



Hawai'i

Statewide Assessment Program



Configurations and Troubleshooting for Linux

For Technology Coordinators

2019-2020

Published July 18, 2019

Updated June 10, 2020

Prepared by Cambium Assessment, Inc.



Descriptions of the operation of the Test Information Distribution Engine, Test Delivery System, and related systems are property of Cambium Assessment, Inc. (CAI) and are used with the permission of CAI.

Table of Contents

Configurations and Troubleshooting for Linux	3
How to Configure Networks for Online Testing.....	3
Which Resources to Whitelist for Online Testing	3
Which Ports and Protocols are Required for Online Testing	4
How to Configure Filtering Systems.....	4
How to Configure for Domain Name Resolution	4
How to Configure for Certificate Revocations	5
How to Configure Network Settings for Online Testing	5
How to Configure the Secure Browser for Proxy Servers	6
How to Uninstall the Secure Browser on Linux.....	7
How to Uninstall the Secure Browser on Linux	7
How to Configure Linux Workstations for Online Testing.....	8
Which Libraries & Packages Are Required	8
How to Add Verdana Font	8
How to Disable the On-Screen Keyboard	9
How to Troubleshoot Linux Workstations	10
How to Reset Secure Browser Profiles on Linux.....	10
User Support	11

Configurations and Troubleshooting for Linux

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

How to Configure Networks for Online Testing

This section contains additional configurations for your network.

Which Resources to Whitelist 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.

Which URLs for Non-Testing Sites to Whitelist

[Table 1](#) lists URLs for non-testing sites, such as Test Information Distribution Engine and Online Reporting System.

Table 1. CAI URLs for Non-Testing Sites

System	URL
Portal and Secure Browser installation files	https://alohahsap.org/
Single Sign-On System	https://sso1.cambiumast.com/auth/realms/hawaii/account
Test Information Distribution Engine	https://www.hitide.org/
Online Reporting System	https://hsa.reports.cambiumast.com/
Centralized Reporting System	hi.reporting.cambiumast.com

Which URLs for TA and Student Testing Sites to Whitelist

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 whitelist 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	*.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
--	-------------------------

Which URLs for Online Dictionary and Thesaurus to Whitelist

Some online assessments contain an embedded dictionary and thesaurus provided by Merriam-Webster. The Merriam-Webster URLs listed in [Table 3](#) should be whitelisted 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

Which Ports and Protocols are 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 whitelisted 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 whitelist these URLs 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 for Certificate Revocations

CAI's servers present certificates to the clients. The following sections discuss the methods used to check those certificates for revocation.

How to Use the Online Certificate Status Protocol

To use the Online Certificate Status Protocol (OCSP), ensure your firewalls allow the domain names listed in [Table 5](#). The values in the Patterned column are preferred because they are more robust.

Table 5. Domain Names for OCSP

Patterned	Fully Qualified
*.thawte.com	ocsp.thawte.com
*.geotrust.com	ocsp.geotrust.com
*.ws.symantec.com	ocsp.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 at https://www.symantec.com/content/en/us/enterprise/other_resources/OCSP_Upgrade_-_New_IP_Addresses.txt.
2. Add the retrieved IP addresses to your firewall's whitelist. Do not replace any existing IP addresses.

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. Click **X** to close **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 6](#) 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 6](#) use the domain proxy.com. When configuring for a proxy server, use your actual proxy server hostname.

Table 6. Specifying proxy settings using the command line

Description	System	Command
Use the browser without any proxy	Linux	<code>./HISecureBrowser.sh -proxy 0 aHR0cHM6Ly9oc2EudGRzLmNhbWJpdW1hc3QuY29tL3N0dW RlbnQ=</code>
Set the proxy for HTTP requests only	Linux	<code>./HISecureBrowser.sh -proxy 1:http.proxy.com:8080 aHR0cHM6Ly9oc2EudGRzLmNhbWJpdW1hc3QuY29tL3N0dW RlbnQ=</code>
Set the proxy for all protocols to mimic the “Use this proxy server for all protocols” of Firefox	Linux	<code>./HISecureBrowser.sh -proxy 1*:proxy.com:8080 aHR0cHM6Ly9oc2EudGRzLmNhbWJpdW1hc3QuY29tL3N0dW RlbnQ=</code>
Specify the URL of the PAC file	Linux	<code>./HISecureBrowser.sh -proxy 2:proxy.com aHR0cHM6Ly9oc2EudGRzLmNhbWJpdW1hc3QuY29tL3N0dW RlbnQ=</code>
Auto-detect proxy settings	Linux	<code>./HISecureBrowser.sh -proxy 4 aHR0cHM6Ly9oc2EudGRzLmNhbWJpdW1hc3QuY29tL3N0dW RlbnQ=</code>
Use the system proxy setting (default)	Linux	<code>./HISecureBrowser.sh -proxy 5 aHR0cHM6Ly9oc2EudGRzLmNhbWJpdW1hc3QuY29tL3N0dW RlbnQ=</code>

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 Configure Linux Workstations for Online Testing

This section contains additional configurations for Linux.

Which Libraries & Packages Are Required

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.

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

User Support

If this document does not answer your questions, please contact the Hawaii Statewide Assessment Program Help Desk.

The Help Desk will be open Monday–Friday from 7:30 a.m. to 4:00 p.m. Hawaiian Standard Time (except holidays).

Hawaii Statewide Assessment Program Help Desk

Toll-Free Phone Support: 1-866-648-3712

Email Support:
hsaphelpdesk@cambiumassessment.com

If you contact the Help Desk, you will be asked to provide as much detail as possible about the issues you encountered. You may choose to use the *Help Desk Intake Form*, available on the <https://alohahsap.org/> portal website in the **Resources >> Technology** section.

Include the following information:

- Test Administrator name and IT/network contact person and contact information
- SSIDs of affected students
- Results ID for the affected student tests
- 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

This Change Log can be used to identify specific changes that are made to any of the information included in the original document throughout the current school year.

Change	Section	Date
Changed "oscp" to "ocsp" in the Fully Qualified column of Table 5.	Table 5. Domain Names for OCSP	9/25/19
Fixed a formatting error in the instructions for step 2.	How to Reset Secure Browser Profiles on Linux	9/25/19
Updated the note and some of the proxy commands.	How to Configure the Secure Browser for Proxy Servers	11/16/19
Updated information throughout the paragraph.	How to Configure Filtering Systems	11/27/19
Changed all references to "American Institutes for Research" and "AIR" to "Cambium Assessment, Inc." and "CAI" respectively.	Global	6/10/20