

reconome

repurposing tech to unlock human potential

DEVICE UNLOCK GUIDE

Step-by-step guidance for clearing each lock type we detect on your devices.

UPDATED AUGUST 2026



CLEARING EACH LOCK

Locks left on a device stop us reusing or reselling it, which lowers the value and impact we can recover for you. It can stop the process completely, including data erasure and beyond. Thankfully, clearing them is quick.

Here is how to release each lock type we detect:

MDM LOCKED

Enrolled in Mobile Device Management (Jamf, Intune, Google Workspace, Kandji, and similar).

- 1 Log into your MDM console (Jamf, Intune, Google Workspace, Kandji, etc.).
- 2 Find the device by serial number or asset tag.
- 3 Unenroll or delete the device from management (this also removes any remote lock).

AUTOPILOT LOCKED (WINDOWS)

Windows Autopilot enrolment, managed through Intune and Azure AD.

- 1 Your IT admin logs into Intune (endpoint.microsoft.com) > Devices > Enrollment > Windows Autopilot Devices.
- 2 Find the device by serial number and delete it from the Autopilot deployment.
- 3 Also remove or delete the corresponding device object from Azure AD if present.

BIOS LOCKED

A supervisor or BIOS password set when the device was imaged.

- 1 Check with your IT team for the BIOS/supervisor password used when the device was imaged (often stored in your deployment tool, e.g. Dell Command, HP BIOS Config Utility).
- 2 Enter BIOS setup (usually F2/F10/Del at boot) and remove the password, or share it securely using the portal. Passwords are encrypted end-to-end, seen only by the team handling your unlock, and deleted for good once all your devices are unlocked.

NOTE

If the password is lost, your IT department can contact the manufacturer (Dell, HP, Lenovo) directly with proof of purchase to request an official BIOS unlock. This is not something we can do on your behalf.

CLEARING EACH LOCK

FRP LOCKED

Android Factory Reset Protection, tied to the Google account last signed in on the device.

- 1 Go to myaccount.google.com > Security > Your devices, and remove the device from the account.
- 2 If that is not possible, your manufacturer (e.g. Samsung) may offer an official proof-of-ownership FRP removal request through their support site.

iCLOUD LOCKED

Apple Activation Lock, tied to an Apple ID through Find My.

- 1 Sign in at icloud.com/find, select the device and choose Erase, then remove it from the account list.
- 2 If you no longer have the Apple ID or password, contact Apple Support with your original proof of purchase to have them clear it.

ABSOLUTE PERSISTENCE / COMPUTRACE

A firmware-level persistence agent that must be deactivated at source.

- 1 Your IT department logs into your organisation's Absolute console and deactivates or unregisters the device by serial number.
- 2 If you do not have console access, contact Absolute Software support directly with proof of ownership to request deactivation.
- 3 Some BIOS versions let you disable the Absolute module directly in BIOS/UEFI settings (requires the BIOS admin password, see the BIOS steps on the previous page).

reconome

repurposing tech to unlock human potential

NEED A HAND?

recono.me

Stuck on a lock this guide does not cover? Share the device securely through your Reconome portal and our team will walk you through it.

Why it matters

Every device you unlock is one we can wipe, recover value from, and route to reuse or responsible recycling, with asset-level reporting throughout. Locked devices reduce the value and community impact we can return to you.