Chromebook Guidance for Kiosk Test Security

February 2024

Who does this affect?

Schools using ChromeOS Stable Channel versions 118 and lower. Long-term Support Channel subscribers are not impacted.

What is happening?

Pearson support is providing guidance to address a potential test security issue that Google recently identified in ChromeOS Stable versions 118 and lower.

This behavior is not limited to TestNav. It can affect all Chrome devices with kiosk applications.

Google has addressed this issue through a fix provided in ChromeOS versions 114 Long Term Support (LTS) and Stable Channel versions 119 and higher; however, schools/organizations should follow Pearson guidance to implement a solution that aligns the Google update with TestNav system requirements with their technology needs/circumstances.

What does this mean?

Pearson support has tested ChromeOS versions Long-term Support 114 and Stable 119+ with TestNav. Schools/organizations should implement one of the options in the next section to address the test security risk.

What do I need to do (and how do I do it)?

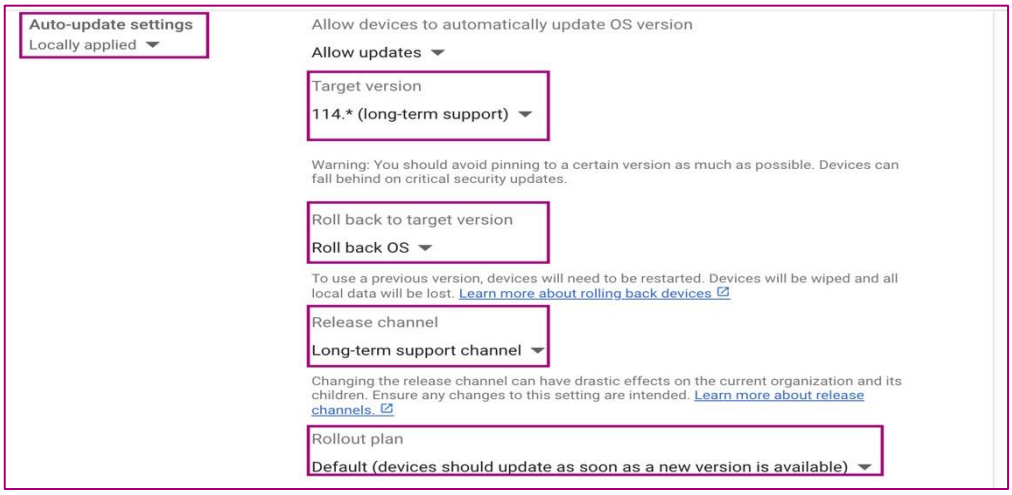
Evaluate the options provided to determine which actions best align with your school/organization, and provide the instructions below to your technology coordinator.

Option 1 - Update operating system (OS) to Long-Term Service Channel version 114 or Stable Channel 119 or higher

1. Log in to your Google Admin Console.
2. Go to **Devices > Chrome > Settings > Device settings > Device update settings.**
3. Select the desired Organizational Unit (OU) for your testing devices.
4. Perform either of the following updates for your desired ChromeOS channel. *See TestNav System Requirements for supported OS versions.*

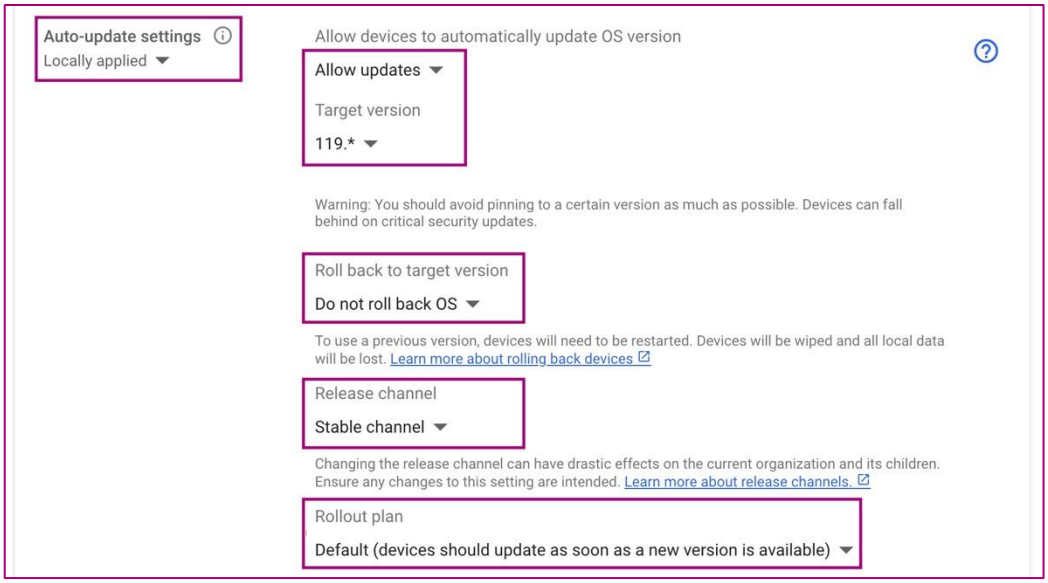
<u>Option 1A:</u> Change from Stable to Long-term Support Channel (LTS)

1. Ensure settings are applied locally if configuring settings for any OU that is not the highest level grouping for your organization.
2. Change **Release channel** to **Long-term Support Channel**.
3. If changing to LTS channel, change **Target version** to **114. * (Long-term Support).**
4. If using Stable 115+, change **Roll back to target version** to **Roll back OS**.
5. To expediate any OS changes, make sure the **Rollout plan** is set to **Default (devices should update as soon as a new version is available).**
6. Select **Save.**



<u>Option 1B:</u> Remain in Stable Channel and update to ChromeOS 119+

1. Ensure settings are applied locally if configuring settings for any OU that is not the highest level grouping for your organization.
2. Verify **Release channel** is set to **Stable.**
3. Change **Target version** to **119 (or higher).**
4. If upgrading from 114-118, under **Roll back to target version** select **Do not roll back OS**.
5. To expediate any OS changes, make sure the **Rollout plan** is set to **Default (devices should update as soon as a new version is available).**
6. Select **Save.**



Option 2 - Block URLs

Schools/organizations can also prevent security issues with URL blocking settings in the Google Admin Console. Because some security issues affect all kiosk apps—not only TestNav—they should restrict all kiosk app URL access and add exceptions for necessary URLs. The URLs needed for TestNav are listed below.

Best Practice

To strategize against this security issue and potential future issues, Pearson recommends that technology coordinators block all traffic to all kiosk apps and *add blocked URLs exceptions* for TestNav, as listed below (and any other kiosk apps used). Pearson cannot advise which additional URLs to exempt for other applications. You should contact other kiosk app vendor support for this information.
Note that this Kiosk URL blocking would be in addition to normal configuration of content filtering or network security rules for online testing.

To modify kiosk blocking URLs:

1. Log in to the Google Admin Console.
2. Navigate to **Devices > Chrome > Settings > Device settings > Kiosk settings > URL blocking.**
3. Select the desired Organizational Unit (OU) for your testing devices.
4. Make the following changes:
    a. Under **Blocked URLs**, add *****
    The * wildcard in the **Blocked URLs** field blocks all requests to URLs except for those listed as a blocked URL exception. This includes any URL scheme, such as **http://google.com**, **https://gmail.com**, and **chrome://policy**.
    b. Under **Blocked URLs exceptions**, add the following URLs:

TestNav Test Delivery URLs (all TestNav users)
testnav.com
pearsontestcontent.com
chime.aws
Certificate Authority URLs (all TestNav users)
thawte.com
usertrust.com
comodoca.com
TestNav Tools/Assistive Technology URLs (TestNav users that use web extensions within TestNav)
cowriter.dev
donjohnston.net
cw-ws.qadji.com
speechstream.net
toolbar.speechstream.net
cache.speechstream.net

speech.speechstream.net
rwgoogle-webservices-7.texthelp.com
testnav-cognitive-auth.dev.texthelp.com
TestNav/Pearson Access Next users
pearsonaccessnext.com
TestNav/ADAM users
adamexam.com
ACT & ACT Aspire TestNav Users
act.org
actaspire.org
Aimsweb users
aimswebplus.com

5. Select **Save**.

Schools using other kiosk apps other than TestNav – Technology coordinators should also add the required URLs for those apps to the **Blocked URLs exceptions** list as they did with the TestNav required URLs above.

If you have any issues with implementing these settings, contact Pearson support.