

Quick Guide for Setting Up Your Online Testing Technology

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 any 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 corporation and schools:

- Step 1.** Setting up the test administrator workstation
- Step 2.** Setting up student workstations
- Step 3.** Configuring your network for online testing
- Step 4.** Configuring assistive technologies

STEP 1: SETTING UP THE TEST ADMINISTRATOR WORKSTATION

It is unlikely that any setup is required for your test administrator (TA) workstations. Nearly any modern device, including mobile devices like tablets, with any modern browser can be used to access the TA site and administer a testing session. The TA Interface is a website. Any device used to access the Internet should be capable of administering tests. Per IDOE policy¹, the TA workstation should be a school-provided device, and not a TA's personal device. Smart phones should not be used to administer assessments.

If your school uses a firewall or other networking equipment that blocks access to public websites, you may need to whitelist AIR websites. See the "Whitelist URLs" section under Step 3: Configuring Your Network for Online Testing in this document.

To print test session information, TA workstations must be connected to a printer.

STEP 2: SETTING UP STUDENT WORKSTATIONS

For students to access online tests, each student workstation needs AIR's Secure Browser installed on it. 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 the test. Unlike conventional web browsers, the Secure Browser displays the student application in full-screen mode with no user interface to the browser itself. It has no back button, next button, refresh button, or URL bar. Students open the Secure Browser and are taken exactly where they need to go.

To setup student workstations, make sure the device and operating system are supported.

¹ See the 2018-2019 Indiana Assessment Policies, Administration, and Security Manual, which can be accessed at <https://www.doe.in.gov/assessment/indiana-assessment-policies>.

The following table highlights basic system requirements for student workstations:

For 2018–2019, a Secure Browser must be installed on each computer or tablet that will be used for student testing. The following table lists which operating systems are supported and which Secure Browser to install.			
Operating Systems	Supported Devices	Secure Browser	Related Requirements*
Desktop			
Windows 7 SP1 (Professional & Enterprise) 8 (Professional & Enterprise) 8.1 (Professional & Enterprise) 10 (Educational, Professional, & Enterprise) (Versions 1507 - 1803, 1809 ^a) Server 2008 R2, 2012 R2, 2016 R2	Desktops/Laptops	Windows Secure Browser	Disable fast user switching. Server 2008 R2, 2012 R2, and 2016 R2 are supported when using a thin client.
Mac 10.9 - 10.14 ^a	Desktops/Laptops	Mac Secure Browser	Depending on your OS version, disable the following features: <ul style="list-style-type: none"> ○ Application Launches from Function/Custom Keys ○ Updates to Third-Party Apps ○ Notification Center ○ Updates to iTunes ○ Look-Up Gesture ○ Mission Control ○ Dictation ○ Siri
Linux Fedora 27 - 28 LTS (Gnome) Ubuntu 14.04, 16.04, 18.04 LTS (Gnome)	Desktops/Laptops	Linux Secure Browser	Depending on your distribution, install SoX and Verdana True Type font. For touchscreen devices, disable on-screen keyboard.

Mobile			
iOS 10.3 11.4 12 ^a	4th Generation (Retina Display) 5th Generation (Retina Display) 6th Generation (Retina Display) iPad Air iPad Air 2 iPad Pro	AIRSecureTest Mobile Secure Browser	Automatic Assessment Configuration requires no further setup. Additional features can be disabled through Mobile Device Management.
Android 7.1 8.1 9 ^a	Lenovo Yoga Tab 3 10 Samsung Galaxy Tab S3 Asus ZenPad Z10	AIRSecureTest Mobile Secure Browser	Enable the Secure Browser keyboard.
Chrome 67+	Chromebooks	AIRSecureTest Kiosk Application	Chromebooks must be in kiosk mode. Automatic updates should be disabled or limited to a specific version used successfully before summative testing begins.
Windows 8 (Professional & Enterprise) 8.1 (Professional & Enterprise) 10 (Educational, Professional, and Enterprise)	AIR supports any tablet running Windows 8, 8.1, and 10, but has done extensive testing only on Surface Pro, Surface Pro 3, Asus Transformer, and Dell Venue.	Windows Secure Browser	Disable fast user switching.
^a Support for this version will begin upon the completion of testing following its release. *For information about implementing the related requirements, refer to <i>Additional Configurations and Trouble Shooting Guides</i> for applicable operating system.			

Note: See Appendix A for full system requirements and supported browsers.

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. Larger resolutions can be applied as appropriate for the monitor or screen being used.

Desktops, laptops, and tablets:

1024 x 768

**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 with "browser back" buttons should not be used.

**Headphones**

Wired headphones with a 3.5 mm connector or USB headphones.

Note: USB headphones are required for devices running VMware.

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 all major operating systems listed above. You can download the Secure Browser from the Indiana Assessment Portal at <https://indiana.portal.airast.org>. The Portal also contains basic installation instructions.

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 likely 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 a MSI package which enables use of MSIEXEC.

If you are from a small school, you can follow the basic installation instructions to install the Secure Browser. The Secure Browser is installed the same way as most other software. You will be asked 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.

For schools and corporations seeking advanced installation and configuration instructions, including how to disable any of the features detailed below, review the following supporting documents, as applicable:

- [Additional Configurations and Troubleshooting Guide for Windows](#)
- [Additional Configurations and Troubleshooting Guide for Mac](#)
- [Additional Configurations and Troubleshooting Guide for Linux](#)
- [Additional Configurations and Troubleshooting Guide for Android](#)
- [Additional Configurations and Troubleshooting Guide for Chrome OS](#)

Other Configurations

For devices running Windows, Mac, Linux, Android, or Chrome OS, there are a few additional configurations before secure testing can begin.

No further configuration is necessary for devices running iOS. A feature in iOS called Automatic Assessment Configuration works with AIR's Secure Browser to prepare an iPad for online testing.

Windows: Disabling Fast User Switching

Fast User Switching is a feature in Windows 7, 8, 8.1, and 10 that allows for more than one user to be logged in at the same time. If Fast User Switching is not disabled and students try to access it during a test, the Secure Browser will pause the test.

Fast User Switching can be disabled using the Local Group Policy Editor or Registry Editor.

Mac: Disabling Mission Control

Mission Control is a feature in Mac OS X 10.9 and later that allows users to switch to open applications running in the background. If Mission Control is not disabled, students will not be able to login to the Secure Browser.

Mission Control can be disabled through the terminal.

Mac: Disabling Look-Up Gesture

Look-up Gesture allows Mac users to look up the definition of a word by highlighting that word and tapping the trackpad with three fingers. This feature is required to be disabled during testing.

Look-up Gesture can be disabled through System Preferences.

Mac: Disabling Siri

Siri is a virtual assistant that uses voice commands to answer questions and perform actions on Mac desktops and laptops running MacOS 10.12 or later. If Siri is not disabled, students could potentially access information that they should not have access to while taking a secure assessment.

While in a test, the AIRSecureBrowser app will detect if a user tries to enable Siri and will disconnect the student from the test. Siri can be disabled through System Preferences.

Linux: Disabling On-Screen Keyboard

Ubuntu and Fedora feature an on-screen keyboard that should be disabled before you administer online tests. If the on-screen keyboard is not disabled, it could pop up on a touchscreen device and cause the Secure Browser to pause the test.

The Linux on-screen keyboard can be disabled through System Settings.

Android: Enabling Secure Browser Keyboard

The default keyboard for Android allows predictive text, which may provide students with hints for answers to tests. For this reason, the Secure Browser for Android requires a mobile keyboard be configured for the Secure Browser itself. The Secure Browser keyboard is a basic keyboard with no row for predictive text functionality.

The Secure Browser keyboard must be enabled through a pop-up the first time the Secure Browser is launched on an Android tablet.

Chrome OS: Managing Auto-Updates

New versions of Chrome OS are released regularly and tested by AIR to ensure no new features pose a risk for online testing.

However, bugs or unintentional features do sometimes show up in the latest release. Because of this, AIR recommends disabling Chrome OS auto-updates or limiting auto-

updates to a version used successfully before summative testing begins to ensure Chromebooks remain stable during the test window.

Chrome OS updates can be disabled or limited through the Device Settings page on the Chromebook. From this page, auto-updates can be stopped or allowed, but only to a specific version.

Chromebooks: Manufactured After 2017

Due to recent changes by Google, users with Chromebooks manufactured in 2017 or later who do not have an Enterprise or Education license will not be able to use those machines for assessments. Google no longer allows users without these licenses to set up kiosk mode, which is necessary to run the AIR Secure Browser. This change restricting kiosk mode does not affect the Chrome operating system. You can still use any version of Chrome OS on hardware manufactured in 2016 or earlier.

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.

Whitelist URLs

Testing servers and satellites may be added or 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	*.airast.org *.tds.airast.org *.cloud1.tds.airast.org *.cloud2.tds.airast.org

Some online assessments contain an embedded dictionary and thesaurus provided by Merriam-Webster. The URLs listed in the table below should also be whitelisted to ensure that students can use them during testing.

AIR URLs for Online Dictionaries and Thesauruses

Domain Name	IP Address
media.merriam-webster.com	64.124.231.250
www.dictionaryapi.com	64.124.231.250

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 the Indiana Assessment Portal or Released Items Repository site through a conventional browser.



Diagnostic Screen

This page allows you to check the **current** bandwidth of your network. Select a test from the drop-down list and enter the maximum number of students likely to test at one time, then click [Run Network Diagnostics Tests].

Your Operating System: Windows 10	Your Browser Version: Chrome v68
Secure Browser: false	
Network Diagnostics: Select Test: <input type="text" value="ELA"/> Enter the total number of students you would like to test at one time: <input type="text" value="7"/> <input type="button" value="Run Network Diagnostics Tests"/> Download Results: 724.034 Mbps download. Upload Results: 79.208 Mbps upload. Bandwidth Summary: <div style="border: 1px solid green; padding: 5px;">Given the current load on your system, you should be able to test the requested number of students at this location. (Please note: The throughput estimates include the encryption/decryption overhead for data transfer. Throughput estimates change as the network conditions change and can vary from run to run.)</div>	

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 testing. The goal of the network diagnostic tool is to determine if your network bandwidth can handle the number of students you intend 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 machine attempting to take the test. If it is, try to prioritize bandwidth for AIR's websites during online testing.

Proxy Servers

If a proxy server is set up at your school, you may need to configure the Secure Browser's proxy settings. For instructions on how to configure the Secure Browser's proxy settings, see the "Configuring the Secure Browser for Proxy Servers" section in the documents titled, *Additional Configurations and Troubleshooting Guides for Windows, Mac, Chrome OS, Android, and Linux*.

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.

Traffic Shaping, Packet Prioritization, & Quality of Service

If your testing network includes devices that perform traffic shaping, packet prioritization, or Quality of Service, ensure AIR URLs have high priority. For a list of websites, you should give high priority, see the "URLs Provided by AIR" section in the document titled, *Additional Configurations and Troubleshooting Guides for Windows, Mac, Chrome OS, Android, and Linux*.

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, *Additional Configurations and Troubleshooting Guides for Windows, Mac, Chrome OS, Android, and Linux* 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 aloud text on the screen. 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, 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 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, *Additional Configurations and Troubleshooting Guides for Windows, Mac, Chrome OS, Android, and Linux*.

Supported Non-Embedded Features

Non-embedded features require the use of other hardware and/or software to make certain functionalities available to students within the Test Delivery System. Non-embedded features require devices be set to permissive mode. This mode, found in TIDE as a student test setting, temporarily lowers the security settings of the Secure Browser so that the student can interoperate with other software on the device like JAWS or ZoomText while taking a test.

Braille

Text-to-speech allows students to read text displayed on a screen with a braille display. Currently, AIR supports Duxbury Braille Translation for TA workstations. TAs need this software to emboss braille test content. Additional information can be found in the *Braille Requirements and Testing Manual*.

Speech-to-Text

Speech-to-text (STT) allows a student to speak into a headset and have their speech converted into text that becomes the response that is entered into the Test Delivery System. Currently, AIR does not offer an embedded STT feature. STT is available for Windows and Mac through Dragon Naturally Speaking or other similar software. Users should verify the security and privacy policies of any third-party software before deciding to use that software. Many STT providers send a

student’s audio recording to the cloud for processing. Users should have a clear understanding of what third-party providers do and do not do with student information. STT is not available for Linux, iOS, Android, or Chrome OS.

ADMINISTER ONLINE TESTS

Before administering an operational test, get comfortable with the system by administering a Practice Test or a Released Items Repository test. Practice Tests can be administered on supported devices via the Secure Browser. Released Items Repository Tests can be administered on supported devices via the Secure Browser or through modern conventional browsers like Chrome or Firefox.

ADMINISTERING RELEASED ITEMS REPOSITORY (RIR) TESTS

To administer a RIR test, complete the following steps:

1. TAs should open a web browser, go to the TA Site, and choose a RIR test to administer.
2. Students should launch the Secure Browser and click the link for RIR tests.
3. TAs should give the students the Session ID.
4. Students should click through the login pages. Students can log in anonymously as a guest or with their real account. In either case, they should use a Session ID from the TA.

For more information about administering practice tests, see the *TA Product Guide (coming Oct 1, 2018)*.

When TAs and students are comfortable using the system, you are ready to administer an operational test.

ADMINISTERING PRACTICE & OPERATIONAL TESTS

The steps for administering a practice or operational test are nearly identical to administering a RIR test.

1. TAs should open a web browser and go to the TA Site.
2. Students should launch the Secure Browser.
3. TAs should give students the Session ID.
4. Students should enter the Session ID, their first name, and their Student ID.

For more information about administering operational tests, see the *TA Product Guide (coming Oct 1, 2018)*.

Contact the Indiana Assessment Help Desk for any additional assistance.

Email: airindianahelpdesk@air.org

Phone: 1.866.298.4256

Chat: <https://indiana.portal.airast.org/chat.stml>

Appendix A. Supported Devices & Related Requirements

This appendix lists information about supported devices and related requirements.

Desktops & Laptops		
Supported Operating Systems	Minimum Requirements	Recommended Specifications
Windows 7 SP1 (Professional and Enterprise) 8, 8.1 (Professional and Enterprise) 10, 10 in S Mode (Educational, Professional, and Enterprise) (Versions 1507-1803, 1809 ^a) Server 2008 R2, 2012 R2, 2016 R2 (thin client)	1 GHZ Processor 1 GB RAM (32-bit) 2 GB RAM (64-bit) 16 GB hard drive (32-bit) 20 GB hard drive (64-bit)	1.4 GHZ Processor 2 or more GB RAM 20 or more GB hard drive space
Mac OS X 10.9-10.14 ^a	1 GHZ Processor 1 GB RAM (32-bit) 2 GB RAM (64-bit) 16 GB hard drive (32-bit) 20 GB hard drive (64-bit)	1.4 GHZ Processor 2 or more GB RAM 20 or more GB hard drive space
Linux (64-bit or 32-bit) Fedora 27-28 LTS (Gnome) Ubuntu 14.04, 16.04 LTS (Gnome)	1 GHZ Processor 1 GB RAM (32-bit) 2 GB RAM (64-bit) 16 GB hard drive (32-bit) 20 GB hard drive (64-bit) Required libraries/packages: GTK+ 2.18 or higher GLib 2.22 or higher Pango 1.14 or higher X.Org 1.0 or higher (1.7+ recommended) libstdc++ 4.3 or higher libreadline6:i386 (required for Ubuntu only) GNOME 2.16 or higher	1.4 GHZ Processor 2 or more GB RAM 20 or more GB hard drive space Recommended libraries/packages: In addition to the required libraries listed under minimum requirements, the following should be installed: NetworkManager 0.7 or higher DBus 1.0 or higher HAL 0.5.8 or higher
Linux (64-bit only) Ubuntu 18.04 LTS (Gnome)	1 GHZ Processor 2 GB RAM 20 GB hard drive space In addition to all libraries and packages listed above, Ubuntu 18.04 LTS (Gnome) also requires the following libraries: Sox Net-tools	1.4 GHZ Processor 2 or more GB RAM 20 or more GB hard drive space

Support for this version is anticipated upon the completion of testing following its release.

ARM-powered devices such as the Raspberry Pi are not supported for online testing.

Tablets and Chromebooks	
Supported Operating Systems	Supported Tablets
iOS (iPads) 10.3, 11.4, 12*	4 th Generation (Retina Display) 5 th Generation (Retina Display) 6 th Generation (Retina Display) iPad Air iPad Air 2 iPad Pro
Android 7.1, 8.1, 9*	Lenovo Yoga Tab 3 10 Samsung Galaxy Tab S3 Asus ZenPad Z10
Windows 8, 8.1 (Professional & Enterprise) 10 (Educational, Professional, & Enterprise)	AIR supports any tablet running these versions of Windows, but has done extensive testing only on Surface Pro, Surface Pro 3, Asus Transformer, and Dell Venue.
Chrome OS 67+	See https://support.google.com/edu/android/answer/6220366 for a full list of supported Chromebooks.

*Support for this version is anticipated upon the completion of testing following its release.

NComputing		
Supported Server Host	Supported Server Software	Supported Terminal
Windows Server 2008 R2	Space Server 8.4	L300, firmware version 1.12.xx
Windows Server 2012 R2 Windows Server 2016 R2 Windows 10	Space PRO 10	L300, L350, M300, firmware version 1.13.xx

Supported Operating Systems	Supported Devices	Supported Web Browsers	TA Sites, Released Items Repository	TIDE, ORS
Windows				
7 SP1 (Professional & Enterprise)	Desktops/Laptops	Chrome 67+	✓	✓
		Firefox 52+	✓	✓
8 (Professional & Enterprise) 8.1 (Professional & Enterprise)	Desktops/Laptops	Chrome 67+	✓	✓
		Firefox 52+	✓	✓
10 (Educational, Professional, & Enterprise) (Versions 1507 - 1803, 1809 ^a)	Desktops/Laptops	Chrome 67+	✓	✓
		Firefox 52+	✓	✓
		Edge	✓	✓
Server 2008 R2, 2012 R2, 2016 R2 (thin client)	Desktops, Laptops	Chrome 67+	✓	✓
		Firefox 52+	✓	✓
Mac				
10.9 - 10.14 ^a	Desktops/Laptops	Chrome 67+	✓	✓
		Firefox 52+	✓	✓
		Safari 9+	✓	✓
Linux				
Fedora 27 - 28 LTS (Gnome)	Desktops/Laptops	Chrome 67+	✓	✓
		Firefox 52+	✓	✓
Ubuntu 14.04, 16.04, 18.04 LTS (Gnome)	Desktops/Laptops	Chrome 67+	✓	✓
		Firefox 52+	✓	✓
iOS^b				

10.3	4th Generation (Retina Display) 5th Generation (Retina Display) 6th Generation (Retina Display) iPad Air iPad Air 2 iPad Pro	Safari 10	✓	
11.4	4th Generation (Retina Display) 5th Generation (Retina Display) 6th Generation (Retina Display) iPad Air iPad Air 2 iPad Pro	Safari 11	✓	
12 ^a	4th Generation (Retina Display) 5th Generation (Retina Display) 6th Generation (Retina Display) iPad Air iPad Air 2 iPad Pro	Safari 12 ^a	✓	
Android				
7.1, 8.1, 9 ^a	Lenovo Yoga Tab 3 10 Samsung Galaxy Tab S3 Asus ZenPad Z10	Chrome 67+	✓	
Chrome OS				
67+	Chromebooks	Chrome 67+	✓	
^a Support for this version will begin upon the completion of testing following its release. ^b When using iOS, ensure the English keyboard is installed and set as the default keyboard.				

Note: TIDE and ORS can be accessed with iOS, Android, and Chrome devices; however, these devices are not fully supported due to the upload and download functionality frequently utilized within the two systems.

Appendix B. Change Log

Updates to this guide after October 1, 2018 are noted.

Section	Page	Description of Change	Revision Date
Step 4	8	Added clarified language on the use and support of Text-to-Speech	12/3/2018