ELPA21
English Language Proficiency Assessment for the 21st Century

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

For Technology Coordinators

2019-2020

Published July 10, 2019

Updated October 24, 2019

Prepared by Cambium Assessment, Inc.

Cambium Assessment

Table of Contents

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 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	iowaelpa21.portal.cambiumast.com
Single Sign-On System	sso2.cambiumast.com/auth/realms/iowa/account
Test Information Distribution Engine	ia.tide.cambiumast.com/
Online Reporting System	ia.reports.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 Ports and Protocols are Required 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.

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 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 4. The values in the Patterned column are preferred because they are more robust.

Table 4. 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 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.

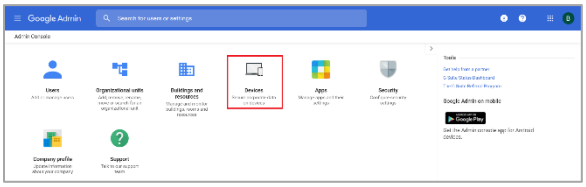
How to Install Secure Test (formerly AIRSecureTest) as a Kiosk App on Managed

These instructions are for installing the Secure Test (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.

Secure Test (formerly AIRSecureTest) is not compatible with public sessions.

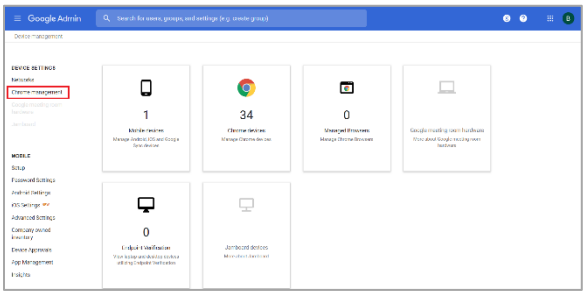
1. As the Chromebook administrator, log in to your admin console (https://admin.google.com)

Figure 1. Google Admin Console



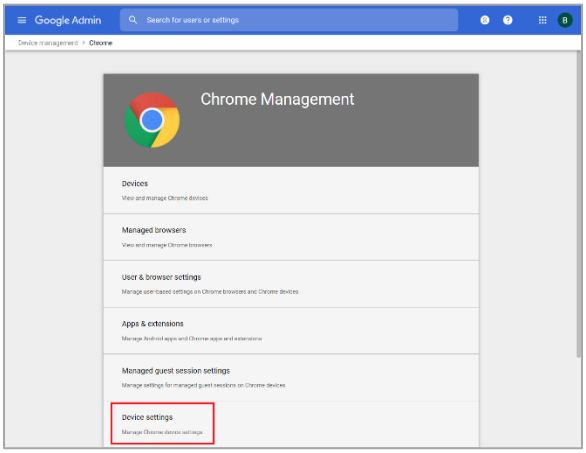
2. Click **Devices**. The ***Device management*** page appears.

Figure 2. Device management Page



3. Under **Device Settings**, click **Chrome management**. The ***Chrome Management*** page appears.

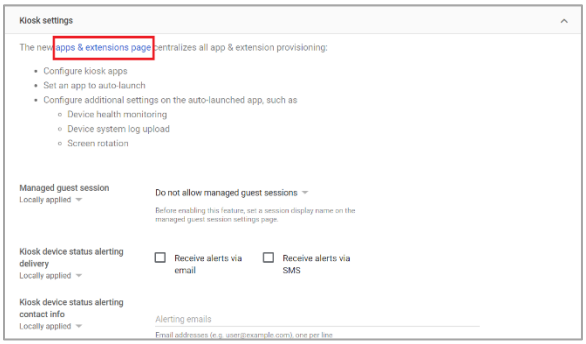
Figure 3. Chrome Management Page



4. Click **Device Settings**. The ***Device Settings*** page appears.

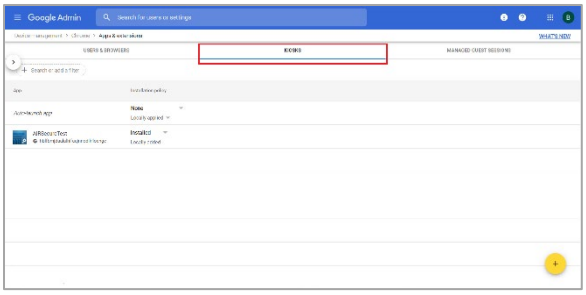
5. Scroll down to **Kiosk Settings**.

Figure 4. Kiosk Settings



6. Click **apps & extensions page**. The ***Apps & extensions*** page opens, displaying the ***Kiosks*** tab. If the ***Kiosks*** tab is not displayed, click **Kiosks** to display it.

Figure 5. Apps & extensions page – Kiosks tab

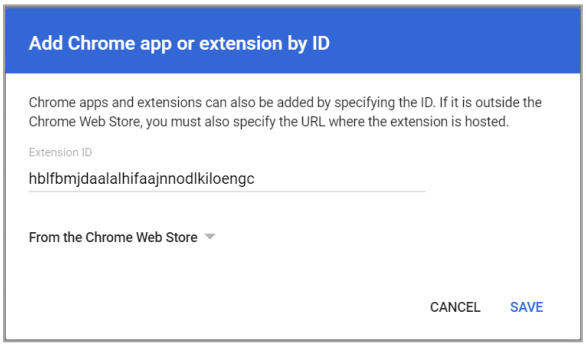


7. Remove any Secure Test (formerly AIRSecureTest) apps that appear by clicking the app name to display the app settings and then clicking  .
8. Click **X** to close app settings.

Figure 6. App Settings

9. Hover over  to display options to add a new app.
10. Click  to add a Chrome app or extension by ID. The ***Add Chrome app or extension by ID*** window appears.
11. Enter `hblfbmjdaalalhifaajnnodlkiloengc` in the *Extension ID* field.
12. Ensure **From the Chrome Web Store** is selected from the drop-down list.

Figure 7. Add Chrome app or extension by ID



13. Click **Save**. The Secure Test (formerly AIRSecureTest) app appears in the app list.
14. Ensure **Installed** is selected from the *Installation Policy* drop-down list.

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

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 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. Click **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. Click **Save**.

Appendix A. Change Log

Change	Location	Date
Updated the steps to install Secure Test (formerly AIRSecureTest) as a Kiosk App on Chromebooks	"How to Install Secure Test (formerly AIRSecureTest) as a Kiosk App on Managed Chromebooks" Section	10/24/19