Offboarding devices from Intune, Entra ID and Autopilot

Ugur Koc

Cloud Engineer

@glueckkanja AG

Twitter: @ugurkocde

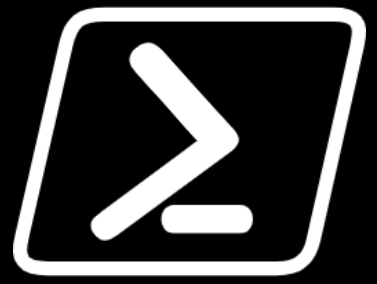
Blog: ugurkoc.de

Organizational and technical reasons to remove a device

Services and Tools

Delete, Retire or Wipe?

Stale Devices



PowerShell Script and GUI

Best practice

But first ….

Time for a Demo!

Organizational and technical reasons to remove a device

1

Hardware Lifecycle Management:
Offboarding is essential when a device reaches the end of its lifecycle or becomes obsolete, ensuring that outdated hardware doesn’t compromise system integrity or security.

2

Security Compliance and Risk Management:
Removing devices that no longer comply with the latest security policies or pose a potential risk (like those that can't support new security updates) is crucial for maintaining a secure IT environment.

3

Employee Turnover and Role Changes:
Offboarding is necessary when an employee leaves the organization or changes roles, to prevent unauthorized access and ensure that each user has appropriate device access aligned with their current position.

4

Device Reassignment and Inventory Optimization:
Offboarding allows for the efficient reassignment of devices within the organization, helping manage inventory effectively and ensuring that resources are optimally utilized.

Services and Tools

Intune

Manage the devices with e. g. profiles, apps and updates.

Autopilot, Apple Business (School) Manager and Android Enterprise

This the place where you manage the ownership of the devices. Your device will always find its way to one of the services above unless they are deleted.

Entra ID

Handles the device Identity and can be used for Conditional Access. You can enforce rules or restrict access to corporate data.

As long as the device is known and registered in Microsoft Autopilot, Apple Business (School) Manager or Android Enterprise you will have control on who can manage or access the device. This services guarantee you the (technical) ownership of the device.

Delete, Retire or Wipe?

Example Use-Case: Wipe a device to restart the autopilot process, or you can delete the device when it will be trashed or sent back to the retailer.

Delete

Goal: Remove stale devices

- Apps will be uninstalled except for Win32 apps installed by Intune and the M365 Apps.
- Sign-In with Entra ID Account will not be possible. Only local user accounts will work.
- Entra ID Object will be deleted.
    - If your device has an **Autopilot** hash assigned it will NOT be deleted from Entra ID.
- Delete will also issue the retire command but it will remove the device from the All devices list immediately.

Retire

Goal: Remove managed apps and configs but don't delete user data on the device.

- The Retire action removes managed app data (where applicable), settings, and email profiles that were assigned by using Intune.
- The device is removed from Intune management.
- Removal happens the next time the device checks in and receives the remote Retire action.
- The device still shows up in Intune until the device checks in. If you want to remove stale devices immediately, use the Delete action instead.
- When you use the Retire device action, the user’s personal data is not removed from the device.

Wipe

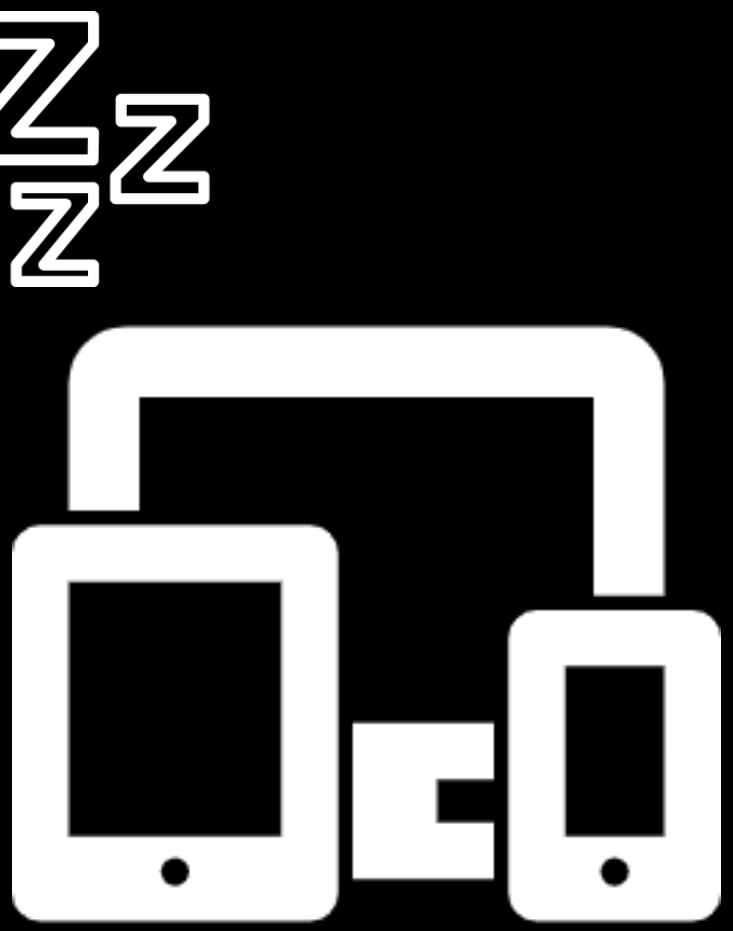
Goal: Restore a device to its default settings (OOBE, out-of-box experience).
There are two options, and you must make a choice after selecting Wipe in Intune for the specific device:

1. Keep the enrollment state and associated user account:

1. Will not be removed from Intune.
2. Wipes all MDM Policies.
3. Keeps user accounts and data (Profile).
4. Resets user settings back to default.
5. Removes user-installed apps.
6. Resets the operating system to its default state and settings.
7. Keeps Entra ID join and MDM policies will be reapplied the next time device connects to Intune.

2. Do not keep the enrollment state and associated user account:

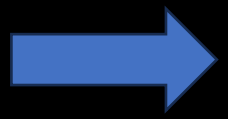
1. Device will be removed from Intune.
2. Wipes all user accounts.
3. Wipes all user data and user-installed apps.
4. Removes MDM policies, and non-default settings.
5. Resets the operating system to its default state and settings (OOBE).



Stale Devices

Stale devices are devices that had no connection to Intune or Entra ID in the last X Days.

Stale Devices are due to test devices enrolled in the environment, workforce changes, users purchasing new devices etc. and can easily skew up the device compliance reporting.

Intune & Entra ID 

Device clean-up rules:

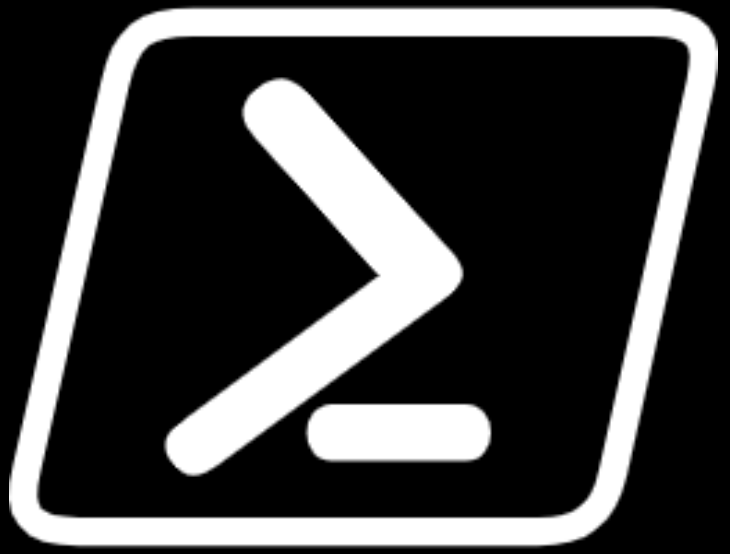
Choose between 30 and 270 days to remove the inactive device records from Intune automatically.

Device will not be deleted from Entra ID.

Device will not wipe or retire.

Attention: BitLocker Key and Startup PIN, FileVault Recovery Key

If you delete a stale device, you also delete the BitLocker keys that are stored on the device.



PowerShell Script and GUI

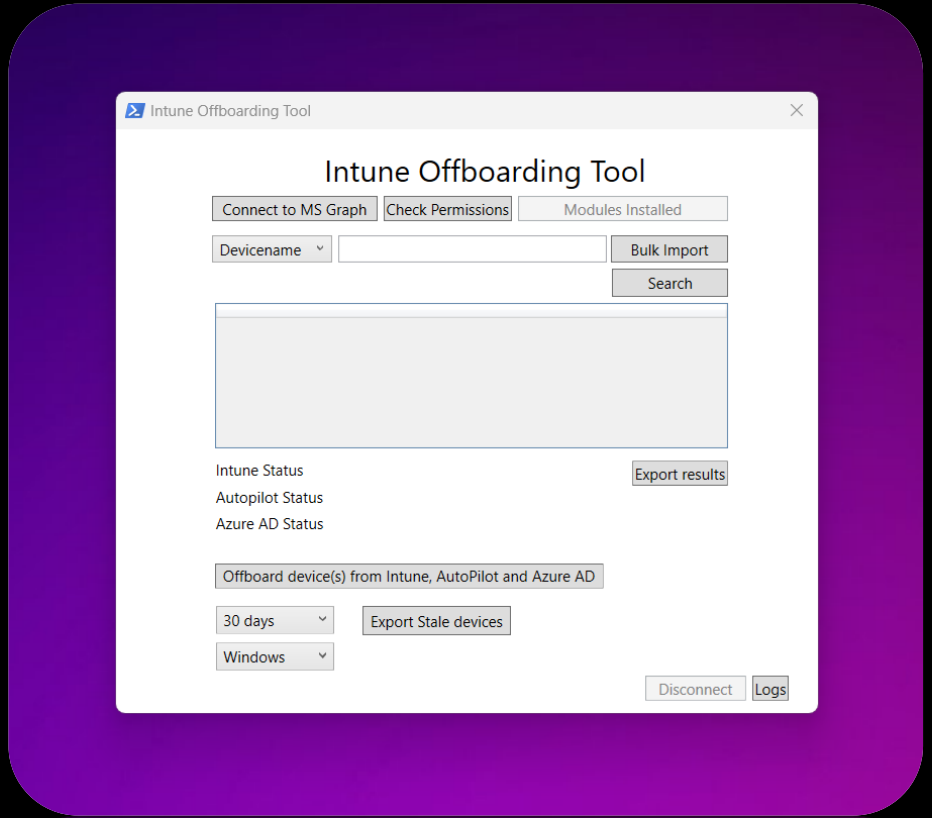
PowerShell Script and GUI

Goal: Clean up Stale Device identities in Intune, Autopilot and EntraID

The script does not Wipe Devices!

Requirements

- Microsoft PowerShell 5.1 or later
- Necessary modules:
  - Microsoft.Graph.Identity.DirectoryManagement
  - Microsoft.Graph.DeviceManagement
  - Microsoft.Graph.DeviceManagement.Enrollment
- Permissions:
  - DeviceManagementManagedDevices.ReadWrite.All,
  - DeviceManagementServiceConfig.ReadWrite.All



Quickstart:

➔ Install-Script -Name Get-IntuneOffboardingTool –Force

➔ Get-IntuneOffboardingTool

ugurkocde/IntuneOffboarding (github.com)

Details in my blog: https://ugurkoc.de/offboarding-devices-from-intune-azure-ad-and-autopilot

Best practice

Offboarding Device

If the device is not going to be used again:

Wipe Device,
Delete Hash from Autopilot,
Delete Device from Entra ID

If the device is going to be used again:

Wipe Device and Reinstall OS

Control who can enroll devices in Intune with Restrictions.

Offboarding User

Always retire or remote wipe devices associated with that user before deleting the user from Entra ID. If the user is deleted prior to cleaning up their devices, Intune's ability to manage the device may become limited.

Delete Device from Autopilot if you sell the device.

Deploy OneDrive KFM wherever you can (Backup).

Entra ID – Cannot be deleted as long as the device is still registered in the autopilot.

Just because it is greyed out in the Portal, does not mean that you can not do it with Graph.

Websites and Blogs

How to manage stale devices in Microsoft Entra ID - Microsoft Entra ID | Microsoft Learn

Intune Wipe vs Fresh Start: Breaking It Down (skymadesimple.io)

Offboarding users from Microsoft Endpoint Manager – Microsoft Intune - Microsoft Community Hub

https://karstenkleinschmidt.de/2020/09/09/intune-what-is-retire-wipe-delete-fresh-start-autopilot-reset/

Offboarding devices from Intune, Entra ID and Autopilot – Cloud Blog (ugurkoc.de)

Using Intune device cleanup rules (Updated version) - Microsoft Community Hub

Offboarding devices from Intune, Entra ID and Autopilot