ELPA21

Configurations, Troubleshooting, and Advanced Secure Browser Installation Guide for Chrome OS

For Technology Coordinators

2020-2021

Published August 17, 2020

Prepared by Cambium Assessment, Inc.

Configurations, Troubleshooting, and Advanced Secure Browser Installation for Chrome OS

This document contains configurations, troubleshooting, and advanced Secure Browser installation instructions for your network and Chrome OS workstations.

How to Configure Chrome OS Workstations for Online Testing

This section contains additional configurations for Chrome OS.

How to Manage Chrome OS Auto-Updates

This section describes how to manage Chrome OS auto-updates. CAI recommends disabling Chrome OS auto-updates or limiting updates to a specific version used successfully before summative testing begins.

How to Disable Auto-Updates for Chrome OS

This section describes how to disable auto-updates for Chrome OS.

1. Display the Device Settings page by following the procedure in ***Manage device settings***, https://support.google.com/chrome/a/answer/1375678. The steps in that procedure assume that your Chromebooks are managed through the admin console.

2. From the *Auto Update* list, select **Stop auto-updates**.

3. Select **Save**.

How to Limit Chrome OS Updates to a Specific Version

This section describes how to limit Chrome OS updates to a specific version.

1. Display the Device Settings page by following the procedure in ***Manage device settings***, https://support.google.com/chrome/a/answer/1375678. The steps in that procedure assume that your Chromebooks are managed through the admin console.

2. From the *Auto Update* list, select **Allow auto-updates**.

3. From the *Restrict Google Chrome version to at most* list, select the required version.

4. Select **Save**.

How to Install the Secure Browser for Chrome OS Using Advanced Methods

This document contains additional installation instructions for installing the Secure Browser for Chrome OS.

Note: Chromebooks manufactured in 2017 or later must have an Enterprise or Education license to run in kiosk mode, which is necessary to run the Secure Browser.

How to Install SecureTestBrowser (formerly AIRSecureTest) as a Kiosk App on Managed Chromebooks

These instructions are for installing the SecureTestBrowser (formerly AIRSecureTest) Secure Browser as a kiosk app on domain-managed Chromebook devices. The steps in this procedure assume that your Chromebooks are already managed through the admin console.

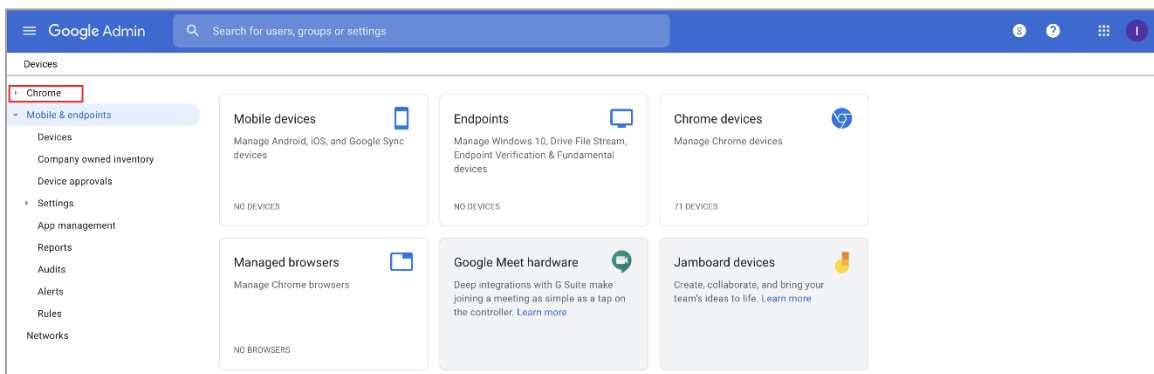SecureTestBrowser (formerly AIRSecureTest) is not compatible with public sessions.

1. As the Chromebook administrator, log in to your admin console (https://admin.google.com)
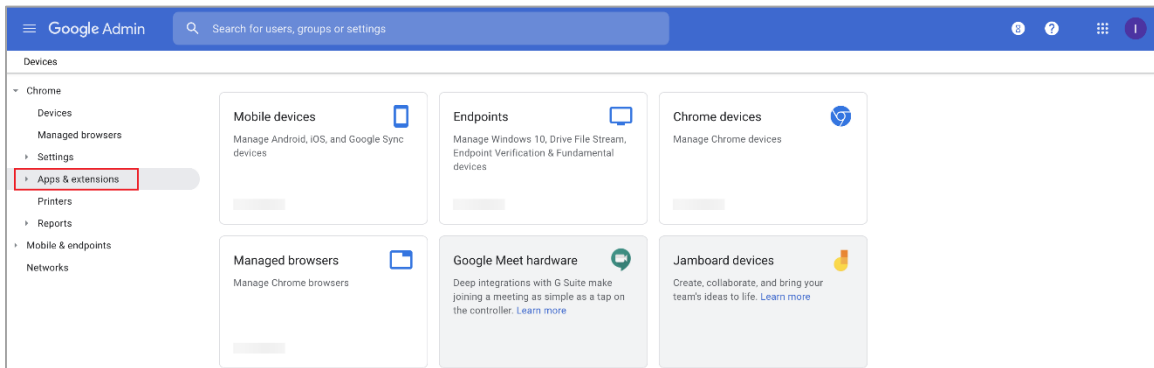
Figure 1. Google Admin Console
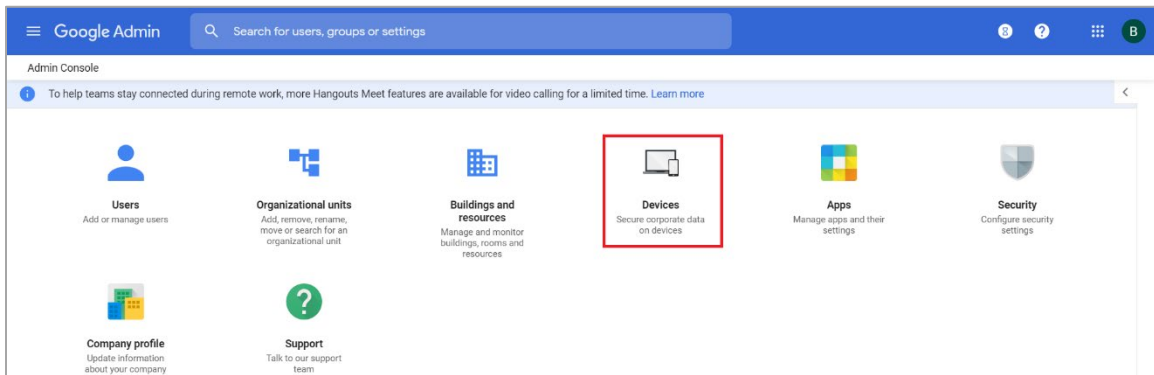
2. Select **Devices**. The *Devices* page appears.

Figure 2. Devices Page

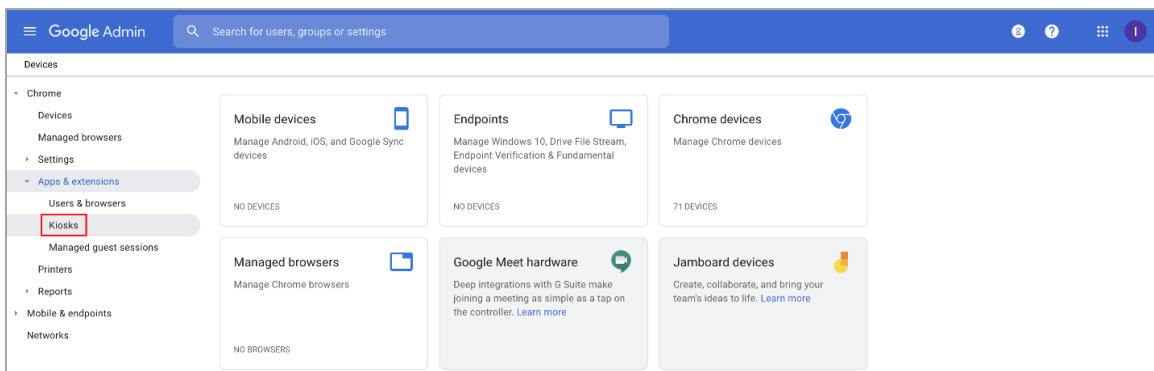**3.** Select **Chrome**. The *Chrome* drop-down list appears.
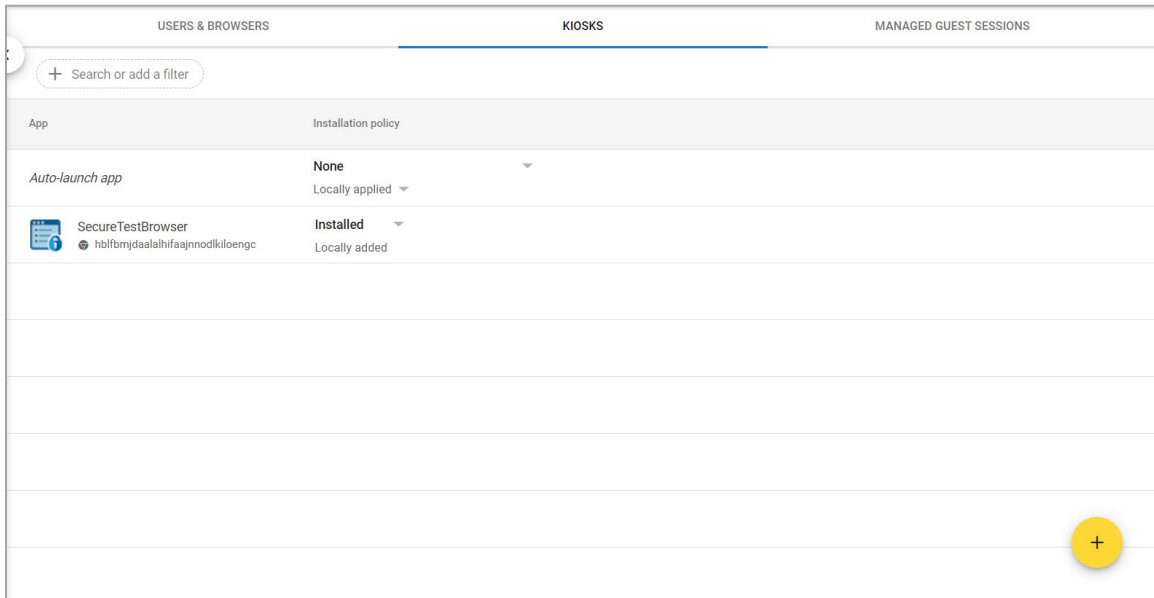
Figure 3. Chrome Drop-down List

4. From the *Chrome* drop-down list, select **Apps & extensions**. The *Apps & extensions* drop-down list appears.

Figure 4. Apps & extensions Drop-down List

5. From the *Apps & extensions* drop-down list, select **Kiosks**. The *Apps & Extensions* page appears, displaying the *Kiosks* tab.

Figure 5. Apps & extensions page – Kiosks tab

6. Remove any previous versions of the apps that appear by selecting the app name to display the app settings and then selecting 🗑 . These may appear as SecureTestBrowser or AIRSecureTest.

Figure 6. App Settings

7. Close app settings.
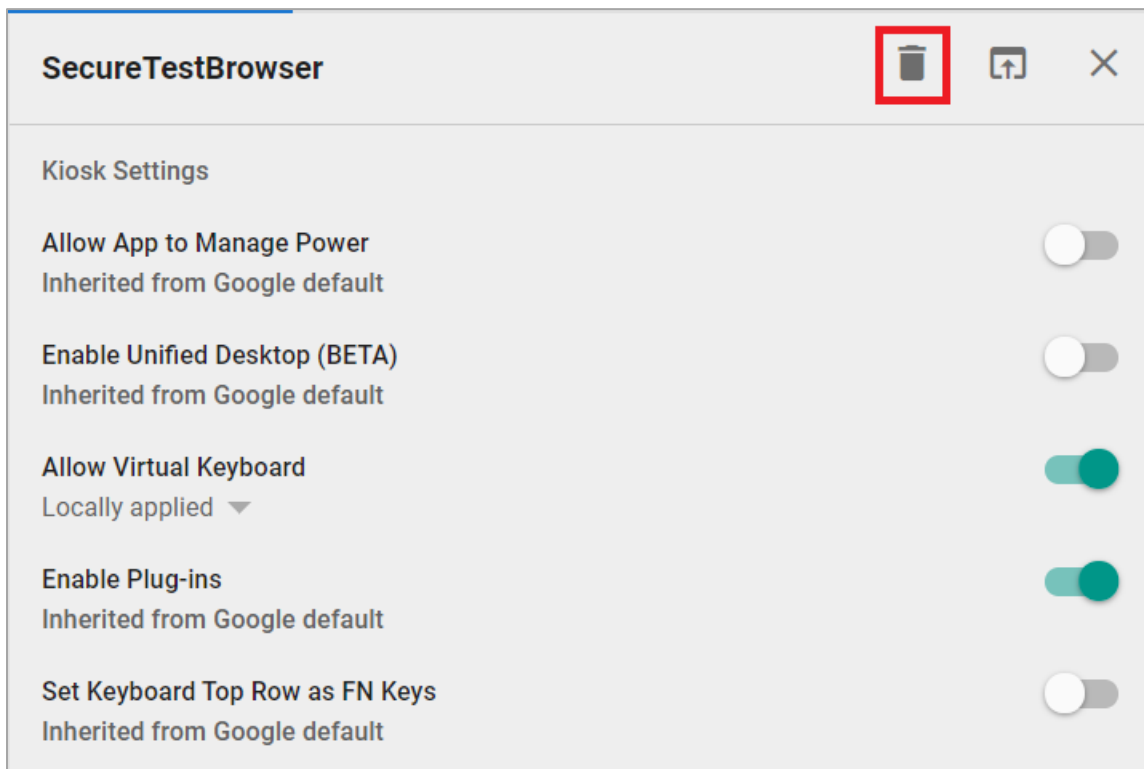
How to Install the Secure Browser for Chrome OS Using Advanced Methods

8. Hover over ⊕ to display options to add a new app.

9. Select ▦ to add a Chrome app or extension by ID. The **Add Chrome app or extension by ID** window appears.

10. Enter `hblfbmjdaalalhifaajnnodlkiloengc` in the *Extension ID* field.

11. Ensure **From the Chrome Web Store** is selected from the drop-down list.

Figure 7. Add Chrome app or extension by ID
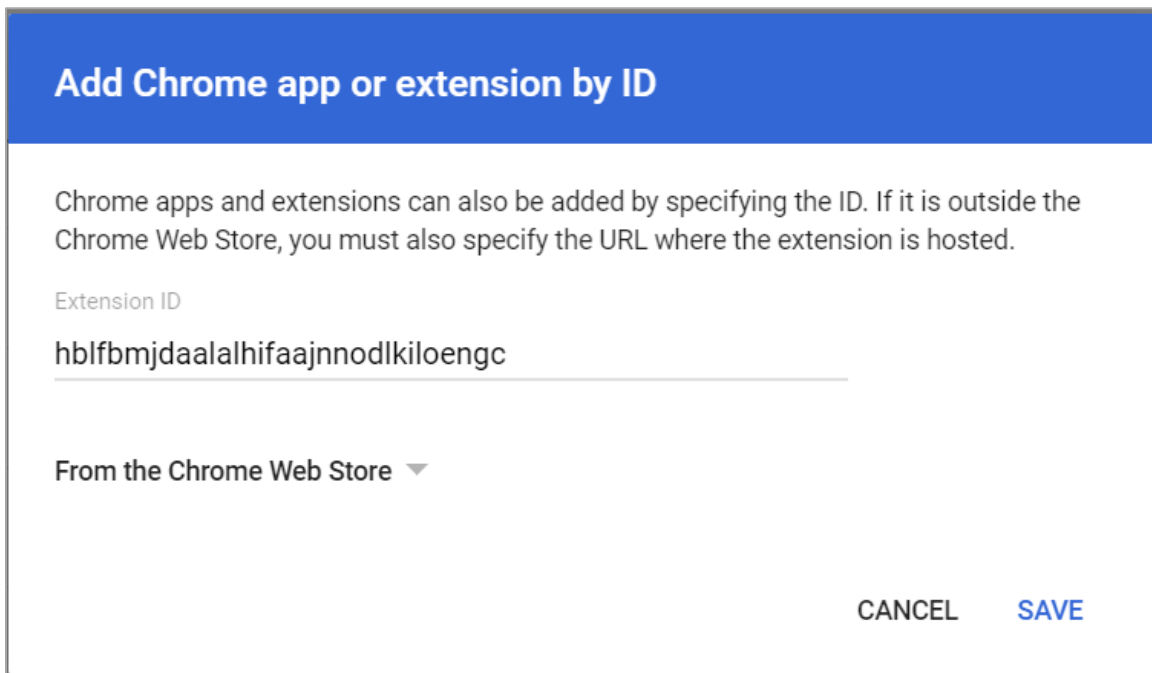
12. Select **Save**. The SecureTestBrowser (formerly AIRSecureTest) app appears in the app list.

13. Ensure **Installed** is selected from the *Installation Policy* drop-down list.

The SecureTestBrowser (formerly AIRSecureTest) app will be installed on all managed devices the next time each managed device is turned on.

How to Install the Secure Browser for Chrome OS Using Advanced Methods

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://la.portal.cambiumast.com/
Single Sign-On System	https://sso2.cambiumast.com/auth/realms/louisiana/account
Test Information Distribution Engine	https://la.tide.cambiumast.com/
Reporting System	https://la.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

Required Ports and Protocols for Online Testing

Table 3 lists the ports and protocols used by the Test Delivery System. Ensure that all content filters, firewalls, and proxy servers are open accordingly.

How to Configure Networks for Online Testing

Table 3. 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 Networks for Online Testing

Change Log

Location	Change	Date