STAAR Online Testing Platform
Technology Guide

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

STAAR 3–8 and End-of-Course (EOC) Online Testing

Updated April 1, 2019
# New Sections in this Version

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.6 Installing Secure Browser for Mac OS X</td>
<td>26</td>
</tr>
<tr>
<td>Section 5: JAWS® and Refreshable Braille Displays</td>
<td>50</td>
</tr>
</tbody>
</table>
# Table of Contents

New Sections in this Version ........................................................................................................................................................................ 2

Section 1: Network Requirements ..................................................................................................................................................................... 6
  1.1 Platform Overview .................................................................................................................................................................................. 6
  1.1.1 Support ............................................................................................................................................................................................ 6
  1.2 Network Connections .............................................................................................................................................................................. 6
    1.2.1 Network Settings ......................................................................................................................................................................... 7
    1.2.2 Network Performance .................................................................................................................................................................. 7
  1.3 Bandwidth ........................................................................................................................................................................................................... 7
    1.3.1 Students Testing Simultaneously ............................................................................................................................................ 8
    1.3.2 Determining Bandwidth Requirements ........................................................................................................................................ 8
    1.3.3 Size of Test Content .................................................................................................................................................................... 9
    1.3.4 LCS (Local Caching Software) .................................................................................................................................................. 9
    1.3.5 Secure Browser Installation ..................................................................................................................................................... 9
  1.4 Wireless Networking ............................................................................................................................................................................ 10
    1.4.1 Wireless Access Points ............................................................................................................................................................... 10
    1.4.2 Recommended Workstations per Wireless Connection ........................................................................................................ 10
  1.5 Online Readiness Tools ........................................................................................................................................................................ 11
    1.5.1 System Requirements ................................................................................................................................................................. 11
    1.5.2 School Capacity Calculator .................................................................................................................................................. 11
    1.5.3 System Check Test .................................................................................................................................................................. 12
  1.6 Network Diagnostic Tools .................................................................................................................................................................... 12
    1.6.1 MS Windows® Specific Tools .................................................................................................................................................. 12
    1.6.2 Mac OS X Specific Tools .......................................................................................................................................................... 12
    1.6.3 Multi-Platform tools ................................................................................................................................................................... 12
  1.7 Network Configurations ...................................................................................................................................................................... 13
    1.7.1 Protocols ........................................................................................................................................................................................ 13
    1.7.2 MIME Types ................................................................................................................................................................................ 13
    1.7.3 Uniform Resource Locators (URLs) ........................................................................................................................................ 13
    1.7.4 Domain Name Resolutions (DNS) ........................................................................................................................................ 13
    1.7.5 Email server ................................................................................................................................................................................ 14
    1.7.6 Firewalls, Content Filters, and Proxy Servers .......................................................................................................................... 14
    1.7.7 QoS/Traffic Shaping ................................................................................................................................................................. 14
  1.8 Virtualization Guidelines ...................................................................................................................................................................... 14
    1.8.1 Security ..................................................................................................................................................................................... 14
    1.8.2 Performance Comparability ...................................................................................................................................................... 14
    1.8.3 Virtualization Evaluation Process ........................................................................................................................................... 14
    1.8.4 Critical Security Standards ................................................................................................................................................ 15
    1.8.5 Critical Performance Standards ........................................................................................................................................ 15

Section 2: Hardware Requirements .................................................................................................................................................................. 16

Section 3: Secure Browser ....................................................................................................................................................................... 17
  3.1 Secure Browser Autoupdates ............................................................................................................................................................ 17
### Table of Contents

3.2 Chromebook Installation ........................................................................................................... 18  
  3.2.1 Managed Chromebook Installation Procedure ................................................................. 18  
  3.2.2 Non-managed Chromebook Installation Procedure ......................................................... 19  
  3.2.3 Disabling ChromeVox ........................................................................................................... 20  
  3.2.4 Closing the Chromebook Secure Browser ......................................................................... 21  
3.3 Installing Secure Browser on Windows Devices ...................................................................... 21  
  3.3.1 Manually Install .msi Package with User Interface ............................................................ 21  
  3.3.2 Installing the .msi Package ................................................................................................. 21  
  3.3.3 Manually Uninstalling Secure Browser ............................................................................ 22  
3.4 Disabling Fast User Switching in Windows ............................................................................. 23  
  3.4.1 Disabling Fast User Switching in Windows 7 ..................................................................... 23  
  3.4.2 Disabling Fast User Switching in Windows 8.1 ................................................................. 23  
  3.4.3 Disabling Fast User Switching in Windows 10 ................................................................. 24  
3.5 Network Installation for Windows (Network Administrators) .................................................. 25  
  3.5.1 Installing Secure Browser to a Shared Drive ..................................................................... 25  
  3.5.2 Secure Browser Installation Directory from Network to Client ........................................ 25  
  3.5.3 Windows 7 Update Secure Browser Issues ...................................................................... 26  
3.6 Installing Secure Browser for Mac OS X .................................................................................. 27  
  3.6.1 Disabling Spaces in Mission Control on Mac OS Computers ........................................... 28  
  3.6.2 Disabling VoiceOver on Mac OS Computers ..................................................................... 28  
  3.6.3 Uninstalling the Mac OS X Secure Browser ...................................................................... 29  
  3.6.4 Uninstall/Reinstall the Mac OS X Secure Browser ............................................................ 29  
  3.6.5 Installation Information for Mac OS X .............................................................................. 30  
  3.6.6 Managing Apple Devices using Server Administration Software .................................... 31  
  3.6.7 Adding Secure Browser as a Trusted Application in Accessibility Preferences ................ 32  
  3.6.8 Launching Secure Browser with the Assessment User Account ....................................... 34  
    3.6.8.1 Creating an Assessment User Account Password ....................................................... 34  
3.7 iOS (iPad) Secure Browser ...................................................................................................... 35  
  3.7.1 Disabling iOS Accessibility Features .................................................................................... 36  
  3.7.2 Installing the iOS Secure Browser ....................................................................................... 36  
  3.7.3 Automatic Assessment Mode for iOS ............................................................................... 36  
  3.7.4 Closing the iPad Secure Browser ....................................................................................... 37  
3.8 Installing Secure Browser on Linux Computers ..................................................................... 37  
  3.8.1 Installing the Secure Browser ............................................................................................ 37  
  3.8.2 Manually Uninstalling the Secure Browser ........................................................................ 38  
Section 4: Local Caching Software ................................................................................................. 38  
  4.1 Introduction .......................................................................................................................... 38  
  4.2 LCS Registration .................................................................................................................... 39  
  4.3 LCS Monitoring Tool ............................................................................................................... 39  
  4.4 Operating Requirements ....................................................................................................... 39  
    4.4.1 Minimum LCS System Requirements ............................................................................... 39  
    4.4.2 Minimum Internet Connectivity and Security Requirements ........................................ 40  
    4.4.3 Internet Connectivity and Security .................................................................................... 40  
    4.4.4 LCS Error Message ........................................................................................................... 40  
  4.5 Creating an LCS Registration Key ........................................................................................ 40
# Table of Contents

4.6 Installing the LCS ........................................................................................................... 41
  4.6.1 Installing LCS for Windows ......................................................................................... 41
  4.6.2 Uninstalling LCS for Windows .................................................................................... 41
  4.6.3 Installing LCS for Mac OS X ....................................................................................... 42
  4.6.4 Uninstalling LCS for Mac OS X .................................................................................. 42
  4.6.5 Configuring the LCS Computer ................................................................................... 42
  4.6.6 Troubleshooting Configurations ................................................................................ 43
  4.6.7 Accessing the LCS Monitoring Web Page ................................................................. 44

4.7 Configuring Test Computers and Devices to Connect to the LCS ..................................... 44
  4.7.1 Chromebook ................................................................................................................ 45
  4.7.2 Windows ....................................................................................................................... 46
  4.7.3 Mac ............................................................................................................................... 46
  4.7.4 Linux ........................................................................................................................... 47
  4.7.5 iPad .............................................................................................................................. 47

Section 5: JAWS® and Refreshable Braille Displays ................................................................. 48
  5.1 Testing Students with Visual Impairments ................................................................. 48
    5.1.1 Technology Requirements ......................................................................................... 48
    5.1.2 Supported Operating Systems and Related Requirements ...................................... 48
    5.1.3 Additional Resources: ............................................................................................... 48
  5.2 Refreshable Braille Displays ........................................................................................ 49
    5.2.1 Using Braille Displays in Assessment Testing .......................................................... 49
    5.2.2 Secure Browser Screen Reader Compatibility ........................................................ 49
      5.2.2.1 Enabling JAWS 18 in the Secure Browser .............................................................. 50
    5.2.3 Adding a Braille Display .......................................................................................... 52
    5.2.4 Configuring the Screen Reader and Refreshable Braille Display ........................... 52
    5.2.5 Activating the Braille Viewer Display ..................................................................... 54
    5.2.6 Configuring the screen reader to Speak “Dollars” .................................................. 54
    5.2.7 Optional JAWS Voice Adjustment Settings ............................................................. 55
    5.2.8 Setting JAWS to Navigate by Custom Regions ....................................................... 56
  5.3 Navigating a Test with JAWS and an RBD ................................................................. 57
    5.3.1 Streamlined Questions and Answer Choices ......................................................... 57
    5.3.2 Reading Passages ...................................................................................................... 59
  5.4 Using the JAWS Reader ............................................................................................... 59
  5.5 Refreshable Braille Display – Test Administrator Guide ............................................... 59
    5.5.1 Navigating Items Optimized for Refreshable Braille Display users ...................... 59
      5.5.1.1 Settings ............................................................................................................... 59
      5.5.1.2 Terms and Additional Notes .............................................................................. 60

Appendix A: URLs .................................................................................................................. 64
Appendix B: IT Staff Readiness Checklist .............................................................................. 65
Appendix C: JAWS Keyboard Commands ............................................................................. 66
Index ...................................................................................................................................... 69
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 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.
Section 1: Network Requirements

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.

<table>
<thead>
<tr>
<th>Number of Students Testing Concurrently</th>
<th>Average Estimated Bandwidth Used for Testing</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>20K bytes/second</td>
</tr>
<tr>
<td>50</td>
<td>250–750K bytes/second (0.25–0.75M bytes/second)</td>
</tr>
<tr>
<td>100</td>
<td>500–1500K bytes/second (0.5–1.5M bytes/second)</td>
</tr>
</tbody>
</table>

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.
Section 1: Network Requirements

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.

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

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 to 1. 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 may cause 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:

<table>
<thead>
<tr>
<th>Workstations per Wireless Connection</th>
<th>802.11g Access Point</th>
<th>802.11n Access Point</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11g wireless cards</td>
<td>20 workstations or devices</td>
<td>40 workstations or devices</td>
</tr>
<tr>
<td>802.11n wireless cards</td>
<td>20 workstations or devices</td>
<td>40 workstations or devices</td>
</tr>
</tbody>
</table>

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


NTtcp ([http://www.microsoft.com/whdc/device/network/TCP_tool.mspx/](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/](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/](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/](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/](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.

<table>
<thead>
<tr>
<th>Port/Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>80/tcp</td>
<td>HTTP (initial connection only)</td>
</tr>
<tr>
<td>443/tcp</td>
<td>HTTPS (secure connection)</td>
</tr>
</tbody>
</table>

1.7.2 MIME Types

Allow downloading and uploading of the MIME types noted below.

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

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/](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 testing devices, confirm that all devices used for testing have the correct version of the Secure Browser installed.
- Secure Browser for Windows, Mac OS, iOS, and Linux includes Ivona Text-to-Speech features which are installed automatically with the application. No separate installation or setup is required.

**NOTE:** When viewing the Secure Browser application on most desktop displays and laptop displays, no scaling is required, and Windows sets a scale factor of 100%. However, some new devices, particularly in the premium laptop and tablet markets, have higher-resolution displays (such as newer Surface devices and 4K monitors). On these devices, check “Disable display scaling on high DPI settings” in Properties > Compatibility (right click on STAAR Online Testing Platform shortcut).

### 3.1 Secure Browser Autoupdates

The Secure Browser application automatically updates on all platforms except Windows, Mac OS and Linux. The autoupdate feature keeps Secure Browser continuously up-to-date. Though Secure Browser updates are needed infrequently, when updates are necessary, ETS makes every effort to give schools as much notice as possible (at least four weeks) before each test window to ensure districts have sufficient time to prepare.

On mobile platforms (ChromeOS and iOS), the autoupdate is handled automatically by the device. On desktop platforms (Windows and Mac), the Secure Browser must be manually updated prior to launching the Secure Browser.

**NOTE:** When an update is found, the user launching the software must have permissions to update software on the system. If students do not have these permissions, technology staff should manage the update process.

<table>
<thead>
<tr>
<th>Platform</th>
<th>Autoupdate Notes</th>
<th>Refer to Section:</th>
<th>For Centrally-Managed Devices</th>
</tr>
</thead>
</table>
| Windows  | • Update manually (autoupdate not currently supported).  
           • Requires update permissions at the operating system level. | 3.3 Installing Secure Browser on Windows Devices  
3.5 Network Installation for Windows (Network Administrators) | |
| Mac      | • Update manually (autoupdate not currently supported).  
           • Requires update permissions at the operating system level. | 3.6 Installing Secure Browser for Mac OS X  
3.6.6 Network Installation Information for Mac OS X | |
### 3.2 Chromebook Installation

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

**NOTES:**

- 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/.

- Secure Browser for Chromebook automatically updates to the latest version. If auto-update is disabled, update via the app store.

#### 3.2.1 Managed Chromebook Installation Procedure

1. Set up a free Google Apps for Education account and enroll all managed Chromebooks.

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.
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 "ecbhjmmfmlnoiahdachhilojbjdijp" 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.

3.2.2 Non-managed Chromebook Installation Procedure

NOTES:

- 2017 and newer Chromebooks require Google managed installation and a Chrome Enterprise or Chrome Education kiosk device management license to run in Kiosk mode. A one-time fee per device applies. Refer to https://support.google.com/chrome/a/answer/7613772 for more information.
- Google does not support kiosk mode for non-managed 2017 and newer Chromebooks. Refer to https://support.google.com/chromebook/answer/3134673?hl=en for more information.

1. Log in to the “Staff/Admin Google” user with the Chromebook owner account.
2. Open a Google Chrome web browser.
4. Click in the address bar to highlight the entire URL.
5. Press Ctrl + C to copy the URL to the clipboard
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.
13. Click the Done button to close the browser window.

NOTES:

- To launch the Secure Browser, click the Apps link, and select the STAAR Online Testing Program application.
- The STAAR Online Testing Platform cannot detect or shut down certain operating system accessibility features. Using these operating system features provides an unapproved accommodation that may affect the validity of an assessment. Please refer to the list of unapproved accessibility features for Chromebook and how to disable them below.

3.2.3 Disabling ChromeVox

ChromeVox is the built-in screen reader for Chrome OS. Students may have turned this feature on while using the Chromebook for instructional purposes. ChromeVox reads everything on the screen to the user, providing an accommodation that students should not have during testing. Visit http://www.chromevox.com/ for more information about ChromeVox.

Follow these steps to disable ChromeVox.

1. Toggle ChromeVox on and off with the keyboard shortcut, Ctrl + Alt + Z.

OR

1. Click the account photo.
2. Click Settings.
3. Click Advanced.
4. In the "Accessibility" section, click Manage accessibility features.
5. Under Text-to-Speech, set the screen reader to off.
3.2.4 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**.

3.3 Installing Secure Browser on Windows Devices

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.
- Due to updates required for added accessibility and language support in Spring 2019 administrations, autoupdate features are currently disabled for Windows devices.
- Before installing a new version of Secure Browser, uninstall Secure Browser before installing the current version. Refer to Section 3.3.3 Manually Uninstalling Secure Browser for directions.

### 3.3.1 Manually Install .msi Package with User Interface

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

2. Under STAAR Online Testing Platform Secure Browsers, click the For Windows® link.
3. Click the `securebrowser.msi` file.
4. Select the `Secure Browser Windows.msi` icon located in the downloads folder.
5. Follow all the application installation directions in the **STAAR Online Testing Setup** installation wizard.
6. Once the installation is complete, click **Finish**.
7. Launch the Secure Browser by double-clicking the icon on the desktop or via the Windows **Start** button on the taskbar.

### 3.3.2 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**

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

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

**Uninstallation Script**

```bash
msiexec /X <Source> /quiet
```

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

### 3.3.3 Manually Uninstalling Secure Browser

Follow the steps below to uninstall the previous Secure Browser.

1. Right-click the Windows **Start button** in the taskbar, open **Settings**, then click **Apps & Features**.
2. On the **Apps & Features** page, under “Apps & Features,” use the **Search this list** search box or scroll down to find **STAAR Online Testing Program**.
3. Click **STAAR Online Testing Program**, then click **Uninstall** to open the Uninstall Wizard.
4. Click **Next**, click **Yes**, then click **OK** to complete the uninstall process.
3.4 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.

3.4.1 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.
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.

3.4.2 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 gedit 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.

3.4.3 Disabling Fast User Switching in Windows 10

Method A: Access the Group Policy Editor

1. Right-click the Windows Start button in the taskbar, then click Run.

2. In the Search text box, type “gpedit.msc” and click OK.

3. In the Local Group Policy Editor window, open Administrative Templates under Local Computer Policy > Computer Configuration, System, and Logon.

4. Click Hide entry points for Fast User Switching.

5. Click the Edit policy setting link in the left pane.

6. In the Hide entry points for Fast User Switching window, set Hide entry points to “Enabled.”

7. Click OK to save the setting and close the Fast User Switching properties window.

8. Close the Local Group Policy Editor window.

Method B: Access the Registry

1. Right-click the Windows Start button in the taskbar, then click Run.

2. In the Search text box, type “regedit.exe” and click OK.

3. In the Registry Editor window, open HKEY_LOCAL_MACHINE, SOFTWARE, Microsoft, Windows, CurrentVersion, Policies, and Open System.

4. Right-click in the left pane of the System folder.
5. Click DWORD (32-bit) value under New > Key.

6. In the New Value #1 textbox, type “HideFastUserSwitching” and press Enter.

7. In the Edit DWORD (32-bit) Value window, Type “1” into the Value data textbox and click OK.

8. Close the Registry Editor window.

NOTE: To force an exit of the Secure Browser before the test completes, enter Shift + Esc + E.

3.5 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.

3.5.1 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.

3.5.2 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

3.5.3 Windows 7 Update Secure Browser Issues

Running Secure Browser on Windows 7 requires installation of a specific Windows update to allow the same Secure Browser installer to work on all supported versions of Windows. If the error message "The procedure entry point ucrtbase.terminate could not be located in the dynamic link library" appears when launching Secure Browser, install this update. Installing the "Update for Universal C Runtime in Windows" resolves the issue and allows Secure Browser to run properly. For more details refer to https://support.microsoft.com/en-us/help/2999226/update-for-universal-c-runtime-in-windows.

Follow these steps to install the “Update for Universal C Runtime in Windows.”

Install the Update via Windows Update

2. Follow the on-screen directions for your operating system.

Install the Update Manually

2. Scroll down to Method 2: Microsoft Download Center under How to Obtain this Update.
3. Locate and download your operating system from the table of updates.
4. Follow the on-screen directions to install the update.

3.6 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.

NOTES:

- Due to updates required for added accessibility and language support in Spring 2019 administrations, autoupdate features are currently disabled for devices running Mac OS.

- For devices running Mac OS X versions 10.14 and above, districts should plan to deploy the Secure Browser using device management software which is also preferred for Mac OS X versions beginning with 10.13.4. Refer to the table below and Section 3.6.6 Managing Apple Devices using Server Administration Software for details.

- Before installing a new version on a device where Secure Browser is already installed, uninstall the previous version. Refer to Section 3.6.3 Uninstalling the Mac OS X Secure Browser for directions.

- Mac OS X includes the native VoiceOver screen reader which students could attempt to use during testing. VoiceOver should be disabled during testing. Refer to Section 3.6.2 for specific instructions. Visit https://support.apple.com/accessibility/mac for more information regarding management of accessibility features.

The table below describes deployment methods based on OS X versions.

<table>
<thead>
<tr>
<th>OS X Version</th>
<th>Preferred Method</th>
<th>Alternate Methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.13.4 and newer</td>
<td>Device Management Software. Refer to Section 3.6.6.</td>
<td>1. Adding Secure Browser as a Trusted Application in system preferences. Refer to Section 3.6.7 for directions. 2. Assessment User Account login. Refer to Section 3.6.8 for directions.</td>
</tr>
<tr>
<td>10.11 - 10.13.3</td>
<td>Assessment User Account. Refer to Section 3.6.8.</td>
<td>1. Adding Secure Browser as a Trusted Application in system preferences. Refer to Section 3.6.7 for directions. 2. Assessment User Account login. Refer to Section 3.6.8 for directions.</td>
</tr>
</tbody>
</table>

1. Open a browser and navigate to http://www.texasassessment.com/technology/.
2. Under STAAR Online Testing Platform Secure Browsers, click on For MacOS (.dmg) or For Mac OS (.pkg) link and click OK in the popup window.
3. Select the securebrowswer.dmg icon located on the desktop or in the downloads folder.
4. Double-click the SecureBrowser app icon in the pop-up window.
5. When the pop-up displays, “STAAROnlineTesting-3.8.0.app is an application downloaded from the Internet. Are you sure you want to open it?” click the Open button.

6. In the next pop-up window, enter the password and click OK.

7. In the Setup window, 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. Click Next in the confirmation window.

11. When the installation completes, click Finish in the Setup window.

12. Launch Secure Browser by double-clicking the Secure Browser icon on the desktop or the STAAROnlineTesting.app in the . . . Applications/STAAR Online Testing Program folder.

3.6.1 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.

3.6.2 Disabling VoiceOver on Mac OS Computers

The STAAR Online Testing Platform cannot detect or shut down certain operating system accessibility features. Using these operating system features provides an unapproved accommodation that may
affect the validity of an assessment. Please refer to the list of unapproved accessibility features for Mac OS X and how to disable them below.

Students could attempt to use the Mac OS X native VoiceOver screen reader during testing. VoiceOver should be disabled prior to testing.

Follow these steps to disable the native VoiceOver screen reader on Mac OS computers prior to testing.

**Mac OS X 10.12.6 and later:**

1. Toggle VoiceOver on and off with the keyboard shortcut, `Command + F5`.

**Mac OS X prior to 10.12.6:**

1. Navigate to Apple, then select `System Preferences`.
2. Click the `Accessibility` icon, then select `VoiceOver`.
3. Uncheck the `Enable VoiceOver` checkbox.

### 3.6.3 Uninstalling the Mac OS X Secure Browser

If the Secure Browser application was installed using the .pkg file, deleting the `/Applications/STAAR Online Testing Program/` folder also uninstalls the application.

If the Secure Browser application was installed using the .dmg file, follow these steps to uninstall the Secure Browser.

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

### 3.6.4 Uninstall/Reinstall the Mac OS X Secure Browser

If the Secure Browser application was installed using the .pkg file, deleting the `/Applications/STAAR Online Testing Program/` folder also uninstalls the application.

If the Secure Browser application was installed using the .dmg file, 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` folder, and then locate and 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. Under STAAR Online Testing Platform Secure Browsers, click on the For MacOS (.dmg) or For Mac OS (.pkg) link and click OK in the popup window.
3. Select the `securebrowswer.dmg` icon located on the desktop or in the downloads folder.
4. Double-click the `SecureBrowser` app icon in the pop-up window.
5. When the pop-up displays, "STAAROnlineTesting-3.8.0.app" is an application downloaded from the Internet. Are you sure you want to open it?" click the `Open` button.
6. In the next pop-up window, enter the password and click `OK`.
7. In the Setup window, 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. Click `Next` in the confirmation window.
11. When the installation completes, click `Finish` in the Setup window.
12. Launch Secure Browser by double-clicking the Secure Browser icon on the desktop or the STAAROnlineTesting.app in the . . . Applications/STAAR Online Testing Program folder.

### 3.6.5 Installation Information for Mac OS X

The appropriate Secure Browser must be installed on each computer used for online testing. While it is strongly recommended to install the Secure Browser on each individual computer, the browser can also be pushed out to all computers through a network by copying browser files from the network to individual computers or by using third-party installation programs. For an example and instructions, refer to Section 3.6.7: Managing Apple Devices using Server Administration Software. For more information about network software distribution with Apple Remote Desktop, refer to https://www.apple.com/remotedesktop/softwaredistribution.html.

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.

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.

3.6.6 Managing Apple Devices using Server Administration Software

The Secure Browser may be installed and managed using third-party device management software. There are many options including Apple School Manager at https://school.apple.com/. As one example, the directions in this section outline how to use Simple MDM Server, which is similar to other mobile device management software solutions. For more information about MDM Server, refer to https://simplemdm.com.

NOTE: Deploying the Secure Browser using device management software is required or preferred for later versions of Mac OS X.

Follow these directions to enroll and manage Mac OS and iOS devices over your network using MDM Server.

**Step 1: Create an MDM Server account.**

1. Navigate to https://simplemdm.com and click the Try for Free button.

2. Click a Start Trial button, complete the fields on the sign-up form, and click the Get Started! button.

3. Follow the on-screen directions on the Let’s pair with Apple page to create a new push certificate.

4. On the Apple Push Certificates Portal page, click the Download button to download and save the certificate.

5. Return to the Let’s pair with Apple page and follow the directions to upload the push certificate file.

**Step 2: Enroll devices.**

1. Scroll through and read the informational screens that appear on the Simple MDM Devices page.

2. Click the green Enroll Devices button.

3. On the Enroll a Device page, click the Show Enrollment button under Group Enrollment to enroll devices as a group or click the Create Enrollment button to enroll devices singly.

4. Follow the on-screen directions to enroll all testing devices.

5. To verify that device profiles are installed, select Configs in the menu on the left of the page, then click Profiles to view the profiles list.
Section 3: Secure Browser

Step 3: Add a profile.

1. In the left menu, select **Configs**, then **Profiles**.
2. On the **Profiles** page, click the **Add Profile** button and select **Custom Configuration Profile** from the list.
3. Enter a profile name (for example - STAARApp.mobileconfig) and upload the .mobileconfig file at https://tx-tss.caltesting.org/installers/sb/macos/STAARApp.mobileconfig.
   - After uploading the file, it appears in the profiles list.

Step 4: Deploy a profile to group devices.

1. In the left menu, select **Devices**, then **Groups**, then choose the **Default** group from the list.
2. (Optional) to change the group name, click the **Settings** tab and enter a new name in the **Group Name** field.
3. On the **Profiles** page, select the profile added previously and click the **Save** button.
   - The device profile is added to all devices enrolled in the group.

Step 5: Install apps on devices

1. In Simple MDM, from the left menu, select **Apps**, then **Catalog**.
2. Click the **Add App** button to the right and select **macOS Package**.
3. Drag and drop or click an upload link to add the STAAROnlineTesting.pkg file.
4. Click the **Done** button.
   - The app appears in the app catalog.
5. In the left menu, click **Assignment** under **Apps**.
6. Complete the fields in the **Apps**, and **Devices > add device group and add device** and click the **Install Apps** button.
   - Apps are normally pushed to and installed on managed devices within 45 minutes.

3.6.7 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. In System Preferences select Security & Privacy settings.

2. In Security and Privacy settings, select Accessibility > Privacy Tab

3. Click the Lock icon in the bottom-left to allow changes.

4. Click the “+” Button to add the STAAROnlineTesting applications from /Applications/STAAR Online Testing Program/ to the list of trusted applications.

5. Check the checkbox next to STAAROnlineTesting.
6. Click the Lock icon again 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, “The application requires secure environment. Contact your Test Center Administrator.”

### 3.6.8 Launching Secure Browser with the Assessment User Account

When Secure Browser is installed on OS X 10.11 and 10.12, districts need to use a special assessment user log in, "STAAR Online Testing Program," before logging in testers. Refer to Section for information about preferred methods for deploying Secure Browser on devices running Mac OS versions 10.13.4 and above.

Follow these steps to run the Secure Browser and test on devices running Mac OS X 10.11 and 10.12.

1. Install the Secure Browser. Refer to [Section 3.6 Installing Secure Browser for Mac OS X](#) for directions.
2. Open the Secure Browser and log out.
3. Log in with the Username "STAAR Online Testing Program"
   - No Password is required.
4. Secure Browser launches and allows testers to enter a login from a test ticket and test normally.

### 3.6.8.1 Creating an Assessment User Account Password

Some systems running Mac OS 10.14 or 10.14.1 may request a password. Follow these steps to set up a password for the Assessment User account.
Option 1: Setup a password manually for the STAAR Online Testing user account from any Admin account.

1. Select the STAAR Online Testing or any other Admin account in the Users & Groups dialog.

2. Enter a password in the New password: and Verify: fields. (Example: STAAROnlineTesting.)

Option 2: Set the password programmatically.

1. Use the Run command on each device or use the MDM server to distribute the following script:

   ```shell
   sudo /usr/bin/dscl . -passwd /Users/STAAROnlineTesting "STAAROnlineTesting"
   ```

NOTES:

- Some pop-up messages may appear when the Secure Browser launches. Users may safely ignore these system messages.
- Logging in with the Username “STAAR Online Testing Program” is available on all supported OS X versions (10.11, 10.12, 10.13, and 10.14).
- For Mac OS X versions 10.13.4 and above, districts should consider deploying the Secure Browser using device management software. This is the Apple preferred method. Refer to Section 3.6.7: Managing Apple Devices using Server Administration Software for more information.

3.7 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/.
NOTES:

- Secure Browser for iOS automatically updates to the latest version. If auto-update is disabled, update via the app store.
- iOS devices include many accessibility features that students may attempt to use during instruction. Turn off all disallowed features during testing. Refer to Section 3.7.1 below for specific instructions. Visit https://support.apple.com/en-us/HT204390 for more information regarding management of accessibility features.

3.7.1 Disabling iOS Accessibility Features

The STAAR Online Testing Platform cannot detect or shut down certain operating system accessibility features. Using these operating system features provides an unapproved accommodation that may affect the validity of an assessment. Please refer to the list of unapproved accessibility features and how to disable them below.

Current accessibility features that should be disabled before using as a testing device include: VoiceOver, Zoom, Display Accommodations, Speak Screen, Highlight Content, Typing Feedback, Switch Control, AssistiveTouch, Touch Accommodations, Shake to Undo, Mono Audio, and Audio Volume Balance.

Follow these steps to disable accessibility features during testing.

1. Open Settings.
2. Navigate to General > Accessibility.
3. Check that the accessibility options listed above are disabled.

3.7.2 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 “Texas STAAR.”
2. Select the Texas STAAR Online Testing Program app.
3. Tap the download icon to download and install the app.
4. Click Update if the window appears.
5. The app will download to the iPad Home screen.

3.7.3 Automatic Assessment Mode for iOS

Section 3: Secure Browser

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.

3.7.4 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.

3.8 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 or Ubuntu) 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/.

<table>
<thead>
<tr>
<th>Minimum LCS System Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Memory</strong></td>
</tr>
<tr>
<td>4 GB RAM (8GB RAM recommended)</td>
</tr>
<tr>
<td><strong>CPU/Processor</strong></td>
</tr>
<tr>
<td>Mac: Intel x86 processor (32 or 64 bit)</td>
</tr>
<tr>
<td>Windows: Pentium 4 processor and above</td>
</tr>
<tr>
<td><strong>Disk Space</strong></td>
</tr>
<tr>
<td>15 - 30 GB free space</td>
</tr>
<tr>
<td><strong>File Permissions</strong></td>
</tr>
<tr>
<td>Full permissions to create or write to any files in the LCS installation folder.</td>
</tr>
<tr>
<td><strong>Operating System</strong></td>
</tr>
<tr>
<td>Microsoft Windows Server: 2008/R2 and 2012</td>
</tr>
<tr>
<td><strong>Web Browsers</strong></td>
</tr>
<tr>
<td>Chrome – Latest version</td>
</tr>
<tr>
<td>Firefox – Latest version and current Extended Support Release (ESR)</td>
</tr>
<tr>
<td>Internet Explorer – v9-11</td>
</tr>
</tbody>
</table>
4.4.2 Minimum Internet Connectivity and Security Requirements

<table>
<thead>
<tr>
<th>Minimum Internet Connectivity and Security Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Network</strong></td>
</tr>
<tr>
<td>All testing computers must be connected to the local area network (LAN).</td>
</tr>
<tr>
<td><strong>Connection</strong></td>
</tr>
<tr>
<td>LCS requires continuous Internet connectivity.</td>
</tr>
<tr>
<td><strong>Power Position</strong></td>
</tr>
<tr>
<td>LCS computer must remain on and must not be powered down or put in “sleep mode” during the test administration window.</td>
</tr>
<tr>
<td><strong>Connection Protocols</strong></td>
</tr>
<tr>
<td>Connections to the intranet using HTTP and HTTPS protocols.</td>
</tr>
</tbody>
</table>

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.
Follow these steps to create an LCS registration 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.
8. Check that Texas LCS is no longer listed in the Start menu.
9. 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:

```json
{
   "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.
Section 5: JAWS® and Refreshable Braille Displays

5.1 Testing Students with Visual Impairments

This section of the guide provides information about supported hardware, software, and supported version requirements and how to configure Job Access with Speech (JAWS®) to use in testing and with a refreshable braille display (RBD).

5.1.1 Technology Requirements

For information about complete requirements for online testing, refer to the Unified Minimum System Requirements for the Administration of Online Assessments document available online at https://www.texasassessment.com/administrators/technology/.

5.1.2 Supported Operating Systems and Related Requirements

For the 2018–2019 test administration, the following must be installed on computers used for braille testing.

NOTE: Districts may wish to add an embosser to print paper braille versions of items for students who use braille.

Supported Operating Systems and Related Requirements

<table>
<thead>
<tr>
<th></th>
<th>Student Computers</th>
<th>Administrator Computers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating Systems</td>
<td>Windows 7, 8.0–8.1, 10</td>
<td>Windows 7, 8.0–8.1, 10</td>
</tr>
<tr>
<td>Hardware</td>
<td>Refreshable Braille Display (RBD)</td>
<td></td>
</tr>
<tr>
<td>Software</td>
<td>Current Windows Secure Browser</td>
<td>Supported Web browser</td>
</tr>
<tr>
<td></td>
<td>Job Access with Speech (JAWS) Screen Reader 18 or other compatible screen reader.</td>
<td></td>
</tr>
</tbody>
</table>

NOTE: For security purposes, tablet and other touch devices are not supported for braille testing and should not be used. Use desktop or laptop computers only when testing with the braille accommodation.

5.1.3 Additional Resources:

- STAAR Assessments Home page — https://www.texasassessment.com/
- STAAR Assessment Management System log in — https://tx-toms.ets.org/
5.2 Refreshable Braille Displays

Visually impaired students use refreshable braille displays to read text and other output from a computer or other screen device. Refreshable braille displays are electromechanical devices that raise and lower sets of plastic or metal pins through braille cells lined up in a row (usually including 40, 70, or 80 cells). Refreshable braille displays work with screen reader software to represent text on the computer screen as braille patterns.

Depending on the screen reader output mode selected, the cells in a refreshable braille display may represent text on the same line the computer cursor is on (line mode), on what is currently being read aloud by the screen reader (speech output mode) or may include other information about what is displayed on-screen along with the text (structured or attribute mode). Most braille displays also include navigation keys and a braille keyboard.

40 Cell Refreshable Braille Display

5.2.1 Using Braille Displays in Assessment Testing

Braille displays are used in testing for deaf and blind students and to provide an additional mode of communication for other students with disabilities.

5.2.2 Secure Browser Screen Reader Compatibility

Although JAWS is used as an example screen reader application in this section, the Secure Browser is compatible with most screen readers and popular browsers running on any device and operating system.

JAWS is a Windows-only application and has some limitations in some browsers. For detailed requirements, refer to the Freedom Scientific System Requirements page at https://www.freedomscientific.com/Downloads/JAWS/jaws-system-requirements. For more information about JAWS or to download the software, refer to the Freedom Scientific Blindness Solutions Web page at https://support.freedomscientific.com/Downloads/JAWS/PreviousVersions.
5.2.2.1 Enabling JAWS 18 in the Secure Browser

Before the JAWS reader can run in the Secure Browser, users must change Secure Browser accessibility settings to allow JAWS to run during testing.

Follow these steps to enable JAWS to run in the Secure Browser.

1. Install the latest version of the Secure Browser. Refer to Section 3.3 Installing Secure Browser on Windows Devices for detailed directions.

2. Check that JAWS 18 for Windows is installed, licensed, and working on the test-taker’s device.

3. Click the **Start** button on the Windows taskbar.

4. Navigate to the STAAR Online Testing Program folder and click the STAAR Online Testing Program Preferences icon.

5. Click the **Yes** button in the “Do you want to allow this app . . . to make changes to your device?” dialog.
The Secure Browser Preferences dialog appears.

6. Click the **Accessibility** button.
7. Click a **Disabled** button to switch it to **Enabled**, then click the **Select** button.
8. Navigate to `C:\Program Files\Freedom Scientific\JAWS\18.0`, select the `jfw.exe` file, and click the **Open** button.

The enabled application address appears in the **Secure Browser Preferences** dialog.

9. Click the **Save** button.
5.2.3 Adding a Braille Display

Refreshable braille displays normally connect to computing devices by Bluetooth or by a USB cable and set up automatically once connected. Check the documentation for the device in use for any other setup requirements.

Braille displays normally work in concert with screen reader software like JAWS, NVDA, ORCA, VoiceOver, etc. and set up may require separate drivers and connections to the testing device by Bluetooth or USB. Refer to the documentation for the display in use for specific system and setup requirements.

5.2.4 Configuring the Screen Reader and Refreshable Braille Display

Several settings should be changed in the screen reader to set up a refreshable braille display for use in testing.

Most students use contracted braille, but younger or new braille learners may still use uncontracted braille with their refreshable braille display.

- **Output mode.** For testing, the mode should be set to “structured” since the student needs to know which region of each question and answer choice is being read to effectively navigate the item and answer choices.

- **Braille text display.** Test administrators or others monitoring testing may need to monitor student progress and where a student is on the screen via a braille text display.

- **Screen reader preferences.** Voice profile, speaking rate, punctuation, and other settings may be changed prior to administering assessments.

These features are set in the **Settings Center** in JAWS. Other screen readers typically have similar settings.

Follow these directions to change JAWS refreshable braille display settings.

1. Open JAWS and select **Settings Center** from the **Utilities** menu.

2. Select the browser in which the Secure Browser will appear (or select **Default (All Applications)**) from the **Application** drop-down list at the top of the Settings Center dialog.
3. In the left panel, expand **Braille** settings, then **General**, then select **Translation**.

4. In the **Translation** section, verify that **Language** is set to **English – United States**.

5. For students who prefer contracted braille, select **Unified English Braille Grade 2** from the **Output** and **Input** dropdowns. (For students who prefer uncontracted braille, select **Unified English Braille Grade 1**).

### JAWS Settings Center

![JAWS Settings Center](image)

6. Select **Structured** in the dropdown list under **Braille Mode**.

7. In the **Braille Mode** section, ensure that the following settings are checked.
   - Active cursor follows Braille display
   - Braille Cursor follows Active cursor
   - Enable Word Wrap
   - Auto Detect Braille Display using Bluetooth (if the display in use supports Bluetooth connection)

8. Make sure that **Display text in 8 Dot Braille Mode** (activates status dots) and **Enable Braille Sleep Mode** are **NOT** checked.

9. Click the **OK** button to save the settings.
5.2.5 Activating the Braille Viewer Display

Follow these steps to activate the braille viewer in JAWS.

1. Select the **Start menu** button.
2. Locate and select the **JAWS program** icon.
3. Select **More**, then select **Open File Location**.
4. In the File Explorer window, navigate to **Tools > Utilities**.
5. Select the **Braille Viewer** icon.
6. The JAWS Braille Viewer opens at the top of the screen.
7. To close Braille Viewer, select the **Exit** button.

5.2.6 Configuring the screen reader to Speak “Dollars”

Follow these steps to configure JAWS to correctly speak the dollar ($) symbol and dollar amounts following the symbol.

1. In the **JAWS Settings Center**, in the left panel, expand **Text Processing**.
2. Select **Speak Dollars**.
3. Check the **Speak Dollars** checkbox.
4. Click the **OK** button to save the settings.
5.2.7 Optional JAWS Voice Adjustment Settings

JAWS voice settings may be adjusted for individual students based on their needs. Voice Profile, Speaking Rate, and Punctuation settings may be changed prior to administering assessments.

NOTE: Students should take one or more practice tests using JAWS to allow time for adjusting settings before live testing.

Follow these steps to adjust the voice settings for the JAWS screen reader.

1. Open JAWS and select Options from the top menu.
2. Select Voices and then Voice Adjustment. The Voice Adjustment interface opens.
Adjust Voice Profile
1. Select a profile from the Profile Name drop-down list.
2. Click the **Apply** button.

Adjust Voice Rate
1. Under Voice, drag the slider to the desired rate of speed.
2. Click the **Apply** button.

Adjust Punctuation Level
1. Under Voice, select None, Some, Most, or All from the Punctuation drop-down list.
2. Click the **Apply** button.
3. Click the **OK** button to save the settings.

5.2.8 Setting JAWS to Navigate by Custom Regions
Streamlined test items include custom regions that help users navigate through test content. The JAWS screen reader is set by default to read only some region announcements, not all.

Follow these steps to ensure the screen reader announces all custom regions.
1. In the JAWS Settings Center, in the left panel, expand Speech Verbosity.
2. Select Verbosity Level.
3. Click the “Beginner, Highest” (the default) radio button, if needed.
4. Click the **OK** button to save the setting.
5.3 Navigating a Test with JAWS and an RBD

Students taking tests using JAWS and a refreshable braille display access special item types (or types of questions and answer choices) that are optimized for use with braille accommodation. In these “streamlined” questions and answer choices, all of the elements are stacked in a single page. Streamlined questions and answer choices also include a limited set of Universal Tools, including the Zoom, Clear, Color, and Mark for Review tools.

5.3.1 Streamlined Questions and Answer Choices

Questions and answer choices used in testing using a screen reader and refreshable braille display are optimized for this testing mode. These items are “stacked,” so that all elements of the question and answer choices appear in a single column within a single frame to minimize the need for a student to navigate to a different frame or page to understand the question and answer choices. Streamlined question and answer choices also include custom regions to aid in navigation and comprehension.

When the screen reader begins reading the question and answer choices, the first thing the student hears is “Page has 9 regions.”

In “structured” mode, the screen reader speaks, and the refreshable braille display translates into braille, the added information about regions, along with the body text and alt-text, as it is scrolled-over and comes into focus on the page.
### Example Streamlined Passage, Questions, and Answer Choices*

**Electric Cars Are Not The Right Choice**

1. The electric car is sometimes praised as a "greener" option for transportation than a gasoline-fueled car. (2) But because the electric car does not emit the harmful pollutants that a traditional vehicle does, many people assume that it must be the cleaner choice. (3) But electric cars are not always better for the environment than gasoline-fueled cars. (4) And they have other drawbacks too. (5) The electric car is not what you should buy today.

2. As mentioned, the electric car's "zero emissions" or carbon dioxide, implying that this car does not pollute the environment. (7) But this claim is misleading, as the electricity used to power the car comes from solar power, wind turbines, or some other source of renewable energy. (8) If the electricity for the car comes from power plants that burn fossil fuels, then an electric car is creating pollution, too.

3. Furthermore, the plants that manufacture electric cars are putting high levels of carbon-dioxide pollutants into the environment. (10) The production of an electric car puts twice as much carbon dioxide into the atmosphere as the production of a conventional car. (11) Even the batteries used in electric cars are harmful to the environment. (12) The process of mining the materials used in these batteries requires use of rare-earth metals.

4. The electric car also has other disadvantages. (14) Because it has to be charged every 75 miles or so, it must be in close proximity to a charging station. (15) Furthermore, the batteries in an electric car weaken over time. (16) Eventually they allow a person to travel even fewer miles between charges. (17) And when the weather is bad, an electrical outage could make an electric car completely inoperable.

5. In spite of the electric car's potential to be the best vehicle to drive, but for now, it is not. (19) This could, of course, happen eventually, but we aren't there yet. (20) Scientists need to develop or use new sources of energy so that the manufacturing of electric cars can truly be green. (21) Communities need to build more charging stations so that drivers have plenty of opportunities to charge as needed. (22) And batteries with a longer range need to be developed so that drivers can travel longer distances without stopping. (23) Until these obstacles are overcome, electric cars are not the best choice for today's drivers.

---

* Prototype image. Layout and design of actual passages, questions, and answers choices may differ.
5.3.2 Reading Passages

Test questions may ask about certain sentences or paragraphs in a reading passage. When a student first encounters a reading passage, sentence and paragraph number and highlight announcements are turned off to make it easier to read. Students may need to reference paragraphs, sentences, or highlighted text to choose the correct answer.

Follow these directions to activate paragraph and sentence numbering and highlighted text announcements.

1. Click the Turn Sentence Numbers On or Turn Paragraph Numbers On button in the Passage Announcements toolbar.

2. Click the Turn Highlights On button on the same toolbar.

3. Click the Show/Hide Sentence button (►) located at the end of the question region to reveal any sentences from the reading passage discussed in the question.

5.4 Using the JAWS Reader

The JAWS screen reader responds to hundreds of keyboard commands. Refer to Appendix C for a list of basic commands students are likely to use during testing. A complete keystroke reference and additional information is also available on the Freedom Scientific website: https://doccenter.freedomscientific.com/doccenter/archives/training/jawskeystrokes.htm.

5.5 Refreshable Braille Display – Test Administrator Guide

These guidelines and the device manuals will help test administrators and their students testing using the refreshable braille display.

5.5.1 Navigating Items Optimized for Refreshable Braille Display users

Students should be familiar with and have some experience using JAWS and the refreshable braille display device before attempting to use these technologies in testing.

NOTE: After logging in, specific navigation directions (as provided in Appendix C) are available to students online prior to beginning a test.

5.5.1.1 Settings

The settings described in Section 5.3.4 Configuring a Screen Reader and Refreshable Braille Display must be set prior to beginning a test for braille features to work as expected.

NOTES:

- Braille mode may be set to contracted, uncontracted, or structured depending on student preference. Note that some items (e.g. spelling questions in braille regions) may require switching modes temporarily.
Status cells should be turned on during testing since some items (e.g. writing items) include buttons or other elements indicated by status cells.

5.5.1.2 Terms and Additional Notes

The terms and notes below describe important information to assist in administering a braille test using refreshable braille display. This includes some instances when JAWS or refreshable display behaviors vary from what is expected. When necessary, a test administrator may need to provide information to the student about the refreshable braille display or JAWS navigation. Prior to the administration, inform the student, "If at any time during the test you have questions about how to move around a question and answer choices, notify your test administrator."

Please contact TEA with any questions about how to offer additional supports to students using JAWS.

Braille booklets. Braille booklets will be available as a supplement for the tests. Students will be advised when a question has a figure or a table represented by a tactile graphic in the braille booklet. On the practice test, the content advising that a tactile is available is present in the questions so that students will become familiar with how that information is conveyed. However, there is not a braille supplement for the practice test.

Entering, loading, pausing, exiting, or submitting the test. The test administrator may need to assist the student during the process of entering, loading, pausing, exiting, or submitting the test.

Page titles. In some cases, the title of a page that is presented to the screen reader may not correspond to the title that is visually presented.

Zoom tool. When a student navigates through the Zoom dialog using the Tab key, tabbing past the last stop takes the student out of the Tool dialog and gives focus to the first tab stop in the content on the page. Test administrators should advise students who use the Zoom tool that this may occur and provide assistance helping them return to the Zoom dialog as needed.

Color tool. Focus retention in this menu can be lost once the student tabs out of the menu. When a student navigates through the Color dialog using the Tab key, tabbing past the last stop takes the student out of the Tool dialog and gives focus to the first tab stop in the content on the page. Test administrators should advise students who use the Color tool that this may occur and provide assistance in helping them return to the Color dialog as needed.

Introductory links. On the JAWS Help screen, pressing Insert+Enter keys may not result in skipping links.

Streamlined navigation:

- When moving from the navigation toolbar or moving to a new screen, JAWS automatically begins reading all region names. Press CTRL+Home or Q to stop JAWS and move it to the top of the current screen.

- Commonly used navigation shortcut keys, such as T for tables or G for graphics, move the student to the next instance of the element, which may be in the next question or in a later question.

- In some cases, the question number for the first question may not be visually present on screen.

Forms Mode. Certain functionalities may put a student into Forms mode accidentally (for example, after pausing and when toggling through Highlight regions). When students enter Forms mode (intentionally or...
accidentally), to return to Virtual PC Cursor mode and continue testing they should click the Escape (Esc) key.

**Space bar.** When entering a response to a written composition or multiple-choice item, students should be directed to use the space bar on the standard QWERTY keyboard ONLY. Using the RBD space bar to select answer choices may result in unexpected behavior.

**Enter.** Students should be instructed not to use the *Enter* key on the standard QWERTY keyboard when responding to items.

**Spacing:**

- In rare cases, spaces between words may be missing in the refreshable braille display and JAWS presentation of the content.
- In some cases, there will be an extra space presented in the braille display. This includes:
  - Dramas — Stage directions in dramas with highlights include an extra space after the characters’ names and before the highlight.
  - Writing Passages — There may be multiple spaces present between sentences in writing passages in the refreshable braille display.

**Passage toolbars:**

- After selecting a button in the *Passage Announcements* toolbar, or after selecting any other toolbar in a streamlined item, the JAWS reader switches to Forms mode. Select the *Esc* key to exit Forms mode and return to Browse mode. (Pressing the *down arrow* key does not return the user to Browse mode on this test.)
- The refreshable braille display and JAWS may lose focus when using the *down arrow* key to navigate past the toolbar. Test administrators may need to provide assistance.
- A button status may announce when using the *down arrow* key to move to the Navigation region.

**“Braille region” or “Braille-only region.”** The JAWS Orientation region will notify a student when he or she will encounter a region that does not allow the audio presentation of the content; these regions are only available via the refreshable braille display. This region will announce when a student enters a Braille region or Braille-only region but will not announce when a student has left a Braille region or Braille-only region. Test administrators will need to be aware of when a student is in Braille region or Braille-only region questions. At this time, test administrators should remove a student’s headphones when entering this region and then return them to the student when exiting this region.

**Highlighted text.** The JAWS Orientation region alerts students to when questions will be asked about highlighted text in a passage. If more than one question in a passage refers to the Highlight region, all of the highlights in the passage are activated. After the highlight toggle button is turned on, the student can navigate to the highlighted region and then must press the *down arrow* key to access the highlighted content. After pressing the *down arrow* key once, the student will encounter the Highlight region. Pressing the *down arrow* key a second time will take the student to the highlighted text, and pressing the *down arrow* key a third time will take the student to the Highlight region end. Highlights are not numbered, but each highlight in a passage is in its own Highlight region.
Section 5: JAWS® and Refreshable Braille Displays

Footnotes:

- When status cells are enabled on the refreshable braille display, JAWS may announce either “same” or “same page link” within the footnote text. JAWS will read footnote text even if the footnote is in a Braille region or Braille-only region.
- When more than one footnote is in a passage, JAWS may read all footnotes and additional page information at once.
- Students may require proctor assistance when navigating between footnotes and passages.

Copyrights. Copyrights may appear directly in the Figure region or in a Content Information region within a Figure region.

Commas. Commas may be announced by JAWS as “low single quote.”

Questions. A Your Selections region is provided in some questions to provide the student with additional context.

- Most questions in the writing sections of English I, English II, Grade 4 Writing, and Grade 7 Writing tests have a Your Selections region. For these tests, the JAWS Orientation region will advise when a Your Selections region is not available.
- Most questions in the grades 3–8 reading tests will not have a Your Selections region. For these tests, the JAWS orientation region will advise when a Your Selections region is available.

Dictionary questions:

- Phonetic spellings present in dictionary questions are presented as “pronunciation spelling” for all grades.
- JAWS will announce unseen information by voicing “figure” and “figure end” for all grades. Students should be advised that a graphic is not actually present.

Spelling questions. Spelling questions are presented in Braille regions or Braille-only regions. In contracted braille mode, pressing the refreshable braille chord (1-2-4-5-7+spacebar) allows the student to toggle between the three braille modes: structured, contracted, and uncontracted braille. The student may experience spelling words in uncontracted mode then switch back to contracted or structured mode as needed. Students should refer to the braille booklet if additional support is needed for these questions.

Block quotes. Block quotes that end within a question reference region may be followed by an em-dash character.

Quotation marks. In some cases, when JAWS encounters text within quotation marks, students may have to access the content by pressing the down arrow several times to move through the content.

Tables. Titles for tables appear as headings and not as captions.

Blanks. Some questions have blank(s) for the student to complete by selecting an answer choice. The blank(s) appear as “[blank]” in the refreshable braille display, are announced as “[blank]” by JAWS, and appear as a question mark “?” in the braille booklet.
Written composition:

- Content that appears visually as headers in "Written Composition" questions will not be identified as headers by JAWS.
- Questions in “Written Composition” questions do not appear in a question region.

Response for Written Composition. It is recommended for a student to use a QWERTY keyboard to enter a response. If students use a braille keyboard to enter a response, it is recommended that a student carefully review their content to ensure the response was entered appropriately.
# Appendix A: URLs

<table>
<thead>
<tr>
<th>Site</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Portal</td>
<td><a href="http://www.texasassessment.com/">http://www.texasassessment.com/</a></td>
</tr>
<tr>
<td>STAAR Assessment Management System</td>
<td><a href="https://tx-toms.ets.org/">https://tx-toms.ets.org/</a></td>
</tr>
<tr>
<td>Online Testing (for configuration use only)</td>
<td><a href="https://tx-tss.caltesting.org/">https://tx-tss.caltesting.org/</a></td>
</tr>
<tr>
<td>Technology Systems and Supports</td>
<td><a href="https://www.texasassessment.com/technology/">https://www.texasassessment.com/technology/</a></td>
</tr>
</tbody>
</table>

**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

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

The tables below include basic keyboard commands students are likely to use during testing. A complete keystroke reference and additional information is also available on the Freedom Scientific website: https://doccenter.freedomscientific.com/doccenter/archives/training/jawskeystrokes.htm.

## General Navigation

### General Navigation Commands

<table>
<thead>
<tr>
<th>Keyboard Command</th>
<th>Go to . . .</th>
</tr>
</thead>
<tbody>
<tr>
<td>Down Arrow</td>
<td>. . . next line.</td>
</tr>
<tr>
<td>Up Arrow</td>
<td>. . . previous line.</td>
</tr>
<tr>
<td>Ctrl+Down Arrow</td>
<td>. . . next content block.</td>
</tr>
<tr>
<td>Ctrl+Up Arrow</td>
<td>. . . previous content block.</td>
</tr>
</tbody>
</table>

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Tab</td>
<td>. . . next control (button, checkbox, etc.)</td>
</tr>
<tr>
<td>Shift+Tab</td>
<td>. . . previous control.</td>
</tr>
</tbody>
</table>

## Navigating by Text Content

### Text Navigation Commands

<table>
<thead>
<tr>
<th>Keyboard Command</th>
<th>Go to . . .</th>
</tr>
</thead>
<tbody>
<tr>
<td>Right Arrow</td>
<td>. . . next character.</td>
</tr>
<tr>
<td>Left Arrow</td>
<td>. . . previous character.</td>
</tr>
<tr>
<td>Ctrl+Right Arrow</td>
<td>. . . next word.</td>
</tr>
<tr>
<td>Ctrl+Left Arrow</td>
<td>. . . previous word.</td>
</tr>
</tbody>
</table>

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Home</td>
<td>. . . beginning of the current line.</td>
</tr>
<tr>
<td>End</td>
<td>. . . end of the current line.</td>
</tr>
<tr>
<td>Ctrl+Down Arrow (or P)</td>
<td>. . . next content block or paragraph.</td>
</tr>
<tr>
<td>Ctrl+Up Arrow (or Shift+ P)</td>
<td>. . . previous content block or paragraph.</td>
</tr>
</tbody>
</table>

## Navigating by Headings

### Headings Navigation Commands

<table>
<thead>
<tr>
<th>Keyboard Command</th>
<th>Go to . . .</th>
</tr>
</thead>
<tbody>
<tr>
<td>H</td>
<td>. . . next heading.</td>
</tr>
</tbody>
</table>

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Shift+H</td>
<td>. . . previous heading.</td>
</tr>
</tbody>
</table>
Navigating by Regions

Regions Navigation Commands

<table>
<thead>
<tr>
<th>Keyboard Command</th>
<th>Go to . . .</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q</td>
<td>. . . &quot;main&quot; region.</td>
</tr>
<tr>
<td>R</td>
<td>. . . next region.</td>
</tr>
<tr>
<td>Shift+R</td>
<td>. . . previous region</td>
</tr>
<tr>
<td>JAWS Key+Ctrl+R</td>
<td>. . . a list of regions (arrow up or down and press Enter to navigate to the region)</td>
</tr>
</tbody>
</table>

Navigating Controls

Students may encounter several HTML controls while testing, including radio buttons, checkboxes, and buttons.

List Controls on the Current Page

Follow these steps to view, navigate, and operate form controls.

1. To view a list of all controls on any web page, press JAWSKey+F5 (INS+F5).
2. Use the up and down arrow keys to navigate the list.
3. Click the ENTER key to navigate to the selected control.

Radio Buttons

Follow these directions to navigate to, select, and de-select radio buttons in JAWS Browse mode, use these commands:

<table>
<thead>
<tr>
<th>Keyboard Command</th>
<th>Go to . . .</th>
</tr>
</thead>
<tbody>
<tr>
<td>A or Tab+Down Arrow</td>
<td>. . . next radio button.</td>
</tr>
<tr>
<td>Shift+A or Shift+Tab+Up Arrow</td>
<td>. . . previous radio button.</td>
</tr>
<tr>
<td>Spacebar</td>
<td>. . . select or deselect radio button.</td>
</tr>
</tbody>
</table>

In JAWS Forms mode, use these commands:

<table>
<thead>
<tr>
<th>Keyboard Command</th>
<th>Go to and select . . .</th>
</tr>
</thead>
<tbody>
<tr>
<td>Down Arrow</td>
<td>. . . next radio button.</td>
</tr>
<tr>
<td>Up Arrow</td>
<td>. . . previous radio button.</td>
</tr>
</tbody>
</table>

NOTES:

- Using the spacebar to select a radio button option while in forms mode may result in an incomplete selection.
- To leave forms mode and return to browse mode, press the + key twice.
### Checkboxes

Follow these directions to navigate to, select, and de-select checkboxes.

<table>
<thead>
<tr>
<th>Keyboard Command</th>
<th>Go to . . .</th>
</tr>
</thead>
<tbody>
<tr>
<td>X or Tab</td>
<td>. . . next checkbox.</td>
</tr>
<tr>
<td>Shift+X or Shift+Tab</td>
<td>. . . previous checkbox.</td>
</tr>
<tr>
<td>Spacebar or Enter</td>
<td>. . . select or deselect checkbox.</td>
</tr>
</tbody>
</table>

### Buttons

Follow these directions to navigate to, select, and de-select buttons.

<table>
<thead>
<tr>
<th>Keyboard Command</th>
<th>Go to . . .</th>
</tr>
</thead>
<tbody>
<tr>
<td>B</td>
<td>. . . next button.</td>
</tr>
<tr>
<td>Shift+B</td>
<td>. . . previous button.</td>
</tr>
<tr>
<td>Spacebar or Enter</td>
<td>. . . activate current button.</td>
</tr>
</tbody>
</table>
Index

A
Accessibility features
disabling on Chrome OS, 20
disabling on iOS, 36
disabling on Mac OS, 29
for students with visual impairments, 48
Acer Chromebook R11, 18
Apple Remote Desktop, 25, 30, 46
ASUS Chromebook Flip, 18
Automatic Assessment Mode, 36
Automatic update
disabling during testing window, 65
on Chrome OS devices, 18
on iOS devices, 35
on Windows, 21
Autoupdate feature. See Secure Browser

Chromebook (continued)
Google Pixel, 18
installation, 18
managed installation, 18
models excluded from stable channel, 18
OS releases, 18
pushing configurations to, 45
Secure Browser installation, 19
settings, 20
support for, 45
ChromeVox, disabling on Chrome OS, 20
Citrix XenDesktop, 15
Configurations
for the LCS computer, 42
imaging systems (do not use), 43
JAWS screen reader, 52, 53, 56
network, 13
Refreshable Braille Display output modes, 52, 53
Refreshable Braille Displays, 52, 53
test computers and devices, 44
troubleshooting, 43
content filters, 14

B
bandwidth
analyzing, 7
determining requirements, 8
estimate of in testing, 7
factors for determining need, 9
for X students testing, 7
forecasting needs for, 8
minimizing need for, 8
network diagnostics tools for, 8
relationship to test content, 9
braille, Braille Booklets availability, 60

C
 caching, and need for LCS, 38
Chrome OS, disabling ChromeVox, 20
Chromebook
  Acer R11, 18
  ASUS R11, 18
  blog, 18
  configuring, 45
  force quit, 21

E
e-mail server, 14
encryption in LCS, 41
encryption requirements, 9
error message, LCS, 40
F

Fast User Switching, disabling in Windows, 23
firewalls, 14
   URLs accessed through, 13
Force quit, Secure Browser, 21

G

Google Apps for Education, 18
   enrolling managed Chromebooks, 18
Google Chromebook Pixel, 18

H

hardware requirements, 16

I

Information Technology Staff Readiness Checklist, 65
installation
   LCS software, 41
   on Mac OS devices, 27
   on non-managed Chromebook devices, 19
   on Windows devices, 21
   Secure Browser, 9
   Windows network, 25
iOS
   automatic assessment mode, 36
   disabling accessibility features, 36
   installing Secure Browser on, 36
iPad
   automatic assessment mode, 36
   installing Secure Browser on, 35
   pushing LCS configurations to, 47
   support for, 47
Iperf, 12
IT Staff Readiness Checklist, 65

J

JAWS
   composing in MS Word with a RBD, 63
   configuring for use in testing, 52, 53
   custom regions navigation, 56
   directions for using during testing, 59
   enabling in Secure Browser, 50
   list of possible issues during testing
   blanks, 62
   block quotes, 62
   color and help tools (focus), 60
   commas, 62
   copyright information, 62
   footnotes, 62
   highlighted text, 61
   navigation, 60
   passage toolbar, 61
   quotation marks, 62
   spelling questions, 62
   stage directions, 61
   submitting test answers, 60
   table navigation, 61
   written composition items, 63
   Zoom tool, 60
   optional voice adjustment settings, 55
   settings for use with an RBD, 52
   technology requirements, 48
   testing with a Refreshable Braille Display, 48

K

kiosk mode, 37
kiosk settings for Chromebook, 20

L

LCS, 6, Refer to Local Caching Software
   accessing monitoring page, 44
   availability, 9
   benefits of using, 38
   configuring the LCS computer, 42
   determining need for, 12
   encryption, 41
   error message, 40
   illustration, 38
   installation and configuration, 39
   installing, 41
   installing for Mac OS, 42
   installing on Windows, 41
   LCS Monitoring Tool, 39
   LCS Monitoring Tool Checklist, 39
   Monitoring Tool, 44
   Monitoring Tool Checklist, 42
   operating requirements, 39
   platform component, 6
   registration, 39
   registration key, creating, 41
   security requirements, 40
LCS (continued)

system requirements, 39
uninstalling from Mac OS, 42
uninstalling from Windows, 41
updating and reinstalling, 40
when not needed, 38

Linux
configuring Secure Browser for, 47
installing Secure Browser on, 37
pushing configurations to, 47
support for, 47

Local Caching Software. refer to LCS

M

Mac
pushing LCS configurations to, 46
support for, 46

Mac OS
adding Secure Browser as a trusted application, 32
disabling Spaces, 28
disabling VoiceOver, 29
installing LCS on, 41
installing Secure Browser on a network, 30
OS X network specific tools, 12
Secure Browser installation, 27
uninstalling LCS from, 42
uninstalling Secure Browser, 29

managed Chromebooks. refer to Chromebooks

MIME types, 13
minimum days of testing, 11
minimum sessions per day, 11

MS Word
composing in using the JAWS reader and an RBD, 63
msi package, installing, 21

N

nComputing, 15
Netstat, 12
network
access point, 10
bandwidth standards, 10
bandwidth recommendations, 10
caching (disabling), 7
configurations, 7
connections requirements, 6

Network (continued)

content caching settings, 7
diagnostic testing tools provided, 7
diagnostic tools, 12
installing Secure Browser, 25
installing Secure Browser directory to client from, 25
IP Suite, 7
LAN performance, 7
LCS connections requirements, 6
packet prioritization, 7
protocols, 13
quality of service, 7
requirements, 6
security during testing, 14
session timeouts, 7
settings, 7
settings to limit interruptions, 7
STAAR Online Testing Platform performance, 7
timeouts, 7
traffic bottlenecks, solving, 7
traffic shaping, 7
whitelisting required URLs, 7

NSLookup, 12
NTtcp, 12

O

online readiness tools, 11

P

Passage Announcements toolbar, 61
PathPing, 12
performance requirements
virtual servers, 15
permissions, read/execute, read/write, 21
Ping, 12
platform, 6
components, 6
online readiness tools, 6
requirements, 6
protocols, network, 13
proxy servers, 14
PRTG Traffic Grapher, 12
Q

Quality of Service (QoS), 14

R

RBD. Refer to Refreshable Braille Display
Readiness Checklist, 65
Refreshable Braille Display
configuring for testing, 52, 53
connections and compatibility, 52
display output modes, 49
introduction, 49
list of possible issues during testing
blanks, 62
block quotes, 62
color and help tools (focus), 60
commas, 62
copyright information, 62
footnotes, 62
highlighted text, 61
navigation, 60
passage toolbars, 61
quotation marks, 62
spelling questions, 62
stage directions, 61
submitting test answers, 60
table navigation, 62
written composition items, 63
Zoom tool, 60
output mode settings during testing, 59
Proctor Guide, 59
status cells setting during testing, 59
technology requirements, 48
testing with, 48
using in assessment testing, 49
registering the LCS, 39
requirements
computers, 11
for online testing, 6
hardware, 16
Internet connection, 6

S

school capacity calculator, 11
maximum students, 11
minimum computers, 11
minimum required test days, 11
minimum test sessions, 11

School Capacity Calculator, System Check Test, 11
Screen Reader. Refer to JAWS
scripted installation, 21
Secure Browser, Preferences dialog, 51
Secure Browser, 17
accessibility preferences, 50
adding as a trusted application for Mac OS X, 32
automatic assessment mode, 36
autoupdate feature, 17
Chromebook installation, 18
enabling JAWS, 50
encryption, 9
features, 17
force quit, 21
installation, 9
installation on Mac OS, 27
installing on a Mac OS network, 30
installing on an iPad, 35
installing on Linux OS, 37
installing to a shared drive on Windows, 25
network installation, 25
Non-managed Chromebook installation, 19
platform component, 6
requirement for use, 17
uninstalling manually, 22
uninstalling on Mac OS, 29
viewing on higher resolution displays, 17
security configuration failure, 37
security during testing, 14
servers
email, 14
proxy, 14
virtual, 14
virtual, performance requirements, 15
virtual, security requirements, 15
single app mode, 37
Spaces, disabling on Mac OS, 28
Stable channel, Chromebooks excluded, 18
streamlined item accommodation
element, 58
introduction, 57
settings for questions with reading passages, 59
student capacity, 11
Support contact information, 6
system check test, 12
systems supported, 6
T
tactile graphic in Braille Booklets, 60
TCPDump, 12
testing, security, 14
Texas Assessment Support Center contact, 6
traceroute, 12
tracert, 12
troubleshooting
  Google Chromebook issues, 18, 36
  LCS configuration issues, 43
  LCS log file location, 44
  LCS version error message, 40
  slow network issues, 6, 8

U
updates to guide, 2
URLs
  accessed through firewall, 13
  list of, 64

V
virtualization, 15
  critical security and performance standards, 15
  guidelines, 14
  software, 15
visual impairments, students with
  example streamlined item, 58
  streamlined items accommodation, 57
  testing using JAWS and an RBD, 48
  universal tools, 57
VMWare, 15
VoiceOver, disabling on Mac OS, 29

W
Windows
  configuring for Secure Browser, 46
  disabling Fast User Switching, 23
  installing LCS on, 41
  installing Secure Browser manually, 21
  installing Secure Browser to a shared drive, 25
  network diagnostic tools, 12
  pushing configurations to, 46
  read/execute and read/write permissions, 21
  Secure Browser installation, 21
  support for, 46
  uninstalling LCS from, 41
  Windows runs Microsoft Edge in background, 21
WinDump, 12
wireless networking
  access points, 10
  transmission rates, 10
  workstations, recommended # of, 10
Wireshark, 12