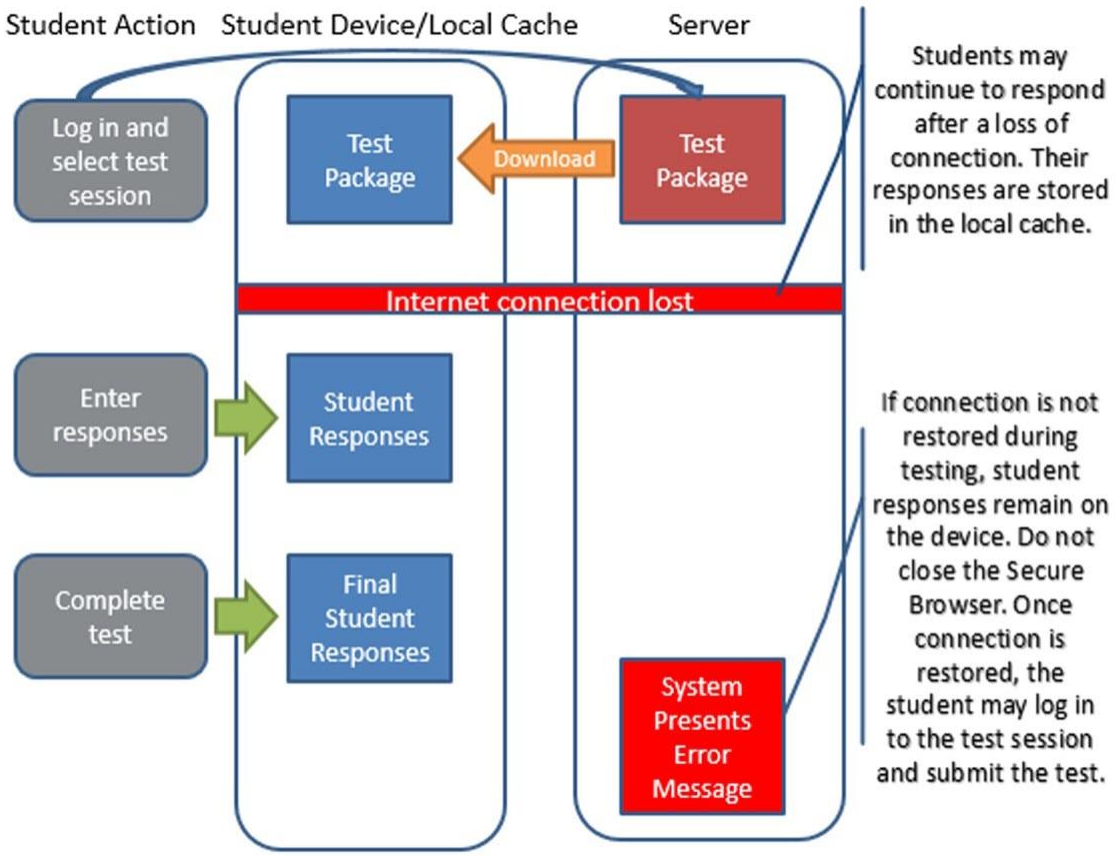


Note: Text-to-Speech (TTS) requires an Internet connection. When the Internet connection is restored, the student with the TTS accommodation will be able to select **play** and TTS will load again.

Internet Connection Lost

If the 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.



Note: Text-to-Speech (TTS) requires an Internet connection. TTS will be unavailable until the Internet connection is restored.

Appendix B – System Requirements

General System Requirements

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

Note: All OS support is for release 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: http://www.questarai.com/readiness/.

Appendix C – Frequently Asked Questions (FAQ)

Can a student continue 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 on which he or she began testing. Only if the device is permanently incapacitated or the student cannot be held any longer should another device be used. Before the student resumes testing, contact NWEA Customer Support by calling 1-800-644-4054 for instructions specific to the situation.

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 the Nextera TDS during testing.

Can a student use a touchscreen device for testing?

Nextera supports any touchscreen interaction from devices with supported operating systems that meet or exceed the minimum specifications as noted on the Test Readiness page at the following link: http://www.questarai.com/readiness/.

Appendix D – Troubleshooting Tips

Issues Loading Test

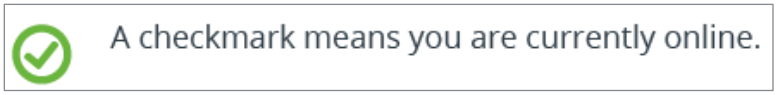
If you experience latency while the test is loading, review the following list of possible solutions presented in an order to most likely resolve the issue:

- 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 domain name (*.questarai.com) is 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 to be top priority in the firewall or content filter.
- Add *.questarai.com to the ignore list/blanket bypass if one is in use.
- Use the secondary mouse button, select **quit secure browser**, and log in again. This issue may be the result of a 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 app, then turn on and off **Airplane mode** under *Settings*. This will reset all radios, allowing the device to create a clean network connection.

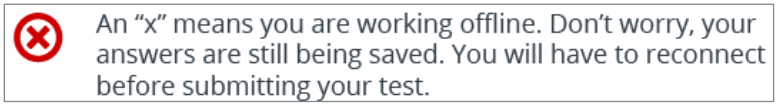
Response Recovery When Internet is Disconnected Prior to Test Session Submission

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 TDS changes from green to red.



- If connectivity is lost, a “Lost Connection” message displays.



- If the network connection is restored, the responses will automatically submit, and the display will return to the Nextera TDS login screen.

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:

1) Have the student log in to the Nextera TDS, select the session that lost connectivity, and enter the session access code.
2) After the "Loading your test" message disappears, have the student select **Start test**. The stored responses are now synced between the device and the NWEA server, and the responses are visible within the TDS. The student may resume or submit the test.

If "Switching Application" Error Has Ended the Testing Session:

1) Turn off all software updates, patching, and data back-ups on testing devices.
2) Turn off anti-virus software on testing devices.
3) For macOS devices, accept any permission pop-ups.
4) Use fully-charged or, preferably, plugged-in devices. A low battery warning can cause this.
5) Turn off any network sniffers that touch devices to monitor student web activity.
6) Disable or uninstall interactive software on the device. **Please note**: this may include device monitoring software such as NetRef, Classwize, and Artistotle.
7) Make sure there are no applications running on the device. (Event/Error Logs may help locate what is running.)
8) Disable all device power-saving and notification settings.
9) Disable Windows Sticky Keys, Fast User Switching, Mac Handoffs, Mac Siri, and Windows 3-finger and 4-finger touchpad functionality.
10) Plug in headphones prior to launching the Secure Browser (if the student has the Text-to-Speech accommodation).
11) Ensure the student did not select any keyboard commands.

-118 Error Code/Unable to Access https://nextera.questarai.com

The workstation is unable to access the site.

1) 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.
2) 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.

Graphing Item Issues/Secure Browser Locks Up After Login (Randomly)

Check the following items for possible conflicts while troubleshooting display issues:

1) Verify the graphics card driver is up to date.
2) Check for conflicts with an anti-virus program.

Issues Editing Constructed Responses

Select the **Insert** key to ensure the keyboard is in insert mode rather than overtype mode. When a keyboard is in overtype mode, existing text is deleted as new text is written. Selecting the **Insert** key again changes back to insert mode.