WYOMING
DEPARTMENT OF EDUCATION

Configurations and Troubleshooting for Linux

For Technology Coordinators

2020-2021

Published August 11, 2020

Prepared by Cambium Assessment, Inc.

Cambium Assessment

Configurations and Troubleshooting for Linux 1
Configurations and Troubleshooting for Linux 3
How to Configure Linux Workstations for Online Testing 3
Required Libraries & Packages to Install 3
How to Add Verdana Font 3
How to Disable the On-Screen Keyboard 4
How to Uninstall the Secure Browser on Linux 5
How to Uninstall the Secure Browser on Linux 5
How to Troubleshoot Linux Workstations 6
How to Reset Secure Browser Profiles on Linux 6
How to Configure Networks for Online Testing 7
Resources to Add to your Allowlist for Online Testing 7
URLs for Non-Testing Sites to Add to your Allowlist 7
URLs for TA and Student Testing Sites to Add to your Allowlist 7
URLs for Online Dictionary and Thesaurus to Add to your Allowlist 8
Ports and Protocols Required for Online Testing 8
How to Configure Filtering Systems 8
How to Configure for Domain Name Resolution 8
How to Configure Network Settings for Online Testing 8
How to Configure the Secure Browser for Proxy Servers 9

Configurations and Troubleshooting for Linux

This document contains configurations and troubleshooting for your network and Linux workstations.

How to Configure Linux Workstations for Online Testing

This section contains additional configurations for Linux.

Required Libraries & Packages to Install

The following libraries and packages are required to be installed on all 32-bit and 64-bit Linux workstations:

- 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

The following libraries and packages are recommended to be installed on all 32-bit and 64-bit Linux workstations:

- NetworkManager 0.7 or higher
- DBus 1.0 or higher
- HAL 0.5.8 or higher

The following libraries and packages are required to be installed on all 64-bit Linux workstations:

- Sox
- Net-tools

How to Add Verdana Font

Some tests have content that requires the Verdana TrueType font. Therefore, ensure that Verdana is installed on Linux machines used for testing. The easiest way to do this is to install the Microsoft core fonts package for your distribution.

- Fedora—Follow the steps in the "How to Install" section of the following website: http://corefonts.sourceforge.net/.
- Ubuntu—In a terminal window, enter the following command to install the msttcorefonts package:

  sudo apt-get install msttcorefonts

How to Disable the On-Screen Keyboard

Fedora and Ubuntu feature an on-screen keyboard that should be disabled before online testing. This section describes how to disable the on-screen keyboard.

1. Open **System Settings**.
2. Select **Universal Access**.
3. In the *Typing* section, toggle **Screen Keyboard** to **Off**.

How to Uninstall the Secure Browser on Linux

This section contains instructions to uninstall the Secure Browser for Linux.

How to Uninstall the Secure Browser on Linux

To uninstall a Secure Browser, delete the folder from the installation directory.

How to Troubleshoot Linux Workstations

This section contains troubleshooting tips for Linux.

How to Reset Secure Browser Profiles on Linux

If the Help Desk advises you to reset the Secure Browser profile, use the instructions in this section.

1. Log on as a superuser or as the user who installed the Secure Browser, and close any open Secure Browsers.
2. Open a terminal, and delete the contents of the following directories:

   /home/username/.cai

   /home/username/.cache/cai

   where `username` is the user account where the Secure Browser is installed. (Keep the directories, just delete their contents.)
3. Restart the Secure Browser.

How to Configure Networks for Online Testing

This section contains additional configurations for your network.

Resources to Add to your Allowlist for Online Testing

This section presents information about the URLs that CAI provides. 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.

URLs for Non-Testing Sites to Add to your Allowlist

Table 1 lists URLs for non-testing sites, such as Test Information Distribution Engine and Centralized Reporting System.

Table 1. CAI URLs for Non-Testing Sites

System	URL
Portal and Secure Browser installation files	https://wyoassessment.org/
Single Sign-On System	https://sso2.cambiumast.com/auth/realms/wyoming/account
Test Information Distribution Engine	https://wy.tide.cambiumast.com/
Centralized Reporting System	https://wy.reporting.cambiumast.com/

URLs for TA and Student Testing Sites to Add to your Allowlist

Testing servers and satellites may be added or modified during the school year to ensure an optimal testing experience. As a result, CAI strongly encourages you to add these URLs to your allowlist at the root level. This requires using a wildcard.

Table 2. CAI and AIR URLs for Testing Sites

System	URL
TA and Student Testing Sites Assessment Viewing Application For 2020-2021, users should add both Cambium and AIR URLs listed in this table to their allowlist.	*.cambiumast.com *.tds.cambiumast.com *.cloud1.tds.cambiumast.com *.cloud2.tds.cambiumast.com *.airast.org *.tds.airast.org *.cloud1.tds.airast.org *.cloud2.tds.airast.org

URLs for Online Dictionary and Thesaurus to Add to your Allowlist

Some online assessments contain an embedded dictionary and thesaurus provided by Merriam-Webster. The Merriam-Webster URLs listed in Table 3 should be added to your allowlist to ensure that students can use them during testing.

Table 3. CAI 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

Ports and Protocols Required for Online Testing

Table 4 lists the ports and protocols used by the Test Delivery System. Ensure that all content filters, firewalls, and proxy servers are open accordingly.

Table 4. Ports and Protocols for Test Delivery System

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

How to Configure Filtering Systems

If the school's filtering system has both internal and external filtering, the URLs for the testing sites (see Table 1) must be added to your allowlist in both filters. Ensure your filtering system is not configured to perform packet inspection on traffic to CAI servers. Please see your vendor's documentation for specific instructions. Also, be sure to add these URLs to your allowlist in any multilayer filtering system (such as local and global layers). Ensure all items that handle traffic to *.tds.cambiumast.com and *.tds.airast.org have the entire certificate chain and are using the latest TLS 1.2 protocol.

How to Configure for Domain Name Resolution

Table 1 and Table 2 list the domain names for CAI's testing and non-testing applications. Ensure the testing machines have access to a server that can resolve those names.

How to Configure 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 Linux machines:

1. Open **System Settings**.
2. Open **Network**.
3. Select **Network Proxy**.
4. From the **Method** dropdown, select **None**.

5. Close the **Network** window.

How to Configure the Secure Browser for Proxy Servers

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. Table 5 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: Domain names in commands The commands in Table 5 use the domain proxy.com. When configuring for a proxy server, use your actual proxy server hostname.

Table 5. Specifying proxy settings using the command line

Description	System	Command
Use the browser without any proxy	Linux	`./WYSecureBrowser.sh -proxy 0 aHR0cHM6Ly93eS50ZHMuY2FtYml1bWFzdC5jb20vc3R1ZGVudA==`
Set the proxy for HTTP requests only	Linux	`./WYSecureBrowser.sh -proxy 1:http:proxy.com:8080 Encoded Test Site URL`
Set the proxy for all protocols to mimic the "Use this proxy server for all protocols" of Firefox	Linux	`./WYSecureBrowser.sh -proxy 1:*:proxy.com:8080 Encoded Test Site URL`
Specify the URL of the PAC file	Linux	`./WYSecureBrowser.sh -proxy 2:proxy.com Encoded Test Site URL`
Auto-detect proxy settings	Linux	`./WYSecureBrowser.sh -proxy 4 Encoded Test Site URL`
Use the system proxy setting (default)	Linux	`./WYSecureBrowser.sh -proxy 5 Encoded Test Site URL`