STAAR Online Testing Platform Technology Guide

Including Secure Browser Installation on Chromebook, iPad, Mac, and Windows

STAAR 3-8 and STAAR EOC
Online Testing Program

Updated March 17, 2017

New Sections in this Version

Table of Contents

Section 1: Network Requirements

The purpose of this manual is to provide instructions for installing and configuring the STAAR Online Testing Platform software.

1.1 Platform Overview

The STAAR Online Testing Platform is flexible and adaptable. It supports a wide variety of desktops, laptops, and network configurations. System support includes virtual networks and thin client environments, as well as other common network configurations.

Requirements include:

- Stable, high-speed Internet connection(s) (wired or wireless)
- Appropriate bandwidth

Components include:

- Online readiness tools
- Secure Browser application
- Local Caching Software (LCS)

1.1.1 Support

For more information, visit https://www.texasassessment.com/ or contact the Texas Assessment Support Center:

Texas Assessment Support Center:

Phone: 855-333-7770

STAAR3-8@ets.org

STAAREOC@ets.org

1.2 Network Connections

A stable, high-speed (wired or wireless) Internet connection is required for online testing. The response time for each assessment depends on the reliability and speed of the campus' Internet connection.

Some districts may not have the bandwidth capacity required for numerous students to test concurrently. A solution for this issue is Local Caching Software (LCS), fully described in Section 4: Local Caching Software.

1.2.1 Network Settings

Network configuration settings should include all the elements noted below.

- Configure the content filters, firewalls, and proxy servers to allow traffic on the protocols and to the servers listed in Section 1.7: Network Configurations.

- Session timeouts on proxy servers and other devices should be set to at least 35 minutes.
  - This will help limit interruptions during testing.
- Content caching must be disabled.
- If the client network uses any devices that perform traffic shaping, packet prioritization, or Quality of Service, the URLs specified in **Appendix A** must be used.
  - This guarantees the highest level of performance.
  - These URLs must be *open* or *whitelisted.*

If the Internet connection is not working properly, students will need to complete their tests at a later time. All submitted test responses will be saved. When the student resumes testing, he or she will be returned to the first unanswered item.

- Verify the network settings so the online testing applications will work properly.
- For any questions about network configurations, contact your network administrator or technology specialist.

1.2.2 Network Performance

All network communications use the Internet Protocol (IP) Suite. The Local Area Network (LAN) must route IP traffic to and from the Internet. Unless using LCS, the online tests are delivered directly through the Internet. Students access their tests using the STAAR Online Testing Platform. All workstations where tests are administered must have reliable Internet connectivity.

Diagnostic testing may determine that the district's network has unreliable Internet connectivity, low bandwidth, or too many simultaneous testers for its transmission capabilities. For complete instructions about running diagnostics on the network, refer to **Section 1.6: Network Diagnostic Tools**. LCS helps reduce bandwidth bottlenecks. The LCS is needed only for districts or campuses with limited bandwidth.

NOTE: For more information about the LCS system requirements and installation procedures, refer to **Section 4: Local Caching Software.**

1.3 Bandwidth

Bandwidth is the measure of the signaling capacity of a network. Bandwidth performance is affected on the internal LAN (Intranet) traffic and Internet traffic from the router. Regardless of hardware or network topology, the LAN should be analyzed to determine the potential for traffic bottlenecks.

The following table details the estimated average bandwidth used by the STAAR Online Testing Platform Secure Browser for testing.

Number of Students Testing Concurrently	Average Estimated Bandwidth Used for Testing
1	20K bytes/second
50	250–750K bytes/second (0.25–0.75M bytes/second)
100	500–1500K bytes/second (0.5–1.5M bytes/second)

Bandwidth varies during a student's testing experience. Some test pages contain low-bandwidth content, such as multiple choice items. Other test pages contain higher-bandwidth content, such as animations.

Consequently, the estimated average values in the column in the chart above are based on computing averages from multiple tests and test subjects.

NOTE: During the initial Secure Browser startup there is a one-time exception to these averages.

1.3.1 Students Testing Simultaneously

As the number of students testing at the same time increases, competition for network bandwidth increases. The LCS will minimize the use of Internet bandwidth in each campus to reduce the possibility for issues and maximize the number of students who can be tested simultaneously.

For more about using an LCS, refer to **Section 4: Local Caching Software**.

1.3.2 Determining Bandwidth Requirements

To determine the necessary campus bandwidth requirements, complete the following steps.

- Run the diagnostics on the network to determine how many students can reasonably test concurrently. The bandwidth should not exceed the peak usage experienced when the test initially loads. STAAR tests include animations and interactive items, which may increase the bandwidth required. For complete instructions about running diagnostics on the network, refer to **Section 1.6: Network Diagnostic Tools**.
- Most campus bandwidth levels are typically sufficient for wired networks. New switches generally operate at speeds of between 100Mbits (per second) to 1000Mbits. However, LAN performance can be hindered in cases where hubs are used instead of switches.
- For Internet networks, the most common bottleneck is the Internet Service Provider's (ISP) router connection, which typically operates at speeds of between 1.5Mbits to 100Mbits.
- Network administrators should test and forecast whether their Internet/intranet infrastructure has the capacity to accommodate needs.

Determining whether the infrastructure is sufficient for current needs involves a number of factors. Listed below are some of these considerations.

- Determine the average daily volume of Internet traffic.
- Determine the desired response time for non-test related applications that require Internet connectivity and will operate during testing.
- Determine the number of students who will test concurrently.

1.3.3 Size of Test Content

The size of the test is determined by two factors.

- The number of items on the test.
- The average size of each item.

The more items a test contains and the larger the average size item, the higher the bandwidth requirement.

1.3.4 LCS (Local Caching Software)

The LCS receives testing content from the data center and delivers it to the testing devices. Under certain circumstances, this application may help reduce network congestion. However, most school district networks offer sufficient bandwidth support to deliver the online tests without the LCS.

The LCS is made available to support districts or campuses with limited bandwidth.

For details, refer to **Section 4: Local Caching Software**.

1.3.5 Secure Browser Installation

The Secure Browser is an application specifically designed for the STAAR Online Testing Platform. Local installation of the Secure Browser onto each individual testing workstation is recommended. This application can be installed on a network or a shared drive, and then have the testing workstations run the Secure Browser from this drive. There may be some performance impacts under this configuration, as noted below.

- There will be competition for network bandwidth, possibly slowing Internet transmissions.
- The network or shared disk drive will also be subject to some resource competition. Multiple clients reading from the network drive can reduce overall application performance.
- Due to the sensitivity of test-related data, encryption is always required. It is highly recommended that wireless traffic use WPA2/AES data encryption. Because encryption/decryption is part of the data exchange process, there may be a slight decrease in the overall speed of the network.

1.4 Wireless Networking

There is a wide variety of wireless network technologies.

Version	Transmission Rate
802.11ac	The fastest and most recent IEEE wireless standard, with a throughput of up to 1.3Gbits (per second).
802.11n	Has a theoretical throughput of up to 300Mbits.
802.11g	Has a theoretical throughput of up to 54Mbits.
802.11b	Has a theoretical throughput of 11Mbits.

1.4.1 Wireless Access Points

It is recommended that each campus maintain a ratio of wireless systems to wireless access points (WAPs) of no more than 20 to1. Typically, the test performance begins to deteriorate after this threshold is surpassed. In some instances, older WAPs have a lower capacity, which may lead to a slower rate and see performance degradation when more than fifteen devices are concurrently attached.

1.4.2 Recommended Workstations per Wireless Connection

The optimal (or maximum) number of student workstations (computers and tablets) supported by a single wireless connection will depend on the type of networking standard being used for the connection.

- The two most common networking standards are 802.11g (54Mbps) and the newer and faster standard, 802.11n (300Mbps).
- Both the access point, which emits the wireless signal, and the computer's wireless card, which receives the signal, will use one of these two standards.

The recommendations below are based on the standard in use:

Workstations per Wireless Connection		
	802.11g Access Point	802.11n Access Point
802.11g wireless cards	20 workstations or devices	40 workstations or devices
802.11n wireless cards	20 workstations or devices	40 workstations or devices

NOTE: Refer to the vendor's wireless access point documentation for specific recommendations and guidelines.

1.5 Online Readiness Tools

The following tools are available to successfully administer online tests by accessing the *Online Readiness Tools* link:

- System Requirements
- School Capacity Calculator
- System Check Test

NOTE: To access the School Capacity Calculator and System Check Test tools, click on the link below:

https://tx-bandwidth.caltesting.org/**.**

1.5.1 System Requirements

The System Requirements check runs automatically each time the Secure Browser application is launched. This resource provides information to confirm that the devices used for testing meet the system requirements.

1.5.2 School Capacity Calculator

The School Capacity Calculator helps plan for the test administration. It is used to determine the following components.

- Maximum Student Capacity
- Maximum Required Computers
- Minimum Test Sessions per Day
- Minimum Required Days of Testing

To determine the **Maximum Student Capacity**, enter the number of computers, the number of test sessions available per day, and the number of days allowed for testing. Select the ***Calculate*** button and the system will provide the maximum student capacity for testing.

To determine the **Minimum Required Computers**, enter the total number of student testing administrations, the number of test sessions available per day, and the number of days allowed for testing. Select the ***Calculate*** button and the system will provide the minimum number of computers required for testing.

To determine the **Minimum Test Sessions per Day**, enter the number of computers, the total number of student testing administrations, and the number of days allowed for testing. Select the ***Calculate*** button and the system will provide the minimum number of sessions needed each day for testing.

To determine the **Minimum Required Days of Testing**, enter the number of computers, the total number of student testing administrations, and the number of sessions available per day. Select the ***Calculate*** button and the system will provide the minimum number of days needed for testing.

1.5.3 System Check Test

The **System Check Test** analyzes the bandwidth and level of readiness for testing implementation. Run this test during peak usage to assess the available bandwidth and network traffic. Local bandwidth will vary with usage and traffic levels, so it should be run when usage is similar to usage on a testing day. This test also confirms when the campus could benefit from the LCS.

1.6 Network Diagnostic Tools

If further diagnostic testing is needed, the following system-specific tools can help identify the network bottlenecks and problems.

1.6.1 MS Windows® Specific Tools

PRTG Traffic Grapher (http://www.paessler.com/prtg/) is Windows software that monitors bandwidth usage and other network parameters via simple network management protocol (SNMP). It also contains a built-in packet sniffer. A freeware version is available.

NTttcp (http://www.microsoft.com/whdc/device/network/TCP_tool.mspx/) is a multi-threaded, asynchronous application that sends and receives data between two or more endpoints and reports the network performance for the duration of the transfer.

Pathping is a network utility included in the Windows operating system. It combines the functionality of Ping with a Traceroute function (Windows filename: tracert). This provides details of the path between two hosts and Ping-like statistics for each node in the path based on samples taken over a time period.

1.6.2 Mac OS X Specific Tools

Network Utility Application is built in to Mac OS X software.

1.6.3 Multi-Platform tools

Wireshark (http://www.wireshark.org/) is a network protocol analyzer that has a large feature set and runs on most computing platforms including Windows, OS X, Linux, and UNIX.

TCPDump (http://sourceforge.net/projects/tcpdump/) is a common packet sniffer that runs under the command line and is compatible with most major operating systems (UNIX, Linux, and Mac OS X). It allows the user to intercept and display data packets being transmitted or received over a network.

A Windows port **WinDump** is also available (http://www.winpcap.org/windump/).

Ping, **NSLookup**, **Netstat**, and **Traceroute** (in Windows**: tracert**) is a set of standard UNIX network utilities. Versions of these utilities are included in all major operating systems (UNIX, Linux, Windows, and Mac OS X).

Iperf (http://sourceforge.net/projects/iperf/) is a tool that measures maximum TCP bandwidth. This allows the user to tune various parameters and user datagram protocol (UDP) characteristics. Iperf reports bandwidth, delay jitter and datagram loss.

1.7 Network Configurations

Networks are configured to access the protocols, multipurpose Internet mail extensions (MIME) type, and URLs listed below.

1.7.1 Protocols

All communication within the network takes place over the following Internet port/protocol combinations. Please ensure that the following ports are open for these systems.

Port/Protocol	Purpose
80/tcp	HTTP (initial connection only)
443/tcp	HTTPS (secure connection)

1.7.2 MIME Types

Allow downloading and uploading of the MIME types noted below.

Application/json	Image/svg+xml	Text/xml
Application/octet-stream	Multipart/form-data	Video/mp4
Image/gif	Printer/prn	
Image/png	Text/html	

1.7.3 Uniform Resource Locators (URLs)

Allow the URLs listed below to be accessed through the firewall:

- http://*.caltesting.org/
- https://*.caltesting.org/
- http://*.ets.org/
- https://*.ets.org/
- http://hello.myfonts.net/
- https://hello.myfonts.net/
- http://tx-tss.caltesting.org/
- https://tx-tss.caltesting.org/
- http://tx-toms.caltesting.org/
- https://tx-toms.caltesting.org/
- http://tx-bandwidth.caltesting.org/
- https://tx-bandwidth.caltesting.org/

1.7.4 Domain Name Resolutions (DNS)

All system URLs must be resolvable by the client hosts attempting to connect to the online testing system.

The client workstations must convert friendly names (URLs) to their corresponding IP address by requesting the information from the DNS server.

1.7.5 Email server

Make sure the following email addresses are whitelisted to ensure delivery:

- @ets.org
- @caltesting.org

1.7.6 Firewalls, Content Filters, and Proxy Servers

NOTE: For locations using SSL filtering, be aware that the SSL certificate for online testing uses san.ets.org as the CN (Common Name).

Configure **firewalls**, **content filters**, and **proxy servers** to allow traffic on the protocols listed above to the servers running the applications. Session timeouts on proxy servers and other devices should also be set to values greater than the average duration it takes a student to complete a given test.

1.7.7 QoS/Traffic Shaping

If the client network uses any device(s) that performs traffic shaping, packet prioritization, or Quality of Service (QoS), then the URLs or IP addresses in **Appendix A: URLs** should be given a high level of priority. This ensures the greatest performance.

1.8 Virtualization Guidelines

There are many different types of virtualization options for schools. Virtualization can potentially impact both test security as well as student testing experience. It is, therefore, the responsibility of district and campus technology staff to ensure security and performance are maintained within virtualized environments.

1.8.1 Security

Test Security is critical for high-stakes assessment. The student testing experience must be adequately controlled to prevent students from gaining access to information, communications, or other resources that could provide assistance during the test. Additionally, test content and student responses must be secured across networks, in order to protect against the potential exposure of test content. The Secure Browser has significant security features that lock down the desktop to protect the integrity of the testing process.

1.8.2 Performance Comparability

The system performance of the virtual environment must be comparable to a non-virtual environment. Verify that performance using the virtualized environment will not negatively impact the student's ability to test.

1.8.3 Virtualization Evaluation Process

Compare and confirm security and performance in the virtualized environment. Performance comparisons should be completed by using the Online Readiness tools and taking tutorials and practice tests. The tools should first be used in a non-virtualized environment and then used in the virtualized environment to validate that security and performance is comparable. Virtualized environments, such as nComputing, VMWare, and Citrix XenDesktop have been used successfully.

1.8.4 Critical Security Standards

Ensure that virtualization solutions meet all of the following criteria:

1. From **login** to **submit**, the desktop is secure and the system does not allow access to any application, content, or other service beyond the STAAR Online Testing Platform.
2. From **login** to **submit**, the system does not allow any screen captures, printing, saving, or other electronic replication or duplication of the display screen or content of the test. This includes the viewing of test materials by district and campus staff.

1.8.5 Critical Performance Standards

Ensure that virtualization solutions meet all of the following criteria:

1. While logging in concurrently with the same number of clients that will be used during normal testing, no error messages are received.
2. The first test item (question) of the practice test loads fully at the same speed as it does in a non-virtualized environment.
3. While interacting with all practice test items (questions) there are no noticeable lags or delays as compared to a non-virtualized environment.
4. The text-to-speech (TTS) feature reads test questions aloud for the student. Be sure to use the tutorials and practice tests for verifying TTS functionality. The TTS feature is available in practice tests and tutorials with the text-to-speech accommodation.
5. When the practice test is submitted (completed normally), no error message is received and the system responds at the same speed as compared to a non-virtualized environment.

Section 2: Hardware Requirements

For information about supported operating systems, hardware recommendations, and requirements for monitors/screens, keyboards, and headphones refer to the *Unified Minimum System Requirements for the Administration of Online Assessments* available online at http://www.texasassessments.com/technology/.

Section 3: Secure Browser

All students must use the Secure Browser application to access the online tests.

- The Secure Browser prevents students from accessing other computer or Internet applications or copying test information.
- Before any installation, check the administration rights to the computer/device.
- If you have disabled the auto-update feature on mobile devices, confirm that all devices used for testing have the correct version of the Secure Browser installed.
- Secure Browser for Windows, Mac OS, and Linux includes Ivona Text-to-Speech features which are installed automatically with the application. No separate installation or setup is required.

3.1 Chromebook Installation

Managed Chromebooks offer a centralized application management, making software deployment consistent and highly efficient.

The following instructions cover the process of preparing and installing the Secure Browser on Chromebooks. Chromebooks are either managed centrally through the Google admin portal (e.g., managed Chromebook), or managed individually on each device (e.g., non-managed Chromebook). Determine how Chromebooks are managed at the location and then select the appropriate starting procedure.

NOTE: The latest production release of Chrome OS from Google, known as "stable channel," has excluded certain Chromebook models, including ASUS Chromebook Flip C100PA, Google Chromebook Pixel (2015), and Acer Chromebook R11. Refer to the Chromebook blog for additional details. While the likelihood of issues is low, if a testing campus has Chromebook models in the exclusion list, it is possible that users may experience Chrome OS-related issues that haven't been tested for or resolved. It is always best practice to ensure that Chromebooks are on the latest stable channel release. Please refer to the Chrome Releases web page for up-to-date information: https://chromereleases.googleblog.com/.

3.1.1 Managed Chromebook Installation Procedure

1. Set up a free Google Apps for Education account and enroll all managed Chromebooks.
   - For complete details, Refer to http://www.google.com/intl/en/chrome/education/devices/features-management-console.html
2. Open a browser and navigate to https://admin.google.com/.
3. Log in using the Google Apps for Education account.
4. Select Device Management.
5. Select Chrome from the list of platforms.
6. Under "Chrome Management," select App Management.

7. In the left-hand column, search for “STAAR Online Testing Program.” In the FIND OR UPDATE APPS field, click Search.
8. If there are issues with the search, search on the string "ecbhjjmmfmlmnoiahdacnhilojbdjijp" to locate the program.
9. Click on the application title STAAR Online Testing Program.
10. On the following screen, click Kiosk Settings, then click Deploy this app as a Kiosk App.”
11. Select the correct organization needed (e.g. "caltesting.org").
12. Enable “Install automatically” and “Allow app to manage power.”
13. Click the ***Save*** button.

    NOTE: The Secure Browser will appear on all managed Chromebooks. This download may take up to fifteen minutes.
14. To launch the Secure Browser, click the *Apps* link in the menu row of a managed Chromebook.
15. Select the STAAR Online Testing Program app.

3.1.2 Non-managed Chromebook Installation Procedure

1. Log in to the “Staff/Admin Google” user with the Chromebook owner account.
2. Open a Google Chrome web browser.
3. Navigate to http://www.texasassessment.com/technology/ and click on the *For Chromebook* link.
4. Click in the address bar to highlight the entire URL.
5. Press ***Ctrl + C*** to copy the URL to the clipboard
6. Navigate to chrome://extensions/.
7. Scroll up to the top of the page.
8. Check the *Developer Mode* box.
9. Click on Manage Kiosk Applications.
10. Enter the *Add Kiosk Applications* field, and then press ***Ctrl + V*** to paste the URL from the clipboard.
11. Click the ***Add*** button.
12. “STAAR Online Testing Program” will appear in the *Manage Kiosk Application* list.
13. Click the ***Done*** button to close the browser window.
14. Sign out of the Chromebook.

NOTE: To launch the Secure Browser, click the Apps link, and select the *STAAR Online Testing Program* application.

3.1.3 Closing the Chromebook Secure Browser

In the event that there is a need to force an exit of the Secure Browser before completion of a test, enter **Shift + Esc + E.**

3.1.4 Chromebook Keyboard Shortcuts

The Chrome OS keyboard shortcuts available when using the Secure Browser are listed below. This only applies to system and network administrators with the appropriate privileges.

Hot Keys	Shortcut Function
Ctrl + Shift + + (plus)	Screen scale is increased
Ctrl + Shift + – (minus)	Screen scale is decreased
Ctrl + + (plus)	Screen zooms in
Ctrl + – (minus)	Screen zooms out
Ctrl + 0 (zero)	Reset zoom
Ctrl + Shift + F5 key	Screen rotates

3.2 Installing Windows Secure Browser

This section provides instructions for installing the Windows Secure Browser on computers with supported Windows operating systems.

NOTES:

- All Windows installations require Read/Execute permissions to the program folder, and Read/Write permissions to the user's home directory.
- Before installing a new version on a device where Secure Browser is already installed, uninstall the previous version. Refer to **Section 3.2.3 Manually Uninstalling Secure Browser** for directions.

3.2.1 Manually Install .msi Package with User Interface

Follow these steps to install the Secure Browser on Windows devices.

1. Open a browser and navigate to http://www.texasassessment.com/technology/.
2. Click on the *For Windows* link.
3. Select the *Secure Browser Windows.msi* icon located on the desktop or downloads folder, or select *Run*… when the pop-up appears.
4. Follow all the application installation directions.
5. Once the installation is complete, launch the Secure Browser by double-clicking the icon on the desktop.

3.2.2 Installing the .msi Package

NOTE: This section only applies to system and network administrators with the appropriate privileges.

Network administrators can install the Windows Secure Browser using an installation script executed by an administrator account on the machine. The script is designed to run without any human interaction (quiet switch).

- Install it in the default directory (C:\Program Files for 32-bit, C:\Program Files (x86) for 64-bit) or any target directory of choice.
- Uninstallation can also be scripted.

Below are two generic scripts. One is for installation and one for uninstallation. Both require the script to have visibility to the *.msi installation file* and can only be executed by an administrator account on the machine.

- This is a Windows-based restriction, not a Secure Browser restriction.
- The msiexec service that installs .msi files is used by administrators only.

Script Conventions

<Source> = Complete path to the Secure Browser msi installation file including .msi installation file name

Example: C:\MSI\securebrowser.msi

<Target> = Complete path to the location where the Secure Browser should be installed, if the default location (C:\Program Files) is not preferred.

Example: C:\MSI\Installation_Dir

NOTE: The target install directory does not have to be created in advance.

Installation Script

msiexec /I <Source> /quiet INSTALLDIR=<Target>

Example: msiexec /I C:\MSI\ securebrowser.msi /quiet INSTALLDIR=C:\MSI\Browser_Install

Uninstallation Script

msiexec /X <Source> /quiet

Example: msiexec /X C:\MSI\securebrowser.msi /quiet

3.2.3 Manually Uninstalling Secure Browser

Follow the steps below to uninstall the previous Secure Browser.

1. Click ***Start*** in the task bar, open *Settings*, then open the *Control Panel*.
2. Select Add or Remove Programs.

3. Open *STAAR Online Testing Program*, click ***Remove*** to open the Uninstall Wizard.
4. Click ***Next***, click ***Yes***, then click ***OK*** to complete the uninstall process.

3.3 Disabling Fast User Switching in Windows

Windows allows multiple users to be logged-in concurrently without requiring one user to log out before another logs in. This is "Fast User Switching."

- It allows a student to access multiple user accounts from a single computer.
- Disabling the "Fast User Switching" function is strongly encouraged.

3.3.1 Disabling Fast User Switching in Windows 7

Method A: Access the Group Policy Editor

1. Click ***Start***, type "gpedit.msc" in the *Start Search* window, and then press *Enter*.
2. Open *Local Computer Policy*, open *Computer Configuration*, open *Administrative Templates*, click System, and then click **Logon.**
3. Set the *Hide entry points* attribute of the Fast User Switching to Enabled.
4. Close the *Fast User Switching* properties window.
5. Close the *Group Policy* window.

Method B: Access the Registry

1. Click ***Start***, type "regedit.exe" in the *Start Search* dialog box, and press *Enter*.
2. Open HKEY_LOCAL_MACHINE, open SOFTWARE, click Microsoft, open Windows, open CurrentVersion, click Policies, and Open System.
3. Right-click in the left pane of the *System* folder.
4. Click New, DWORD (32-bit) value.
5. In the window, type "HideFastUserSwitching," and press *Enter*.
6. Click the HideFastUserSwitching value.
7. Type "1" into the *Value* data field, and click ***OK***.
8. Close the *Registry Editor* window.

3.3.2 Disabling Fast User Switching in Windows 8.1

1. In the *Home* screen, move the mouse to the lower-right corner, and click the *Search* icon.
2. In the search box, type "gpedit.msc."

3. Double-click on the *gpedit* icon in the *Apps* pane.
   - The Local Group Policy Editor window opens.
4. Open *Computer Configuration*, open *Administrative Templates*, open *System*, and then open *Logon*.
5. In the "Setting" pane, double-click *Hide entry points for Fast User Switching*.
6. Select *Enabled*, then click ***OK***.
7. From the *Home* screen, mouse to the lower right corner, and click the *Search* icon.
8. Type "Run" in the search field and a dialogue box will open.
9. Enter the command "gpupdate /force" into the text box, and then click ***OK***.

NOTES:

- Note the space before the backslash.
  - The Windows system command box will open.
  - When *Computer policy update has completed successfully* displays, the Fast User Switching function has been successfully disabled.

3.3.3 Disabling Fast User Switching in Windows 10

1. Click the ***Start*** button.
2. Type "gpedit.msc" in the search box, and press *Enter*.
3. Open *Computer Configuration*, open *Administrative Templates*, open *System*, and then click *Logon*.
4. Double-click *Hide entry points for Fast User Switching*.
5. Select *Enabled*, and click ***OK***.
6. In the search box, type "Run**"** to open the dialogue box.
7. Enter the command "gpupdate /force" into the text box, and then click ***OK***.

NOTES:

- Note the space before the backslash.
- The Windows system command box will open.
- When, *Computer policy update has completed successfully* displays, the Fast User Switching function has been successfully disabled.
- To force an exit of the Secure Browser before the test completes, enter *Shift* + *Esc* + *E*.

3.4 Network Installation for Windows (Network Administrators)

Install the Secure Browser to all computers on a network by copying browser files from the network to individual computers or through third-party programs to run the installers, such as Apple Remote Desktop (ARD). This section describes how to install the Secure Browser using a network.

3.4.1 Installing Secure Browser to a Shared Drive

Follow these steps to install the browser onto the server.

1. Map the network directory to where the Secure Browser was installed previously on each client machine.
2. In the network location where the Secure Browser is installed, create a shortcut by right-clicking the *STAAR Online Testing Program* icon and selecting *Create Shortcut*.
   - Optional: Rename the new shortcut, e.g., STAAR Online Testing Program.
   - This becomes the shortcut link name used in Step 4.
3. In the properties menu of the shortcut, change the path to use the mapped path as if on the client machine.
4. Add the following command to each user (computer) profile, which will execute upon login through the user group login script:

   COPY "<X> \ STAAR Online Testing Program.lnk" "%USERPROFILE%\Desktop"

   NOTE: <X> refers to the shared directory from which the browser will be run. The script will need to reference the correct directory.

3.4.2 Secure Browser Installation Directory from Network to Client

Follow these steps to place the Secure Browser installation directory from the network to client computers.

1. Identify the network directory where the browser file was saved.
   - These instructions will refer to that network directory as <X>.
2. Identify the target directory on the local user computers where the browser will copy the file(s).

   NOTES:
   - These instructions will refer to that directory as <Y>.
   - User must have write access to <Y>.
   - Restricted users will have access only to certain folders on the local computers.
3. Create a shortcut in the network directory by right-clicking the *Securebrowser.exe* icon, and selecting *Create Shortcut*.

4. Rename the new shortcut "STAAR Online Testing Program."

   NOTE: In the shortcut Properties, the Target and Start In attributes will show the <X> network installation directory.

5. In both the *Target* and *Start In* attributes windows, change the shortcut properties to the <Y> directory instead of the default <X> network directory on the local computers.

   NOTE: The Secure Browser shortcut will point to the designated installation directory.

6. Add the following lines to the login script for each user, replacing the actual local and source network directories for <Y> and <X>.

   IF EXIST <Y> GOTO DONE

   XCOPY "<X>" "<Y>" /E /I

   COPY "<Y>\ STAAR Online Testing Program.lnk" "%USERPROFILE%\Desktop"

   :DONE EXIT

3.5 Installing Secure Browser for Mac OS X

The following instructions cover the process of preparing and installing Secure Browser on supported Mac OS X devices.

NOTE: Before installing a new version on a device where Secure Browser is already installed, uninstall the previous version. Refer to **Section 3.5.3 Uninstalling the Mac OS X Secure Browser** for directions.

1. Open a browser and navigate to http://www.texasassessment.com/technology/.
2. Click on the *For MacOS*® link and click OK in the popup window.
3. Select the *securebrowswer.dmg* icon located on the desktop or downloads folder.
4. Double-click the *SecureBrowser* icon in the pop-up window.
5. When the pop-up displays, "SecureBrowser is an application downloaded from the Internet. Are you sure you want to open it?" click the ***Next*** button.
6. In the next pop-up window, enter the password and click ***OK***.
7. Click ***Next*** to allow the software to install.
8. Accept the licensing agreement, and click ***Next***.
9. Specify where Secure Browser should be installed, and click ***Next***.
10. When the installation completes, launch Secure Browser by double-clicking the Secure Browser icon on the desktop or the dBT.app in the . . . Applications/STAAR Online Testing Program folder.

3.5.1 Disabling Spaces in Mission Control on Mac OS Computers

Spaces should be disabled on computers that students will be using. Follow the instructions below to disable Spaces.

1. Navigate to *Apple*, then select *System Preferences*.
2. In *System Preferences*, click the ***Keyboard*** icon. The *Keyboard* window displays.
3. Click the Keyboard Shortcuts tab.
   - The keyboard shortcuts options list will display.
   - Mac OS 10.9 uses the label *Shortcuts*.
4. In the left panel, click *Mission Control.*
   - The right panel displays all Mission Control options.
5. In the right panel, uncheck the following boxes:
   - Move left a space.
   - Move right a space.
   - Switch to Desktop 1.

NOTE: To re-enable these functions, follow Steps 1 thru 5 again, checking the boxes.

3.5.2 Adding Secure Browser as a Trusted Application in Accessibility Preferences

Earlier Mac operating systems automatically added Secure Browser as a trusted application during installation. Installing Secure Browser on computers running Mac OS X requires that this step be performed manually.

Follow these steps to add Secure Browser as a trusted application in *Accessibility Preferences*.

NOTE: Performing these extra steps is only required once per installation.

1. After installing Secure Browser, a window appears displaying the message, "*dBT would like to control this computer using accessibility features*."
2. Open *System Preferences* (under the Apple icon).
3. The *System Preferences* (accessibility) window appears. Click the lock icon in the bottom left.
4. Enter the admin credentials when prompted.
5. Check the *dBT* checkbox with the STAAR icon under "Allow the apps below to control your computer." to enable accessibility features.
6. Click on the lock icon again on the bottom left to save the settings.

NOTE: If Secure Browser is not added as a Trusted Application on systems running Mac OS X and above, system check fails and returns the following error message, "Accessibility features have not been enabled for this application."

3.5.3 Uninstalling the Mac OS X Secure Browser

Follow these steps to uninstall the Secure Browser.

- Open the Applications window, then open *STAAR Online Testing Program*, and then open the uninstall.app file.
- Follow the on-screen directions to allow the software to uninstall.
- When complete, click ***OK*** *in the pop-up dialog*.

3.5.4 Uninstall/Reinstall the Mac OS X Secure Browser

Follow these steps to uninstall/reinstall the Secure Browser.

To uninstall:

1. Open the Applications folder, then open the STAAR Online Testing Program – Secure Browser, and then double-click the uninstall.app file.
2. Follow the on-screen directions to allow the software to uninstall.
3. When complete, click ***OK***.

To reinstall:

1. Open a browser and navigate to http://www.texasassessment.com/technology/.
2. Click on the *For MacOS®* link.
3. Select the *securebrowser.dmg* icon located on the desktop or downloads folder.
4. Double-click the *SecureBrowser* icon in the pop-up window.
5. When the pop-up displays "SecureBrowser is an application downloaded from the Internet. Are you sure you want to open it?" click the **Next** button.
6. In the next pop-up window, enter the password and click ***OK***.
7. Click ***Next*** to allow the software to install.
8. Accept the licensing agreement and click ***Next***.
9. Specify where Secure Browser should be installed, and click ***Next***.
10. When the installation completes, launch the Secure Browser by double-clicking the icon in the Application folder.

3.5.5 Network Installation Information for Mac OS X

The appropriate Secure Browser must be installed on each computer that will be used for online testing. While it is strongly recommended to install the Secure Browser on each individual computer that will be used, the browser can be pushed out to all computers through a network by copying browser files from the network to individual computers or through third-party installation programs.

Follow these steps to install the Secure Browser on Mac OS X Operating Systems using the Apple Remote Desktop (ARD) application.

1. Log in to an administrator computer on the network. This computer should have Apple Remote Desktop installed and running.
2. Download the correct Mac OS X browser from the portal.
3. Click the downloaded icon to unzip and save the .dmg file onto the administrator computer.
4. Open the .dmg file and select the .app file.
5. Open the Apple Remote Desktop.
6. In the Apple Remote Desktop window, select a Computer List.
7. Select the correct computers from the *Computer List* to install the Secure Browser.
8. Open *Manage*, then select *Copy Items*.
9. Select the browser .app file (from Step 4).
10. Select *Copy Options*, including the preferred destination on the target machine.
11. Click ***Copy***.

3.6 iOS (iPad) Secure Browser

The Secure Browser for iPad can be downloaded from the App store. The process for installing the Secure Browser is the same as for any other iOS app.

For information about supported operating systems, hardware recommendations, and requirements for monitors/screens, keyboards, and headphones refer to the *Unified Minimum System Requirements for the Administration of Online Assessments* available online at http://www.texasassessments.com/technology/.

NOTE: The "Guided Access" feature must be enabled to run Secure Browser.

3.6.1 Installing the iOS Secure Browser

The Secure Browser for online testing on iPads can be downloaded from the App store.

1. Open and search the Apple App Store for "STAAR."
2. Select the STAAR Online Testing Program app.
3. Click ***GET*** to download the app.
4. Click ***Update*** if the window appears.
5. The app will download to the *iPad Home* screen.

3.6.2 Automatic Assessment Mode for iOS 9.3.2 and Later Devices

For devices running iOS 9.3.2 and later, Secure Browser uses Apple's "Automatic Assessment Configuration" feature to lock and configure iPads in single app mode. Refer to the Apple Support website at https://support.apple.com/en-us/HT204775 for more information about Automatic Assessment Configuration.

Single app mode locks iPads to the Secure Browser application and disables the Home button. The single app mode automatically starts when Secure Browser runs a system check and automatically stops when the ***Exit*** button is clicked.

Follow these steps to enable single app mode in the **Secure Browser**.

1. Open the Secure Browser app. During the 'Security Configuration' of System Check, a "Confirm App Self-Lock" notification pops up.
2. Click "Yes" to start single app mode. The system check passes and Secure Browser starts normally.

NOTES:

- Clicking "No" causes the Security Configuration to fail and Secure Browser displays the message, *The application runs only in single app mode*. You must enable it in the 'Confirm App Self-Lock' pop-up notification. Contact your Test Center Administrator. Click the ***Retry*** button to run the app again and confirm app self-lock.
- **Secure Browser** runs in single app mode until the ***Exit*** button is clicked. After clicking the ***Exit*** button, the "Exit Page" appears displaying the message, *You are out of secure mode. Press the home button to exit the app.*

3.6.3 Enabling Guided Access

Secure Browser automatically locks and configures devices running iOS 9.3.2 and higher. Use these directions to enable Guided Access on devices running earlier supported iOS versions. The following instructions are based on iOS 8.1.2.

1. In the *Settings* window, open *General*.
2. Open *Accessibility*.
3. Scroll down and open the *Guided Access* window under "Learning."
4. Change the *Guided Access* setting to *ON*.
5. Open *Passcode Settings*.
6. Click *Set Guided Access Passcode*.
7. Enter a four-digit passcode.
8. Re-enter the four-digit passcode.

NOTES:

- Settings may vary slightly based on iOS version.
- Remember the passcode(s). The passcode is needed for exiting the Secure Browser app and prevents the iPad test taker from using other apps during testing. The test taker should NOT be given the passcode.

3.6.4 Activating Guided Access Before a Test Session Begins

Before using the Secure Browser, *Guided Access* must be engaged. *Guided Access* must be enabled. refer to **Section 3.6.3 Enabling Guided Access** for details.

1. Select the *STAAR Online Testing Program* app icon on the desktop.
2. When the app launches for the first time after installation, when the *Security Configuration* fails, triple-press the ***Home*** button to initiate *Guided Access*.
3. On the *Guided Access* page, toggle *Touch* to the on position.
4. Click the ***Options*** button under "Hardware Buttons" and toggle the settings there to the on position.
5. Choose *Start* in the upper right of the screen.
6. Enter and confirm your passcode in the pop-ups that appear.

NOTE: When Guided Access is activated, students cannot switch to any other applications or take screenshots.

3.6.5 Deactivating Guided Access After a Test Session Ends

1. Triple-press the ***Home*** button.
2. Enter the *Guided Access* passcode.
3. Click the ***End*** button in the upper-left corner.
   - A confirmation message appears.
4. Press the iPad's Home button to close Secure Browser.

NOTE: If the passcode is unknown, then force a reboot of the device by pressing the Home and Power keys simultaneously for ten seconds.

3.6.6 Closing the iPad Secure Browser

1. Double-click the ***Home*** button. This opens the multitasking screen.
2. Locate the *STAAR Online Testing Program* app preview, and slide it upward.

3.7 Installing Secure Browser on Android Devices

The Secure Browser can be downloaded from the Play Store or from the Technology Systems and Supports page at http://www.texasassessment.com/technology/. The process for installing the application is the same as for any other Android app.

Follow these steps to install and configure Android devices.

1. Download *STAAR Online Testing Program* from the Play Store.
2. Choose *INSTALL*.

3. The app downloads and installs automatically leaving the *STAAR Online Testing Program* icon on the device home screen.
4. After opening, the app checks the device configuration and connectivity settings for adequate memory and Internet connection.
5. Run the *LCS Settings* app when prompted.

NOTES:

- The current version may request access to the device's storage and permissions to draw over other apps, disable screen lock, reorder running apps, full network access, prevent device from sleeping, retrieve running apps, change audio settings, view network and Wi-Fi connections.
- Kiosk mode is available.

3.8 Installing Secure Browser on Linux Computers

NOTE: Before installing a new version on a device where Secure Browser is already installed, uninstall the previous version.

The following instructions cover the process of preparing and installing the Secure Browser on Linux computers.

1. Open a browser and navigate to http://www.texasassessment.com/technology/.
2. Select the appropriate package for your Linux distribution (Fedora, Ubuntu, or Distro) to download the software and package manager files.
3. In the download pop-up, indicate that you want to open the file.
4. Double-click the downloaded package in the *Software Center* or *Manager*.
5. Use the appropriate installation tool for your particular Linux distribution to install.
6. Accept the licensing agreement and click ***Next***.
7. Specify where the Secure Browser should be installed, and click ***Next***.
8. When the installation completes, launch the Secure Browser.

NOTE: Installation procedures vary slightly on some versions of Linux based on distribution type. Refer to https://www.linux.com/blog/how-install-software-linux-introduction for more information.

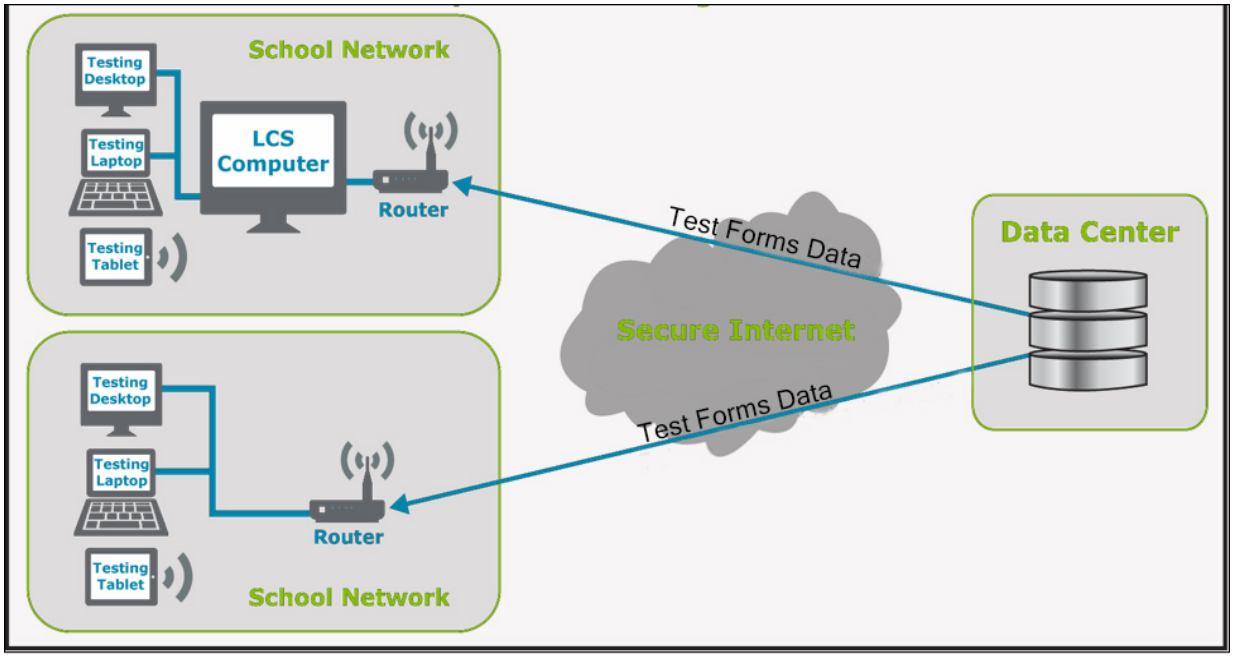
Section 4: Local Caching Software

4.1 Introduction

The STAAR Online Testing Platform Secure Browser has caching capabilities that should eliminate the need for local caching software for most districts. However, under extreme circumstances where bandwidth is known to be insufficient or Internet connectivity is considered unreliable, a second layer of caching, called Local Caching Software (LCS) will be required. For more information, refer to the *STAAR Online Testing Platform LCS District Guide* at http://www.texasassessment.com/technology/.

LCS performs effectively when a large number of students are testing simultaneously. Downloading test data directly from the Internet may over-burden a campus Internet connection. With LCS, all the tests are cached on a local system, and students taking a test download the data from the LCS rather than from a remote Internet location.

- This process eliminates the need to download the same test multiple times from a remote server.
- Each testing device downloads test data from the LCS.
- Using the LCS reduces the reliance on Internet bandwidth during testing and increases the number of possible simultaneous testers.



The image above illustrates how using the LCS differs from a direct Internet connection to the Data Center.

4.2 LCS Registration

Due to the secure nature of the test content, an LCS Registration Key is required for operating this application. The LCS needs to be configured for deployment and use with testing devices the first time it is launched.

NOTES:

- Test content is automatically downloaded once the LCS is installed, registered, and configured.
- Downloading the application and test data may take several hours, depending on available bandwidth.
- The *LCS Monitoring Tool Checklist* provides the status of these activities.

4.3 LCS Monitoring Tool

The LCS includes a Web-based LCS Monitoring Tool that provides a convenient way to track testing activity.

4.4 Operating Requirements

This section details the minimum system and Internet connectivity requirements for LCS.

4.4.1 Minimum LCS System Requirements

The LCS requires installation and configuration. It does not require commercial server hardware. A high-end desktop that satisfies the minimum requirements to run the LCS can be used. The LCS must be installed on an extremely reliable and secure system, since all test data will be stored on it.

NOTE: For additional information about supported operating systems, hardware recommendations, and requirements for monitors/screens, keyboards, and headphones refer to the *Unified Minimum System Requirements for the Administration of Online Assessments* (also known as the UMSR) available online at http://www.texasassessments.com/technology/.

Minimum LCS System Requirements	
Memory	4 GB RAM (8GB RAM recommended)
CPU/Processor	Mac: Intel x86 processor Windows: Pentium 4 processor and above
Disk Space	15 - 30 GB free space
File Permissions	Full permissions to create or write to any files in the LCS installation folder.
Operating System	Microsoft Windows Server: 2008/R2 and 2012
Web Browsers	Chrome – Latest version Firefox – Latest version and current Extended Support Release (ESR) Internet Explorer – v9-11

4.4.2 Minimum Internet Connectivity and Security Requirements

Minimum Internet Connectivity and Security Requirements	
Network	All testing computers must be connected to the local area network (LAN).
Connection	LCS requires continuous Internet connectivity.
Power Position	LCS computer must remain on and must not be powered down or put in "sleep mode" during the test administration window.
Connection Protocols	Connections to the intranet using HTTP and HTTPS protocols.

4.4.3 Internet Connectivity and Security

Testing computers must be part of a local area network. The LCS must be connected to the Internet via a broadband Internet connection.

- LCS requires continuous Internet connectivity.
- LCS must remain ON and not powered down or put in "sleep mode" during the test administration window.
- Allow connections to the Internet using HTTP and HTTPS protocols.
- Allow communication to *.caltesting.org.

4.4.4 LCS Error Message

If users launch a Secure Browser with an outdated version of the LCS, they receive the following message:

"You are using an old version of the LCS. Contact your Technology Coordinator for assistance."

To correct this issue, the administrator needs to complete the following steps:

1. Verify that no tests in the current administration were taken with the old LCS.
2. If tests were taken with the old LCS, back up and sync the installer directory.
3. Reinstall the current version of the LCS.
    - Refer to **Section 4.6 Installing the LCS** for additional information.

4.5 Creating an LCS Registration Key

LCS Registration Keys are used to encrypt the downloaded content. Due to the secure nature of the test content, an LCS Registration Key is required to complete the LCS installation. LCS keys can be created in the Assessment Management System by District Testing Coordinators. Users can create as many keys as are necessary, but only one LCS key should be issued to each LCS instance. LCS computers should not share the same key.

1. Open a browser and log in to the Assessment Management System at https://tx-toms.ets.org/
2. Click the *Online Testing* tab in the left navigation menu, and then select the *LCS Management* tab.

3. Click *Select Campus* and choose a campus from the pop-up.
4. Create and confirm a password for the LCS.
5. Add a description for the LCS key, such as a classroom location or a number if the campus will be using multiple LCS instances.
6. Click *Create LCS Key*. The *School*, *Password*, *Key*, *Create Date*, and *Status* will all be listed at the bottom of the screen.

4.6 Installing the LCS

LCS installation must be done manually on any computer that is being designated as an LCS.

NOTE: The LCS must not be installed to a location that has a space (‘ ‘) in the path name.

4.6.1 Installing LCS for Windows

Follow these steps to install the LCS on Windows devices.

NOTE: Prior to installing the LCS on devices running Windows 10, a default browser must be set.

1. Determine a location that has internal network connectivity/routing between test client workstations/devices and the LCS computer/server.
2. Use the link provided by the Support Center to download the LCS installer.
3. Open lcs_windows-exe-{version}.exe.
4. Follow the on-screen installation directions to allow the software to install.
5. When the installation is complete, double-click the *LCS* icon on the desktop.

4.6.2 Uninstalling LCS for Windows

Follow these steps to uninstall the LCS on supported Windows devices.

1. Click ***Start*** in the task bar, open *Settings*, then open the *Control Panel*.
2. Click *Programs and Features*.
3. Locate and click *Texas LCS*.
4. Select *Uninstall* and complete the uninstall process.
5. Follow with deletion of the C:\Program Files (x86)\Texas directory.
6. Restart the computer.
7. Verify that Texas LCS is fully uninstalled.
   - Check that Texas LCS is no longer listed in the *Start* menu.
   - Check that the *Texas LCS* entry in *Programs and Features* has been removed.

4.6.3 Installing LCS for Mac OS X

Follow these steps to install the LCS on supported Mac OS X devices.

1. Determine a location that has internal network connectivity or routing between test client workstations and devices and the LCS computer.
2. Use the link provided by the Support Center to download the LCS installer.
3. Select the *lcs-osx.dmg* icon located on the desktop or in the *Downloads* folder.
4. Drag *TexasLCS* into the *Applications* folder.
5. When the installation completes, launch the LCS by double-clicking the desktop shortcut.

4.6.4 Uninstalling LCS for Mac OS X

Follow these steps to uninstall the LCS on supported Mac OS X devices.

1. Open the *Applications* window, find *TexasLCS* and drag it into the *Trash*.
2. Empty the *Trash*.
3. Restart the computer.

4.6.5 Configuring the LCS Computer

The first time the LCS is started, it must be configured for deployment and use with test computers.

1. Launch *Texas – LCS* from the desktop.
2. In the event of a firewall alert, select *Allow access*.
   - A browser will open with the *LCS Monitoring Tool Checklist*.
3. Click ***Connect*** to start the connection to the Data Center.
   - Once connected, registering LCS will be available.
4. Enter the *Key* and *Password*, and click ***Go***.
5. The *LCS Registration Key* and password can be found in using the Assessment Management System.
6. Open a browser and log in to the Assessment Management System at https://txtoms.ets.org/. In the left navigation pane, select *Online Testing*, then select *LCS Management*.
   - Users can create as many LCS keys as are necessary
   - Each LCS should be issued its own unique *Registration Key*.
   - Refer to **Section 4.5: Creating an LCS Registration Key** for additional information.
   - Configuring LCS will be available.
7. Confirm the following and click ***Go***:
   - Cache directory.
   - The default file location displays where the test content will be stored.
8. Confirm that this directory has significant free disk space.

NOTES:

- This process may take several hours, depending on available bandwidth. If the download is interrupted, it will resume from the point of interruption provided the same cache directory is specified. It is recommended that the computer is not set to go into "sleep" mode during the download process.
- 30 GB is sufficient for most installations.
- The default port number displays.
- The port number must be between 1024 and 65535.
- The default port is sufficient for most installations.
- Once complete, the LCS will then download *App and Test Data*.

4.6.6 Troubleshooting Configurations

Follow these instructions if any step in the process fails.

1. Recheck that the LCS is connected to the Internet.
2. Confirm the LCS Registration Key is not already in use by another LCS instance.
3. Confirm the Registration Key and password from the Assessment Management System were entered correctly.
4. Enter a different port number.
5. Refresh the browser, and click ***GO*** again if it displays.
6. Close the browser window and relaunch *Texas – LCS*.
7. Restart the LCS computer.

NOTE: Do **not** use disk imaging systems such as DeepFreeze with the LCS.

4.6.7 Accessing the LCS Monitoring Web Page

The LCS provides the LCS Monitoring Tool. It is a web-based monitoring tool that tracks current test volume and shows the status of cached data as well as data center connectivity.

NOTE: The LCS Monitoring Tool displays only after the test content has been downloaded.

1. Open the computer's web browser
2. In the *Address* field, enter http://localhost:28880/admin.html.
3. Input the LCS key and password.
4. Press the ***Login*** button.

The descriptions below outline the fields on the LCS Monitoring Tool page.

Data Status – displays the status of the Data Center, the testing data, and when it was last checked.

Memory Cache – shows the amount of memory that is currently being used to cache content.

Shutdown – click the *Shutdown Application* link to stop the LCS.

Students Currently Testing – displays the current number of testers using the LCS over the past 5 minutes.

Service Addresses – displays the available IP address(es), port number(s), and URL(s).

Configure Chromebook – Select this button to access the JavaScript Object Notation (JSON) needed to remotely push LCS configurations to managed Chromebooks.

Log File – displays the location of the log file, which may be useful for troubleshooting.

After logging in to the LCS Monitoring Tool, the LCS remains running, even after the browser window has been closed.

NOTES:

- The LCS continues to run until the computer is completely shut off.
- When the LCS computer is restarted, the LCS must be launched again.
- Enter the same *LCS Registration Key* and password again.
- The LCS computer should remain ON while testing is in progress.
- It is recommended that the LCS computer is **not** set to go into sleep mode, during testing.

4.7 Configuring Test Computers and Devices to Connect to the LCS

When an LCS or multiple LCSs are being used, configure the Secure Browser on every testing computer to connect to a specific LCS IP Address.

NOTES:

- Set the *LCS IP Address* on all testing devices before using the testing devices.
- Failure to do this will not prevent students from testing, but devices will not make use of the LCS.

4.7.1 Chromebook

Follow these steps to configure Chromebooks individually.

1. Launch the Secure Browser, and press ***Shift + Ctrl + 5***.
2. Click on *LCS switch* to enable it.
3. Enter the LCS/IP Address.
4. Enter the LCS Port Number.
5. Click ***Save***.

Follow these steps to push LCS configurations to managed Chromebooks.

1. Sign in to the *Admin console*.
2. Open the Device Management tab, open Chrome, and then click *App Management*.
   - A list appears displaying all of the Chromebooks across the domain running the LCS and the status of each.
3. Select Texas STAAR Online Testing Program.
4. Select Kiosk settings.
5. Select the organization where settings will be configured.
6. When configuring policies and settings for everyone in the organization unit, select the *top-level org unit*. Otherwise, select one of the *child org units*.
7. Select UPLOAD CONFIGURATION FILE.
8. Select the appropriate JSON configuration file to apply to this org unit. JSON is available in the *LCS Monitoring Tool*.

   Example:

```
{
"lcs_url" : {
"Value" : "10.11.66.170"
},
"lcs_enabled" : {
"Value" : true
},
"lcs_port" : {
"Value" : 28443
}
}
```

9. When finished with the configuration, save the file.
10. Repeat steps 5-7 for all org units.

NOTE: To disable LCS configuration, upload a new JSON configuration file with *lcs enabled* set to false.

4.7.2 Windows

Follow the steps to configure Windows computers individually.

1. Open the **Start** menu, select All Programs, open STAAR Online Testing Program, and select Secure Browser Preferences.
2. Set the correct LCS settings.

3. Select Local Caching Software.
4. Set the LCS switch to *Enable*.
5. Enter the LCS Hostname/IP Address.
6. Enter the LCS Port Number.
7. Click ***Save***.

Follow these steps to remotely push LCS configurations to Windows devices.

1. Configure the LCS manually on one computer (IP and port).
2. Copy the configurations file from this machine to all testing machines that will use this LCS.
3. Use network administration tools for this.
   - *e.g.* System Center Configuration Manager (SCCM) group policy.
4. Use the configurations file noted below.

   C:\Program Files (x86)\STAAR Online Testing Program\conf\system.properties

4.7.3 Mac

Follow these steps to configure Mac computers individually.

1. Open the Applications tab, click STAAR Online Testing Program, and then select Preferences.
2. Input the LCS settings.
3. Select Local Caching Software.
4. Set the LCS switch to *Enable*.
5. Enter the LCS Hostname/IP Address.
6. Enter the *Port Number*.
7. Click ***Save***.

Follow these steps to remotely push LCS configurations to Mac devices.

1. Configure the LCS manually on one computer, IP, and port.
2. Copy the configurations file from this machine to all testing machines that will use this LCS.
3. Use the *Network Administration Tools* to do this (e.g., ARD).
4. Use the configurations file noted below.

   /Applications/STAAR Online Testing Program/conf/system.properties

4.7.4 Linux

Follow these steps to configure the Secure Browser to utilize the LCS on Linux computers individually.

1. Locate the *STAAR Online Testing Program* in the path where it is installed.
2. Select Preferences.
3. Input the LCS settings.
4. Select Local Caching Software.
5. Set the LCS switch to *Enable*.
6. Enter the LCS Hostname/IP Address.
7. Enter the *Port Number*.
8. Click ***Save***.

Follow these steps to remotely push LCS configurations to Linux devices.

1. Configure the LCS manually on one computer, IP, and port.
2. Use OpenSSH or another Network Administration Tool to copy the configurations file from this machine to all testing machines that will use this LCS.
3. Use the configurations file noted below.

   /usr/bin/STAAR Online Testing Program/conf/system.properties

4.7.5 iPad

Follow these steps to configure iPads individually:

1. Open the *System Settings* icon.
2. Select *STAAR Online Testing Program*, from the left column.
3. Enter the LCS Hostname/IP Address.
4. Enter the *Port Number*.

Follow these steps to remotely push LCS configurations to iPads.

1. Use the MDM solution to push out the *App Settings* for, *STAAR Online Testing Program*.
2. Consult with the MDM vendor for instructions.

Appendix A: URLs

Site	URL
Portal	http://www.texasassessment.com/
STAAR Assessment Management System	https://tx-toms.ets.org/
Online Testing (for configuration use only)	https://tx-tss.caltesting.org/
Technology Systems and Supports	https://www.texasassessment.com/technology/

NOTE: For enhanced scalability, these URLs are delivered through the cloud, so specific IP addresses are not available.

Appendix B: IT Staff Readiness Checklist

Information Technology Staff Readiness Checklist

☑	Action Item	Preparation Timeline	Information Resource
☐	**Step 1:** Verify that the network meets the requirements, is configured for testing, and can connect to the Internet. Conduct network diagnostics to confirm sufficient bandwidth.	Can begin immediately.	STAAR Assessment Management System Technology Guide Section 1
☐	**Step 2:** Verify that all of the computers used for online testing meet the minimum hardware and software requirements.	Can begin immediately.	STAAR Assessment Management System Technology Guide Section 2
☐	**Step 3:** Install the Secure Browser on all testing devices.	3 to 4 weeks before testing begins.	STAAR Assessment Management System Technology Guide Section 3
☐	**Step 4:** Determine if the local network would benefit from the LCS. Install the LCS and configure testing computers to connect to the LCS.	3 to 4 weeks before testing begins.	STAAR Assessment Management System Technology Guide Section 5
☐	**Step 5:** Take a practice test from each testing device (using a student network or device login as necessary.)	3 to 4 weeks before testing begins.	STAAR Assessment Management System Technology Guide Section 3
☐	**Step 6:** For Windows computers, disable Fast User Switching.	2 to 3 weeks before testing begins.	STAAR Assessment Management System Technology Guide Section 3
☐	**Step 7:** For Mac computers, disable Spaces in Mission Control.	2 to 3 weeks before testing begins.	STAAR Assessment Management System Technology Guide Section 3
☐	**Step 8:** Ensure that all applications, except those identified as necessary by the technology staff, are uninstalled from testing computers.	1 to 2 weeks before testing begins.	
☐	**Step 9:** Shutdown any automatic updates during testing window.	1 to 2 weeks before testing begins.	
☐	**Step 10:** During the testing window, ensure staff availability to follow up internally on any technical issues that may arise.	Ongoing throughout the testing window.	

Index

I *(continued)*

K

L

M

N

N *(continued)*

O

P

Q

R

S

Secure Browser *(continued)*

T

U

V

V *(continued)*

W

Windows *(continued)*