Setup & Installation Guide

Nextera®

GAA 2.0 Spring 2022
# Contents

Introduction to the Nextera Assessment System ................................................................. 5
   Overview .................................................................................................................. 5
   Security and the Student Experience ........................................................................ 5
Preparing your Site - General ......................................................................................... 6
   Checklist of Preparation Activities ............................................................................ 6
      4 Weeks Prior to Testing ....................................................................................... 6
      3 Weeks Prior to Testing ....................................................................................... 6
      2 Weeks Prior to Testing ....................................................................................... 6
      During Testing ........................................................................................................ 6
Preparing your Site – Step by Step  .................................................................................... 7
   OS-Specific System Requirements ............................................................................. 7
   Perform System Scan ................................................................................................ 7
   Perform Test Readiness ............................................................................................ 8
Network Considerations and Setup ................................................................................. 8
   Proxy Servers / Firewalls / Web Content Filters ..................................................... 8
Nextera Test Delivery System (TDS) Installation ............................................................ 10
   Windows Installation .............................................................................................. 10
      Uninstall .............................................................................................................. 11
      Basic Installation - Individual Device ................................................................. 11
   macOS Installation ................................................................................................. 14
      Uninstall .............................................................................................................. 14
      Install .................................................................................................................. 14
   Apple iPad Installation ............................................................................................. 18
      Using Automatic Assessment Configuration (AAC) ............................................. 18
   Chromebook Installation ......................................................................................... 19
      Preparing Chromebooks ...................................................................................... 19
Additional Settings .......................................................................................................... 20
   Disable Sticky Keys: Windows ............................................................................... 20
   Disable Alexa/Cortana: Windows ............................................................................ 20
      Disable Alexa ........................................................................................................ 20
      Disable Cortana ................................................................................................... 20

Last Updated: 12/16/2021
Disable Siri: MacOS Versions Prior to 11.4 ................................................................. 21
Disable Fast User Switching: Windows & MacOS Versions Prior to 11.4 .................. 21
  Windows .............................................................................................................. 21
  MacOS Versions Prior to 11.4 ............................................................................. 22
Disable Handoff on Mac Devices .......................................................................... 22
  macOS Versions Prior to 11.4 ............................................................................ 22
  iOS ....................................................................................................................... 23
Disable App Power Management: Chromebook ...................................................... 24
Sample Test Login .................................................................................................. 25
Appendix A – Frequently Asked Questions (FAQ) .................................................... 26
Appendix B – Troubleshooting Tips ........................................................................ 27
  Issues Loading Test .......................................................................................... 27
  Response Recovery When Internet is Disconnected Prior to Test Session Submission ................................................................................................................. 27
  If “Switching Application” Error Has Ended the Testing Session: ..................... 28
  Graphing Item Issues/Secure Browser Locks Up After Login (Randomly) ............ 29
  Issues Editing Constructed Responses ................................................................ 29
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.

- **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 Questar Secure Browser.
- The **Nextera Test Delivery System (TDS)** is a software application for completion of student assessments delivered through the Questar Secure Browser.

The technology coordinator should have received an email with a URL, username, and password to access the Nextera Admin. If this information has not been received, or has been misplaced, contact Customer Support by calling 1-866-997-0698 or emailing ga@questarai.com.

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 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.

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 Questar 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
- Verify that your testing devices meet the minimum OS-Specific System Requirements
- Perform System Scan
- Perform Test Readiness
  - If using wireless networks, ensure there is ample coverage and capacity to support testing.
- Download/deploy the Questar Secure Browser to all devices being used for student testing.

3 Weeks Prior to Testing
- Log in to the Sample Test using the Questar Secure Browser.

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 — Student Response Flowcharts).

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 on the Questar website at http://www.questarai.com/readiness/ or in a subsequent Questar 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

**OS-Specific System Requirements**

For details on specific supported devices, operating systems, and specifications, please visit the Questar Readiness page at the following link: [http://www.questarai.com/readiness/](http://www.questarai.com/readiness/).

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

**Perform System Scan**

**Please note:** The System Scan is designed to validate desktop device configurations. Select the following link for additional detail about tablet devices and Chromebooks: [Appendix B – System Requirements](http://www.questarai.com/readiness/).

2) Locate the *System Scan* message 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/](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 message 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 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 Questar’s Customer Support by calling 1-866-997-0698 or emailing ga@questarai.com.

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, 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 at any point you would like assistance, contact Questar’s Customer Support by calling 1-866-997-0698 or emailing ga@questarai.com.

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; blocks undesired websites and/or content.

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

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://GA.nextera.questarai.com  **PORT**: 443
- **URL**: http://GA.nextera.questarai.com  **PORT**: 80

If you need to whitelist by IP address, the IP’s for ga.nextera.questarai.com are currently Enter IP address for program and 104.17.137.108 and 104.17.138.108. Please verify with “nslookup Choose an item.” 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 Test Delivery System (TDS), please contact Questar’s Customer Support at 1-866-997-0698 or ga@questarai.com.
Nextera Test Delivery System (TDS) 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
- **Questar Mobile App** – for Apple iOS iPad Devices
- **Questar-<Program Abbreviation>** – for Google Chromebooks

The link to download the **Questar Secure Browser** for each platform is available on Nextera Admin. To view the system requirements for each operating system, select the following link: [http://www.questarai.com/readiness/](http://www.questarai.com/readiness/).

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 mass deployment push 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 Questar 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 Questar 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 Questar Secure Browser.
4) Select using the secondary mouse button (commonly configured as a "right-click") the Questar 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 Questar 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 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 Questar’s Customer Support team by calling 1-866-997-0698 or emailing ga@questarai.com.

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 *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 10 and later*, 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 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.

**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 11.4 and above. 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 select using 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 select using the secondary mouse button the application and select Move to Trash.

Install

The Questar Secure Browser requires accessibility permission for all MacOS versions prior to 11.4. If permission is not already granted, the installation will prompt for permission to access the Accessibility API and will open the correct pane in System Preferences.

(System Preferences -> Security & Privacy -> Privacy -> Accessibility). To grant the permission:

1) Select the padlock icon.

1) Enter your administrative credentials, then select Unlock.
2) Select the checkbox next to the QuestarStudent application.

The Questar 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 using the URL, User ID, and Password provided by your District Test Coordinator.

2) Under the HELP tab, select Downloads, then select the appropriate link for the macOS Questar 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 this summary page. 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 for MacOS Versions Prior to 11.4:*

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 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 Assessment for Students app from the iTunes 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 iOS home page, select Settings > General > Keyboard > Keyboards > English.

b. Select QWERTY from the available options.

AAC will automatically set other necessary restrictions.

3) After launching the app, select Choose an item. 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 Questar’s Customer Support by calling 1-866-997-0698 or emailing customerservice@questara.com or refer to Apple Support at https://www.apple.com/education/docs/Assessment_Overview.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 or URL in conjunction with the following scenarios:

  App ID: alghbelckolpianljmnjmaedakphepfo
  URL: https://chrome.google.com/webstore/detail/questar-ga/alghbelckolpianljmnjmaedakphepfo

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.

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.
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 Change how your keyboard works.
4) Deselect the Turn on Sticky Keys check box.
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 Siri: MacOS Versions Prior to 11.4

Siri must be disabled prior to testing. Open Siri in System Preferences and deselect the Enable Ask Siri checkbox.

![Siri Preferences](image)

**Note:** You may need to restart the device after disabling Siri.

Disable Fast User Switching: Windows & MacOS Versions Prior to 11.4

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 and Mac 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.
MacOS Versions Prior to 11.4

1) From the Apple menu, select System Preferences.
2) From the View menu, select Accounts. On MacOS Catalina Accounts is listed as “Users & Groups”
3) Select Login Options.
4) Deselect the Enable fast user switching.

Note: Make sure to complete all iCloud or other configuration tasks prior to testing to assure that prompts or popups do not interfere with testing.

Disable Handoff on Mac Devices

When your macOS computers and iOS 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 macOS and iOS, 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 macOS versions prior to 11.4 and iOS devices prior to testing.

macOS Versions Prior to 11.4

1) From the Apple menu, select System Preferences.
2) Select General.
3) Ensure the Allow Handoff between this Mac and your iCloud devices box is deselected.
iOS

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

![Handoff setting](image)

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.
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 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:
   
a. The test loads at an acceptable speed (select the following link to see details: Perform Test Readiness)

b. Items render correctly and can be answered (items/answers don’t bleed off the screen, etc.)

c. Available tools work appropriately

d. The test can be submitted upon completion via the Review screen
Appendix A – 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. 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.

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.

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 Questar Readiness page at the following link: [http://www.questarai.com/readiness/](http://www.questarai.com/readiness/).
Appendix B – 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 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.
- Close out of the app and toggle Wifi Off then back On.
- 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.

  ![A checkmark means you are currently online.](image)

- If connectivity is lost 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.](image)

- 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 Questar server. From the device that lost connectivity, follow the steps below to upload the stored responses:

- Refer to the State Department of Education 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:

  1) Log in to the Nextera TDS with the user’s login username and password, select the session that lost connectivity, and enter the session access code.

  2) After the “Loading your test” message disappears, select Start test. The stored responses are now synced between the device and the Questar server, and the responses are viewed within the TDS. The user may resume completing and/or submitting 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 sniffer that touch devices to monitor student web activity.

6) Disable or uninstall interactive software on the device.

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 press any keyboard commands.
-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.

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

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

- Verify the graphics card driver is up to date.
- 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 overwrite mode, existing text is deleted as new text is written. Selecting the **Insert** key again changes back to insert mode.