Hybrid Azure AD Join Checklist (Prerequisites)

* On-prem Active Directory (obviously)
* Joining computer has a line of sight to a domain controller
* Azure AD Connect
  + The OU the computer belongs to must be included in sync scope
  + The **userCertificate** attribute must be included in sync scope
  + You must enable HAADJ within Azure AD Connect settings which configures on-prem Active Directory with a **Service Connection Point** (**SCP**) per forest
    - The SCP properties contain details of your Azure AD tenant, so computers know which to go to
    - You can find the SCP in ADSI Edit’s **Configuration Naming Context** under **Services\Device Registration Configuration**, under an attribute called **keywords**.
  + You *don’t* need Seamless SSO configured because when the device becomes HAADJ, Azure AD issues **Primary Refresh Tokens** (**PRTs**) for SSO, instead of Seamless SSO’s **Windows Integrated Auth**
  + You *don’t* need the user to sync to Azure AD for HAADJ as the device registers using a computer object credential, but you *will*need a synced (licensed) user for Intune
* The Azure AD devices setting **Users may join devices to Azure AD** *can* be set to **none** as the device join to Azure AD is done by the *device*, not the *user*.  But note this setting may have unintended consequences, such as Azure AD Join during Autopilot.

Intune MDM Enrollment Checklist (Prerequisites)

* Device is Hybrid Azure AD Joined
* User is synced to Azure AD
  + You *can* sign in with the **sAMAccountName** or**User Logon Name** (UPN) as long as the user is properly synced – you don’t need to sign in using the Azure AD address
* User is licensed to **Intune**
* User is licensed to **Azure AD Premium P1** (required for auto-enrollment)
* User is within scope for MDM automatic enrollment, configured in **Azure AD** > **Mobility** **(MDM and MAM)**
  + Make sure it’s **Intune** and not **Intune Enrollment** if you have the choice
* MDM URLs within **Mobility (MDM and MAM)**are configured to Intune
* User is within scope to join devices to Azure AD within **Azure AD**> **Devices – Device Settings**> **Users may join devices to Azure AD**
  + The number of devices they’re allowed to join, configured in this same page, is also important – if it’s exceeded, they won’t enrol
* The GPO **Enable Automatic MDM Enrollment Using Default Azure AD Credentials** is scoped to devices using **User Credential**
  + **Device Credential** is used for ConfigMgr co-management or third-party MDM.  I have never got Device Credential to work with the GPO, testing Windows 10 versions up to 1903, but *some* report success.  I kept getting **Device based token is not supported for enrollment type** errors in Event Viewer.
* **Windows (MDM)** is allowed in **Intune**> **Device enrollment – Enrollment restrictions**

The Process – Part 1 – Hybrid Azure AD Join

1. The computer joins on-prem Active Directory
2. The computer retrieves the **SCP** (tenant) information from Active Directory
   * This is achieved by a Task Scheduler entry within **\Microsoft\Windows\Workplace Join** called **Automatic-Device-Join** which runs whenever there’s a login.
3. The computer generates its self-signed **userCertificate** attribute and stores it in Active Directory (and can be found in Active Directory Users & Computers property page in the Attribute Editor tab)
   * This step is not required in an ADFS environment
4. The computer begins trying to register with Azure Active Directory and continues to do until it succeeds
   * It can only do so after the object has been synced by AAD Connect so may be delayed depending on the sync cycle
     + You can force a sync on the AAD Connect server using **Import-Module ADSync** then **Start-ADSyncSyncCycle -PolicyType Delta**
   * It won’t sync if the userCertificate isn’t yet stored in Active Directory
5. Azure AD issues a **Primary Refresh Token** (PRT) to users who log in for AAD authentication.
6. Azure AD issues an **MS-Organization-P2P-Access** certificate to the local computer (**certlm.msc**) in **AAD Token Issuer\Certificates**.  This certificate manages two additional certificates in **Local Computer\Personal\Certificates**and **Current** **User\Personal\Certificates**.  These are all for facilitating remote desktop (RDP) connections to computers joined to the same tenant.

The device is now Hybrid Azure AD Joined.  You can confirm this by looking at the object in the Azure AD devices list or using **dsregcmd /status** on the client, where **AzureAdJoined** within **Device State** is**YES**and **AzureAdPrt** within **SSO State** is **YES**.

The Process – Part 2 – Intune MDM Enrollment

1. At next GPO refresh, the device receives and applies the GPO from Active Directory
   * As this could be at the first login, it may happen before the device is HAADJ due to sync cycle and userCertificate timing – in such a case, MDM enrollment will fail (but keep trying; see below)
   * The device does not need to reboot for the GPO and subsequent steps to apply
   * If you have MFA enabled, users will be prompted via a toaster notification; if you don’t, it’s completely transparent
2. A Task Scheduler entry for **Schedule created by enrollment for automatically enrolling in MDM from AAD** is created to run once every five minutes for one day
3. This runs **deviceenroller.exe /c** **/AutoEnrollMDM**which then enrols the device into Intune MDM
4. The above Task Scheduler entry is removed and replaced by many more for things such as certificate renewal

The device is now Intune MDM enrolled.  You can confirm this by going to **Settings**> **Access work or school**> [account] > **Info** and confirming the **Management Server Address**within **Connection info** is **r.management.microsoft.com**.  You can also check **dsregcmd /status**, looking for the appropriate URLs against **MdmUrl**and **MdmtoURL** under **Device State**.