

How to Roll Back ChromeOS to a Previous Version

Instructions Copied from Google Management Console Support Files (2023)

For administrators who manage ChromeOS devices for a business or school.

As an admin, you can temporarily roll back ChromeOS to a previous version. For example, you might need to restore a previous ChromeOS version if your users' critical apps don't work properly after a version update.

To make sure that users are protected by the latest security updates, we recommend that they use the latest ChromeOS version. By running earlier versions of ChromeOS, you'll expose your users to known security issues.

Considerations

- You can roll back to the 3 latest ChromeOS versions on the Stable channel, n-3, where n is the current stable release. Or, for devices on the Long-term support candidate (LTC) or Long-term support (LTS) channel, you can roll back to the current version on those channels.
- Rollback to ChromeOS version 106 or earlier is not supported.
- Move the devices that you want to roll back into their own organizational unit. For details, see [Move a device to an organizational unit](#).
- Check to make sure that rolling back ChromeOS to the version you want solves the issue. Consider setting up a test group and roll back a small number of devices before you roll back the ChromeOS version for a large organizational unit or your entire organization.
- For the restored ChromeOS version to take effect, devices need to restart, wipe, and re-enroll into your account. Users see a notification that lets them know their local data will be automatically deleted during rollback. The next time they sign out, devices automatically restart and wipe all local data, including data in the Downloads folder for all accounts on the device. For kiosk devices, deleted data might also include locally-cached extension data, and might require a significant amount of data to be downloaded over the network after rollback is completed, if applicable.
- Devices with ChromeOS version earlier than the pinned version that you choose don't roll back. Instead, they update to the pinned version. If the update was skipped for a specific model, the device updates to an earlier version than the one you specify. For information about pinning ChromeOS versions, see [Pin ChromeOS updates to a specific version](#).

Turn on rollback

In the Google Admin console, use the **Roll back to target version** setting together with the **Target version** setting to specify the ChromeOS version that you want devices to roll back to.

1. [Sign in](#) to your [Google Admin console](#).


Sign in using your *administrator account* (does *not* end in @gmail.com).

2. From the Admin console Home page, go to **Devices** **Chrome**.

3. Click **Settings** > **Device**.
4. To apply the setting to all devices, leave the top organizational unit selected. Otherwise, select a child [organizational unit](#).
5. Go to **Device update settings** > **Auto-update settings**.
6. For **Allow devices to automatically update OS version**, select **Allow updates**.
7. For **Target version**, select a ChromeOS version.
8. For **Roll back to target version**, select **Roll back OS**.
9. Click **Confirm**.
10. Click **Save**.

Verify that devices rolled back

You can check users' devices to make sure they successfully rolled back.

1. Sign into a managed ChromeOS device. Make sure that it belongs to the organizational unit where you turned on rollback.
2. At the bottom right, click the time.
3. Click Settings .
4. To check the OS version:
 1. At the bottom of the left panel, click **About ChromeOS**.
 2. Under Google ChromeOS, you'll find which ChromeOS version the device uses.

Troubleshoot

Devices do not automatically roll back

Users need to restart their ChromeOS devices for the rollback to take effect. Because local data is lost during rollback, sometimes users might be reluctant to restart their devices.

To speed up rollback, configure the settings:

- **Auto reboot after updates**—Select **Allow auto-reboots** to automatically restart ChromeOS devices the next time users sign out after an update. For details, see [Set ChromeOS device policies](#).
- **Relaunch notification**—Select **Show notification recommending relaunch** to show users a recurring message that they should restart their ChromeOS device. Or, select **Force relaunch after a period to force devices** to automatically restart ChromeOS devices after a certain amount of time, if users have not already restarted their devices. For details, see [Set Chrome policies for users or browsers](#).

For kiosk devices, consider remotely restarting them using **Reboot** on the device details page. For details, see [View ChromeOS device details](#).

Organizational unit is pinned to an older ChromeOS version

If you configure rollback for an organizational unit with devices that are pinned to a version that's earlier than the 3 latest ChromeOS versions, n-3, devices remain pinned to that version. Unpinned devices, such as newly added devices, do not roll back to the pinned version because the rollback image is available only for the 3 latest ChromeOS versions.

Some devices do not support rollback

Devices that don't support rollback include:

- All ChromeOS Flex devices
- Devices that are incompatible with the target version
- Devices with unsupported network configuration:
 - Note:** Devices with both supported and unsupported networks should still roll back as expected.
 - Networks using certificate-based authentication
 - Wireless networks other than PSK and EAP
 - Some mobile networks

As an admin, it's hard to tell which ChromeOS devices are incompatible with the target version, or have firmware or kernel rollback protection.

You can use your Admin console to view policy-configured networks. For details, see [Set up networks for managed devices \(Wi-Fi, Ethernet, VPN, cellular\)](#).

To view locally-configured networks, you need to check the network setting on devices themselves. For details, see [Connect your Chromebook](#).

Note: For devices with policy-configured unsupported network configuration, devices might re-enroll using their locally-configured network, if available.