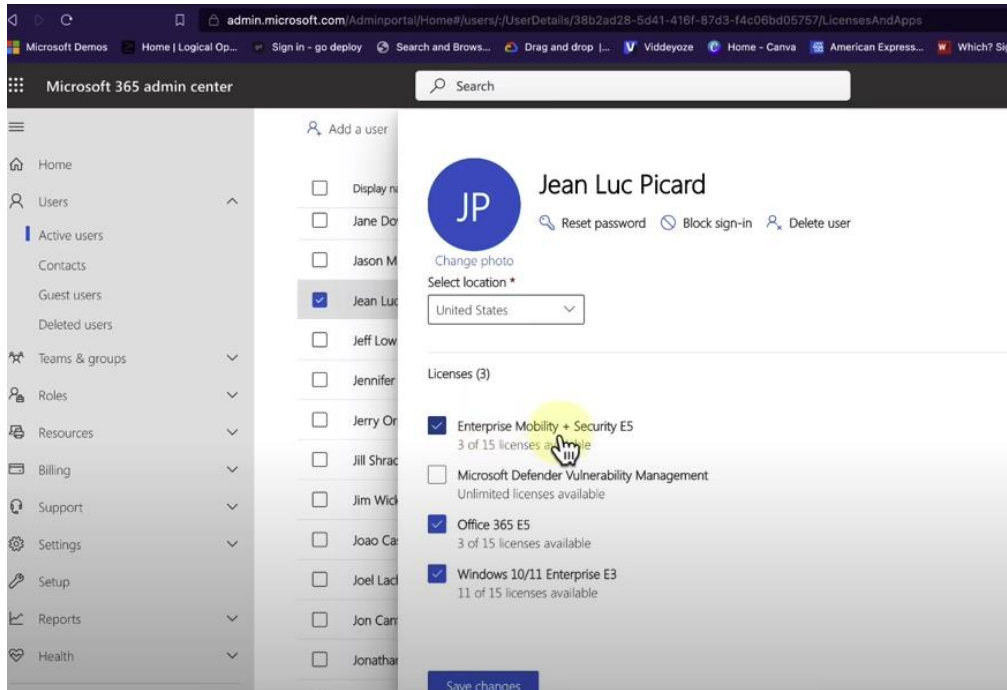


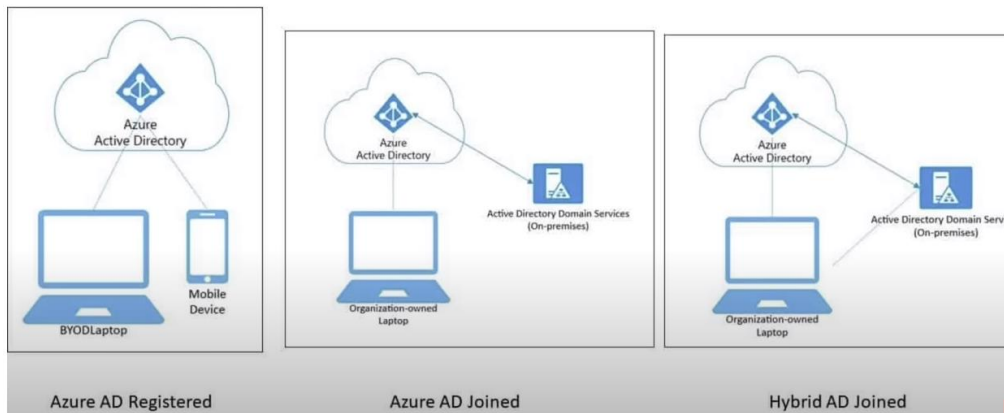
Microsoft Intune in Azure AD-Connect.

1. Step1: Check license for O365

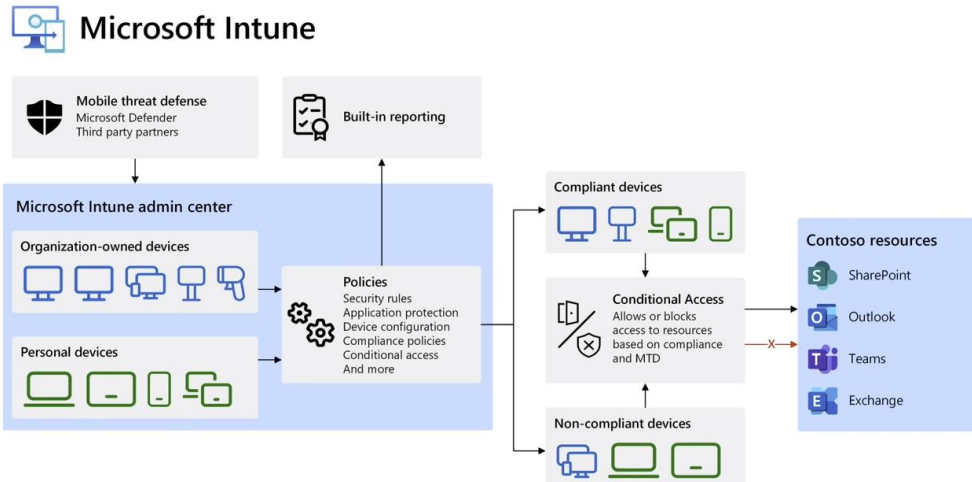


Azure Device Management

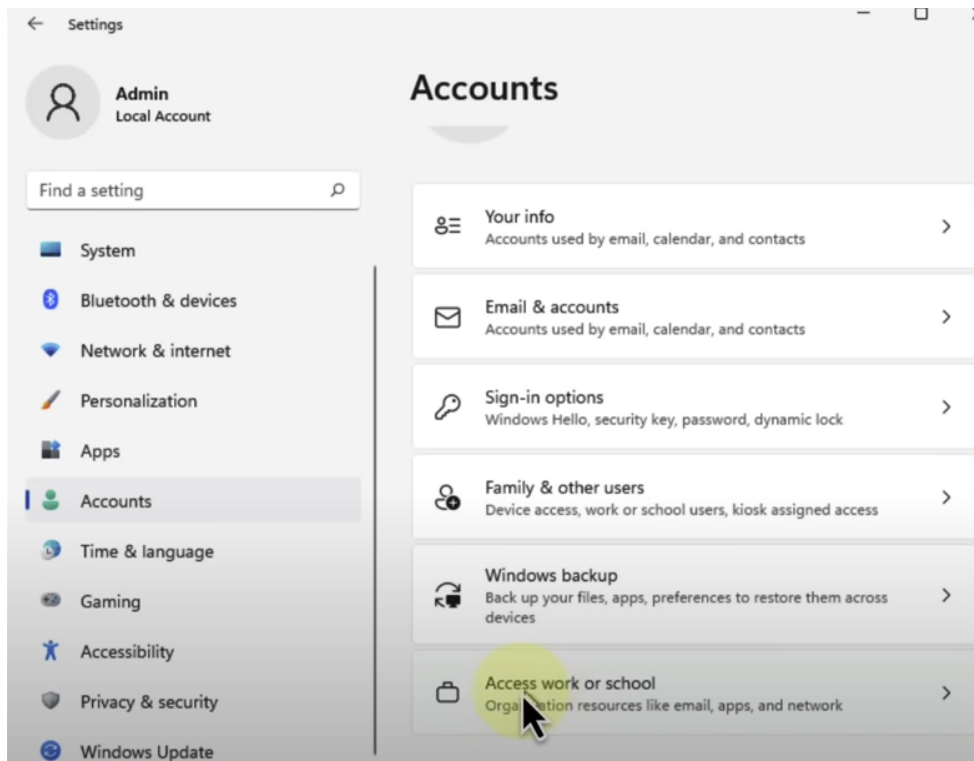
Azure Device Management



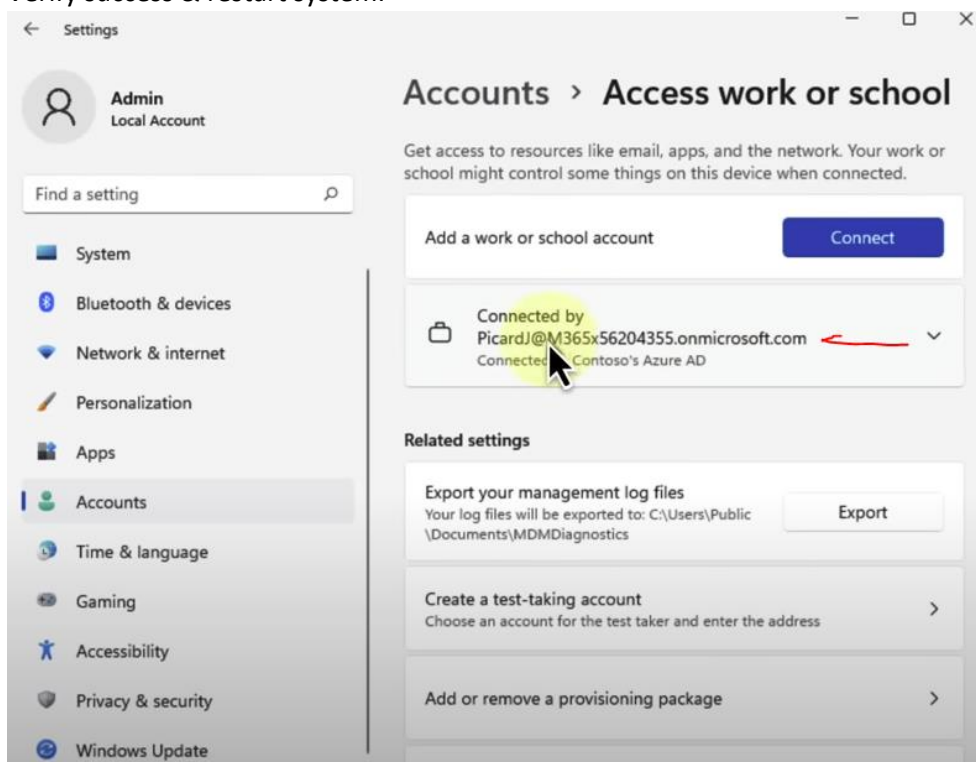
2. Microsoft Intune:



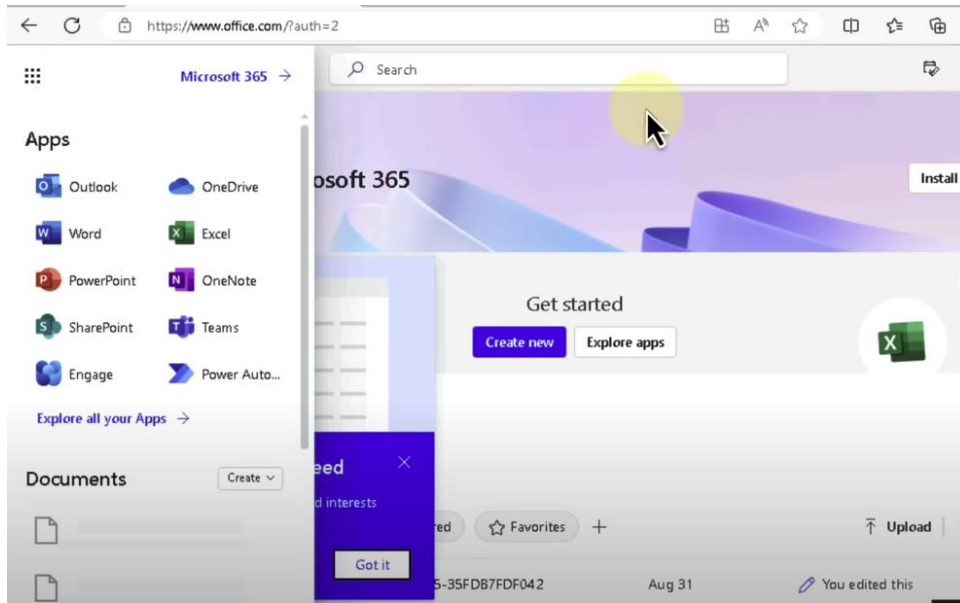
3. EntraID join **Azure AD**: (InTune manage every apps)



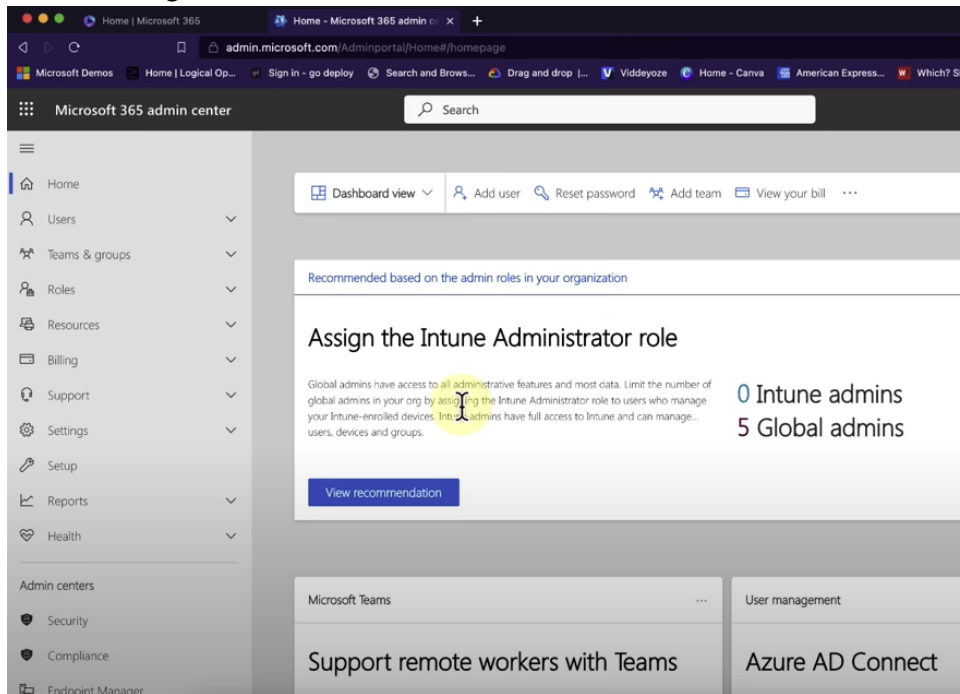
4. Verify success & restart system.



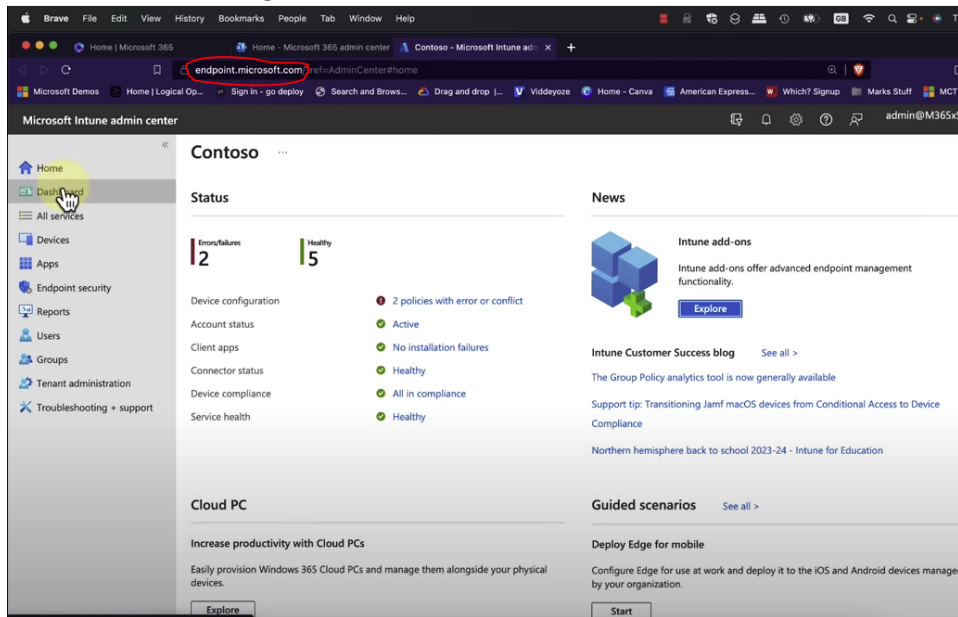
5. Login Workstation and test user account to verify SSO
user AD\account or Email account login



6. Use Admin login - Go to M365 to

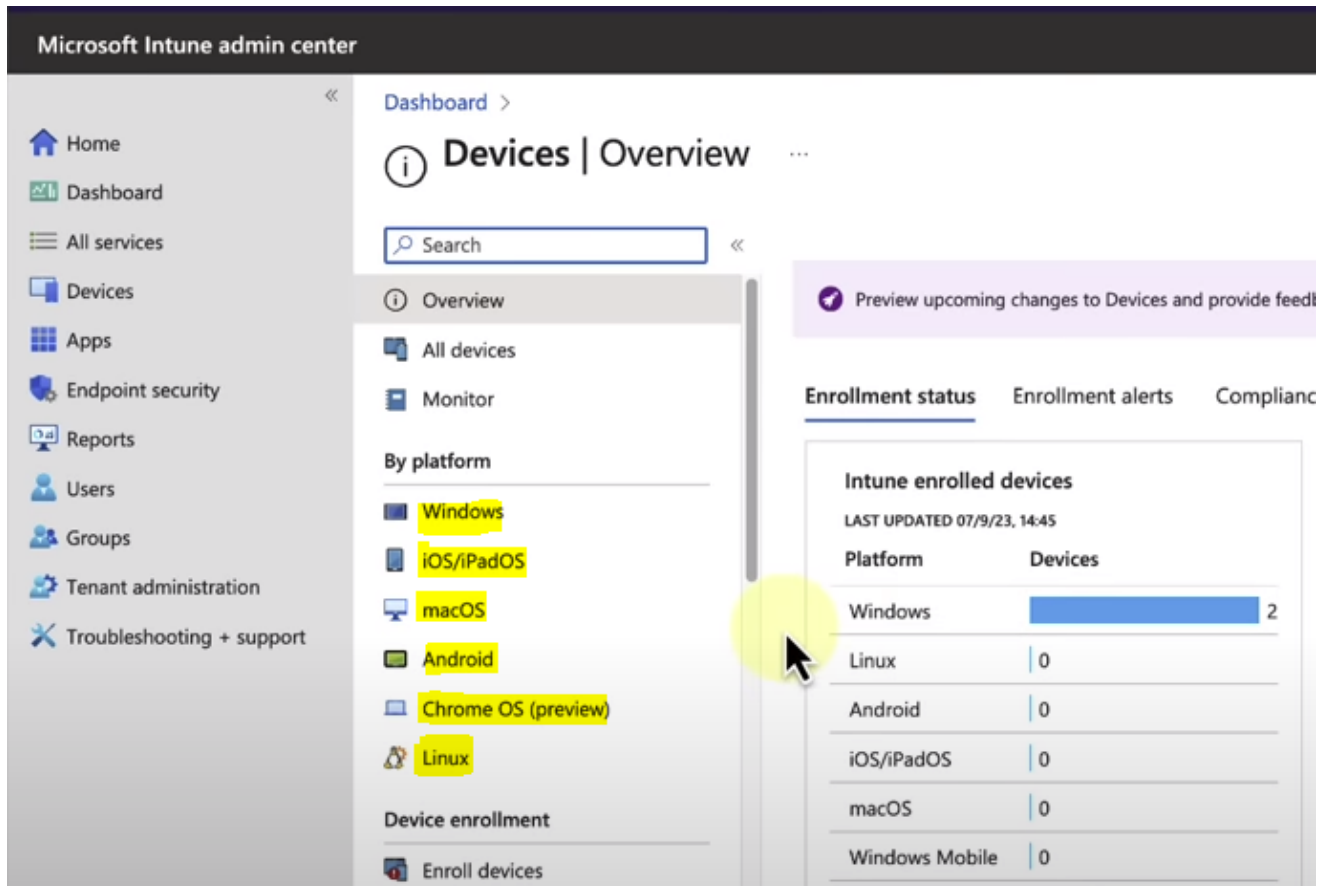


7. Go to EndPoint manager:



8. Go to Devices & Apps & Endpoint security.

9. All Devices enroll



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

Home > Devices

Devices | All devices

Contoso - Azure Active Directory

Download devices Refresh Manage view Enable Disable Delete Manage Preview features

Want to switch back to the legacy devices list experience? Click here to turn off the preview and refresh your browser. You may need to toggle it on and off once more.

Azure Active Directory is becoming Microsoft Entra ID

Search by name or device ID or object ID Add filters

8 devices found

Name	Enabled	OS	Version	Join Type	Owner	MDM
SEA-W10-CL3	Yes	Windows	10.0.19041.1415	Hybrid Azure A...	None	None
SEA-WS1	Yes	Windows	10.0.22000.556	Azure AD joined	Joni Sherman	Microsoft Intune
SEA-WS3	Yes	Windows	10.0.22000.556	Azure AD joined	Jean Luc Picard	Microsoft Intune
SEA-CL1	Yes	Windows	10.0.22000.556	Hybrid Azure A...	None	None
SEA-SVR2	Yes	Windows	10.0.20348.230	Hybrid Azure A...	None	None
SEA-CL2	Yes	Windows	10.0.22000.318	Hybrid Azure A...	None	None
SEA-DC1	Yes	Windows		Hybrid Azure A...	None	None
SEA-SVR1	Yes	Windows	10.0.20348.230	Hybrid Azure A...	None	None

11. Go to Entra admin Center:

Home > Mobility (MDM and MAM) (Preview)

Browse Azure AD MDM Gallery

Create your own application Got feedback?

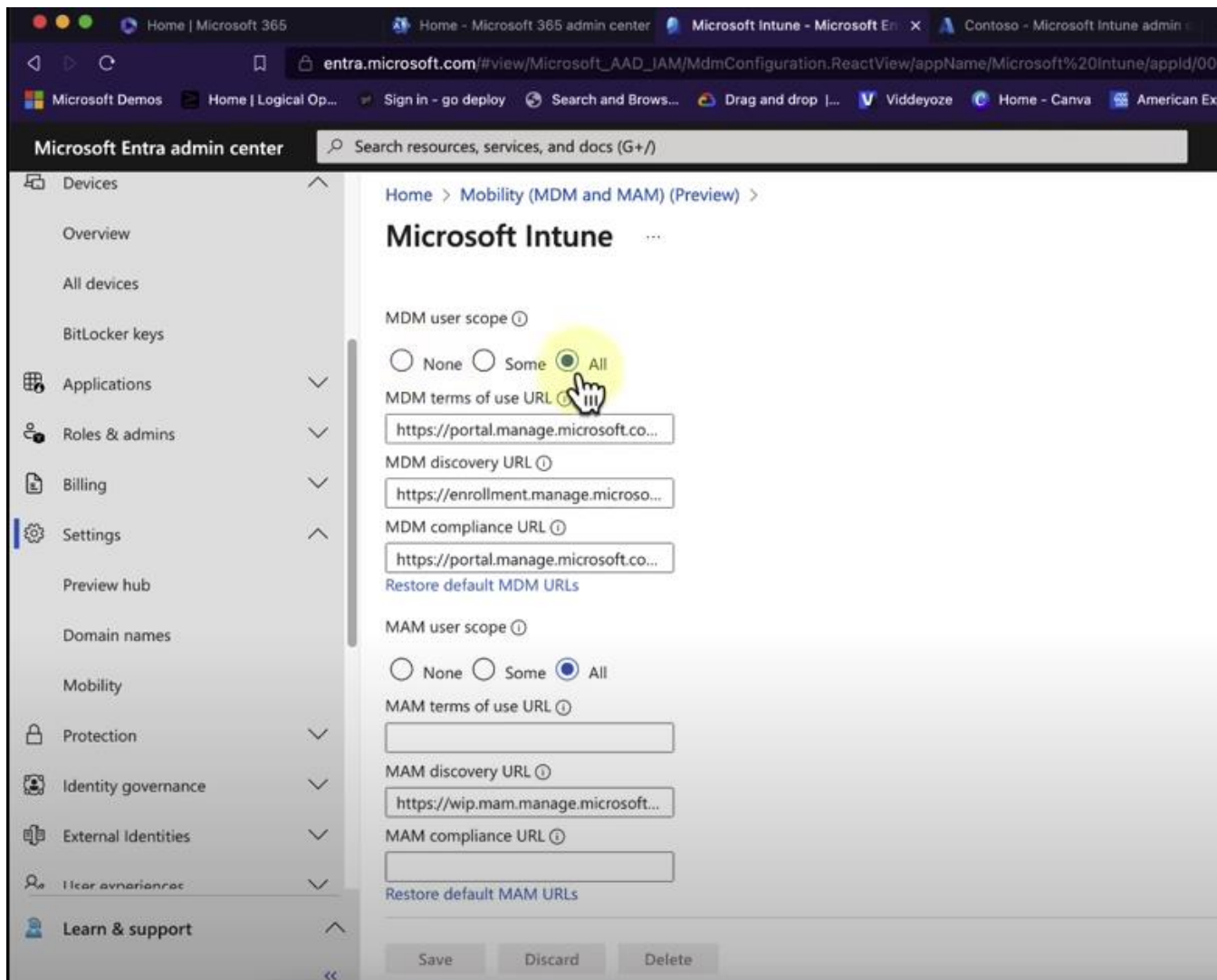
Integrating Azure AD with MDM (Mobile Device Management) allows you to enforce compliance in devices with corporate policies, add or remove applications from the compliance status, and more. [Learn more](#)

Pre-integrated MDM applications

Search application

- AirWatch by VMware
- AppTec360 MDM
- FENCE-Mobile RemoteManager MDM
- Hexnode UEM
- IBM MaaS360
- KACE Cloud
- ManageEngine MDM
- Microsoft Intune
- Miradore Online

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 admin center Devices - Microsoft Intune admin center

entra.microsoft.com/view/Microsoft_AAD_Devices/DevicesMenuBlade/-/DeviceSettings/menuld/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+/)

Home > Devices

Devices | Device settings Contoso - Azure Active Directory

Save Discard Got feedback?

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

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

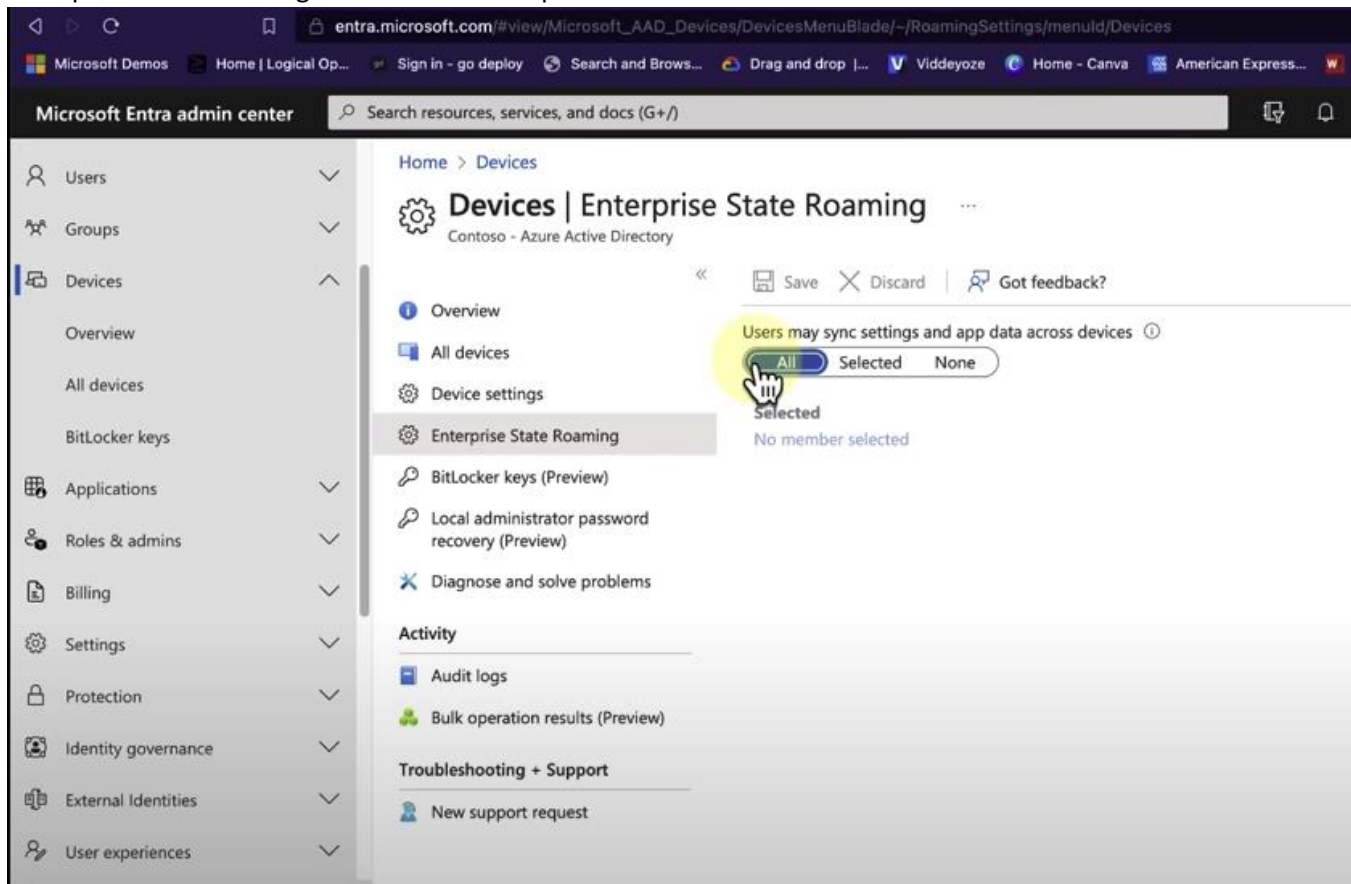
Learn more on how this setting works

Require Multi-Factor Authentication to register or join devices with Azure AD ⓘ

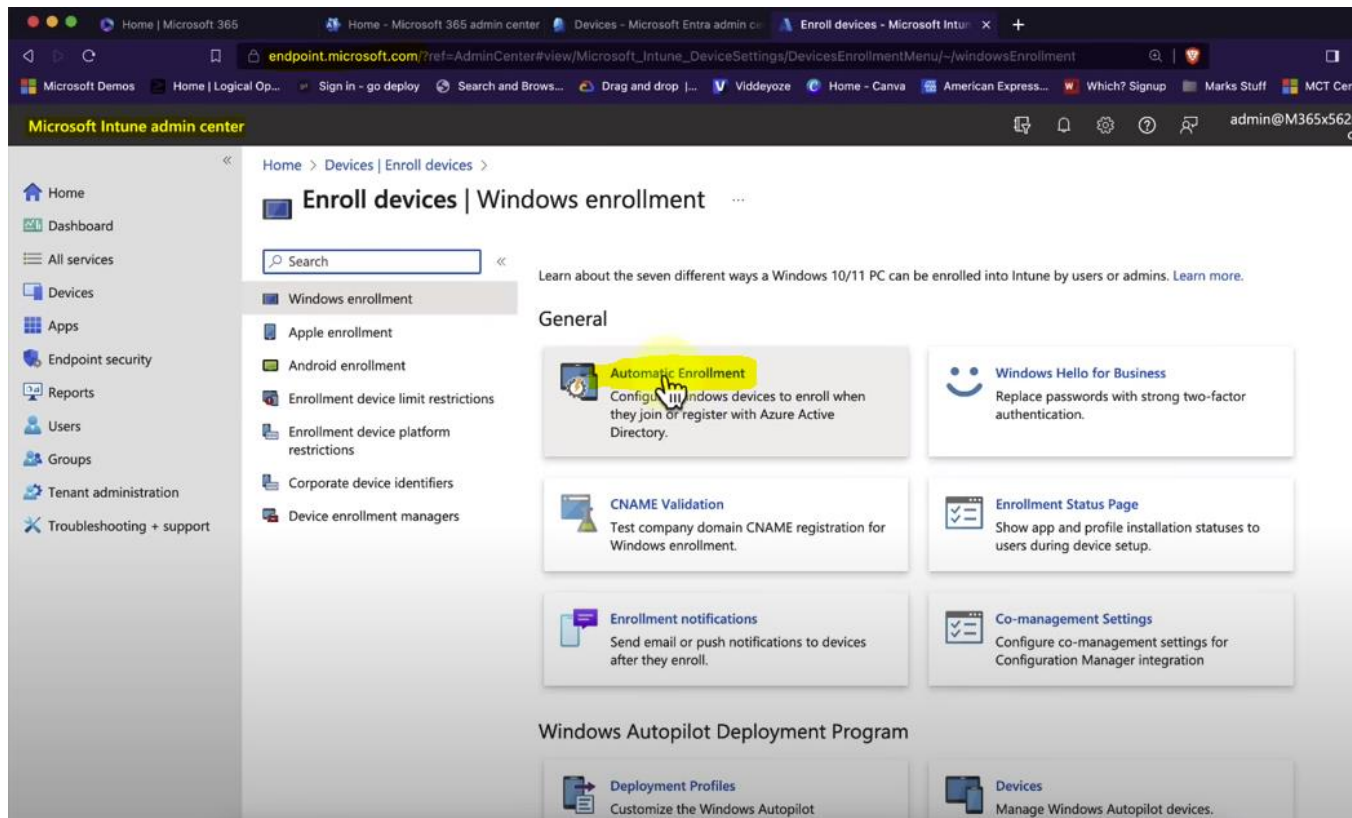
Yes No

⚠ We recommend that you require Multi-Factor Authentication to register or join devices with Azure AD. [Access](#). Set this device setting to No if you require Multi-Factor Authentication using Conditional Access.

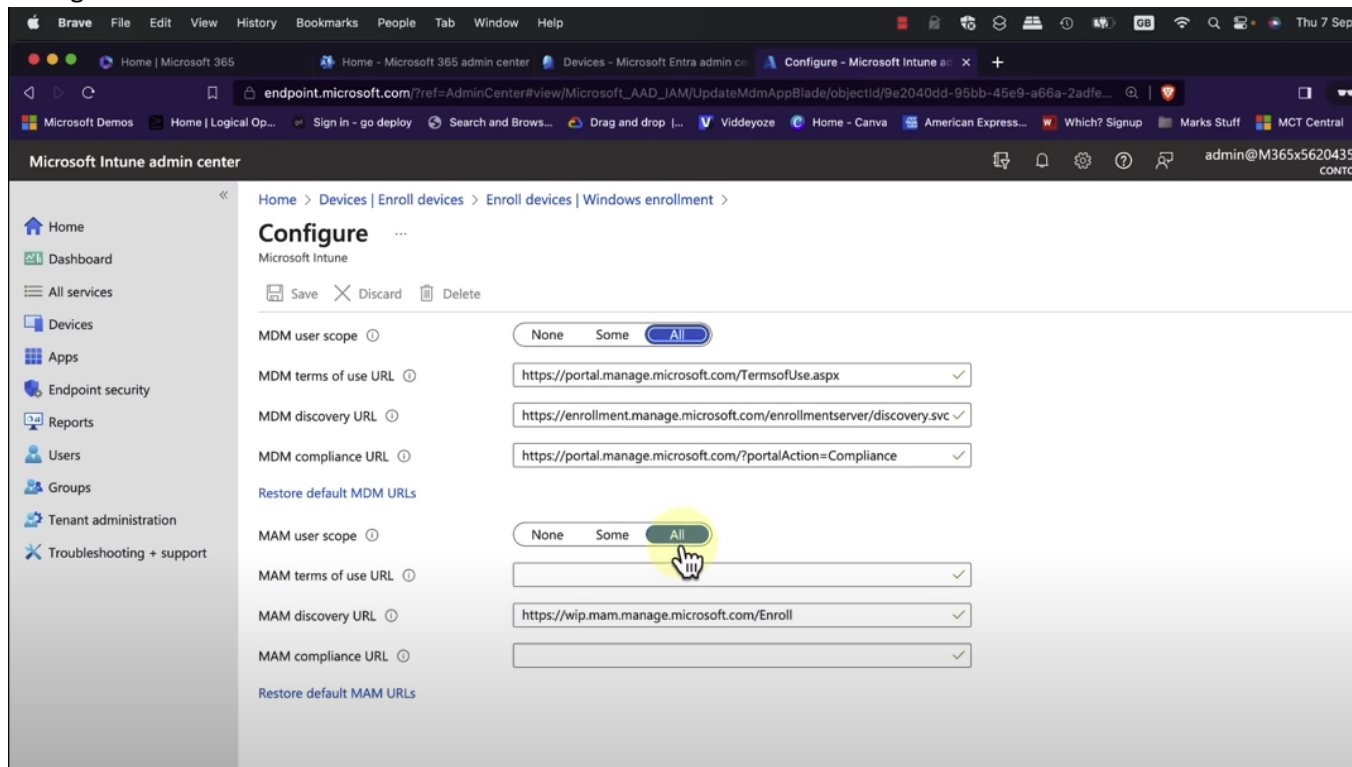
14. Enterprise State Roaming – Good idea to keep on



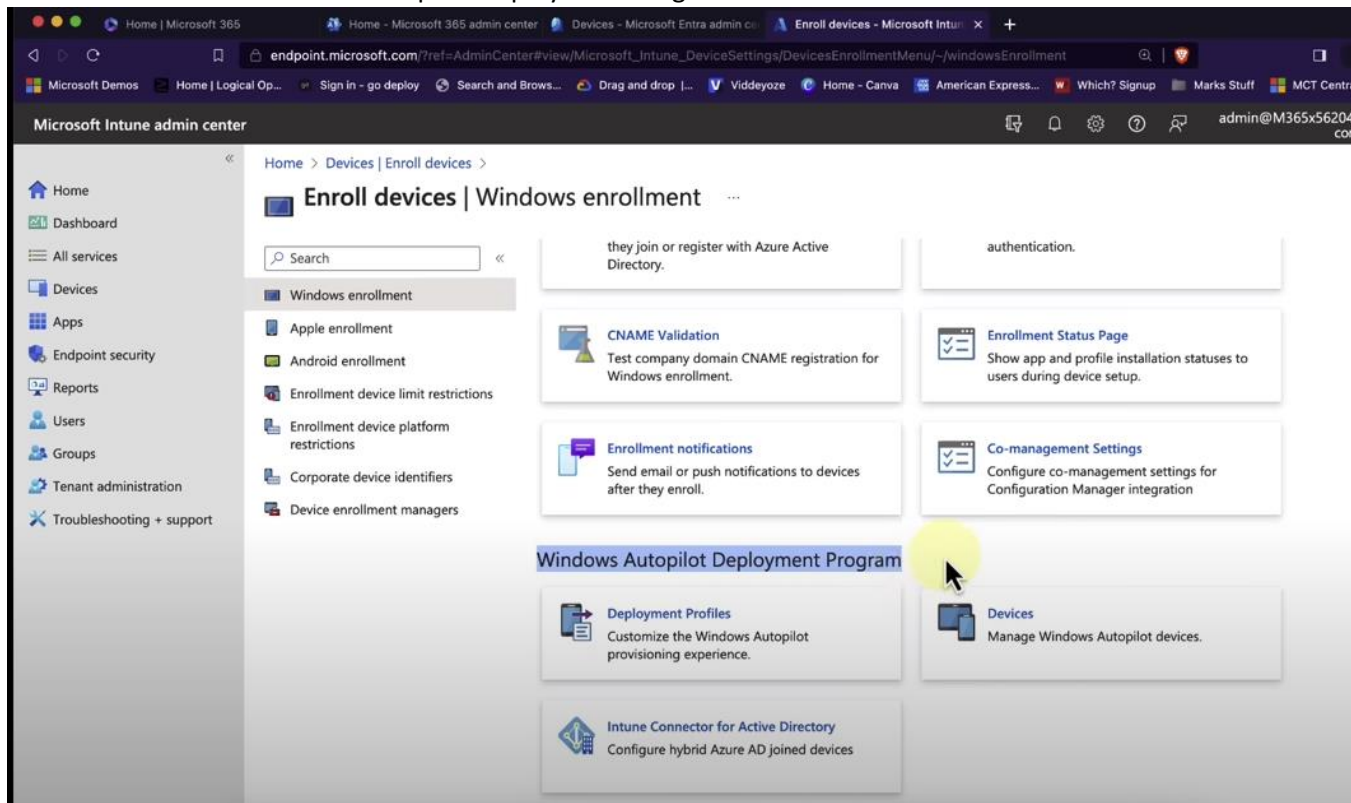
15. Go to Intune admin and Set Automatic Enrollment: All & All



16. Configure to enroll all



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



18. Apple enrollment need MDM push CERTIFICATE :

Brave File Edit View History Bookmarks People Tab Window Help

Home | Microsoft 365 Home - Microsoft 365 admin center Devices - Microsoft Entra admin center 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 devices. You need to create an Apple MDM Push certificate to begin. [Learn more.](#)

Prerequisites

Apple MDM Push certificate

Create an Apple MDM Push certificate required to manage Apple devices

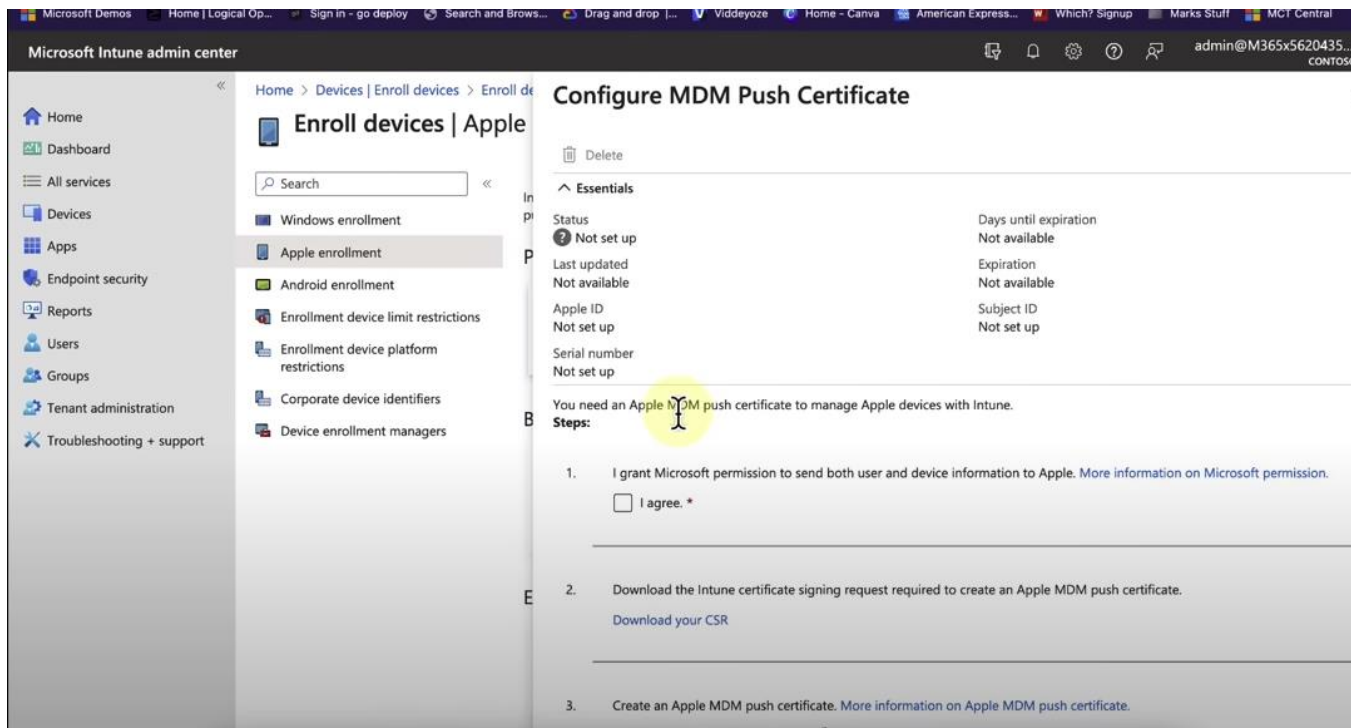
Bulk enrollment methods

Apple Configurator

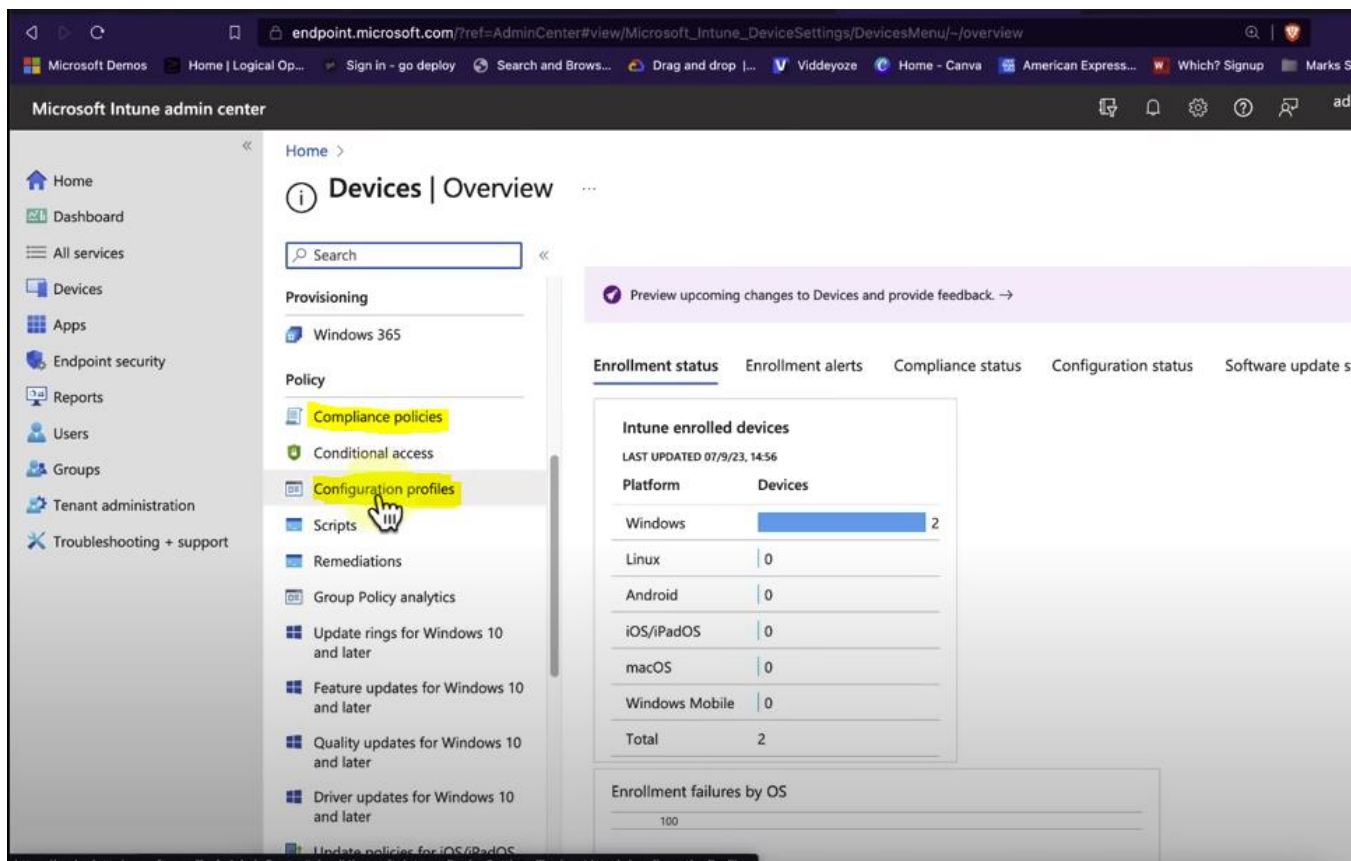
Manage Apple Configurator enrollment

Enrollment options

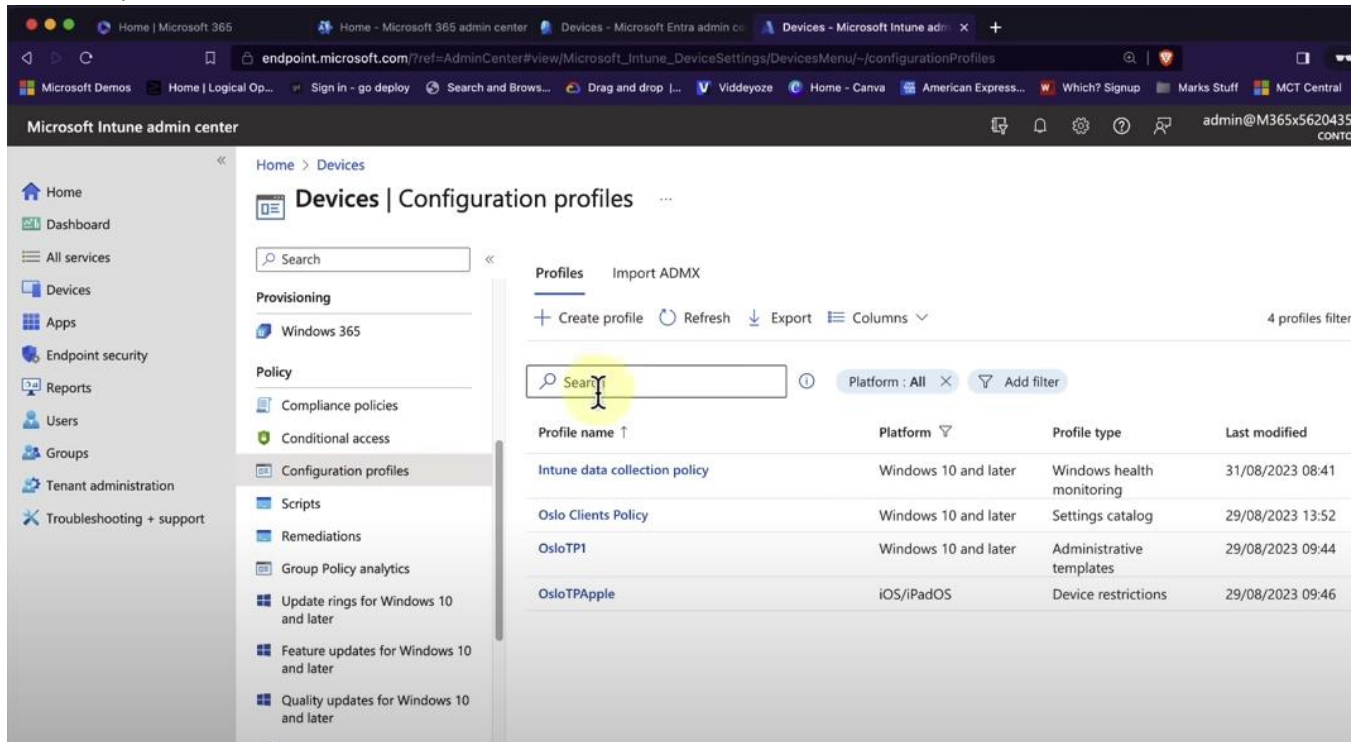
19.



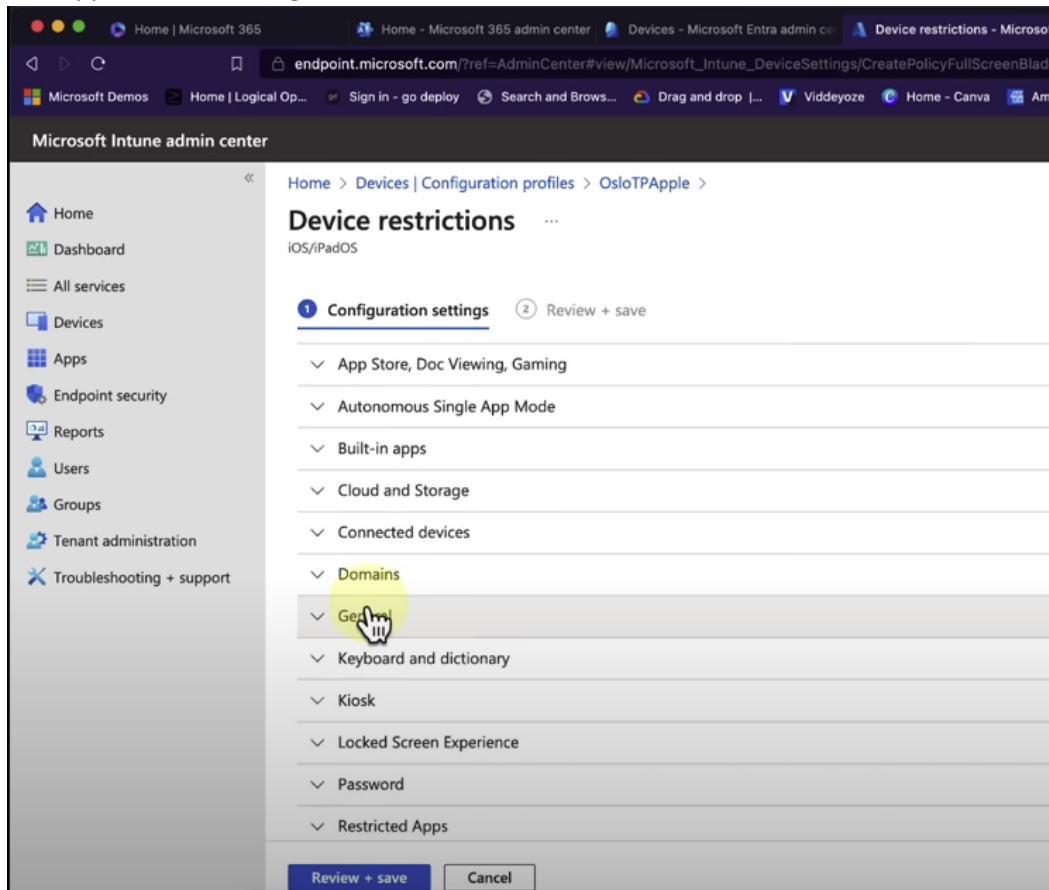
20. After device enroll, configuration policy and profiles



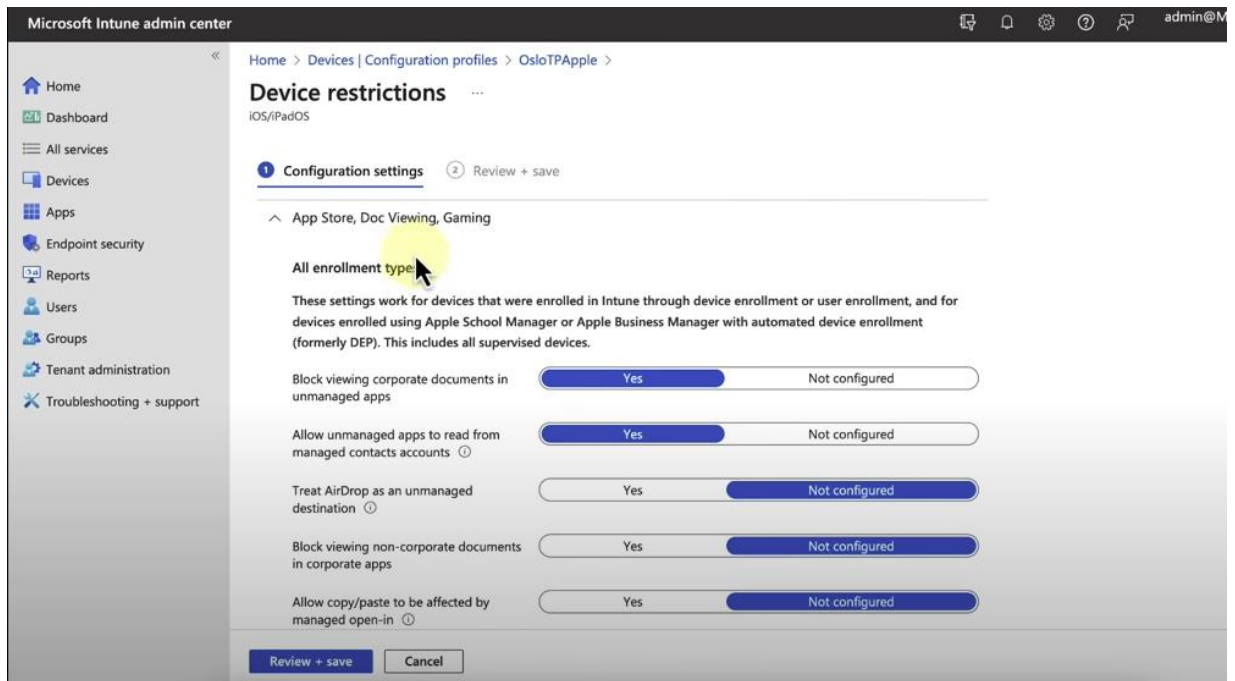
21. Create a profile :



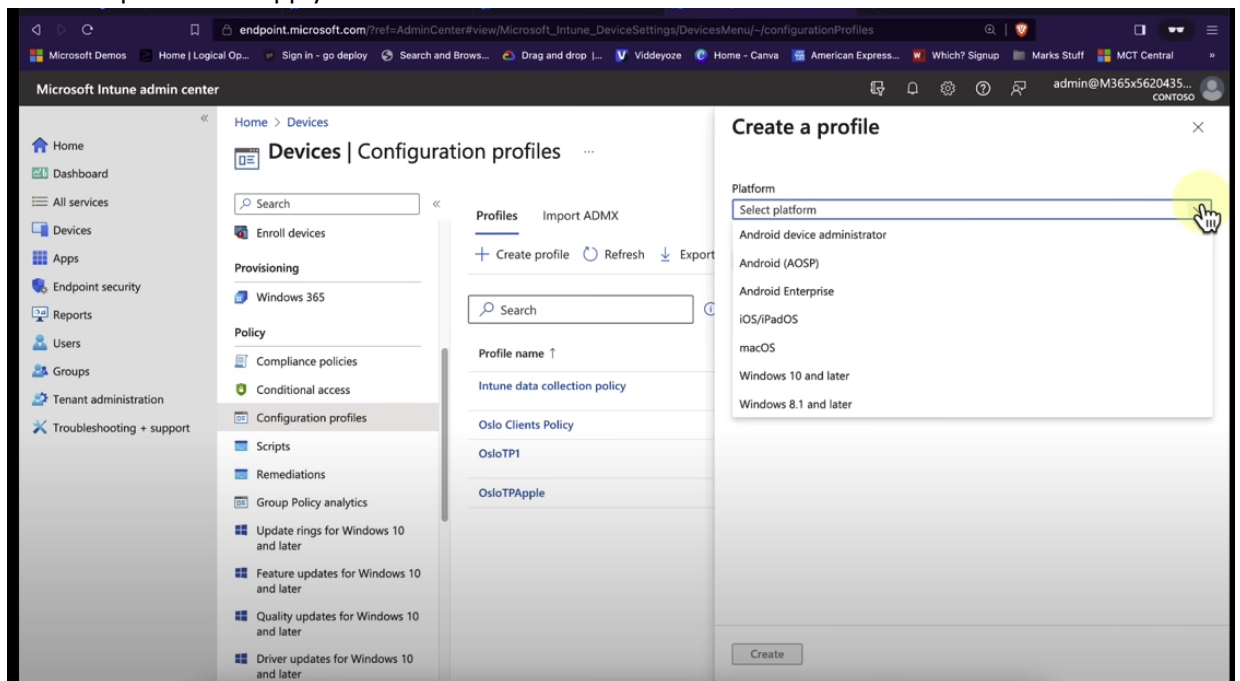
22. Set Apple devices configure restrictions



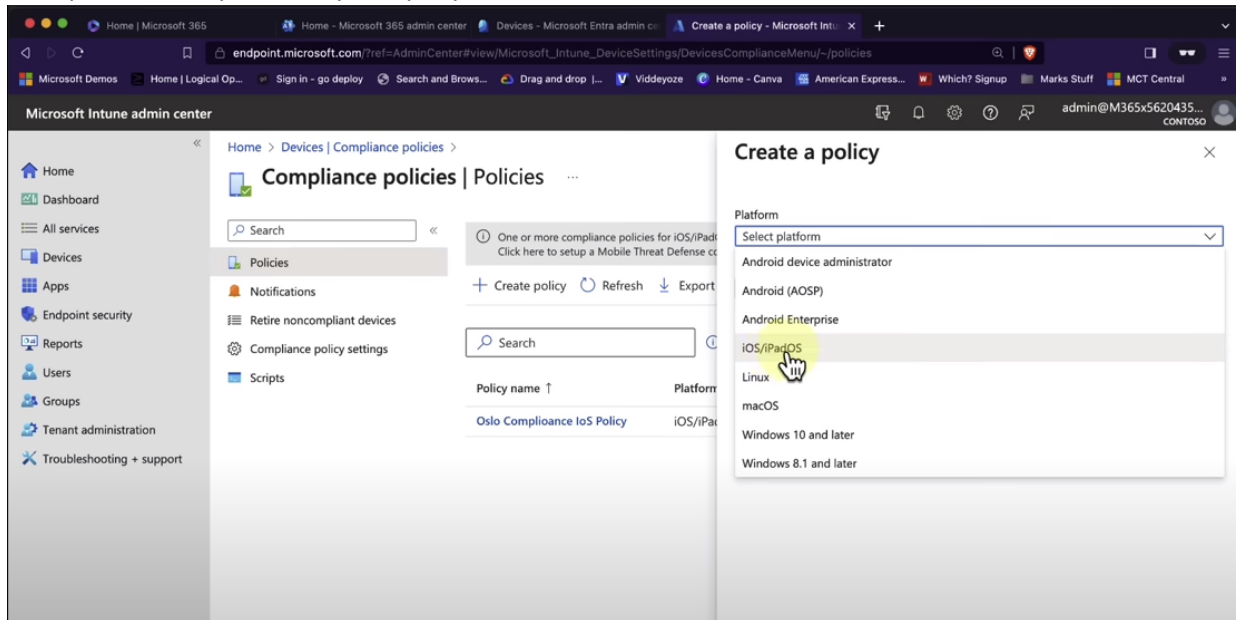
23. & Detail restrictions:



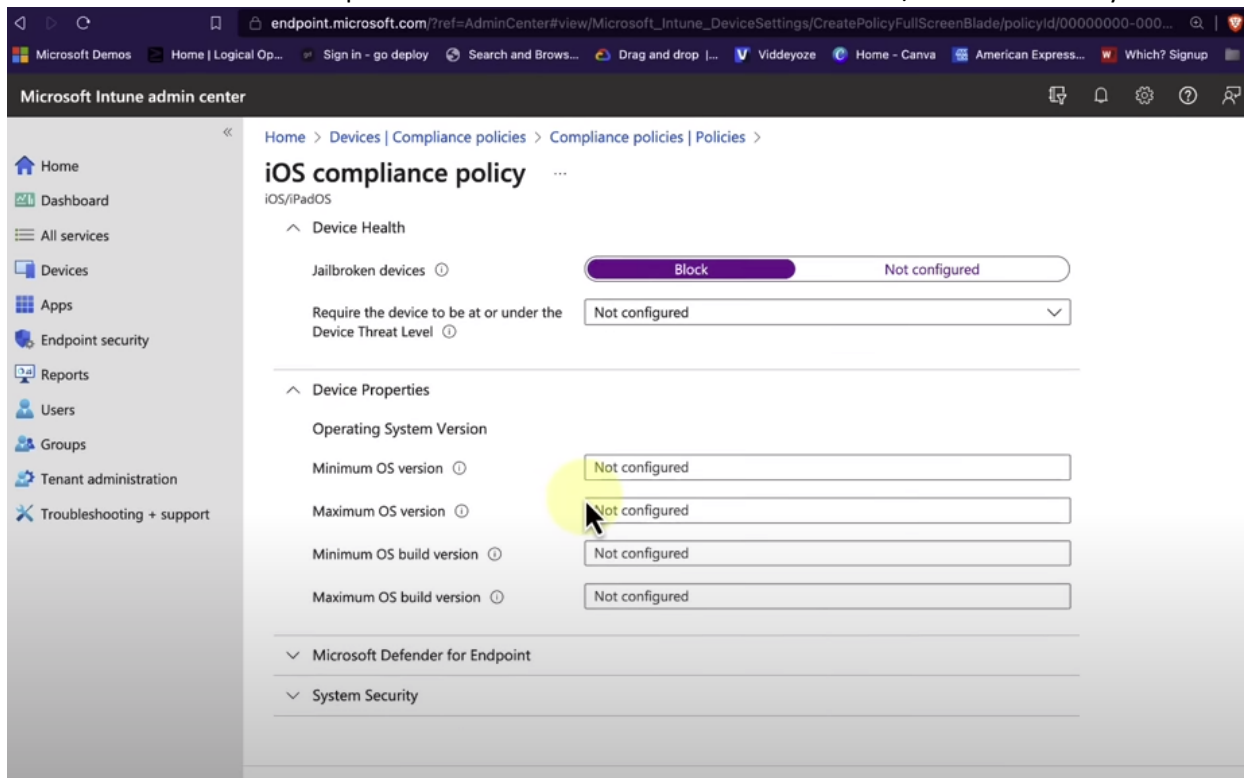
24. Create a profile and Apply to Platform:



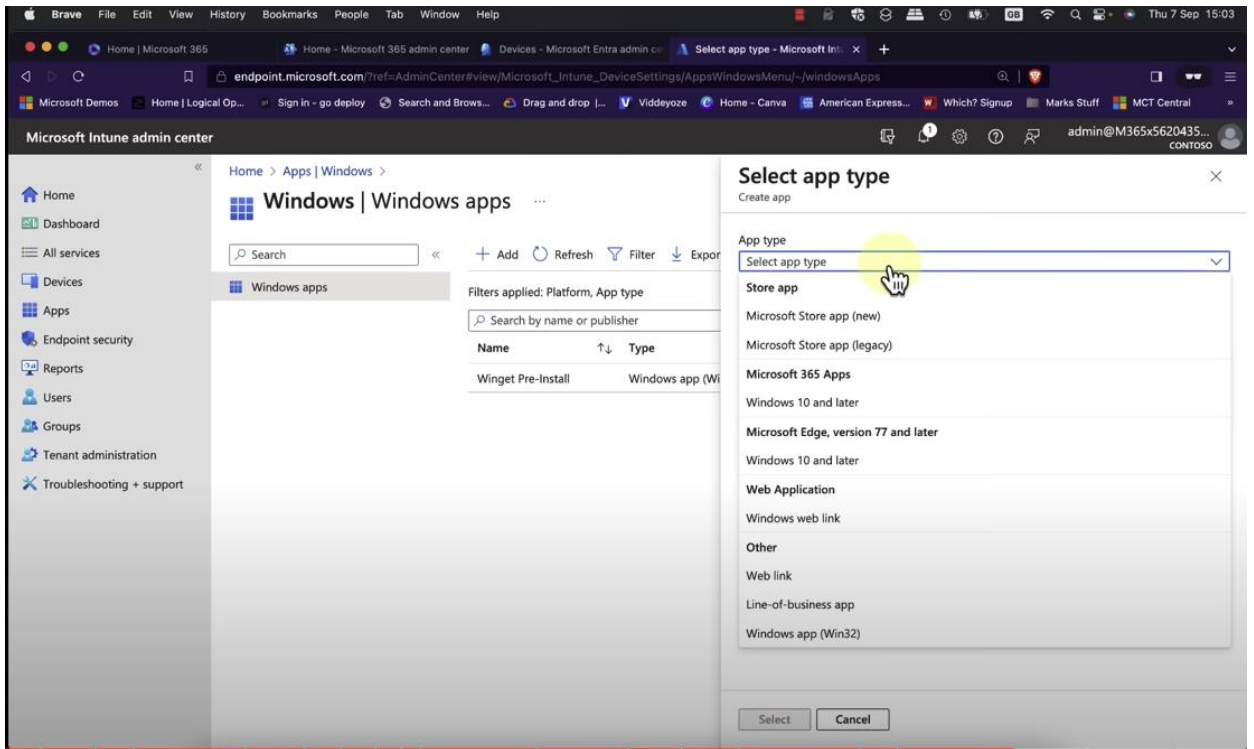
25. Compliance Policy for Policy company :



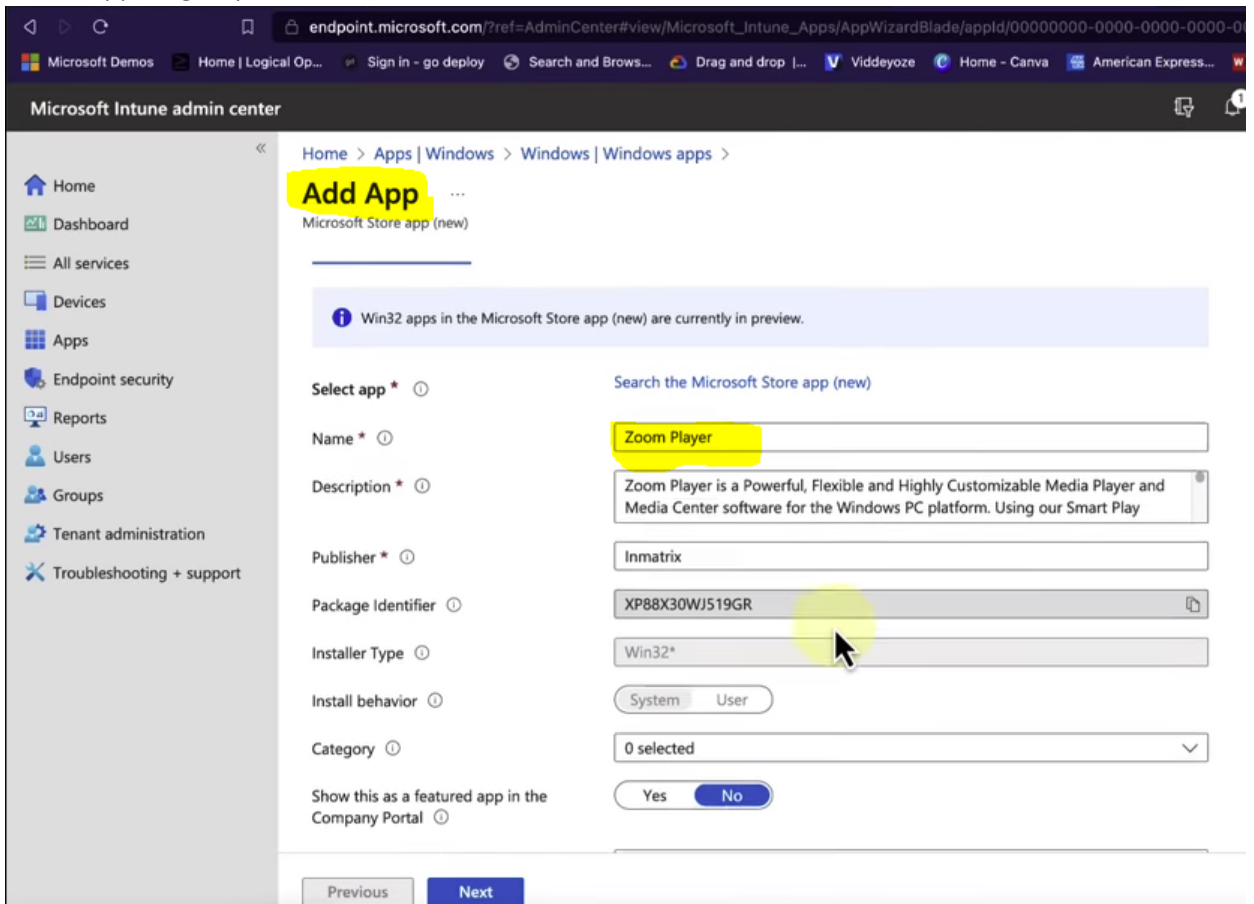
26. No Jailbroken – Password expired – Minutes locked – Send reminder to use/block after 30days.



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



28. Select apps & group enrolled devices



29. Report apps used:

The screenshot displays the Microsoft Intune admin center interface. The left sidebar contains navigation links: Home, Dashboard, All services, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area shows the 'Zoom Player' app details under the 'Apps > Windows > Windows apps' path. The app is categorized as a 'Client App'. A search bar and a 'Delete' button are visible. The 'Overview' tab is selected, showing a 'Manage' section with 'Properties' and a 'Monitor' section with 'Device install status' and 'User install status'. A notification banner states: 'Win32 apps in the Microsoft Store app (new) are currently in preview.' The 'Essentials' section displays the following information:

Property	Value	Created
Publisher	Inmatrix	07/09/2023, 15:06:03
Operating system	Windows	Assigned
		Yes

The 'Device status' section features a donut chart showing the distribution of app installations across devices. The chart indicates 0 total installations. A legend on the right lists the following categories and counts:

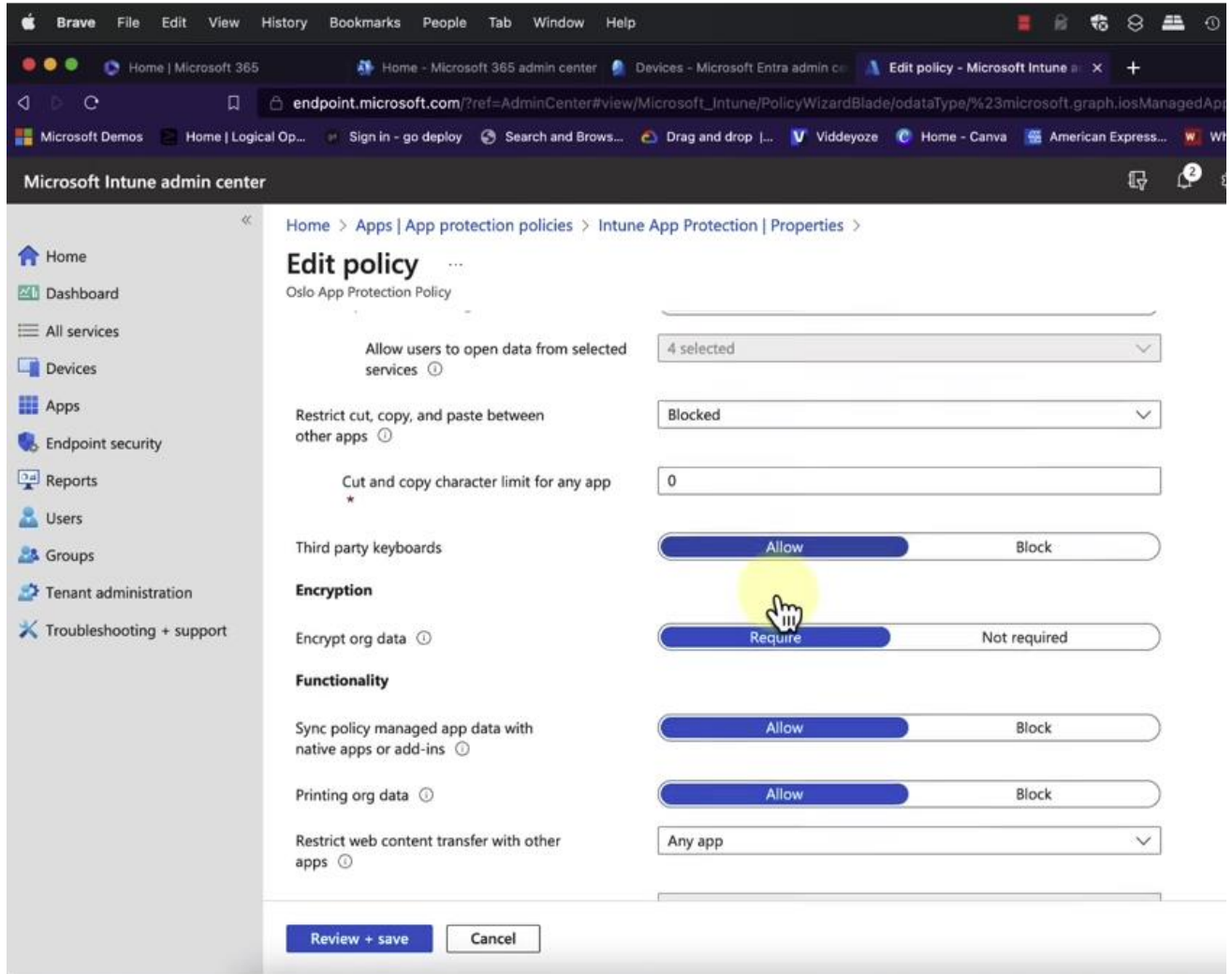
Category	Count
Installed	0
Not Installed	0
Failed	0
Install Pending	0
Not Applicable	0

30. Intune protection policy

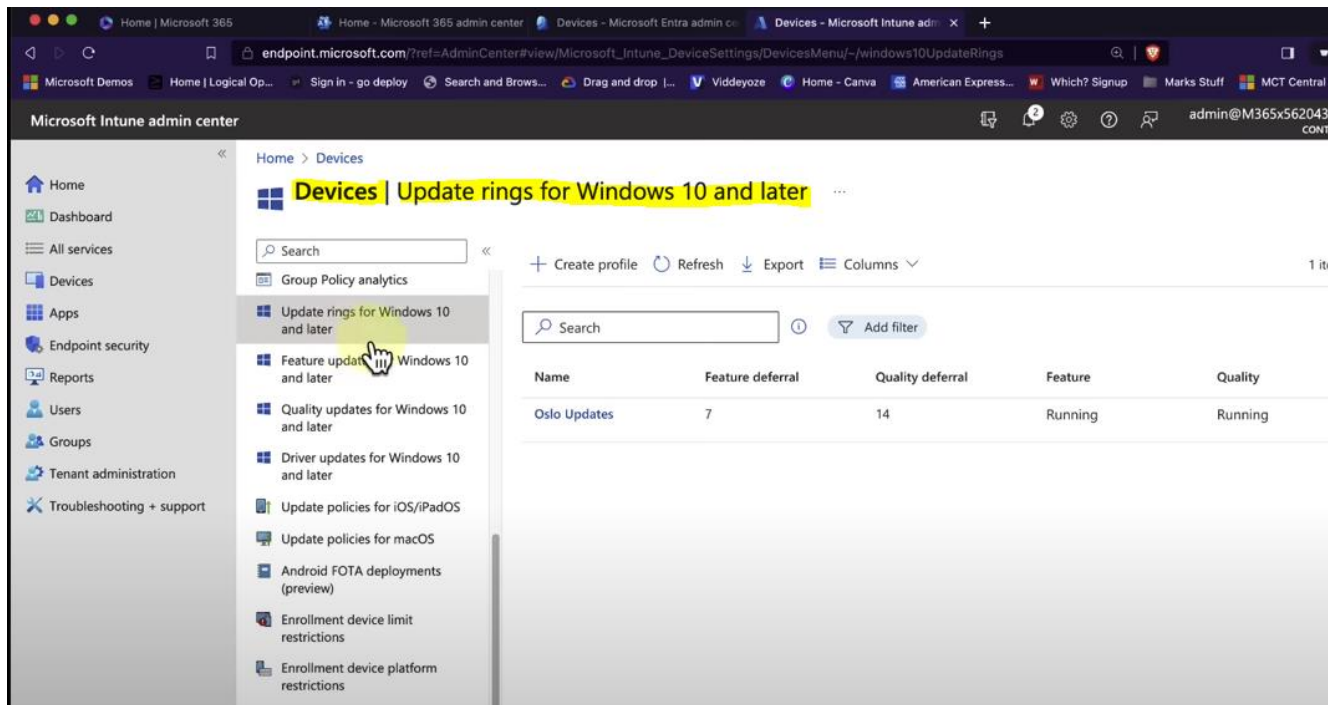
The screenshot shows the Microsoft Intune admin center interface. The left sidebar contains navigation links: Home, Dashboard, All services, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area is titled 'Intune App Protection | Properties' for the 'Oslo App Protection Policy'. The 'Apps' tab is selected, and the 'Apps Edit' button is highlighted with a yellow circle and a hand cursor. The page displays various settings for app protection, including target device types, public apps, and data protection options.

Section	Property	Value
Basics	Name	Oslo App Protection Policy
	Description	--
	Platform	iOS/iPadOS
	Target to apps on all device types	Yes
Device types	Device types	--
	Public apps	Zoom for Intune
	Custom apps	--
Data protection	Prevent backups	Block
	Send org data to other apps	Policy managed apps
	Select apps to exempt	Default: skype;app-settings;calshow;itms;itmss;itms-apps;itms-appss;itms-services;
	Select universal links to exempt	http://facetime.apple.com http://maps.apple.com https://facetime.apple.com https://maps.apple.com

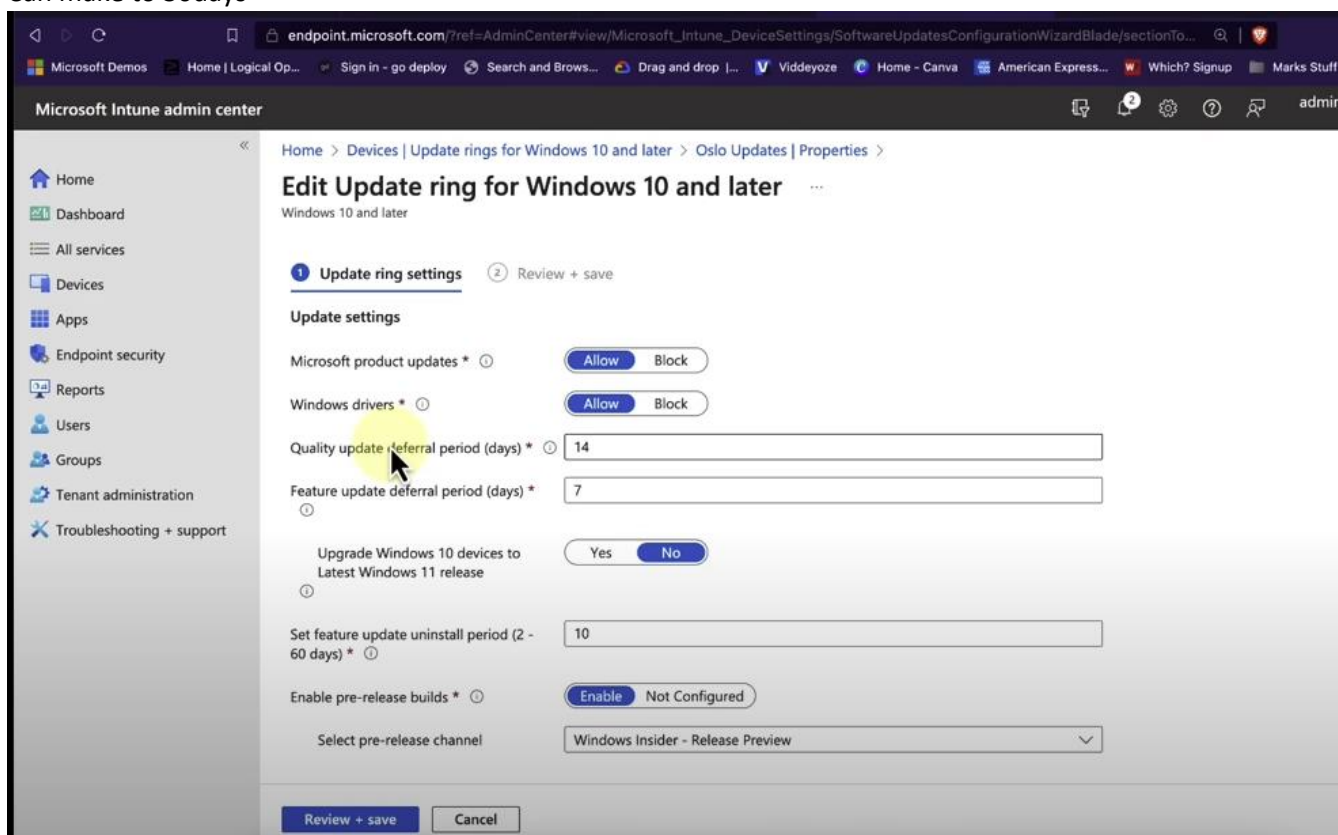
31. Edit Policy apps:



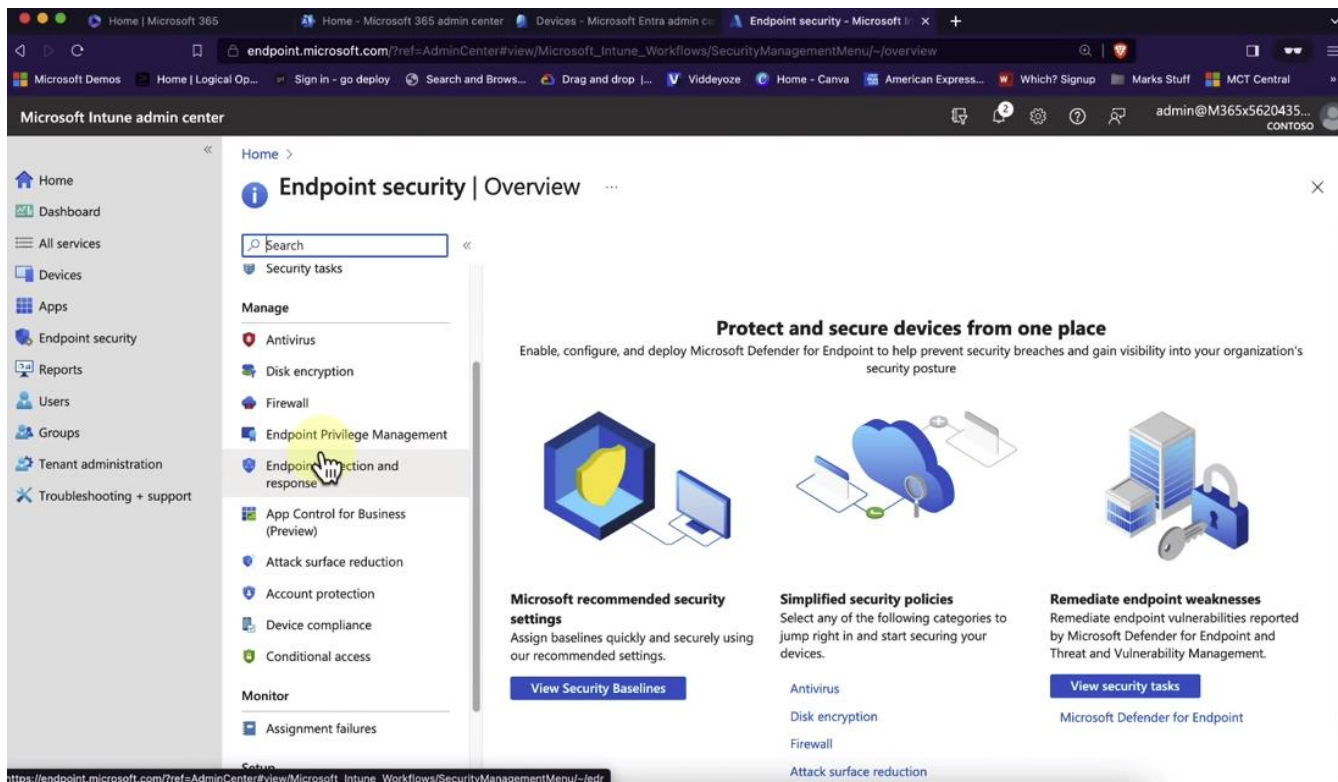
32. Update ring Policy



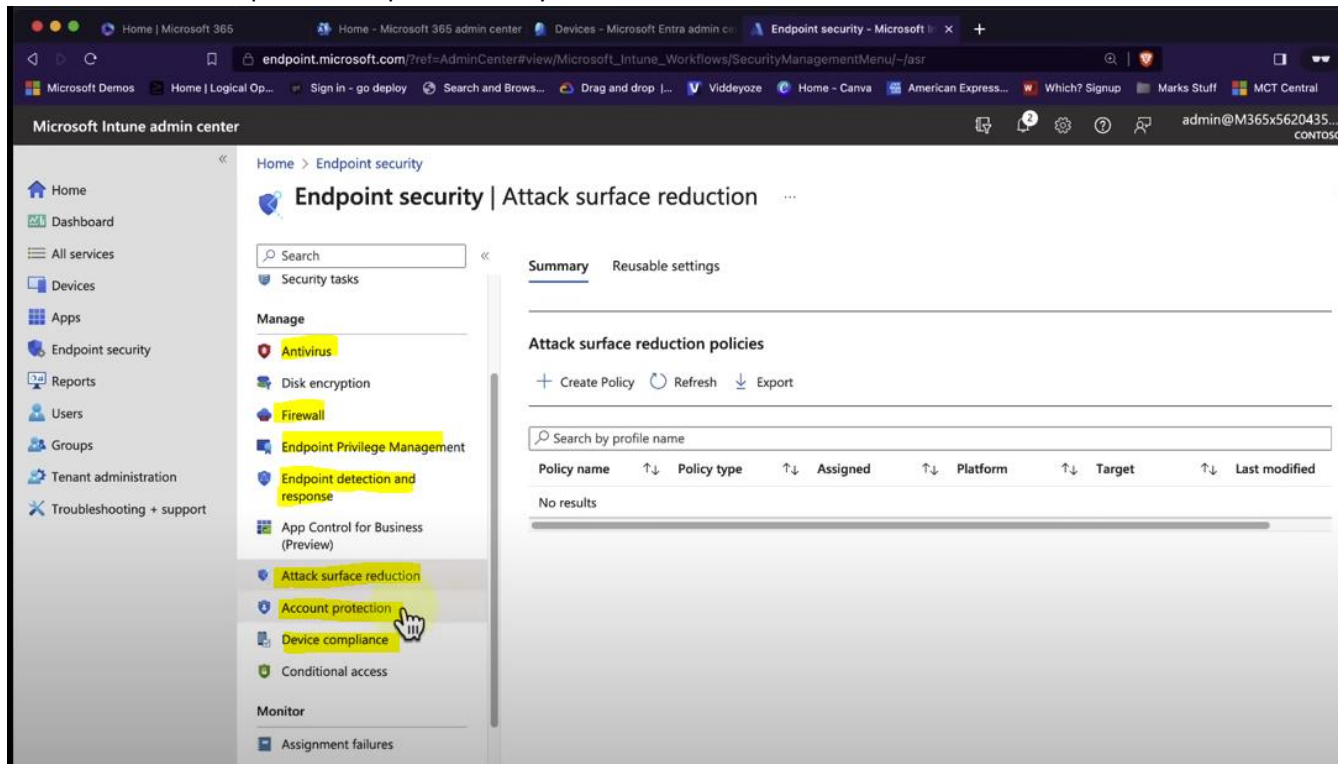
33. Can make to 30days



34. Windows EndPoint security



35. Make Windows compliance Endpoint security



36.

37.

