Table of Contents

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

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 .......................................................... 5
How to Install the Secure Browser for Chrome OS using Advanced Methods .......... 6
  How to Install Secure Test (formerly AIRSecureTest) as a Kiosk App on Managed Chromebooks .................................................................................. 6
How to Configure Chrome OS Workstations for Online Testing ............................ 9
How to Manage Chrome OS Auto-Updates ................................................................. 9
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

<table>
<thead>
<tr>
<th>System</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Portal and Secure Browser installation files</td>
<td><a href="https://de.portal.cambiumast.com/">https://de.portal.cambiumast.com/</a></td>
</tr>
<tr>
<td>Test Information Distribution Engine</td>
<td><a href="https://de.tide.cambiumast.com/">https://de.tide.cambiumast.com/</a></td>
</tr>
<tr>
<td>Online Reporting System</td>
<td><a href="https://de.reports.cambiumast.com">https://de.reports.cambiumast.com</a></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, CAI strongly encourages you to whitelist at the root level. This requires using a wildcard.

Table 2. CAI and AIR URLs for Testing Sites

<table>
<thead>
<tr>
<th>System</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>TA and Student Testing Sites Assessment Viewing Application</td>
<td>*.cambiumast.com</td>
</tr>
<tr>
<td></td>
<td>*.tds.cambiumast.com</td>
</tr>
<tr>
<td></td>
<td>*.cloud1.tds.cambiumast.com</td>
</tr>
<tr>
<td></td>
<td>*.cloud2.tds.cambiumast.com</td>
</tr>
<tr>
<td></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>
</tbody>
</table>
How to Configure Networks for Online Testing

Which URLs for Online Dictionary and Thesaurus to Whitelist

Some online assessments contain an embedded dictionary and thesaurus provided by Merriam-Webster. The Merriam-Webster URLs listed in Table 3 should be whitelisted to ensure that students can use them during testing.

Table 3. CAI URLs for Online Dictionaries and Thesauruses

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>media.merriam-webster.com</td>
<td>64.124.231.250</td>
</tr>
<tr>
<td><a href="http://www.dictionaryapi.com">www.dictionaryapi.com</a></td>
<td>64.124.231.250</td>
</tr>
</tbody>
</table>

Which Ports and Protocols are 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

<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 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 5. The values in the Patterned column are preferred because they are more robust.

Table 5. Domain Names for OCSP

<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 Secure Test (formerly AIRSecureTest) as a Kiosk App on Managed Chromebooks

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.

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

   ![Figure 1. Google Admin Console](image1.png)

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

   ![Figure 2. Device management Page](image2.png)
3. Under Device Settings, click **Chrome management**. The *Chrome Management* page appears.

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

5. Scroll down to **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.
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.

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 hblfbmjdaalalhiaajnnodlkiloengc in the Extension ID field.

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

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 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.
## Change Log

<table>
<thead>
<tr>
<th>Change</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Changed &quot;oscp&quot; to &quot;ocsp&quot; in Fully Qualified column</td>
<td>8/5/19</td>
</tr>
<tr>
<td>Updated instructions to match changes made by Google to the admin console.</td>
<td>9/30/19</td>
</tr>
</tbody>
</table>