Exclusion of Microsoft Intune Enrollment Service Principal from Conditional Access Policies  
  
Current State:  
  
During our device migration, an MFA exclusion was applied to the Intune service principal and the Intune Enrollment service principal, which means it currently affects both traditional GPO + scheduled task enrollments and Autopilot enrollments utilizing the Intune based Automatic Enrollment process.   
  
The driver for this change was the migration method: background enrollments triggered by GPO and scheduled tasks cannot satisfy MFA, so enrollment would fail without the exclusion. Traditional Autopilot devices did not require this exclusion to function, but because the exclusion was applied at the service principal level, it currently impacts both Autopilot enrollments and the GPO+scheduled task migration path. This makes the exclusion a temporary compromise to accommodate the coexistence of enrollment methods.   
  
Once the migration is complete and we retire the GPO + scheduled task process, the exclusion can be removed, and MFA requirements will automatically re-apply to traditional enrollment paths while Autopilot remains the standard, identity-driven approach. Even though this exclusion was made we have discovered that:  
  
Several Conditional Access Policies (CAPs) currently block or inhibit the device registration and enrollment workflow:  
  
**CAP06 - Non-Cloud PCs Require compliant hybrid-joined devices for all users**  
  
Requires compliance and hybrid-join *before* enrollment can.   
  
**Problem:**  
  
A device cannot be marked compliant until it has been enrolled into Intune, this policy requires compliance and hybrid-join before enrollment takes place. This creates a “chicken-and-egg” problem, because compliance and hybrid join is the outcome of device registration and device enrollment, not a prerequisite for it. In practice, this misalignment can stall onboarding workflows and add unnecessary complexity to what should be a straightforward process.

From an access perspective, requiring **hybrid join** means every device must maintain a dependency on on-premises Active Directory, which prevents physical machines from doing a true cloud-native Entra ID join-only enrollment. This restriction blocks organizations from adopting future innovations in identity and device management that are designed to optimize for a cloud-first model. As long as hybrid join remains enforced, the organization is locked into legacy access patterns and unable to take full advantage of modern, streamlined enrollment and management capabilities that eliminate on-premises dependencies.  
  
**CAP00b - All Resources Block Intune Access from Non-Trusted Ips**  
  
Blocks Intune access from non-trusted IPs, preventing offsite resets and enrollments.  
  
**Problem**:   
  
When a Conditional Access policy such as **CAP00b** blocks Intune access from non-trusted IPs, it can create significant challenges for organizations with a remote workforce and distributed support teams. Because the policy prevents devices from accessing Intune services outside of trusted corporate networks, employees working offsite are unable to perform device resets, re-enrollments, or Autopilot provisioning without physically returning to a trusted location. This restriction undermines the flexibility of modern endpoint management, delays troubleshooting and recovery, and increases support overhead, as IT teams cannot assist with enrollment or remediation remotely. For a remote workforce, this effectively removes one of the core advantages of cloud-based management enabling seamless support and lifecycle operations from anywhere.

**CAP12 - Microsoft Admin Portals and Graph Block devices coming from untrusted locations**  
  
Blocks Graph calls from untrusted Ips.  
  
Intune enrollment restrictions are already configured to block personal device enrollments across all self-service paths (OOBE, Settings, Company Portal, Microsoft 365 apps). This ensures that only IT-approved methods Autopilot, GPO, provisioning packages, or Device Enrollment Manager accounts are permitted, so unmanaged/personal devices cannot be added to Intune. In other words, corporate ownership is already enforced by policy.

Conditional Access adds another layer by blocking Intune enrollment from non-trusted IPs. While this control provides additional assurance, in practice it prevents legitimate scenarios such as remote device resets, re-enrollments, and Autopilot provisioning for hybrid users who are not connected to the corporate network. This restriction introduces unnecessary friction for modern work, where devices are often shipped directly to users or supported offsite.

Because personal/self-service enrollments are already prohibited at the Intune policy level, the network-location restriction is redundant. It does not improve governance but does create operational bottlenecks and negative user experiences. Removing the dependency on a corporate network location, while retaining the personal device block, would maintain security posture while enabling seamless enrollment for remote and hybrid users.  
  
For more detailed information on Windows Device Enrollment Restrictions I talk about it here:  
  
[Windows Device Enrollment Restrictions](https://orr365.tech/windows-device-enrollment-restrictions-c066e496cb5f)

**Background and Context:**  
  
The team has previously invested a level effort into building an ad hoc solution for uploading hardware hashes to Autopilot by calling Microsoft Graph directly and authenticating with certificates. While functionally viable, this approach was developed outside of Microsoft’s standard tooling and supported device registration methods and has introduced additional complexity in both setup and maintenance. Certificate-based authentication requires managing cert lifecycles, distribution, and security controls, which add operational overhead and risk. The solution effectively re-created capabilities that already exist in Microsoft’s supported enrollment methods, thus leading to unnecessary work efforts, increased attack surface, and a less streamlined process for device registration.

**Proposal:**

Exclude Microsoft Intune and Microsoft Intune Enrollment service principals from any policy targeting the Windows platform that enforces:   
  
Device Compliance Checks  
Hybrid-join requirements

Location-IP Restrictions  
  
This would allow the end-point management team to use the supported Microsoft device registration methodology. Get-WindowsAutoPilotInfo is a Microsoft supported PowerShell module that streamlines device onboarding into Windows Autopilot. Authored by Michael Niehaus, a long-time Microsoft program manager and recognized expert in Windows deployment, the script is published through the PowerShell Gallery and widely used across enterprises. It collects device hardware identifiers, uploads them directly into the Autopilot service via Microsoft Graph, and applies a predefined group tag. This eliminates the need for manual CSV handling, ad hoc script solutions like the above solution presented in the background, reduces errors, and ensures consistent tagging that drives automatic policy and profile assignment. For endpoint management teams, the benefits are significant: faster device intake, predictable provisioning, and simplified targeting of Autopilot profiles across production and test environments. The ability to instantly register and categorize devices empowers the IT team to rapidly validate new configurations, reset/re-enroll hardware with minimal effort, and maintain agility in both rollout and testing workflows.

Because the script is officially maintained and aligned with Microsoft best practices, it avoids the risks and inefficiencies of custom solutions. Attempts to replace it with bespoke scripts that upload hardware hashes using certificate-based authentication are not only less secure but also re-invent the wheel adding unnecessary complexity and overhead to a process already optimized by Microsoft. By relying on the trusted, supported Get-WindowsAutoPilotInfo.ps1 workflow, Guggenheim Securities can gain both operational efficiency and confidence in long-term supportability.  
  
Example Device Registration Workflow and Enrollment:  
  
[How to Register Windows Devices into Autopilot from OOBE with Get-WindowsAutoPilotInfo](https://orr365.tech/how-to-register-windows-devices-into-autopilot-from-oobe-with-get-windowsautopilotinfo-970de0b3ba9d)

**Certificate based Authentication versus Identity Based Authentication**

|  |  |
| --- | --- |
| **Certificate-Based Enrollment** | **Admin Initiated - Identity-Based Enrollment** |
| Certificates must be distributed to **every technician**. | No secrets to distribute. Technicians use their own Entra ID identities. |
| Certificates are **transferable** and can be copied or stolen. | Bound to user identities, with **Directory Role** **PIM and MFA** protections. |
| Certificates are **long-lived**; compromise risk persists until revocation/expiry. | Full accountability logs show which technician performed the action. |
| Audit logs show only the app/cert **no accountability** for which technician acted. | Identities are dynamic; PIM sessions are **time-bound** and revocable. |
| High operational overhead: renewal, rotation, secure storage. | Low overhead: Microsoft-managed service principal, built into Intune/Autopilot. |
| **Custom script maintenance required**: certificate-based upload scripts must be built, secured, and updated as APIs evolve. | **No custom maintenance**: Get-WindowsAutoPilotInfo.ps1 is officially authored by Microsoft (Michael Niehaus), published in the PowerShell Gallery, and supported long-term. |

**Conclusion**

Conditional Access in its current form is blocking the use of Microsoft’s officially supported enrollment workflow and has forced the endpoint team to rely on temporary workarounds that are less secure, harder to maintain, and operationally inefficient. Continuing down the certificate-based path introduces long-lived, transferable secrets, audit blind spots, and ongoing script maintenance that re-creates functionality Microsoft already provides and maintains.

By excluding the Microsoft Intune and Microsoft Intune Enrollment service principals from Conditional Access policies that enforce compliance checks, hybrid-join requirements, and IP/location restrictions, we can utilize an identity-based enrollment model. This ensures that enrollment traffic is properly aligned with Microsoft best practices while administrative activity remains protected through Privileged Identity Management (PIM), MFA, and existing CA controls.

This proposal is not a relaxation of security. On the contrary, it reduces risk by eliminating certificate sprawl, strengthening accountability through identity-based auditing, and ensuring enrollment processes remain aligned with Microsoft’s roadmap. The requested exclusions are temporary where tied to the GPO+scheduled task migration and will be reevaluated once those paths are retired, allowing MFA enforcement to return for traditional enrollments.

**Request**

We request that the Microsoft Intune and Microsoft Intune Enrollment service principals be excluded from any Conditional Access policies targeting Windows that enforce:

* Device compliance checks
* Hybrid-join requirements
* Location/IP restrictions

Specifically, this requires exclusions from:

* CAP06 – Non-Cloud PCs: Require compliant, hybrid-joined devices for all users
* CAP00b – All Resources: Block Intune Access from Non-Trusted IPs
* CAP12 – Microsoft Admin Portals and Graph: Block devices coming from untrusted locations

These exclusions will allow us to leverage the Microsoft-supported Get-WindowsAutoPilotInfo.ps1 -GroupTag -Online workflow, eliminate insecure certificate-based workarounds, and restore a streamlined, identity-driven enrollment process that remains protected through PIM, MFA, and Conditional Access for all administrative actions.