Google shares workarounds for auth failures on ChromeOS devices - Agai

Data: 2025-08-29 00:57:11

Autor: Inteligência Against Invaders

Google is working to resolve authentication issues affecting some ChromeOS devices, which are

preventing affected users from signing into theirClever and ClassLink accounts.

As the company explains in a recently updated incident report on the Google Workspace Status Dashboard, these authentication failures impact devices running version 16328.55.0 with Chrome browser version 139.0.7258.137.

These issues are disrupting Single Sign-On access to Clever and ClassLink educational partner platforms that are used to manage student access to digital resources.

ClassLink is used by over 22 million students and staff in more than 3,000 school systems across 50U.S. states and 42 countries, whileClever is used by over 110,000 schools, including 95 of the largest 100 districts (approximately 60% of U.S. students).

“Google, a service that works with Clever, is experiencing issues with users being unable to login using their Google credentials for those who updated to ChromeOS 139,” Clever also told users in a separate incident report on its official status page.

“This is preventing users from being able to login to their Clever account. We are monitoring the issue and will provide status updates as they become available.”

The same authentication problem also affects 2-Step Verification (2SV) processes for some users, potentially blocking access to some Google services that require enhanced security authentication.

Woarkarounds available until a fix rolls out

While its engineering teams are conducting automated testing on a potential solution before releasing the fix to affected users, Google shared two temporary fixes that could help those impacted work around the authentication failures.

The first requires administrators to roll back their ChromeOS installation to the previous M138 version, using the detailed instructions provided in this Google support document.

To do that, they have to go through the following steps:

1. Sign in with an *administrator* account to the Google Admin console.
2. Go to Menu > Devices > Chrome > Settings > Device settings (which requires having the Mobile Device Management administrator privilege).
3. To apply the setting to all devices, leave the top organizational unit selected. Otherwise,

select a child organizational unit.
4. Go to **Device update settings** and click **Auto-update settings**.
5. For **Allow devices to automatically update OS version**, select **Allow updates**.
6. For **Target version**, select a ChromeOS version.
7. For **Roll back to target version**, select **Roll back OS**.
8. Click **Roll back OS** and then click **Save**.

To verify that the affected users' devices have successfully rolled back, administrators must sign in to a managed ChromeOS device belonging to the organizational unit where rollback was enabled. Then, they should go to Settings and check the OS version in the About ChromeOS dialog.

Alternatively, they can also modify the LoginAuthenticationBehavior setting to use "Authentication via the default GAIA flow," which bypasses the problematic authentication pathway causing these ongoing failures.

"Fix is undergoing automated testing. Once completed, engineering will validate the results and we'll make the fix available to users," the company added earlier today."We currently don't have ETA for the version with the fix to be available. We will provide an update by Thursday, 2025-08-28 17:30 US/Pacific with current details."

[IMAGEM REMOVIDA]