CambiumAssessment

SecureTest PWA Browser Troubleshooting Guide

Contents

SecureTest PWA Browser Troubleshooting Guide 1

What Is the SecureTest PWA app? 1

What's new for School Year 2026-27. 2

ChromeOS General Notes. 2

General Troubleshooting Notes. 2

Upgrade SecureTest PWA to v11.1 3

SecureTest PWA Configuration Steps. 4

Common Errors due to Configuration Issues 13

BVP Failed 13

Chrome v.### or "You cannot take this test with this browser." 14

Microphone check cannot be completed 15

Unsupported OS/Browser 16

LoginShell.Alert.GetChallengeResponseFailed 17

LoginShell.Alert.GetChallengeResponseCertificateError 18

LoginShell.Alert.SecureEnvFail 19

What Is the SecureTest PWA app?

The **SecureTest Progressive Web App (PWA)** secure browser adheres to Google's requirements which require all kiosk apps to be built as a progressive web app. The SecureTest PWA browser requires multiple steps in the Google Admin Console (GAC) for it to be configured correctly for student testing. This document provides step-by-step installation instructions and a guide to how to address errors due to configuration issues.

CambiumAssessment

What's new for School Year 2026-27.

Cambium Assessment, Inc. (CAI) introduced a new, improved version of the SecureTest PWA browser (Secure v11.1) which will be required by mid-October for school year (SY) 2026-27 as the version (Secure v10.1) introduced last SY will be phased out. Please review section Upgrade SecureTest PWA to v11.1. If you are installing the SecureTest PWA browser for the first time or wish to perform a fresh installation, please go to section SecureTest PWA Configuration Steps.

ChromeOS General Notes.

The ChromeOS SecureTest PWA browser is supported on Chromebook and ChromeOS Flex devices running Chrome OS version **148 or newer in the Stable channel or version 144 or newer in the Long-Term Support (LTS) or Long-Term Candidate (LTC) channels**. Chromebooks or ChromeOS Flex devices running in Tablet Mode and tablets running ChromeOS are not supported.

The **SecureTest PWA** requires managed ChromeOS devices through either a **Chrome Enterprise Upgrade** or **Chrome Education Upgrade** subscription. If your devices are not currently managed through either subscription, please review Google's article for setup instructions.

General Troubleshooting Notes.

When installing the **SecureTest PWA** app on a root Organizational Unit (OU), verify that all sub-OUs with devices needing access to the app are configured to ***inherit*** the app and its settings from the parent OU. This applies to both the **Kiosk** & **Verified Mode** settings. The app should only be set to "locally applied" at the intended parent OU.

We recommend installing the **SecureTest PWA** app in a **Test OU** separated from your live testing environment and moving one or more test devices into this **Test OU** to validate the configuration. This ensures that the app installs and runs correctly within your **Google Admin Console** & **Network** environment.

Once the app functions properly in the **Test OU**, determine how and where to install it across your testing OUs. If issues occur in your live testing OUs, compare its settings with those in the test OU.

If you have multiple sub-OUs (for example, grouped by grade level, school, or OS version) ensure the **SecureTest PWA** app is available to each sub-OU through inheritance rather than local installation.

If students experience issues when launching or use of the **SecureTest** app, please review the "**Common Errors due to Configuration Issues**" section below. These errors are linked to misconfiguration of the SecureTest PWA app. If only a few devices in one OU are affected by errors, the issue may be device specific such as corrupt policies or app cache. This is resolved by moving devices between OUs or power washing the device to force a refresh of applied policies.

Finally, because the SecureTest browser communicates with multiple URLs, all required URLs must be in the allow lists in your content filters, firewalls, and any other device that regulates school network traffic and configured to bypass SSL inspection. Refer to the "Resources to Add to Allowlists" section of your state's Technology Guide for a complete list of required URLs.

Upgrade SecureTest PWA to v11.1

If you have SecureTest PWA v10.1 installed on your students' devices, please follow these steps to upgrade to v.11.1 which will be supported throughout SY 2026-27.

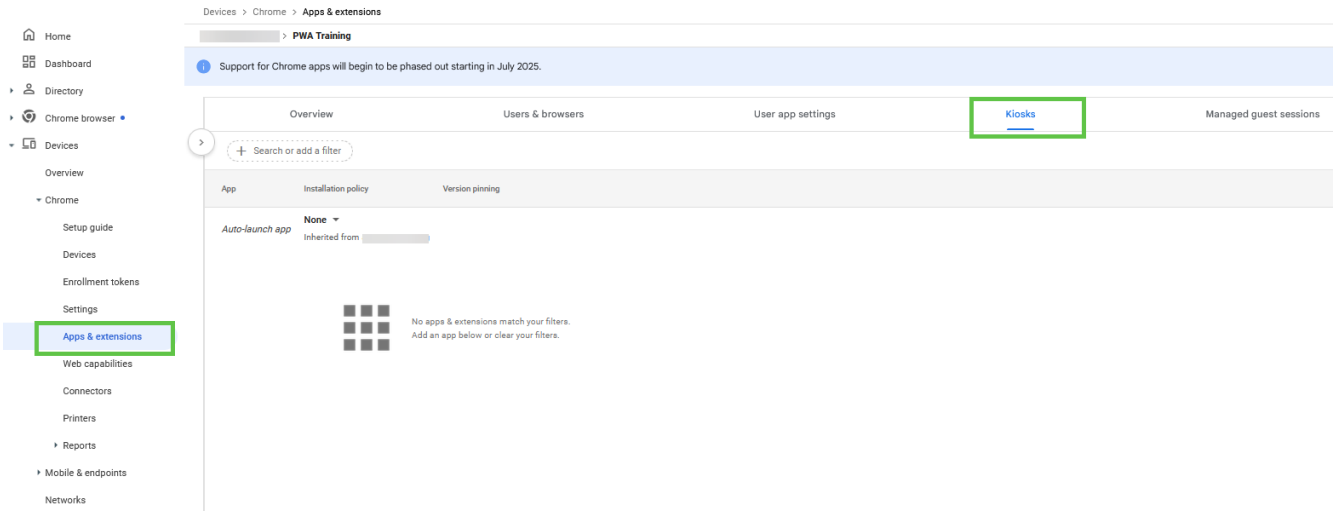
1. Log in to the Google Admin Console and navigate to the top-level OU in which the SecureTest PWA browser is installed. If the sub-OUs are properly set up to inherit the Parent OU Apps & extensions and Device settings, the upgrade will appear in all devices.
2. Navigate to Apps & Extensions -> Kiosks and then select the desired OU.
3. Select the SecureTest kiosk app for its settings menu to open on the right
4. Scroll down to the ADD EXTENSION section. If the App ID present starts with "**jgabch**", it is version 10.1 which will be supported only until October 2026.
5. Click on the trash can to delete it.
6. Click on ADD EXTENSION -> **Add from custom URL** to enter the App ID and URL for version 11.1:
   Extension ID: **cblbmnlkfgdiagbghnilmekjjlibbkmg**
   Custom URL: **https://pwa.cambiumtds.com/secure_browser.xml**
7. Hit **SAVE** in the upper right.
8. If visuals help with this change, please refer to steps 9 – 11 under the next section, *SecureTest PWA Configuration Steps*.
   NOTE: If SecureTest v10.1 is in use or open on any device at the time the upgrade is done through the GAC, it might need to be closed on the device and then launched **twice** for the device to acquire the new configuration and show "Secure v11.1" in the upper right corner.

CambiumAssessment

SecureTest PWA Configuration Steps.

1. **Log in to admin.google.com**
   Access the Google Admin Console to manage device and app policies.

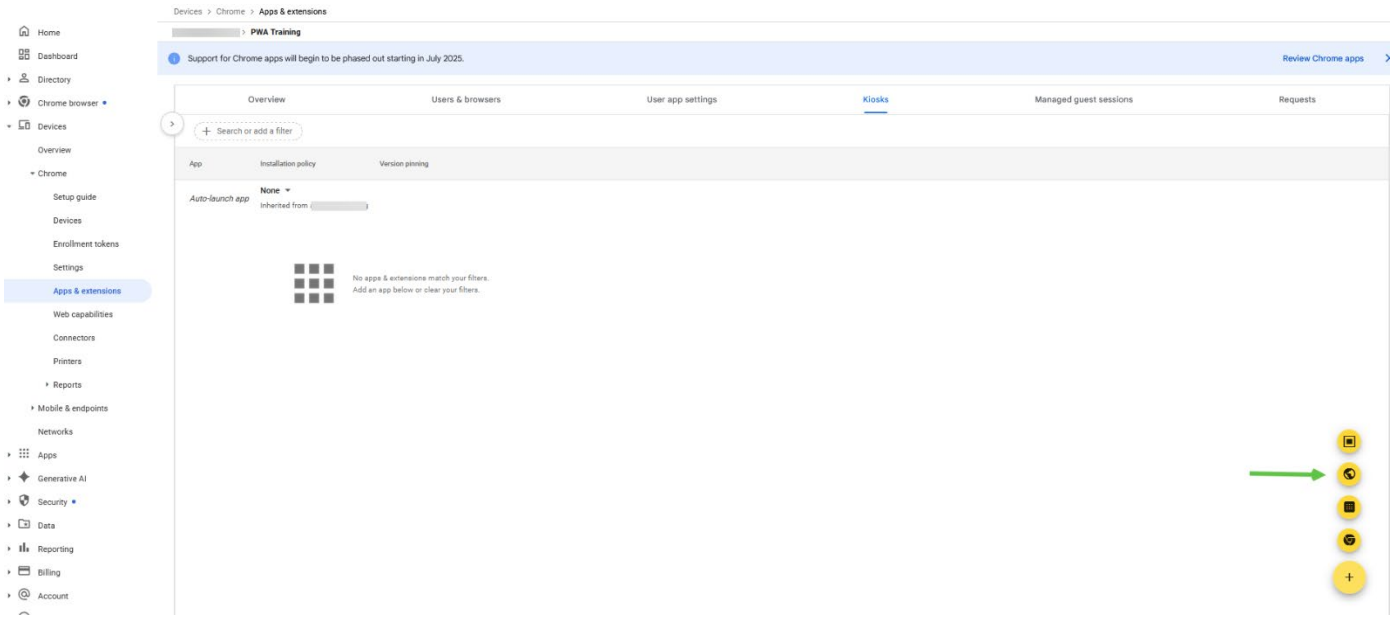
2. **Navigate to Devices > Chrome > Apps & Extensions to select the Kiosks tab on the Apps & Extensions page**
   The Kiosks tab is specifically for configuring apps that will run in kiosk mode (single-app mode).



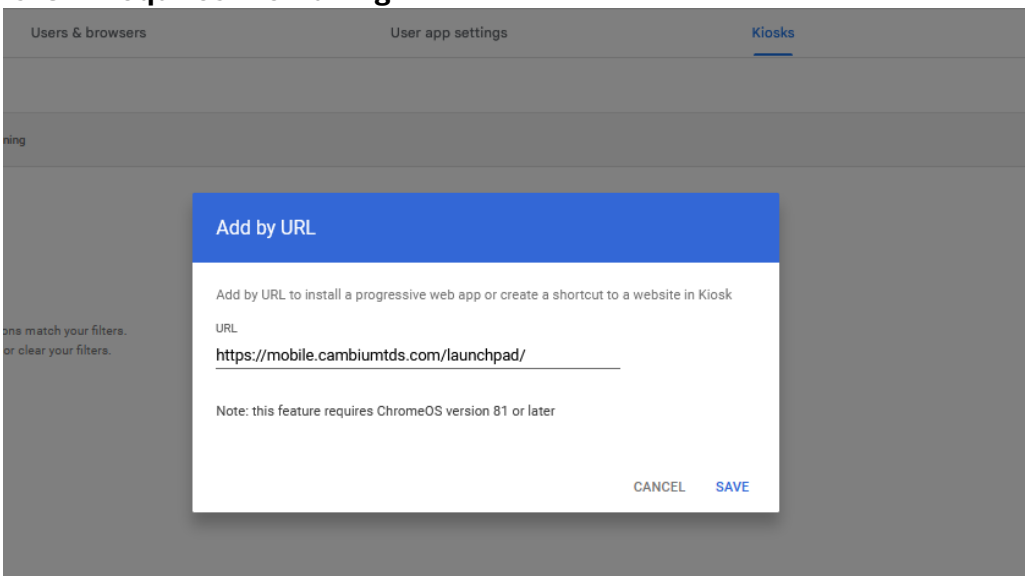
3. **Choose the Organizational Unit (OU) to add the SecureTest v.11.1 PWA.**
   Only devices within the selected OU will receive and enforce this PWA configuration.

   ***NOTE:** When troubleshooting your test device for the installation, or students' testing devices, please ensure that the serial number of the device in question is indeed located within the OU hierarchy that you are currently configuring and/or troubleshooting.*

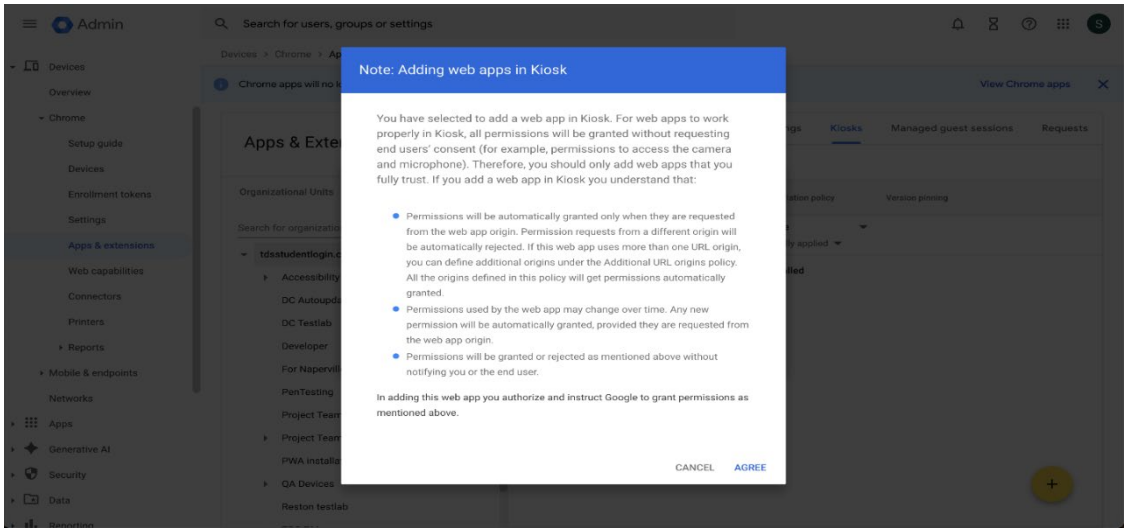
4. **Hover over the + icon on the right and click the globe icon to Add by URL.**
   This allows adding a web-based kiosk app (a PWA) using its direct URL instead of from the Chrome Web Store.



5. **Enter the Launchpad URL - https://mobile.cambiumtds.com/launchpad/ - and click Save.**
   This is the main student testing application. Adding it here enables it to run in kiosk mode.
   NOTE: This URL requires the trailing /

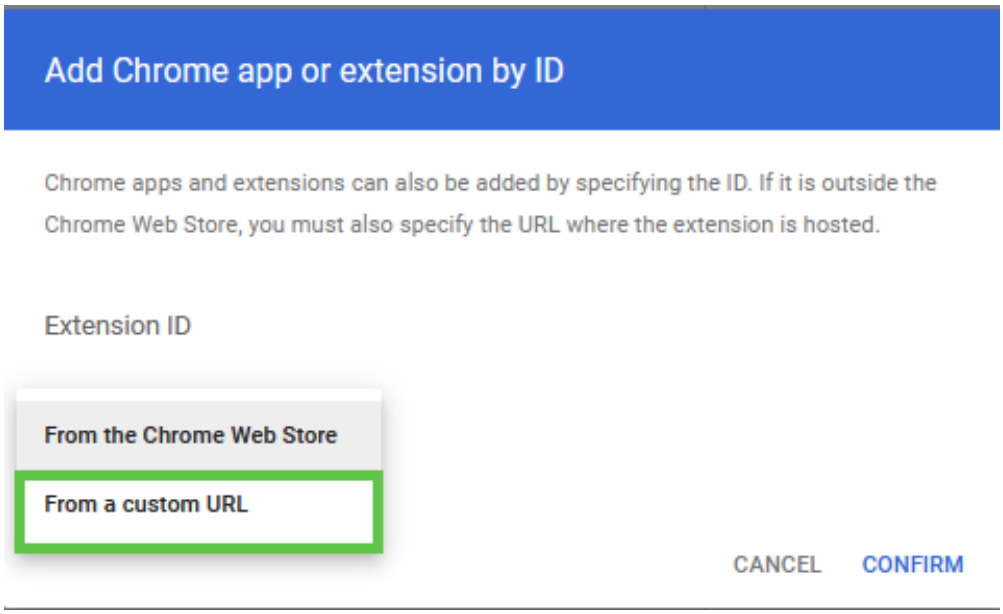


6. **Click Agree in the dialog prompt confirming web app addition.**
   Google requires confirmation for adding third-party web apps in kiosk mode.



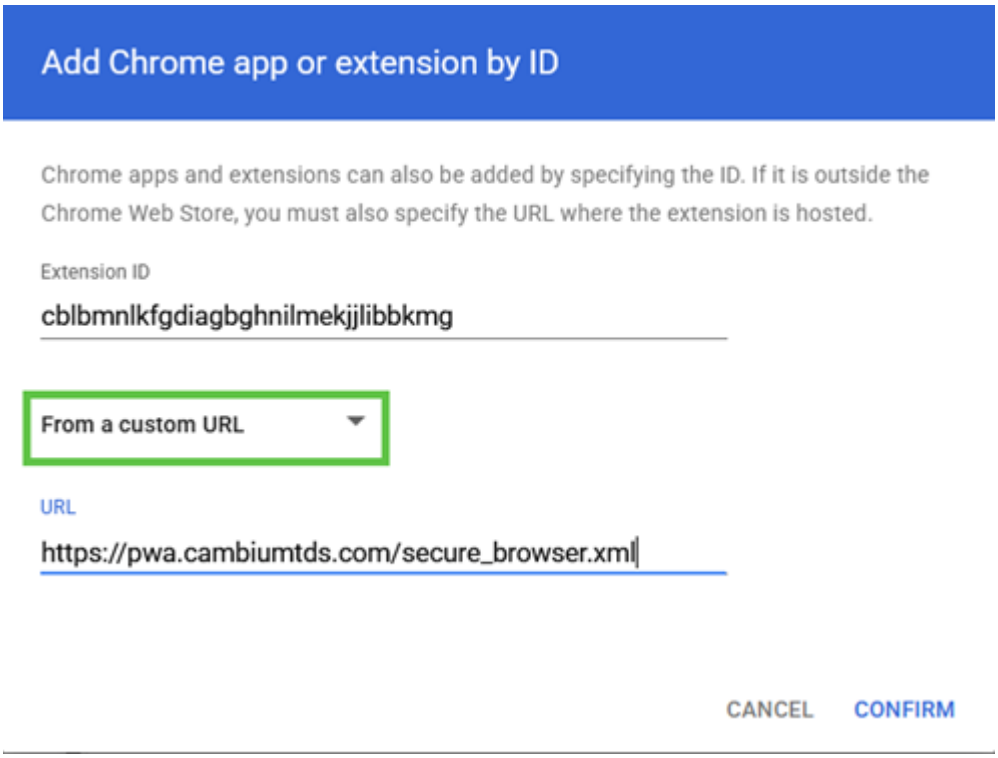
7. **In the right-hand panel, scroll to the Extensions section.**
   This section allows you to attach additional functionality (e.g., the Secure extension) to the web app.

   a. **Click Add Extension > Add from a custom URL**
   We are using a private extension (not in Chrome Web Store), so a custom URL is needed to manually specify the private extension ID. This ID activates the Chrome extension that enables kiosk security checks and lockdown features.



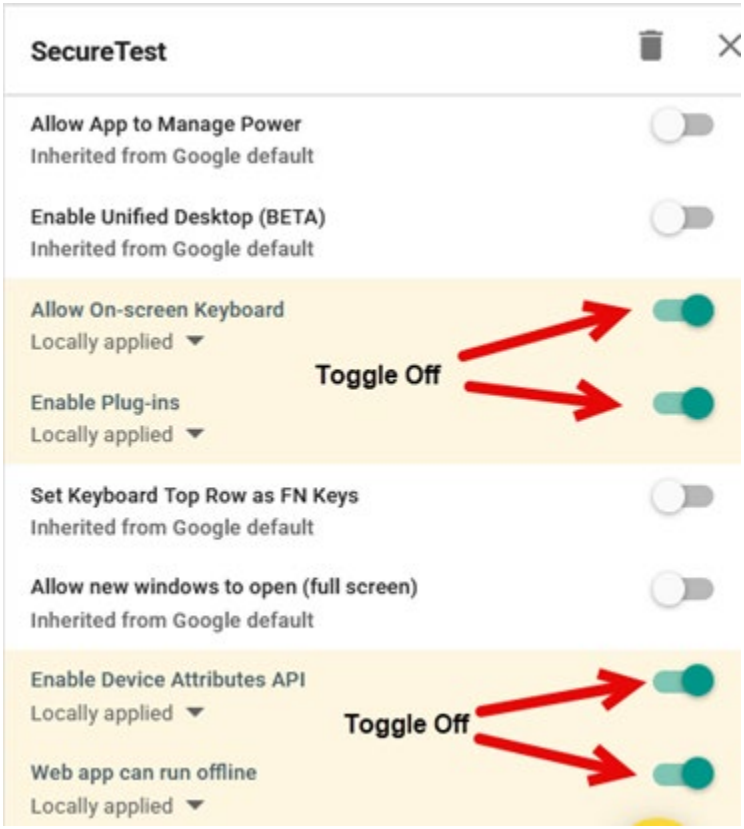
b. **Enter the following:**

1. **Extension ID: cblbmnlkfgdiagbghnilmekjjlibbkmg**
2. **Custom URL: https://pwa.cambiumtds.com/secure_browser.xml**
3. **Click SAVE.**

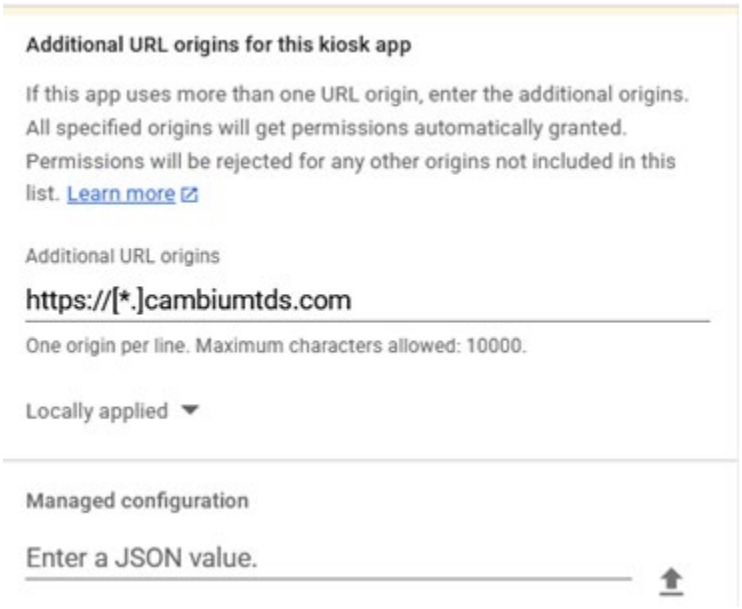


8. **Customize the SecureTest** PWA browser.

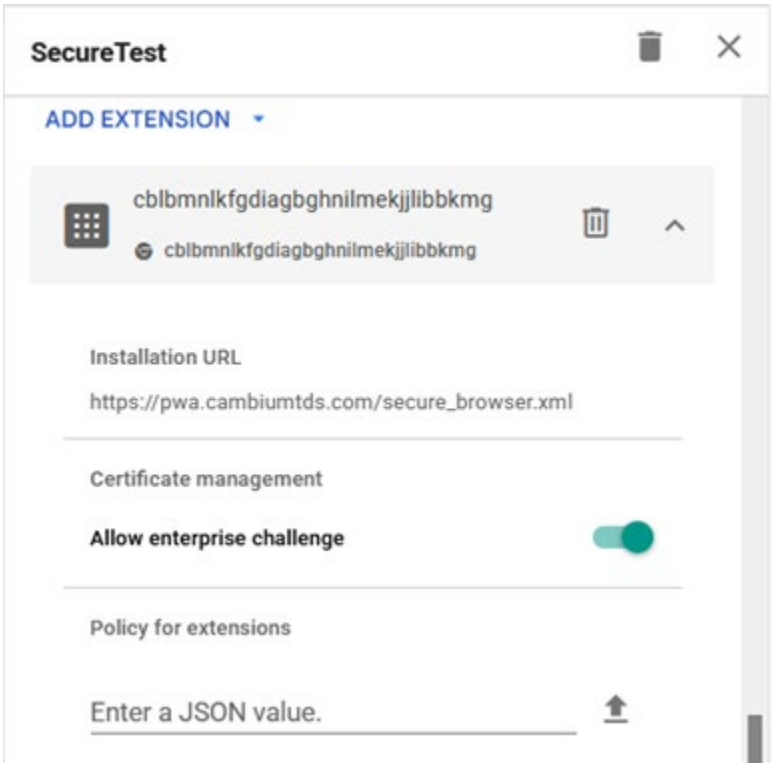
   a. Select **SecureTest** app (**Devices->Chrome->Apps & extensions-> Kiosks)** to disable all settings by toggling them off**.**



   b. Under ***Additional URL origins for this kiosk app***, add Additional URL Origins**:**
   https://[*.]cambiumtds.com
   This domain is required to load media content (e.g., videos, audio) through the SecureTest browser. Without the URL, media playback will fail. **Click Save in the top-right to apply for changes.**

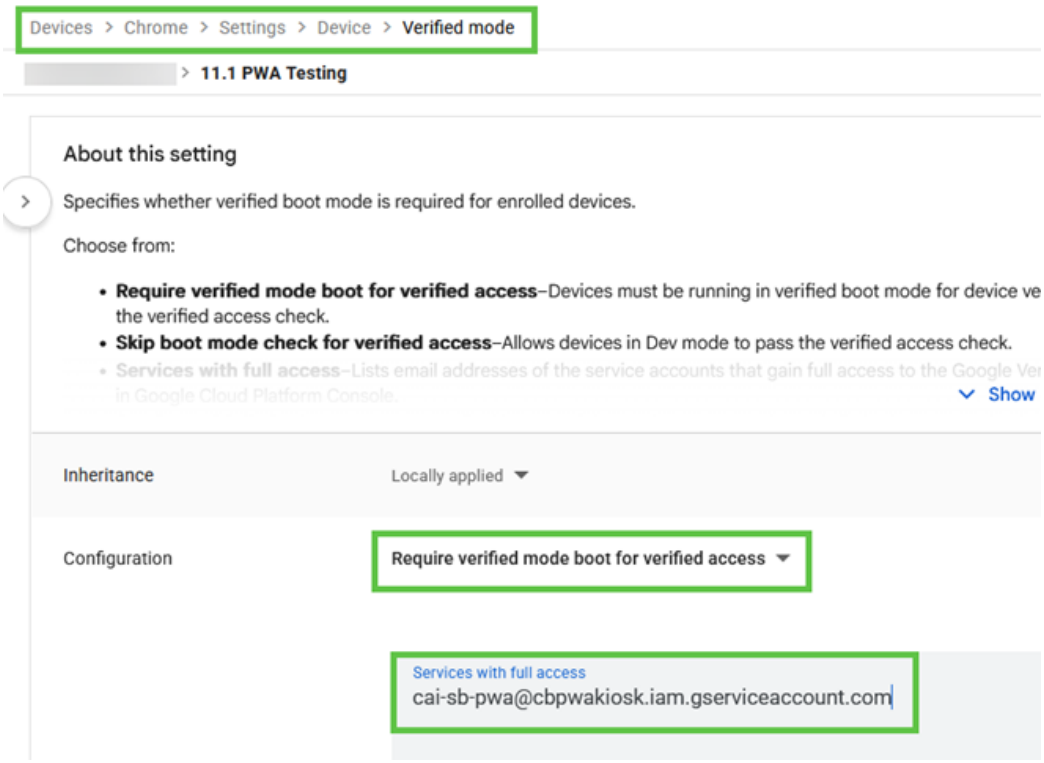


c. Verify '**Allow enterprise challenge**' (by expanding the **Extension ID** section) setting is enabled for the SecureTest extension.



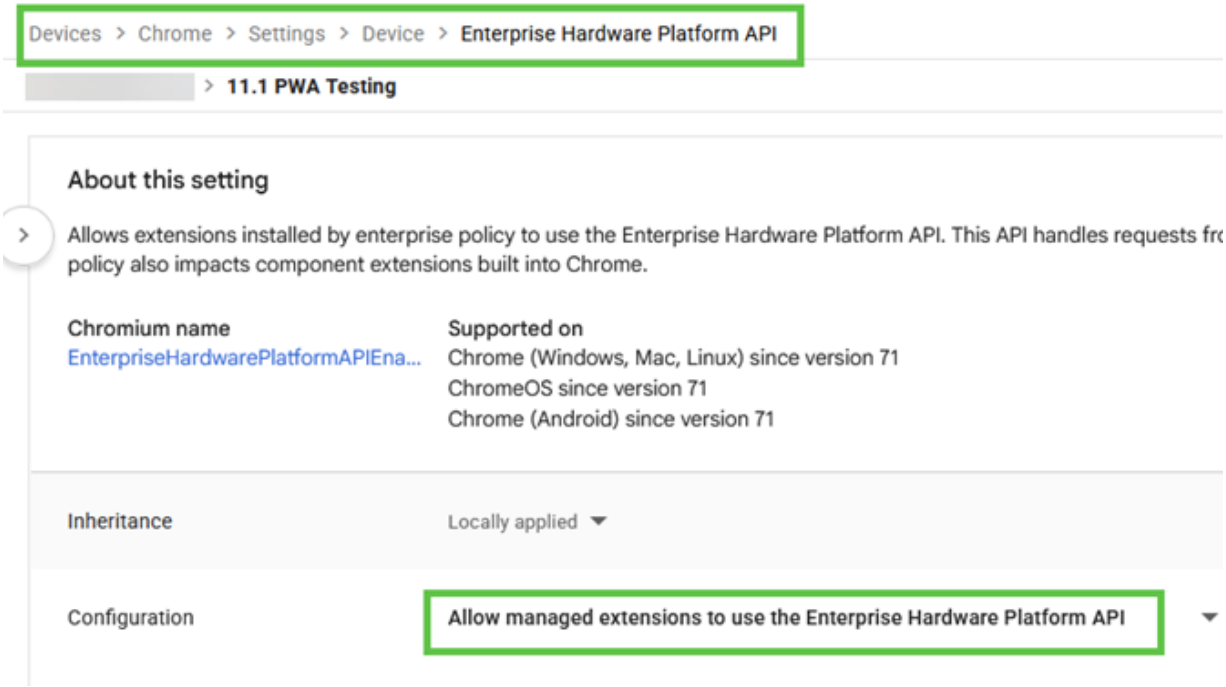
9. **Verified Mode Setup** [**Required**]
   Verified Mode ensures that only enrolled, trusted ChromeOS devices can run the SecureTest PWA secure browser, helping to maintain a secure and authenticated testing environment. It also enables service account authorization needed for secure media and content access.

    1. **Go to Devices > Chrome > Settings:**
        a. Choose the Organizational Unit used for the previous Secure Test PWA installation steps.
        Only devices in this OU will have verified access enforced.
        b. Click **Device settings** tab.
        This is where security-related configurations are applied to managed devices.
        c. Under Enrollment and access, locate **Verified mode**.
        Verified mode checks to ensure the ChromeOS device is secure and enrolled properly.
        d. Set configuration to: ***Required verified mode boot for verified access***.
        Devices must be running in verified boot mode for device verification to succeed.
        Devices in Dev mode will always fail the verified access check.
        e. Add the Verified Mode Service Account:
        cai-sb-pwa@cbpwakiosk.iam.gserviceaccount.com to **Services with full access** accounts list.
        This service account is required to authenticate and authorize secure operations during the session.
        f. Click Save at the bottom of the page to finalize Verified Mode configuration for the selected OU.

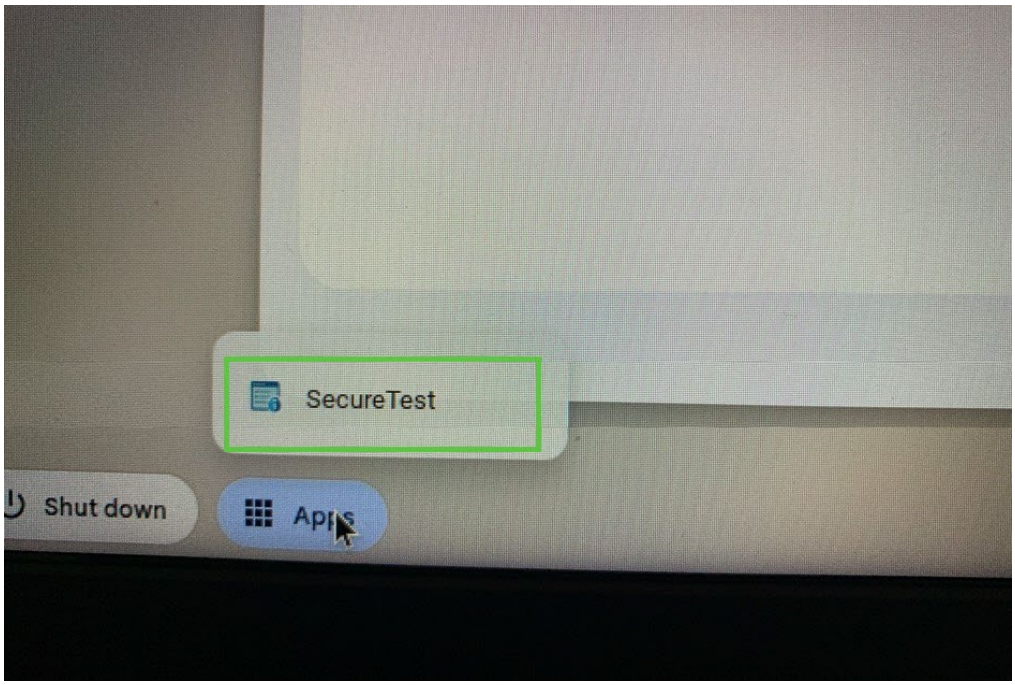


10. **Enable Hardware Platform API [Required]**

a. Navigate to **Devices > Chrome > Settings > Device settings** in your Google Admin Console
b. Select the OU in which the SecureTest browser was installed.
c. Under Device settings scroll to **Kiosk settings**
d. Set **Enterprise Hardware Platform API** to '*Allow managed extensions to use the Enterprise Hardware Platform API*'
e. Click **Save** at the bottom of the page.



11. **Verification** - To verify your settings are correct, go to a ChromeOS device that is in the OU in which the **SecureTest** browser was installed to validate **SecureTest** is present in the Apps tray, and once launched it shows **Secure v11.1** in the upper right corner and that it is working as expected by accessing a practice test.

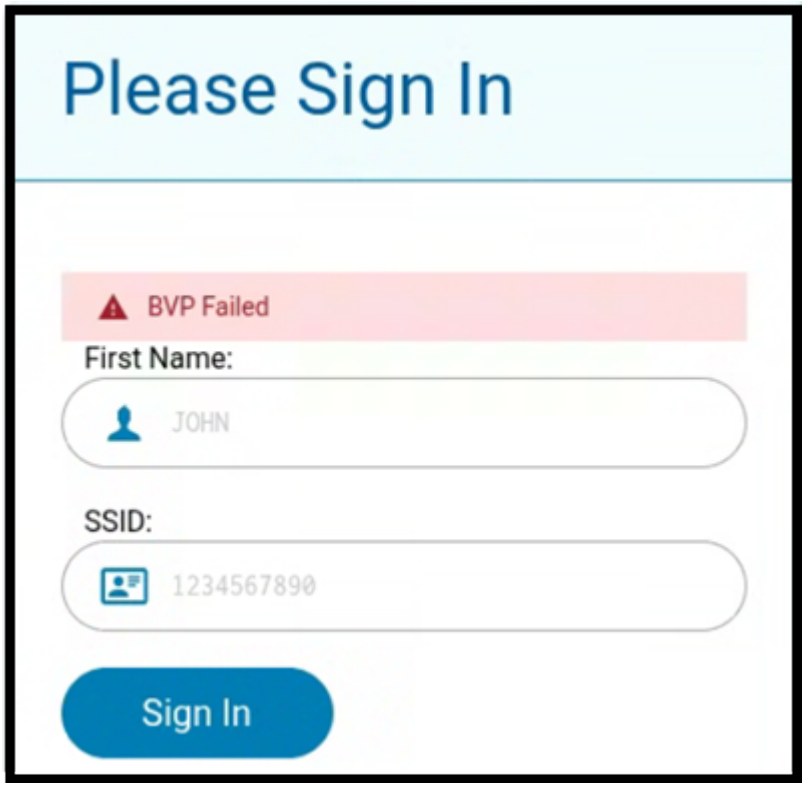


Common Errors due to Configuration Issues

A general note about each of the errors below and their resolutions. While each resolution has been thoroughly validated to address the error once applied and devices restarted, each district or school's set up is unique to them. As such, there might be times when changes to settings or configurations will require additional steps. Again, based on our own testing, we have found that moving devices between Organizational Units (OUs) has been effective in forcing a refresh of app settings and device policies. In extreme circumstances, factory resetting (power washing) may be needed when one or a few of many devices in any given OU continue to exhibit the error. Resetting the devices clears out corrupt policies/settings.

BVP Failed

BVP Failed appears on the login screen.

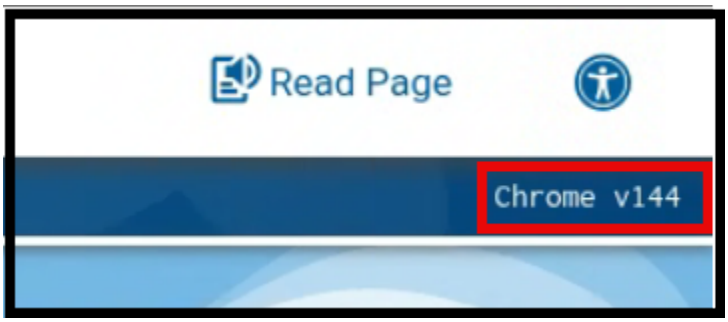


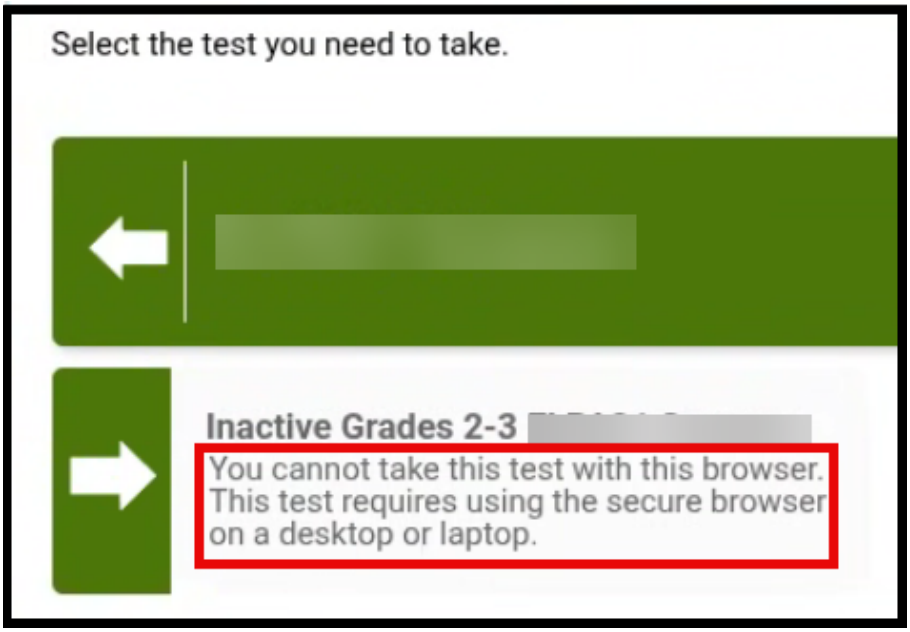
Root Cause: Verified Mode account is not present or not set correctly.

Resolution: Review **Step #9** to set the account required for **Verified Mode.**

Chrome v.### or "You cannot take this test with this browser."

PWA secure browser shows **"Chrome v.###"** in the upper right corner instead of "**Secure v11.1**" **OR** student sees "**You cannot take this test with this browser**" message in the test selection page.



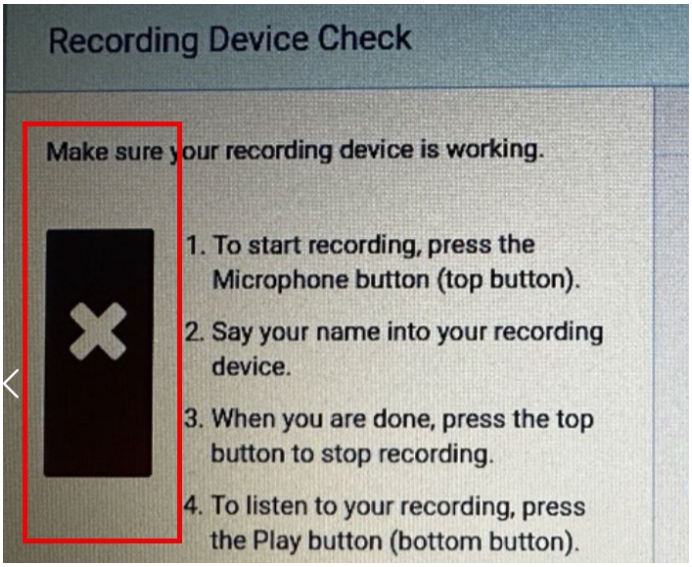


Root Cause: The **Extension ID** and/or the **custom URL** is/are missing.

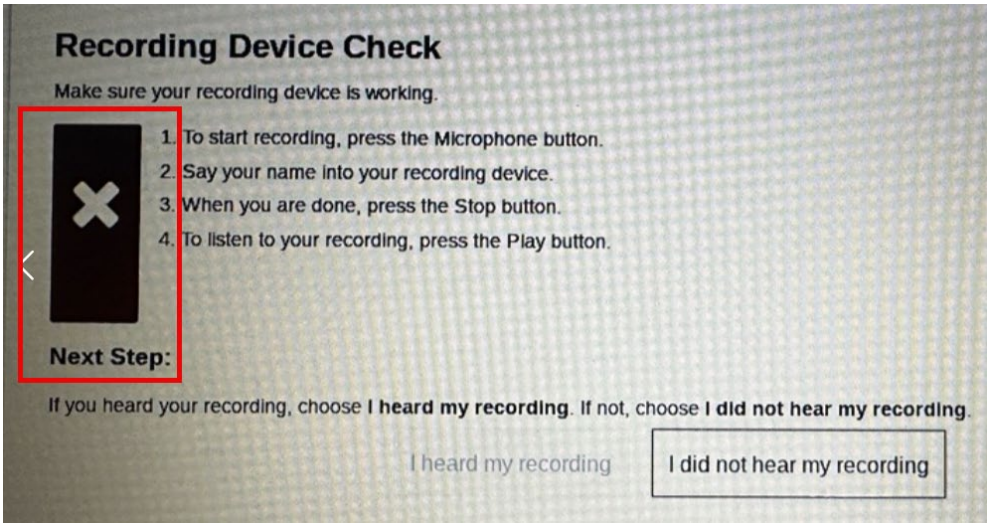
Resolution: Review Step #7 and Step #8. If there is an Extension showing after selecting SecureTest, delete the extension to add it anew. Restart the device(s) with the error.

Microphone check cannot be completed

Students using Speech-to-Text (STT) or tests requiring a microphone check, see a big X on the microphone check, either before entering the test or on the diagnostic page.



OR

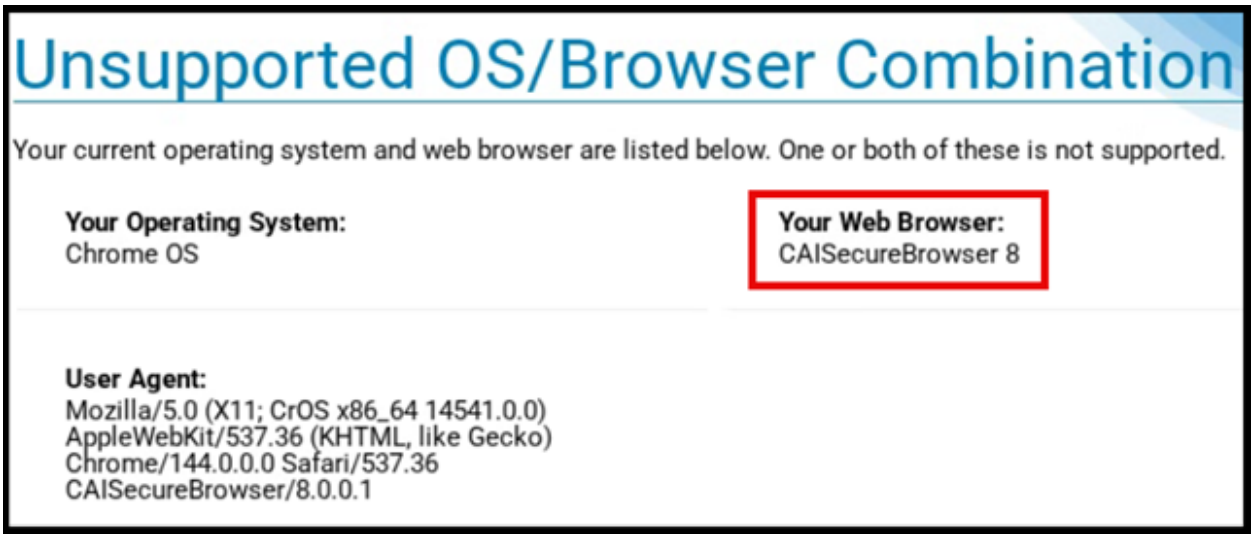


Root Cause: Settings per **Step #8** were not completed.

Resolution: Review **Step #8** for all OUs in which the SecureTest was installed and restart the affected devices.

Unsupported OS/Browser

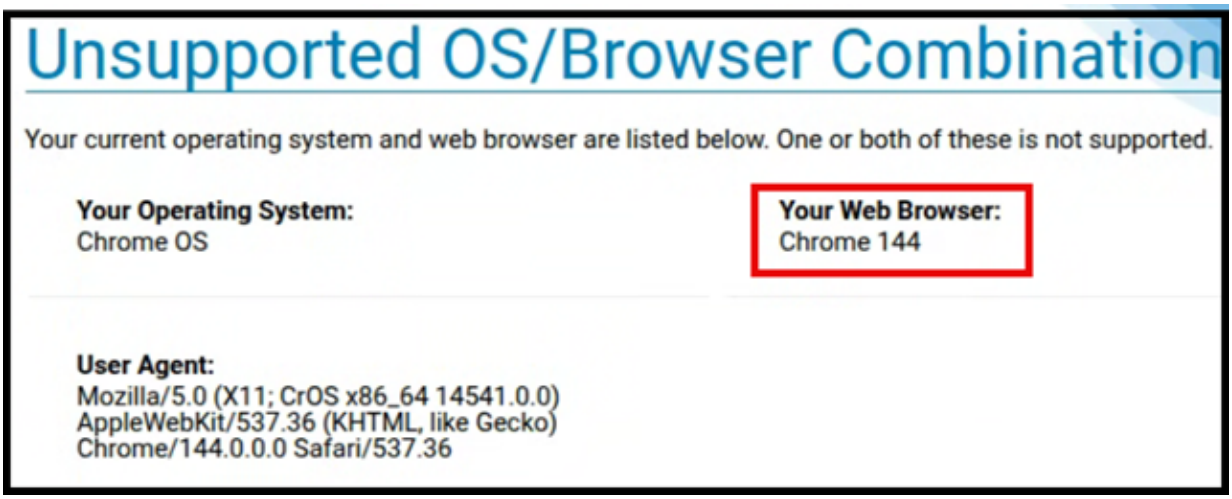
A. **Unsupported OS/Browser page on ChromeOS version 144 + shows "Your Web Browser:" as "CAISecureBrowser 8"**



Root Cause: Students are trying to use the legacy, deprecated kiosk SecureTestBrowser v.8

Resolution: Remove the SecureTestBrowser v.8 as it is no longer supported. Guide students to use the SecureTest browser or if not installed, install it according to the instructions listed above.

B. **Unsupported OS/Browser page shows "Your Web Browser:" as "Chrome ###"**

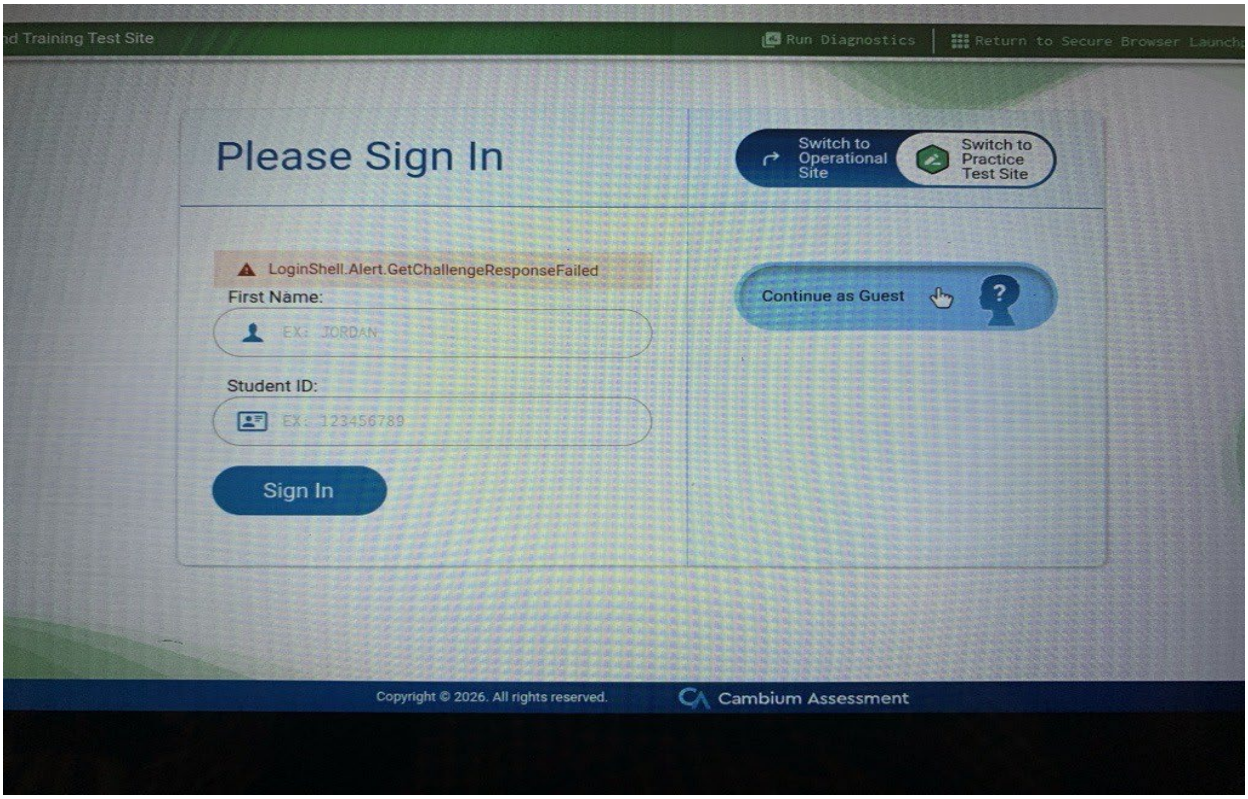


Root Cause: SecureTest v.11.1 is showing Chrome browser version due to misconfigured extension.

Resolution: Remove and reinstall the extension as per Step #7 and then restart the device(s) with the error.

LoginShell.Alert.GetChallengeResponseFailed

Student or Guest user login attempts on **Chromebooks** result in **LoginShell.Alert.GetChallengeResponseFailed**.

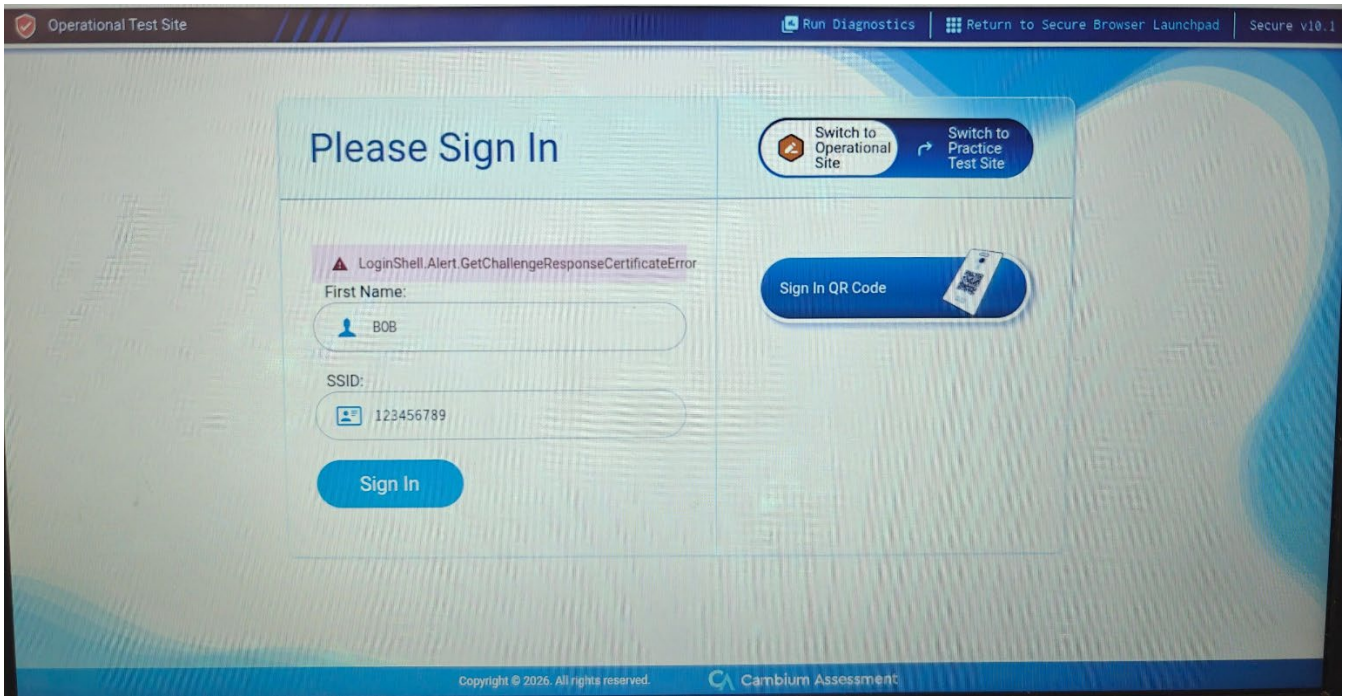


Root Cause: The **Allow enterprise challenge** setting as per **Step #8** was not set.

Resolution: Review **Step #8** for all OUs in which the SecureTest was installed.
If the **Allow enterprise challenge** setting is showing as enabled but the error persists, delete the extension to add it anew as per Step #7 and Step #8.

LoginShell.Alert.GetChallengeResponseCertificateError

Student or Guest user login attempts on **ChromeOS Flex** result in **LoginShell.Alert.GetChallengeResponseCertificateError.**

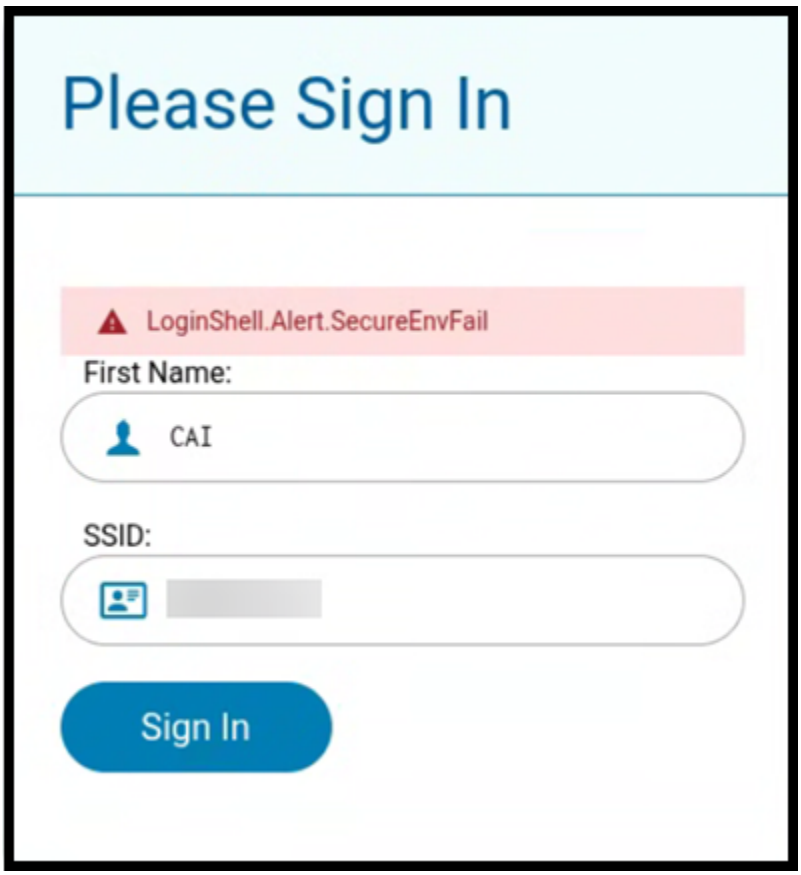


Root Cause: The **Enterprise Hardware Platform API** setting was not enabled.

Resolution: Review **Step #10** for all OUs in which the SecureTest was installed. Restart the device(s).

LoginShell.Alert.SecureEnvFail

Student or Guest user login attempts result in **LoginShell.Alert.SecureEnvFail.**



Root Cause: The SecureTest browser has more than one extension ID configured.

Resolution: Verify the extension for version 10.1 was removed before adding extension v.11.1. Review Step #7 to ensure only extension ID starting with "**cblbmn**" is present. If any other is listed, delete it.