Configurations and Troubleshooting for Linux

For Technology Coordinators

2022-2023

Published December 15, 2022

Prepared by Cambium Assessment, Inc.

Table of Contents

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.

Linux Basic Secure Browser Installation

These procedures install the Secure Browser on desktop and laptop computers running one of the supported versions of Fedora or Ubuntu. Be sure to download the correct Secure Browser for your version of Linux. These instructions may vary for your individual Linux version.

After installing, ensure all backgrounds jobs, such as virus scans or software updates, are scheduled outside of test windows. For example, if your testing takes place between 8:00 a.m. and 3:00 p.m., schedule background jobs outside of these hours.

Installing the Secure Browser for Fedora

This procedure installs the Secure Browser on desktop or laptop computers running one of the supported Fedora distributions using a .rpm package. These instructions may vary for your individual Fedora version.

1. Uninstall any previous versions of the Secure Browser by completing the following steps:

    a. Open the terminal.

    b. Enter sudo apt remove -y UTSecureBrowser and hit enter.

    c. Enter the sudo password and hit enter.

2. Obtain the root or super-user password for the computer on which you are installing the Secure Browser.

3. From the Linux tab on your Secure Browser page, click **Download Secure Browser 15 for all supported versions of Fedora**. Be sure to click the link for Fedora. A dialog window opens. If prompted for a download location, select the Downloads folder.

4. Ensure the Universe and Multiverse repositories are enabled and updated by performing either of the following procedures. This will allow the correct information for the dependencies to be installed. After the repository information is updated, continue with the installation process.

    a. Using the built-in Software updater, update the system as needed.

OR

    b. Update repository information through the terminal:

i. Open the terminal.

ii. Enter sudo yum update and hit enter.

iii. Enter the administrator password and hit enter.

5. After the Secure Browser installation package downloads and the Universe and Multiverse repositories are updated, select one of the following installation techniques:

Installing through the built-in Package Manager:

a. Open the Downloads folder, right-click on the Secure Browser installation package, and select **Open with Software Install.**

b. It may take a few moments for the system to examine the package. When the installation window opens, do the following to install the package:

i. Select **Install**.

ii. Enter the administrator password.

iii. Select **Authenticate**.

c. Restart the device to ensure all packages are active.

d. *Optional*: If the icon is not present in the Taskbar, open the terminal and run /usr/lib/UTSecureBrowser/install-icon.sh -i. This will install the icon to the to the Taskbar.

Installing through the Terminal:

1. Open the Downloads folder, right-click on the Secure Browser installation package, and select **Open in Terminal**. The terminal window opens.

2. Enter sudo yum install ./UTSecureBrowser.rpm and hit enter.

3. Enter the sudo password and hit enter.

4. When prompted *Is it ok?*, select **Y**.

5. The Secure Browser and dependencies will install.

6. Restart the device to ensure all packages are active.

Installing the Secure Browser for Ubuntu

This procedure installs the Secure Browser on desktop computers running one of the supported Ubuntu distributions using a .deb package. These instructions may vary for your individual Ubuntu version.

1. Uninstall any previous versions of the Secure Browser by completing the following steps:

a. Open the terminal.

b. Enter sudo apt remove -y UTSecureBrowser and hit enter.

c. Enter the sudo password and hit enter.

2. Obtain the root or super-user password for the computer on which you are installing the Secure Browser.

3. From the Linux tab on your Secure Browser page, click **Download Secure Browser 15 for all supported versions of Ubuntu**. Be sure to click the link for Ubuntu. A dialog window opens. If prompted for a download location, select the Downloads folder.

4. Ensure the Universe and Multiverse repositories are enabled and updated by performing either of the following procedures. This will allow the correct information for the dependencies to be installed. After the repository information is updated, continue with the installation process.

    a. Using the built-in Software updater, update the system as needed.

OR

    b. Update repository information through the terminal:

        i. Open the terminal.

        ii. Enter sudo apt update and hit enter.

        iii. Enter the administrator password and hit enter.

5. After the Secure Browser installation package downloads and the Universe and Multiverse repositories are updated, select one of the following installation techniques:

Installing through the built-in Package Manager:

a. Open the Downloads folder and right-click on the Secure Browser installation package. If the top line displays **Open with Archive Manager**, select **Open with Other Application** and choose **Software Install**. If the first line displays **Open with Software Install**, select that option.

b. It may take a few moments for the system to examine the package. When the installation window opens, do the following to install the package:

    i. Select **Install**.

    ii. Enter the administrator password.

    iii. Select **Authenticate**. The package will install.

c. Restart the device to ensure all packages are active.

d. *Optional*: If the icon is not present in the Favorites bar, open the terminal and run /usr/lib/UTSecureBrowser/install-icon.sh -i. This will install the icon to the Favorites bar. Note you do not need to use sudo for this.

Installing through the Terminal:

1. Open the Downloads folder, right-click on the Secure Browser installation package, and select **Open in Terminal**. The terminal opens.
2. Enter sudo apt install ./UTSecureBrowser.deb and hit enter.
3. Enter the sudo password and hit enter.
4. When prompted *Do you want to continue?*, select **Y**. The Secure Browser and dependencies will install.
5. Restart the device to ensure all packages are active.
6. *Optional*: If the icon is not present in the Favorites bar, open the terminal and run /usr/lib/<SecureBrowser>/install-icon.sh -i. This will install the icon to the Favorites bar. Note you do not need to use sudo for this.

Troubleshooting:

If the installation fails, please try the following steps:

7. Open the terminal.
8. Enter sudo apt-add-repository multiverse and hit enter.
9. Enter the sudo password and hit enter.
10. Enter sudo apt install ./UTSecureBrowser.deb and hit enter.

Required Libraries & Packages to Install

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

- GTK+ 3.14 or higher
- X.Org 1.0 or higher (1.7+ recommended)
- libstdc++ 4.8.1 or higher
- glibc 2.17 or higher

The following libraries and packages are recommended to be installed on all Linux workstations:

- NetworkManager 0.7 or higher
- DBus 1.0 or higher
- GNOME 2.16 or higher

- PulseAudio

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 Helpdesk 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 Online Reporting System.

Table 1. CAI URLs for Non-Testing Sites

System	URL
Portal and Secure Browser installation files	https://utahrise.org/
Single Sign-On System	https://sso2.cambiumast.com/auth/realms/utah/account
Test Information Distribution Engine	https://ut.tide.cambiumast.com/
Reporting System	https://ut.reports.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. CAI strongly encourages adding domains (and not IP addresses) and using wildcards when adding these URLs to your allowlist, as servers may be added or removed from the field without notice.

Table 2. CAI and AIR URLs for Testing Sites

System	URL
TA and Student Testing Sites Assessment Viewing Application	*.cambiumtds.com *.tds.cambiumtds.com *.cloud1.tds.cambiumtds.com *.cloud2.tds.cambiumtds.com *.cambiumast.com *.tds.cambiumast.com *.cloud1.tds.cambiumast.com *.cloud2.tds.cambiumast.com

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

Domains for Email Exchange Server and Single Sign-On System

CAI systems send emails for password resets and login codes for the single sign-on system from cambiumast.com and from cambiumassessment.com. Add both domains to your allowlist to ensure you receive these emails.

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 *.cambiumtds.com and *.tds.cambiumast.com 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	./UTSecureBrowser.sh -proxy 0 https://ut.tds.cambiumtds.com/student==
Set the proxy for HTTP requests only	Linux	./UTSecureBrowser.sh -proxy 1:http:proxy.com:8080 https://ut.tds.cambiumtds.com/student==
Set the proxy for all protocols to mimic the "Use this proxy server for all protocols" of Firefox	Linux	./UTSecureBrowser.sh -proxy 1:*:proxy.com:8080 https://ut.tds.cambiumtds.com/student==
Specify the URL of the PAC file	Linux	./UTSecureBrowser.sh -proxy 2:proxy.com https://ut.tds.cambiumtds.com/student==
Auto-detect proxy settings	Linux	./UTSecureBrowser.sh -proxy 4 https://ut.tds.cambiumtds.com/student==
Use the system proxy setting (default)	Linux	./UTSecureBrowser.sh -proxy 5 https://ut.tds.cambiumtds.com/student==