**Current State – (Microsoft Intune)**: Personal Windows Device Enrollment is Blocked

When personal Windows device enrollment is blocked in Intune, users cannot join or enroll personal devices into Microsoft Entra ID through self-service methods such as OOBE setup, Settings, Company Portal, or Microsoft 365 apps. Only IT-approved enrollment methods (Autopilot, GPO, ConfigMgr, PPKG, or Device Enrollment Manager, see notes below) are allowed. This ensures that only corporate-owned and IT-managed devices can be enrolled into Intune, strengthening governance and device control.

**Current State (Conditional Access Policy)**: Block Intune Enrollment from Non-Trusted IP’s

However, requiring enrollment from a known network location or corporate-controlled environment introduces additional limitations. Remote or hybrid users who are not on the corporate network cannot complete enrollment. This breaks down in practice, as it does not align with modern work scenarios where employees often set up devices from home or while traveling. As a result, enrollment policies that tie eligibility to network trust can create operational bottlenecks and poor user experiences.

I have linked to the Microsoft documentation outlining Enrollment Restrictions.

[What are enrollment Restrictions?](https://learn.microsoft.com/en-us/intune/intune-service/enrollment/enrollment-restrictions-set)

Enrollment Scenarios in Practice

**Blocked Scenarios (Personal Devices)**

These enrollment attempts are blocked to prevent unmanaged or personal devices from being added:

1. Personal laptop during OOBE (Out-of-Box Experience)

* User selects “Set up for work or school” during Windows setup.
* Device attempts Entra ID join with automatic MDM enrollment.
* **Blocked** unless registered with Autopilot.

2. Existing personal laptop (from Settings)

* User goes to Settings → Accounts → Access work or school → Connect → Entra ID join.
* Device attempts automatic MDM enrollment.
* **Blocked** because it is personal.

3. Add Work Account (without join)

* User adds a work account in Settings → Access work or school.
* Triggers automatic MDM enrollment.
* **Blocked** as personal.

4. MDM enrollment only from Settings

* User attempts manual MDM enrollment without Entra join.
* **Blocked** as personal.

5. Enrollment via Intune Company Portal app

* User installs and signs into Company Portal on a personal device.
* Enrollment attempts are **blocked**.

6. Enrollment via Microsoft 365 apps

* User signs into Teams, Outlook, or Office on a personal device.
* Selects “Allow my organization to manage this device.”
* Enrollment is **blocked**.

**Allowed Scenarios (Corporate Devices)**

Corporate-owned or IT-provisioned devices are recognized and allowed to enroll:

1. Autopilot-registered device

* Device recognized as corporate (Device HASH uploaded to Intune) during OOBE through Autopilot registration.
* Enrollment is **allowed**.

2. Domain Join + Group Policy

* Device joined to MyGSec manually or during Quest Migration
* Enrollment initiated by IT configuration, using the device token.
* **Allowed**.

3. Bulk provisioning package (PPKG)

* Device provisioned using IT-provided PPKG.
* **Allowed**.

4. Device Enrollment Manager (DEM) account

* Enrollment performed using DEM account.
* **Allowed**.

**Summary of Proposed Approach**

We propose removing the known network location restriction for Intune device enrollment. While this restriction provides an additional safeguard, it prevents legitimate remote and hybrid users from enrolling devices outside of the corporate network, which would be needed for (Device Reset, Intune Reset and other support scenarios) creating operational and user experience challenges.

Instead, we will rely solely on the Intune personal device enrollment block configuration. This policy already ensures that only IT-approved enrollment scenarios are permitted, while preventing personal/self-service enrollment attempts. The result is a cleaner, more flexible model:

•  Blocked: Personal/self-service enrollment methods (OOBE, Settings, Company Portal, Microsoft 365 apps).

•  Allowed: IT-controlled enrollment methods (Autopilot, GPO, ConfigMgr, PPKG, Device Enrollment Manager, see notes below).

This approach maintains strong security and compliance by preventing personal device enrollment, while removing the unnecessary dependency on a corporate network location. It enables seamless enrollment for remote and hybrid users without weakening enforcement of corporate-only device management.

Additional notes:

 Description of Enrolment types for Company devices:

* **Autopilot:**A modern deployment method that configures devices from the cloud during OOBE (Out-of-Box Experience).  Ideal for new devices being shipped directly to users.  Only an IT role can add the Hash required to use this enrollment.
* **Group Policy (GPO) Enrollment:**Uses Active Directory Group Policy to automatically enroll domain-joined Windows 11 devices into Intune.  Ideal for Hybrid joined non-Autopilot devices.  Only an IT role can add the device to AD and the correct OU required to use this enrollment.
* **ConfigMgr (SCCM) Co-management:**Allows devices managed by Configuration Manager to also be managed by Intune. We do not use SCCM so this option is not available.
* **Provisioning Package (PPKG):**A Windows configuration file that can be used to enroll devices into Intune.  Package must be created on prem by an administrator.  We do not use this and it would not be available for enrolment.
* **Device Enrollment Manager (DEM):**A special Intune account that can enroll multiple devices (up to 1000).  Can enforce kiosk or restricted-use policies.  We do not use this and it would not be available for enrolment.