Setup & Installation Guide

Nextera™

New York Spring 2016

Contents

Introduction to the Nextera Assessment System

Overview

The Nextera Assessment System is a suite of software applications used for conducting test 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** – a web-based application for loading and managing district, school, class, and student information. The Help Tab contains links and downloads, including the Questar Secure Browser.
- **Questar Secure Browser** – a client software application for administering practice and student assessments delivered through the **Nextera Test Delivery System**.

> 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, please contact **Customer Support** by calling **877-997-0422** or emailing **customerservice@questarai.com**.

Security and the Student Experience

As a technology coordinator you may be asked about test security, recommendations, and the student experience. The testing delivery system is designed to prevent a student from navigating away from the Questar Secure Browser while testing. Many keyboard shortcuts are disabled. If a student testing with a Windows PC attempts to use the Print Screen key or Ctrl+Alt+Delete, 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.

If a student experiences loss of internet connectivity during testing, they may continue testing. The student's responses are saved to an encrypted local cache on the device. Refer to Appendix A for flowcharts and scenarios.

Preparing your Site - General

Preparedness is the first step towards a successful assessment program. Use the following checklist as a guideline for your preparation. Following the checklist, see the instructions to evaluate your site using the Site Setup tools available on the Questar website at http://www.questarai.com/support . 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 Site Setup – System Scan
- ✓ Perform Site Setup – Test Readiness
  - o If using Wireless Networks, ensure ample coverage and capacity to support testing
- ✓ Download/deploy Questar Secure Browser to all devices being used for student testing

3 Weeks Prior to Testing

- ✓ Log in to Sample Form using the Questar Secure Browser

2 Weeks Prior to Testing

- ✓ Ensure Test Administrators are aware of district policies, expectations and processes for troubleshooting issues (see Appendix A)

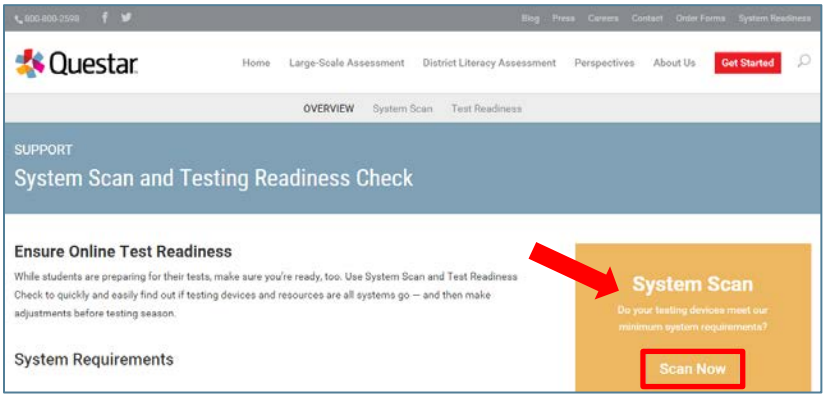
During Testing

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

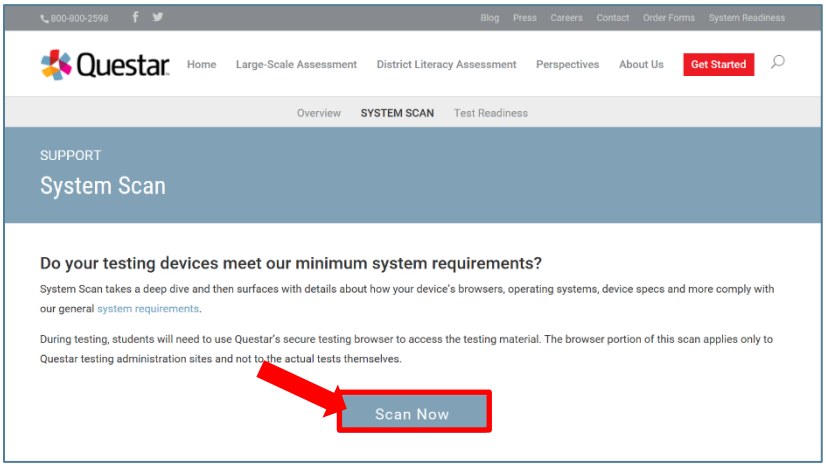
Preparing your Site – Step by Step

Perform Site Setup – System Scan

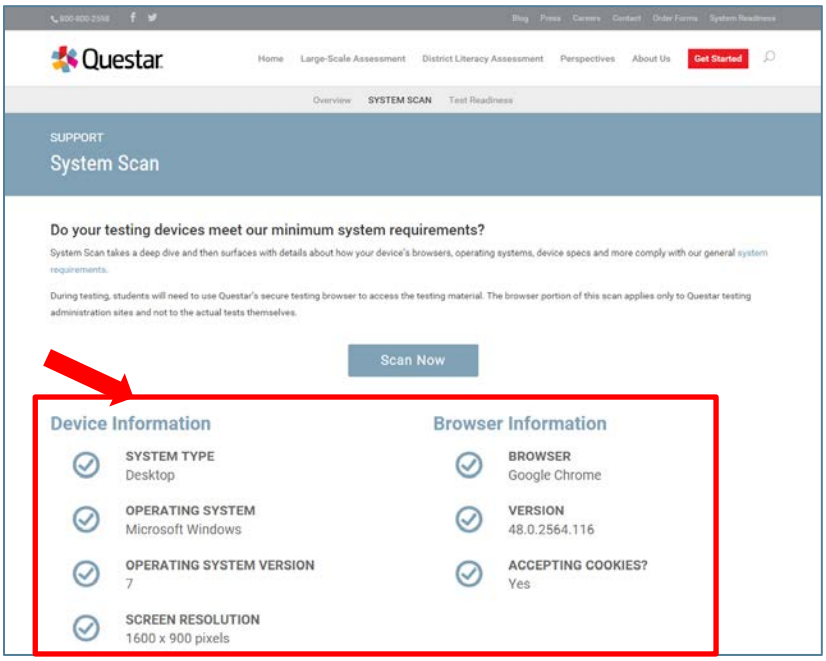
1) Open a web browser and access www.questarai.com/support
2) Locate the *System Scan* message and select *Scan Now*



3) Select *Scan Now*



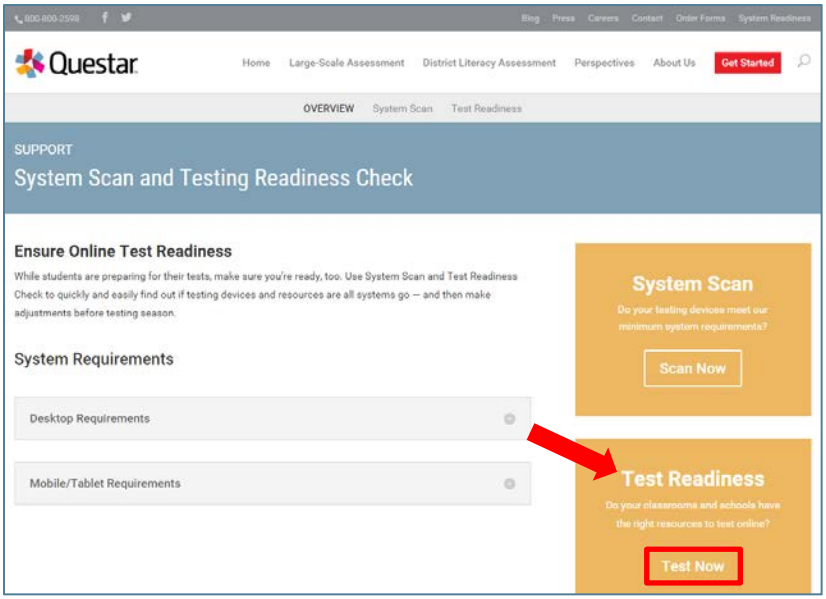
4) The scan results display. If a warning message displays, verify the workstation has the minimum system requirements specified for that type of device. See Appendix B for System Requirements.



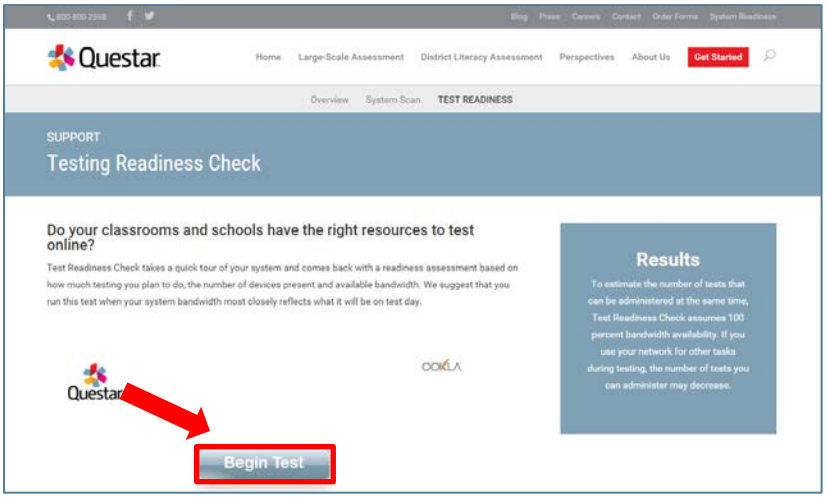
Perform Site Setup – Test Readiness

If you have just completed System Scan, begin at step 2

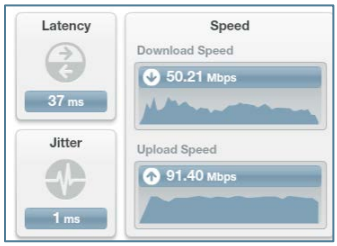
1) Open a web browser and access www.questarai.com/support
2) Locate the *Test Readiness* message and select *Test Now*



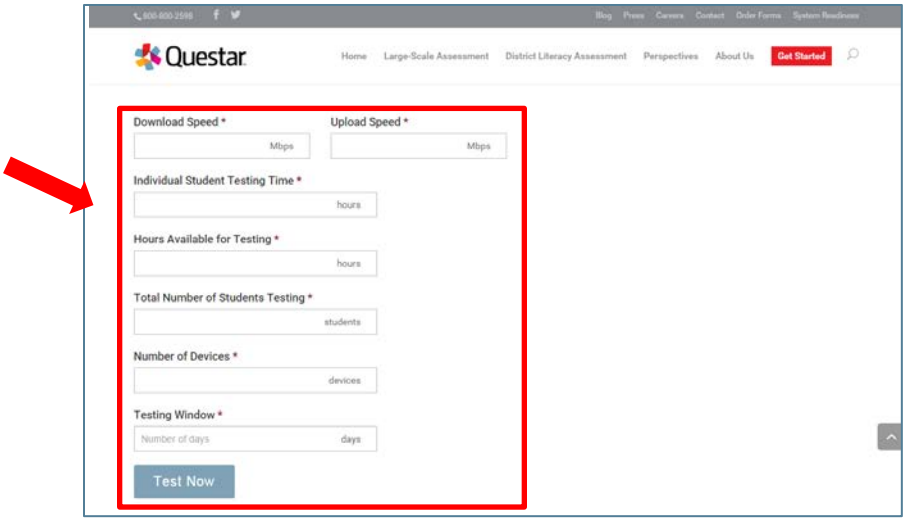
3) Select *Begin Test.* The test process may take a few minutes to complete. It is recommended that you run this test at the same time of day you will be testing.



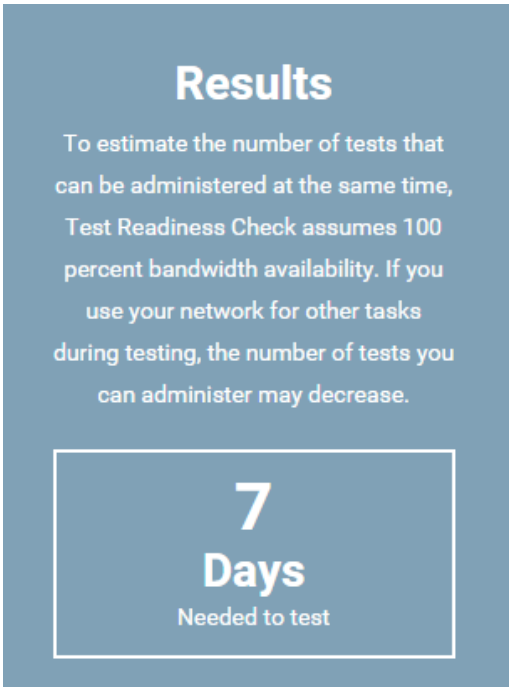
4) The results display and include latency, jitter and speed test results.



5) To estimate the number of tests that can be administered at the same time, input data in highlighted fields and select *Test Now.* The download and upload speeds are found in the test results from the prior step.



6) 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 **877-997-0422** or emailing **customerservice@questarai.com**.

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 Questar Secure Browsers from desktop of student device(s).

2) Enter User ID: Practice
Password: Practice

3) Navigate through the sample test to ensure:

* Test loads at an acceptable speed (see Perform Site Setup – Test Readiness for details)

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

* Available tools work appropriately

* The test can be submitted upon completion via the Review screen

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 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 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 Questar Assessment System 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**

***.questarai.net**

***.mobileapp.questarai.com (**for Apple iPad devices)

When using authenticating proxies, ensure the proxy is configured to allow access **without authentication**.

The Questar Assessment System must be able to communicate with the proxy server using the hostname and port number, which is typically obtained from the system-defined Internet properties (i.e., browser settings).

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: http://ny.nextera.questarai.com/ **PORT**: 80

Direct IP: 192.229.163.149

Nextera Test Delivery System Installation

- 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 virus.

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

- **Questar Secure Browser** – for Windows OS and Mac
- **Questar Mobile App** – for Apple iOS iPad Devices
- **Chrome Secure Browser or Chrome App** – for Google Chromebooks

The Questar Secure Browser for each platform is available on the Nextera Admin and the system requirements for each operating system are listed in Appendix B.

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

Windows Installation

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

For each Windows installation type, the location of the client cache, which contains the encrypted student responses, must be managed individually for each student according to the deployment method used. Each student account must also have sufficient rights to this cache location, which is used to protect the student's test responses if network connectivity is lost. Refer to Cache Location for instructions on changing the default location of the cache files.

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

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 whether or not there is a previous version of the Questar Secure Brower on the device, follow steps 1 through 3 below.

1) From the **Start menu**, select **Control Panel**
2) Select **Programs and Features**
3) Locate the previous Questar Secure Browser
4) Right-click on 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**

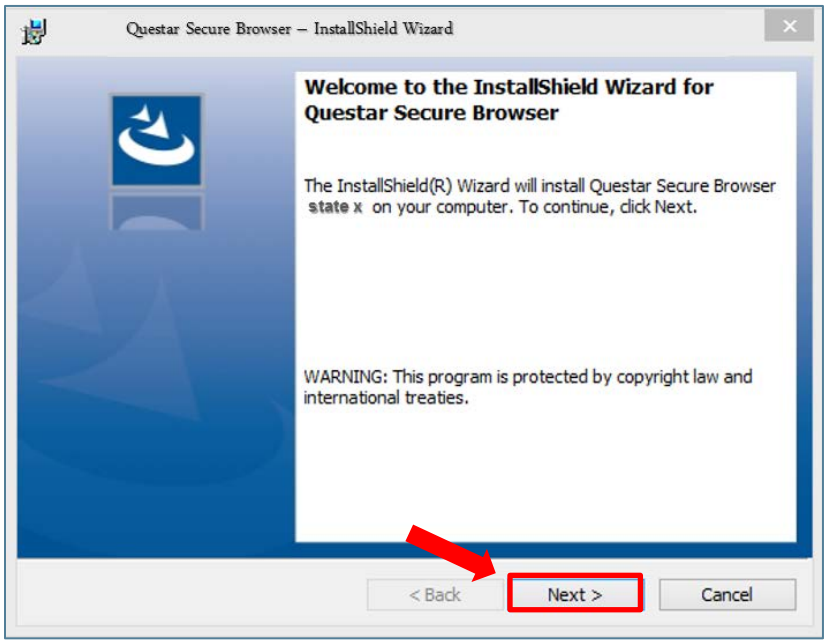
Basic Installation- Individual Device

1) Access the 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) To use the default destination folder, select **Next**
   To change the default destination folder, select **Change**
5) Select **Install** to start the installation process
6) Select **Finish** to complete the installation wizard
7) Verify the installation is complete by launching the *Questar Secure Browser* icon from your Desktop
8) Follow the Sample Test Login steps

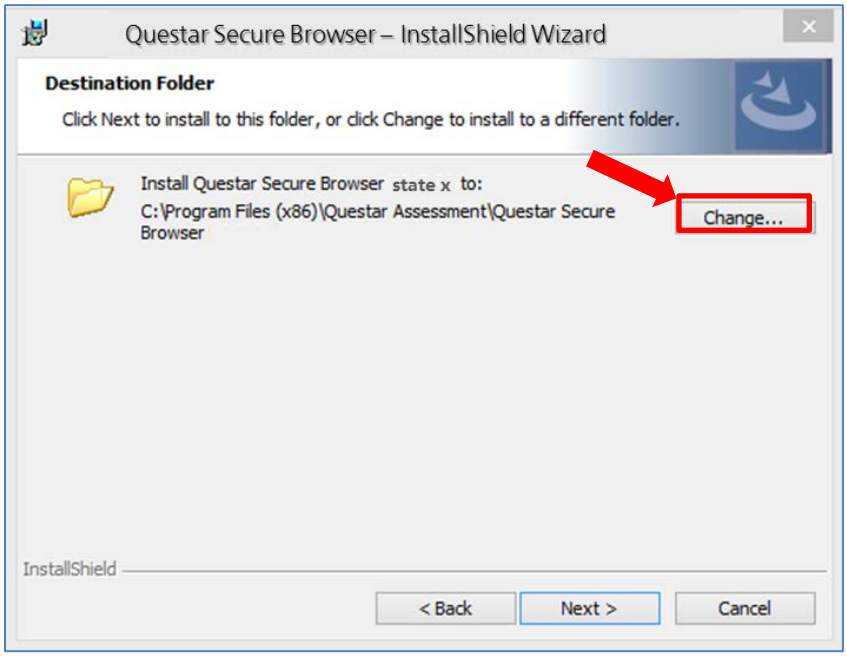
File Server Installation

The steps to perform a file server installation are similar to a basic installation with the primary difference being the location of the files and the method for sharing the shortcut to the Questar Secure Browser. Since this method depends largely on the local environment and your preferences, the following steps highlight the key requirements for deploying the application.

1) Access the Nextera Admin.
2) Locate and select the appropriate.*msi* file.
3) Select **Next** to begin the installation wizard.

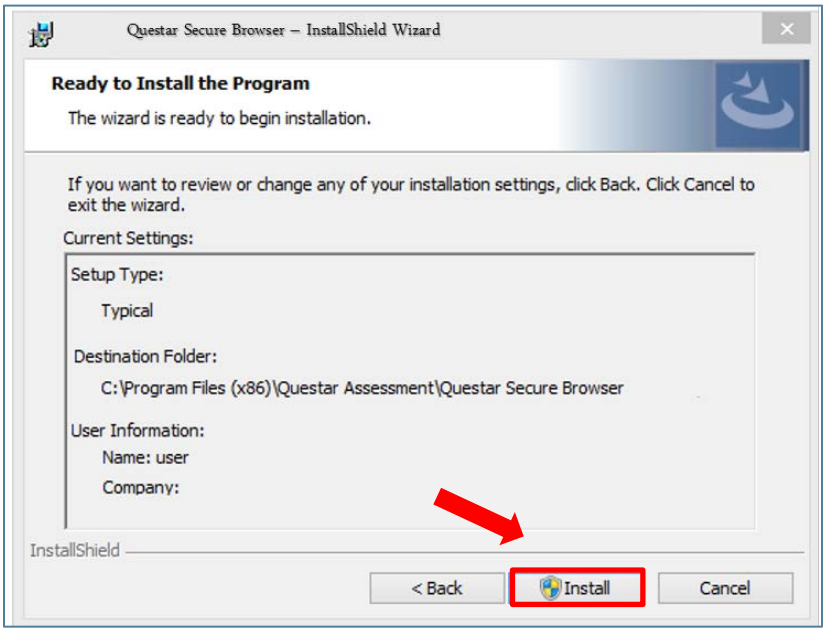


4) Select **Change** and enter the UNC file path to your file server folder.

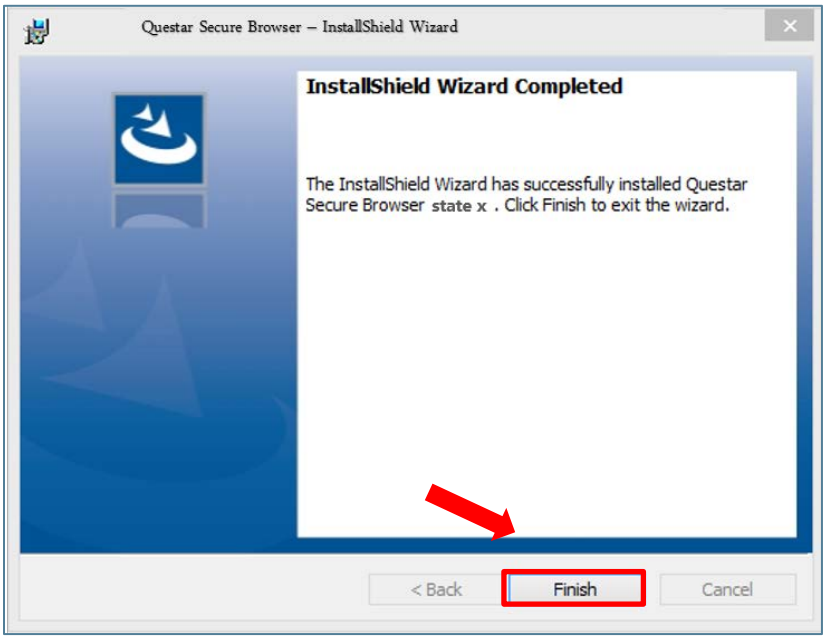


5) Select **Next.**

6) Select **Install** to start the installation process.



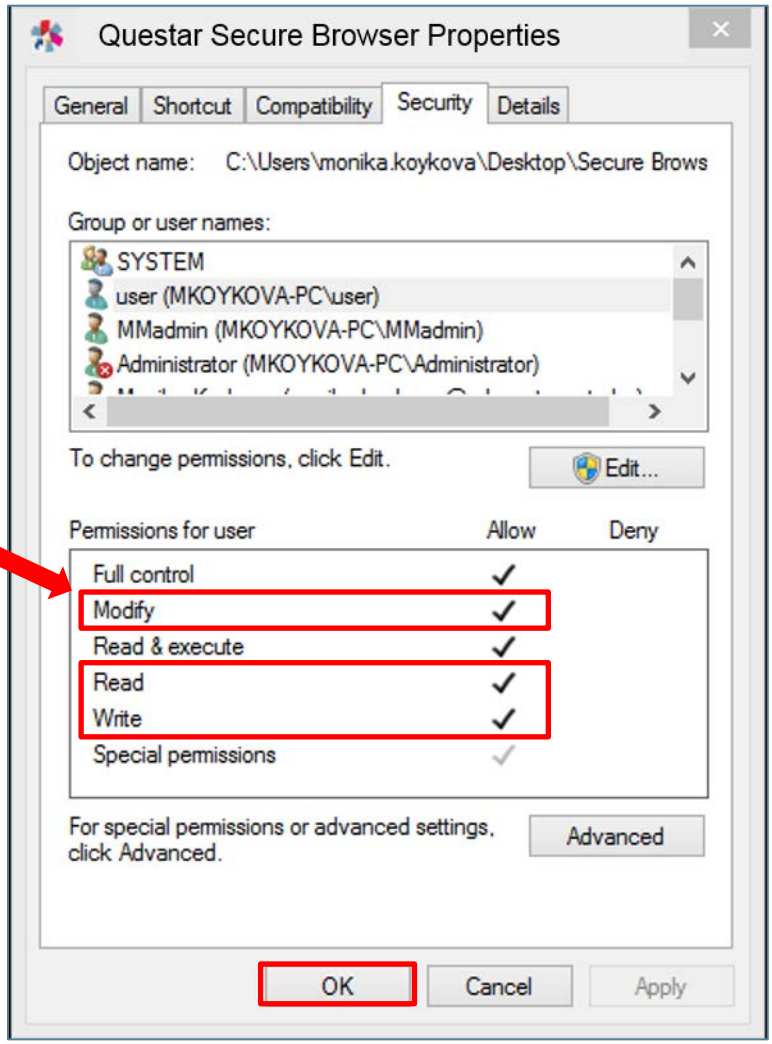
7) Select **Finish** to complete the installation wizard.



8) The final step in a file server installation is to create and share a shortcut with each Windows account. This can be accomplished in many ways by using Windows Group Policy, login scripts, PowerShell, or simple batch files. The critical step here is to **ensure students' accounts have sufficient rights to launch the application**. The following steps demonstrate how to create and apply security rights to a Windows shortcut.

Creating and Sharing a Shortcut

1) Right-click on the *QuestarStudent.exe* file created from your File Server installation, pasting the new shortcut to your file share location.
2) Right-click on the *shortcut*, select **Properties** and select **Security**.
3) Using a Windows security group (as shown below), apply **Read**, **Write** and **Modify access** rights to the group and select **OK**.
4) 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. The following are some examples of how to use the Windows Installer command line parameters.

- **Silent Install** - msiexec /i /qn c:\Downloads\QuestarSecureBrowser-ny-x32.msi
- **Silent Install to a specified directory** - msiexec /i /qn c:\Downloads\QuestarSecureBrowser-ny-x32.msiINSTALLDIR="c:\StudentData\Username\"

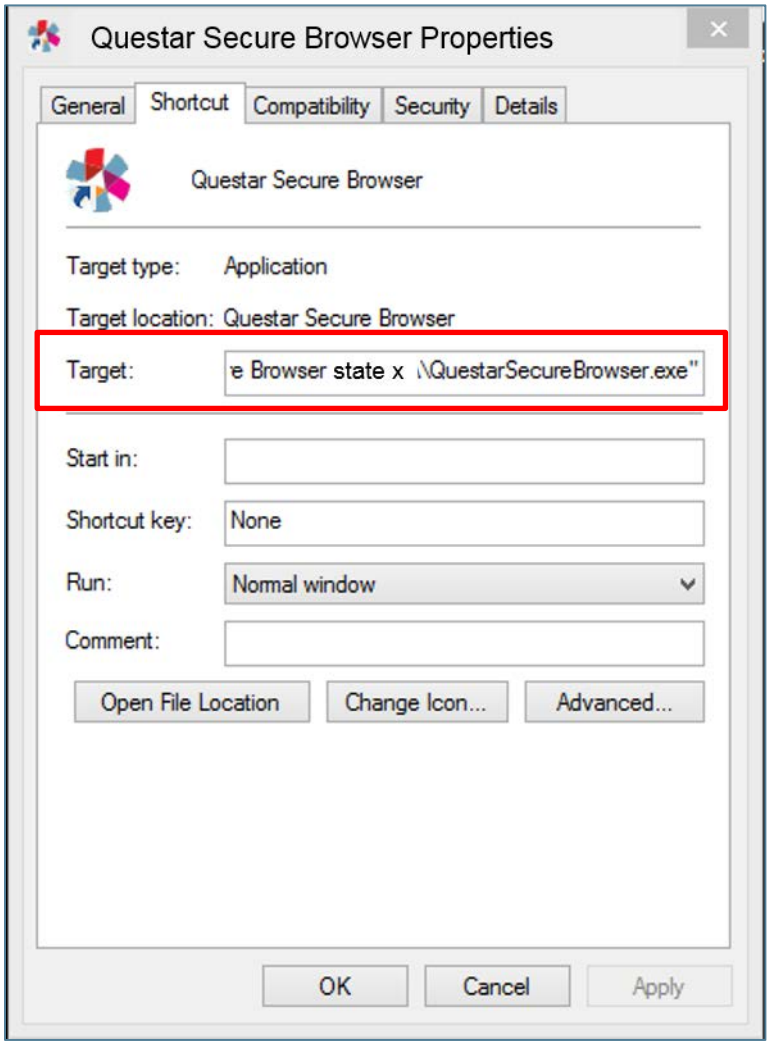
Cache Location

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 7 and later*, the cache location is created under the directory C:\ProgramData\QuestarSecureBrowser***(***username***)***
- On the *legacy version of the secure browser*, the cache location is located in %ALLUSERSPROFILE%\Questar Secure Browser\Cache directory\%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 this switch and how it can be used to change the location of the cache.



In this example, the Windows shortcut has been modified by adding the command line switch in the Target field (QuestarSecureBrowser.exe—user-data-dir="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.

- 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 following the instructions Creating and Sharing a Shortcut in this guide, with the additional command line switch added to change the cache location to a network share.

- In this case, the following cache path was used in the Windows shortcut being distributed: QuestarSecureBrowser.exe—user-data-dir="\\Server\%USERNAME%\cache"

Here a UNC path is being used to store the cache along with the Windows %USERNAME% variable to create individual cache directories. Using this command line switch provides technology coordinators with flexibility when deploying the Secure Browser client.

Workstation Lockout Applications (DeepFreeze™ or CleanSlate™)

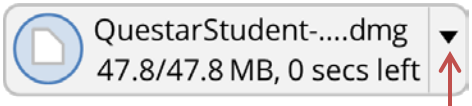
If you have any scripts or applications, such as DeepFreeze™ or CleanSlate™, that clear out student profiles, complete one of the following actions:

- 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.

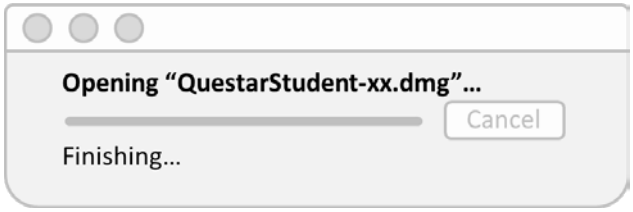
Mac OS X Installation

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 Mac OS client.

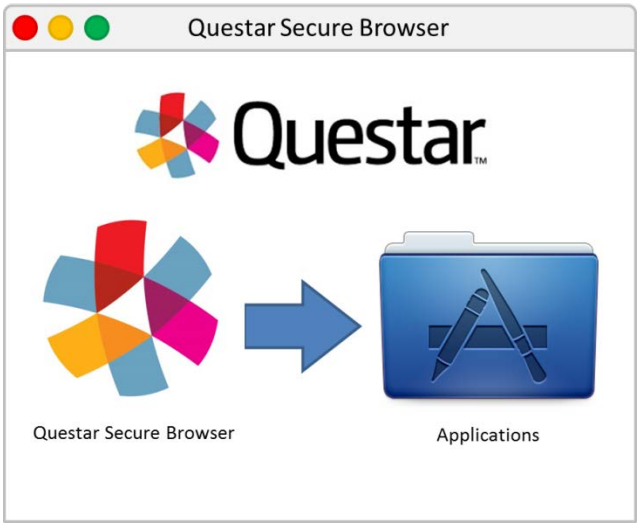
1) Access the Nextera Admin.
2) Select the appropriate *Mac OS Questar Secure Browser.*
3) The download starts. The following image appears in the lower left corner of the screen



4) After the download is complete, click on the arrow to open the file. You will see the following image.



5) Save the Questar Secure Browser to the Applications folder.

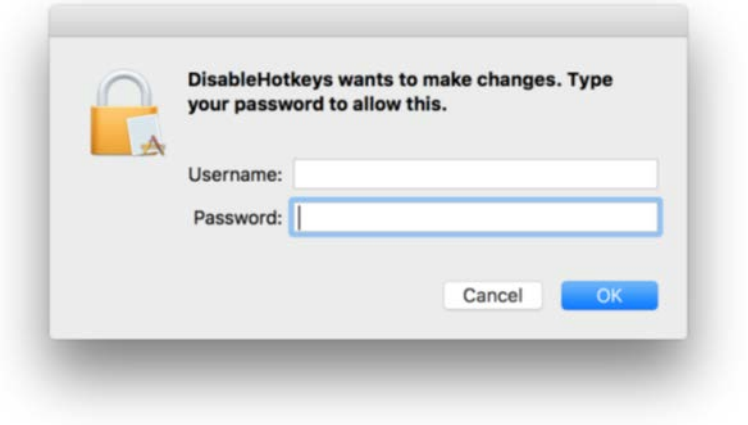


Enabling Enhanced Permissions on Mac OS X

The activation of enhanced permissions is required to enforce the security of our Questar Secure Browser for all Mac OS X. Enhanced permissions will lock down the ability to use certain keystrokes that could enable a student to navigate away from the Secure Browser. If enhanced permissions is not active, test security is at risk.

A proctor or administrator must allow enhanced permissions on each device. The process to allow accessibility of the Secure Browser is determined upon the version of the Mac OS X.

Users of Mac OS X 10.9 or later: After clicking on the Questar Secure Browser icon, a dialog box will appear with a dialog box that states *"DisableHotkeys wants to make changes. Type your password to allow this."*



The proctor or administrator will need to enter the administrator's username and password. There will be a 3-5 second wait while the Questar Secure Browser is added to the accessible applications. This process only needs to be performed the first time the Questar Secure Browser is opened.

Users of Mac OS 10.7 to 10.8: Manually enable the accessibility options.
Mac OS 10.7:

1. Open System Preferences, then Universal Access
2. Check the box next to "Enable access for assistive devices"

Mac OS 10.8:

1. Open System Preferences, then Accessibility
2. Check the box next to "Enable access for assistive devices"

For further detail including screen shots, see the following link:
http://mizage.com/help/accessibility.html

Additional Notes:

In the event that you access your Security & Privacy settings, you may notice the Questar logo with the name of "nwjs" in the Security & Privacy box.

Mac installations do not require changing student cache settings.

Apple iPad Installation

Apple iPad devices can be managed using Apple Configurator 2 or a similar Mobile Device Management (MDM) platform, such as AirWatch, Mobile Iron, or others. MDM management platforms provide administrators with tools for deploying device profiles, device settings, and pushing application packages. Apple Configurator 2 is a free application. Contact other MDM vendors for cost information.

Enabling Autonomous Single App Mode (ASAM) with MDM is the recommended method for secure testing in the **Questar Assessment for Students** app. Single App Mode (SAM) is also recommended. Guided Access mode with manual configuration may be used on iPads using iOS 7 or 8.

Please refer to the following table to determine the recommended solution for configuring iPads.

iOS	Using MDM?	Recommended Configuration
9+	Yes	ASAM or SAM
9+	No	Contact Customer Support
7, 8	Yes	ASAM or SAM
7, 8	No	Guided Access with manual configuration

In addition to configuring iPads, ensure iPads are 100% charged or plugged into a wall socket during the test.

Using Autonomous Single App Mode or Single App Mode with Apple Configurator or other MDM

Questar's preferred configuration for iPad use is iOS 9+ enabled using ASAM via an MDM platform. Technology coordinators need to enable ASAM or SAM before the test and disable it when testing is complete.

Use the following steps as a guide for configuring devices.

1) Download and install the free *Questar Assessments for Students* app from the iTunes store.
2) Select New York from the *Select Group or State* dropdown on the landing page, and select *Continue*.
3) Create an MDM profile and supervisory profile. Refer to your MDM vendor for details.
4) Navigate to *Systems manager > MDM > Settings > Restrictions > iOS supervised restrictions*
5) From the dropdown that appears, select the *Questar Assessments for Students* app.
6) For iOS 8.1.3 or later, access the *custom settings* section of MDM and insert the *profile key* and *value* for each of the following features:

Feature	Profile Key	Value
Dictionary Lookup	<key>allowDefinitionLookup</key>	False
Spell Checking	<key>allowSpellCheck</key>	False
Predictive Keyboard	<key>allowPredictiveKeyboard</key>	False
Auto-Correction	<key>allowAutoCorrection</key>	False
Share selected text (iOS 9+)	This feature is disabled when the Dictionary Lookup feature is disabled.	False

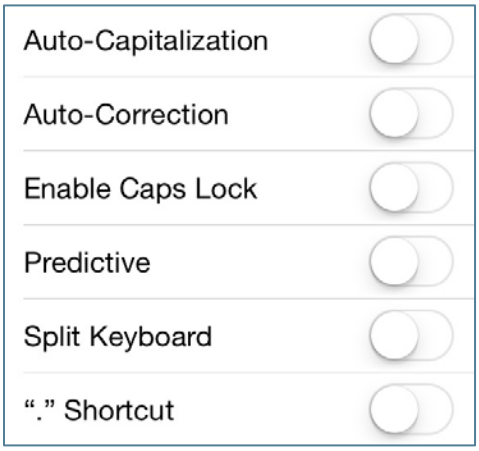
1) Select *Save Changes*

Guided Access with Manual Configuration

Guided Access with manual configuration can be used with iPads on iOS 7 or 8 when MDM is not available. Test administrators or staff will need to enable Guided Access before the test and disable it when testing is complete (see steps 6-8 below).

Use the following steps as a guide for configuring devices.

1) Download and install the free *Questar Assessments for Students* app from the iTunes store.
2) Select your state from the *Select Group or State* dropdown on the landing page, and select *Continue*.
3) Navigate to *Settings > General > Keyboard*
    - Turn *off* all settings



4) Disable *Speech to Text* (SIRI) by navigating to *General > Siri > Off*
5) Navigate to *Settings > General > Accessibility > Guided Access* and
    - Turn *on Guided Access*
    - Set a *passcode* for Guided Access
    - Save the passcode in a safe place to use after testing to deactivate Guided Access. There is no method for retrieving a forgotten passcode.
6) Open the Questar Assessment for Students App. Validate that you have the correct passcode for Guided Access. Triple-click the Home button to turn on Guided Access.
7) Adjust the settings using the options along the bottom of the screen (see image below). With the iPad displaying in landscape mode, set the following parameters:
    - Hardware Buttons > Always OFF
    - Touch > ON
    - Motion > OFF (this will lock further operation in landscape mode)
    - Tap on Start to enter Guided Access mode

8) When the student completes testing, triple-click the Home button again to enter the passcode to end the Guided Access session. Navigate to *Settings > General > Accessibility > Guided Access* and turn *off* Guided Access.

Additional Resources

For further information about configuration options, contact your MDM vendor or refer to Apple Support at the following link. https://support.apple.com/en-us/HT204271

For more information about using iPads for assessments, contact Questar Customer Support or refer to Apple Support at the following link.
http://images.apple.com/education/docs/Assessment_with_iPad.pdf

Chromebooks Installation

There are two options available to setup Chromebooks: Questar's Chrome Kiosk app and Chrome Enterprise User Accounts.

Questar's Chrome Kiosk App

Questar's Chrome app is kiosk-enabled so it can be run in a variety of secure modes for student assessment and testing. Using the Chrome management console, test administrators can push the app to Chrome devices in several ways, allowing the app to be run in two primary modes: 1) as a Single App Kiosk Mode app or 2) as a Single App Kiosk Mode app with Auto-Login to Kiosk App. Both of these modes allow the student to begin testing while preventing access to other apps or their account.

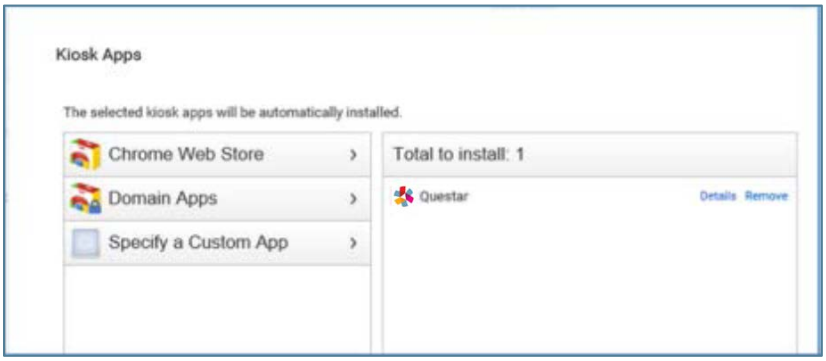
The Chrome app can be obtained from *Help > Downloads* on the Nextera Admin.

Managing Kiosk Applications

Before delivering the app, administrators must configure the app under the Kiosk Apps section within the *Device Management > Chrome > Device Settings menu. Select the Manage Kiosk Applications option > Chrome Web Store option.*

Search "gdehbmmmjkddbonbmknngoigkleicpec" or use the link below.

https://chrome.google.com/webstore/detail/gdehbmmmjkddbonbmknngoigkleicpec/



Delivery Modes

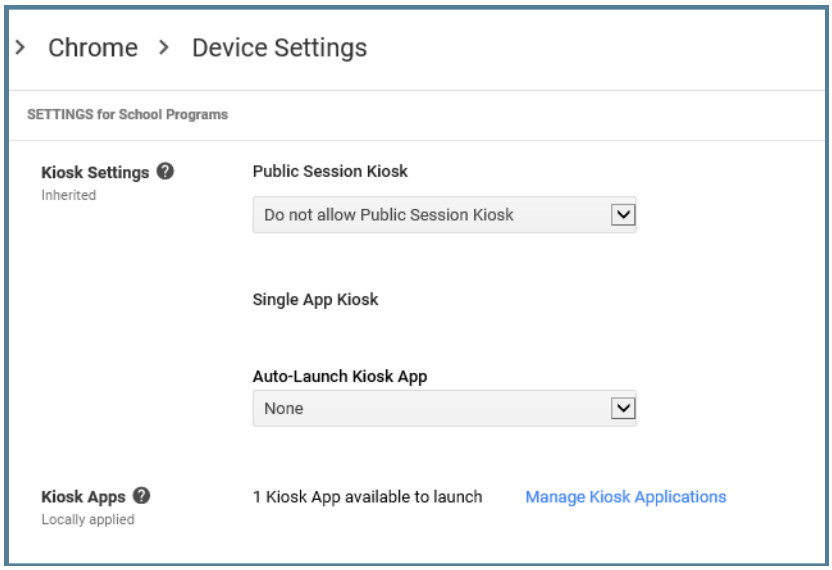
The following sections briefly describe the two primary delivery methods for Questar's Chrome app.

Single App Kiosk Mode

To deliver the app in Single App Kiosk Mode, administrators must first add the app to the Device Settings profile as shown above for each organizational unit (OU) where they want to deliver the app. In this example, we show "School Programs" as our organizational unit. Depending on your OU structure, you may want to move devices between OUs to dynamically deliver the app to testing centers or student devices. Also note the "Locally applied" text indicating these device settings are applied directly to this OU.

If the app is applied at the highest OU, all lower OUs will automatically inherit the app. If you want to limit the distribution of the app, then you need to apply different settings to distribute the app only to the desired OUs.

Note: It may take a period of time for the application to appear on the actual Chromebook. It depends on how often the Chromebooks are set to link back to the organizational entity for updates.



In this delivery mode, students are able to launch the app from the Apps menu on the system tray, which is located in the lower left area of the login screen. No additional account login is required to launch the app. Upon launch, the app appears in kiosk mode (full screen), where the students are then required to log into the assessment with the unique usernames and passwords in order to access the assessment content.

Single App Kiosk Mode – Non-managed Chrome devices

Non-managed Chrome devices, those without the Google Admin or Chrome management console, may also be configured to run Single App Kiosk Mode once the app has been manually installed on the device. If you are using a non-managed device, follow the steps below:

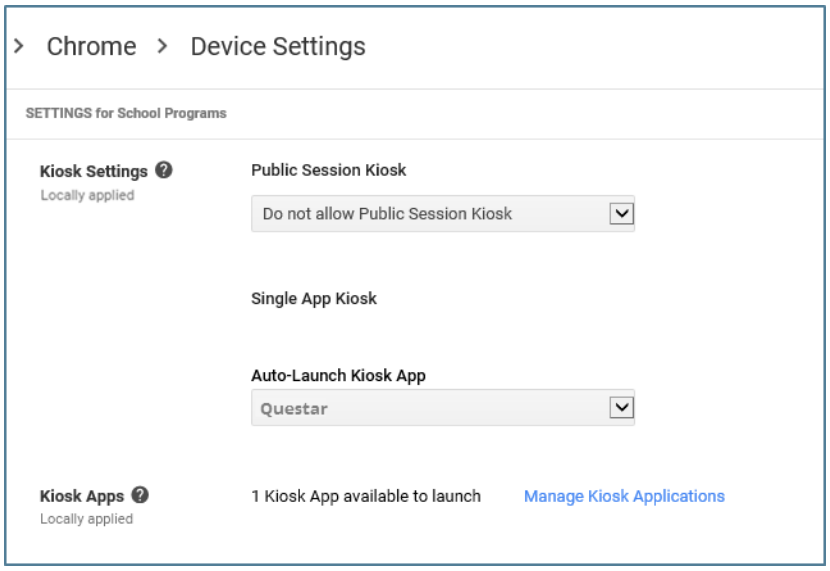
1) Open a new tab in Chrome, and enter **chrome://extensions** in the address bar. Select *Enter*.
2) Select the box next to *Developer Mode*.
3) Select *Add kiosk application*, and enter the ID of the Kiosk App you'd like to enable.
4) Select *Enter*.

The installed Kiosk App will now show up in the tray under Apps for a user to open from the tray.

Single App Kiosk Mode with Auto-Login

The second delivery method is configured the same as above with the exception being that the app is selected under Auto-Launch Kiosk App. In this configuration, the device will automatically launch the

app when powered on thus preventing the login screen from appearing. While the device is booting up, test administrators (and students) may press the keyboard shortcut **Ctrl+Alt+S** to escape out of this boot up sequence, returning the device to the login screen. This deployment method is better suited for testing centers where shared devices are used. *Please note that this deployment method is not supported for unmanaged Chrome devices.*



Questar Chrome Enterprise User Account Accounts

An alternate method of setting up the Chromebooks is to request an enterprise user account for each Chromebook to be used for testing. You **MUST** request the enterprise user accounts 5 days ahead of testing and install prior to the student testing start date. Technology coordinators need to add a unique Chromebook secure account to each Chromebook that will be used for testing. The account only needs to be requested once per Chromebook and can be used for the duration of the year. *Note: Device accounts must be requested from Questar during Registration. If additional accounts are needed, please contact Questar's Customer Support.*

Add the enterprise user account provided by Questar, using the steps below:

1) Sign in to the school's administration console used to manage the students' Chromebooks.
2) Go to Chrome Management > Device Settings and select the organizational unit the students' devices are in.
3) Under Sign-in Restriction, enter "*@questarai.net" and "*@questarai.com" to restrict sign-in to a list of users. This will restrict those who can sign in to the device as only belonging to the assessment domain.
4) Log the Chromebook in to the Google Secure Device account.
5) Once set up, the Chromebook is unable to navigate to any websites or applications other than the Nextera Test Delivery System.
    a. If you can perform any of these actions, the Chromebook is improperly secured.

6) Enter CTRL+ALT+E to display the enterprise login screen.
7) Setup is complete. The student can now login and take a test.

About Managed Chromebooks

Managed Chromebooks are set up and maintained by the school. If there is a managed icon in the status area in the lower right-hand side of the screen when signed into the Chromebook, the device is managed.

Managed Chromebooks will have sign-in restrictions enabled. The administrator settings may apply to the Chromebook even when signed in to a personal Google Account. If students are using managed Chromebooks, the Chromebook administrator will need to authorize the secure domain.

1) As the Chromebook administrator, log into the Chrome OS management console.
2) Select *Settings*.
3) Select *Device Settings* and scroll down to the *Sign-in Restriction* section.
4) In the text box, enter the following text: *@questarai.net, *@questarai.com
5) Select *Enter*.

Preparing Chromebooks

Ensure that Chromebooks are 100% charged or plugged into a wall socket during the test.

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.

If you are using secured accounts, complete the following steps:

1) Clear the *Chrome cache* before the first administration and between administrations to avoid issues of students logging in and getting a blank page.
2) Log the Chromebook into the Questar-provided Chromebook secure device account.
3) Start the Chrome browser. In doing so, the Questar Assessment System login screen will be automatically displayed.

Note: When the test administration window is closed, under User Data, select *Erase all local user data* to erase the student's data from the device. **This is not recommended until after all testing is complete, as once the student data is deleted, any responses that did not transmit to Questar for any reason cannot be recovered, and the student will have to take the assessment again**.

Additional Settings

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

Disable Fast User Switching: Windows & Mac

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. Please disable Fast User Switching using one of the processes below.

Windows, Process 1

1. Control Panel
2. Open User Accounts
3. Click Change the way users log on or off
4. Uncheck the Use Fast User Switching check box
5. Click Apply Options

Windows, Process 2

1. From Start, type *gpedit.msc*
2. Select Apps from the sidebar on the right
3. Click *gpedit.msc* in the main window
4. In the Local Group Policy Editor window, locate and select Logon in the left pane
5. On the right, double-click *Hide entry points for Fast User Switching*
6. In the *Hide entry points for Fast User Switching* dialogue box, select *Enabled* and click *OK*
7. Close the Local Group Policy Editor and open the Run dialog box (Windows + R). Enter *gpupdate/force* and click *OK*

Mac

1. From the Apple menu, choose System Preferences
2. From the View menu, choose Accounts
3. Click the Login Options button
4. Deselect the "Enable fast user switching" option

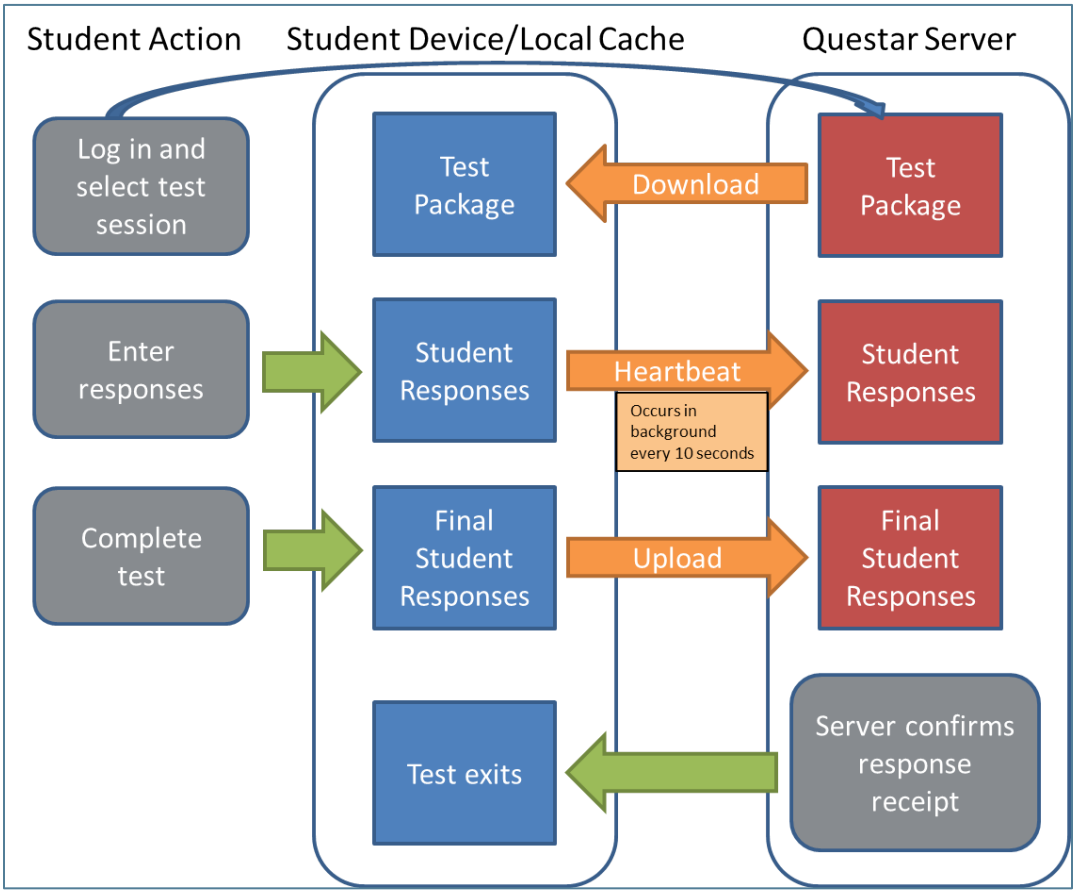
Appendix A – Student Response Flowcharts

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.

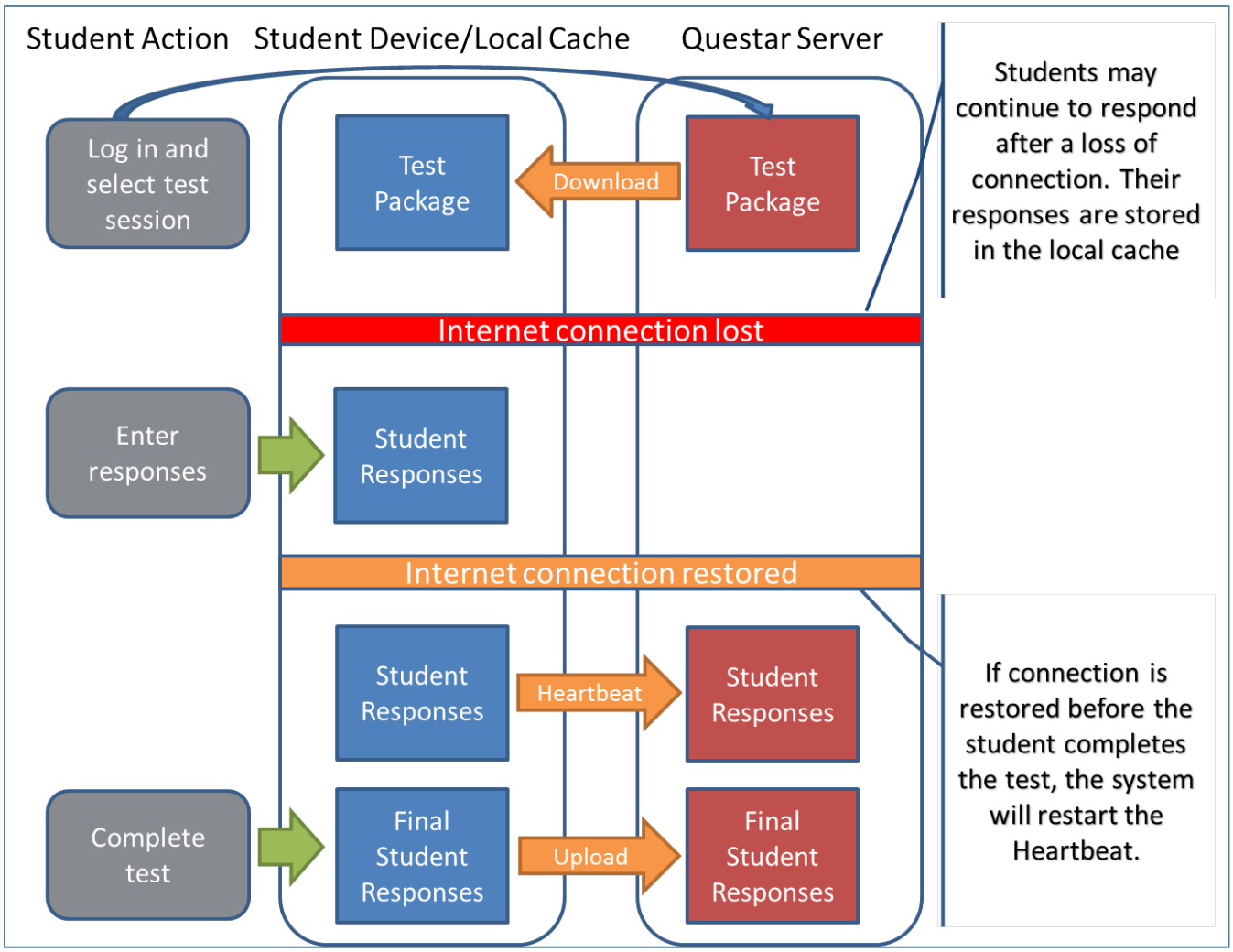
Continuous Internet Connection

Optimally, the student's device will have continuous internet connection during testing. The student's responses are sent to the Questar Server in the background every 10 seconds. This is referred to as a "heartbeat." When the student completes testing, the final responses are uploaded to the Questar Server. The Questar Server confirms response receipt and the test 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 reestablished. The testing system continuously attempts to reestablish connection with the Questar Server. When the internet connection is restored, the responses are automatically sent to the Questar Server. When the student completes testing, the final responses are uploaded to the Questar Server. The Questar Server confirms response receipt and the test will exit on the student's device.



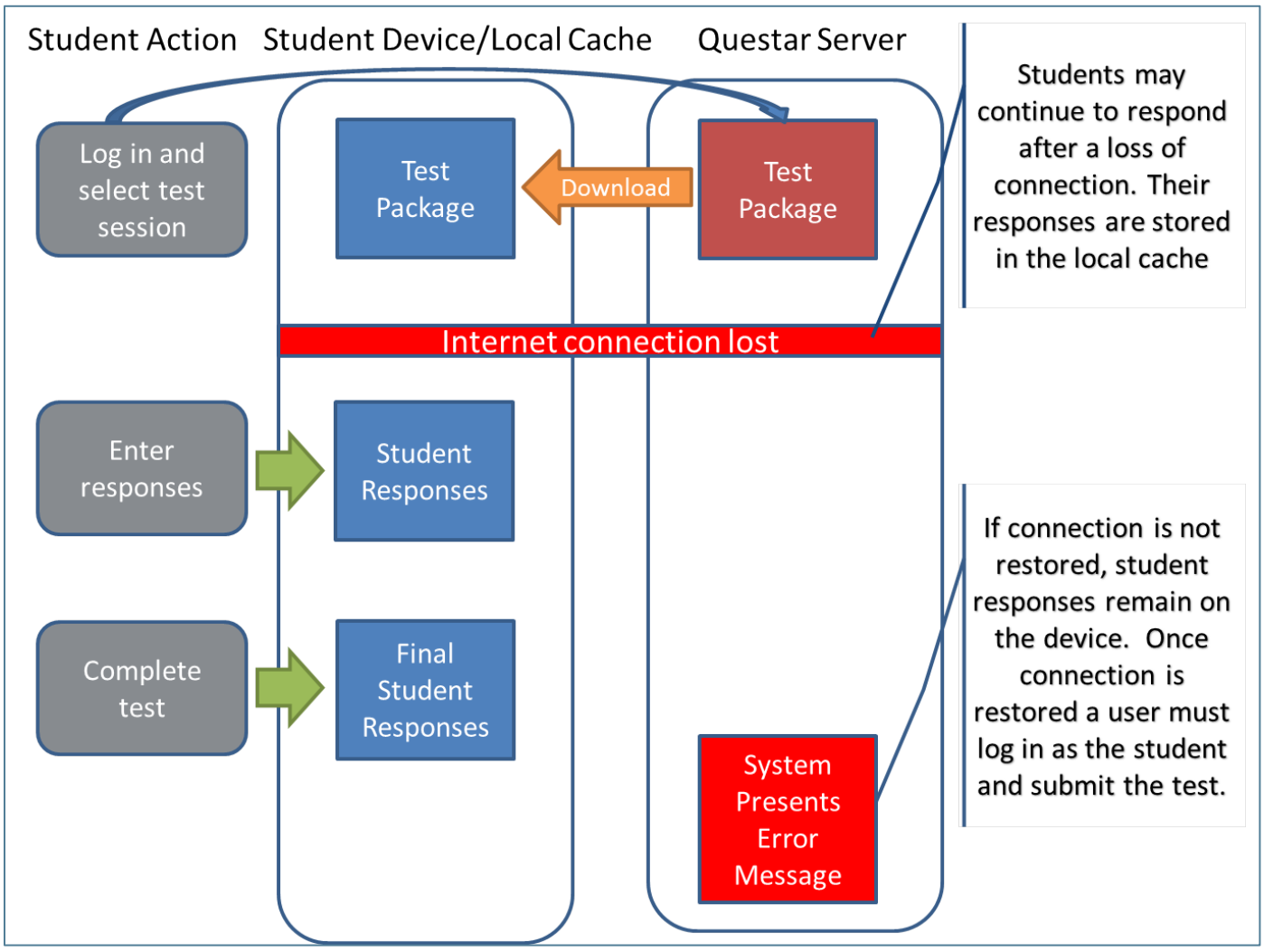
Internet Connection Lost

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 reestablished. 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:**
    a. Restore internet connection to the device
    b. If the student has logged out, direct them to log in again
    c. Submit the test
- The Questar Server confirms response receipt and the test will exit on the student's device.
- Another student can now use the device.

Special note for Chromebook users: If connection is lost on a Chromebook prior to the student submitting the test, do not exit the Secure Browser or Kiosk App. Exiting will erase the student responses. Instead, restore internet connection to the device and submit the responses.

Internet Connection Lost, continued



Appendix B – System Requirements

Operating System	OS Version	Processor	System Memory/ Hard Disk Space	Screen Size Resolution	LAN Network	Internet Speed
Windows	Vista/ 7/8/10 2003/ 2008/ 2012 (latest service pack)	Intel Pentium 4 1.0 GHz equivalent or higher CPU Recommended Intel Core 2 Duo 1.6 Ghz equivalent or higher performing CPU	Minimum 512MB Free Ram Recommended 1 GB Free RAM Minimum 1 GB Free Storage Space	Minimum 9.7" screen size Minimum 1024 X 768 screen resolution Recommended 11.6" or larger screen size	Minimum 100 Mbps LAN/802.11g Wireless 54Mbps or greater Minimum available LAN bandwidth at each workstation: 1Mbps Recommended 1 Gbps LAN/802.11n Wireless 150 Mbps or higher Recommended available LAN bandwidth at each workstation 2 Mbps	Minimum per device: 150 Kbps Recommended: 300 Kbps
Mac	Mac OS X 10.6+	Intel Core 2 Duo 1.6 GHz equivalent or higher performing CPU	Minimum 512MB Free Ram Recommended 1 GB Free RAM Minimum 1 GB Free Storage Space	Minimum 9.7" screen size Minimum 1024 X 768 screen resolution Recommended 11.6" or larger screen size	Minimum 100 Mbps LAN/802.11g Wireless 54Mbps or greater Minimum available LAN bandwidth at each workstation: 1Mbps Recommended 1 Gbps LAN/802.11n Wireless 150 Mbps or higher Recommended available LAN bandwidth at each workstation 2 Mbps	Minimum per device: 150 Kbps Recommended: 300 Kbps
iOS	7, 8, 9	1.0 Ghz dual core equivalent or higher	Minimum 512MB Free Ram Recommended 1 GB Free RAM Minimum 1 GB Free Storage Space	Minimum 9.7" screen size Minimum 1024 X 768 screen resolution	Minimum Wireless 54Mbps or greater Minimum available LAN bandwidth at each workstation: 1Mbps Recommended 802.11n Wireless 150 Mbps or higher Recommended available LAN bandwidth at each workstation 2 Mbps	Minimum per device: 150 Kbps Recommended: 300 Kbps

Operating System	OS Version	Processor	System Memory/ Hard Disk Space	Screen Size Resolution	LAN Network	Internet Speed
Chrome OS	Version 29+	1.6 Ghz equivalent or higher	Minimum 512MB Free Ram Recommended 1 GB Free RAM Minimum 1 GB Free Storage Space	Minimum 9.7" screen size Minimum 1024 X 768 screen resolution	Minimum Wireless 54Mbps or greater Minimum available LAN bandwidth at each workstation: 1Mbps Recommended 802.11n Wireless 150 Mbps or higher Recommended available LAN bandwidth at each workstation 2 Mbps	Minimum per device: 150 Kbps Recommended: 300 Kbps

Appendix C – iPad and Chromebook Frequently Asked Questions (FAQ)

Q1. How do I obtain secure device user accounts for Chromebooks?

Testing securely on Chromebooks requires a secure user account be added to each Chromebook prior to testing. Corporations enter counts during the iPad and Chromebook Registration process. If additional accounts are needed, call or email Questar Customer Support with the number of devices being used at least five days in advance of your school's testing window. Login credentials for these secure user accounts will be issued to the corporation and the technology coordinator will need to add a user account to each Chromebook. Logging a Chromebook into this user account provides secure access to any current and future Questar Assessment System assessment.

Q2. 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 he or she 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 reentered before submitting the test.

Q3. 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 Questar Assessment System Student Client during testing.

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 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.
- Right-click, select quit secure browser, and log in again – 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 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 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 lower left corner of the Nextera Test Delivery System changes from green to red.
- If connectivity is lost for 45 seconds or more, a “Lost Connection” message displays.
- If the network connection is restored, the responses will automatically submit and the display will return to the Questar Assessment System Student Client login screen. It is strongly recommended the device be left in this state until the network connection is restored.

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:

- 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 Questar 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.

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.

Missing Begin Button

After logging into the test, the Begin button is missing. Launching multiple instances of the secure browser may cause the Begin button to disappear. Log out of the test, and close all instances of the secure browser. Relaunch a single instance of the secure browser and login.

Guided Access Mode - iPad

Some iPad versions, especially iPad2, experience problems and/or display error messages with the guided access mode. This is an iPad issue that is unrelated to the Questar application. To resolve this issue, reset all settings on the device. This is done under Settings > General > Reset > Reset All Settings.

Issues Editing English Essays

Press the Insert key to ensure the keyboard is for insert mode rather than overtype mode. When a keyboard is in overwrite mode, existing text is deleted as new text is written. Pressing the Insert key again changes back to insert mode.