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®

Descriptions of the operation of the Test Information Distribution Engine, Test Delivery System, and related systems are property of the American Institutes for Research (AIR) and are used with the permission of AIR.
# Table of Contents

Configurations, Troubleshooting, and Advanced Secure Browser Installation for Chrome OS .................................................................................................................................................. 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 ........................................................................................................................ 4

How to Install the Secure Browser for Chrome OS Using Advanced Methods ............................................................. 5
  How to Install AIRSecureTest as a Kiosk App on Managed Chromebooks .............................................................................. 5

How to Configure Chrome OS Workstations for Online Testing .......................................................................................... 6
  How to Manage Chrome OS Auto-Updates ............................................................................................................................... 6
  How to Disable Auto-Updates for Chrome OS .......................................................................................................................... 6
  How to Limit Chrome OS Updates to a Specific Version ......................................................................................................... 6
Configurations, Troubleshooting, and Advanced Secure Browser Installation for Chrome OS

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 Non-testing Sites to Whitelist

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

<table>
<thead>
<tr>
<th>System</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Portal and Secure Browser installation files</td>
<td>oh.portal.airast.org</td>
</tr>
<tr>
<td>Single Sign-On System</td>
<td>sso1.airast.org</td>
</tr>
<tr>
<td>Test Information Distribution Engine</td>
<td>oh.tide.airast.org</td>
</tr>
<tr>
<td>Online Reporting System</td>
<td>oh.reports.airast.org</td>
</tr>
</tbody>
</table>

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>
<thead>
<tr>
<th>System</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>TA and Student Testing Sites</td>
<td>*.airast.org</td>
</tr>
<tr>
<td></td>
<td>*.tds.airast.org</td>
</tr>
<tr>
<td></td>
<td>*.cloud1.tds.airast.org</td>
</tr>
<tr>
<td></td>
<td>*.cloud2.tds.airast.org</td>
</tr>
</tbody>
</table>
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>
<thead>
<tr>
<th>Port/Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>80/TCP</td>
<td>HTTP (initial connection only)</td>
</tr>
<tr>
<td>443/TCP</td>
<td>HTTPS (secure connection)</td>
</tr>
</tbody>
</table>

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>
<thead>
<tr>
<th>Patterned</th>
<th>Fully Qualified</th>
</tr>
</thead>
<tbody>
<tr>
<td>*.thawte.com</td>
<td>ocsp.thawte.com</td>
</tr>
<tr>
<td>*.geotrust.com</td>
<td>ocsp.geotrust.com</td>
</tr>
<tr>
<td>*.ws.symantec.com</td>
<td>ocsp.ws.symantec.com</td>
</tr>
</tbody>
</table>

If your firewall is configured to check only IP addresses, do the following:


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).

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.