Microsoft Intune & Entra ID Device Enrollment Lab

Objective:

To successfully enroll and manage both Windows and iOS devices using Microsoft Intune and Entra ID.

Tasks Done:

- Windows & iOS device enrollment
- Apple MDM Push Certificate setup
- Device restriction & compliance configuration
- Group creation with dynamic rules
- Device sync validation

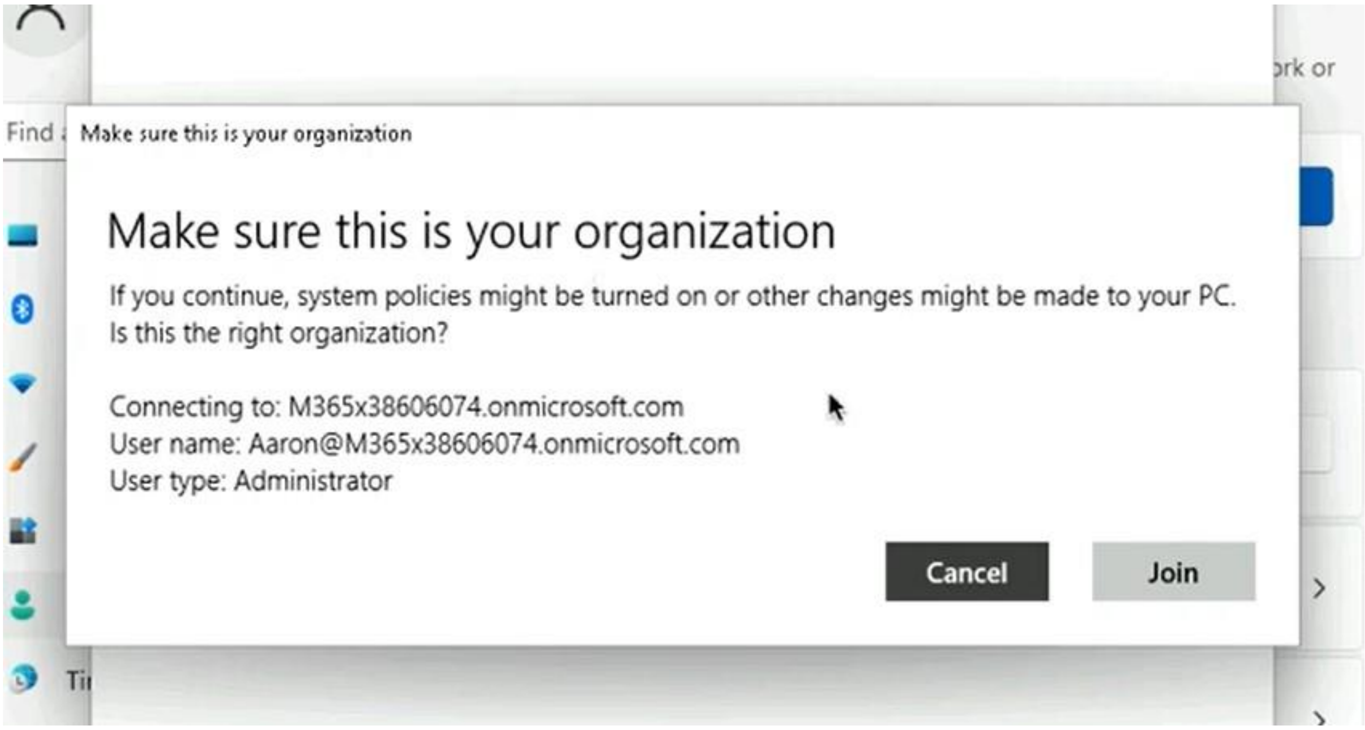
- App deployment via intune

Tools Used:

Microsoft Intune Admin Center, Microsoft Entra Admin Center, Apple Push Certificates Portal, Windows Settings

Outcome:

All devices were successfully enrolled and policies were applied. Compliance and sync statuses were verified.



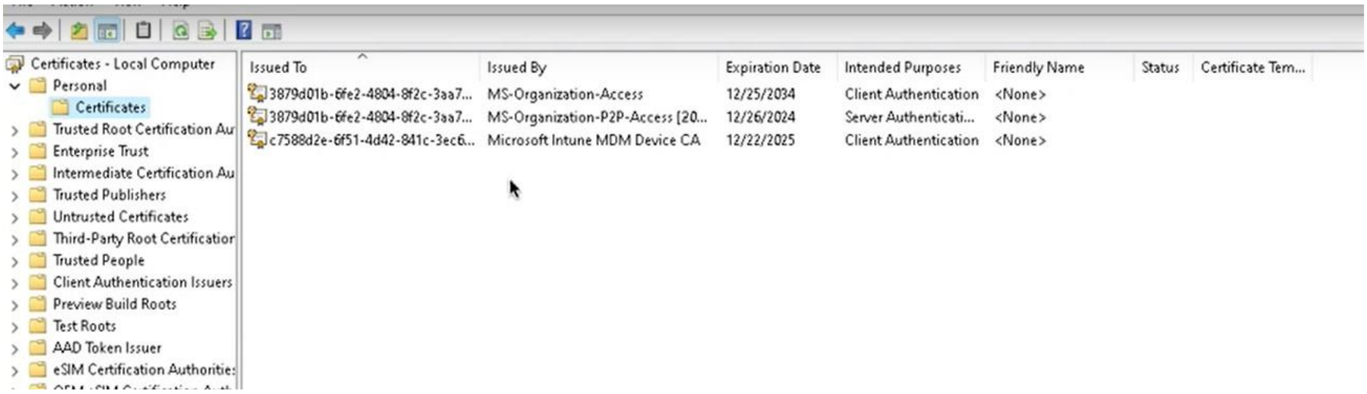
Make sure this is your organization

Make sure this is your organization

If you continue, system policies might be turned on or other changes might be made to your PC. Is this the right organization?

Connecting to: M365x38606074.onmicrosoft.com
User name: Aaron@M365x38606074.onmicrosoft.com
User type: Administrator

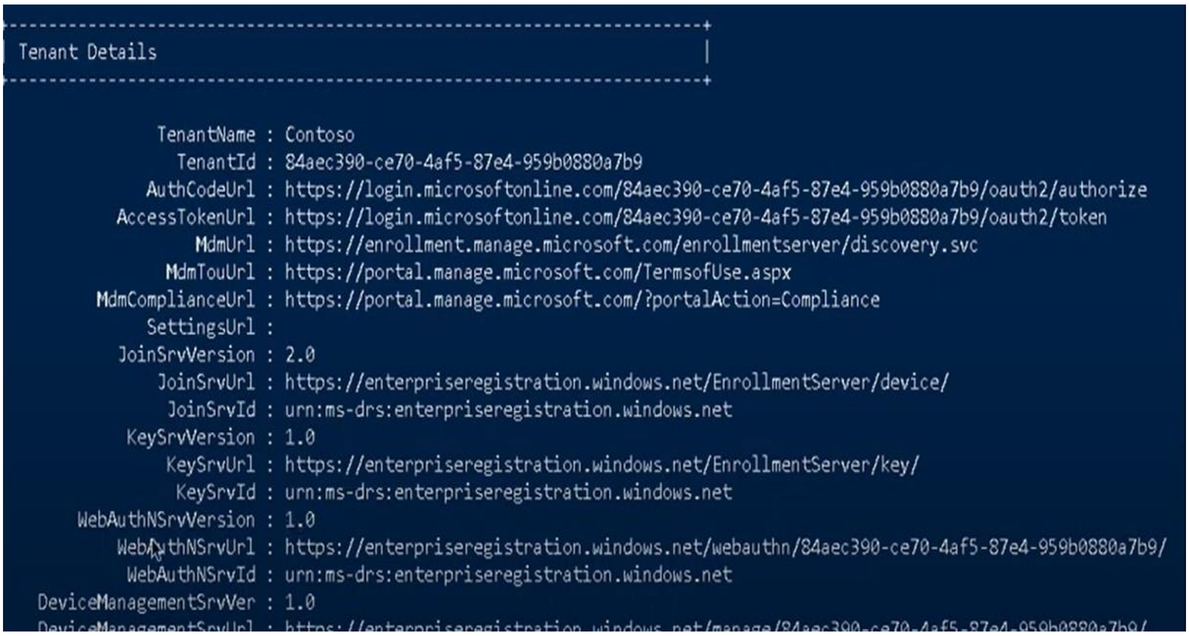
Confirmation prompt when joining the Windows device to Microsoft Entra ID using a user with Administrator role.



- Certificates - Local Computer
  - Personal
    - Certificates
  - Trusted Root Certification Au
  - Enterprise Trust
  - Intermediate Certification Au
  - Trusted Publishers
  - Untrusted Certificates
  - Third-Party Root Certificatior
  - Trusted People
  - Client Authentication Issuers
  - Preview Build Roots
  - Test Roots
  - AAD Token Issuer
  - eSIM Certification Authoritie:

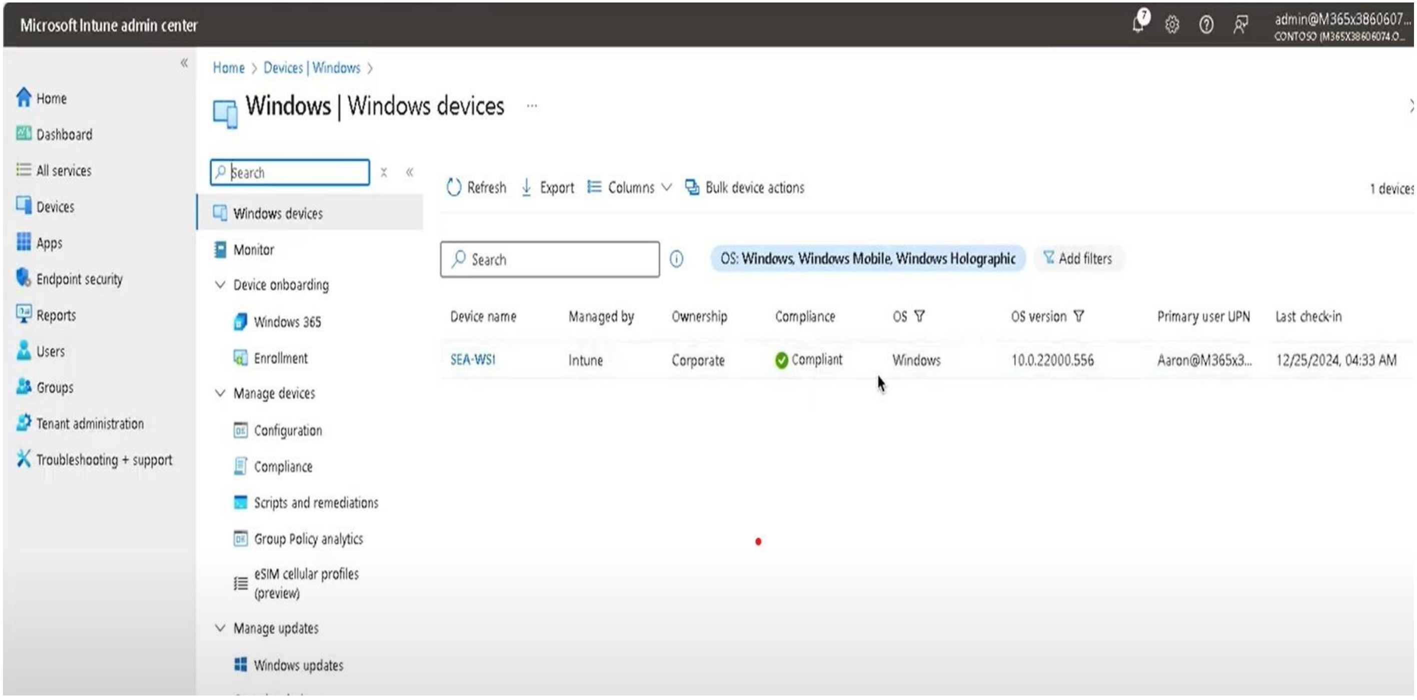
Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Tem...
3879d01b-6fe2-4804-8f2c-3aa7...	MS-Organization-Access	12/25/2034	Client Authentication	<None>		
3879d01b-6fe2-4804-8f2c-3aa7...	MS-Organization-P2P-Access [20...	12/26/2024	Server Authenticati...	<None>		
c7588d2e-6f51-4d42-841c-3ec6...	Microsoft Intune MDM Device CA	12/22/2025	Client Authentication	<None>		

Device certificates showing enrollment to Microsoft Intune MDM and organization authentication certificates.



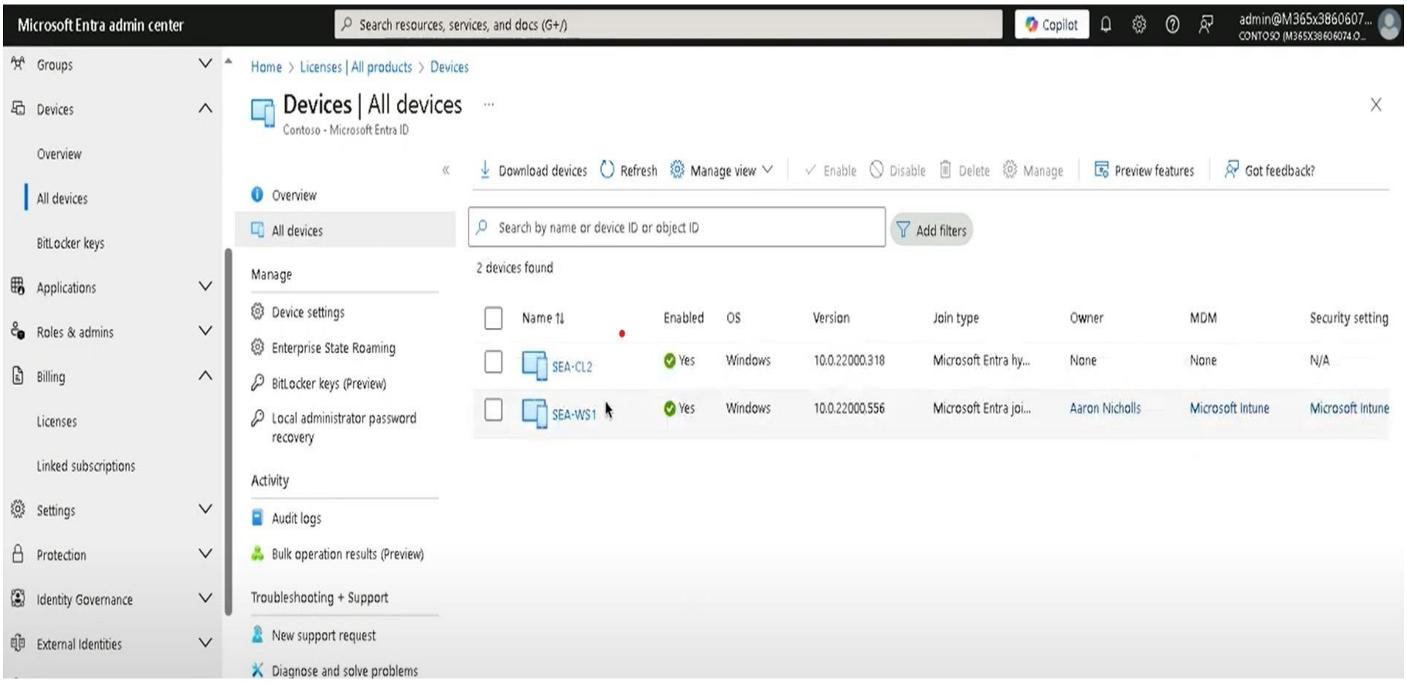
```
+----------------------------------------------------------------------+
| Tenant Details                                                       |
+----------------------------------------------------------------------+

             TenantName : Contoso
               TenantId : 84aec390-ce70-4af5-87e4-959b0880a7b9
            AuthCodeUrl : https://login.microsoftonline.com/84aec390-ce70-4af5-87e4-959b0880a7b9/oauth2/authorize
         AccessTokenUrl : https://login.microsoftonline.com/84aec390-ce70-4af5-87e4-959b0880a7b9/oauth2/token
                 MdmUrl : https://enrollment.manage.microsoft.com/enrollmentserver/discovery.svc
              MdmTouUrl : https://portal.manage.microsoft.com/TermsofUse.aspx
       MdmComplianceUrl : https://portal.manage.microsoft.com/?portalAction=Compliance
            SettingsUrl :
         JoinSrvVersion : 2.0
             JoinSrvUrl : https://enterpriseregistration.windows.net/EnrollmentServer/device/
              JoinSrvId : urn:ms-drs:enterpriseregistration.windows.net
          KeySrvVersion : 1.0
              KeySrvUrl : https://enterpriseregistration.windows.net/EnrollmentServer/key/
               KeySrvId : urn:ms-drs:enterpriseregistration.windows.net
    WebAuthNSrvVersion : 1.0
        WebAuthNSrvUrl : https://enterpriseregistration.windows.net/webauthn/84aec390-ce70-4af5-87e4-959b0880a7b9/
         WebAuthNSrvId : urn:ms-drs:enterpriseregistration.windows.net
DeviceManagementSrvVer : 1.0
DeviceManagementSrvUrl : https://enterpriseregistration.windows.net/manage/84aec390-ce70-4af5-87e4-959b0880a7b9/
```

PowerShell output displaying tenant details and service endpoints related to device registration and MDM.



Device name	Managed by	Ownership	Compliance	OS	OS version	Primary user UPN	Last check-in
SEA-WS1	Intune	Corporate	✓ Compliant	Windows	10.0.22000.556	Aaron@M365x3...	12/25/2024, 04:33 AM

Microsoft Intune admin center showing a compliant Windows device successfully enrolled and managed.



Home > Licenses | All products > Devices

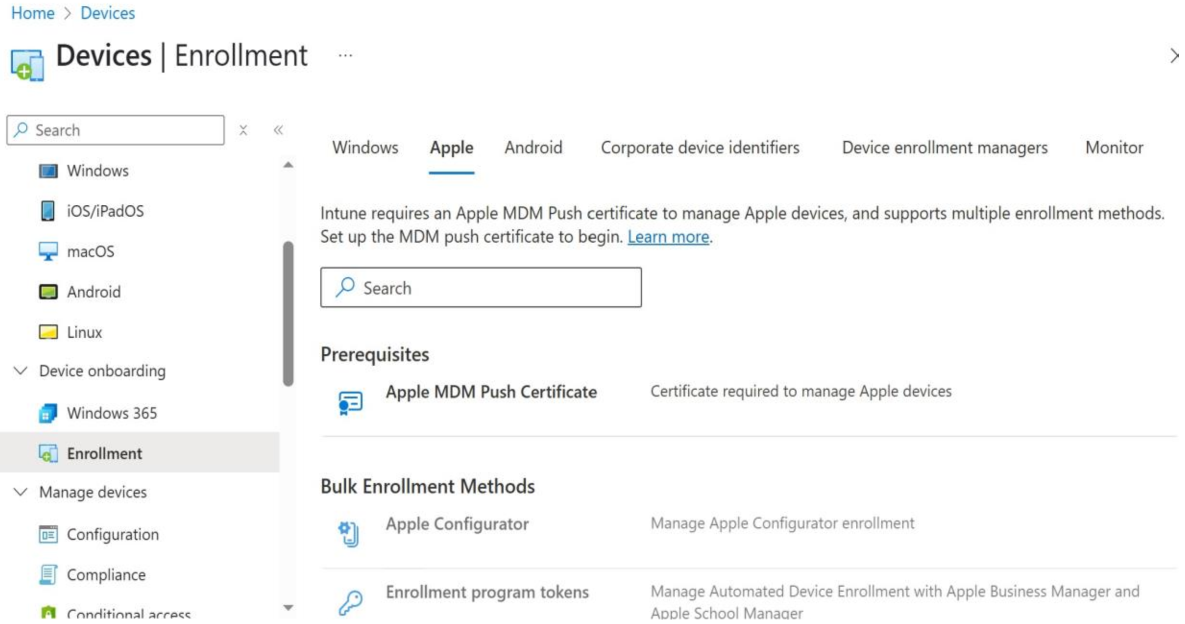
Devices | All devices

Contoso - Microsoft Entra ID

2 devices found

Name	Enabled	OS	Version	Join type	Owner	MDM	Security setting
SEA-CL2	✓ Yes	Windows	10.0.22000.318	Microsoft Entra hy...	None	None	N/A
SEA-WS1	✓ Yes	Windows	10.0.22000.556	Microsoft Entra joi...	Aaron Nicholls	Microsoft Intune	Microsoft Intune

Microsoft Entra admin center listing enrolled devices, including the device SEA-WS1 joined via Entra.



Home > Devices

Devices | Enrollment

Intune requires an Apple MDM Push certificate to manage Apple devices, and supports multiple enrollment methods. Set up the MDM push certificate to begin. Learn more.

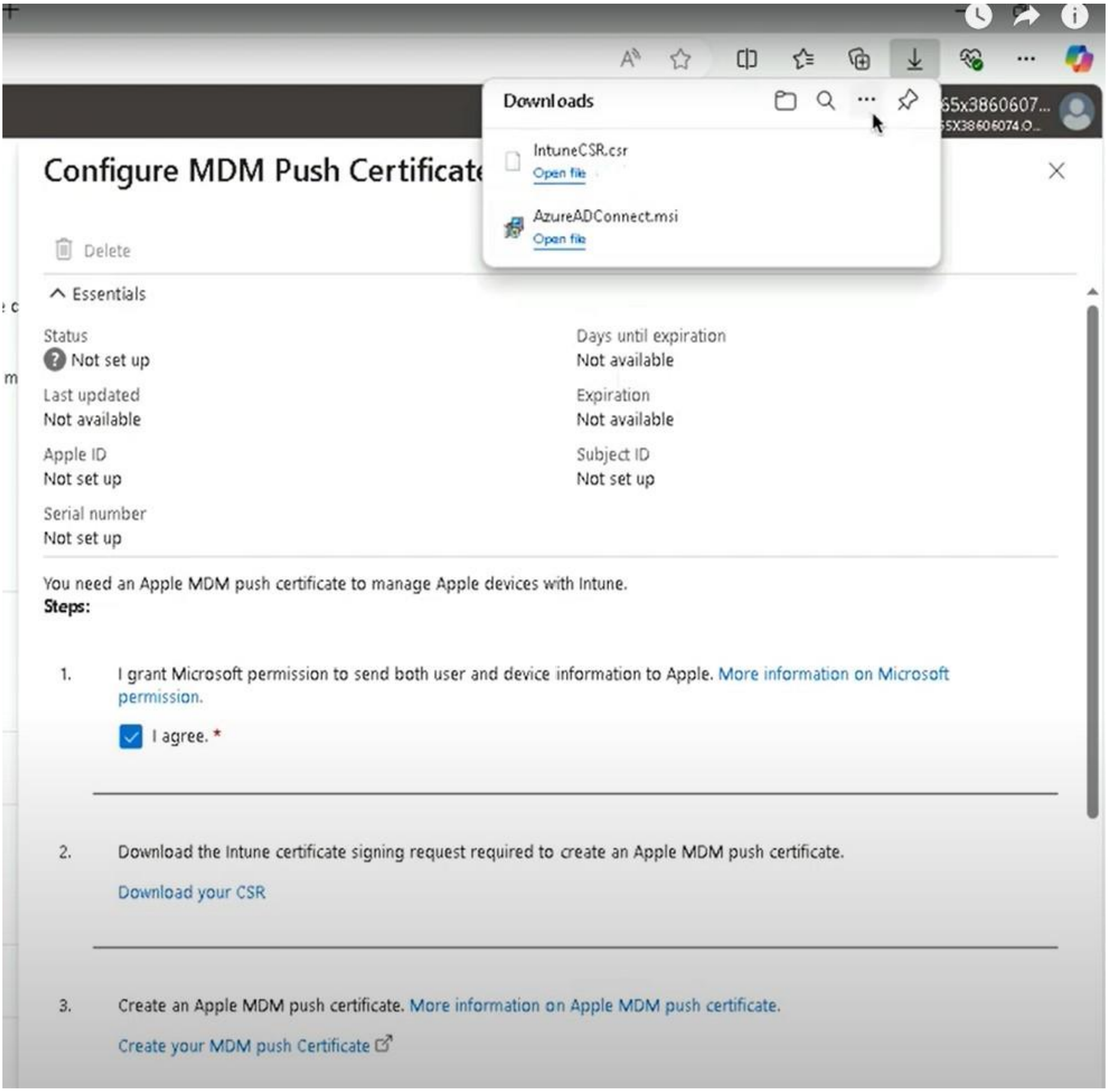
Prerequisites

Apple MDM Push Certificate	Certificate required to manage Apple devices

Bulk Enrollment Methods

Apple Configurator	Manage Apple Configurator enrollment
Enrollment program tokens	Manage Automated Device Enrollment with Apple Business Manager and Apple School Manager

Apple device enrollment options in Intune, showing prerequisites and bulk enrollment methods.



Configure MDM Push Certificate

Status
Not set up

Days until expiration
Not available

Last updated
Not available

Expiration
Not available

Apple ID
Not set up

Subject ID
Not set up

Serial number
Not set up

You need an Apple MDM push certificate to manage Apple devices with Intune.
Steps:

1. I grant Microsoft permission to send both user and device information to Apple. More information on Microsoft permission.

   ☑ I agree. *

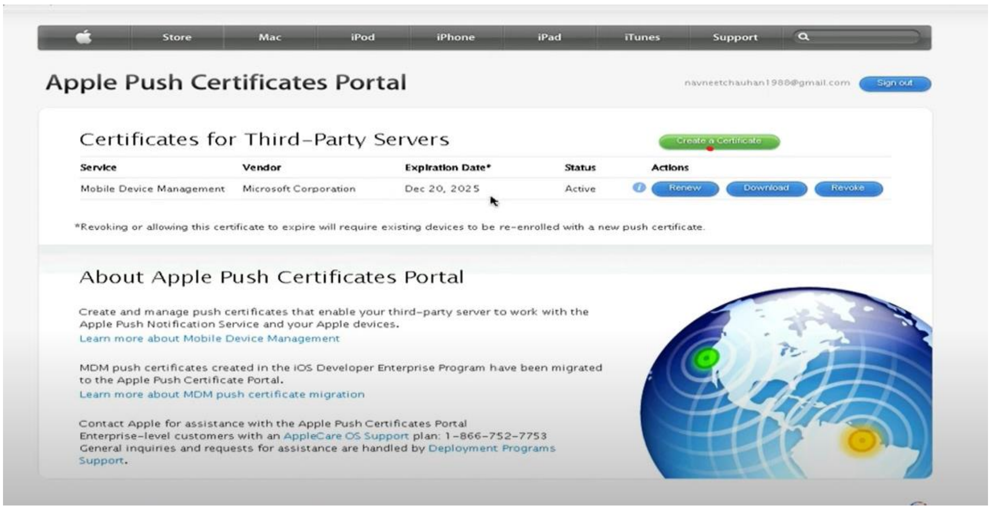
2. Download the Intune certificate signing request required to create an Apple MDM push certificate.

   Download your CSR

3. Create an Apple MDM push certificate. More information on Apple MDM push certificate.

   Create your MDM push Certificate

Downloading the certificate signing request (CSR) needed to create the Apple MDM Push Certificate.



Apple Push Certificates Portal

navneetchauhan1988@gmail.com

Certificates for Third-Party Servers

Service	Vendor	Expiration Date*	Status	Actions
Mobile Device Management	Microsoft Corporation	Dec 20, 2025	Active	Renew Download Revoke

*Revoking or allowing this certificate to expire will require existing devices to be re-enrolled with a new push certificate.

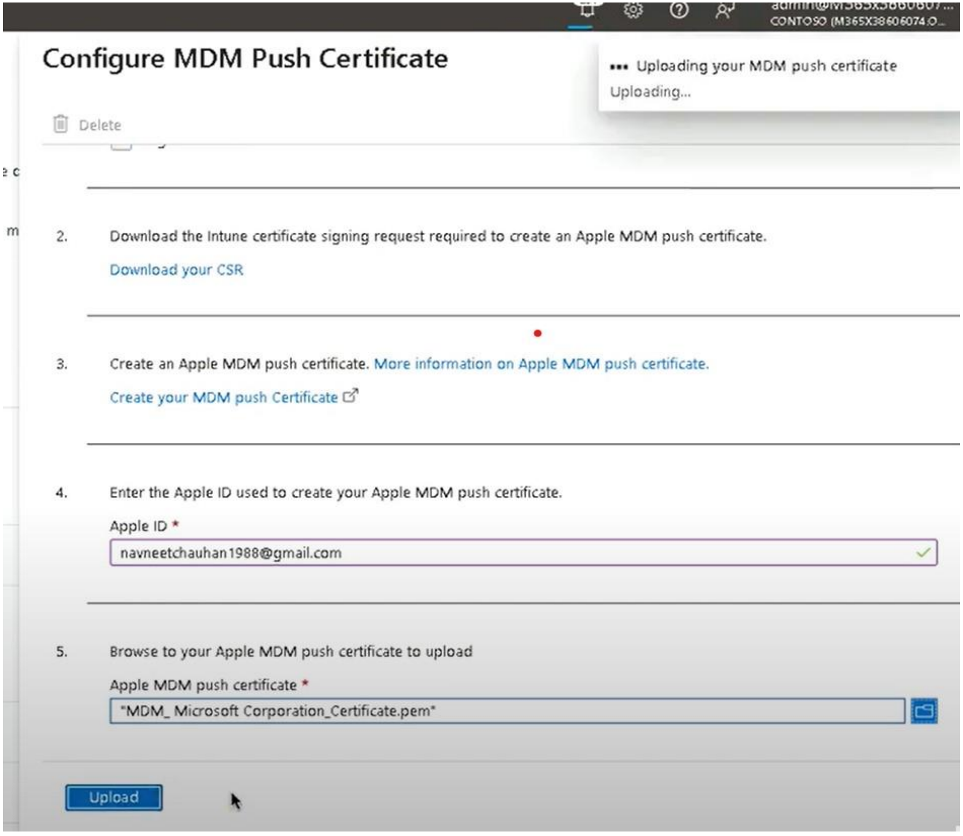
About Apple Push Certificates Portal

Create and manage push certificates that enable your third-party server to work with the Apple Push Notification Service and your Apple devices.
Learn more about Mobile Device Management

MDM push certificates created in the iOS Developer Enterprise Program have been migrated to the Apple Push Certificate Portal.
Learn more about MDM push certificate migration

Contact Apple for assistance with the Apple Push Certificates Portal
Enterprise-level customers with an AppleCare OS Support plan: 1-866-752-7753
General inquiries and requests for assistance are handled by Deployment Programs Support.

Apple Push Certificates Portal showing an active MDM certificate issued to Microsoft Corporation.



admin@M365x3860607...
CONTOSO (M365X38606074.O...

Configure MDM Push Certificate

••• Uploading your MDM push certificate
Uploading...

2. Download the Intune certificate signing request required to create an Apple MDM push certificate.

   Download your CSR

3. Create an Apple MDM push certificate. More information on Apple MDM push certificate.

   Create your MDM push Certificate

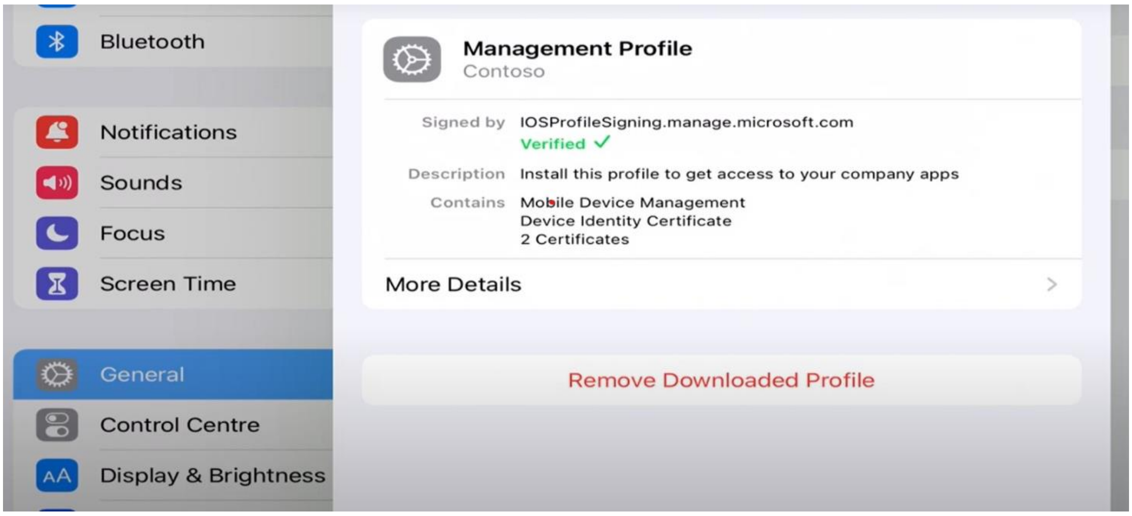
4. Enter the Apple ID used to create your Apple MDM push certificate.

   Apple ID *
   navneetchauhan1988@gmail.com

5. Browse to your Apple MDM push certificate to upload

   Apple MDM push certificate *
   "MDM_ Microsoft Corporation_Certificate.pem"

Uploading the Apple MDM Push Certificate in Intune after generation from the Apple portal.



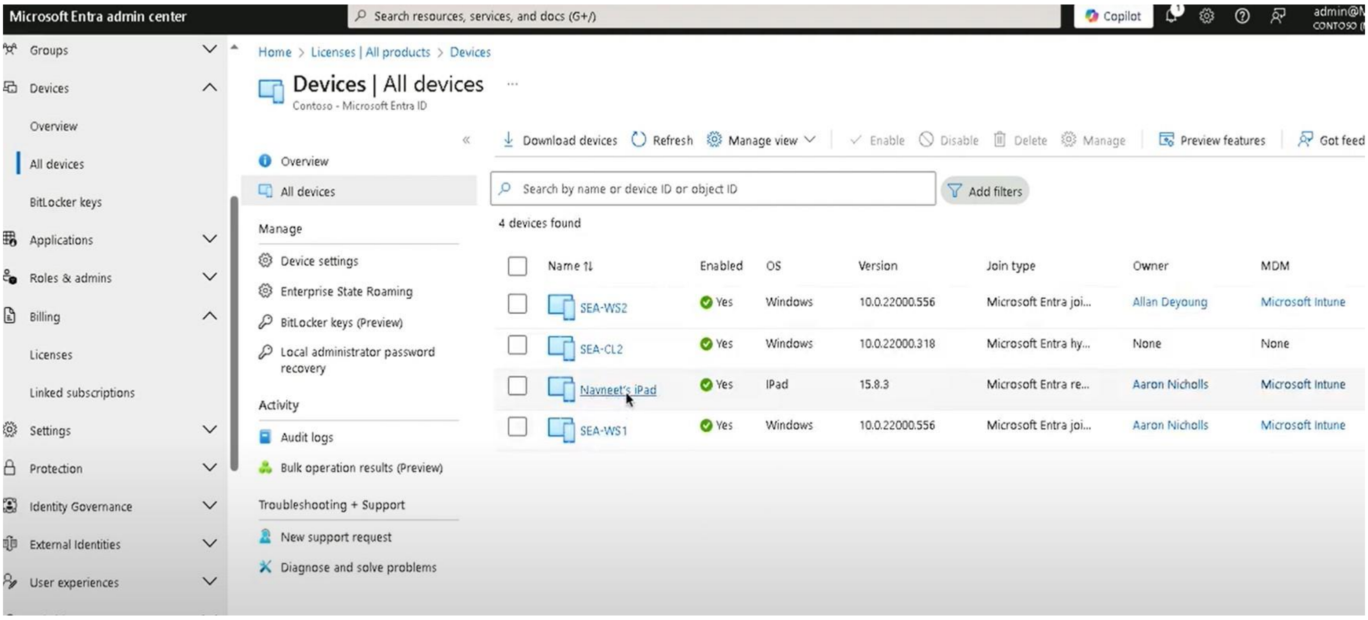
Management Profile
Contoso

Signed by: IOSProfileSigning.manage.microsoft.com
Verified ✓

Description: Install this profile to get access to your company apps

Contains: Mobile Device Management
Device Identity Certificate
2 Certificates

iOS management profile installed on the iPad device confirming MDM enrollment and certificate presence.

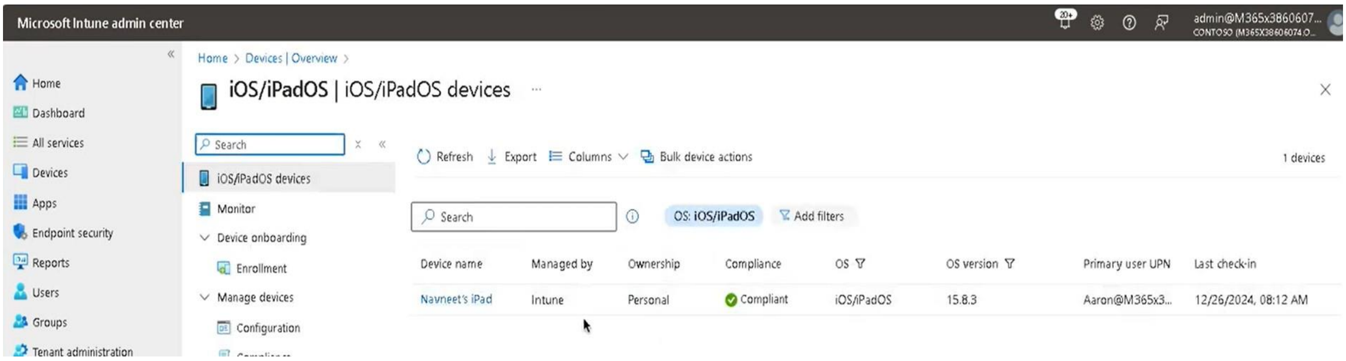


Devices | All devices
Contoso - Microsoft Entra ID

4 devices found

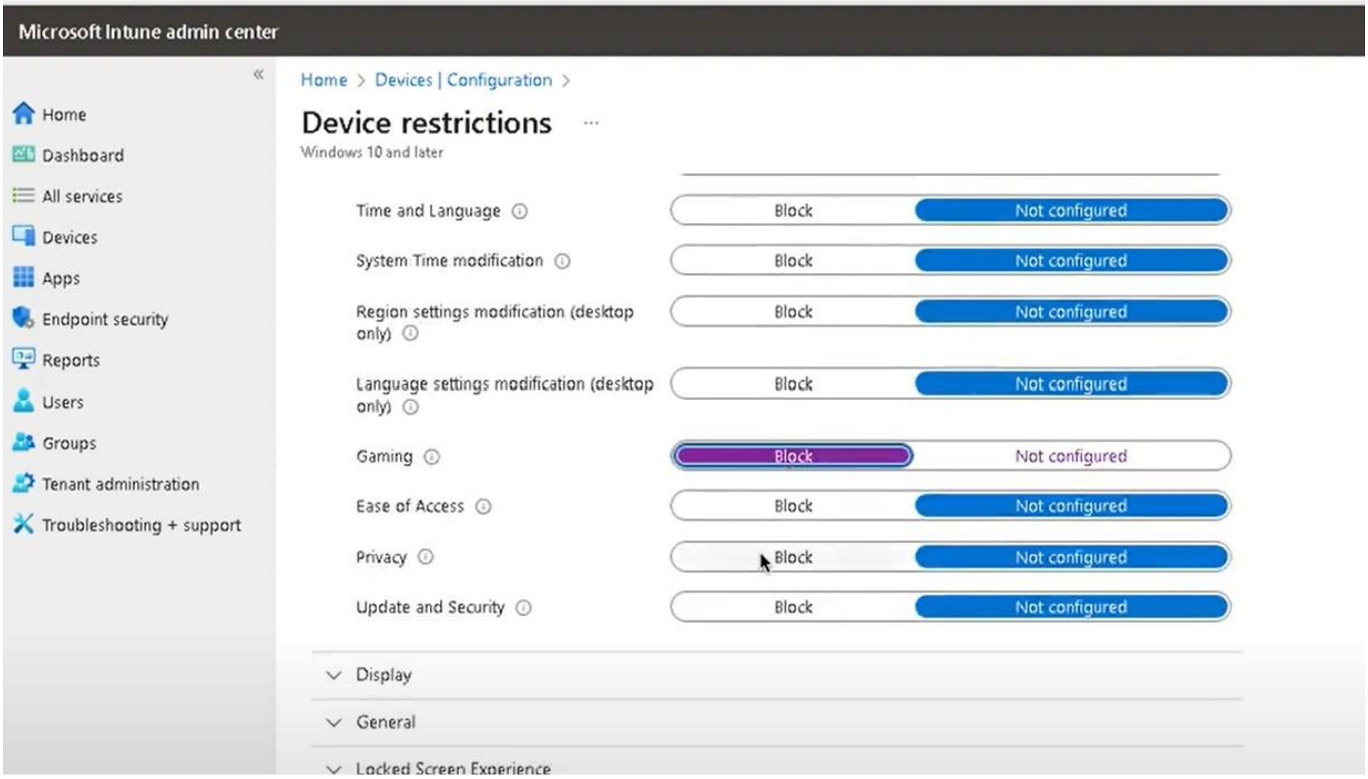
Name	Enabled	OS	Version	Join type	Owner	MDM
SEA-WS2	✓ Yes	Windows	10.0.22000.556	Microsoft Entra joi...	Allan Deyoung	Microsoft Intune
SEA-CL2	✓ Yes	Windows	10.0.22000.318	Microsoft Entra hy...	None	None
Navneet's iPad	✓ Yes	IPad	15.8.3	Microsoft Entra re...	Aaron Nicholls	Microsoft Intune
SEA-WS1	✓ Yes	Windows	10.0.22000.556	Microsoft Entra joi...	Aaron Nicholls	Microsoft Intune

Microsoft Entra admin center showing successful iOS device registration (Navneet's iPad).



Device name	Managed by	Ownership	Compliance	OS	OS version	Primary user UPN	Last check-in
Navneet's iPad	Intune	Personal	✓ Compliant	iOS/iPadOS	15.8.3	Aaron@M365x3...	12/26/2024, 08:12 AM

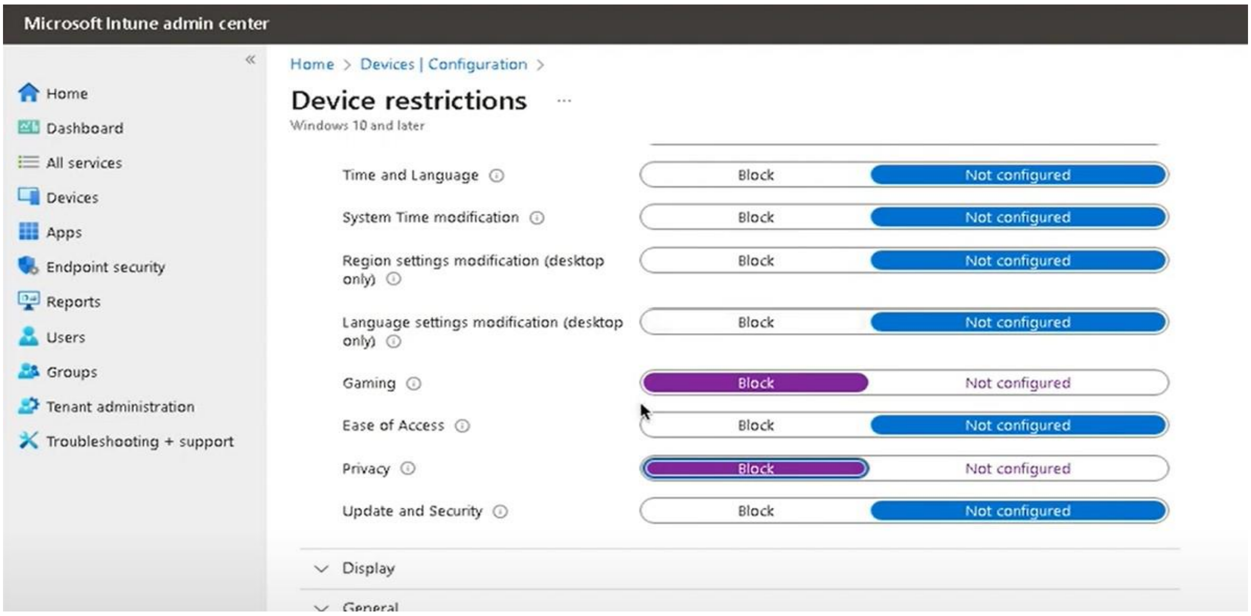
Intune admin center verifying that the enrolled iPad is marked as compliant.



Setting	Value
Time and Language	Not configured
System Time modification	Not configured
Region settings modification (desktop only)	Not configured
Language settings modification (desktop only)	Not configured
Gaming	Block
Ease of Access	Not configured
Privacy	Not configured
Update and Security	Not configured

Creating a configuration profile in Intune to apply policies to Windows devices.

Applying device restrictions in Intune to block system and user settings modifications.

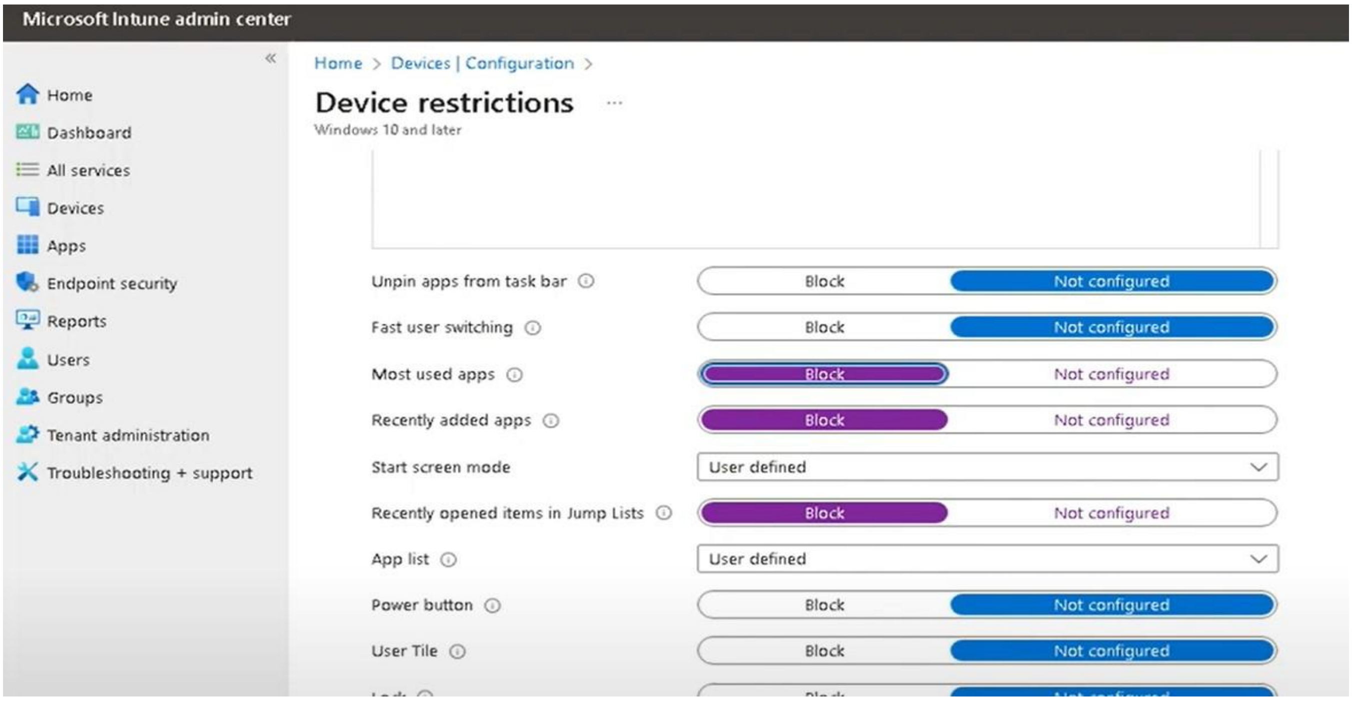


Device restrictions

Windows 10 and later

- Time and Language: Not configured
- System Time modification: Not configured
- Region settings modification (desktop only): Not configured
- Language settings modification (desktop only): Not configured
- Gaming: Block
- Ease of Access: Not configured
- Privacy: Block
- Update and Security: Not configured

Further device restriction settings applied to user environment (apps, start screen, etc.).

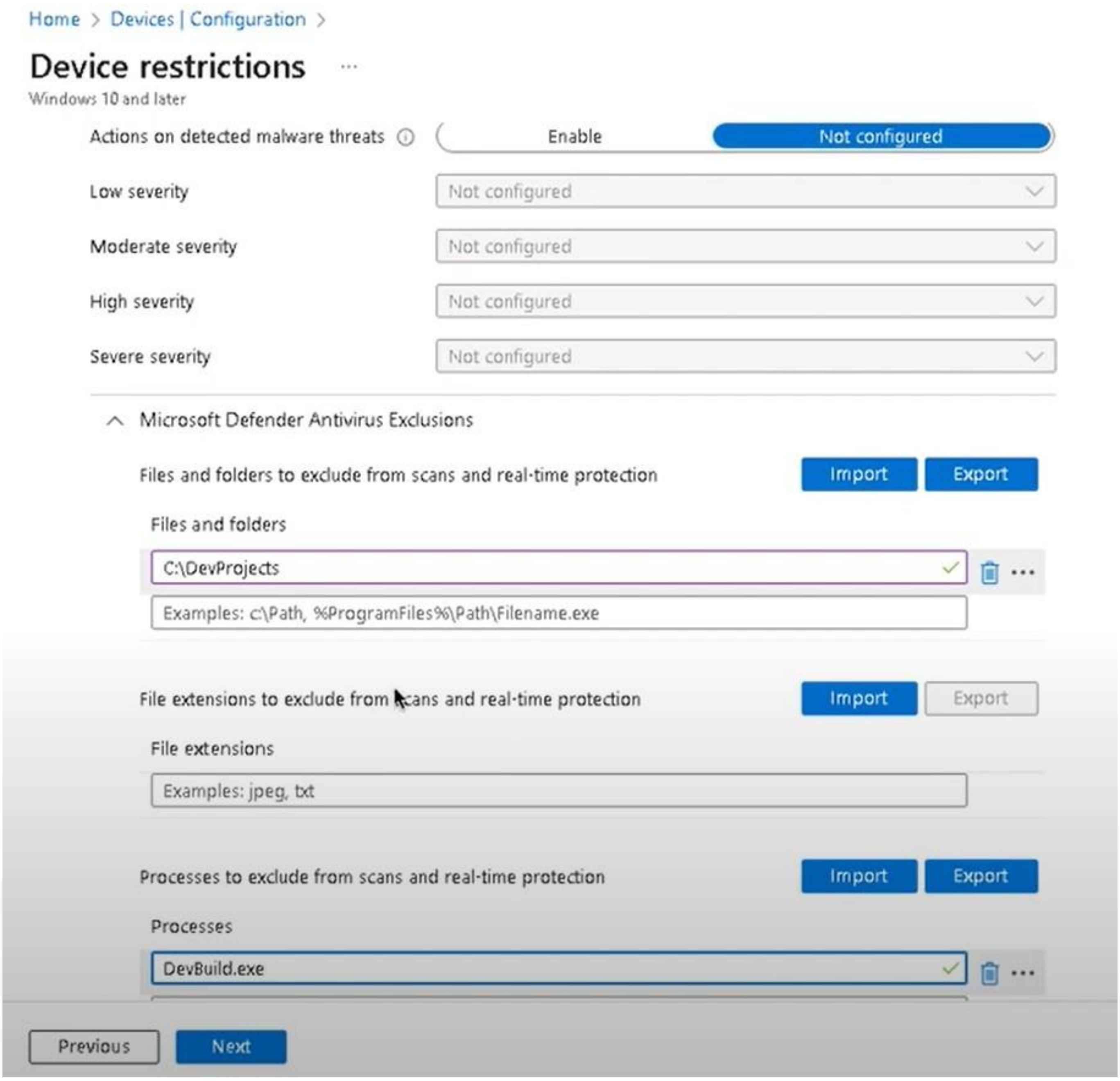


Device restrictions

Windows 10 and later

- Unpin apps from task bar: Not configured
- Fast user switching: Not configured
- Most used apps: Block
- Recently added apps: Block
- Start screen mode: User defined
- Recently opened items in Jump Lists: Block
- App list: User defined
- Power button: Not configured
- User Tile: Not configured

Excluding specific files and folders from Microsoft Defender Antivirus scans.



Home > Devices | Configuration >

Device restrictions

Windows 10 and later

Actions on detected malware threats: Enable / Not configured (selected: Not configured)

Low severity: Not configured

Moderate severity: Not configured

High severity: Not configured

Severe severity: Not configured

Microsoft Defender Antivirus Exclusions

Files and folders to exclude from scans and real-time protection

Files and folders

C:\DevProjects

Examples: c:\Path, %ProgramFiles%\Path\Filename.exe

File extensions to exclude from scans and real-time protection

File extensions

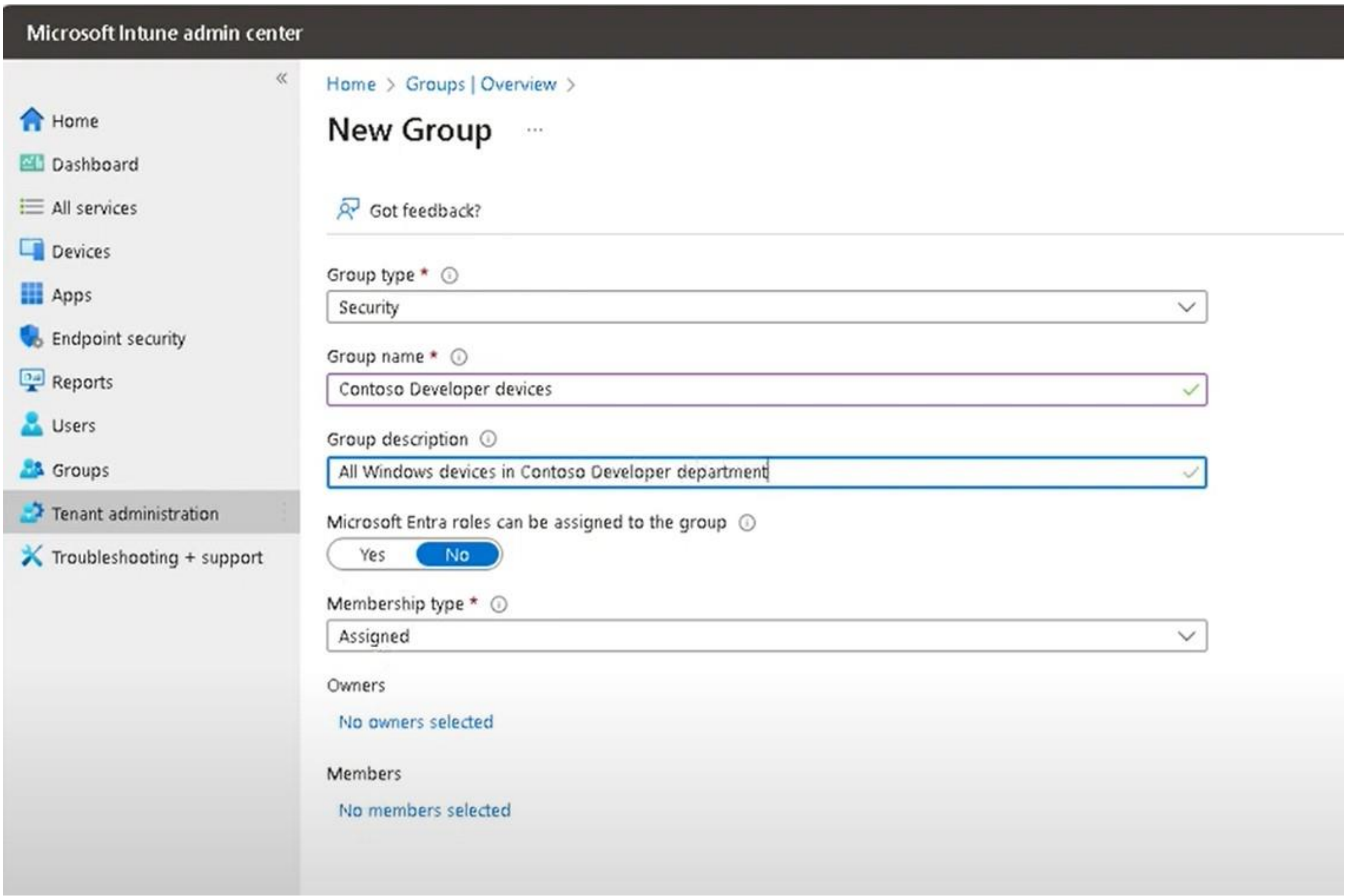
Examples: jpeg, txt

Processes to exclude from scans and real-time protection

Processes

DevBuild.exe

Creating a new security group for developer Windows devices.



New Group

Got feedback?

Group type *: Security

Group name *: Contoso Developer devices

Group description: All Windows devices in Contoso Developer department

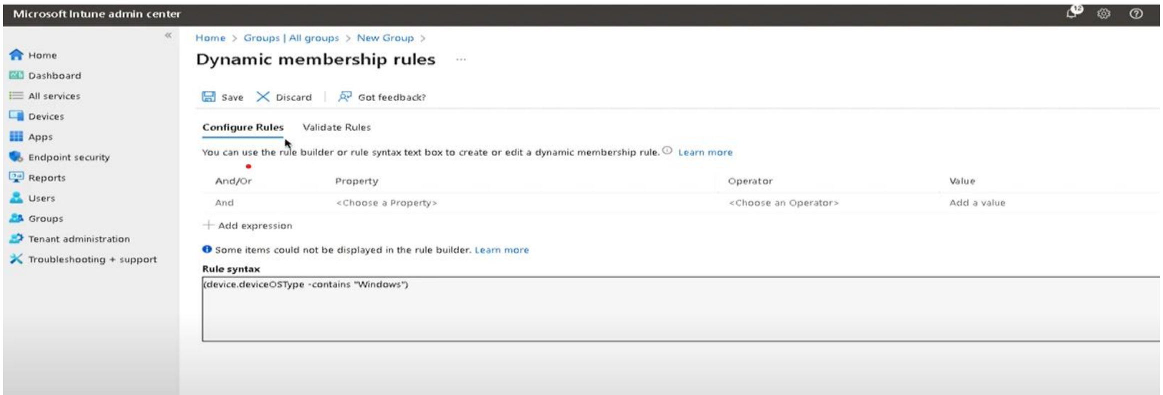
Microsoft Entra roles can be assigned to the group: Yes [✓ No]

Membership type *: Assigned

Owners: No owners selected

Members: No members selected

Applying dynamic membership rules to group based on OS type (Windows).



Dynamic membership rules

You can use the rule builder or rule syntax text box to create or edit a dynamic membership rule. Learn more

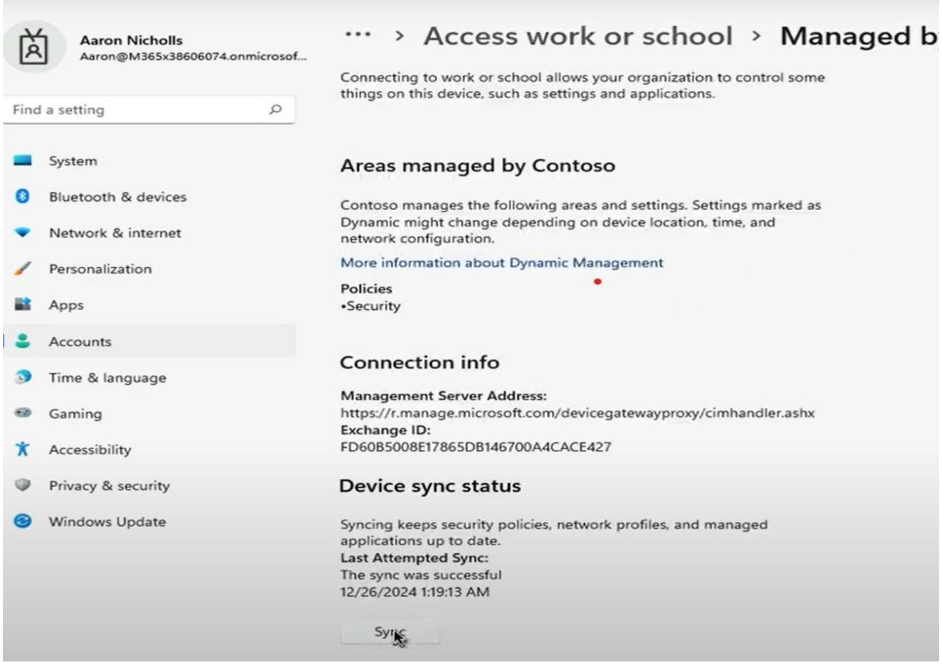
And/Or	Property	Operator	Value
And	<Choose a Property>	<Choose an Operator>	Add a value

Some items could not be displayed in the rule builder. Learn more

Rule syntax

```
(device.deviceOSType -contains "Windows")
```

Verifying device sync and connection info from the enrolled Windows device.



Connecting to work or school allows your organization to control some things on this device, such as settings and applications.

Areas managed by Contoso

Contoso manages the following areas and settings. Settings marked as Dynamic might change depending on device location, time, and network configuration.

More information about Dynamic Management

Policies
•Security

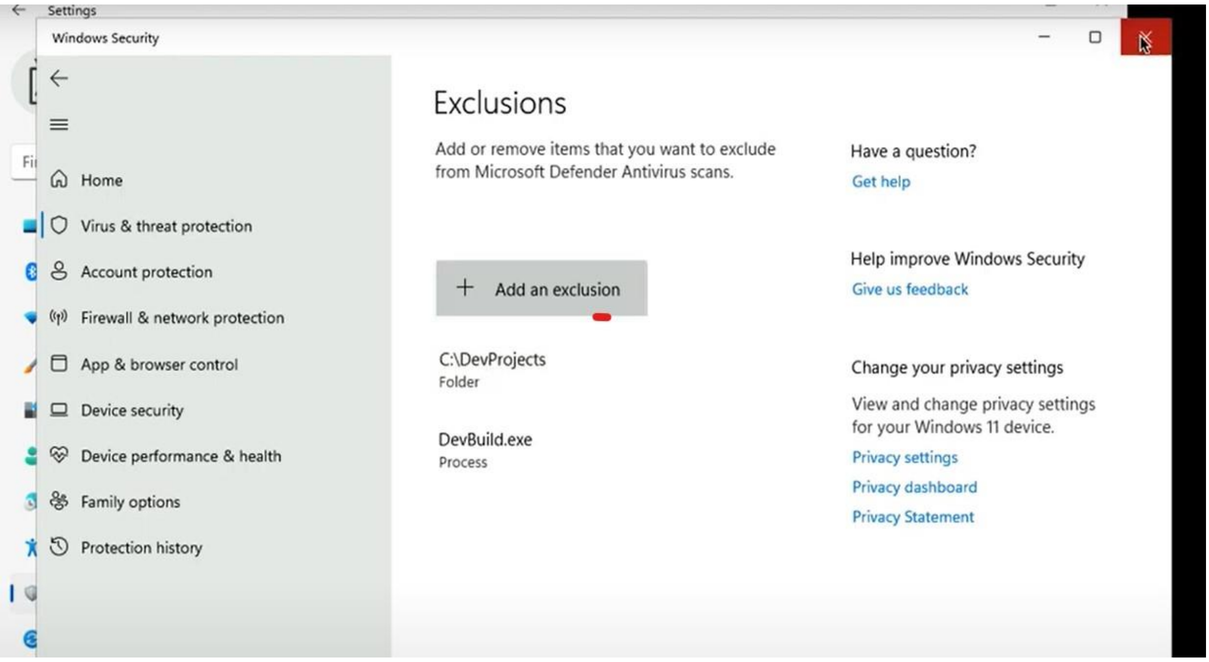
Connection info

Management Server Address:
https://r.manage.microsoft.com/devicegatewayproxy/cimhandler.ashx
Exchange ID:
FD60B5008E17865DB146700A4CACE427

Device sync status

Syncing keeps security policies, network profiles, and managed applications up to date.
Last Attempted Sync:
The sync was successful
12/26/2024 1:19:13 AM

Manually adding antivirus exclusions from Windows Security settings.



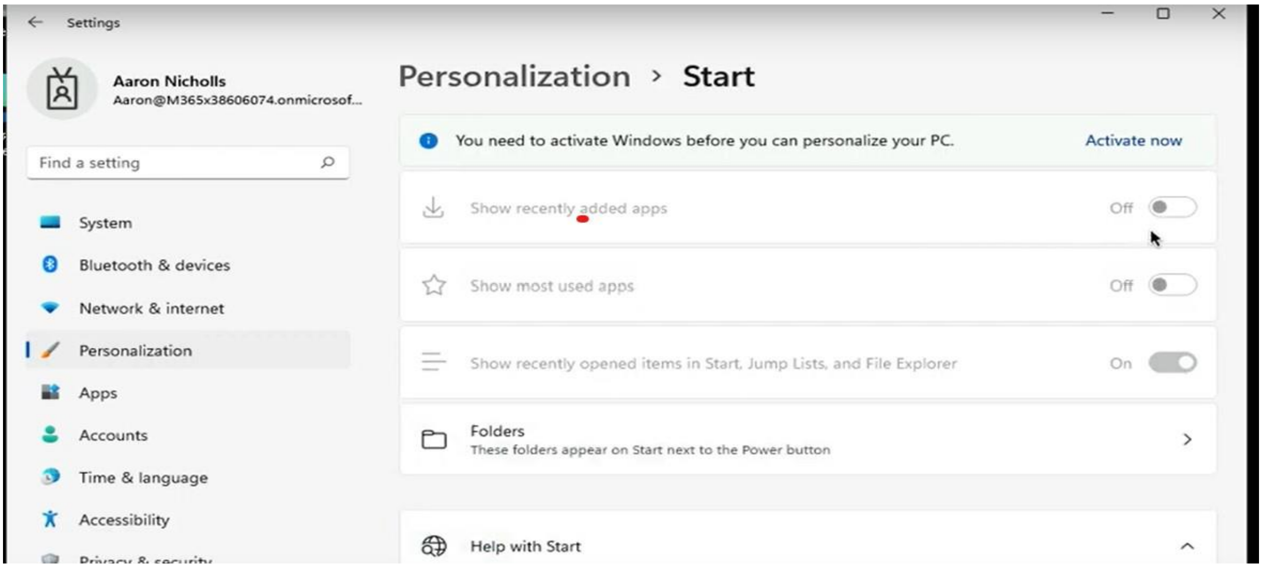
Exclusions

Add or remove items that you want to exclude from Microsoft Defender Antivirus scans.

C:\DevProjects
Folder

DevBuild.exe
Process

Personalization settings showing app usage options turned off.



Personalization > Start

You need to activate Windows before you can personalize your PC.

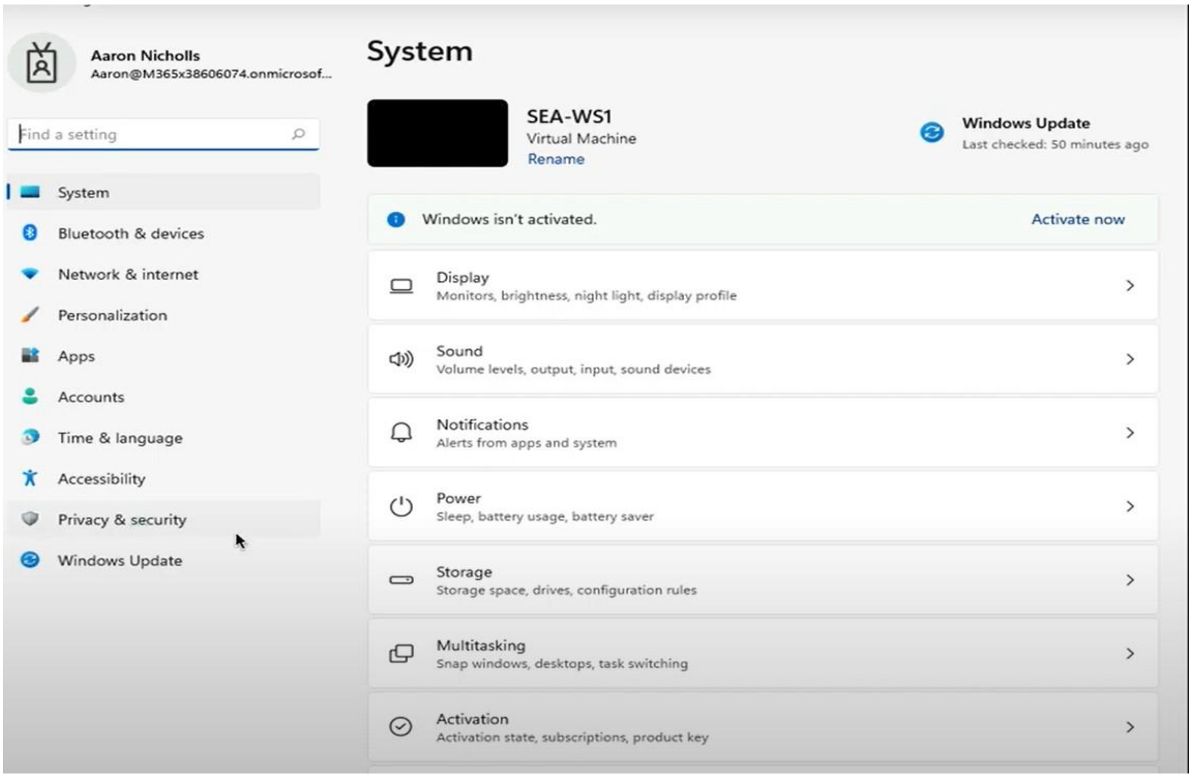
Show recently added apps — Off

Show most used apps — Off

Show recently opened items in Start, Jump Lists, and File Explorer — On

Folders
These folders appear on Start next to the Power button

Windows system settings of the enrolled virtual machine.



Aaron Nicholls
Aaron@M365x38606074.onmicrosof...

Find a setting

- System
- Bluetooth & devices
- Network & internet
- Personalization
- Apps
- Accounts
- Time & language
- Accessibility
- Privacy & security
- Windows Update

System

[redacted]

SEA-WS1
Virtual Machine
Rename

Windows Update
Last checked: 50 minutes ago

Windows isn't activated. Activate now

Display
Monitors, brightness, night light, display profile

Sound
Volume levels, output, input, sound devices

Notifications
Alerts from apps and system

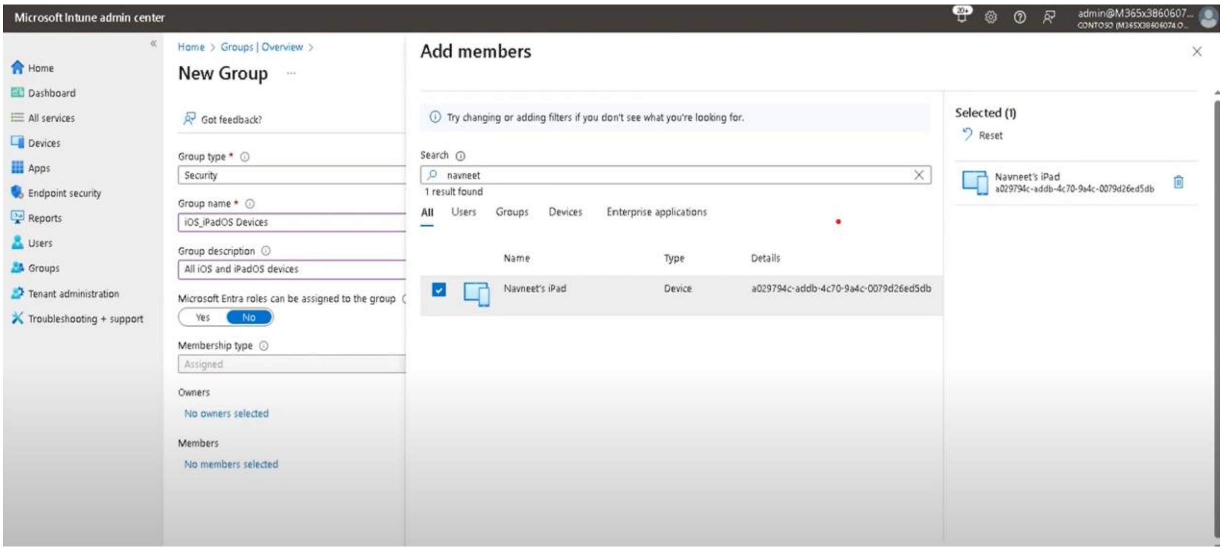
Power
Sleep, battery usage, battery saver

Storage
Storage space, drives, configuration rules

Multitasking
Snap windows, desktops, task switching

Activation
Activation state, subscriptions, product key

Adding Navneet's iPad to a new Intune group for iOS/iPadOS devices.



Microsoft Intune admin center

admin@M365x3860607...
CONTOSO (M365X38606074.O...

- Home
- Dashboard
- All services
- Devices
- Apps
- Endpoint security
- Reports
- Users
- Groups
- Tenant administration
- Troubleshooting + support

Home > Groups | Overview >

New Group ···

Got feedback?

Group type * : Security

Group name * : iOS_iPadOS Devices

Group description : All iOS and iPadOS devices

Microsoft Entra roles can be assigned to the group: Yes [✓ No]

Membership type : Assigned

Owners
No owners selected

Members
No members selected

Add members

Try changing or adding filters if you don't see what you're looking for.

Search : navneet
1 result found

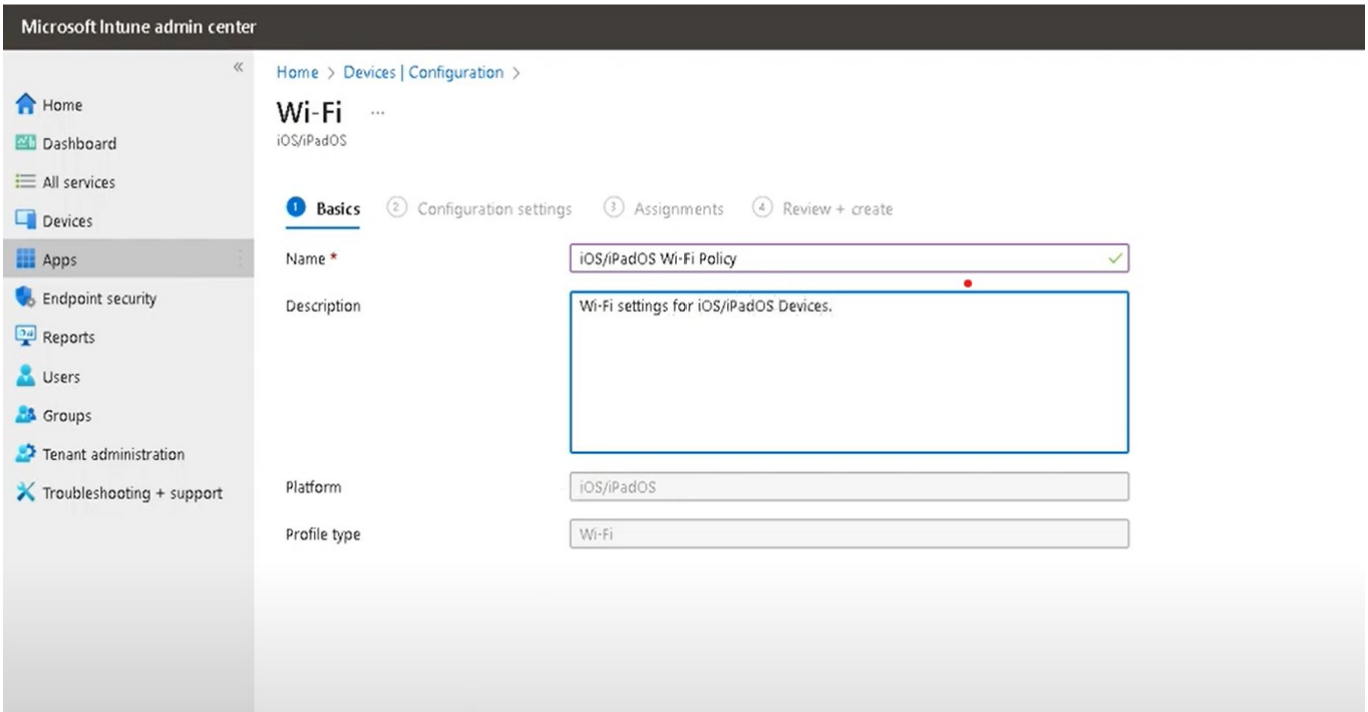
All | Users | Groups | Devices | Enterprise applications

	Name	Type	Details
☑	Navneet's iPad	Device	a029794c-addb-4c70-9a4c-0079d26ed5db

Selected (1)
Reset

Navneet's iPad
a029794c-addb-4c70-9a4c-0079d26ed5db

Creating a Wi-Fi configuration profile for iOS/iPadOS devices.



Wi-Fi
iOS/iPadOS

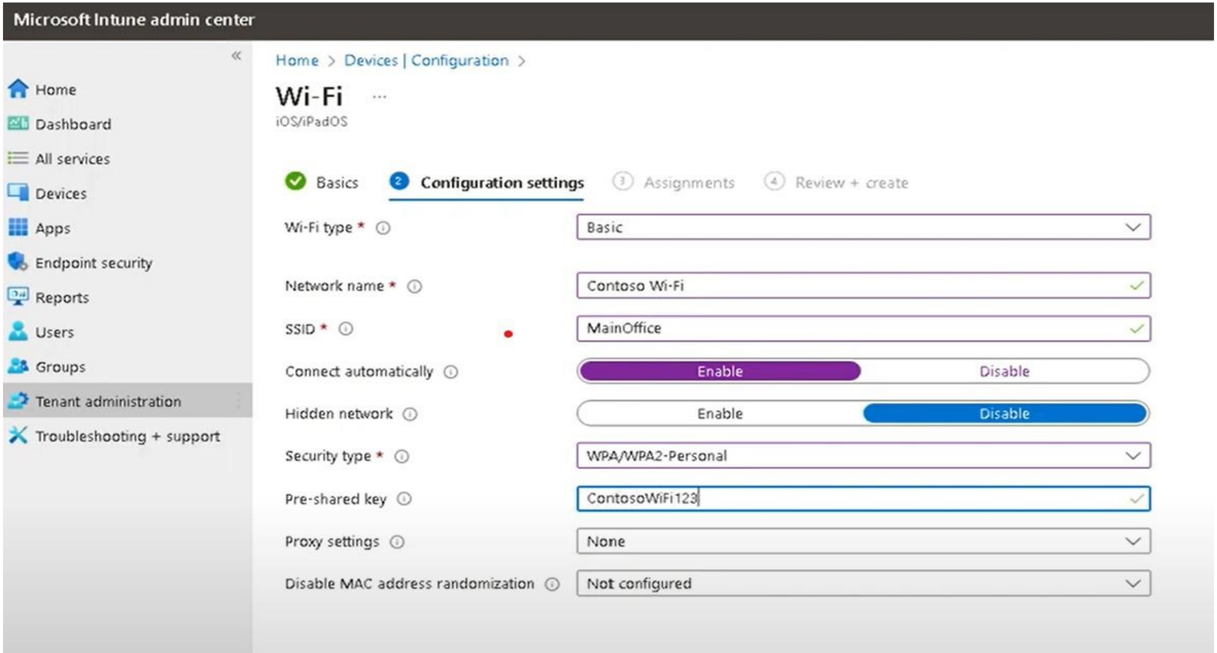
Name * iOS/iPadOS Wi-Fi Policy

Description Wi-Fi settings for iOS/iPadOS Devices.

Platform iOS/iPadOS

Profile type Wi-Fi

Defining Wi-Fi settings such as SSID, security type, and password for mobile devices.



Wi-Fi
iOS/iPadOS

Wi-Fi type * Basic

Network name * Contoso Wi-Fi

SSID * MainOffice

Connect automatically [✓ Enable] Disable

Hidden network Enable [✓ Disable]

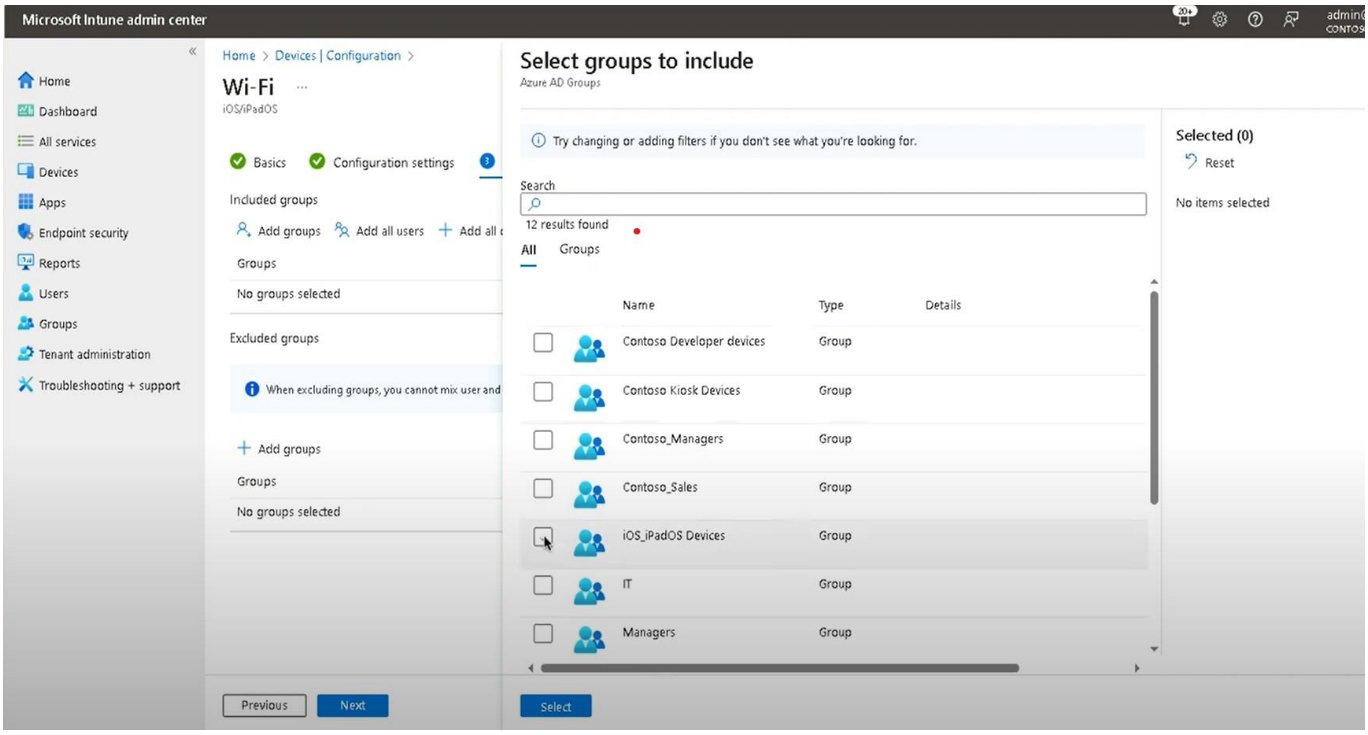
Security type * WPA/WPA2-Personal

Pre-shared key ContosoWiFi123

Proxy settings None

Disable MAC address randomization Not configured

Assigning the Wi-Fi profile to a specific device group (iOS/iPadOS Devices).



Wi-Fi ...

iOS/iPadOS

Included groups

Groups

No groups selected

Excluded groups

When excluding groups, you cannot mix user and

Groups

No groups selected

Select groups to include

Azure AD Groups

Try changing or adding filters if you don't see what you're looking for.

Search

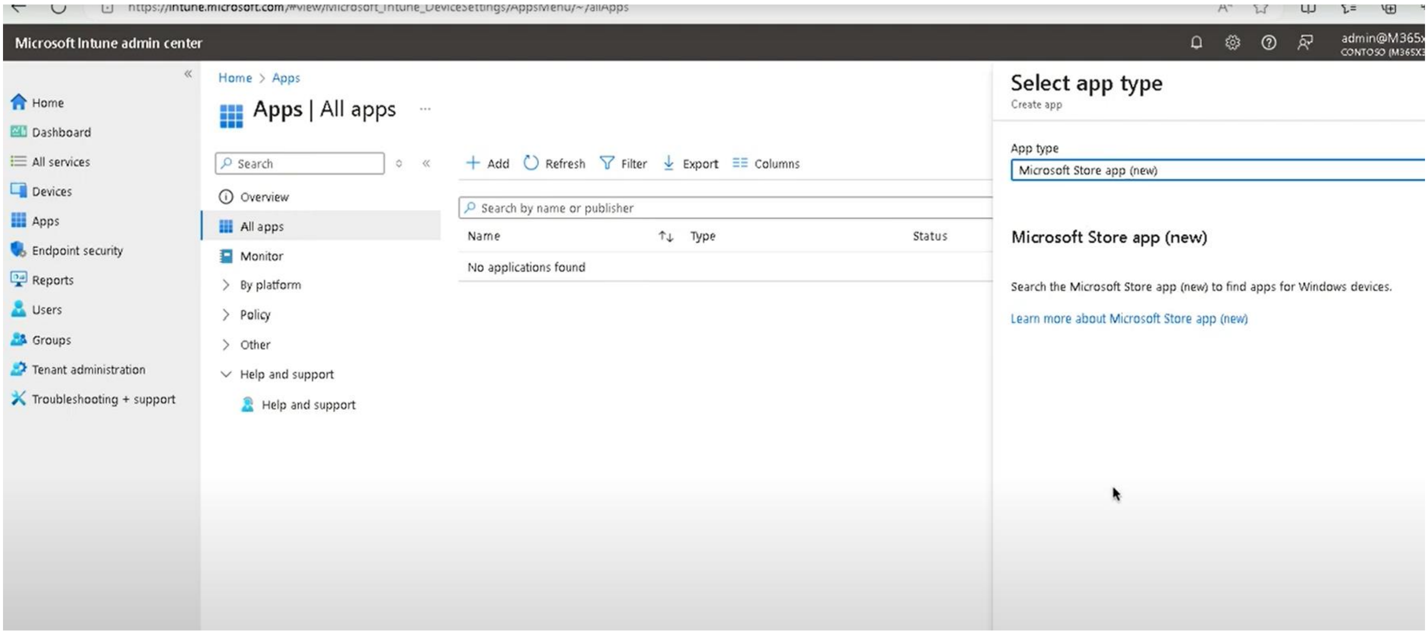
12 results found

Name	Type	Details
Contoso Developer devices	Group	
Contoso Kiosk Devices	Group	
Contoso_Managers	Group	
Contoso_Sales	Group	
iOS_iPadOS Devices	Group	
IT	Group	
Managers	Group	

Selected (0)

No items selected

Additional configuration screens for validating profile creation and assignments.



Apps | All apps

Name	Type	Status
No applications found		

Select app type

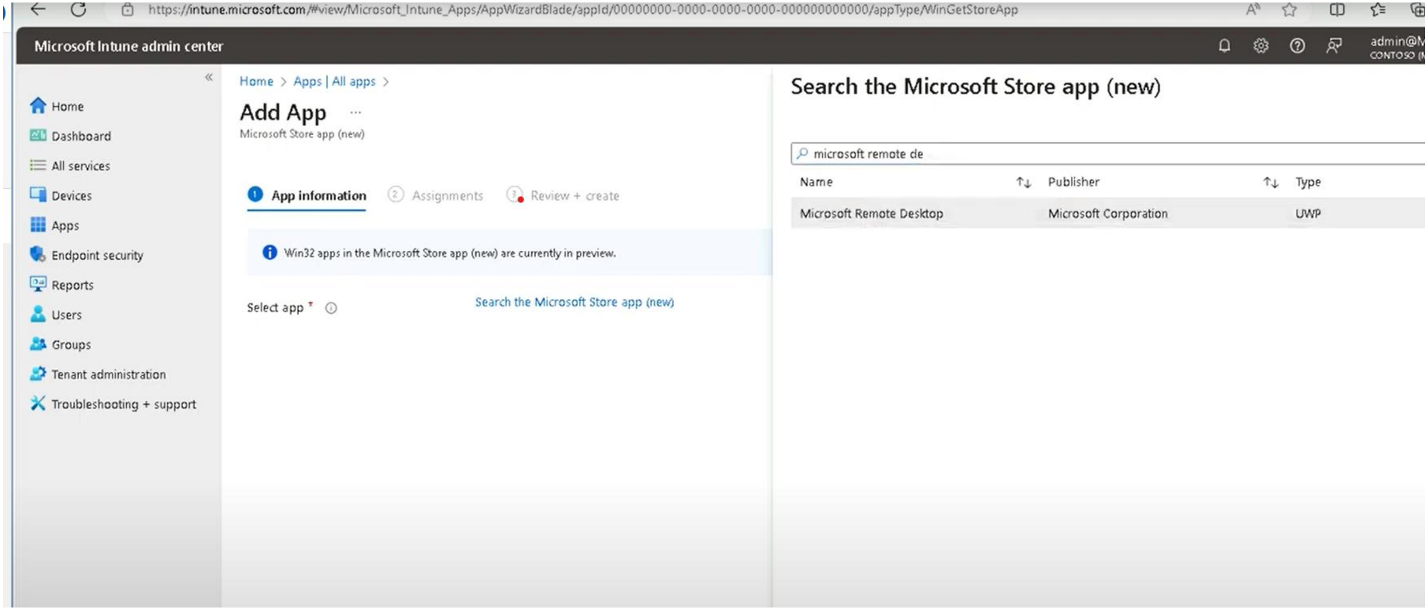
Create app

App type: Microsoft Store app (new)

Microsoft Store app (new)

Search the Microsoft Store app (new) to find apps for Windows devices.

Learn more about Microsoft Store app (new)


https://intune.microsoft.com/#view/Microsoft_Intune_Apps/AppWizardBlade/appId/00000000-0000-0000-0000-000000000000/appType/WinGetStoreApp
Microsoft Intune admin center
admin@M
CONTOSO (M
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Apps | All apps >
1 App information
2 Assignments
3 Review + create

Add App

Microsoft Store app (new)

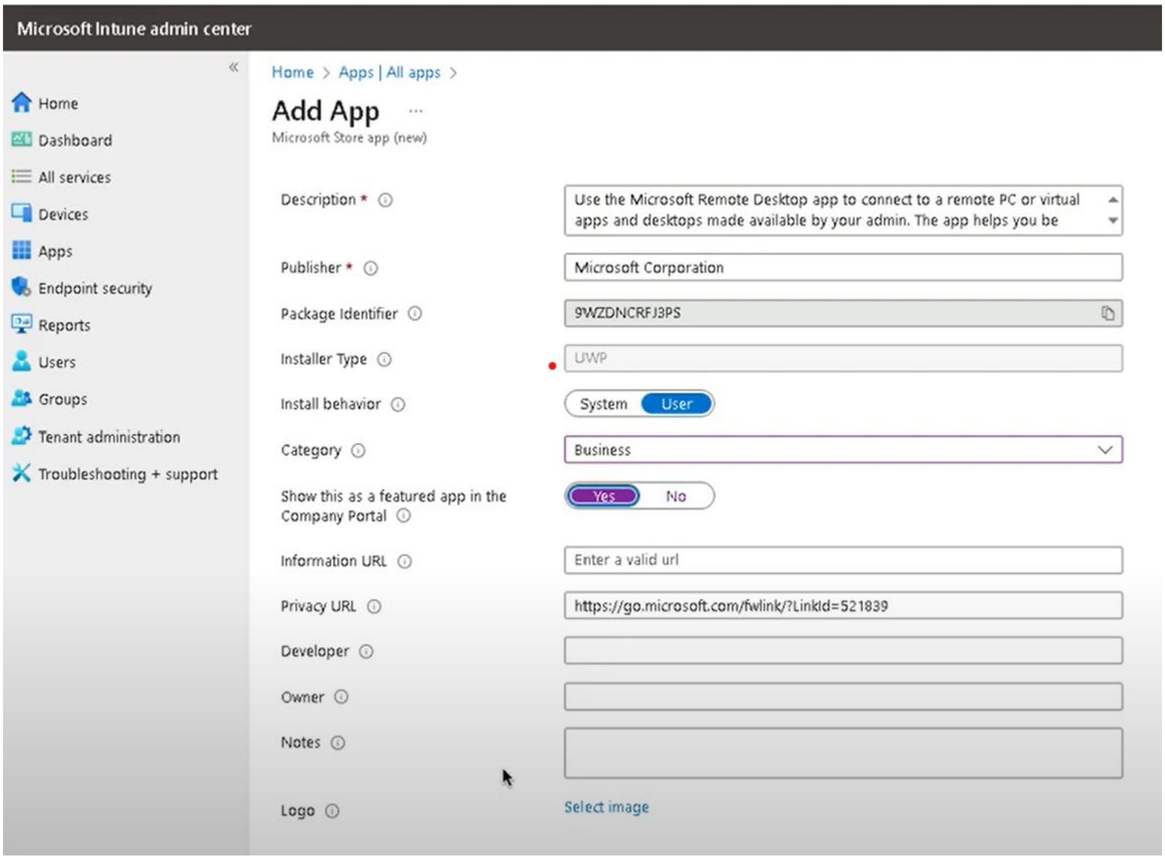
Win32 apps in the Microsoft Store app (new) are currently in preview.

Select app * — Search the Microsoft Store app (new)

Search the Microsoft Store app (new)

microsoft remote de

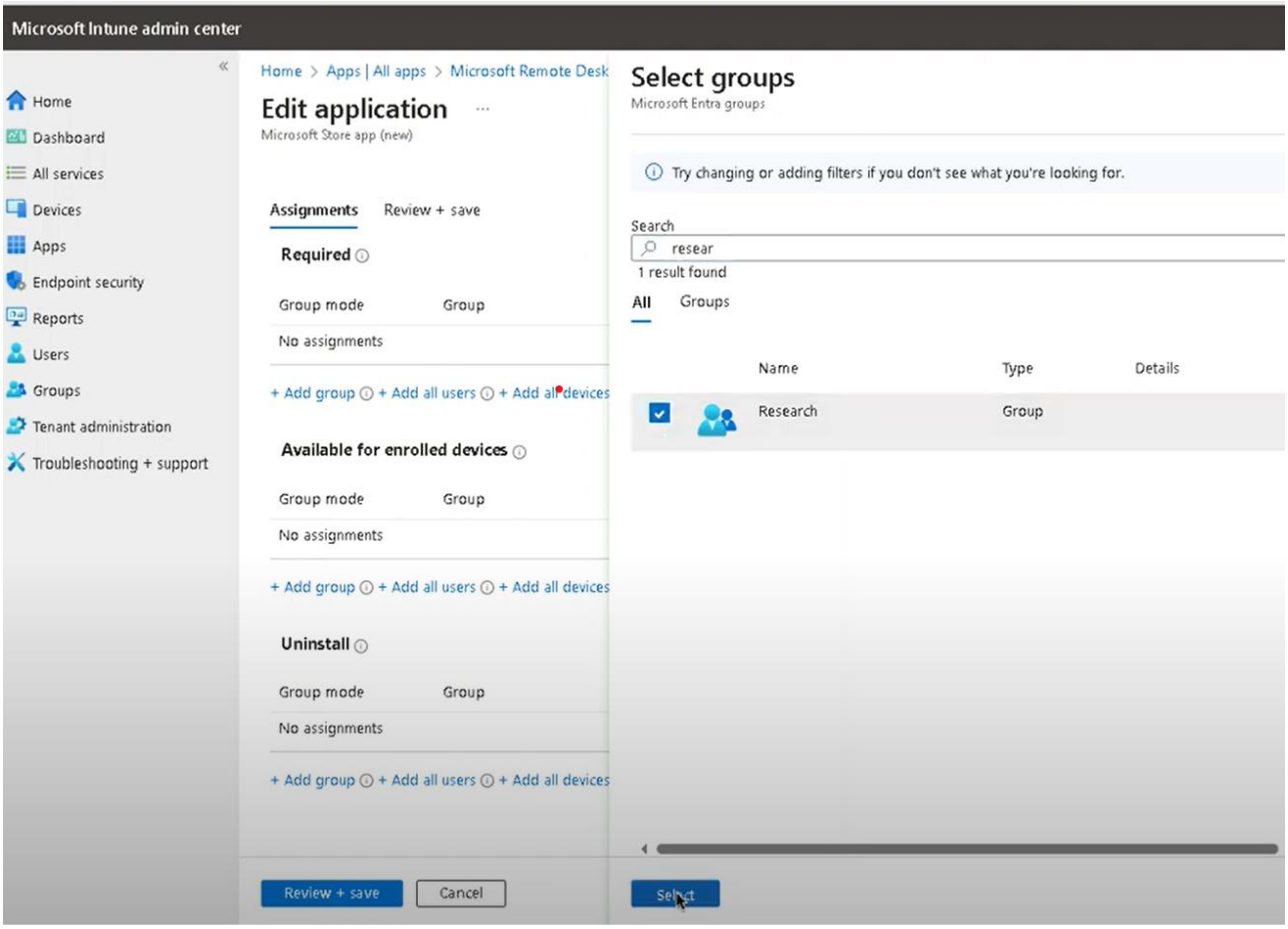
Name	Publisher	Type
Microsoft Remote Desktop	Microsoft Corporation	UWP



Add App

Microsoft Store app (new)

Description *	Use the Microsoft Remote Desktop app to connect to a remote PC or virtual apps and desktops made available by your admin. The app helps you be
Publisher *	Microsoft Corporation
Package Identifier	9WZDNCRFJ3PS
Installer Type	UWP
Install behavior	System [✓ User]
Category	Business
Show this as a featured app in the Company Portal	[✓ Yes] No
Information URL	Enter a valid url
Privacy URL	https://go.microsoft.com/fwlink/?LinkId=521839
Developer	
Owner	
Notes	
Logo	Select image



Edit application

Microsoft Store app (new)

Required ⓘ

Group mode	Group
No assignments	

Available for enrolled devices ⓘ

Group mode	Group
No assignments	

Uninstall ⓘ

Group mode	Group
No assignments	

Select groups

Microsoft Entra groups

ⓘ Try changing or adding filters if you don't see what you're looking for.

Search: resear

1 result found

	Name	Type	Details
☑	Research	Group	