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

For Technology Coordinators

2019-2020

Published July 17, 2019

Prepared by the American Institutes for Research®

Table of Contents

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 AIR 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 Nontesting Sites to Whitelist

Table 1 lists URLs for nontesting sites, such as the Test Information Distribution Engine (TIDE) and Online Reporting System (ORS).

Table 1. AIR URLs for Non-Testing Sites

System	URL
Portal and Secure Browser installation files	oh.portal.airast.org
Single Sign-On System	sso1.airast.org
Test Information Distribution Engine	oh.tide.airast.org
Online Reporting System	oh.reports.airast.org

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, AIR strongly encourages you to whitelist at the root level. This requires using a wildcard.

Table 2. AIR URLs for Testing Sites

System	URL
TA and Student Testing Sites	*.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. 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).

How to Configure for Domain Name Resolution

Table 1 and Table 2 list the domain names for AIR'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

AIR'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 due to use of the wildcard (*).

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.

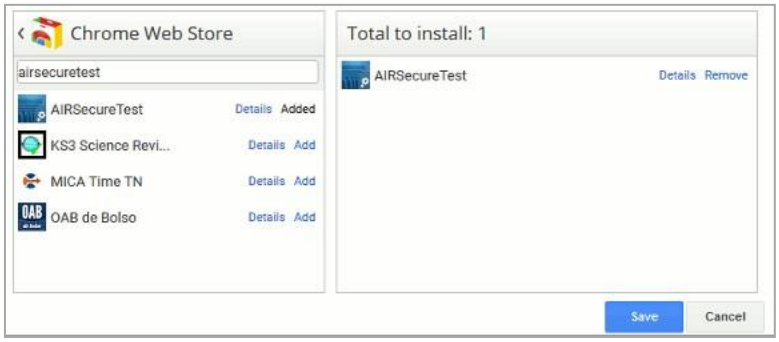
How to Install AIRSecureTest as a Kiosk App on Managed Chromebooks

These instructions are for installing the 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.

AIRSecureTest is not compatible with public sessions.

1. As the Chromebook administrator, log in to your admin console (https://admin.google.com).
2. Click **Device management**. The Device management page appears.
3. In the left side of the page, click **Chrome management**, and in the next page click **Device settings**.
4. In the ***Device settings*** page, scroll down to the *Kiosk Settings* section.
5. Click **Manage Kiosk Applications**. The ***Kiosk Apps*** window appears (see Figure 1).

Figure 1. Kiosk Apps Window



6. If any AIRSecureTest apps appear in the right column, remove them by clicking **Remove**.
7. Add the AIRSecureTest app by doing the following:
    a. Click **Manage Kiosk Applications**. The ***Kiosk Apps*** window appears.
    b. Click **Chrome Web Store**.
    c. In the search box, enter AIRSecureTest and press **Enter**. The AIRSecureTest app appears.
    d. Click **Add**. The app appears in the *Total to install* section.
    e. Click **Save**. The AIRSecureTest application appears on all managed Chromebook devices.

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. AIR 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. 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**.