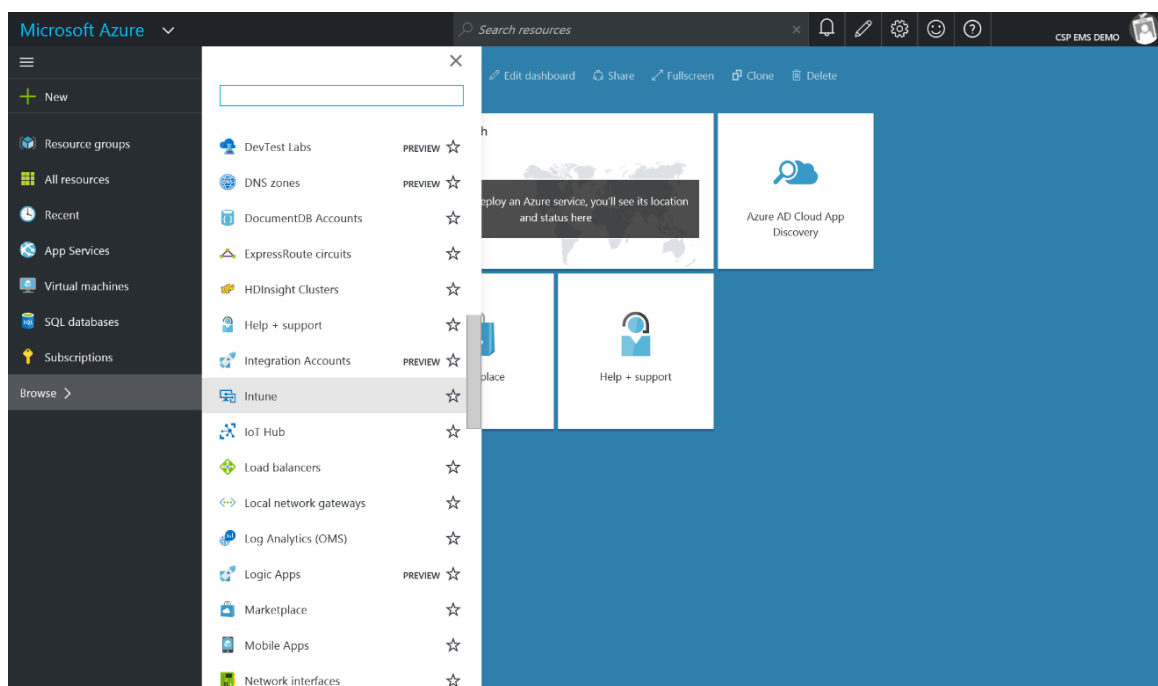


Microsoft Intune Mobile Application Management without device enrollment

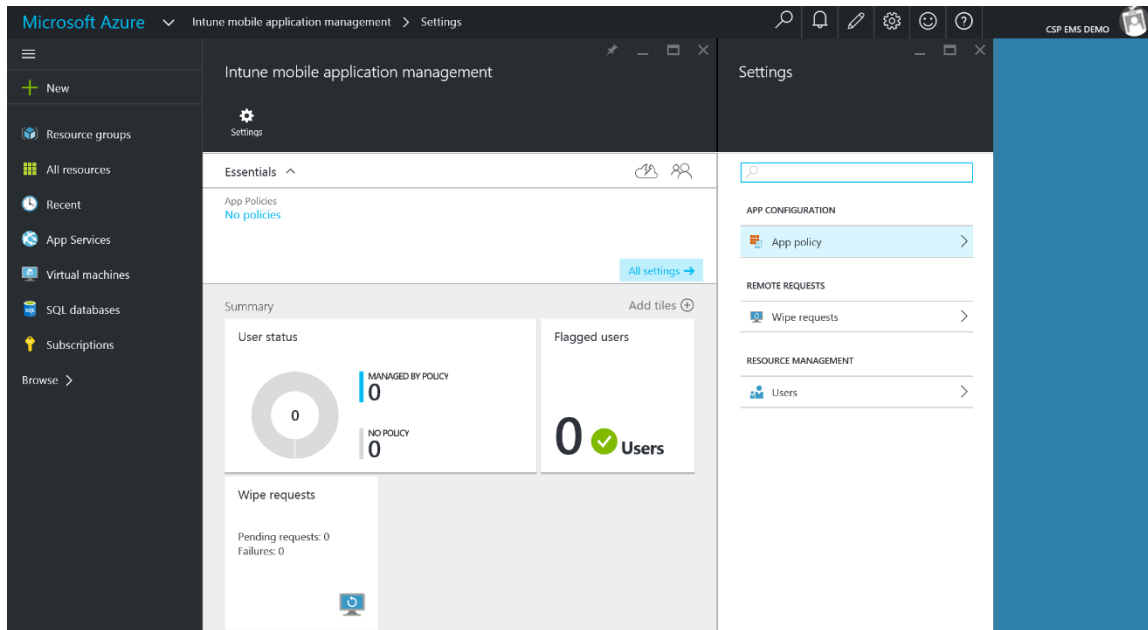
The Intune MAM without enrollment features allow organizations to protect their Office apps on iOS and Android without the need to enroll their devices in Intune MDM. This means end customers who already have an MDM vendor, or don't wish to manage their user's devices via MDM, can protect access to Office 365 and company data. This includes cut/copy/paste restrictions, preventing 'save-as', jailbreak detection, PIN requirements and the ability to remote wipe MAM protected data.

In the following **example**, a Microsoft Intune MAM policy is created to manage Microsoft OneNote on iOS devices that have not been enrolled.

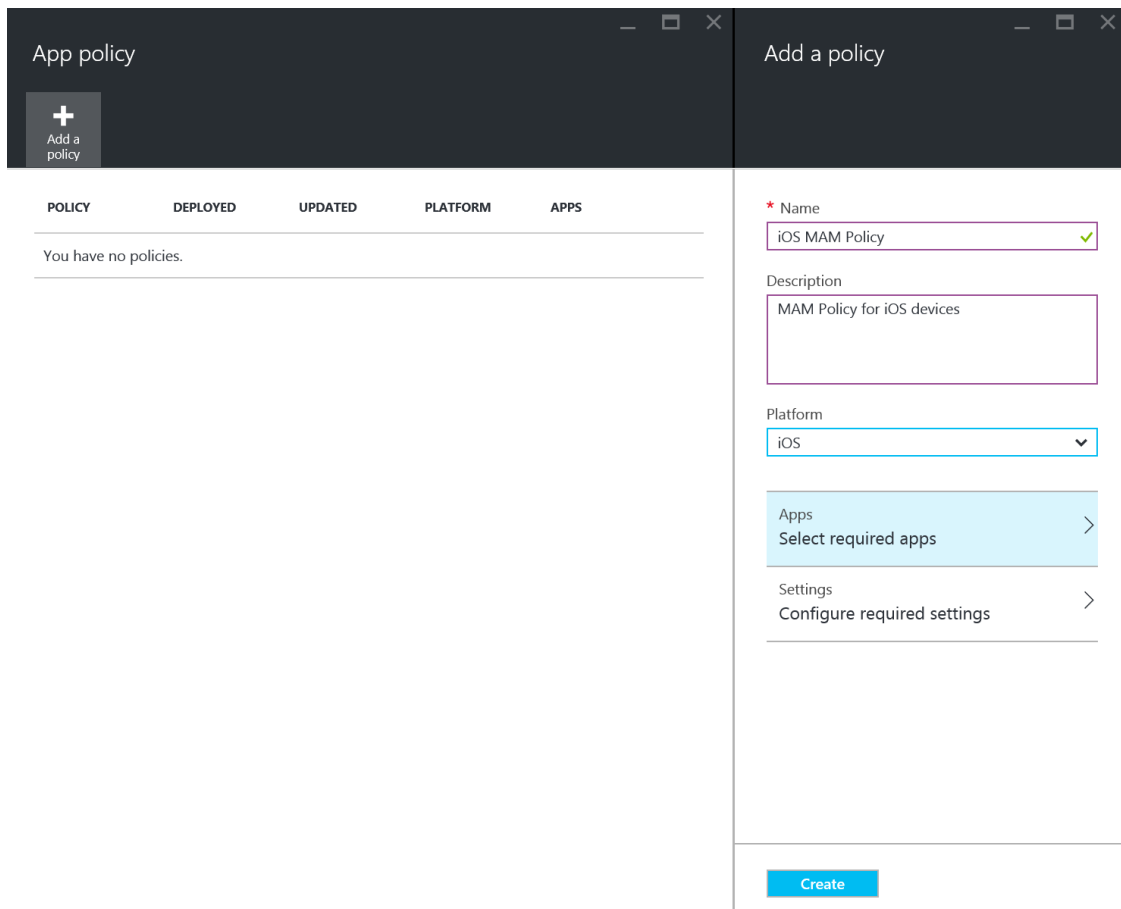
1. Log in to the [Microsoft Azure portal](#). From the menu, select **Browse** and then **Intune**.



2. Select **App policy**.











3. Select **Add a Policy** and fill in the required fields.



4. Click on **Select required apps**, and then select **OneNote** as the application targeted for this **example** policy. Administrators can also select multiple applications in the list to meet the end customer's requirement.



APP		PLATFORM
	OneDrive	iOS
	Excel	iOS
	PowerPoint	iOS
	Word	iOS
	 OneNote	iOS
	Outlook	iOS
	Managed Browser	iOS
	Remote Desktop	iOS

5. Select **Configure required settings** and configure with the settings as agreed upon with the end customer.

Settings

Data relocation

Prevent iTunes and iCloud backups ⓘ

Yes

No

Allow app to transfer data to other apps ⓘ

Policy managed apps

Allow app to receive data from other apps ⓘ

All apps

Prevent "Save As" ⓘ

Yes

No

Restrict cut, copy, and paste with other apps ⓘ

Policy managed apps with paste in

Restrict web content to display in the Managed Browser ⓘ

Yes

No

Encrypt app data ⓘ

When device is locked

Disable contacts sync ⓘ

Yes

No

Access

Require simple PIN for access ⓘ

Yes

No

Number of attempts before PIN reset ⓘ

5

Allow fingerprint instead of PIN (iOS 8+) ⓘ

Yes

No

Require corporate credentials for access ⓘ

Yes

No

Block managed apps from running on jailbroken or rooted devices ⓘ

Yes

No

Recheck the access requirements after (minutes)

Timeout ⓘ

30

Offline grace period

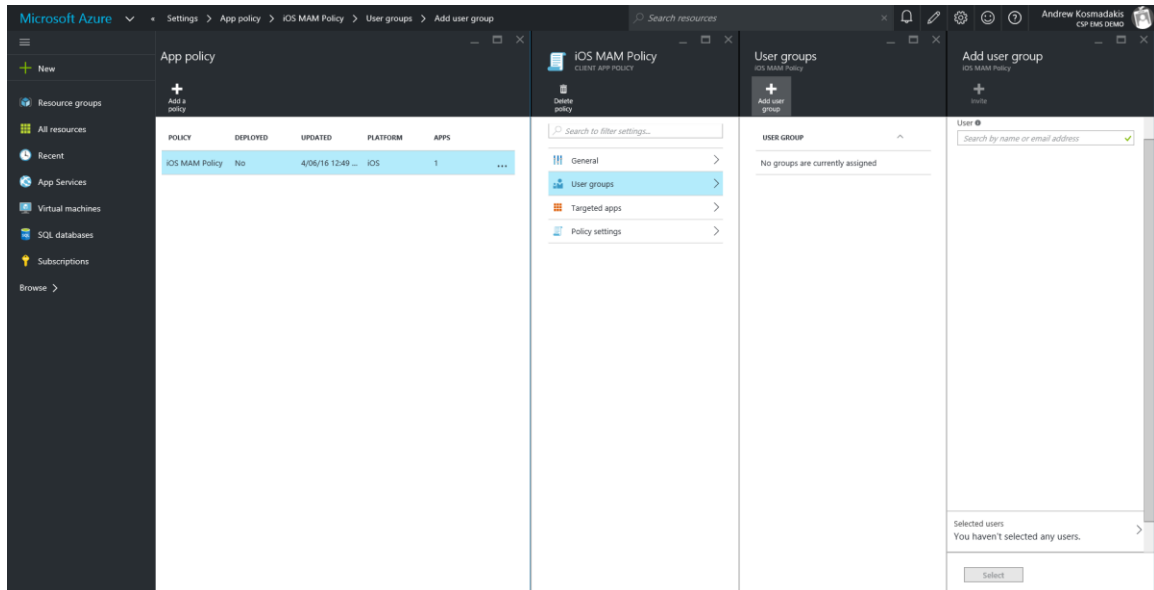
720

Offline interval (days) before app data is wiped ⓘ

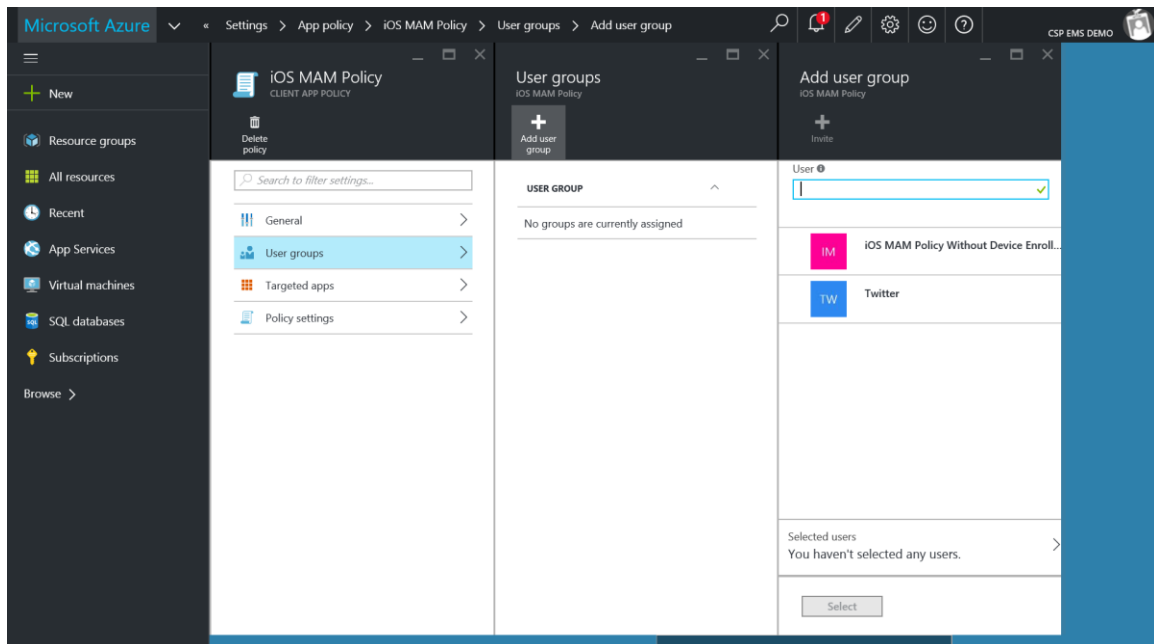
90

OK

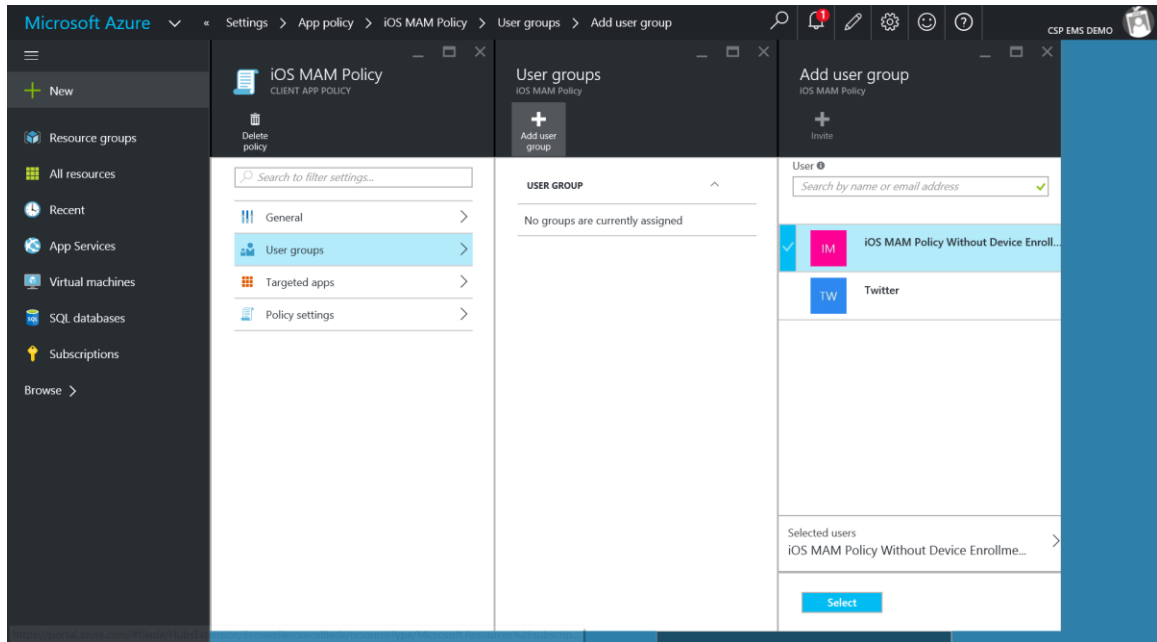
6. Once the applications and settings have been configured, select **Create**.
7. Once the policy is created, select **User Groups**.



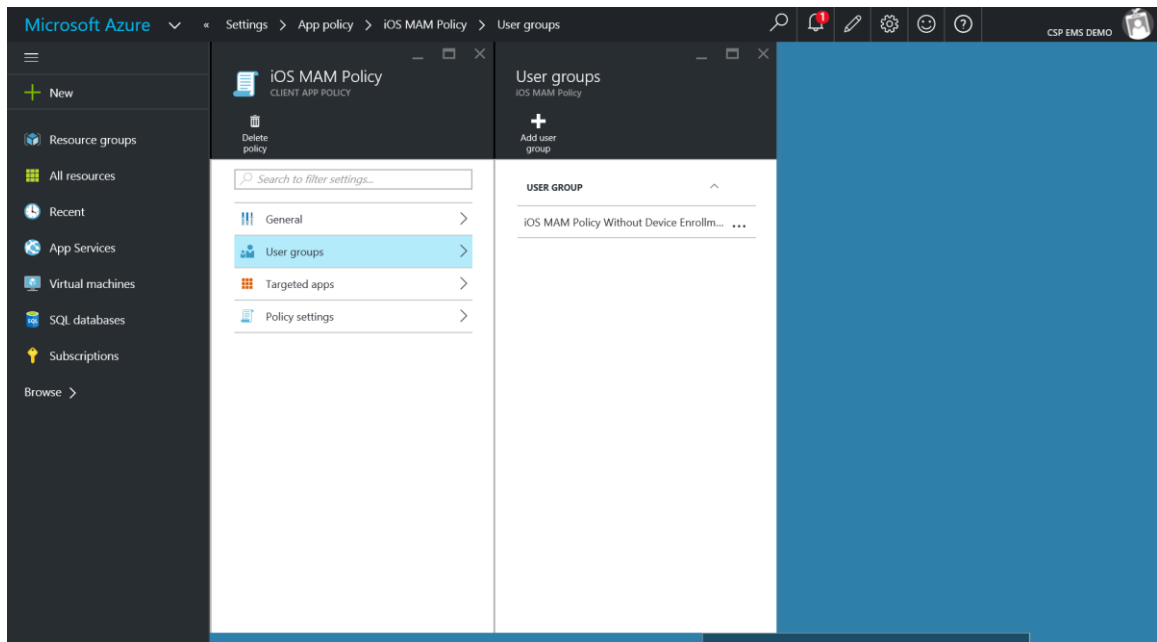
8. Select **Add user group**.



9. Select the security group **iOS MAM Policy Without Device Enroll...** to assign this policy to members of this group.



10. Click on **Select** at the bottom



This Policy has now been successfully created and deployed to the members of this group.