

# Dynamic Device Group for Company-Owned Windows Devices

Field	Details
Document Type	How-To Guide - Create a Dynamic Group Runbook
Applies To	Microsoft Entra ID & Microsoft Intune
Audience	2nd Line, Entra ID & Intune Admin
Author	AK. Udofeh
Last Updated	Nov 2025

## Overview

This document explains how to create a dynamic device group in Microsoft Entra ID (formerly Azure AD) that automatically includes all Company-owned Windows devices that are Microsoft Entra-Joined. This group can then be targeted for Intune policies.

## Key properties used

- Devices: Windows 10 and Windows 11
- Enrollment: Manual Microsoft Entra join by users
- Ownership: Company (Corporate-owned)
- Management: Intune-managed (MDM)
- *Goal: Automatically group these devices without manual assignment.*

## Steps to Create the Dynamic Device Group

- Sign in to Entra Admin Center
- Go to Intune Admin Center [Microsoft Intune admin center](#)
- Navigate to Groups > All Groups.
- Click + New Group.
- Group type: Security
- Group name: Corporate Windows Devices
- Membership type: Dynamic Device
- Add Dynamic Membership Rule
- Under Dynamic membership rules, click Edit.
- Choose Rule syntax and paste the following:

```
(device.deviceOSType -eq "Windows") and (device.trustType -eq "AzureAD") and  
(device.deviceOwnership -eq "Company") and (managementType -eq "MDM")
```

## Rule Breakdown

- *device.deviceOSType -eq "Windows"* - Includes Windows devices only.
- *device.trustType -eq "AzureAD"* - Ensures the device is Microsoft Entra-Joined (not hybrid or registered only).
- *device.deviceOwnership -eq "Company"* - Filters for University-owned devices.
- *managementType -eq "MDM"* - Includes devices managed by MDM (Intune), excludes None and co-managed hybrid devices (MDM/AD) in most cases.

**Limitation: Some co-managed or misreported devices may still appear; manual validation may be required.**

## Validate and Save

- Click **Validate Rules** to confirm matching devices.
- Save and create the group.

## Common Device Attributes & Values

Property	Value	Meaning
device.trustType	AzureAD	Microsoft Entra joined (cloud-only)
	ServerAD	Hybrid joined (on-prem AD + Entra)
	Workplace	Registered only (personal/BYOD)
device.deviceOwnership	Company	Corporate-owned device
	Personal	User-owned device
device.deviceOSType	Windows	Windows OS devices only
managementType	MDM	Managed via Intune or another MDM
	MDM/AD	Hybrid-managed
	Unknown	Not managed
device.deviceCategory	Type in your device category name	This depends on the category name that has been provisioned already

Dynamic groups are evaluated automatically whenever device properties change.

Ensure devices are marked as Company-owned during or after enrollment.

Combine a broad dynamic device group with compliance/enrollment policies and manual validation to ensure only Intune-managed devices receive policies.

---

Revision #4

Created 2026-03-13 09:23:44 UTC by AK. Udofeh

Updated 2026-03-13 09:48:35 UTC by AK. Udofeh