MultiLine for Intune Installation Guide for Intune Admins

Last Modified on 04/25/2024 11:39 am EDT

This guide is for Intune admins who are setting up MultiLine for Intune in the Endpoint Manger.

Overview

MultiLine for Intune must be deployed as an Intune Managed App before onboarding users. A user with administrator privileges in Endpoint Manager (Intune Admin) must complete the following steps:

- Step 1: Add MultiLine for Intune to Endpoint Manager
- Step 2: Create user group for MultiLine for Intune users
- Step 3: Create and add an app protection policy
- Step 4: Grant MultiLine permission to access resources in your organization

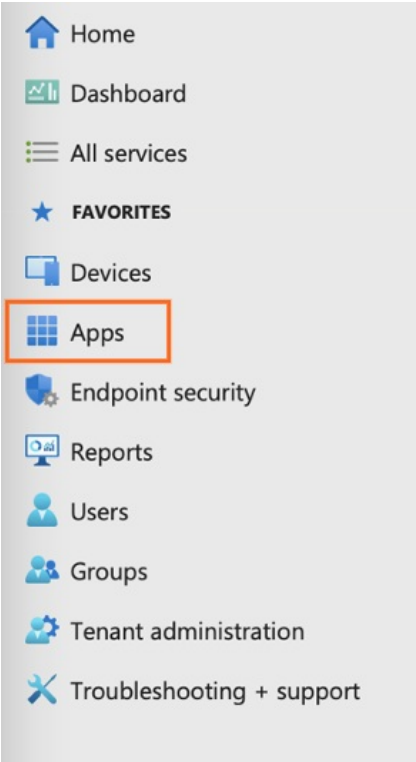
Once this process is complete the MultiLine administrator can begin onboarding users.

> Organizations can set up MultiLine for Intune under MAM or MDM policies. SeeMicrosoft Intune's documentation [External] (https://learn.microsoft.com/en-us/microsoft-365/business/ui/mam-and-mdm?view=o365-worldwide) for more information.

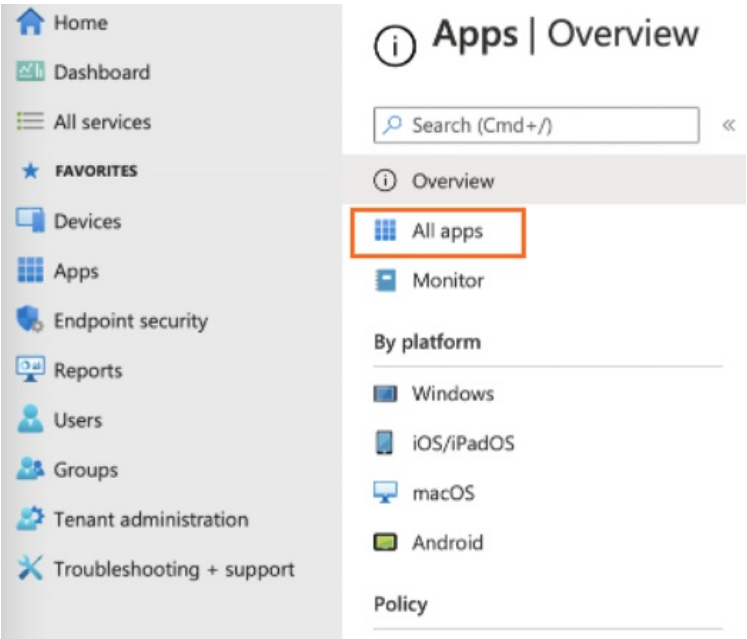
Step 1 - Add MultiLine for Intune to Endpoint Manager

The first step to deploy MultiLine for Intune as an Intune app is to add the application to Microsoft Endpoint Manger.

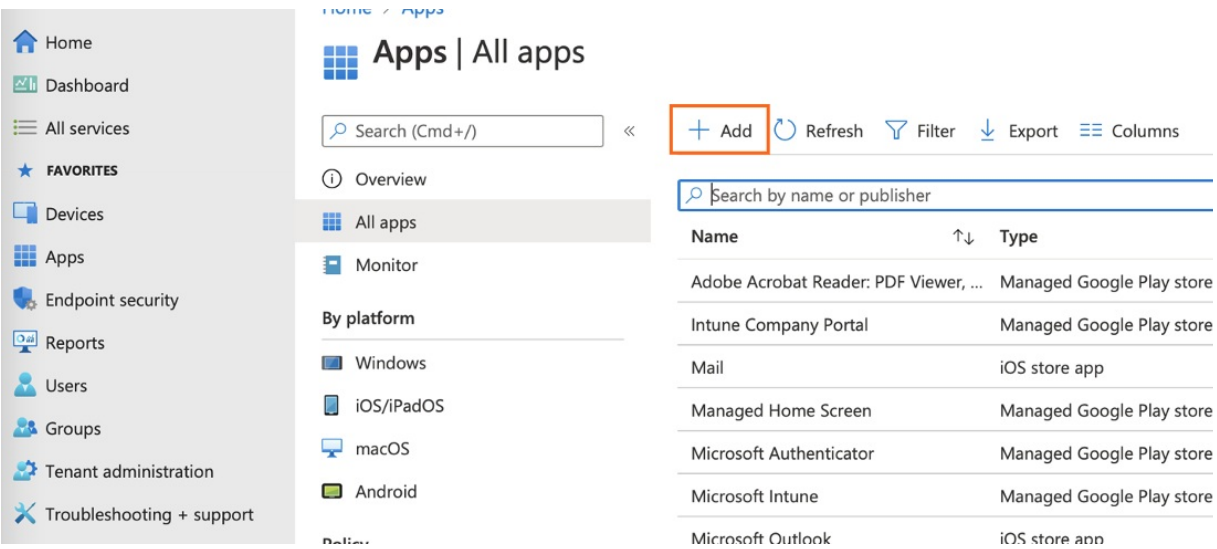
1. Log into the portal manager at https://endpoint.microsoft.com (https://endpoint.microsoft.com/)
2. In the left menu, select **Apps**



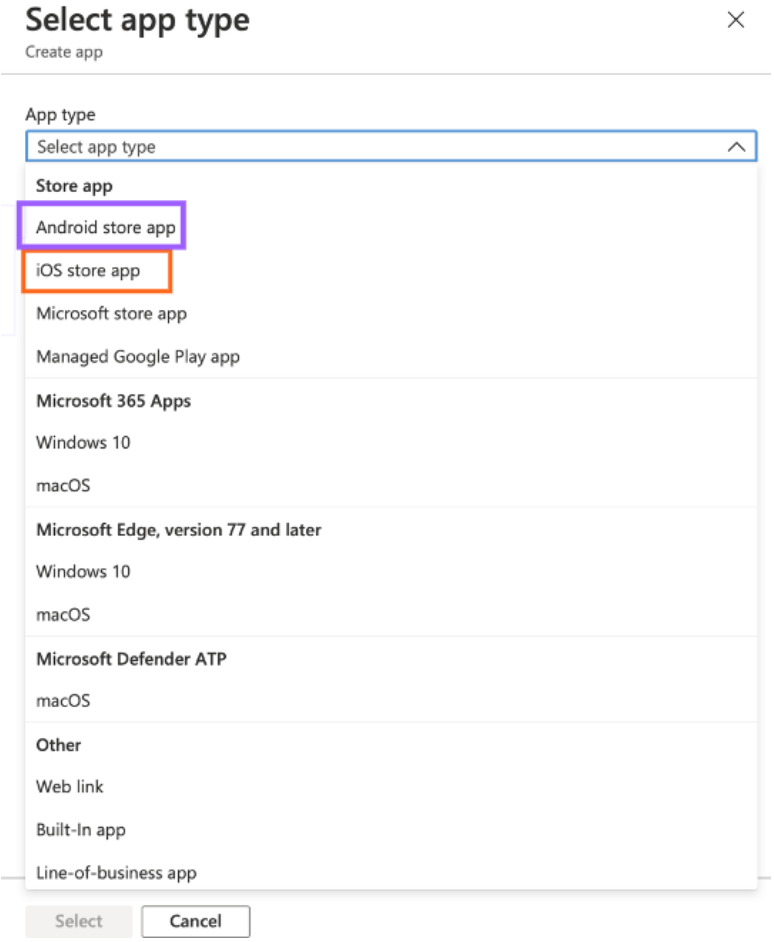
3. Select **All apps** from the sub menu



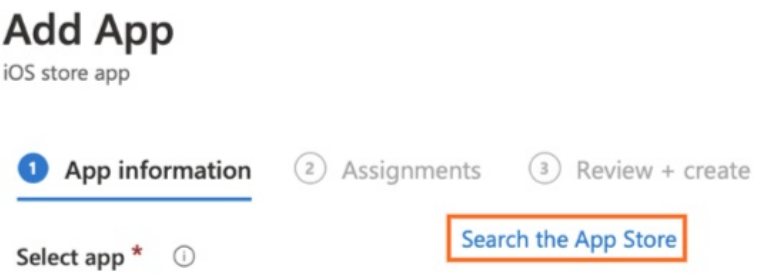
4. Select **+Add** from the top menu



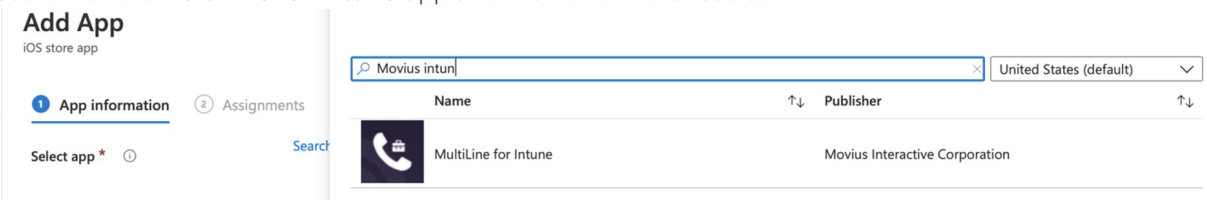
5. Choose **iOS store app** for iOS or **Android store app** for Android from the menu then click **Select**



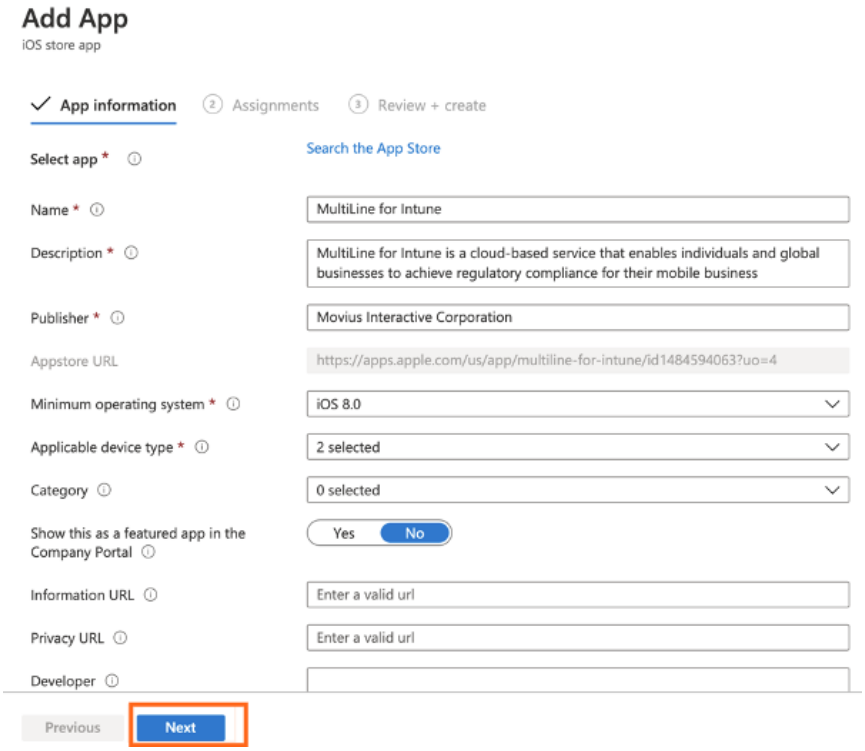
6. Click the **Search the App Store** link



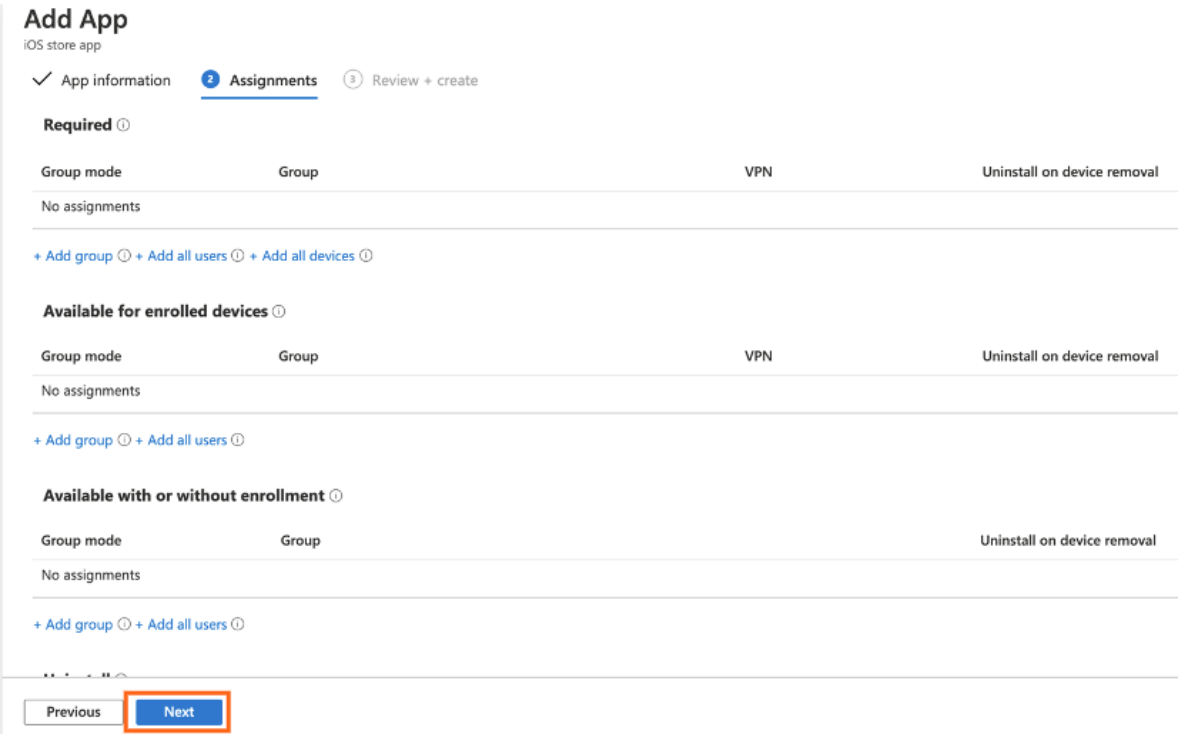
7. Search for the **MultiLine for Intune** app and click it from the results



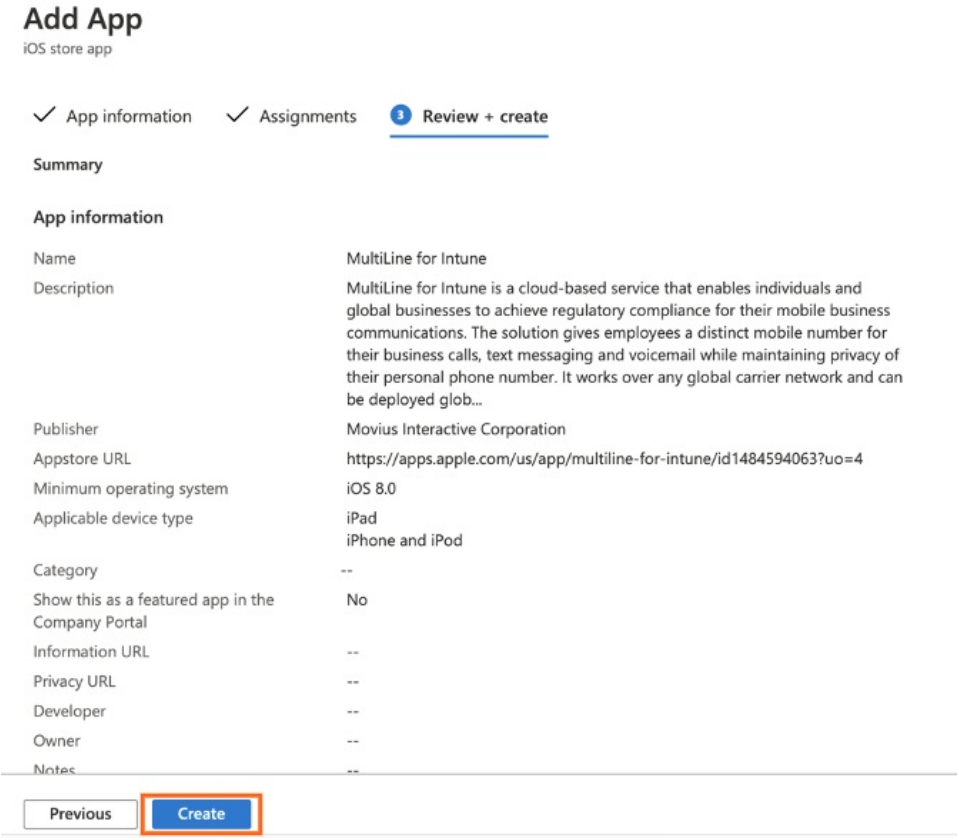
8. Click **Next** on the App Information screen. *The details automatically populate from the app store.*
   1. For iOS, select **iOS 8.0** for minimum operating system
   2. For Android, select **Android 4.0 (Ice Cream Sandwich)** for minimum operating system



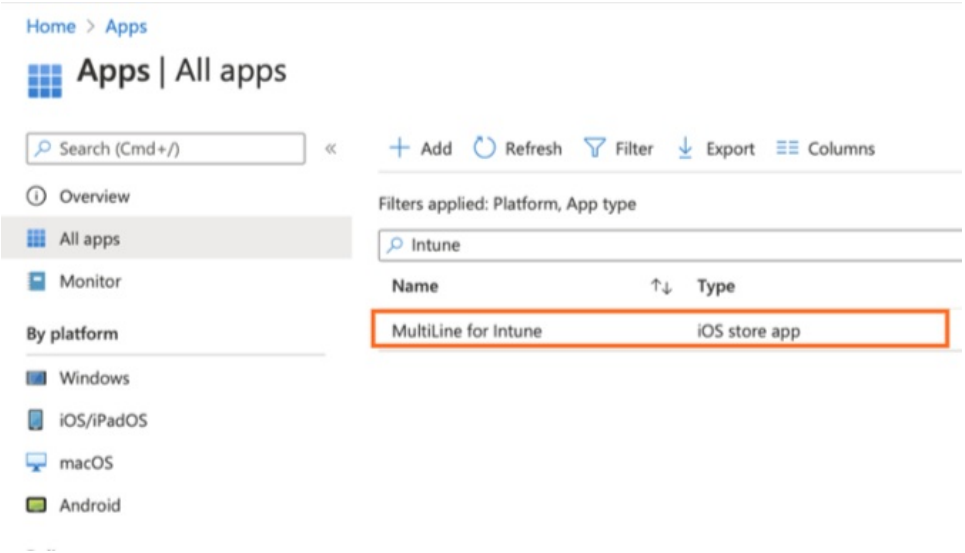
9. Assign the App to your groups and click next



10. Verify the information in the **Summary** on the **Review + Create** page, then click **Create**



When completed, your application will appear in the **Apps** view



Now that we've added MultiLine for Intune to Endpoint Manager, the next step is to Create User Group.

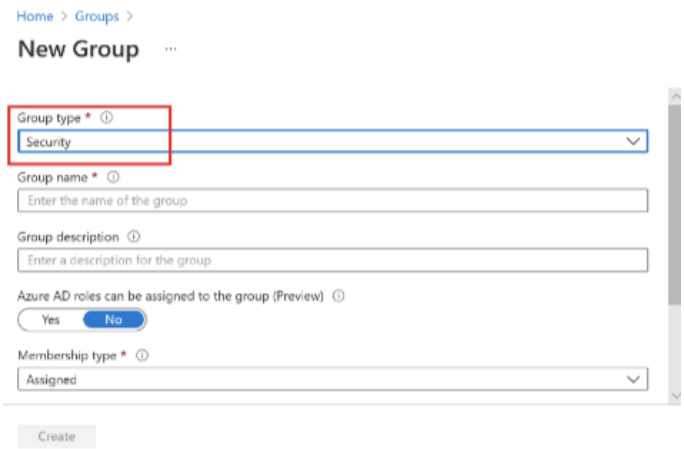
Step 2 - Create User group for MultiLine Intune users

This procedure guides the Azure Admin in the steps to add a user group that will receive the Intune App Protection Policy specific to MultiLine for Intune.

Pre-requisites

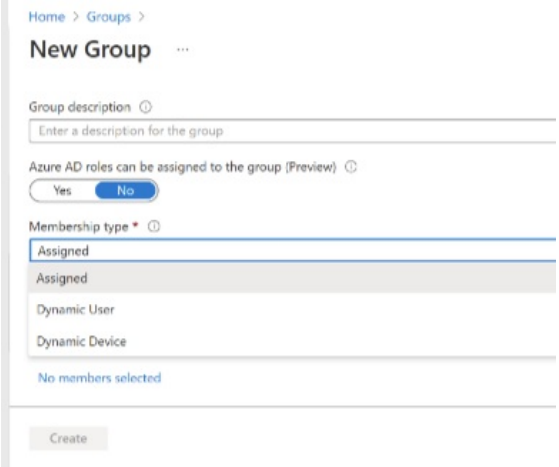
- This user needs administrator permissions on Endpoint Manager to perform these instructions
- MultiLine for Intune must be added to Microsoft Endpoint Manager

1. Create a user group [External Link] (https://docs.microsoft.com/en-us/mem/intune/fundamentals/groups-add) for MultiLine for Intune users, or edit the group according to the details below:
    1. MultiLine for Intune users need to be in a **Security** user group. *This is required.*



Security groups are used to give group members access to applications, resources and assign licenses. Group members can be users, devices, service principals, and other groups.

2. Set the **Group name** and **Description** such that all Azure admins will know the purpose of this group.
3. Set **Membership** type to **Assigned**.



4. Add members and create the group as usual.

The newly added Group will be listed under **Groups > All Groups**.

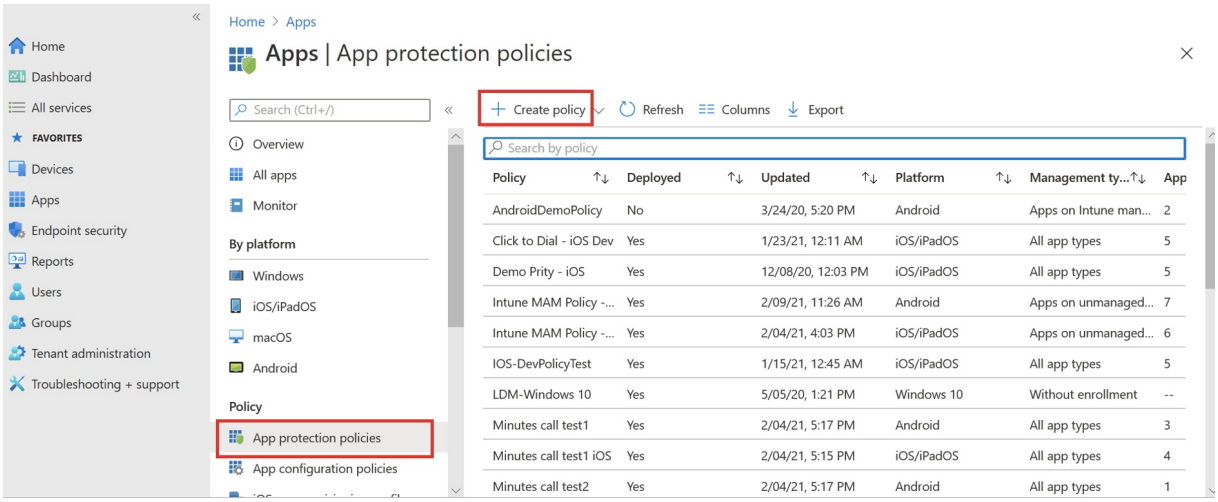
Now that we have created the user group, we can now apply the appropriate protection policies to it.

Step 3 - Create and add an app protection policy

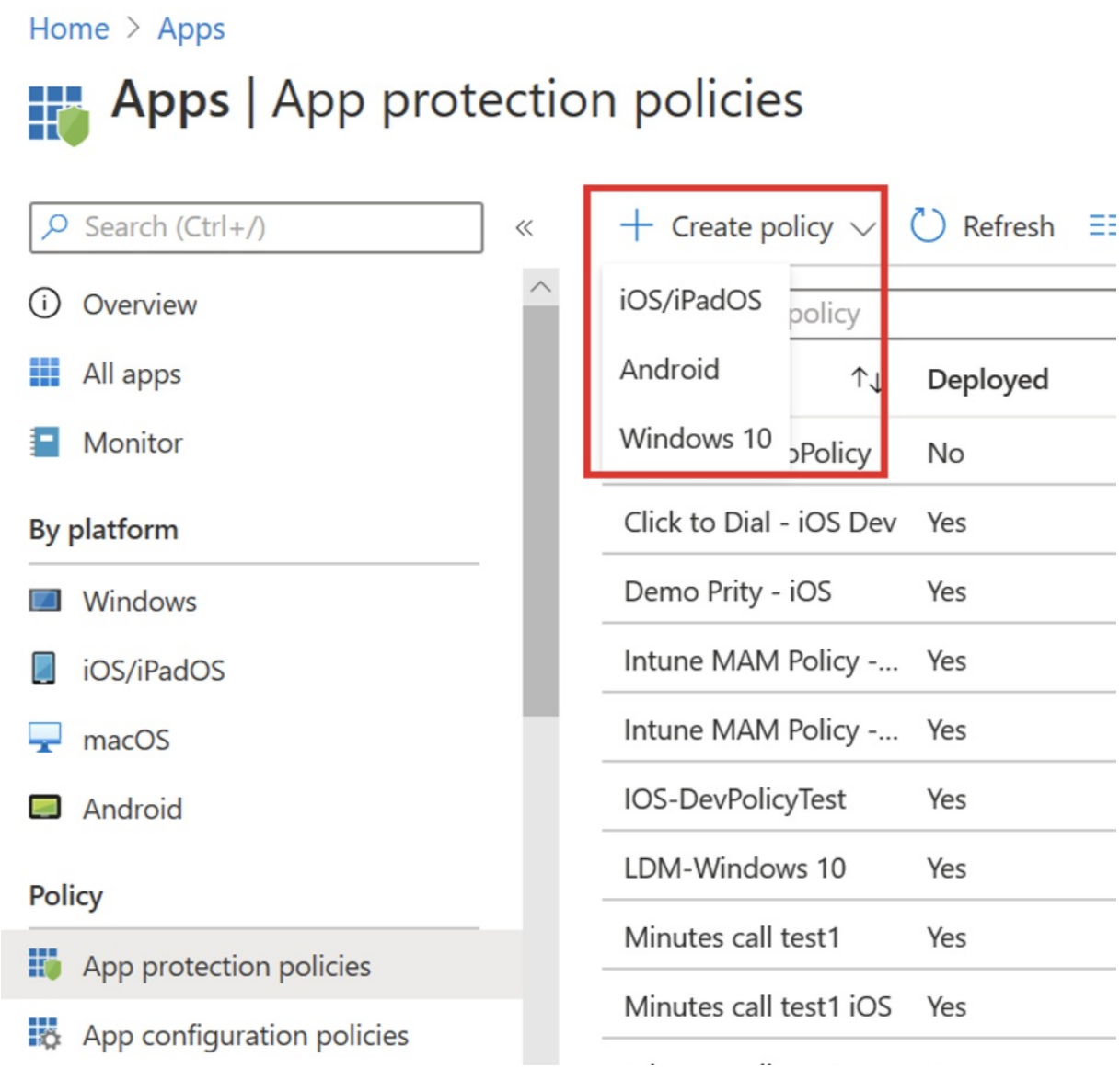
To complete deploying the app, you must create the app protection policy, add the MultiLine for Intune app to it, configure the policies, and then assign it to the user group.

1. Create new policy

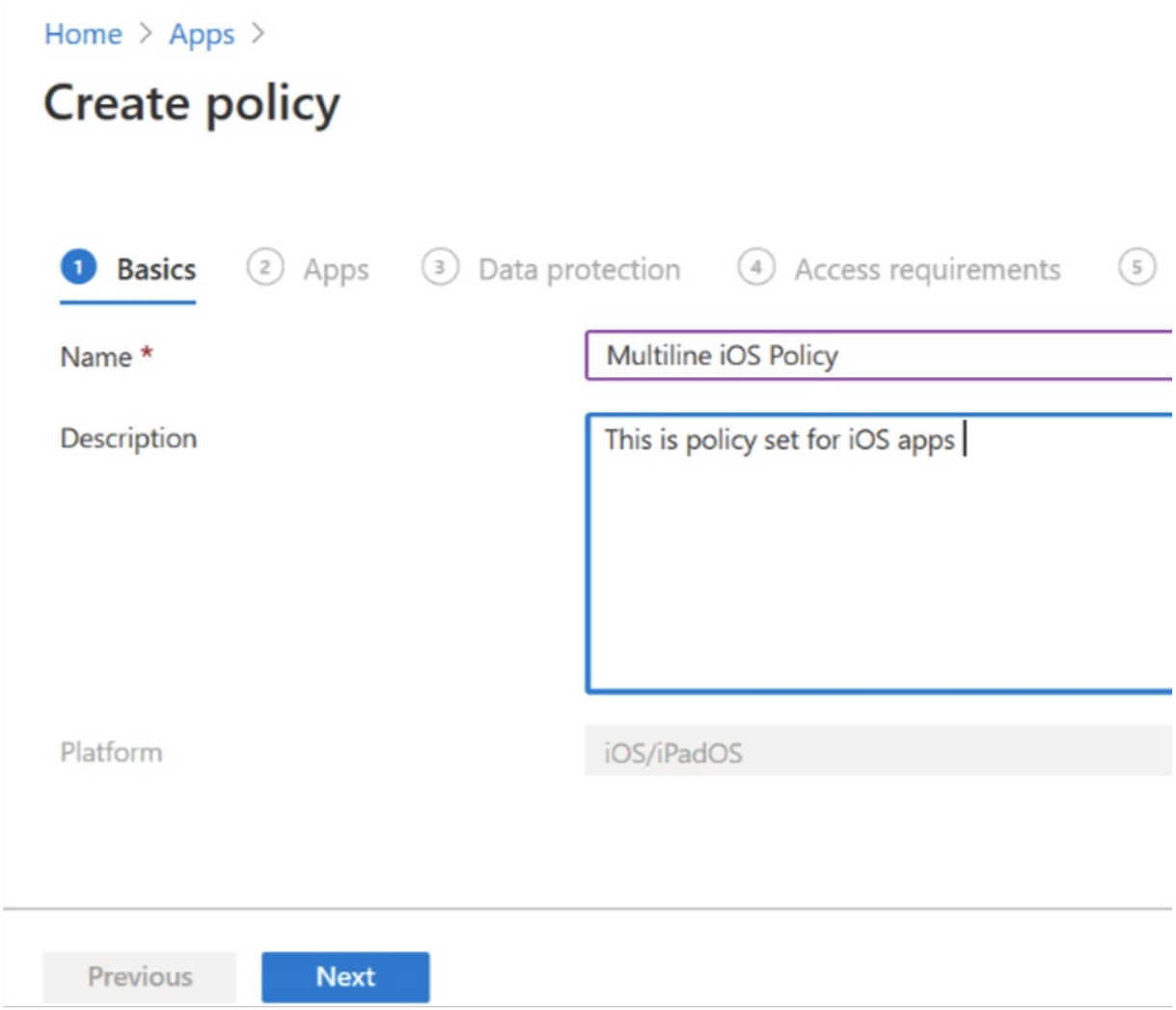
1. Go to **Home > Apps > App Protection Policies** and click **+Create Policy**.



2. Select **iOS/iPadOS** for IOS and **Android** for Android.

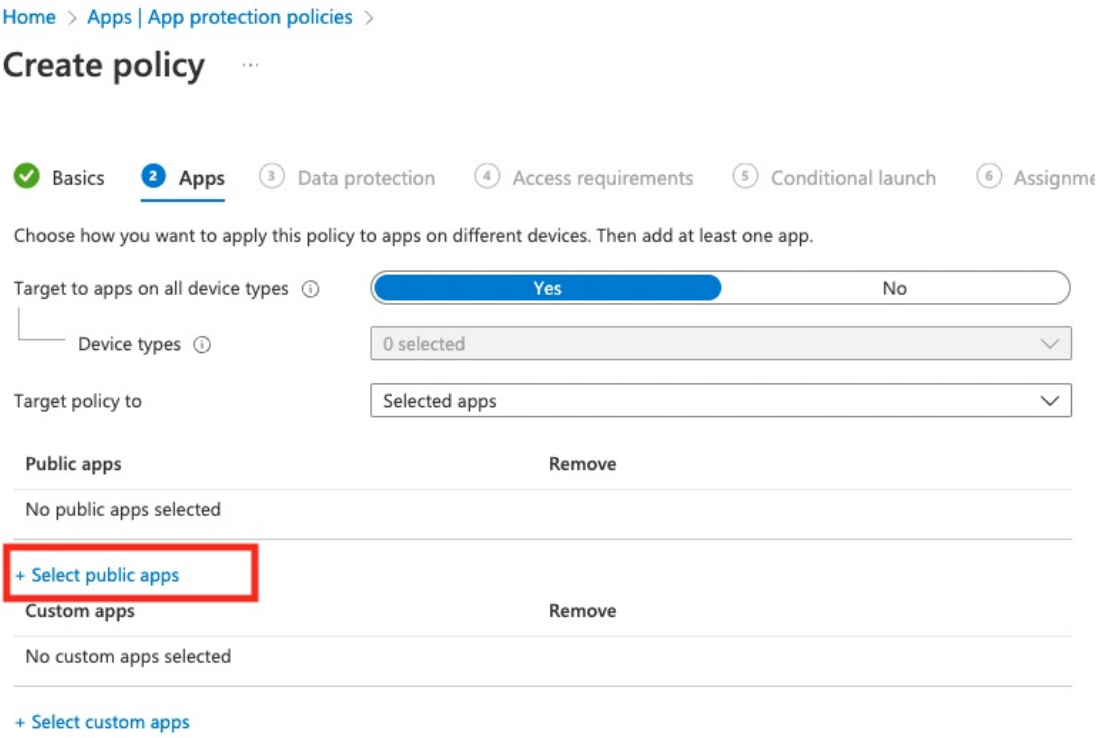


3. Give the policy a name and description.

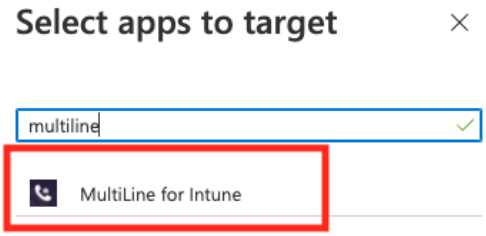


2. Add the MultiLine for Intune app to the policy set

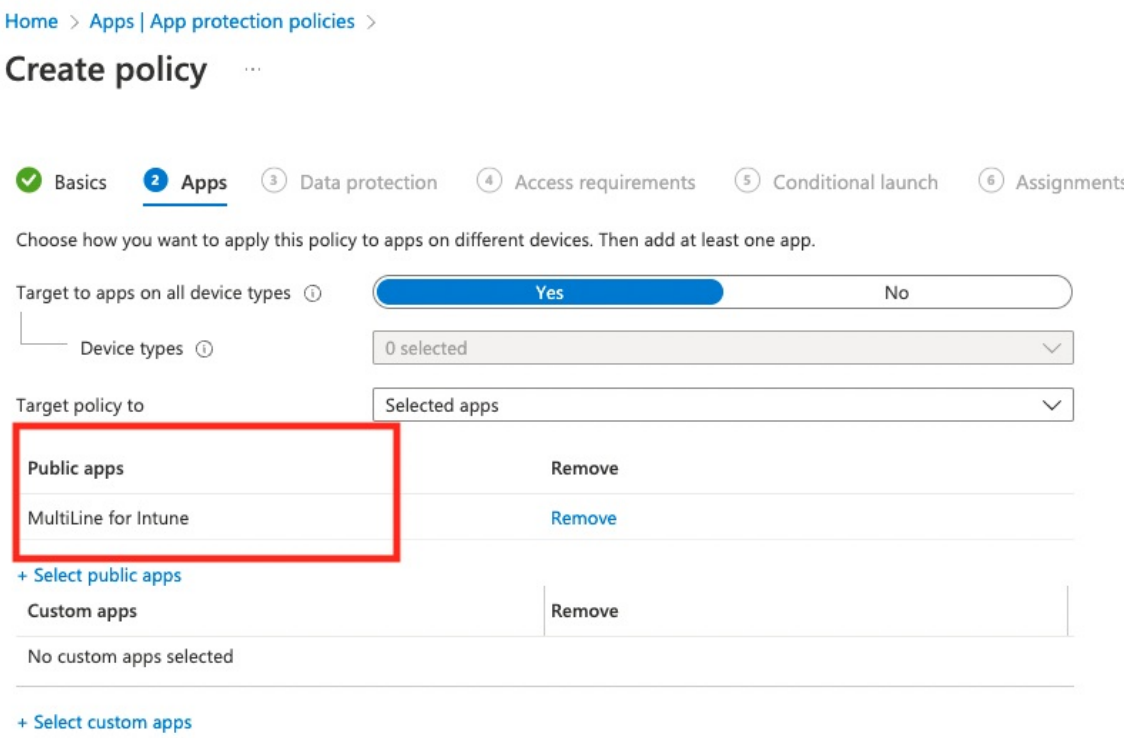
1. Click on **+Select public apps** to add MultiLine for Intune app in the policy set.



2. Search for MultiLine for Intune



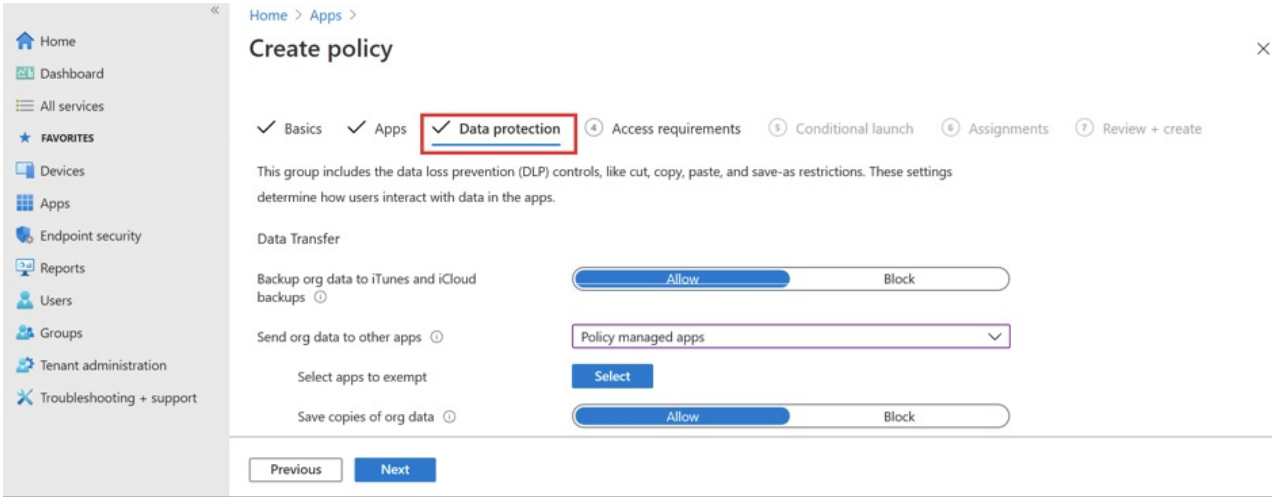
3. The selected MultiLine app should be listed under Public apps.



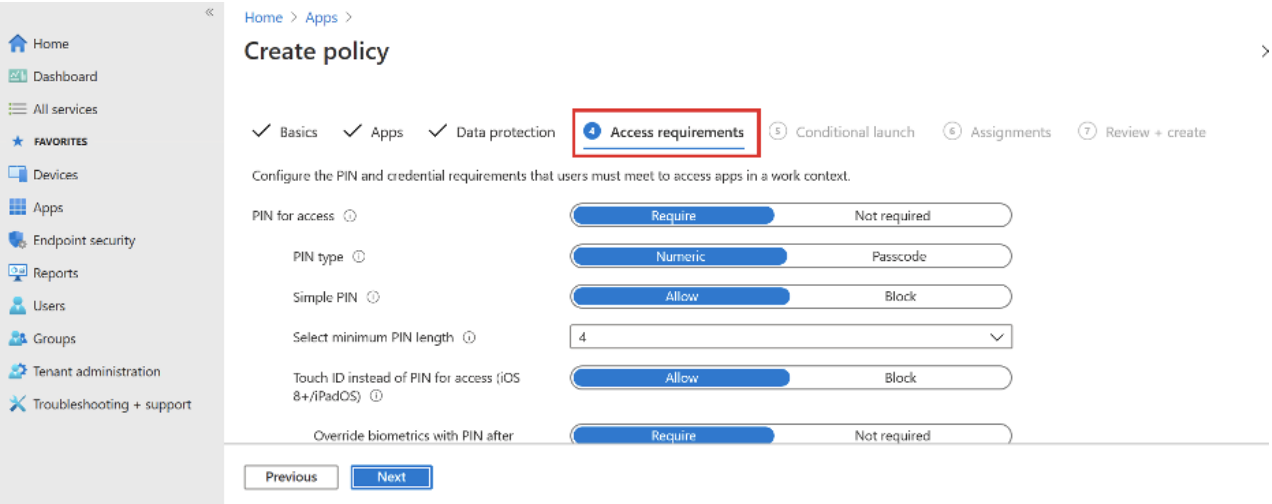
3. Configure protection policies

The next three screens are for setting application protection policies. There are specific policies you need to set for MultiLine for Intune described below. These policies must be configured separately for iOS and Android Apps.

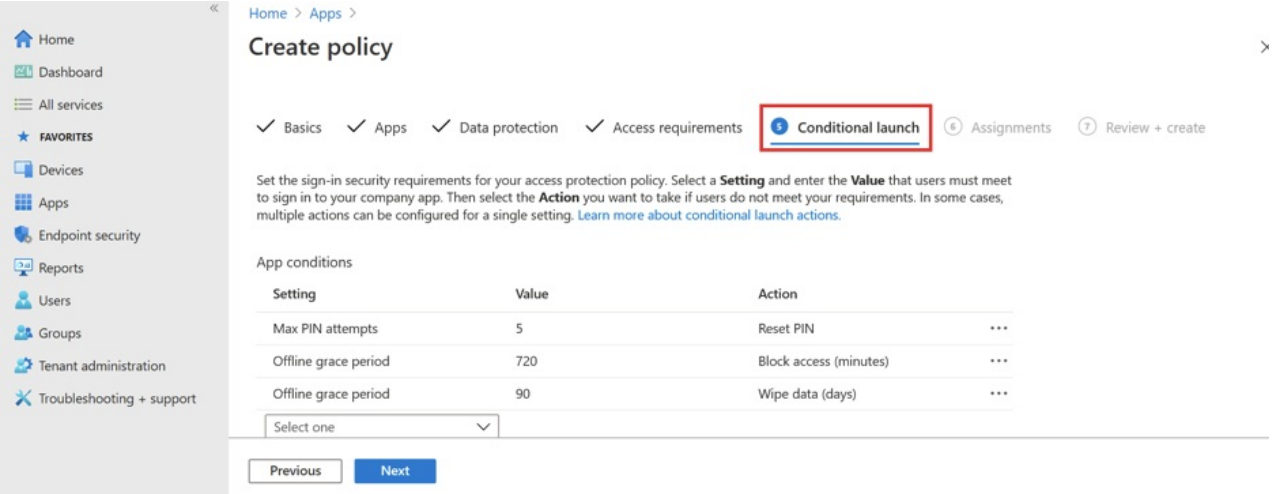
A. Configure the Data protection settings



B. Configure the Access requirements.



C. Configure the Conditional launch settings



Policies

Policies for iOS

Intune Policy Profile for iOS MultiLine for Intune App – A separate policy profile must be applied to the iOS MultiLine for Intune App. The following policies must be configured with the values shown below.

Policy Name	Value to be configured	Policy Description
Send org data to other apps	Policy managed apps with Open in/Share filtering	This policy controls the data exchange between two Apps
Select apps to exempt	Default	This policy is enabled only when the previous policy is configured to “Policy managed apps”. Please use the default value provided by Intune.

Transfer telecommunication data to	Any dialer app	This policy controls click-to-dial policy. For the MultiLine for Intune iOS App, this policy **MUST** be configured to **"Any dialer app".** This policy enables minutes calling mode of MultiLine for Intune *App Protection policies created before June 15, 2020 include **tel** and **telprompt** URL scheme as part of the **default data transfer exemptions** (**exemptedAppProtocols**). The App Protection policy setting **Transfer telecommunication data to** has replaced this functionality. Administrators should remove tel;telprompt; from the data transfer exemptions for the **Transfer telecommunication data to** App Protection policy setting to be honored.*
Dialer App URL Scheme	--	This policy is associated with the previous policy for Click-to-dial. For the MultiLine for Intune iOS App, this **MUST** be left blank.
Receive data from other Apps	Policy managed apps	This policy is also required to enable Click-to-dial. This is the prescribed configuration by Microsoft for the feature to work correctly.
Encrypt Org data	Require	This policy controls encryption of all data stored in the App. This policy **MUST** be configured to **"Require"** in order to enable Intune encryption.
Sync policy managed app data with native apps	Allow	This policy allows sharing of data with native Apps. This policy **MUST** be set to "Allow" to ensure that native contacts are accessible by the MultiLine for Intune iOS App.
Org data notification	Allow	This policy controls the App notifications. It **MUST** be set to "Allow" for the MultiLine for Intune App. Else, inbound data calls and inbound SMS messages will not work correctly.

MOVIUS

MultiLine for Intune App policies

The following policies affect the MultiLine for Intune App, but they can be configured to any option in the separate profile for the App. The MultiLine for Intune App will honor the configured policy. The remaining policies have no effect on the MultiLine App.

Policy Name	Value to be configured	Policy Description
Restrict cut, copy and paste between other apps	Any option can be configured	This policy controls the ability to cut, copy and paste between the MultiLine for Intune App and other Apps on the device. The MultiLine for Intune iOS App honors any of the possible configurations for this policy.
Third party Keyboard	Any option can be configured	This policy allows third party keyboards to be used within the App. The MultiLine for Intune iOS App honors any of the possible configurations for this policy.
Restrict web content transfer with other apps	Any option can be configured	This policy controls how web links in the MultiLine for Intune App (Ex: in SMS messages or MultiLine Help), are opened.
Unmanaged Browser Protocol	Any option can be configured	This policy also controls how web links in the MultiLine for Intune App (Ex: in SMS messages or MultiLine Help), are opened.

Other managed apps

Intune Policy Profile for other managed Apps – This is the profile applied to all other Intune managed Apps. There are specific policies that need to be configured so that interaction with MultiLine for Intune iOS App can happen successfully. Only these specific policies are identified below.

Policy Name	Value to be configured	Policy Description
Send org data to other apps	Policy managed apps with Open in/Share filtering	This policy controls the data exchange between two Apps

Select apps to exempt	Default	This policy is enabled only when the previous policy is configured to “Policy managed apps”. Please use the default value provided by Intune.
Transfer telecommunication data to	A specific dialer app	This policy controls click-to-dial policy. This policy MUST be configured to “A specific dialer app”. Else, clicking on a phone number in a managed App will not open MultiLine for Intune App. *App Protection policies created before June 15, 2020 include **tel** and **telprompt** URL scheme as part of the **default data transfer exemptions** (**exemptedAppProtocols**). The App Protection policy setting **Transfer telecommunication data to** has replaced this functionality. Administrators should remove tel;telprompt; from the data transfer exemptions for the **Transfer telecommunication data to** App Protection policy setting to be honored.*
Dialer App URL Scheme	x-msauth-moviusApp	This policy is associated with the previous policy for Click-to-dial. This **MUST** be configured as the provided string. This allows the managed App to securely open the MultiLine for Intune App.
Transfer messaging data to	A specific messaging app	This policy is associated with click to text for MultiLine for Intune, when a user clicks on a hyperlinked messaging link within any Microsoft-managed app, the MultiLine for Intune app will automatically open, with the phone number pre-filled and ready for sending messages.
Messaging App Package ID	x-msauth-moviusApp-SMS	This policy is associated with click to text for MultiLine for Intune, when a user clicks on a hyperlinked messaging link within any Microsoft-managed app, the MultiLine for Intune app will automatically open, with the phone number pre-filled and ready for sending messages.

Receive data from other Apps	All apps	This policy is also required to enable Click-to-dial. For the MultiLine for Intune iOS App, this MUST be set to “All apps”. This is the prescribed configuration by Microsoft.

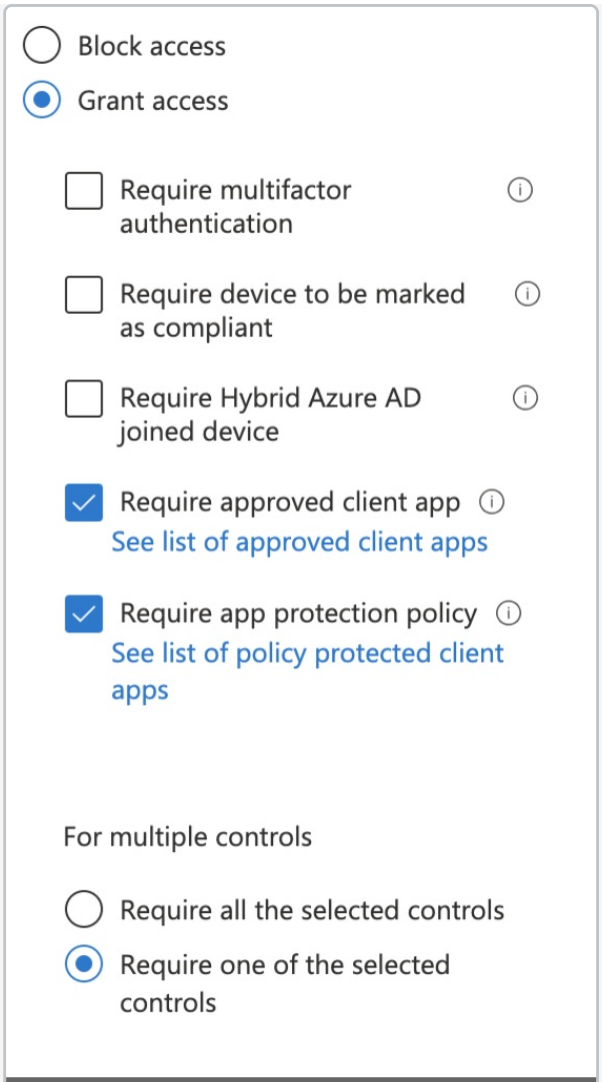
Conditional Access

If your organization uses Conditional Access, please note the following:

- MultiLine for Intune iOS and Android both support the *Required app protection policy* grant.
- MultiLine for Intune iOS supports the *Require approved client app* grant, but MultiLine for Intune Android does not.

Microsoft has stopped adding applications to the list of approved client apps and recommends app developers use the *Required app protection policy* grant for security reasons.

We recommend having a set of policies that apply specifically to the MultiLine application. You can configure a grant that requires either approved client app or app protection policy.



Screenshot: Grant configured to require either approved client apps or policy protected client apps.

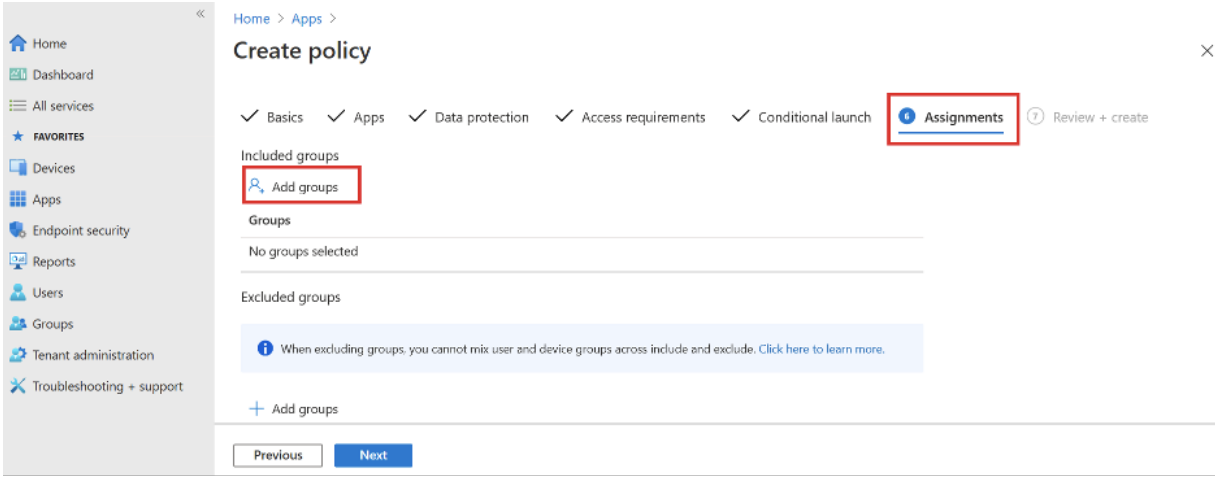
Alternatively, you can set up a policy for *Required approved client app* grant and a policy for *Required app protection policy* grant, and exclude the MultiLine for Intune Apps from the *Require approved client* app grant.

See [Azure AD Conditional Access Documentation](https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/) for more information.

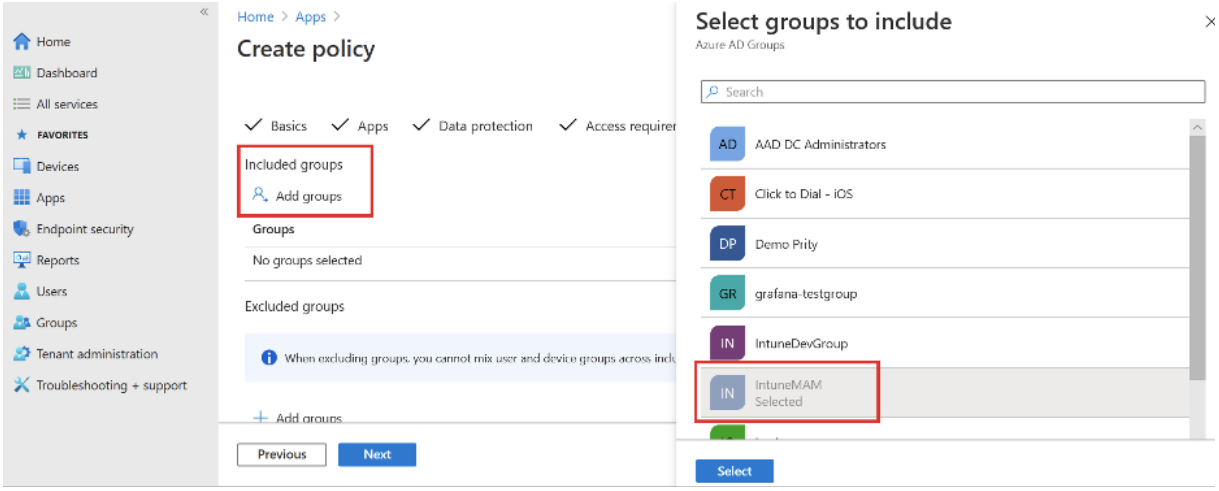
4. Assign to user groups

The sixth screen is for assigning the policy to the user group you made earlier.

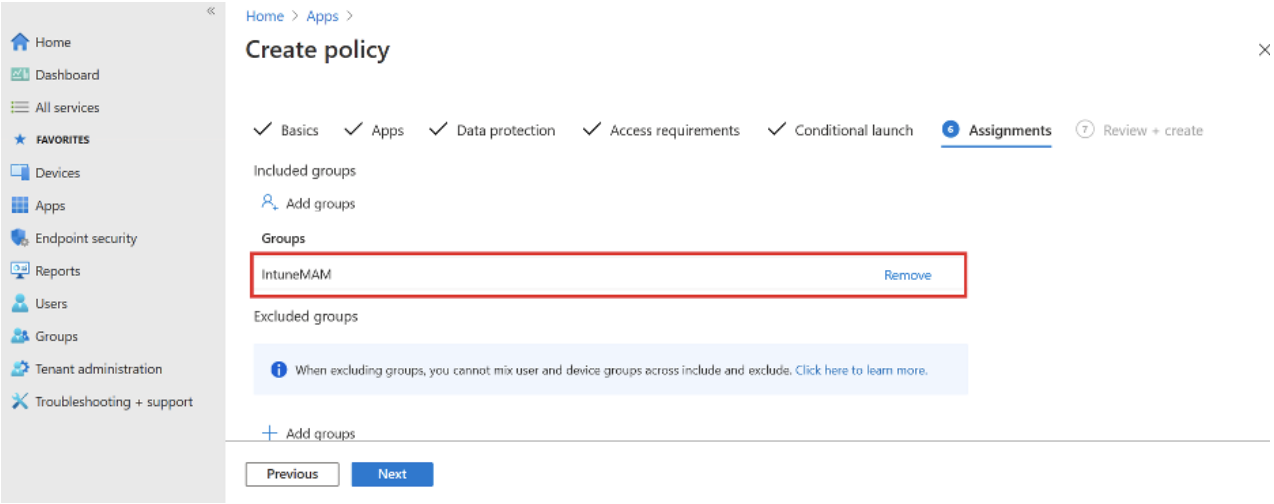
1. Click **Add Groups**.



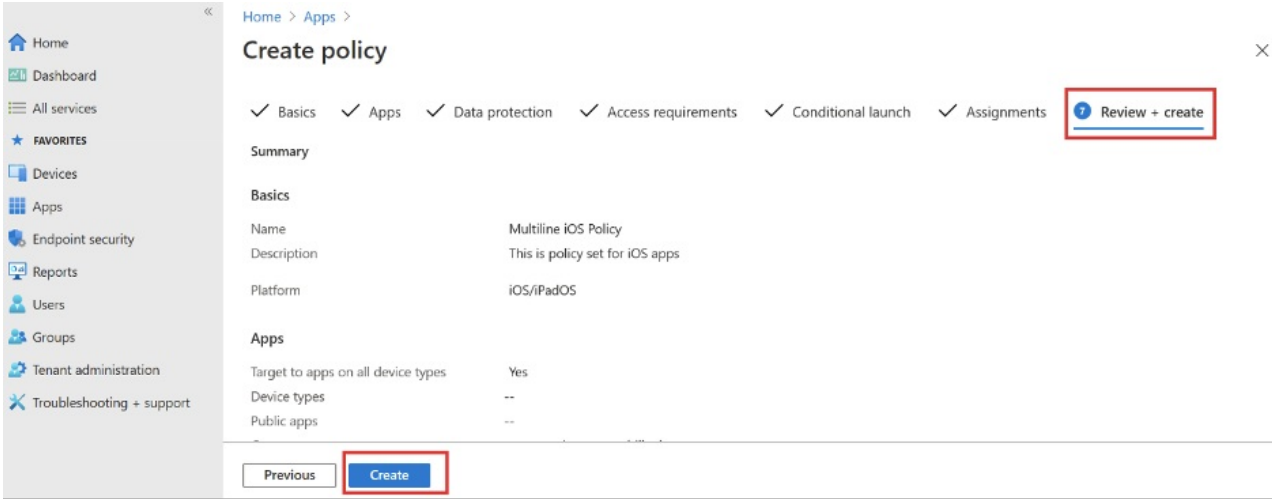
2. Select the group you created in Step 2 (in our example below, we called it "IntuneMAM")



3. You should see the group listed



4. Review what you've entered on all the tabs and click **Create**.



Step 4 - Grant MultiLine permission to access resources in your organization

An Azure AD Global Administrator needs to grant tenant-wide admin consent by registering a service principal for MultiLine for Intune. The admin consent URL needs to be built following this format:

For MultiLine for Intune iOS:

```
https://login.microsoftonline.com/{tenant-id}/adminconsent?client_id=d658ce6b-6fc6-4491-bb50-099c264f53f0
```

For MultiLine for Intune Android:

```
https://login.microsoftonline.com/{tenant-id}/adminconsent?client_id=85690b2e-8dce-40c6-95e3-2bb2495a1c2e
```

Where **{tenant-id}** is your organization's tenant ID in Azure AD.

The permission the application requires are listed in **Table-1**.

Table-1

API Name	Value	Description
Microsoft Graph	Contacts.ReadWrite	Allows the app to create, read, update, and delete user contacts.
	People.Read	Allows the app to read a scored list of people relevant to the signed-in user. The list can include local contacts, contacts from social networking or your organization's directory, and people from recent communications (such as email and Skype).

	User.Read	Allows users to sign-in to the app, and allows the app to read the profile of signed-in users. It also allows the app to read basic company information of signed-in users.

You're done!

To onboard MultiLine users, the MultiLine Administrator takes it from here by logging into the Admin portal.

Policies for Android

Intune Policy Profile for Android MultiLine for Intune App – A separate policy profile must be applied to the Android MultiLine for Intune App. The following policies must be configured with the values shown below.

Policy Name	Value to be configured	Policy Description
Send org data to other apps	Policy managed apps with Open in/Share filtering	This policy controls the data exchange between two Apps
Select apps to exempt	--	This policy is enabled only when the previous policy is configured to "Policy managed apps". Please use the default value provided by Intune.
Transfer telecommunication data to	Any dialer app	This policy controls click-to-dial policy. For the MultiLine for Intune Android App, this policy **MUST** be configured to **"Any dialer app".** This policy enables minutes calling mode of MultiLine for Intune. *App Protection policies created before June 15, 2020 include **tel** and **telprompt** URL scheme as part of the **default data transfer exemptions** (**exemptedAppProtocols**). The App Protection policy setting **Transfer telecommunication data to** has replaced this functionality. Administrators should remove tel;telprompt; from the data transfer exemptions for the **Transfer telecommunication data to** App Protection policy setting to be honored.*

Dialer App Package ID	--	This policy is associated with the previous policy for Click-to-dial. For the MultiLine for Intune Android App, this **MUST** be left blank.
Dialer App Name	--	This policy is associated with the previous policy for Click-to-dial. For the MultiLine for Intune Android App, this **MUST** be left blank.
Receive data from other Apps	Policy managed apps	This policy is also required to enable Click-to-dial. This is the prescribed configuration by Microsoft for the feature to work correctly.
Encrypt Org data	Require	This policy controls encryption of all data stored in the App. This policy **MUST** be configured to **"Require"** in order to enable Intune encryption.
Sync policy managed app data with native apps	Allow	This policy allows sharing of data with native Apps. This policy **MUST** be set to "Allow" to ensure that native contacts are accessible by the MultiLine for Intune Android App.
Org data notification	Allow	This policy controls the App notifications. It **MUST** be set to "Allow" for the MultiLine for Intune App. Else, inbound data calls and inbound SMS messages will not work correctly.

MultiLine for Intune App Policies

The following policies affect the MultiLine for Intune App, but they can be configured to any option in the separate profile for the App. The MultiLine for Intune App will honor the configured policy. The remaining policies have no effect on the MultiLine App.

Policy Name	Value to be configured	Policy Description
Restrict cut, copy and paste between other apps	Any option can be configured	This policy controls the ability to cut, copy and paste between the MultiLine for Intune App and other Apps on the device. The MultiLine for Intune Android App honors any of the possible configurations for this policy.

Third party Keyboard	Any option can be configured	This policy allows third party keyboards to be used within the App. The MultiLine for Intune Android App honors any of the possible configurations for this policy.
Restrict web content transfer with other apps	Any option can be configured	This policy controls how web links in the MultiLine for Intune App (Ex: in SMS messages or MultiLine Help), are opened.
Unmanaged Browser Protocol	Any option can be configured	This policy also controls how web links in the MultiLine for Intune App (Ex: in SMS messages or MultiLine Help), are opened.

Other Managed Apps

Intune Policy Profile for other managed Apps – This is the profile applied to all other Intune managed Apps. There are specific policies that need to be configured so that interaction with MultiLine for Intune Android App can happen successfully. Only these specific policies are identified below.

Policy Name	Value to be configured	Policy Description
Send org data to other apps	Policy managed apps with Open in/Share filtering	This policy controls the data exchange between two Apps
Select apps to exempt	-	This policy is enabled only when the previous policy is configured to “Policy managed apps”. Please use the default value provided by Intune.

Transfer telecommunication data to	A specific dialer app	This policy controls click-to-dial policy. This policy **MUST** be configured to "A specific dialer app". Else, clicking on a phone number in a managed App will not open MultiLine for Intune App. *App Protection policies created before June 15, 2020 include **tel** and **telprompt** URL scheme as part of the **default data transfer exemptions** (**exemptedAppProtocols**). The App Protection policy setting **Transfer telecommunication data to** has replaced this functionality. Administrators should remove tel;telprompt; from the data transfer exemptions for the **Transfer telecommunication data to** App Protection policy setting to be honored.*
Dialer App Package ID	com.moviuscorp.multilineforintune	This policy is associated with the previous policy for Click-to-dial. This **MUST** be configured as the provided string. This allows the managed App to securely open the MultiLine for Intune App.
Dialer App Name	MultiLine for Intune	This policy is associated with the previous policy for Click-to-dial. This **MUST** be configured as the provided string. This allows the managed App to securely open the MultiLine for Intune App.
Transfer messaging data to	A specific messaging app	This policy is associated with click to text for MultiLine for Intune, when a user clicks on a hyperlinked messaging link within any Microsoft-managed app, the MultiLine for Intune app will automatically open, with the phone number pre-filled and ready for sending messages.
Messaging App Package ID	com.moviuscorp.multilineforintune	This policy is associated with click to text for MultiLine for Intune, when a user clicks on a hyperlinked messaging link within any Microsoft-managed app, the MultiLine for Intune app will automatically open, with the phone number pre-filled and ready for sending messages.

Messaging App Name	MultiLine for Intune	This policy is associated with click to text for MultiLine for Intune, when a user clicks on a hyperlinked messaging link within any Microsoft-managed app, the MultiLine for Intune app will automatically open, with the phone number pre-filled and ready for sending messages.
Receive data from other Apps	Policy managed Apps	This policy is also required to enable Click-to-dial. For the MultiLine for Intune Android App, this MUST be set to “All apps”. This is the prescribed configuration by Microsoft.

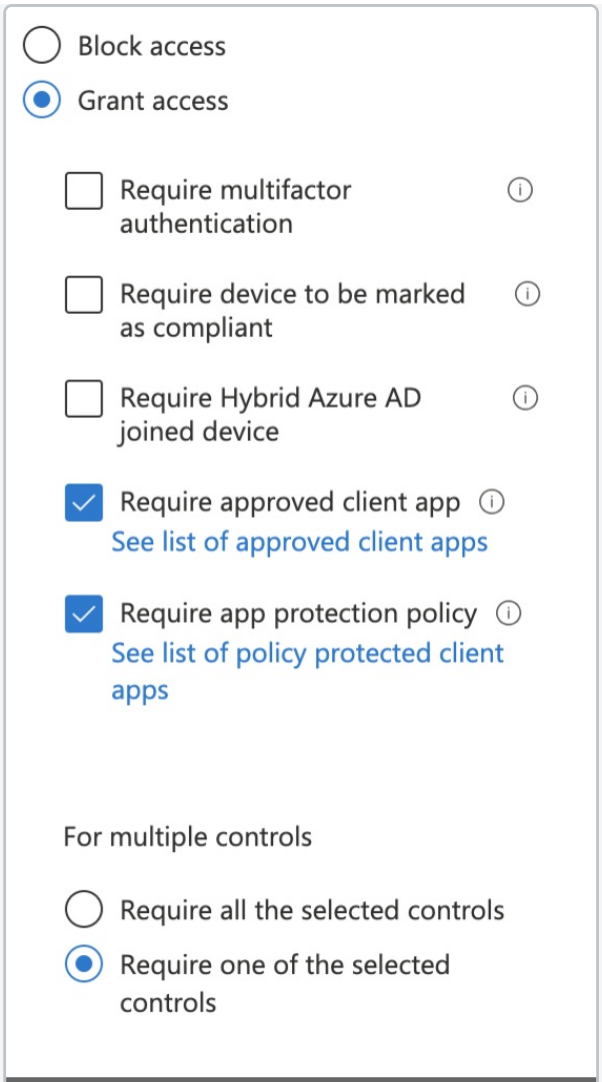
Conditional Access

If your organization uses Conditional Access, please note the following:

- MultiLine for Intune iOS and Android both support the *Required app protection policy* grant.
- MultiLine for Intune iOS supports the *Require approved client app* grant, but MultiLine for Intune Android does not.

Microsoft has stopped adding applications to the list of approved client apps and recommends app developers use the *Required app protection policy* grant for security reasons.

We recommend having a set of policies that apply specifically to the MultiLine application. You can configure a grant that requires either approved client app or app protection policy.



Screenshot: Grant configured to require either approved client apps or policy protected client apps.

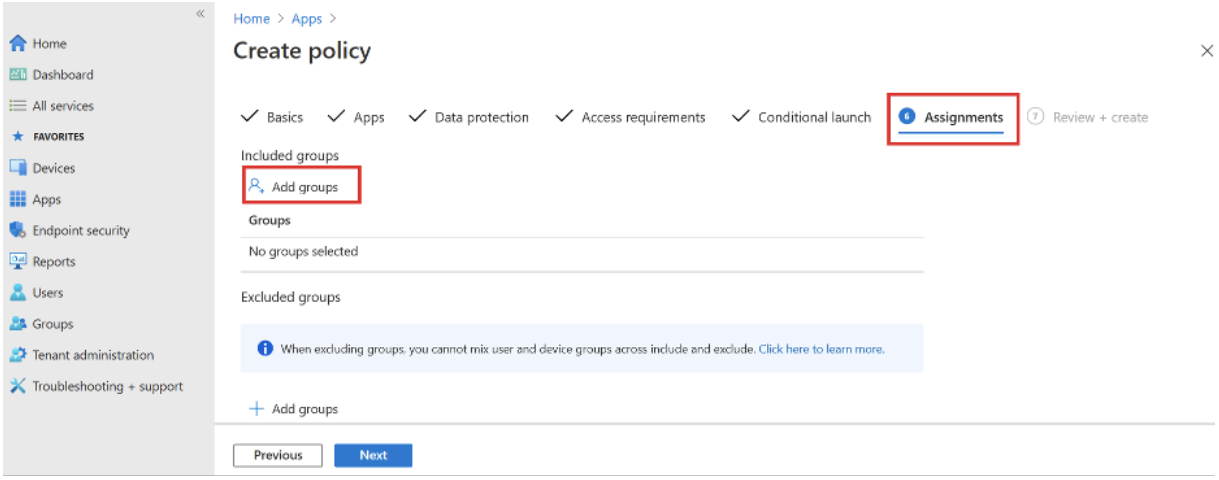
Alternatively, you can set up a policy for *Required approved client app* grant and a policy for *Required app protection policy* grant, and exclude the MultiLine for Intune Apps from the *Require approved client* app grant.

See [Azure AD Conditional Access Documentation](https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/) for more information.

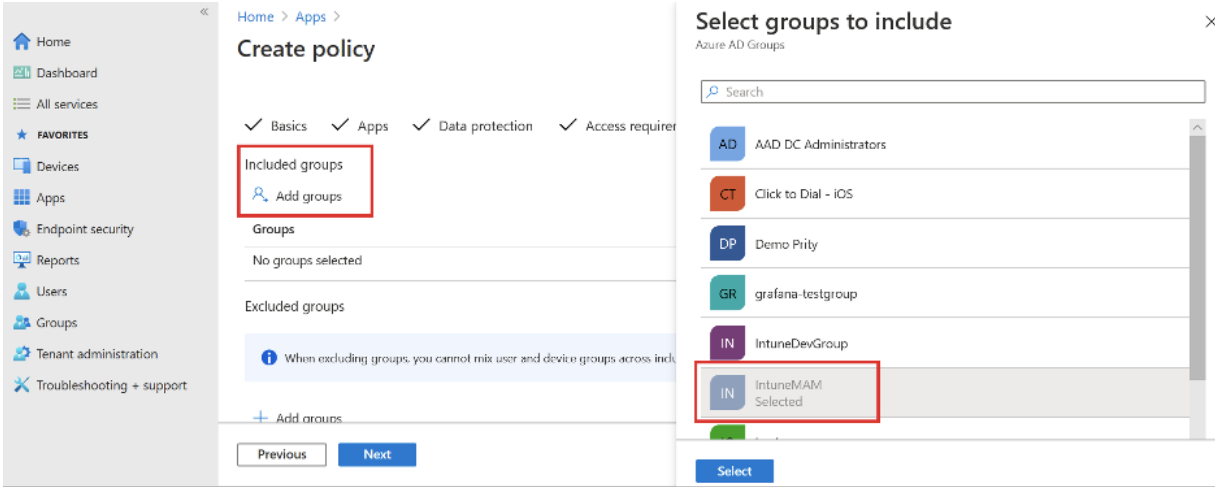
4. Assign to user groups

The sixth screen is for assigning the policy to the user group you made earlier.

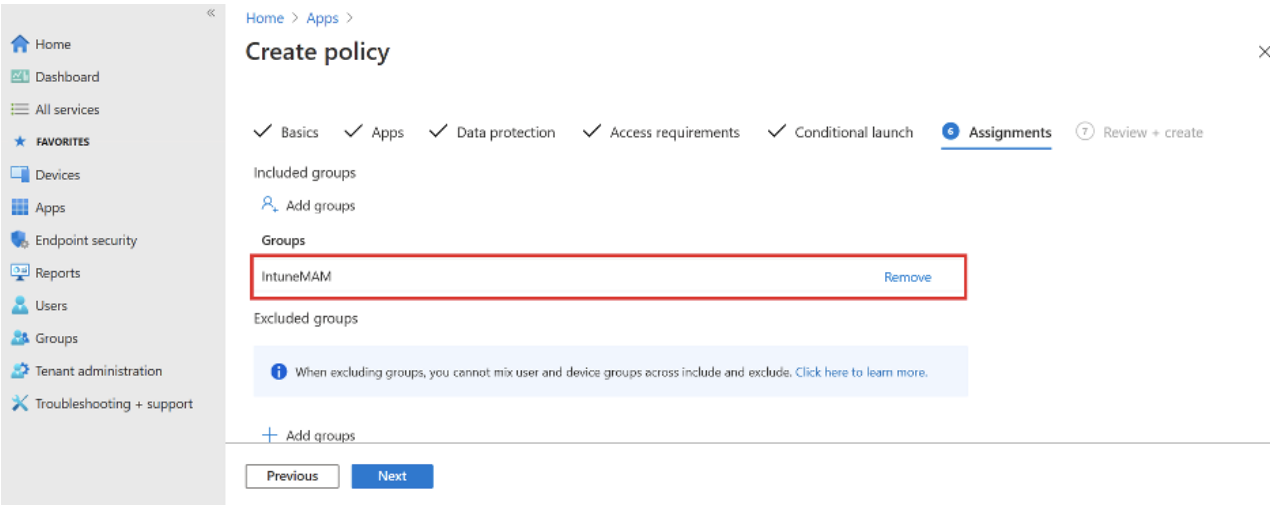
1. Click **Add Groups**.



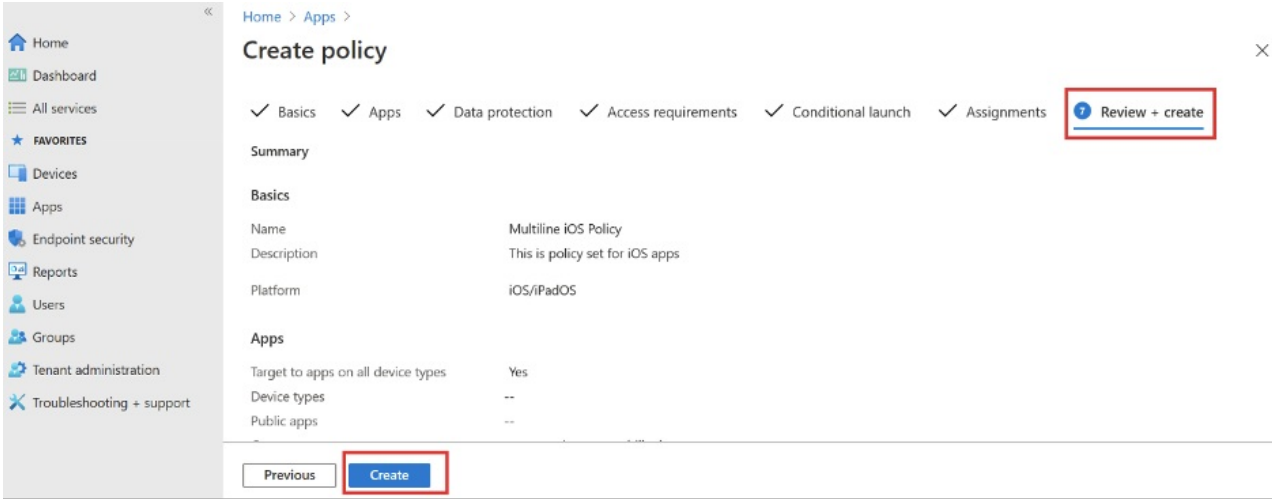
2. Select the group you created in Step 2 (in our example below, we called it "IntuneMAM")



3. You should see the group listed



4. Review what you've entered on all the tabs and click **Create**.



Step 4 - Grant MultiLine permission to access resources in your organization

An Azure AD Global Administrator needs to grant tenant-wide admin consent by registering a service principal for MultiLine for Intune. The admin consent URL needs to be built following this format:

For MultiLine for Intune iOS:

```
https://login.microsoftonline.com/{tenant-id}/adminconsent?client_id=d658ce6b-6fc6-4491-bb50-099c264f53f0
```

For MultiLine for Intune Android:

```
https://login.microsoftonline.com/{tenant-id}/adminconsent?client_id=85690b2e-8dce-40c6-95e3-2bb2495a1c2e
```

Where **{tenant-id}** is your organization's tenant ID in Azure AD.

The permission the application requires are listed in **Table-1**.

Table-1

API Name	Value	Description
Microsoft Graph	Contacts.ReadWrite	Allows the app to create, read, update, and delete user contacts.
	People.Read	Allows the app to read a scored list of people relevant to the signed-in user. The list can include local contacts, contacts from social networking or your organization's directory, and people from recent communications (such as email and Skype).

	User.Read	Allows users to sign-in to the app, and allows the app to read the profile of signed-in users. It also allows the app to read basic company information of signed-in users.
Microsoft Mobile Application Management	DeviceManagementManagedApps.ReadWrite	Allows the Application to read and write the user's data pertaining to itself in the Intune Mobile Application Management service.

You're done!

To onboard MultiLine users, the MultiLine Administrator takes it from here by logging into the Admin portal.