To join a Windows 11 device to Azure Active Directory (Azure AD) and Intune, you'll need administrative access to both your Azure AD and Intune portals.

Here's a step-by-step guide to accomplish this:

Join Windows 11 to Azure AD:

1. Sign in to Azure AD:

- Go to the Azure portal (<u>https://portal.azure.com</u>) and sign in with your Azure AD administrator credentials.
- 2. Navigate to Azure AD Devices:
 - In the Azure portal, go to Azure Active Directory -> Devices -> All devices. ← → C [©] https://aad.portal.azure.com/#blade/Microsoft_AAD_Devices/DevicesMenuBlade/DeviceSettings/menuId/ A* 10 1 Azure Active Directory admin center Contoso > Devices Devices | Device settings ····
 Contoso - Azure Active Directory Dashboard K Save X Discard R Got feedback? Users may join devices to Azure AD 💿 Al Selected None Device settings Enterprise applications Selected Enterprise State Roaming BitLocker keys (Preview) X Diagnose and solve problems Users may register their devices with Azure AD 💿 All None Activity B Learn more on how this setting works Audit logs Bulk operation results (Preview) equire Multi-Factor Authentication to register or join devices with Azure AD 🛈 Troubleshooting + Support No 2 New support request We recommend that you require Multi-Factor Authentication to register or join devices with Azure AD using <u>Conditional</u> <u>Access</u> Set this device setting to No if you require Multi-Factor Authentication using Conditional Access. Maximum number of devices per user \odot -Optional: Add local admin:

Azure Active Directory adm	in center			다 다 (@ ① R admin@M365x8439805 comoso		
Dashboard All services	Dashboard > Contoso > Devices > Device Administrators			Add assignments		
FAVORITES Azure Active Directory Users	 Diagnose and solve problems Manage 	+ Add assignments ×	Remove assignment	Uny groups engine for role assignment are displayed, can more o Search ⊘		
Enterprise applications	Assignments	Tou can also assign built-in roles to groups no Search Type		Alan Depung Alan 2 Selected Stal 4398050 Dn Microsoft.com		
	Activity	Search by name Name	All			
	Bulk operation results Troubleshooting + Support	No role assignments found		Selected items		
	New support request			Allan Deyoung Remove Remove		

- 3. Add a New Device:
 - Click on the + New device button.
- 4. Choose Device Type:
 - Select Windows 10 and 11 as the device platform.
 - Login Admin & Go setting



- 5. Configure Device Information:
 - Enter the required device information, such as a display name for the device.
- 6. Generate Enrollment Profile (optional):
 - You can create an enrollment profile to customize the device enrollment experience. This step is optional but can be helpful for managing multiple devices.
- 7. Complete the Enrollment Process:
 - Follow the on-screen instructions to complete the enrollment process. This typically involves downloading an enrollment package or using an enrollment URL on the Windows 11 device.

Set Up Windows 11 for Azure AD and Intune:

1. Open Settings:

• On your Windows 11 device, open the Settings app.

2. Go to Accounts:

Navigate to Accounts -> Access work or school.



- 3. Join Azure AD:
 - Click on Connect and choose Join this device to Azure Active Directory.



4. Sign In & Join without intune:

• Enter the Azure AD credentials (username and password) of your Azure AD administrator



5. Complete the Join Process:

- Follow the on-screen prompts to complete the device registration and join Azure AD.
- Verify and manually intune synch process at this option & SSO office365.



MDM - Configure Intune Device Management:

1. Sign in to Intune:

• Open the Microsoft Endpoint Manager admin center (<u>https://endpoint.microsoft.com</u>) and sign in with your Intune administrator credentials.

2. Set Up Device Configuration Profiles:

- In the Intune portal, go to Devices -> Configuration profiles.
- Create and assign device configuration profiles to manage settings such as security policies, Wi-Fi, VPN, and more.

3. Deploy Applications:

• Go to Apps -> All apps to add and deploy applications to your Windows 11 devices managed by Intune.

4. Assign Intune Licenses (if necessary):

• Ensure that the user accounts associated with the Windows 11 devices have appropriate Intune licenses assigned to enable Intune management features.

5. Monitor and Manage Devices:

• Use the Intune portal to monitor device compliance, apply updates, troubleshoot issues, and manage device configurations remotely.

6. Open Settings:

• On your Windows 11 device, open the Settings app.

7. Go to Accounts:



8. Join to inTune with SSO & synch with inTune to Office365



10. Verify the different in Device – All device and see MDM :



11. Now it can manage the Device with all functions:

Deshboard All services	SEA-WS2				
AVORITES	P Search (Ctrl+/)	Katire 🤊 Mar 🗈 Delete 🛆 Remote loci	k 🔾 Sync 🖉 Reset passcode 🔿 Restart 🛓 Collect diag		
Azure Active Directory Lucers	Overview Manage	^ Essentials			
Enterprise applications	III Properties	Device name SEA+WS2	Primary user Aaron Nicholls		
	Monitor	Management name Aaron_Windows_7/19/2022_10:03 AM	Enrolled by Aaron Nicholls		
	Hardware	Ownership Corporate	Compliance Compliant		
	Discovered apps Device compliance	Serial number 8043-2669-8752-0736-3849-9668-52	Operating system Windows		
	B Device configuration	Phone number	Device model Virtual Machine		
	P App configuration	See more			
	Recovery keys	Device actions status			
	User experience	Action Status	Date/Time Error		
	Device diagnostics	No data			
	Group membership Managed Apps				

12.

Endpoint manage Center Windows 11 to Azure AD:

To verify device have compliance & firewall:

Microsoft Endpoint Manager	admin center						
4	Home > Devices >						
Acme	Windows Window	ws devices					
Dashboard							
All services	P Search (Ctrl+/)	C Refresh 🖓 Fi	iter 📰 Columns 🗌 🚽	Export Bulk C	Vevice Actions		
Devices	Windows devices	Filters applied: OS					
Apps	Windows enrollment	P Search					
Endpoint security	Windows policies						
Reports		Showing 1 to 1 of 1 m	ecords		4	Previous Pa	
L Users	Configuration profiles	Device name †4	Managed by \uparrow_\downarrow	Ownership †	Compliance 1	os	
Groups	PowerShell scripts	SEA-WS2	Intune	Corporate	O Compliant	Windows	
Tenant administration Troubleshooting + support	Update rings for Windows 10 and later						
	Feature updates for Windows 10 and later (preview)						
	Quality updates for Windows 10 and later (preview)						
Microsoft Endpoint Manager	admin center				ଟ୍ଟେ ବ୍ ବ୍) 🔊 admi	
A Home	Home > Devices >						
Dashboard	windows windows	s devices					
All services	₽ Search (Ctrl+A) ≤	C Refrech 😽 Filter	EE Columns J Fax	ort Rulk Device /	kctions		
Devices	Windows devices						
Apps	Windows enrollment	Filters applied: OS					
Endpoint security	Windows policies	Search	2				
Repi Sudpoint security	General Compliance policies	showing i to i or i record	0		< Previou	Page 1	
Users	Configuration profiles	Device name ↑↓	Managed by ↑↓ C	wnership †↓ C	ompliance †4 C	35	
Groups	PowerShell scripts	SEA-WS2	intune C	orporate (Compliant V	Nindows	
 Tenant administration Troubleshooting + support 	Update rings for Windows 10 and later						
	Feature updates for Windows 10 and later (preview)						
	Quality updates for Windows 10 and later (preview)						

3- MDM - Hybrid Azure AD join:

1. From AD servers, go to Group Policy Management:

Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit
Certification Authority
Component Services
Computer Management
Defragment and Optimize Drives
DHCP
Disk Cleanup
DNS
Event Viewer
Group Policy Management
Internet In sation Services (IIS) Manager
SCSI Initiation
Local Security Policy
Microsoft Azure Services
ODBC Data Sources (32-bit)
ODBC Data Sources (64-bit)

3. Then AD have full control all device on premise



4.

2.

5. Go inside the Policies then Administrative Templates



- 6.
- 7. Then Go Windows Component Devices Registration



9. Then Enabled Devices...

	4.	Br Register domain;	owed computers	as devices	_	
	10	Register domain)	joined computers	as devices	Trenthery	1 NRESS
		Not Configured Enabled	Comment			
		O Disabled	Supported on:	At least Windows Serv	er 2012 R2 or Windows 8.1	
10.		Options		Help		

11. The run: gpupdate /force

🚸 Azure AD Connect

- 12. The go Azure AD connect:
- 13. Then go into Configure device option:



- 14.
- 15. Then choose Configure Hybrid Azuze AD join:





19. From SCP select Azure AD.

Tasks Overview Connect to Azure AD Device options	The samice connection point (DCP) is used by your devices to discover your Asure AD tenant information. If your devices are in different forests, each forest needs an SCP. Asure AD connect configure the SCP for you and also provide a storget for you to configure the SCP. Select the forests where you want Asure AD Cornect to configure the SCP. ●				
Hybrid Azure AD join Device systems	Forest 🕖	Authentication Service 0	Enterprise Admin		
	Optionally, if you don't have configure the SCP offline. Download ConfigureSCI	Enterprise Admin credentials for a f	orest, download this PowerShell sci		
		_			

21. Complete:



23. After Synch 20 minutes all device on premise will show in Hybrid Azure AD & No MDM .



25.