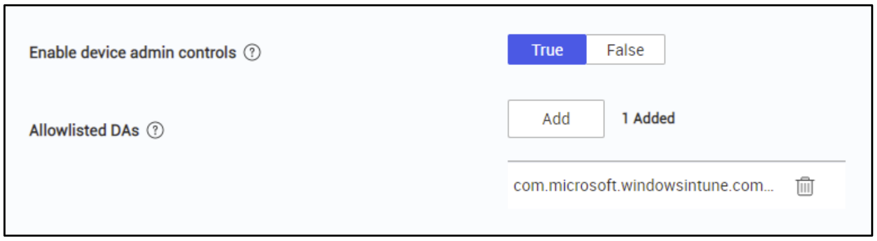
Knox Manage + Intune Mobile Application Management Setup Guide

Pre-requisites: Knox-enabled devices, Knox Suite license or KPE License for KSP policies

1. Enroll your device to Knox Manage. For more information, see Enroll devices.
2. Login to your **Knox Manage** then go to Applications and add **Intune Company Portal** from Playstore.
3. Go to Profile then modify your policy. Look for **Knox Service Plugin** under Samsung Knox: Android Enterprise.
   Look for Device-wide policies and set the following:
   Enable device policy controls: **True**
   Enable device admin controls (under Device Admin allowlisting): **True**
   Then add Intune Company Portal to the Allowlisted DAs

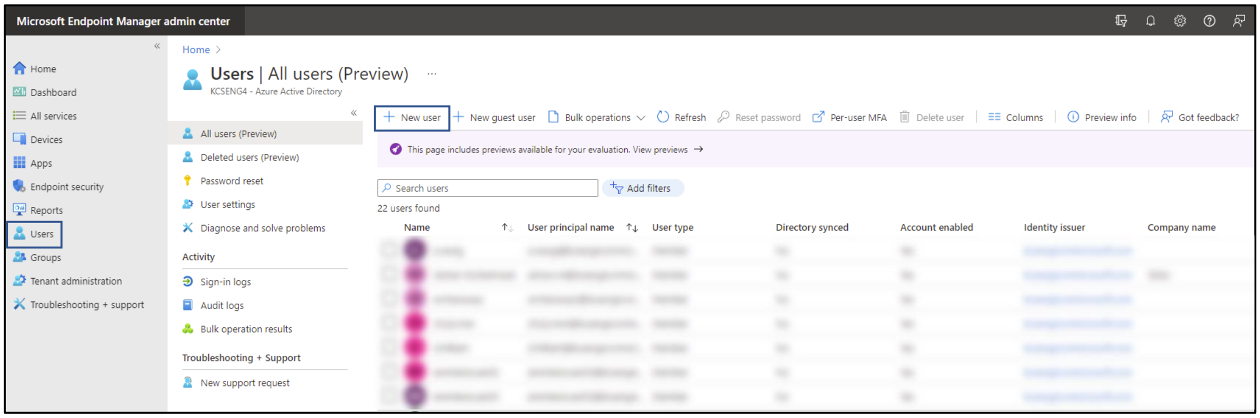


Enable device admin controls ⓘ — [✓ True] False

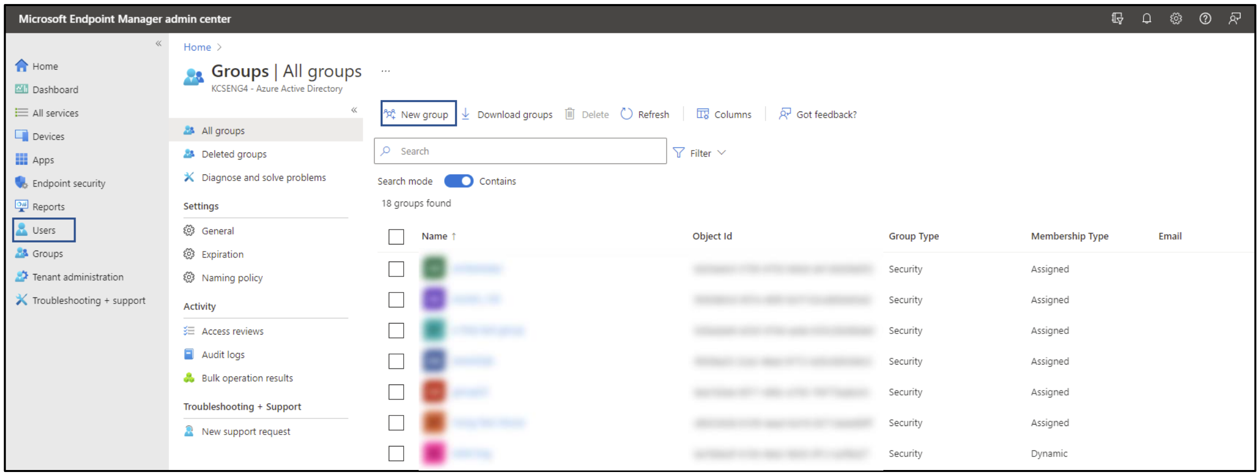
Allowlisted DAs ⓘ — Add — 1 Added

com.microsoft.windowsintune.com...

   Save the changes on your profile and apply it to your devices.
4. Login to your **Microsoft Endpoint Manager admin center**.
5. On the left-hand navigation menu, click **Users** to create a user for your new devices.

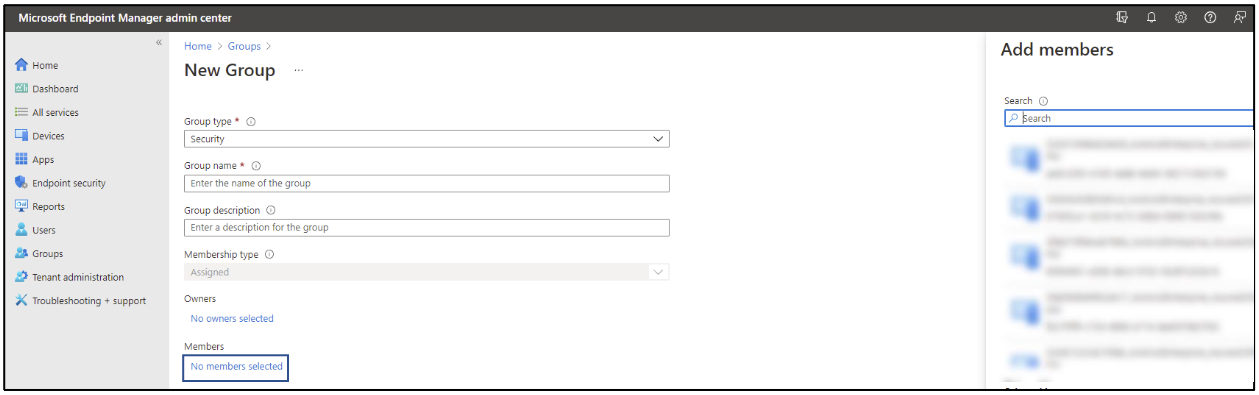


6. After creating a user, click **Groups** to create a group where you can assign your users and policies.



□	Name ↑	Object Id	Group Type	Membership Type	Email
□	[redacted]	[redacted]	Security	Assigned	
□	[redacted]	[redacted]	Security	Assigned	
□	[redacted]	[redacted]	Security	Assigned	
□	[redacted]	[redacted]	Security	Assigned	
□	[redacted]	[redacted]	Security	Assigned	
□	[redacted]	[redacted]	Security	Assigned	
□	[redacted]	[redacted]	Security	Dynamic	

Click **No members selected** to assign the created user on step 5 to the group.



Group type * Security

Group name * Enter the name of the group

Group description Enter a description for the group

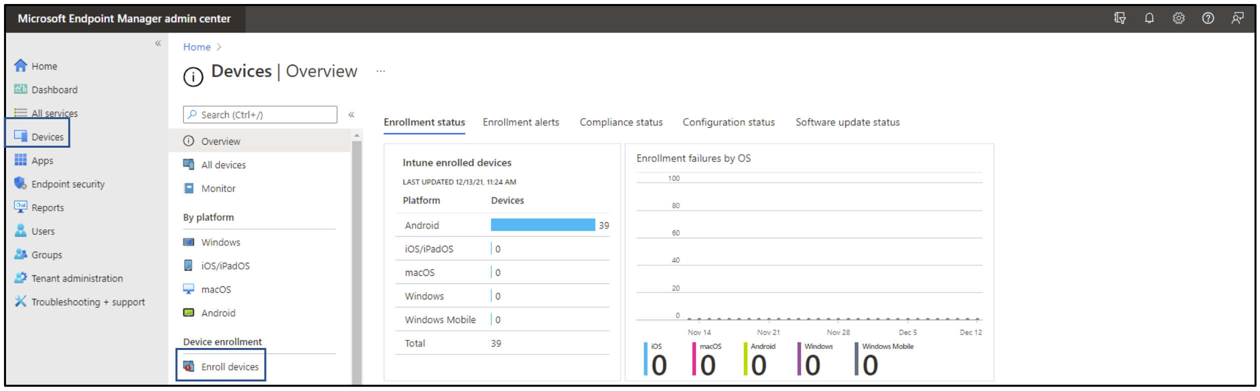
Membership type Assigned

Owners No owners selected

Members No members selected

[redacted]

7. Go to **Devices** and click **Enroll devices** under **Device Enrollment**.

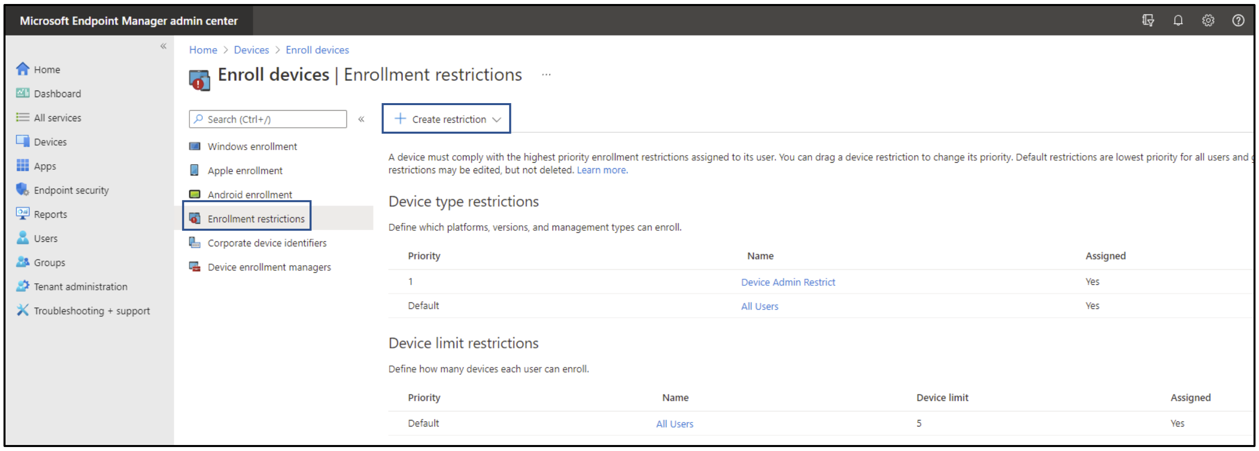


Intune enrolled devices

LAST UPDATED 12/13/21, 11:24 AM

Platform	Devices
Android	39
iOS/iPadOS	0
macOS	0
Windows	0
Windows Mobile	0
Total	39

Then click **Enrollment restrictions > Create restriction > Device type restriction** to create restriction that will define what devices can enroll into management with Intune. For more information, see Set enrollment restrictions.



Enroll devices | Enrollment restrictions

A device must comply with the highest priority enrollment restrictions assigned to its user. You can drag a device restriction to change its priority. Default restrictions are lowest priority for all users and restrictions may be edited, but not deleted. Learn more.

Device type restrictions

Define which platforms, versions, and management types can enroll.

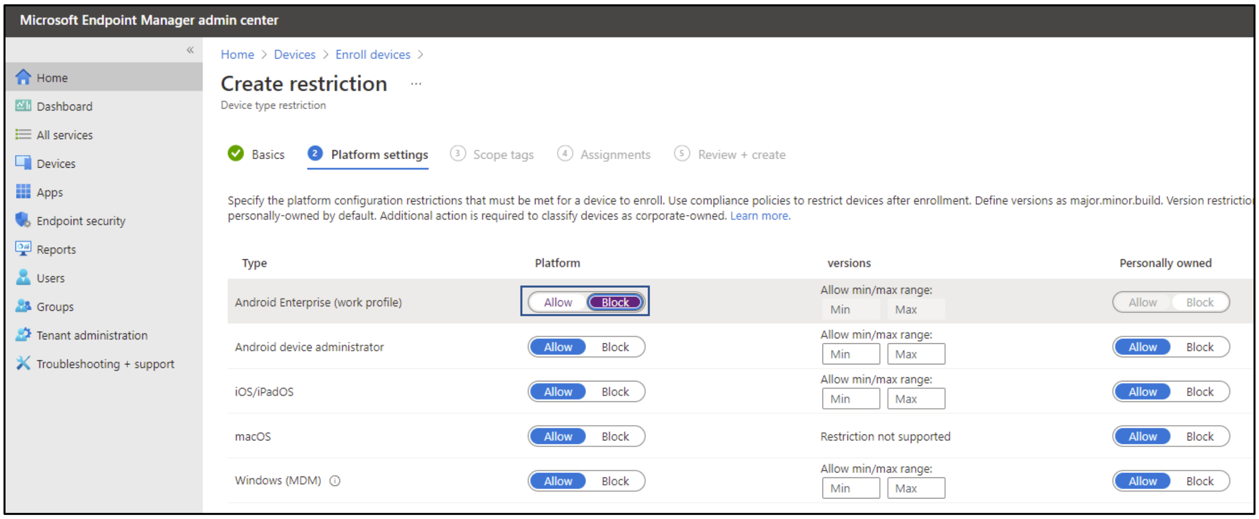
Priority	Name	Assigned
1	Device Admin Restrict	Yes
Default	All Users	Yes

Device limit restrictions

Define how many devices each user can enroll.

Priority	Name	Device limit	Assigned
Default	All Users	5	Yes

On **Platform Settings**, block **Android Enterprise (Work Profile)**. This will prevent Intune installing a Work Profile to our managed devices as it will cause conflict with Knox Manage.



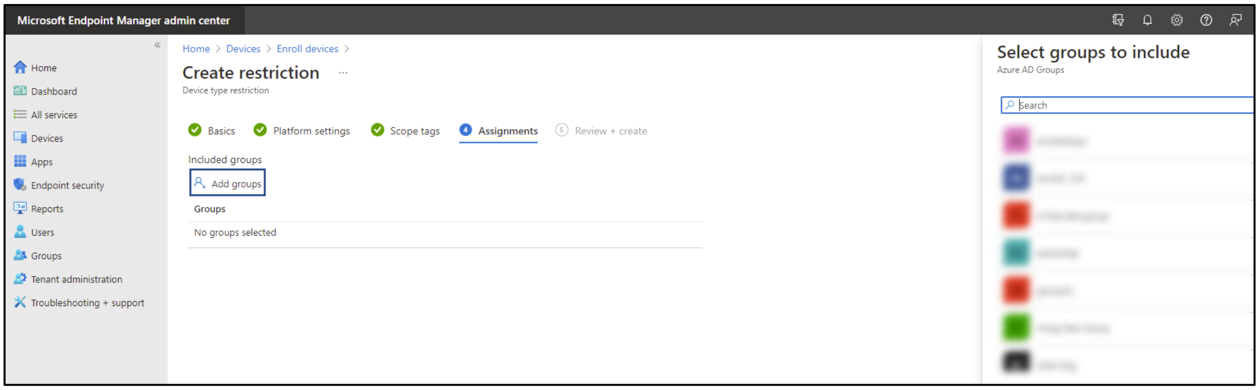
Create restriction

Device type restriction

Specify the platform configuration restrictions that must be met for a device to enroll. Use compliance policies to restrict devices after enrollment. Define versions as major.minor.build. Version restrictio personally-owned by default. Additional action is required to classify devices as corporate-owned. Learn more.

Type	Platform	versions	Personally owned
Android Enterprise (work profile)	Allow [✓ Block]	Allow min/max range: Min Max	Allow Block
Android device administrator	[✓ Allow] Block	Allow min/max range: Min Max	[✓ Allow] Block
iOS/iPadOS	[✓ Allow] Block	Allow min/max range: Min Max	[✓ Allow] Block
macOS	[✓ Allow] Block	Restriction not supported	[✓ Allow] Block
Windows (MDM) ⓘ	[✓ Allow] Block	Allow min/max range: Min Max	[✓ Allow] Block

After configuring the platform settings, assign the restriction to the created group on step 6.



Create restriction

Device type restriction

Included groups

Groups

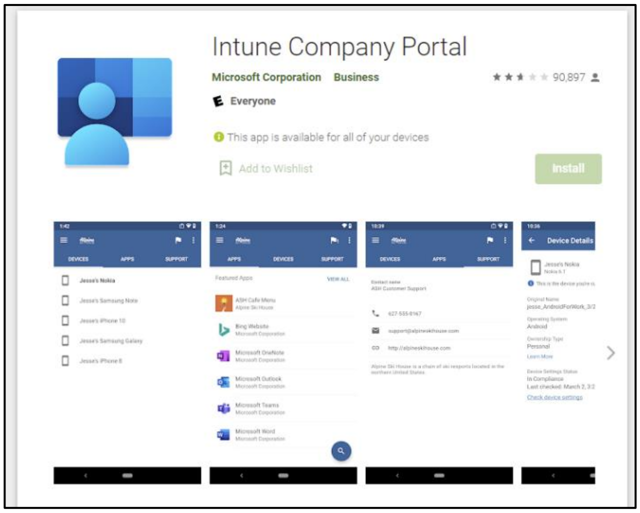
No groups selected

Select groups to include

Azure AD Groups

[redacted]

8. Enroll your device to Intune by logging on the created user on step 5 to **Intune Company Portal**. You can download the app on Playstore or you can push it to your managed devices using Knox Manage.



Intune Company Portal

Microsoft Corporation Business

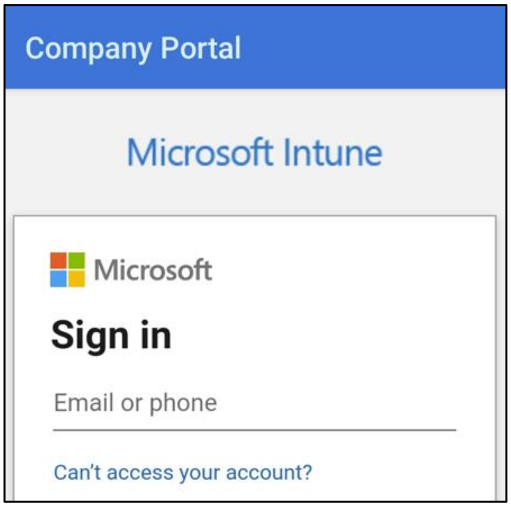
★★★★★ 90,897

Everyone

This app is available for all of your devices

Add to Wishlist

Install



Company Portal

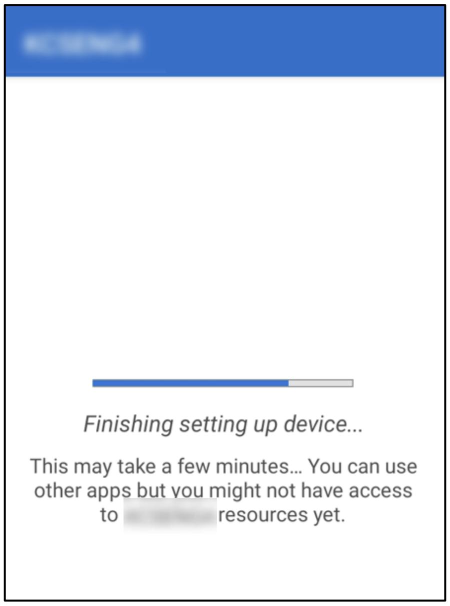
Microsoft Intune

Microsoft

Sign in

Email or phone

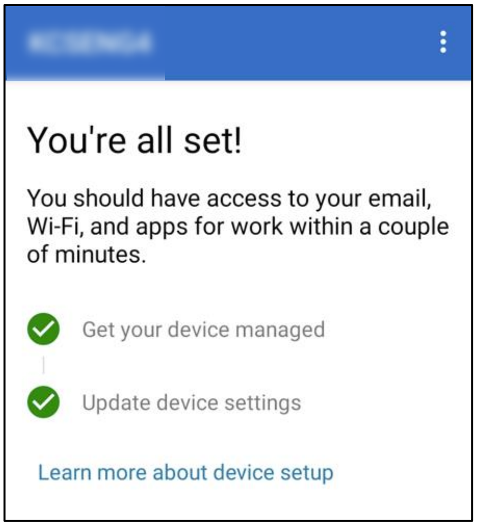
Can't access your account?



[redacted]

Finishing setting up device...

This may take a few minutes... You can use other apps but you might not have access to [redacted] resources yet.



[redacted]

You're all set!

You should have access to your email, Wi-Fi, and apps for work within a couple of minutes.

✓ Get your device managed

✓ Update device settings

Learn more about device setup

Note: Accept all system permission requests. You can go to Settings > Apps > Intune Company Portal > Permissions to check all the app permissions needed.

9. After successfully enrolling the device to Intune, you can now add internal applications or applications from android playstore. For more information, see Add android store apps to Microsoft Intune and Add apps to Microsoft Intune.

Additionally, you can also add Microsoft Intune app protection policies for the users of your group. For more information, see How to create and assign app protection policies

Note: All applications will be installed on the Device Owner area and there will be no Work Profile installed on the device.