

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. See<u>Microsoft Intune's</u> documentation [External] [2] (https://learn.microsoft.com/en-us/microsoft-365/business/ui/mam-and-mdm?view=o365-worldwide) [2] 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
- 2. In the left menu, select Apps



1 Home	
Z Dashboard	
E All services	
★ FAVORITES	
Devices	
Apps	
🛼 Endpoint security	
Reports	
📩 Users	
Sroups	
Tenant administration	
X Troubleshooting + support	

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

A Home	Apps Overview
Dashboard	0
E All services	
★ FAVORITES	(i) Overview
Devices	All apps
Apps	Monitor
Endpoint security	By platform
Reports	Windows
L Users	iOS/iPadOS
🐣 Groups	🖵 macOS
Tenant administration	Android
X Troubleshooting + support	
	Policy

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



	nome / mpps		
A Home	Apps All apps		
Z Dashboard			
E All services	✓ Search (Cmd+/) «	+ Add 💍 Refresh 🖓 Filter	
★ FAVORITES	(i) Overview	Search by name or publisher	
Devices	All apps	Name 1	Туре
Apps	Monitor		Managed Canada Discotory
Endpoint security		Adobe Acrobat Reader: PDF Viewer,	Managed Google Play store
Panaets	By platform	Intune Company Portal	Managed Google Play store
Reports	Windows	Mail	iOS store app
Lusers	iOS/iPadOS	Managed Home Screen	Managed Google Play store
🔉 Groups	_		inanagea eeegie naj store
Tonant administration	wacOS	Microsoft Authenticator	Managed Google Play store
	Android	Microsoft Intune	Managed Google Play store
Iroubleshooting + support	Delieu	Microsoft Outlook	iOS store app

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

рр туре	
Select app type	/
Store app	
Android store app	
iOS store app	
Microsoft store ann	
Managed Google Play app	
Microsoft 365 Apps	
Windows 10	
macOS	
Microsoft Edge, version 77 and later	
Windows 10	
2026	
Microsoft Defender ATP	
macOS	
Other	
Web link	
Built-In app	

6. Click the Search the App Store link



Add App		
1 App information	Assignments	③ Review + create
Select app * (i)	Sear	rch the App Store

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

iOS store app			intun		×	United States (default)	\sim
 App information 	Assignments		Name	\uparrow_{\downarrow}	Publisher		\uparrow_{\downarrow}
Select app * ①	Search	٩	MultiLine for Intune		Movius Interactive Corporat	tion	

- 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
 - For Android, select Android 4.0 (Ice Cream Sandwich) for minimum operating system Add App iOS store app

Select app * 🕕	Search the App Store
Name * 🕕	MultiLine for Intune
Description * ①	MultiLine for Intune is a cloud-based service that enables individuals and global businesses to achieve regulatory compliance for their mobile business
Publisher * 🕕	Movius Interactive Corporation
Appstore URL	https://apps.apple.com/us/app/multiline-for-intune/id1484594063?uo=4
Minimum operating system * 🕕	iOS 8.0
Applicable device type * 🕕	2 selected
Category ①	0 selected
Show this as a featured app in the Company Portal ①	Yes No
Information URL ①	Enter a valid url
Privacy URL ①	Enter a valid url
Developer ①	

9. Assign the App to your groups and click next



Add App iOS store app			
\checkmark App information	Assignments 3 Review +	create	
Required ①			
Group mode	Group	VPN	Uninstall on device removal
No assignments			
+ Add group 🛈 + Add a	all users ① + Add all devices ①		
Available for enrol	lled devices ①		
Group mode	Group	VPN	Uninstall on device removal
No assignments			
+ Add group 🛈 + Add a	all users ①		
Available with or v	without enrollment 🛈		
Group mode	Group		Uninstall on device removal
No assignments			
+ Add group ① + Add a	ill users ①		
Previous Ne	xt		

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

Add App iOS store app

Summary	
App information	
Name	MultiLine for Intune
Description	MultiLine for Intune is a cloud-based service that enables individuals and global businesses to achieve regulatory compliance for their mobile business communications. The solution gives employees a distinct mobile number for their business calls, text messaging and voicemail while maintaining privacy of their personal phone number. It works over any global carrier network and can be deployed glob
Publisher	Movius Interactive Corporation
Appstore URL	https://apps.apple.com/us/app/multiline-for-intune/id1484594063?uo=4
Minimum operating system	iOS 8.0
Applicable device type	iPad iPhone and iPod
Category	
Show this as a featured app in the Company Portal	No
Information URL	**
Privacy URL	
Developer	
Owner	
Notes	

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



Search (Cmd+/) «	+ Add 🕐 Refresh 🍸	Filter 🞍 Export 🗮 Columns
) Overview	Filters applied: Platform, App t	ype
All apps	₽ Intune	
Monitor	Name	↑↓ Туре
y platform	MultiLine for Intune	iOS store app
Windows		
iOS/iPadOS		
macOS		

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. <u>Create a user group [External Link]</u> (<u>https://docs.microsoft.com/en-us/mem/intune/fundamentals/groups-add</u>) [2] for MultiLine for Intune users, or edit the group according to the details below:

.	MultiLine fo	r Intune users	s need to	be in a	a Security user	group. T	his is i	required
---	--------------	----------------	-----------	---------	------------------------	----------	----------	----------

Home > Groups >		
New Group		
Sroup type * ①	1	
Security		\sim
Group name * 🕕	3	
Enter the name of the gr	roup	
Group description 🕕		
Enter a description for th	ne group	
Azure AD roles can be assi	ianed to the group (Preview)	
Azure AD roles can be assi	igned to the group (Preview) ①	
Azure AD roles can be assi Yes No Membership type * ①	igned to the group (Preview) ()	

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.

roup de	scription ()	
Enter a	description for the group	
zure AD	roles can be assigned to the group (Preview)	
Yes	No	
lembers	hip type * ①	
Assigne	d	
Assigne	1	
Dynami	User	
Dynami	2 Device	
	1	

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.

*	Home > Apps									
1 Home	👥 Apps App prote	Apps App protection policies ×								
🖾 Dashboard										
E All services		~	$+$ Create policy \smallsetminus	🕐 Refresh	≣≣ Colu	mns 🞍 Export				
★ FAVORITES	(i) Overview	^								
Devices	All apps		Policy ↑↓	Deployed	↑↓	Updated 🐴	Platform	\uparrow_{\downarrow}	Management ty $\uparrow\downarrow$	Арр
Apps	Monitor		AndroidDemoPolicy	No		3/24/20, 5:20 PM	Android		Apps on Intune man	2
Endpoint security	By platform		Click to Dial - iOS De	/ Yes		1/23/21, 12:11 AM	iOS/iPadOS		All app types	5
Reports	Windows		Demo Prity - iOS	Yes		12/08/20, 12:03 PM	iOS/iPadOS		All app types	5
Lusers	iOS/iPadOS		Intune MAM Policy	. Yes		2/09/21, 11:26 AM	Android		Apps on unmanaged	7
Groups	🖵 macOS	1	Intune MAM Policy	. Yes		2/04/21, 4:03 PM	iOS/iPadOS		Apps on unmanaged	6
Tenant administration	Android		IOS-DevPolicyTest	Yes		1/15/21, 12:45 AM	iOS/iPadOS		All app types	5
X Troubleshooting + support	Policy		LDM-Windows 10	Yes		5/05/20, 1:21 PM	Windows 10		Without enrollment	
	App protection policies		Minutes call test1	Yes		2/04/21, 5:17 PM	Android		All app types	3
	App configuration policies		Minutes call test1 iOS	Yes		2/04/21, 5:15 PM	iOS/iPadOS		All app types	4
		\sim	Minutes call test2	Yes		2/04/21, 5:17 PM	Android		All app types	1

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



Home > Apps

Apps | App protection policies

✓ Search (Ctrl+/) «	$+$ Create policy \smallsetminus	C Refresh ■
(i) Overview	iOS/iPadOS policy	
All apps	Android ↑J	Deployed
Monitor	Windows 10 Policy	No
By platform	Click to Dial - iOS Dev	Yes
Windows	Demo Prity - iOS	Yes
iOS/iPadOS	Intune MAM Policy	. Yes
🚽 macOS	Intune MAM Policy	. Yes
Android	IOS-DevPolicyTest	Yes
Policy	LDM-Windows 10	Yes
App protection policies	Minutes call test1	Yes
App configuration policies	Minutes call test1 iOS	Yes
The soundard on bounder	······································	

3. Give the policy a name and description.



Home > Apps >	
Create policy	У
1 Basics 2 A	pps ③ Data protection ④ Access requirements ⑤
Name *	Multiline iOS Policy
Description	This is policy set for iOS apps
Platform	iOS/iPadOS
Previous	Next

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.

M	MOVIUS
---	--------

Sasics 2 Apps 3 Data	protection	(4) Access requirements	5 Conditional launch	6 Assign
Choose how you want to apply this polic	y to apps on di	fferent devices. Then add at le	ast one app.	
Target to apps on all device types i		Yes	No	
Device types ③	0 selected			\sim
Target policy to	Selected a	pps		\sim
Public apps		Remove		
No public apps selected				
+ Select public apps				
Custom apps		Remove		
No custom apps selected				

2. Search for MultiLine for Intune

Select	apps	to ta	rget	\times
--------	------	-------	------	----------



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



Home > Apps | App protection policies >

Create policy				
💙 Basics 🛛 Apps 🕔 Data p	protection ④ Acces	s requirements 5 Cond	itional launch	6 Assignmen
Choose how you want to apply this policy	to apps on different devi	ces. Then add at least one app.		
Target to apps on all device types ①	Yes		No	
Device types (i)	0 selected			\sim
Target policy to	Selected apps			\sim
Public apps	R	emove		
MultiLine for Intune	R	emove		
+ Select public apps Custom apps	R	emove		
No custom apps selected				

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

~	Home > Apps >	
A Home	Create policy	×
Z Dashboard		
E All services		
* FAVORITES	Basics Apps Data protection Access requirements Conditional launch Assignments Review + create	
Devices	This group includes the data loss prevention (DLP) controls, like cut, copy, paste, and save-as restrictions. These settings	
Apps	determine how users interact with data in the apps.	
Endpoint security	Data Transfer	
Reports	Backup oro data to iTunes and iCloud Allow Block	
🚨 Users	backups O	
24 Groups	Send org data to other apps ① Policy managed apps V	
Tenant administration	Select apps to exempt Select	
X Troubleshooting + support		
	Save copies of org data	
	Previous Next	

B. Configure the Access requirements.



»	Home > Apps >	
A Home	Create policy	>
Dashboard		
⊟ All services		
* FAVORITES	✓ Basics ✓ Apps ✓ Data protection	
Devices	Configure the PIN and credential requirements that users must meet to access apps in a work context.	
Apps	PIN for access ① Require Not required	
🌏 Endpoint security		
😭 Reports	Pile type (
🚨 Users	Simple PIN () Allow Black	
🎿 Groups	Select minimum PIN length 🛈 4	
Tenant administration	Touch ID instead of PIN for access (iOS Allow Block	
🔀 Troubleshooting + support	8+/iPadOS) ①	
	Override biometrics with PIN after Require Not require	
	Previous Next	

C. Configure the Conditional launch settings

«	Home > Apps >							
A Home	Create policy					>		
Z Dashboard								
E All services								
* FAVORITES	✓ Basics ✓ Apps ✓ Data	protection 🗸 Access requirements	s S Conditional launch	Assignments	⑦ Review + create			
Devices	Set the sign-in security requirements for	your access protection policy. Select a Set	ting and enter the Value that users	must meet				
Apps	to sign in to your company app. Then sel multiple actions can be configured for a	to sign in to your company app. Then select the Action you want to take if users do not meet your requirements. In some cases, multiple actions can be configured for a single acting law more about configured law do actions.						
Endpoint security	maniple decisits can be comigated for a	ingle second, control about contation						
Reports	App conditions							
🚨 Users	Setting	Value	Action					
🎎 Groups	Max PIN attempts	5	Reset PIN					
Tenant administration	Offline grace period	720	Block access (minutes)					
💥 Troubleshooting + support	Offline grace period	90	Wipe data (days)					
	Select one]						
	Previous Next							

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 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.



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	Policy managed apps with	This policy controls the data exchange between
apps	Open in/Share filtering	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.



configuration by Microsoft.	Apps All apps This policy is also required to enable click-to- Apps dial. For the MultiLine for Intune iOS App, this MUST be set to "All apps". This is the prescribed
-----------------------------	--

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.



Block access		
• Grant access		
Require multifactor authentication	Ĵ	
Require device to be marked as compliant	(i)	
Require Hybrid Azure AD joined device	(i)	
Require approved client app (i) See list of approved client apps		
Require app protection policy (See list of policy protected client apps)	
For multiple controls		
Require all the selected controls		
 Require one of the selected controls 		
Screenshot: Grant configured to require either ap client apps or policy protected client apps.	proved	

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 <u>Azure AD Conditional Access Documentation</u> (<u>https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/)</u> of 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.



~	Home > Apps >	
A Home	Create policy	×
📶 Dashboard		
E All services	Resirs Anns Data protection Access requirements Conditional launch Assignments Review + create	
★ FAVORITES		
Devices	Included groups	
Apps	8, Add groups	
ᠲ Endpoint security	Groups	
Reports	No groups selected	
🚨 Users	Excluded groups	
🚑 Groups		
Tenant administration	() When excluding groups, you cannot mix user and device groups across include and exclude. Click here to learn more.	
💥 Troubleshooting + support		
	+ Add groups	
	Previous Next	

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

~	Home > Apps >	Select groups to include
A Home	Create policy	Azure AD Groups
📶 Dashboard		
E All services		₽ Search
★ FAVORITES	✓ Basics ✓ Apps ✓ Data protection ✓ Access requirer	AD AAD DC Administrators
Devices	Included groups	
Apps	Add groups	CT Click to Dial - iOS
🌏 Endpoint security	Groups	D. Dura Dite
Reports	No groups selected	DP Demo Pitty
🚨 Users	Excluded groups	GR grafana-testgroup
🎥 Groups		and the second s
Tenant administration	() When excluding groups, you cannot mix user and device groups across indu	IN IntuneDevGroup
🗙 Troubleshooting + support		IN IntuneMAM Selected
	+ Add aroups	
	Previous Next	Select

3. You should see the group listed

»	Home > Apps >	
A Home	Create policy	×
🖾 Dashboard		
⊟ All services		
* FAVORITES	V Basics V Apps V Data protection V Access requirements V Conditional launch 3 Assignments 7 Review + create	
Devices	Included groups	
Аррз	A Add groups	
🔍 Endpoint security	Groups	
Reports	IntuneMAM Remove	
🚨 Users	Excluded arouns	
🎎 Groups	munand Grada	
Tenant administration	() When excluding groups, you cannot mix user and device groups across include and exclude. Click here to learn more.	
🗙 Troubleshooting + support		
	+ Add groups	
	Previous Next	

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



»»	Home > Apps >	
A Home	Create policy	
Z Dashboard		
E All services	✓ Basics ✓ Apps ✓ Data p	rotection 🗸 Access requirements 🗸 Conditional launch 🗸 Assignments 👩 Review + create
* FAVORITES	Summary	
🛄 Devices	600-100 and 7	
Apps	Basics	
Endpoint security	Name	Multiline iOS Policy
Reports	Description	This is policy set for iOS apps
🚨 Users	Platform	iOS//PadOS
24 Groups	Apps	
Tenant administration	Target to apps on all device types	Yes
X Troubleshooting + support	Device types	
	Public apps	
	Previous	· • • • • • •

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
	Contacts.ReadWrite	Allows the app to create, read, update, and delete user contacts.
Microsoft Graph	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 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 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.



Block access		
• Grant access		
Require multifactor authentication	(i)	
Require device to be marked as compliant	(i)	
Require Hybrid Azure AD joined device	i	
Require approved client app ① See list of approved client apps)	
Require app protection policy (See list of policy protected client apps	1	
For multiple controls		
 Require all the selected controls Require one of the selected controls 	,	
Screenshot: Grant configured to require either ap client apps or policy protected client apps	oproved s.	

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 <u>Azure AD Conditional Access Documentation</u> (<u>https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/)</u> of 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.



~	Home > Apps >	
A Home	Create policy	×
📶 Dashboard		
E All services	Resirs Anns Data protection Access requirements Conditional launch Assignments Review + create	
★ FAVORITES		
Devices	Included groups	
Apps	8, Add groups	
ᠲ Endpoint security	Groups	
Reports	No groups selected	
🚨 Users	Excluded groups	
🚑 Groups		
Tenant administration	() When excluding groups, you cannot mix user and device groups across include and exclude. Click here to learn more.	
💥 Troubleshooting + support		
	+ Add groups	
	Previous Next	

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

>>>	Home > Apps >	Select groups to include
A Home	Create policy	Azure AD Groups
Zh Dashboard	1 5	
) All services		₽ Search
* FAVORITES	✓ Basics ✓ Apps ✓ Data protection ✓ Access requirer	AD AAD DC Administrators
Devices	Included groups	
Apps	R. Add groups	CT Click to Dial - iOS
퉋 Endpoint security	Groups	DR Deems Brite
Reports	No groups selected	Denormay
🚨 Users	Excluded groups	GR grafana-testgroup
🎥 Groups		Contract of the second s
Tenant administration	() When excluding groups, you cannot mix user and device groups across inclu	IN IntuneDevGroup
🗙 Troubleshooting + support		IN IntuneMAM Selected
	+ Add arouns	
	Previous Next	Select

3. You should see the group listed

»	Home > Apps >	
A Home	Create policy	×
🖾 Dashboard		
⊟ All services		
* FAVORITES	V Basics V Apps V Data protection V Access requirements V Conditional launch 🧕 Assignments 🕜 Review + create	
Devices	Included groups	
Аррз	R ₂ Add groups	
🕵 Endpoint security	Groups	
Reports	IntuneMAM Remove	
🚨 Users	Excluded aroups	
🎎 Groups	munaaa Jaaba	
Tenant administration	() When excluding groups, you cannot mix user and device groups across include and exclude. Click here to learn more.	
🗙 Troubleshooting + support		
	+ Add groups	
	Previous Next	

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



»	Home > Apps >	
A Home	Create policy	
Z Dashboard		
E All services	✓ Basics ✓ Apps ✓ Data p	rotection 🗸 Access requirements 🗸 Conditional launch 🗸 Assignments 🥑 Review + create
	Summary	
Devices	80910241800*	
Apps	Basics	
Endpoint security	Name	Multiline iOS Policy
Reports	Description	This is policy set for iOS apps
🚨 Users	Platform	iOS//PadOS
	Apps	
Tenant administration	Target to apps on all device types	Yes
✗ Troubleshooting + support	Device types	-
	Public apps	
	Previous	· · · · · ·

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
	Contacts.ReadWrite	Allows the app to create, read, update, and delete user contacts.
Microsoft Graph	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).



Т

	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	Device Management Man aged Apps. Read Write	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.