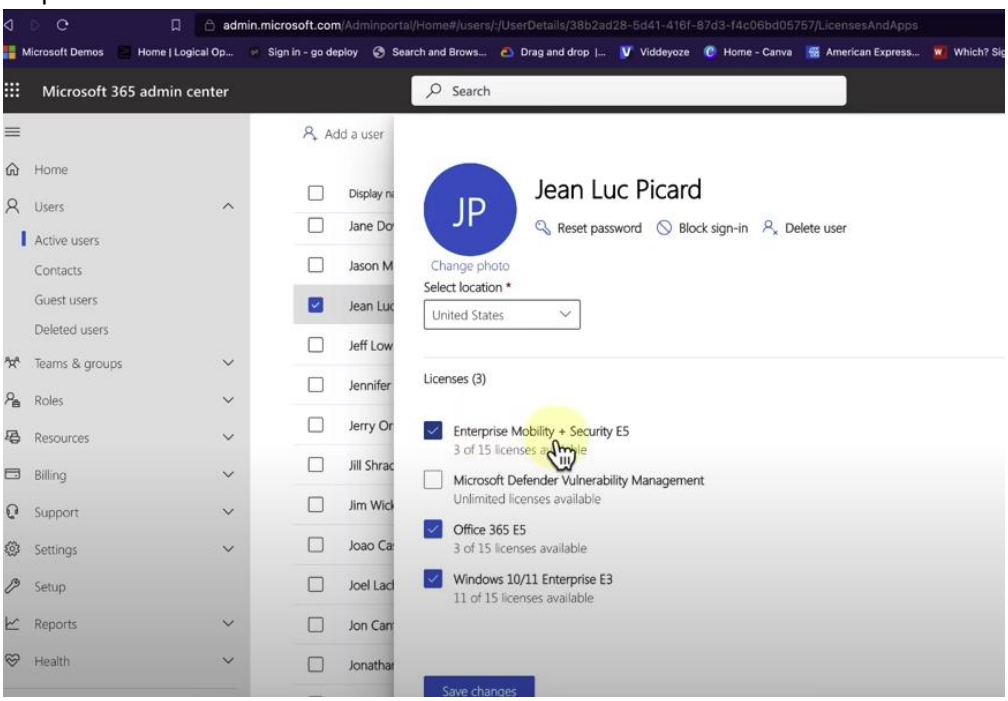
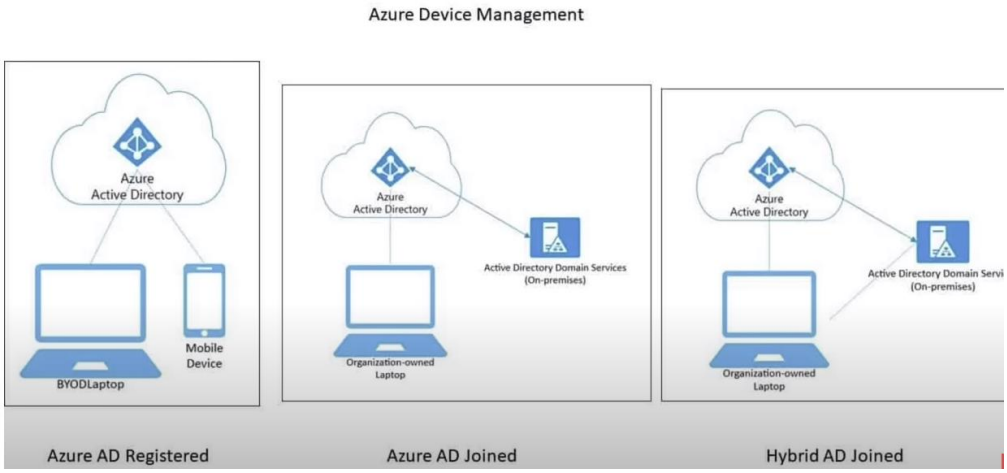
Microsoft InTune in Azure AD-Connect.

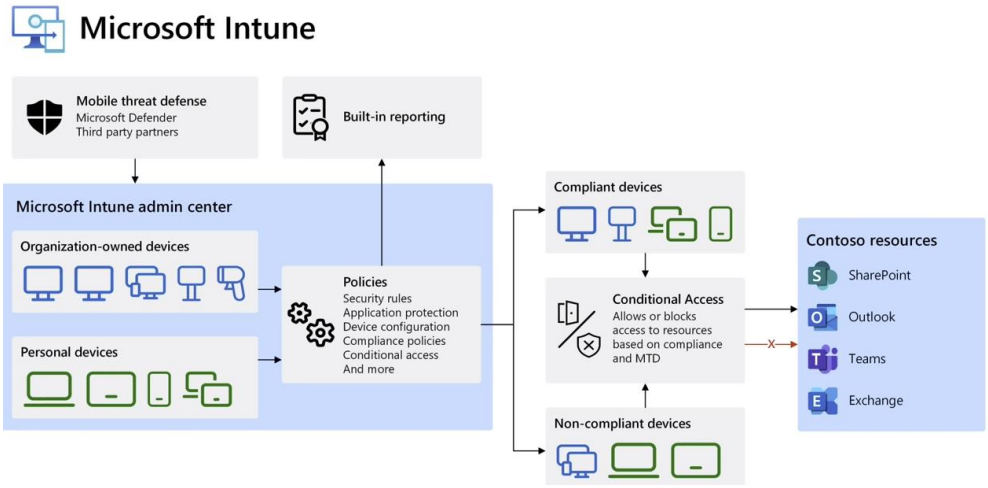
1. Step1: Check license for O365



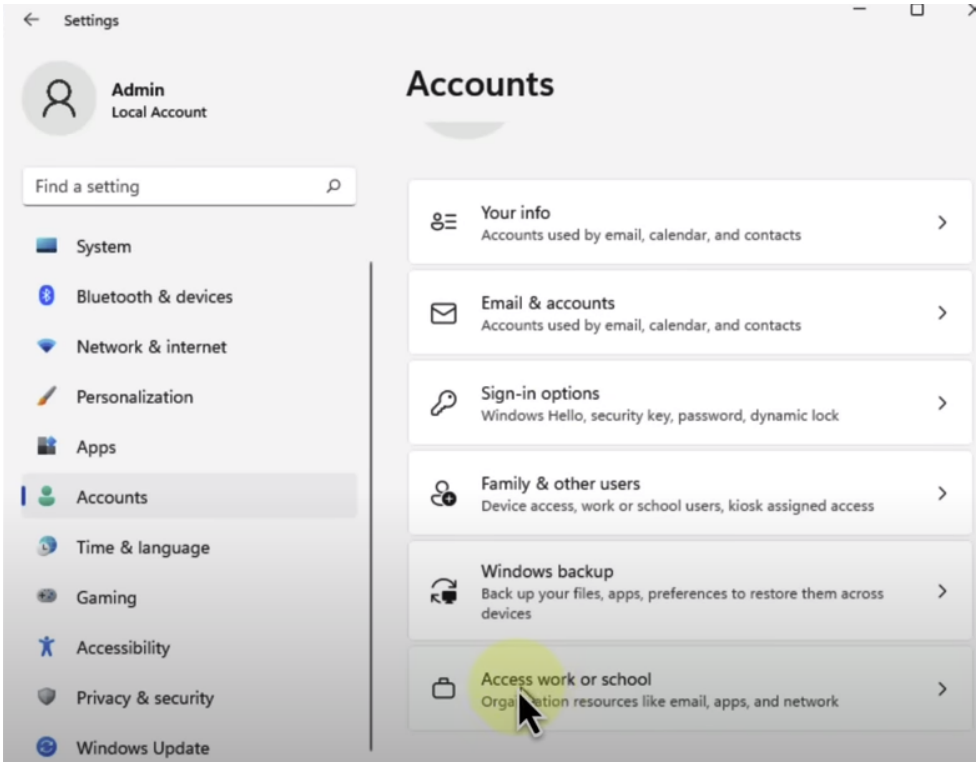
Azure Device Management



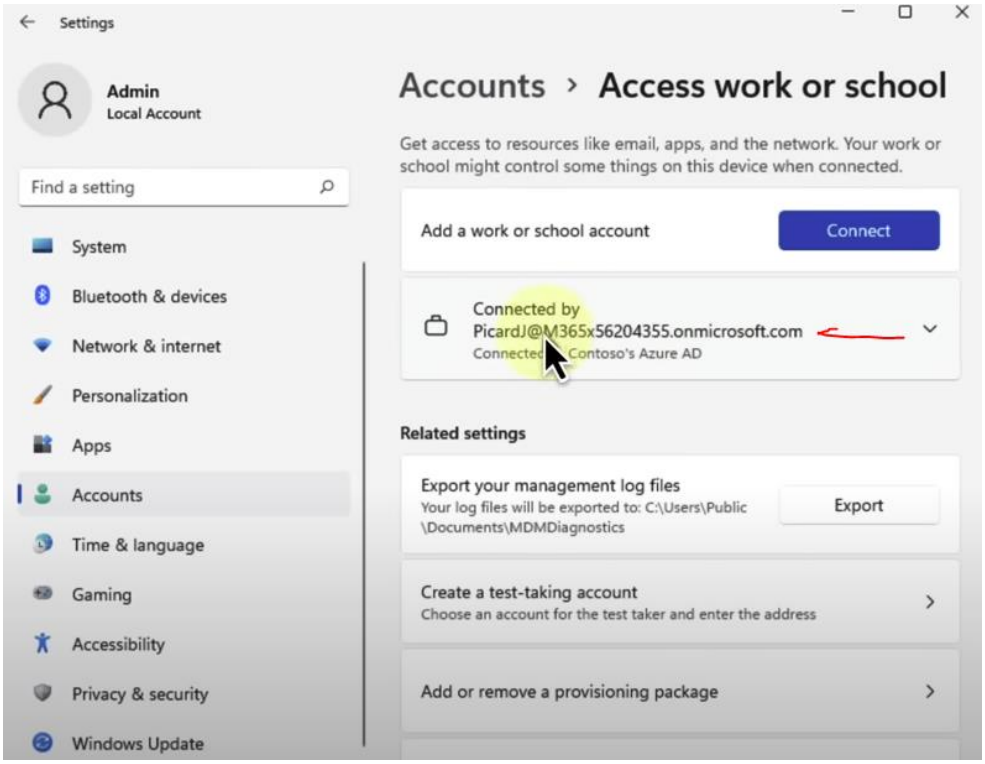
2. Microsoft Intune:



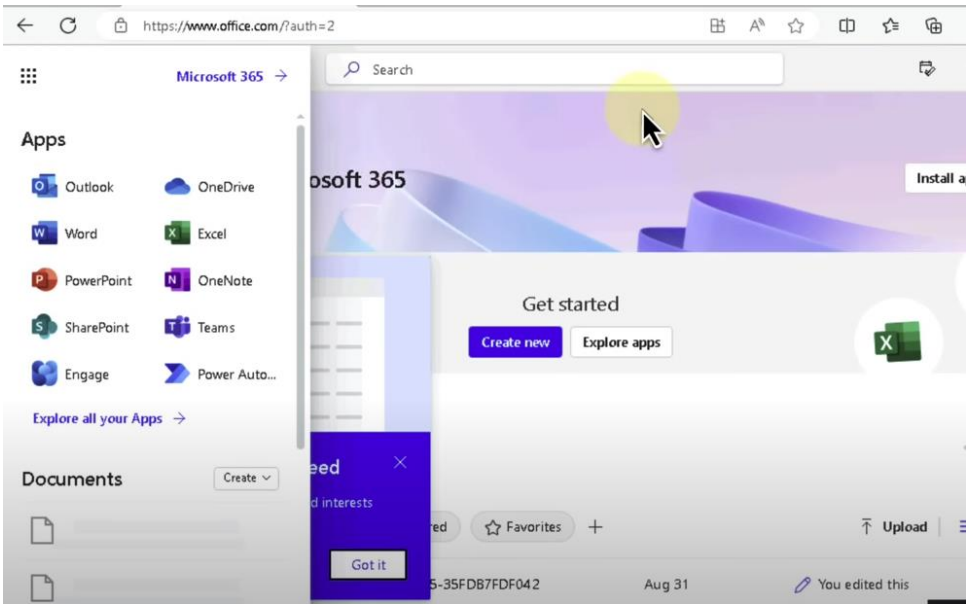
3. EntraID join Azure AD: (InTune manage every apps)



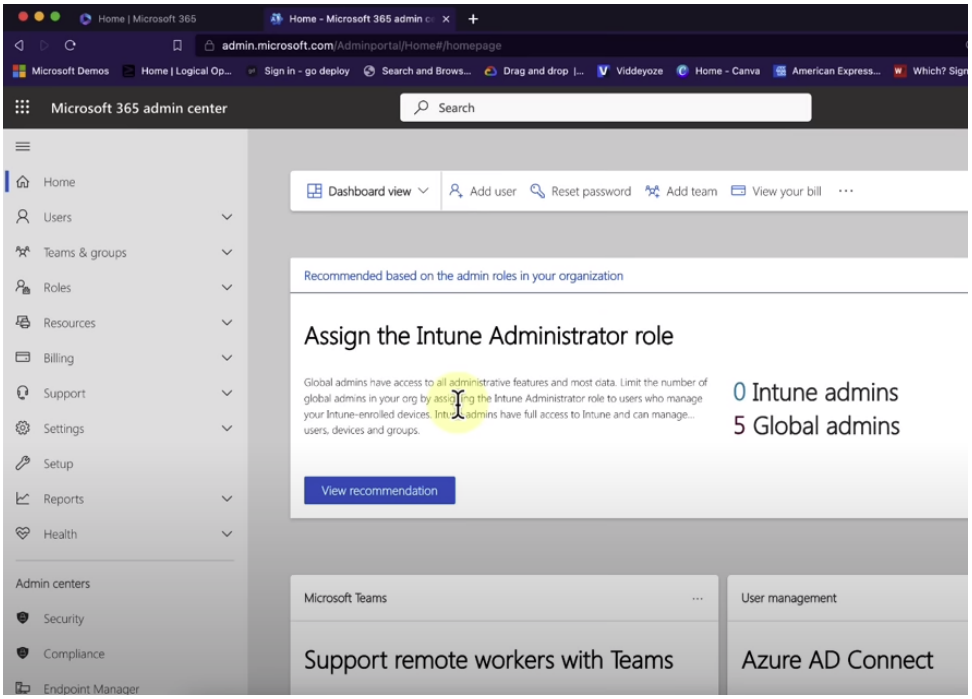
4. Verify success & restart system.



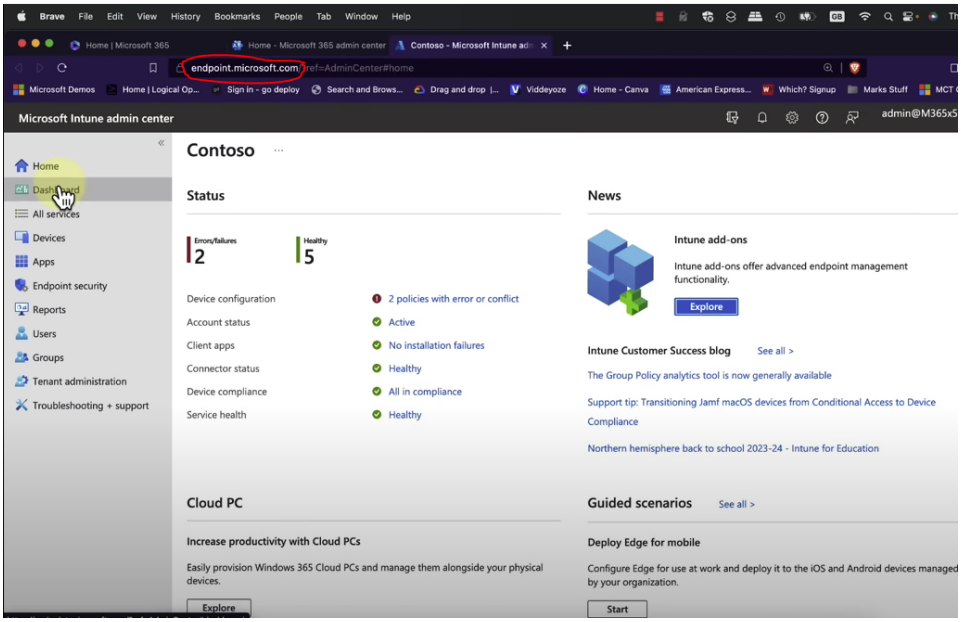
5. Login Workstation and test user account to verify SSO
   user AD\account or Email account login



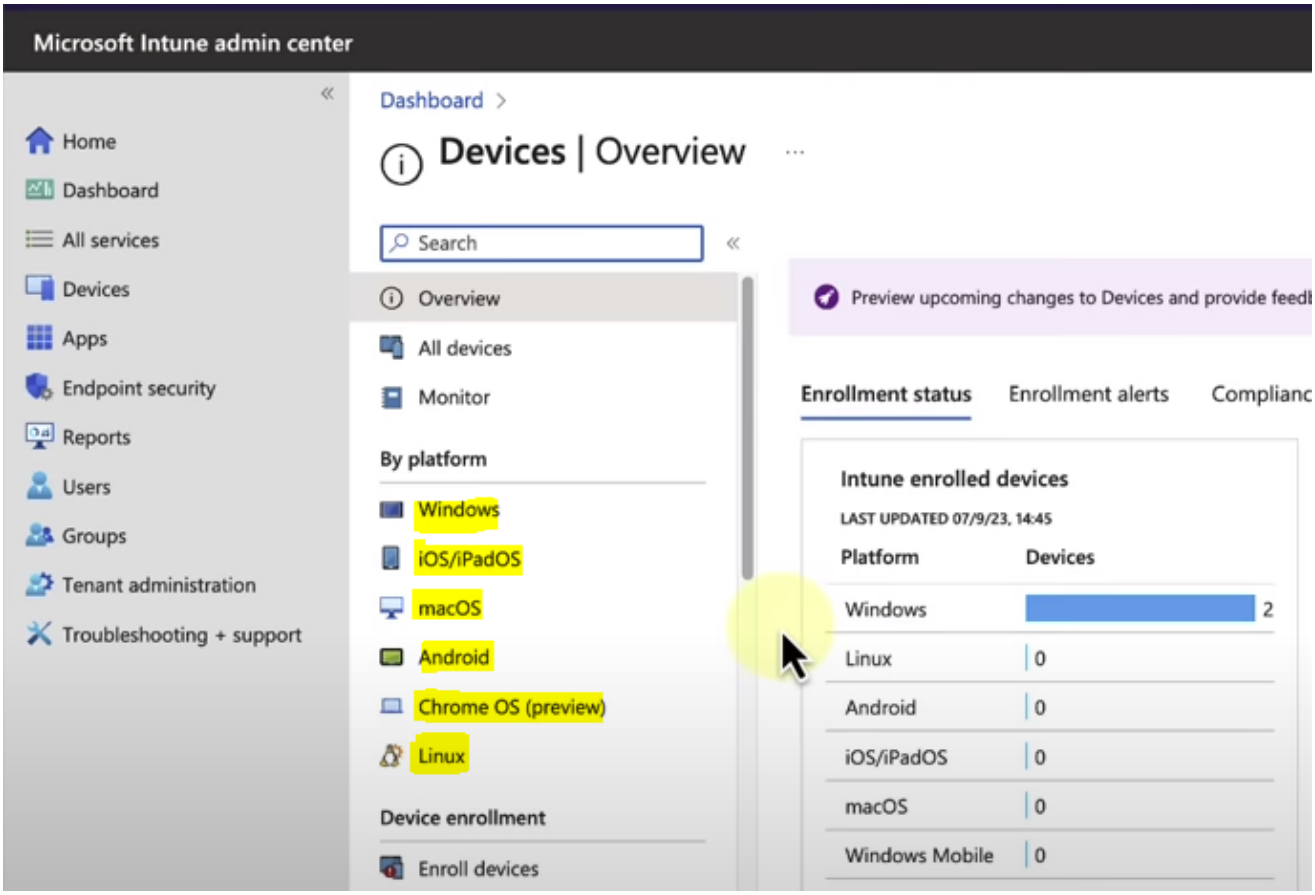
6. Use Admin login - Go to M365 to



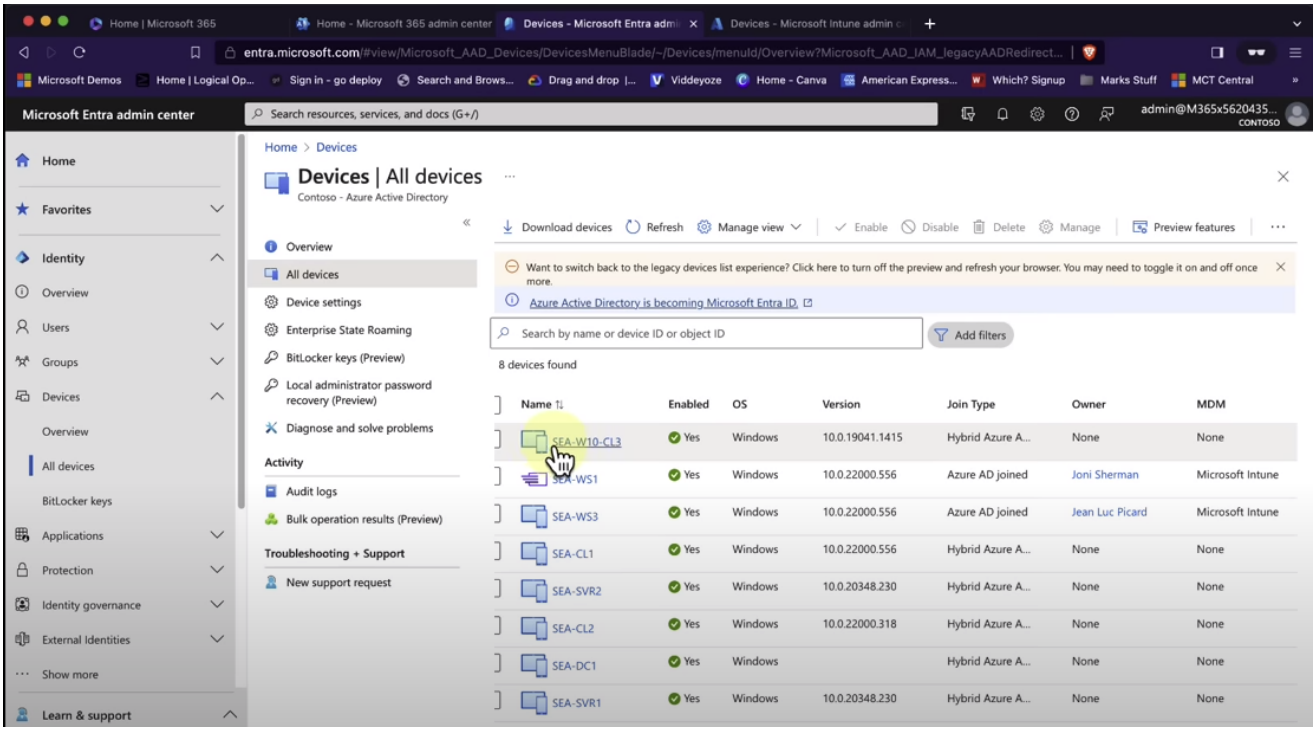
7. Go to EndPoint manager:



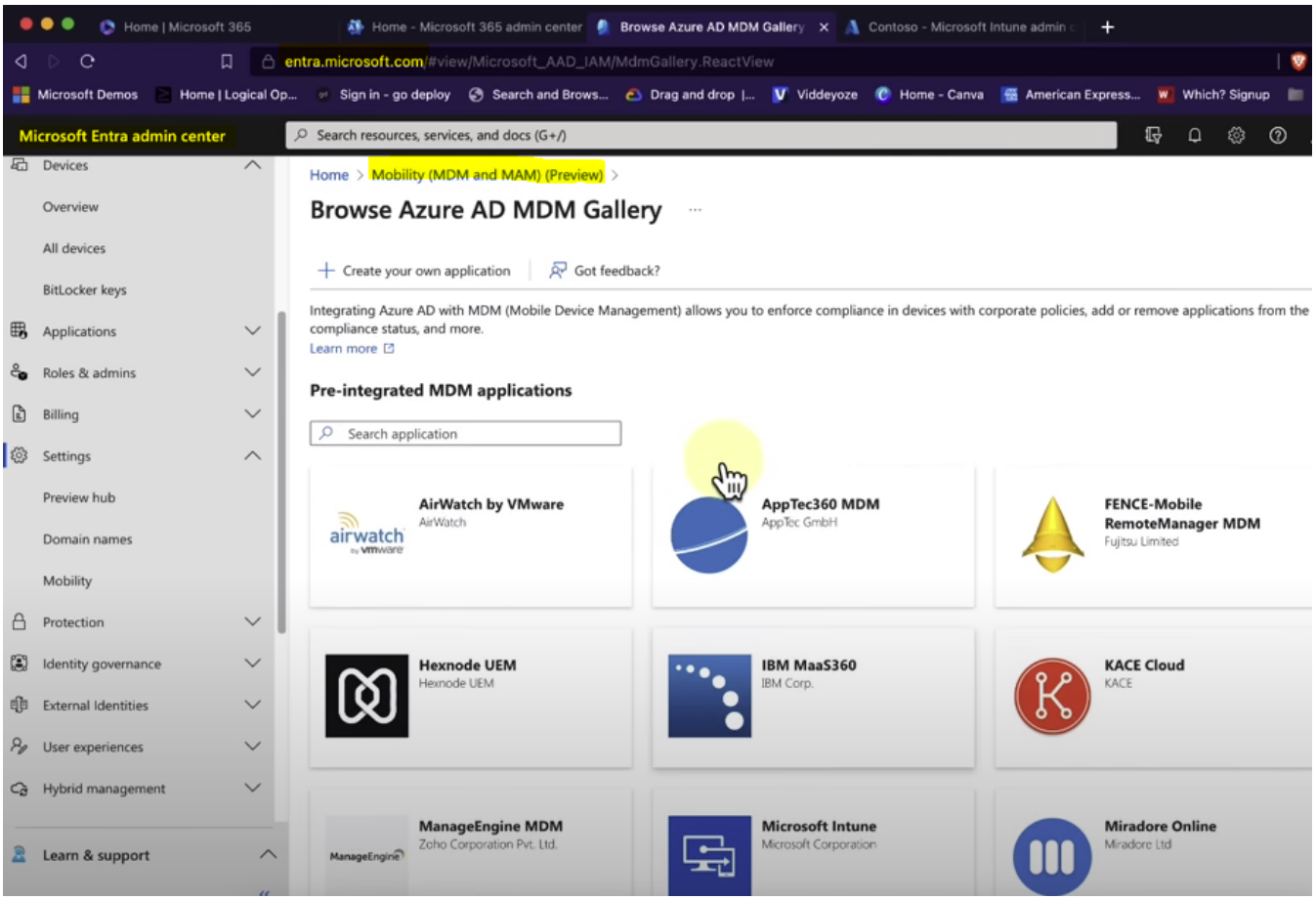
8. Go to Devices & Apps & Endpoint security.
9. All Devices enroll



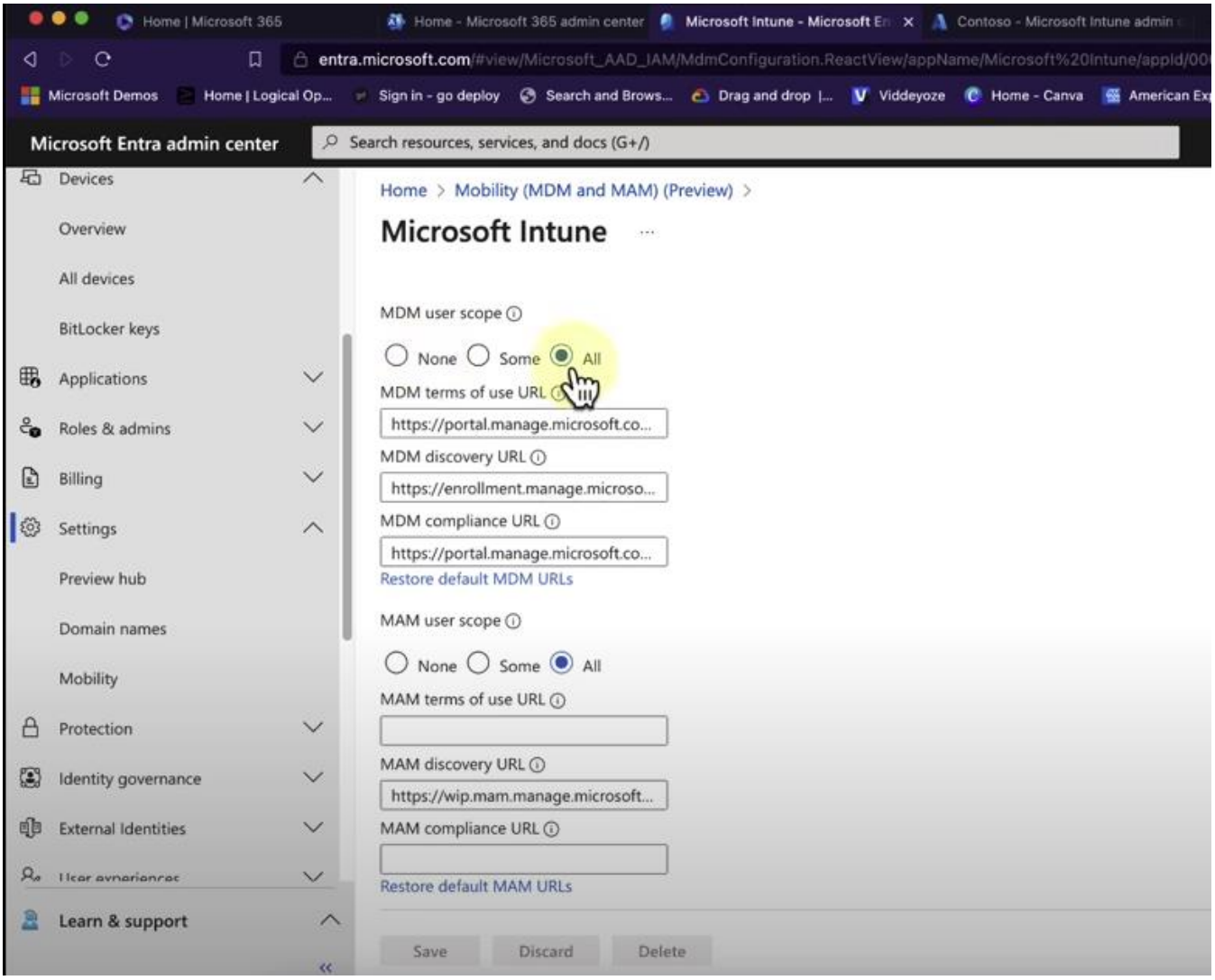
10. All Devices from on Azure management an on Premise (Entra ID)



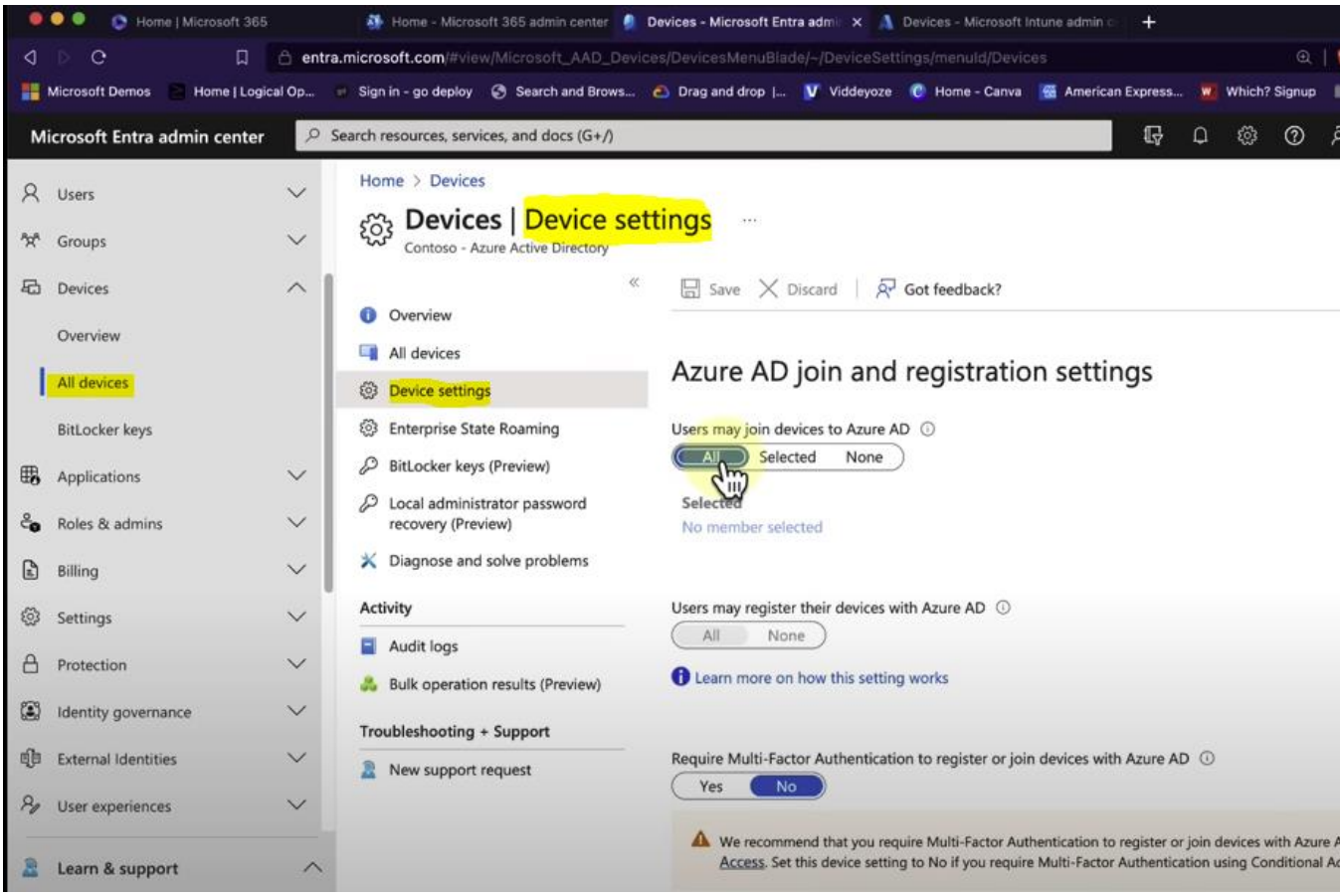
11. Go to Entra admin Center:



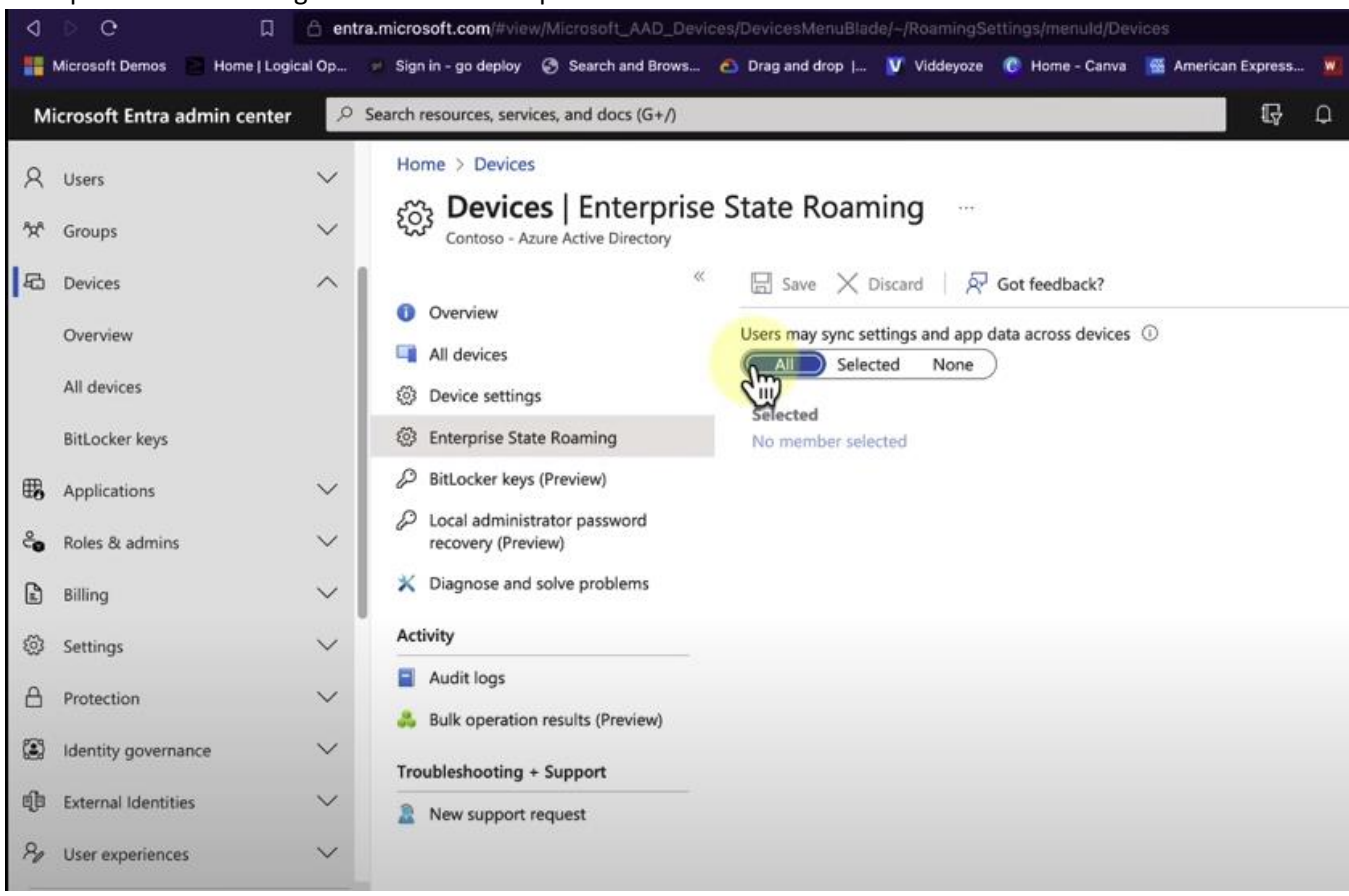
12. Go to Microsoft Intune (Manage Mobil device + PC+ Mac)



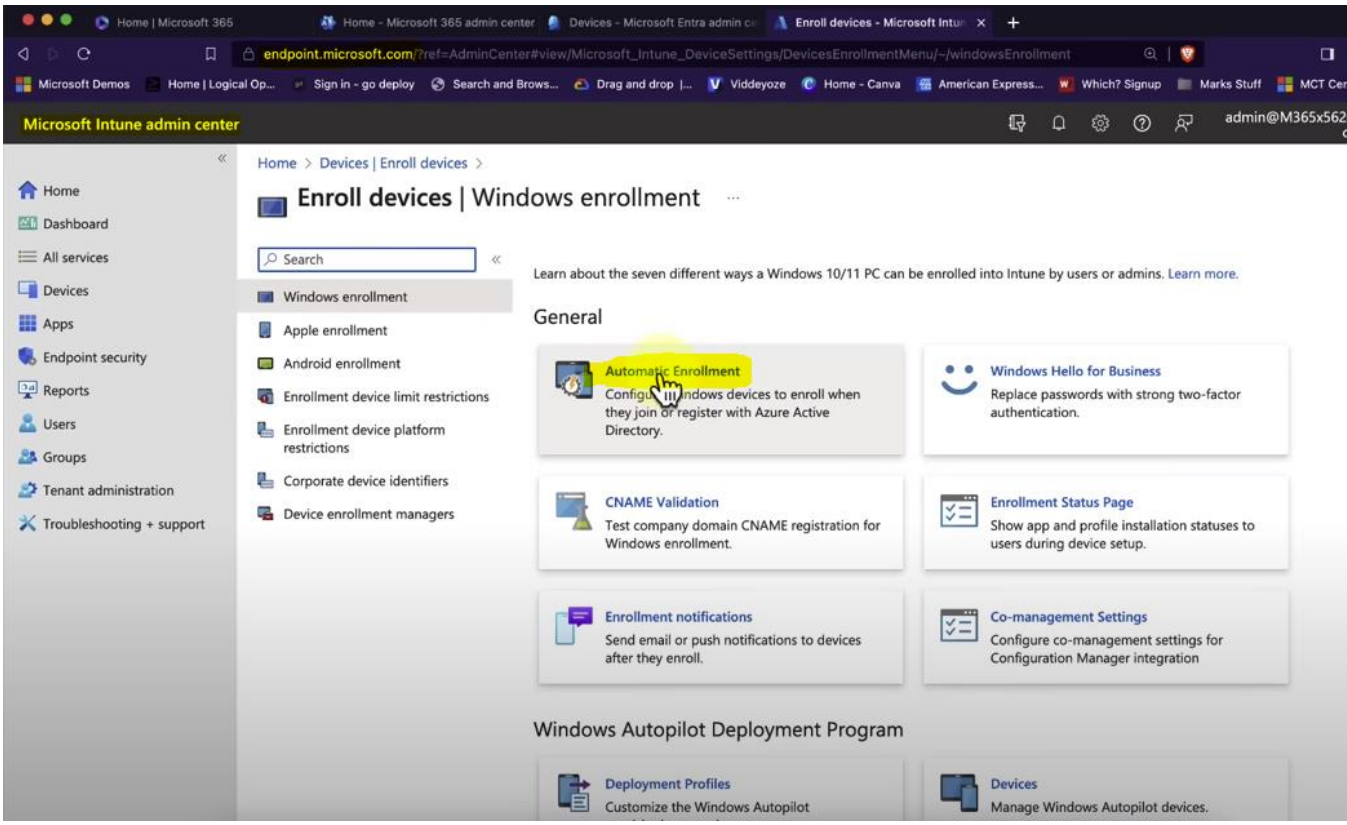
13. Go to All Entra – Devices setting: modify settin


Home | Microsoft 365
Home - Microsoft 365 admin center
Devices - Microsoft Entra adm
Devices - Microsoft Intune admin c
entra.microsoft.com/#view/Microsoft_AAD_Devices/DevicesMenuBlade/~/DeviceSettings/menuId/Devices
Microsoft Demos
Home | Logical Op...
Sign in - go deploy
Search and Brows...
Drag and drop |...
Viddeyoze
Home - Canva
American Express...
Which? Signup
Microsoft Entra admin center
Search resources, services, and docs (G+/)
Users
Groups
Devices
Overview
All devices
BitLocker keys
Applications
Roles & admins
Billing
Settings
Protection
Identity governance
External Identities
User experiences
Learn & support
Home > Devices
Devices | Device settings
Contoso - Azure Active Directory
Overview
All devices
Device settings
Enterprise State Roaming
BitLocker keys (Preview)
Local administrator password recovery (Preview)
Diagnose and solve problems
Activity
Audit logs
Bulk operation results (Preview)
Troubleshooting + Support
New support request
Save
Discard
Got feedback?
Azure AD join and registration settings
Users may join devices to Azure AD
All
Selected
None
Selected
No member selected
Users may register their devices with Azure AD
All
None
Learn more on how this setting works
Require Multi-Factor Authentication to register or join devices with Azure AD
Yes
No
We recommend that you require Multi-Factor Authentication to register or join devices with Azure A
Access. Set this device setting to No if you require Multi-Factor Authentication using Conditional Ac

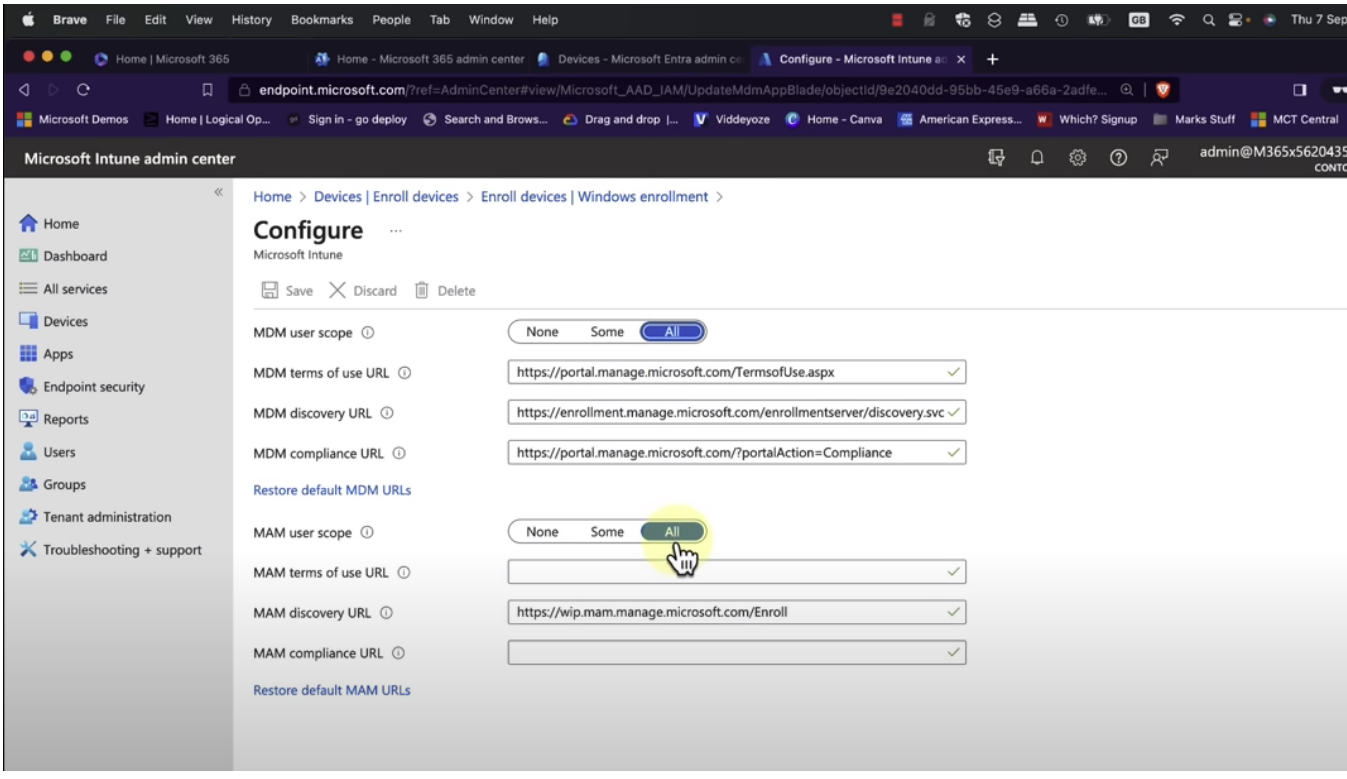
14. Enterprise State Roaming – Good idea to keep on



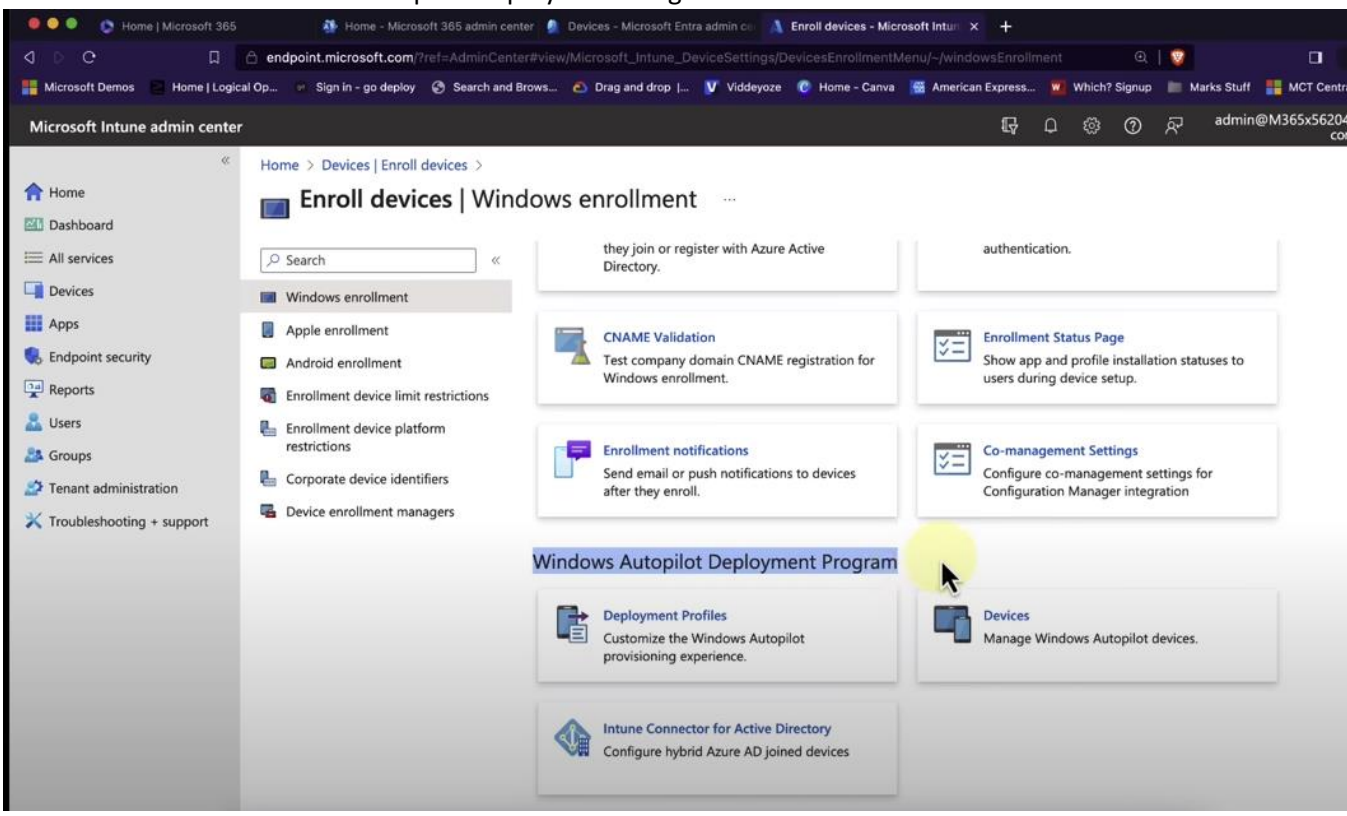
15. Go to InTune admin and Set Automatic Enrollment: All & All



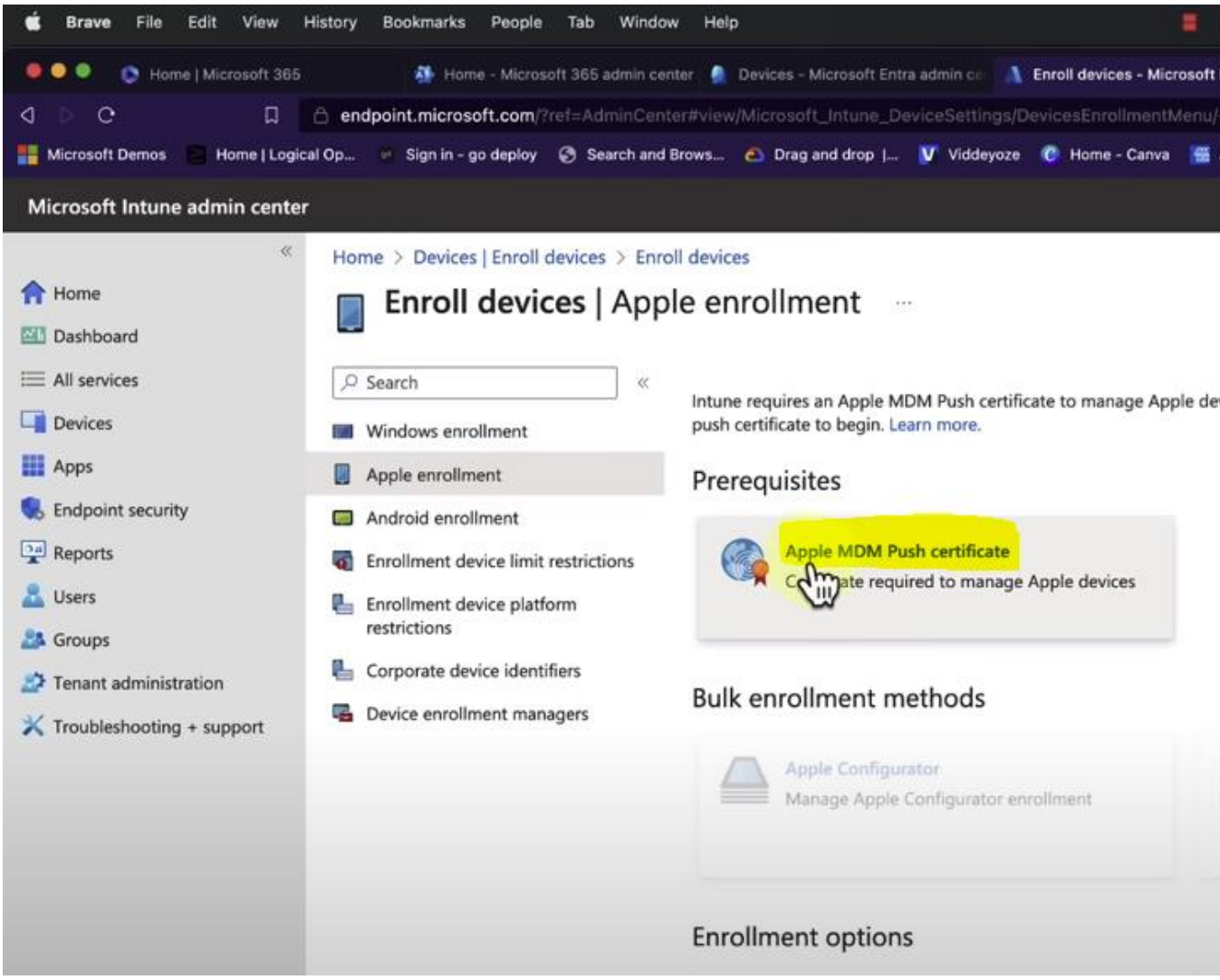
16. Configure to enroll all

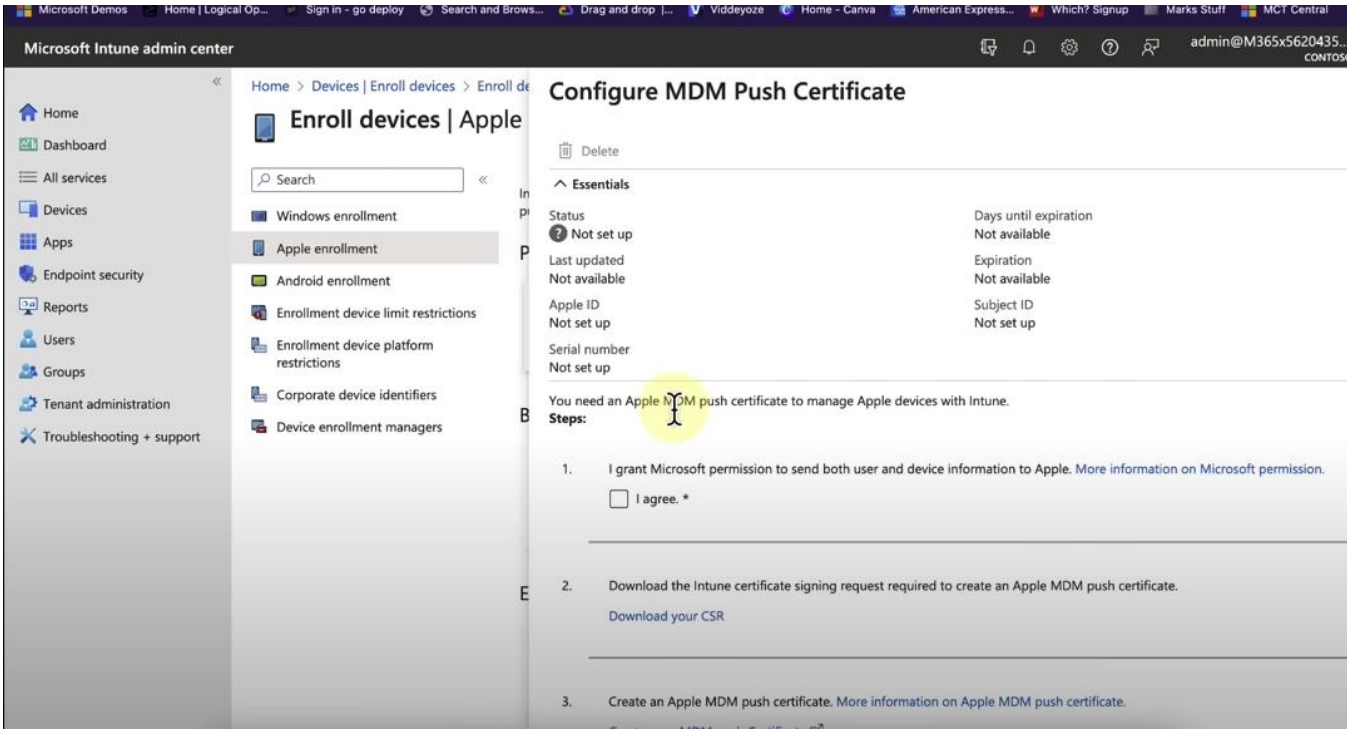


17. Make it & use This: Windows Autopilot Deployment Program

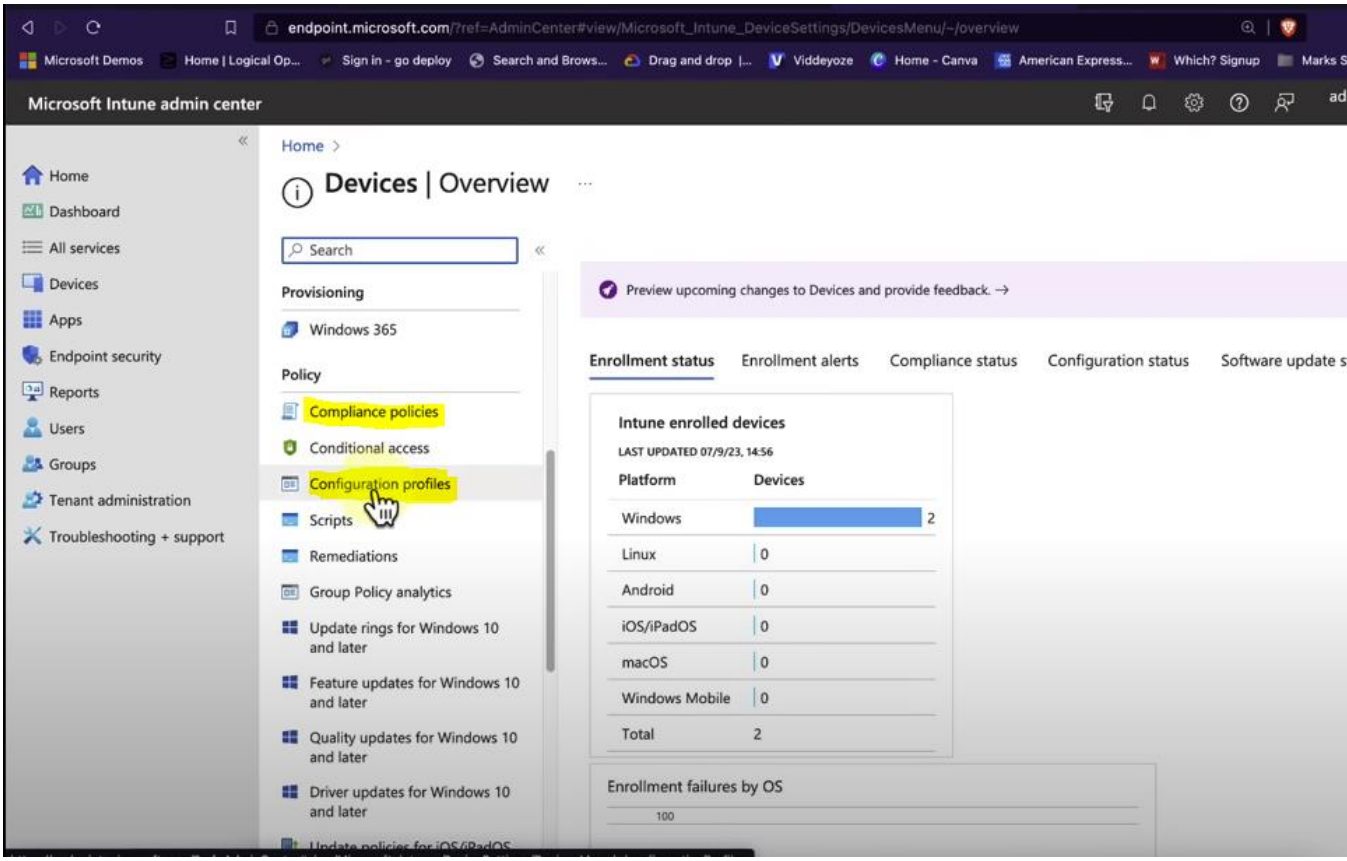


18. Apple enrollment need MDM push CERTIFICATE :

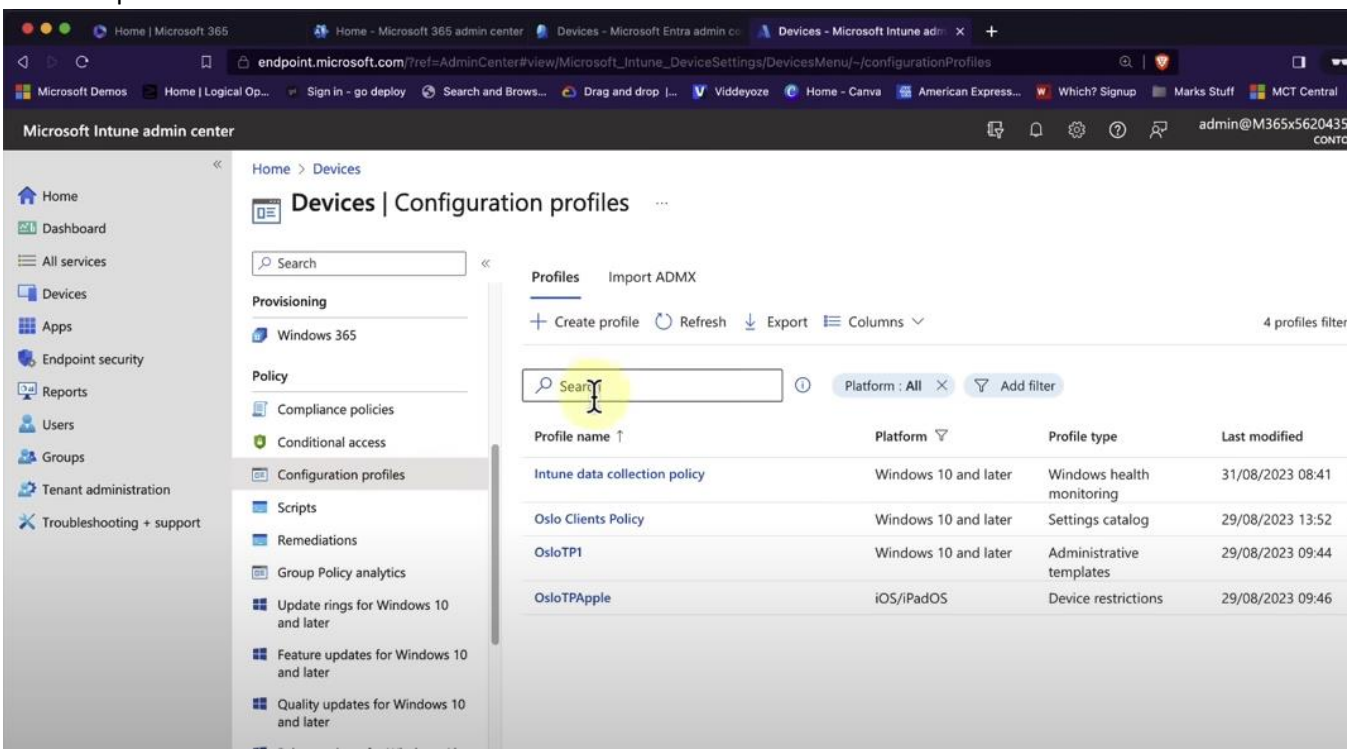
19. 
Brave File Edit View History Bookmarks People Tab Window Help
Home | Microsoft 365
Home - Microsoft 365 admin center
Devices - Microsoft Entra admin ce
Enroll devices - Microsoft
endpoint.microsoft.com/?ref=AdminCenter#view/Microsoft_Intune_DeviceSettings/DevicesEnrollmentMenu/
Microsoft Demos
Home | Logical Op...
Sign in - go deploy
Search and Brows...
Drag and drop |...
Viddeyoze
Home - Canva
Microsoft Intune admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Devices | Enroll devices > Enroll devices
Enroll devices | Apple enrollment
Search
Windows enrollment
Apple enrollment
Android enrollment
Enrollment device limit restrictions
Enrollment device platform restrictions
Corporate device identifiers
Device enrollment managers
Intune requires an Apple MDM Push certificate to manage Apple de
push certificate to begin. Learn more.
Prerequisites
Apple MDM Push certificate
ate required to manage Apple devices
Bulk enrollment methods
Apple Configurator
Manage Apple Configurator enrollment
Enrollment options



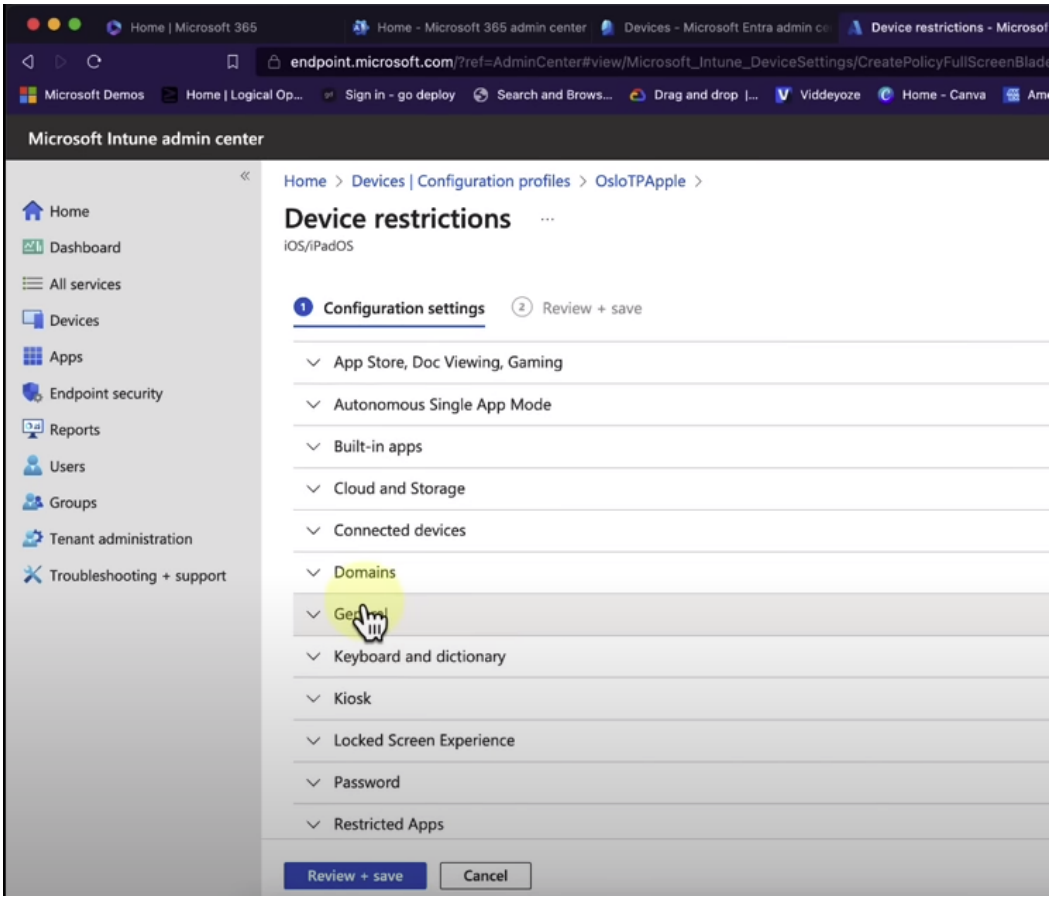
20. After device enroll, configuration policy and profiles



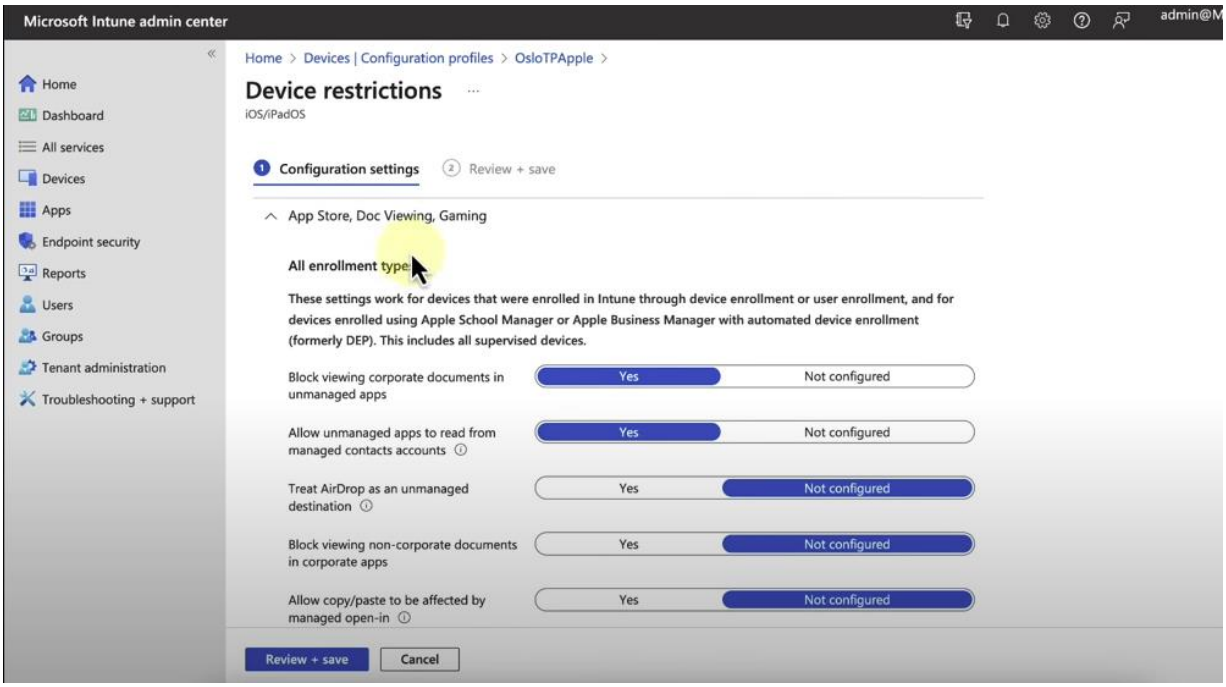
21. Create a profile :



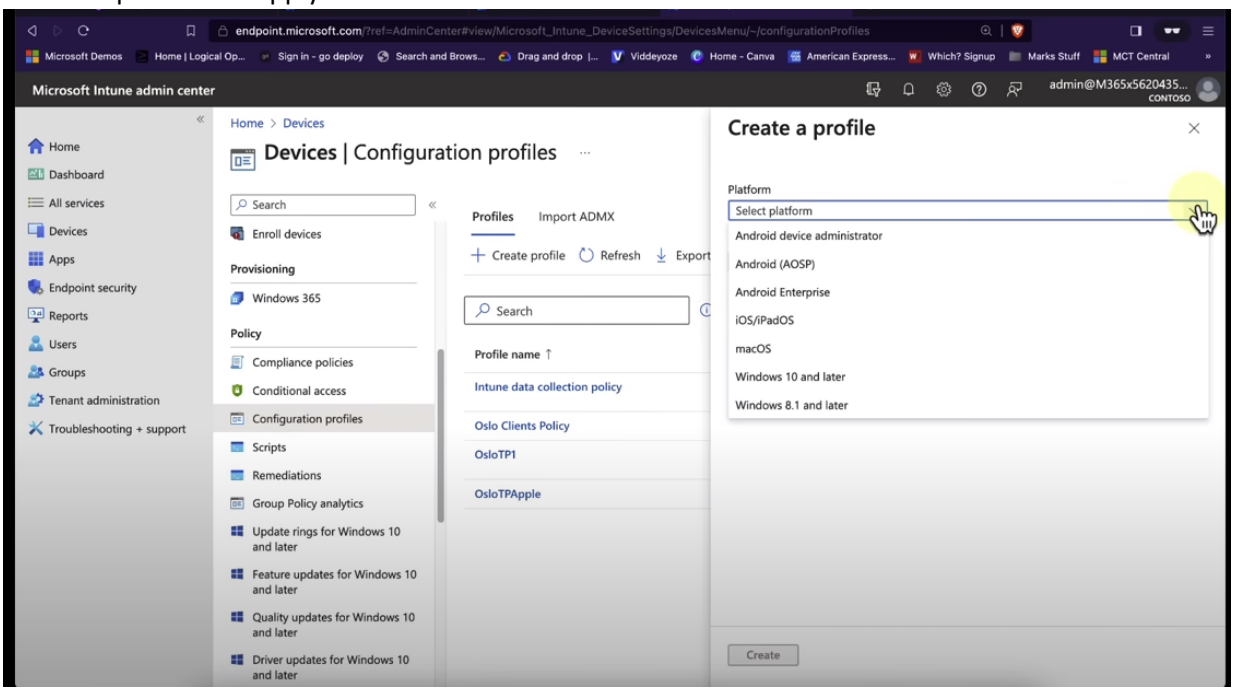
22. Set Apple devices configure restrictions



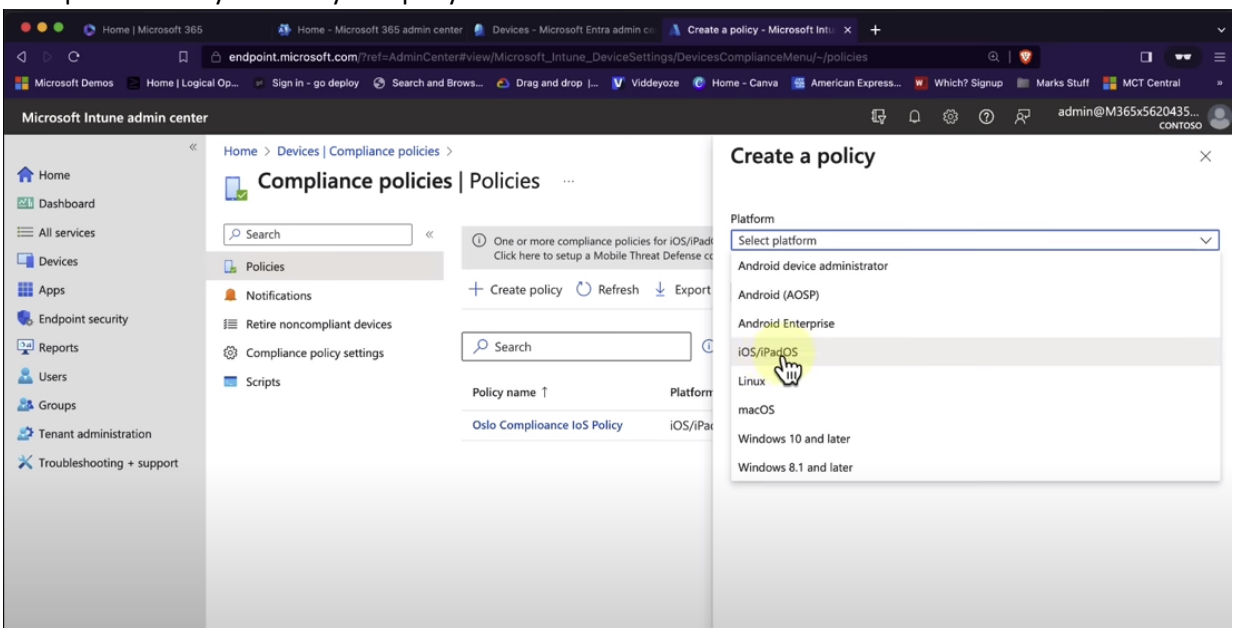
23. & Detail restrictions:



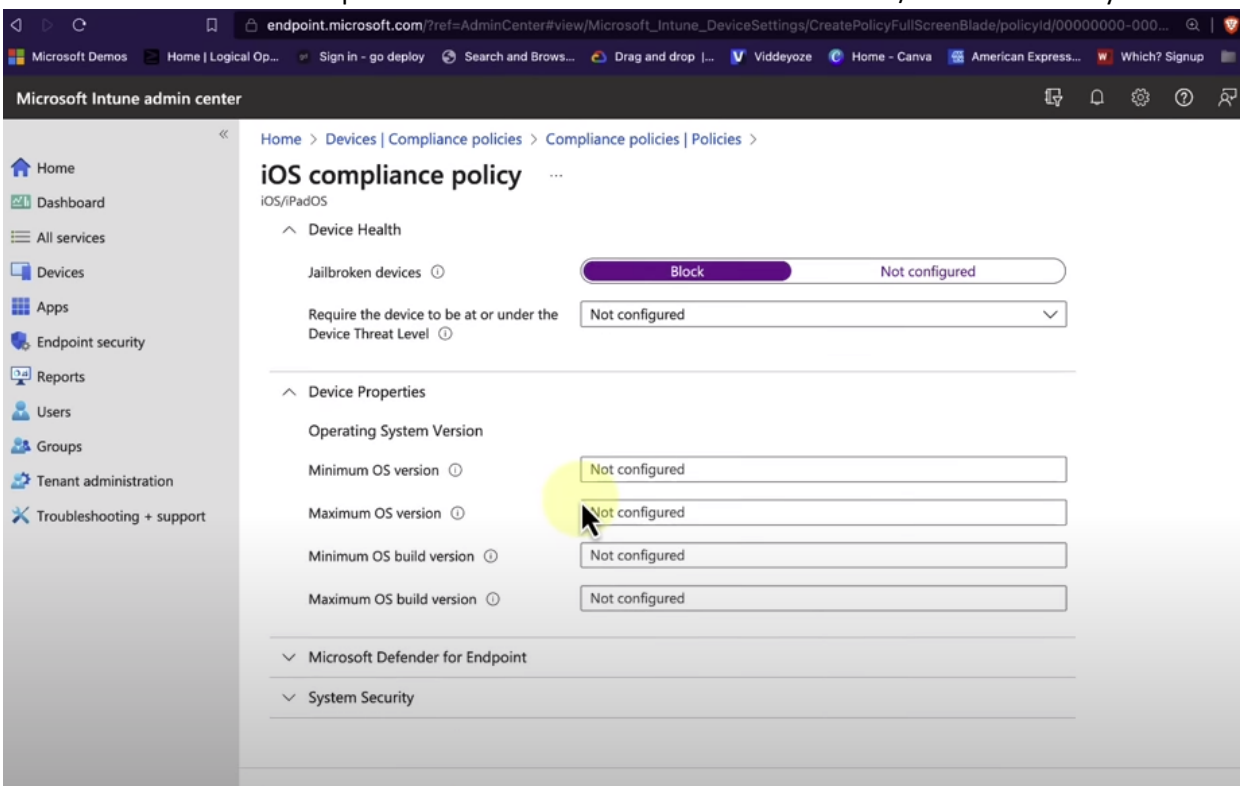
24. Create a profile and Apply to Platform:



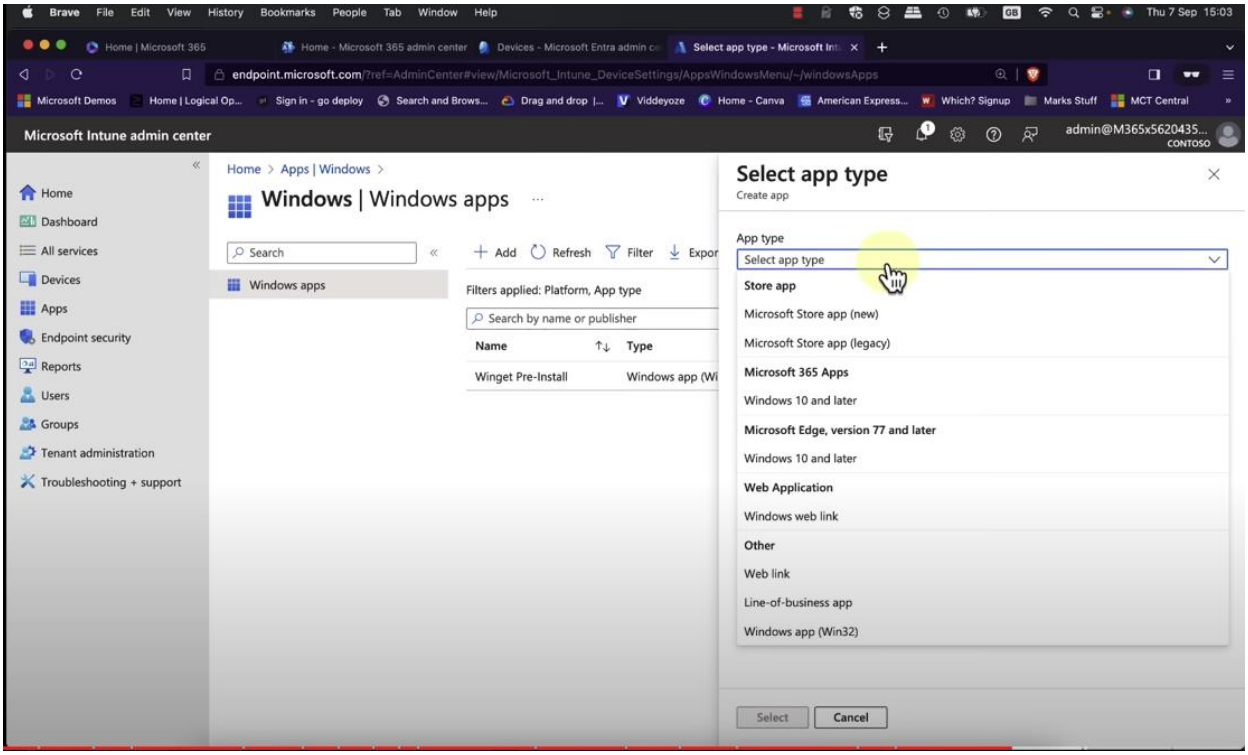
25. Compliance Policy for Policy company :



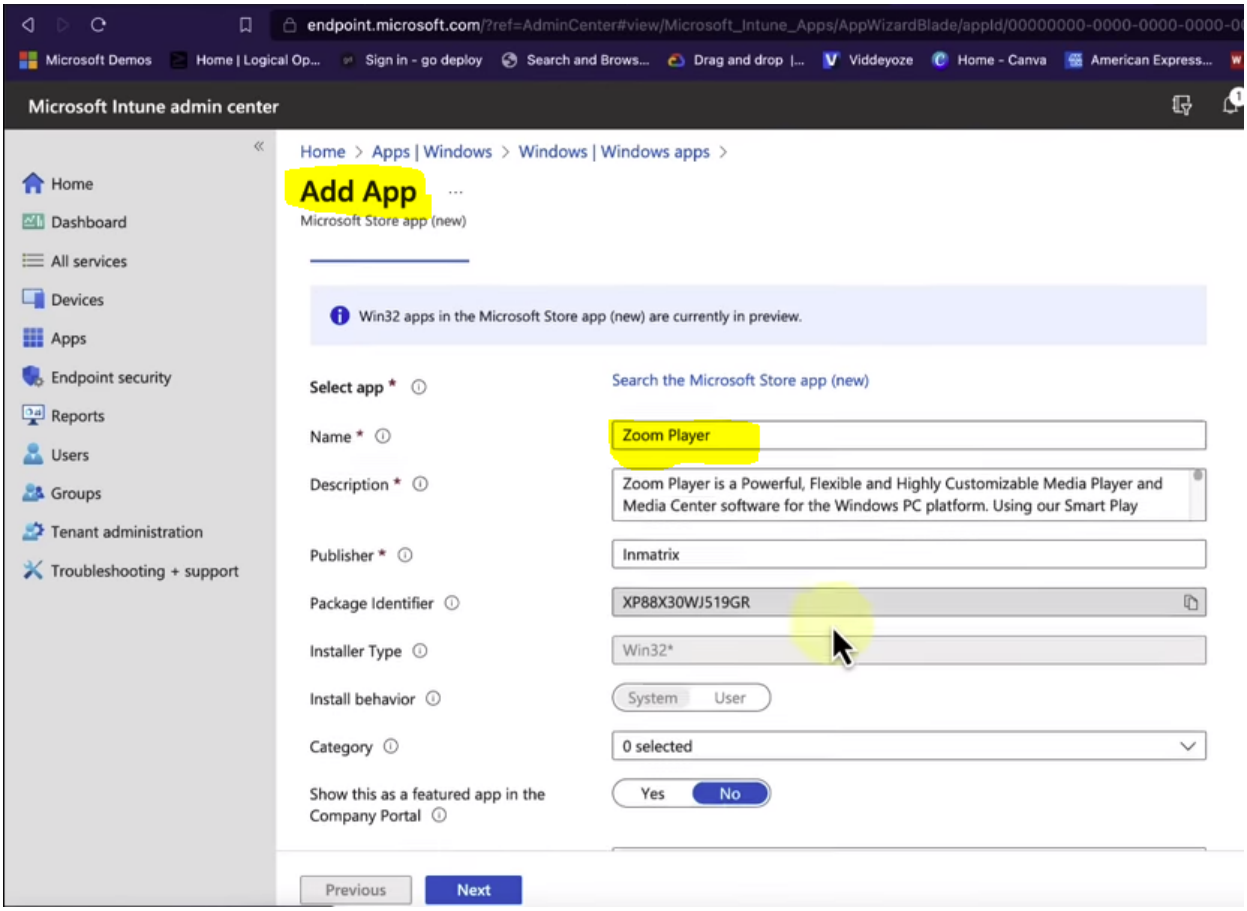
26. No Jailbroken – Password expired – Minutes locked – Send reminder to use/block after 30days.



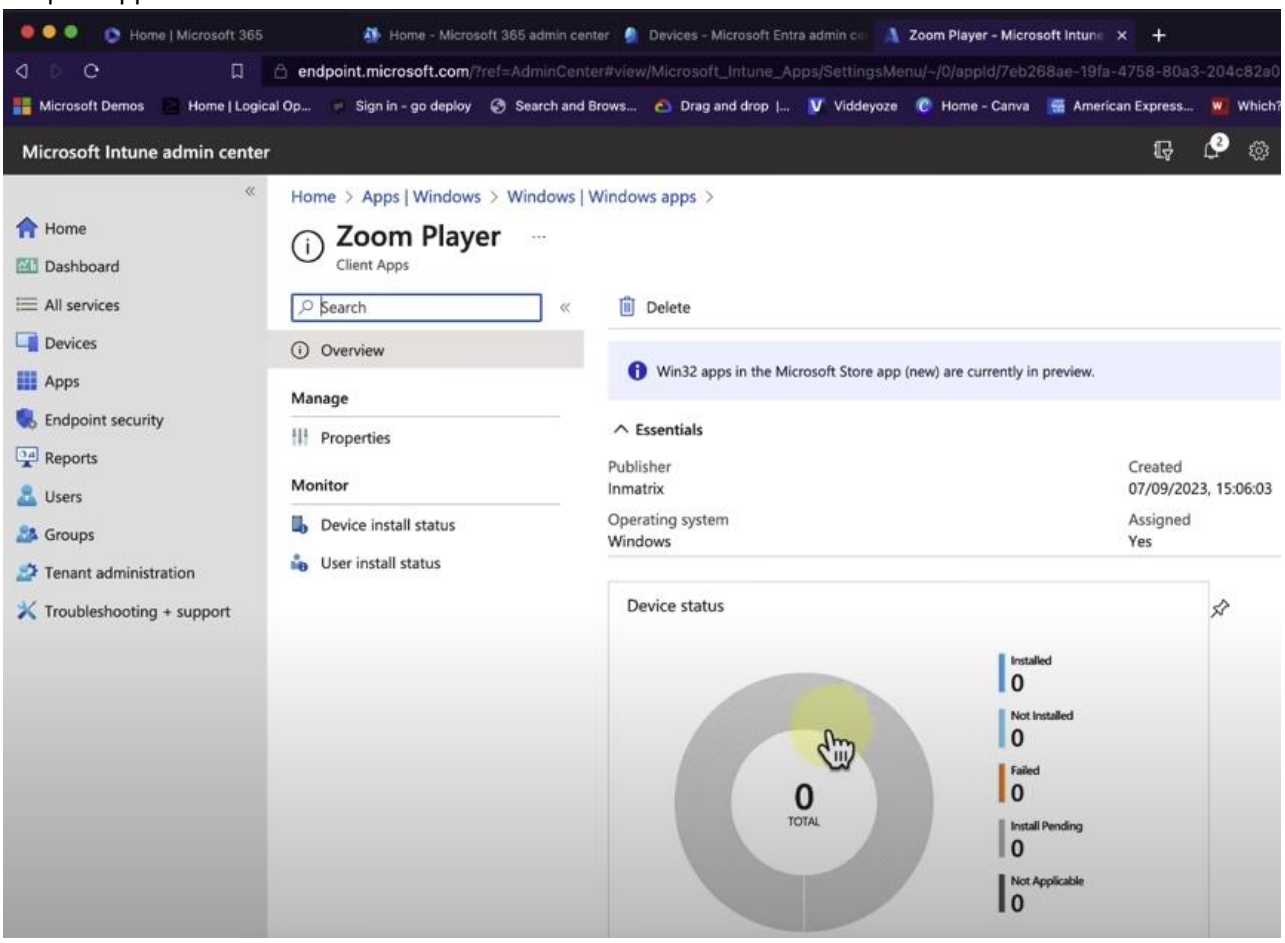
27. Add APPS to inTune to deploy: for device or Windows



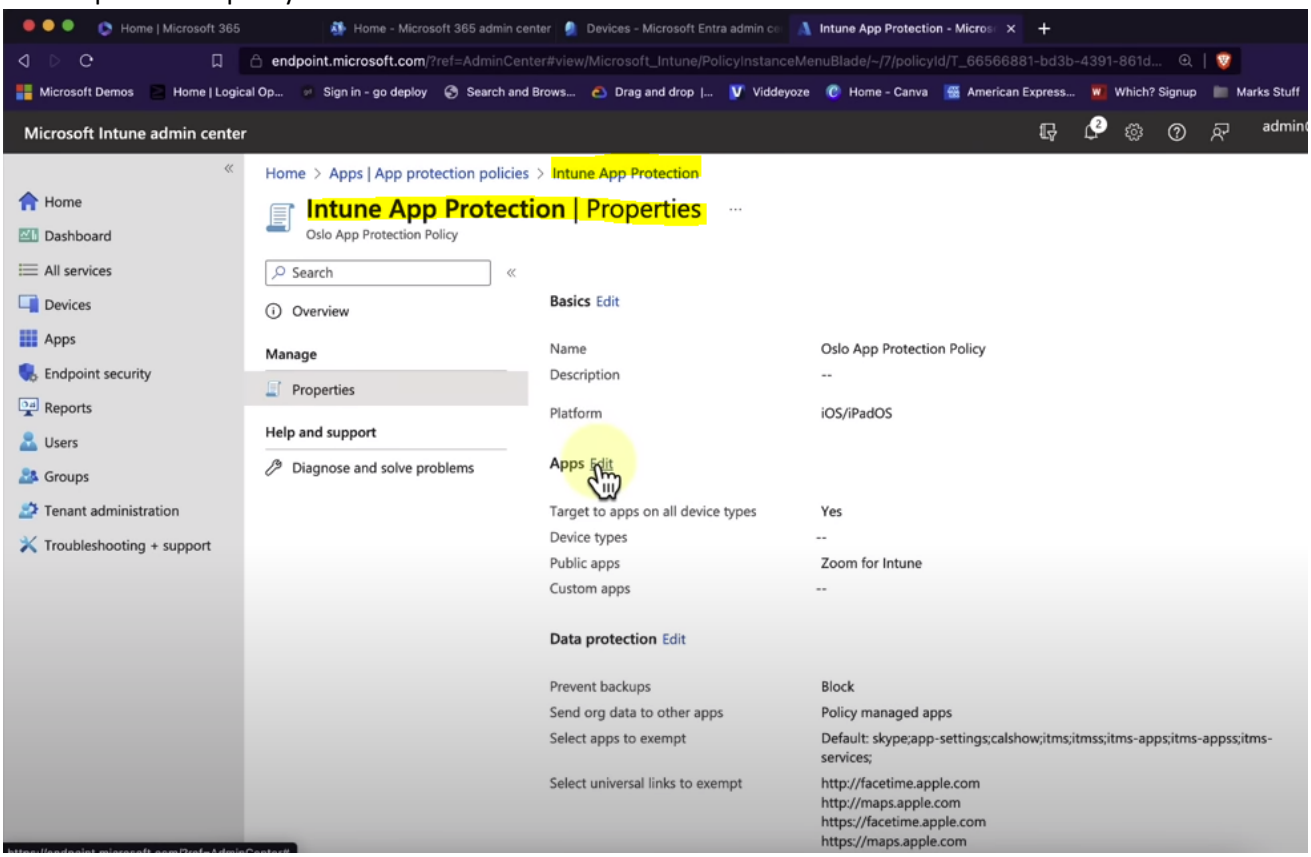
28. Select apps & group enrolled devices



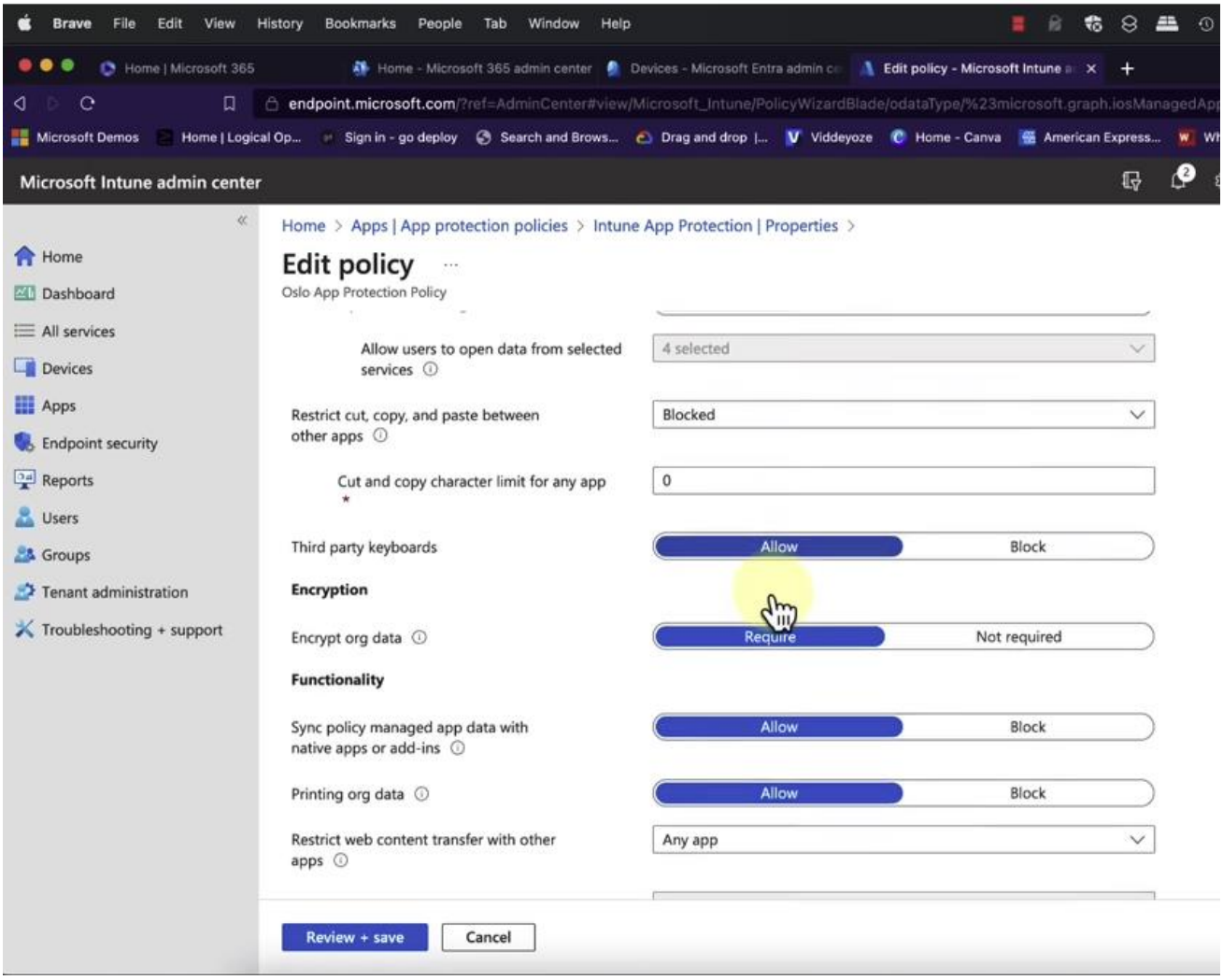
29. Report apps used:



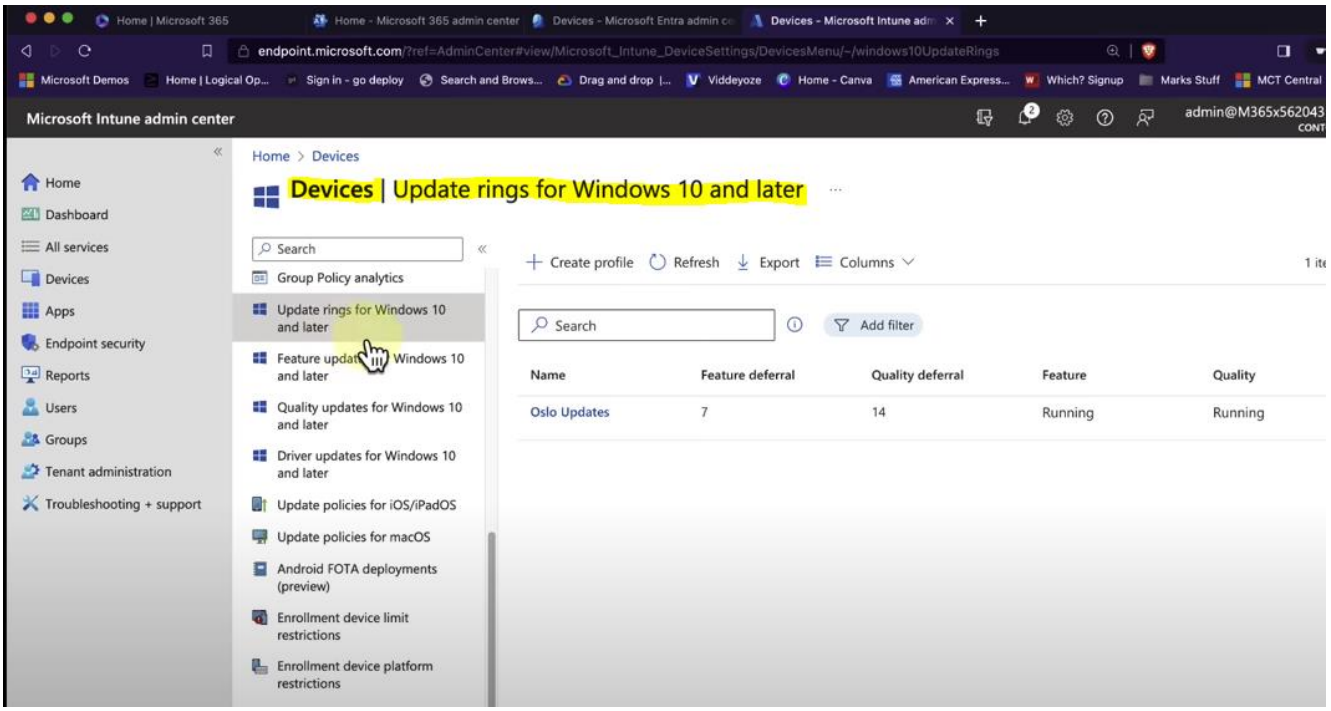
30. Intune protection policy



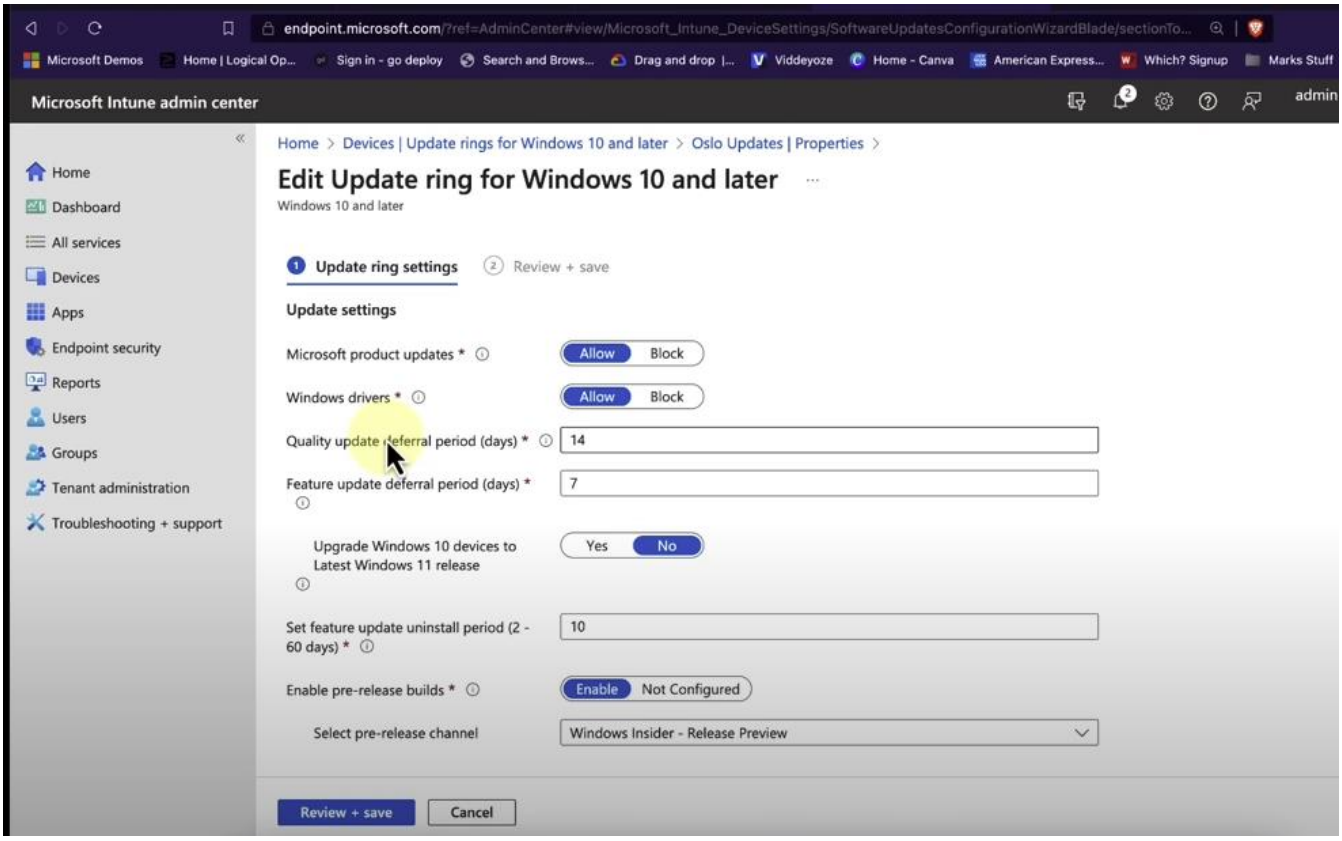
31. Edit Policy apps:



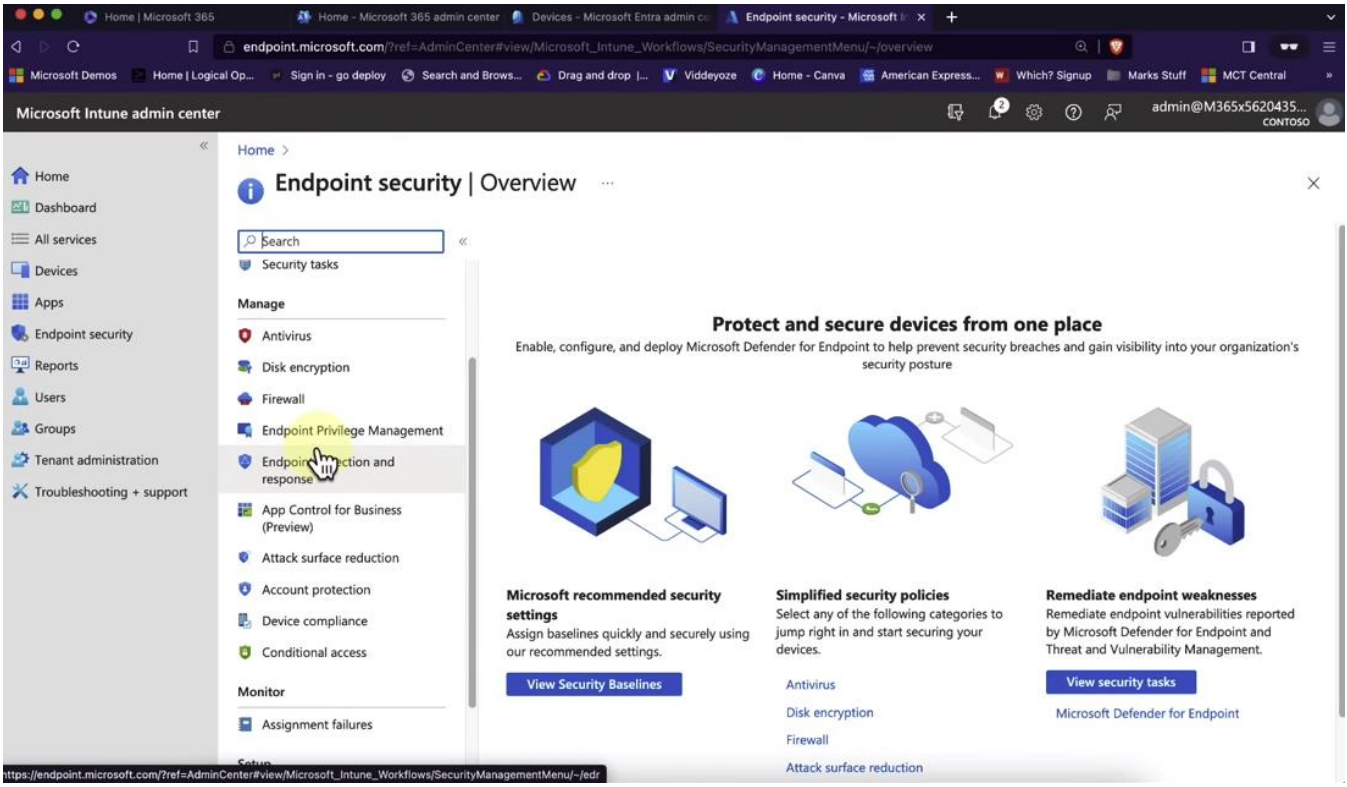
32. Update ring Policy



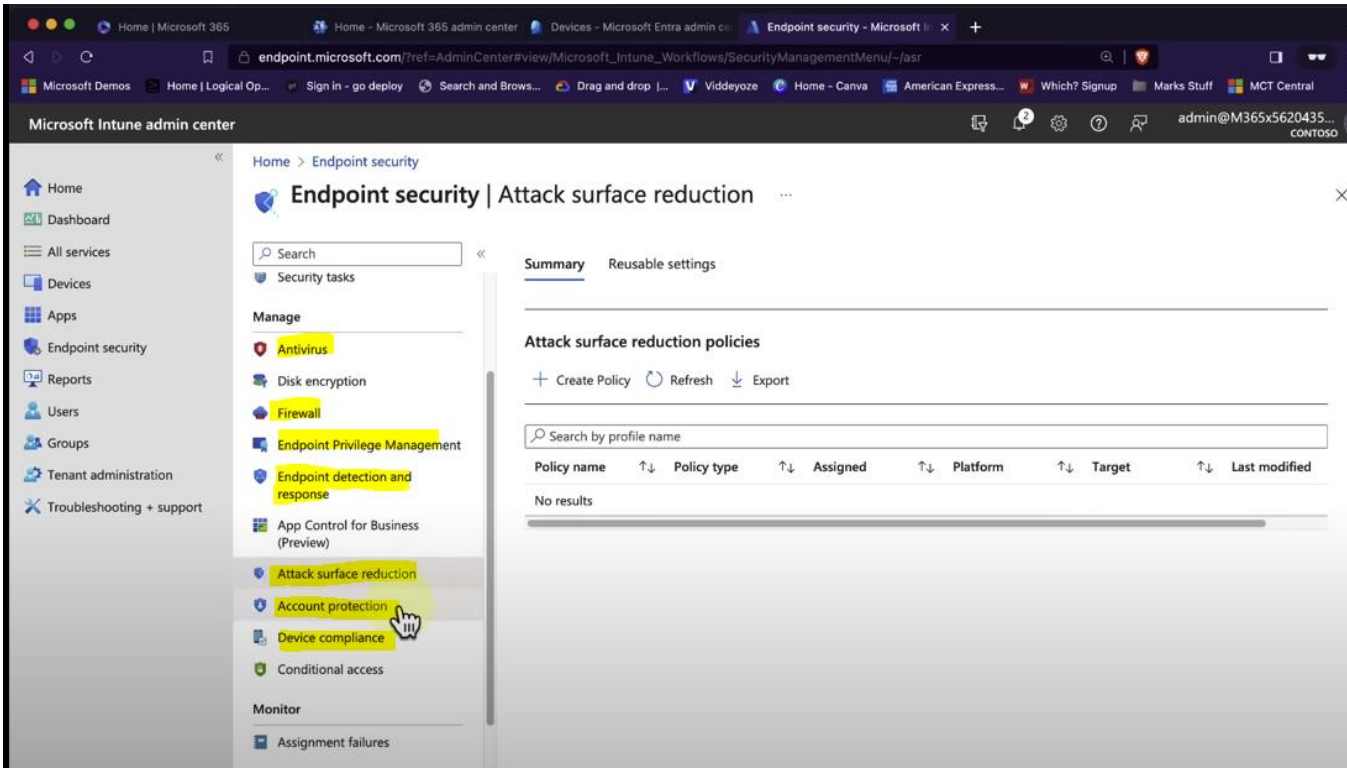
33. Can make to 30days



34. Windows EndPoint security



35. Make Windows compliance Endpoint security



36.

37.