Florida
Standards Assessments

TECHNOLOGY SETUP FOR ONLINE TESTING

AIR's Test Delivery System (TDS) has two components, the **Test Administrator (TA) Interface** and the **Student Interface**.

- Test administrators use the TA Interface to create and manage test sessions from a web browser.
- Students access and complete their tests through the Student Interface via the Secure Browser.

This document explains in 4 steps how to set up technology in your schools and district:

Step 1. Setting Up the Test Administrator Computer/Device
Step 2. Setting Up Student Computers/Devices
Step 3. Configuring Your Network for Online Testing
Step 4. Configuring Assistive Technologies

STEP 1: SETTING UP THE TEST ADMINISTRATOR COMPUTER/DEVICE

The TA Interface is a website and can be accessed through any approved and updated browser listed on the ***Supported Systems & Requirements*** page to administer a testing session.

If your school uses a firewall or other networking equipment that blocks access to public websites, you may need to whitelist AIR websites. For a list of websites you should whitelist, see the "Whitelisting Resources for Online Testing" section in the document titled *Configurations, Troubleshooting, and Secure Browser Installation* for your operating system.

TAs that wish to print test session information must be connected to a printer.

STEP 2: SETTING UP STUDENT COMPUTERS/DEVICES

For students to access online tests, each student computer/device needs AIR's Secure Browser installed. The Secure Browser is AIR's customized web browser designed to keep tests secure by locking down the student desktop and preventing the student from accessing anything except their test.

To get started setting up your student computers/devices, you should first make sure they meet minimum hardware requirements and supported operating systems as listed on the ***Supported Systems & Requirements*** page. Since some Operating Systems are updated more frequently, such as Chrome and iOS, please be sure to check this page for the most recent supported operating systems.

All supported computers, laptops, tablets, and approved testing devices must meet the following requirements:

Screen Dimensions
Screen dimensions must be 10" or larger (iPads with a 9.7" display are included).

Screen Resolution
All devices must meet the minimum resolution of **1024 x 768**. Larger resolutions can be applied as appropriate for the monitor or screen being used.

Keyboards
The use of external keyboards is highly recommended for tablets that will be used for testing.

Mice
Wired two- or three-button mice can be used on desktops or laptops. Mice on mobile devices are not supported. Mice with "browser back" buttons should not be used.

Headphones
Wired headphones with a 3.5mm connector or USB headphones are supported. Bluetooth headphones are not permitted.

Installing the Secure Browser

Once you have made sure your device is supported, you are ready to download and install the Secure Browser. This section explains where you can go to download the Secure Browser and how to install it.

The Secure Browser is available for the operating systems listed on the ***Supported Systems & Requirements*** page. You can download the Secure Browser and find installation instructions from the ***Secure Browser*** page on the FSA Portal.

If you are a Technology Coordinator and it is your responsibility to manage a large number of machines across your school or district, you can use the same tools you are already familiar with to push the Secure Browser out to all of your machines at scale. For example, the Secure Browser ships as an MSI package which enables use of MSIEXEC.

The Secure Browser is installed the same way as most other software. You will need to download a file, open that file, and follow prompts along the way to install the Secure Browser. If you are familiar with installing software, install the Secure Browser the same way.

For iPads, Android tablets, and Chromebooks, the AIRSecureTest app is AIR's mobile version of the Secure Browser. It is available in each app store to download and install. The first time you open this app, it will ask you to choose your state and assessment program. Your choice is saved and from then on, the Mobile Secure Browser works just like the desktop version, allowing you to access operational tests, practice tests, and the network diagnostic tool. You can also use any mobile device management utility to install the Secure Browser on multiple managed devices and configure those devices.

Windows 10 and Windows 10 in S Mode come with Microsoft's Take a Test app, which enforces a locked-down, secure testing environment identical to AIR's Secure Browser. Users of the Take a Test app do not need to install the AIR Secure Browser on the testing machine. Instructions for configuring

the Take a Test app can be found in *the Configurations, Troubleshooting, and Secure Browser Installation for Windows* document.

Additional installation instructions for Windows, Mac, Chrome OS, Android, or Linux (including instructions on how to install the Secure Browser on multiple devices) can be found in the following documents on the Secure Browser page tabs:

- *Configurations, Troubleshooting, and Secure Browser Installation for Windows*
- *Configurations, Troubleshooting, and Secure Browser Installation for Mac and iOS*
- *Configurations, Troubleshooting, and Secure Browser Installation for Linux*
- *Configurations, Troubleshooting, and Secure Browser Installation for Android*
- *Configurations, Troubleshooting, and Secure Browser Installation for Chrome OS*

Other Configurations

For all devices and operating systems, there are additional configurations necessary before secure testing can begin. Please refer to each individual installation guide located on the OS specific tab on *Secure Browser* page.

Several necessary configurations for Mac computers/devices are performed by installing the Mac Secure Profile.

STEP 3: CONFIGURING YOUR NETWORK FOR ONLINE TESTING

In this section, we provide some tools and recommendations to help configure your network for online testing. To ensure a smooth administration, AIR recommends network bandwidth of at least 20 kilobits per second for each student being concurrently tested.

Additionally, FDOE suggests that a guest WiFi network used for personal devices should be set up separately from the primary school WiFi network to ensure that bandwidth strength is optimal.

Whitelisting URLs, Configuring Filtering Systems, and Configuring Domain Name Resolution

Ensure your network's firewalls are open for these URLs. If your testing network includes devices that perform traffic shaping, packet prioritization, or Quality of Service, ensure these URLs have high priority.

If both internal and external filtering systems are used, the URLs must be whitelisted in both filters. Please see your vendor's documentation for specific instructions. Also, be sure to whitelist these URLs in any multilayer filtering system (such as local and global layers).

Additionally, ensure the devices used for testing have access to a server than can resolve the below domain names.

Testing servers and satellites may be added to modified during the school year to ensure an optimal

testing experience. As a result, AIR strongly encourages you to whitelist at the root level. This requires using a wildcard.

AIR URLs for Testing Sites	
System	**URL**
TA and Student Testing Sites Assessment Viewing Application (AVA)	*.airast.org *.tds.airast.org *.cloud1.tds.airast.org *.cloud2.tds.airast.org

AIR URLs for Non-Testing Sites	
System	**URL**
FSA Portal and Secure Browser Installation Files	FSAssessments.org
Single Sign-On System	sso2.airast.org/auth/realms/florida/account
Practice Tests	flpt.tds.airast.org
Test Information Distribution Engine	fl.tide.airast.org
FSA Reporting System	fsareports.airast.org

Required Ports and Protocols

Ensure that all content filters, firewalls, and proxy servers are open accordingly.

Ports and Protocols for the Test Delivery System	
Port/Protocol	**Purpose**
80/TCP	HTTP (initial connection only)
443/TCP	HTTPS (secure connection)

Configuring for Certificate Revocations

AIR's servers present certificates to the clients. The following section discusses the methods used to check those certificates for revocation. To use the Online Certificate Status Protocol (OCSP), ensure your firewalls allow the domain names listed the table below. The values in the Patterned column are preferred because they are more robust.

Domain Names for OCSP	
Patterned	**Fully Qualified**
*.thawte.com	oscp.thawte.com
*.geotrust.com	oscp.geotrust.com
*.ws.symantec.com	oscp.ws.symantec.com

If your firewall is configured to check only IP addresses, do the following:

1. Get the current list of OCSP IP addresses from Symantec. The list is available here.
2. Add the retrieved IP addresses to your firewall's whitelist. Do not replace any existing IP addresses.

Configuring Network Settings for Online Testing

Local Area Network (LAN) settings on testing machines should be set to automatically detect network settings.

To set LAN settings to auto-detect on Windows machines:

1. Open **Control Panel**.
2. Open **Internet Options**.
3. Click **Connections** tab.
4. Click **LAN Settings**.
5. Click the **Automatically detect settings** checkbox.
6. Click **OK** to close **Local Area Network (LAN) Settings** window.
7. Click **OK** to close **Internet Properties** window.

Proxy Servers

If your technology coordinator has set up a proxy server at your school, you may need to configure the Secure Browser's proxy settings. Proxy servers must be configured to not cache data received from servers.

Session timeouts on proxy servers and other devices should be set to values greater than the typically scheduled testing time. For example, if test sessions are scheduled for 60 minutes, consider session timeouts of 65–70 minutes.

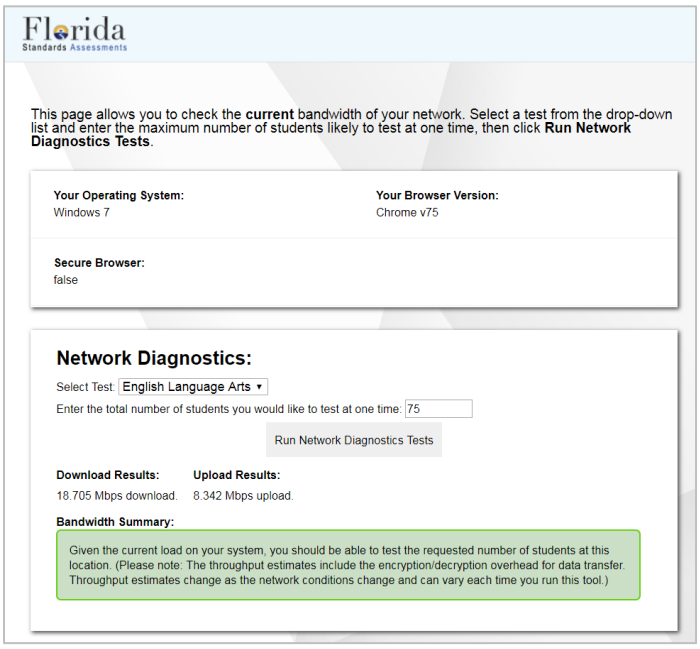
By default, the Secure Browser attempts to detect the settings for your network's web proxy server. However, users of web proxies should execute a proxy command once from the command prompt. This command does not need to be added to the Secure Browser shortcut. The table below lists the form of the command for different settings and operating systems. To execute these commands from the command line, change to the directory containing the Secure Browser's executable file.

Note the commands in the table on the next page use the domains foo.com and proxy.com. When configuring for a proxy server, use the actual testing domain names as listed in the above table AIR URLs for Testing Sites.

Specifying Proxy Settings Using the Command Line		
Description	**System**	**Command**
Use the browser without any proxy	Windows	FSASecureBrowser.exe -proxy 0 aHR0cHM6Ly9mbC50ZHMuYWIyYXN0Lm9yZy9zdHVkZW50Lw==
	Mac	./FSASecureBrowser -proxy 0 aHR0cHM6Ly9mbC50ZHMuYWIyYXN0Lm9yZy9zdHVkZW50Lw==
	Linux	./FSASecureBrowser.sh -proxy 0 aHR0cHM6Ly9mbC50ZHMuYWIyYXN0Lm9yZy9zdHVkZW50Lw==
Set the proxy for HTTP requests only	Windows	FSASecureBrowser.exe -proxy 1:http:foo.com:80 aHR0cHM6Ly9mbC50ZHMuYWIyYXN0Lm9yZy9zdHVkZW50Lw==
	Mac	./FSASecureBrowser -proxy 1:http:foo.com:80 aHR0cHM6Ly9mbC50ZHMuYWIyYXN0Lm9yZy9zdHVkZW50Lw==
	Linux	./FSASecureBrowser.sh -proxy 1:http:foo.com:80 aHR0cHM6Ly9mbC50ZHMuYWIyYXN0Lm9yZy9zdHVkZW50Lw==
Set the proxy for all protocols to mimic the “Use this proxy server for all protocols” of Firefox	Windows	FSASecureBrowser.exe -proxy 1:*:foo.com:80 aHR0cHM6Ly9mbC50ZHMuYWIyYXN0Lm9yZy9zdHVkZW50Lw==
	Mac	./FSASecureBrowser -proxy 1:*:foo.com:80 aHR0cHM6Ly9mbC50ZHMuYWIyYXN0Lm9yZy9zdHVkZW50Lw==
	Linux	./FSASecureBrowser.sh -proxy 1:*:foo.com:80 aHR0cHM6Ly9mbC50ZHMuYWIyYXN0Lm9yZy9zdHVkZW50Lw==
Specify the URL of the PAC file	Windows	FSASecureBrowser.exe -proxy 2:proxy.com aHR0cHM6Ly9mbC50ZHMuYWIyYXN0Lm9yZy9zdHVkZW50Lw==
	Mac	./FSASecureBrowser -proxy 2:proxy.com aHR0cHM6Ly9mbC50ZHMuYWIyYXN0Lm9yZy9zdHVkZW50Lw==
	Linux	./FSASecureBrowser.sh -proxy 2:proxy.com aHR0cHM6Ly9mbC50ZHMuYWIyYXN0Lm9yZy9zdHVkZW50Lw==
Auto-detect proxy settings	Windows	FSASecureBrowser.exe -proxy 4 aHR0cHM6Ly9mbC50ZHMuYWIyYXN0Lm9yZy9zdHVkZW50Lw==
	Mac	./FSASecureBrowser -proxy 4 aHR0cHM6Ly9mbC50ZHMuYWIyYXN0Lm9yZy9zdHVkZW50Lw==
	Linux	./FSASecureBrowser.sh -proxy 4 aHR0cHM6Ly9mbC50ZHMuYWIyYXN0Lm9yZy9zdHVkZW50Lw==
Use the system proxy setting (default)	Windows	FSASecureBrowser.exe -proxy 5 aHR0cHM6Ly9mbC50ZHMuYWIyYXN0Lm9yZy9zdHVkZW50Lw==
	Mac	./FSASecureBrowser -proxy 5 aHR0cHM6Ly9mbC50ZHMuYWIyYXN0Lm9yZy9zdHVkZW50Lw==
	Linux	./FSASecureBrowser.sh -proxy 5 aHR0cHM6Ly9mbC50ZHMuYWIyYXN0Lm9yZy9zdHVkZW50Lw==

The Network Diagnostic Tool

AIR provides a network diagnostic tool to test your network's bandwidth to ensure it can handle administering online tests. The network diagnostic tool can be accessed through the Secure Browser or from your portal or practice test site through a conventional browser.



Once you are in the network diagnostic tool, enter the number of students you will test at peak volume and the tool will indicate if your network can handle online testing. The goal of the network diagnostic tool is to determine if your network bandwidth can handle the number of students you hope to test at peak volume. If the tool indicates you should test with fewer students, try running a third-party network speed test like speedtest.net. If a third-party tool also indicates you lack proper bandwidth, determine if other activity on your network is drawing bandwidth away from devices attempting to take the test. If it is, try to prioritize bandwidth for AIR's websites during online testing.

STEP 4: CONFIGURING ASSISTIVE TECHNOLOGIES

AIR's Test Delivery System is a website visible through a customized web browser.

Students who use assistive technologies with a standard web browser should be able to use those same technologies with the Test Delivery System. The best way to test compatibility with assistive technologies is by taking a practice test with those technologies turned on. If they do not work, contact the help desk or see the "Troubleshooting Text-to-Speech" section in the document titled *Configurations, Troubleshooting, and Secure Browser Installation* for your operating system for more information.

Supported Embedded Features

Embedded features work directly within the Test Delivery System. They can be accessed without additional third-party software.

Text-to-Speech

Text-to-speech (TTS) reads text on the screen aloud. Using TTS requires at least one voice pack to be installed on the student workstation. Voice packs that ship with the operating systems out of the box for Windows, Mac, and iOS are fully compatible with the Secure Browser. The Secure Browser recognizes voice packs that ship out of the box for Android and Chrome OS devices for playback and stop but the pause feature does not work properly on these devices. Consider testing students who need TTS on desktops or laptops running Windows or Mac or on iPads. A workaround for Chrome OS is available. It allows students to highlight a passage of text and have TTS read just that passage, eliminating the need for the pause feature.

For a full list of voice packs that have been tested and are whitelisted by the Secure Browser and for instructions about configuring TTS settings for Windows or Mac, see the "Troubleshooting Text-to-Speech" section in the document titled *Configurations, Troubleshooting, and Secure Browser Installation* for your operating system.

HELP DESK AND USER SUPPORT

If this document does not answer your questions, please contact the FSA Help Desk. The Help Desk is open **Monday–Friday from 7:00 a.m. to 8:30 p.m. Eastern Time** (except holidays or as otherwise indicated on the FSA Portal).

Toll-Free Phone Support: 1-866-815-7246

Email Support: fsahelpdesk@air.org

In order to help us effectively assist you with your issue or question, please be ready to provide the FSA Help Desk with detailed information that may include the following:

- Device, operating system, and browser version information
- Any error messages and codes that appeared, if applicable
- Information about your network configuration:
    - Secure browser installation (to individual machines or network)
    - Wired or wireless Internet network setup

CHANGE LOG

Location	Change	Date
Specifying Proxy Settings Using the Command Line Table	Added instructions for Mac and Linux	9/12/19