

How to configure Microsoft Intune for Workspace public app

Document revision: 04

Add-On Products Roms Hule 8 – 7100 Vejle – Denmark Phone: +45 7944 7000 Fax: +45 7944 7001

Mail: info@add-on.com Internet: www.add-on.com



No parts of this publication may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without the permission from Add-On Products.



Table of contents

TABLE OF CONTENTS	2
INTRODUCTION	3
DETAILED INSTRUCTION	4
Configure for Android platform	4
Configuration on Microsoft Intune for Android	4
Deploy Android app on Microsoft Intune	4
Create app configuration policies	6
Create app protection policies	8
Configuration on Android device	11
Configure for iOS platform	16
Configuration on Microsoft Intune for iOS/iPad OS	16
Create app provisioning profiles	16
Create app configuration policies	18
Create app protection policies	
Configuration on iOS/iPad OS device	



CHAPTER 1. Introduction

Currently, it is required that Workspace applications downloaded from stores cannot access their server. Some changes need to be done so that the special revision of the app (deployed via Microsoft Intune) can work. The changes also prevent apps deployed by other channels from accessing their server.



CHAPTER 2. Detailed instruction

Configure for Android platform

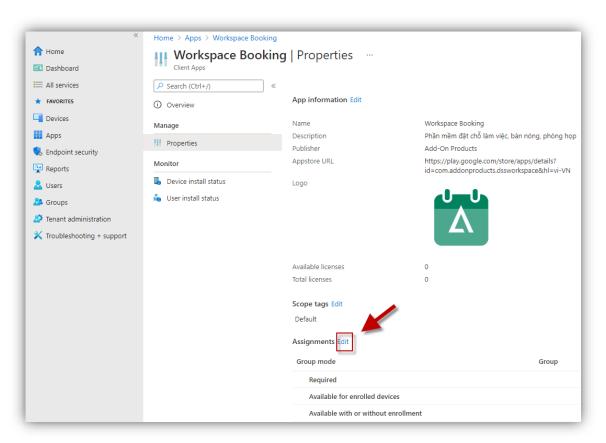
Configuration on Microsoft Intune for Android

Deploy Android app on Microsoft Intune

- Go to Intune website (<u>https://endpoint.microsoft.com</u>) and select Endpoint Manager → Apps → Android. Click [Add] button.
- 2. In the **Select app type** panel, click on App type, scroll down to select **Managed Google Play app**, and click [**Select**] button at the bottom of the panel.
- 3. Search for the workspace booking app in Google Play.
- 4. Select the app from the result list and click [**Sync**] button:

Microsoft Endpoint Manager a	admin center 🖓
 ≪ ↔ Home ☑ Dashboard ➡ All services ★ FAVORITES ➡ Devices ➡ Apps 	Home > Managed Google Play … ← Search Q
 Endpoint security Reports Users Groups Tenant administration Troubleshooting + support 	 Workspace Booking Add-on Products Add-on Products Add-on Products This app offers managed configuration This app offers managed configuration This app is only available in certain countries Select Unapprove Approval Preferences
	Workspace Workspace

5. After that, the app shows up in the list. Click on it and select **Properties**, then click [Edit] on **Assignments** label.



6. In the **Edit application** page, you can add group/users/devices based on your preferences. Then click [**Review + save**] → [**Save**].

Home > Apps > An	droid > WSA >		
Edit applicat Managed Google Play pr			
Assignments Rev	view + save		
Required 🛈			
Group mode	Group	Filter mode	Filter (preview)
(Included	All devices	None	None
Included	All users	None	None
Available for en			
Group mode	Group	Filter mode	Filter (preview)
Included	Workspace Booking Users	None	None
+ Add group ① Ad	d all users 🛈		
Review + save	Cancel		



Create app configuration policies

1. On the left panel, select Apps \rightarrow App configuration policies. Click [Add] \rightarrow Managed devices.

×	Home > Apps		
A Home	🙀 Apps App configura	ation policies	
🖾 Dashboard			
E All services	✓ Search (Ctrl+/) «	+ Add \sim	
★ FAVORITES	(i) Overview	Managed devices	
Devices	All apps	Managed apps	Platform ↑↓
Apps	Monitor	Config for Zoom	iOS
Endpoint security	By platform	ManagedAppConfig c	Android
Reports	Windows	Test app config policy	
Losers	iOS/iPadOS	Test WSARestriction	Android
Groups	🖵 macOS	Workspace Booking In	Android
Tenant administration	Android	Workspace Booking In	iOS
X Troubleshooting + support	Policy	WSA configuration po	Android
	App protection policies		
	App configuration policies		
	iOS app provisioning profiles		

- 2. Fill in details for the configuration policy \rightarrow **Basics** section:
- Enter configuration policy name
- Platform: Android Enterprise
- Profile Type: All Profile Types
- Targeted app: Click to select the created app (WSA) in the Associated app panel and click [OK] → [Next].

*	Home > Apps >		
A Home	Create app configuration policy		
🖾 Dashboard			
I All services	•		
* FAVORITES	Basics (2) Settings (3) Scop	be tags ④ Assignments ⑤ Review + create	
Devices	Name *	WSA configuration	
Apps	Description		
뤇 Endpoint security			
Reports			
💄 Users			
Sroups			
Tenant administration	Device enrollment type	Managed devices 🗸	
X Troubleshooting + support	Platform * (i)	Android Enterprise V	
	Profile Type * 🕡	All Profile Types V	
	Targeted app * 🛈	Workspace Booking	

3. In Settings section, click [Add] button, then select Use configuration designer for Configuration settings format label, then enter value for 2 keys: Server URL and Workspace Secret.



A Home	Edit app configuration policy	
🖾 Dashboard		
E All services		() Use the JSON editor to configure the disabled configuration
* FAVORITES	Settings Review + save	keys.
Devices	Permissions	
Apps	Permissions granted here will override the "Default app permissions" policy for the selected apps.	Search to filter items X
Endpoint security	Learn more about Android runtime permissions	✓ Configuration key ↑↓ Value type ↑↓ Description
Reports	*Add	Server URL string Server URL
Lusers	Not configured	Workspace Secret string Workspace S
Groups	Not comigured	
Tenant administration	Configuration Settings	
_	Configuration settings format ① Use configuration designer	
X Troubleshooting + support ★	Use the JSON editor to configure the disabled configuration keys.	
	+Add	
	Not configured	
	Review + save Cancel	
		οκ

- a. Server URL (similar to workspace_server_url key in XML file): Automatically establish server address on login panel of workspace app which was installed from MS Intune.
- b. Workspace Secret (similar to workspace_secret key in XML file): This is a security key. When this key is similar to the key on DS Server (parameter: Workspace.Secret), DS Server only allows Workspace with this key to connect.

«	Home > Apps > WSA Android Config Policy >	
숚 Home	Edit app configuration policy	
🖾 Dashboard		
All services		
★ FAVORITES	Settings (2) Review + save	
Devices	Permissions	
Apps	Permissions granted here will override the "Default app permissions" policy for the selected apps.	
🔩 Endpoint security	Learn more about Android runtime permissions	
🕎 Reports	+Add	
📩 Users	Not configured	
A Groups	Configuration Settings	
Tenant administration	Configuration settings Configuration settings format ① Use configuration designer	\sim
🗙 Troubleshooting + support	Use the JSON editor to configure the disabled configuration keys.	
	+Add	
	Configuration key Value type Configuration value Description	
	Server URL string V https://dssclients.aod.vn Server URL	

Then click [Review + save].

- 4. The Scope tags can be optionally established, then click [Next].
- 5. In Assignments section, you can add groups, users and devices, then click [Next].
- Proceed to Review + create section and click [Create] to finish. The "WSA configuration policy" is created and displayed in the list of App configuration policies.
- 7. Repeat the same procedure to add Chrome or Edge browser app on Intune.



Create app protection policies

1. On the left panel, select Apps \rightarrow App protection policies. Click [Create policy] \rightarrow Android.

Microsoft Endpoint Manager admin center				
 Home Dashboard 	Home > Apps Apps App protectio			
All services FAVORITES Devices Apps	Search (Ctrl+/) « Overview All apps Monitor	+ Create policy ∨ C Refresh iOS/iPadOS Android ↑↓ Windows 10 and later		
 Endpoint security Reports Users Groups Tenant administration Troubleshooting + support 	By platform Windows iOS/iPadOS macOS Android	WSA protection		
	Policy App protection policies App configuration policies			

- 2. Fill in details for the protection policy \rightarrow **Basics** section:
- Enter protection policy name
- Platform: Android

Home > Apps >	
Create policy	
1 Basics 2 Apps	③ Data protection ④ Access requirements ⑤ Conditional launch ⑥ Scope tags
Name *	Workspace Booking App Protection policy 🗸
Description	
Platform	Android 🗸

Then click [Next] to proceed.

3. In **Apps** section, configure as in the following figure:

Home > Apps >			
Create policy			
🔗 Basics 🙆 Apps ③ Data p	protection ④ Access requirements	5 Conditional launch	6 Scope tag
Choose how you want to apply this policy	y to apps on different devices. Then add at l	east one app.	
Target to apps on all device types i	Yes	No	
Device types ①	0 selected		\sim
Target policy to	Selected apps		\sim
Public apps	Remove		
Microsoft Edge	Remove		
+ Select public apps			
Custom apps	Remove		
com.addonproducts.dssworkspace	Remove		
+ Select custom apps			

NOTE: To setup Custom apps, click [+ Select custom apps] to open Select apps to target:

lome > Apps >		Select apps to target
Create policy		
		Search by Package ID 🗸
🗸 Basics 🛛 Apps 🔅 Data j	protection ④ Access requirements ⑤ Conditional launch ⑥ Scope ta	ags (7) Assignments More apps Package ID
Choose how you want to apply this polic	/ to apps on different devices. Then add at least one app.	com.contoso.app
Target to apps on all device types ①	Yes No	Add
Device types (i)	0 selected V	7.144.4
Target policy to	Selected apps	
Public apps	Remove	
Microsoft Edge	Remove	
+ Select public apps		
Custom apps	Remove	
No custom apps selected		
+ Select custom apps		
		Selected Apps:
		No Apps selected
Previous		
		Select

In More apps → Package ID, enter "com.addonproducts.dssworkspace" then click [Add]:

Δ	Add-On Products	Sign	Service
	<u> </u>	0	

ome > Apps > Create policy …				Select apps to target)
freate policy				App added	
Sasics 2 Apps 3 Data	protection ④ Access requirements (Conditional launch 6 Scop	pe tags (7)Assignment	Search by Package ID	~
Choose how you want to apply this polic	y to apps on different devices. Then add at least	one app.		More apps	
Target to apps on all device types 🕕	Yes	No	\supset	Package ID	
Device types ()	0 selected		7	com.contoso.app	~
Target policy to	Selected apps		×	Add	
Public apps	Remove			com.addonproducts.dssworkspace	
Microsoft Edge	Remove				
+ Select public apps					
Custom apps	Remove				
No custom apps selected					
+ Select custom apps					
				Selected Apps:	
				No Apps selected	

Finally, select the "com.addonproducts.dssworkspace" app that you have added and click [Select]. This app will now appear in your list of Custom apps.

Then click [Next] to proceed.

- 4. Keep the default configuration for **Data protection**, **Access requirements**, **Condition launch** sections, and proceed.
- 5. The Scope tags can be optionally established, then click [Next].
- 6. In Assignments section, you can add groups, then click [Next].
- 7. Proceed to **Review + create** section and click [**Create**] to finish. The "Workspace Booking App protection policy" is created and displayed in the list of **App protection policies**.

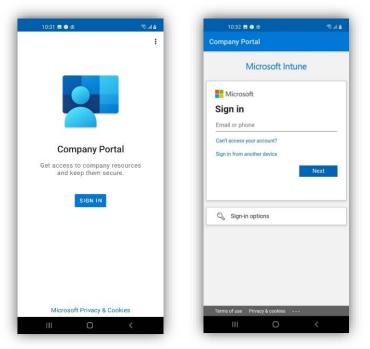
Configuration on Android device

1. In your device, go to Google Play and search for the key word "company portal app"





2. Install and sign in with the account that was used to do the configuration in Microsoft Intune in the previous section

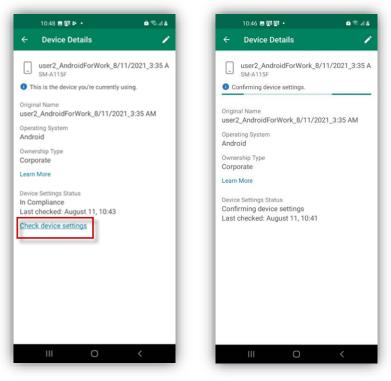


3. After signing in, proceed with setting up the work profile (keep clicking **Next** to proceed) until the following screen shows up:



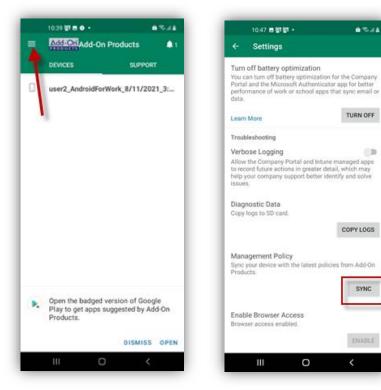


4. Touch the device name on the screen and touch Check device settings on the next screen.



5. After that, you are back at the screen with device name at the top, touch Options button and select Settings:





6. Once again, go back to the screen with the device name at the top, now touch [Open] button at the bottom right corner.

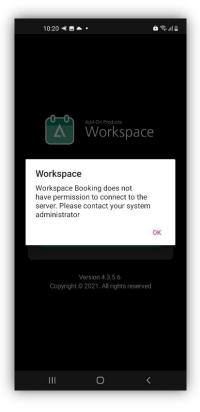


7. Select the WSA that was configured in Microsoft Intune and install it.





8. After installation, fill in the server address (similar to the URL you entered when creating the **configuration policy** in the previous section) to sign in. You might encounter the following warning message:



 In this case, you need to go to DSS web backend, create parameter Workspace.Secret and enter the secret key (that you entered when creating the configuration policy in the previous section) in Value field.

DS Service	Edit Parameter - "Workspace.Secret"	
DASHBOARD	BACK SAVE	
V DAILY TASKS	* Key	Create Date
✓ REPORTS	Workspace.Secret	Dec 20, 2021 17:00:54
∧ SYSTEM	Value	Last Update Date
License	71d84fa3-2f1f-49e0-bd1a-80b067f1ef35	Dec 20, 2021 10:35:25
Connections	Description	
Settings	Used in conjunction with Microsoft Intune to restrict ser for Microsoft Intune deployed Workspace Booking app	ver access
Outputs		
Categories		
Parameters		

10. Click [Save] to finish.

Configure for iOS platform

Configuration on Microsoft Intune for iOS/iPad OS

Create app provisioning profiles

- 1. Go to Intune website (<u>https://endpoint.microsoft.com</u>) and select Endpoint Manager → Apps → iOS/iPadOS.
- 2. Select iOS app provisioning profiles → Create Profile.

«	Home > Apps	
A Home	膏 Apps iOS app prov	visioning profiles
🖾 Dashboard		
E All services		+ Create profile
★ FAVORITES	💂 macOS 🔷	Use iOS app provisioning profiles to p
Devices	Android	${\cal P}$ Search by name
Apps	Policy	Name
Security	App protection policies	WSA Dev
Reports	App configuration policies	Workspace AdHoc
Let Users	🕤 iOS app provisioning profiles	Workspace AppStore
Sroups	S mode supplemental policies	Workspace Dev
Tenant administration	Policies for Office apps	WSA AdHoc
X Troubleshooting + support	Policy sets	WSA AppStore

3. Go to the following link to download iOS provisioning profile:



https://developer.apple.com/library/archive/recipes/ProvisioningPortal_Recipes/Downloadinga ProvisioningProfile/DownloadingaProvisioningProfile.html

...then upload to the **Basics** section of the **Create profile** page.

Home > Apps >	
Create profile	
1 Basics ⁽²⁾ Scope tags ⁽³⁾ A	Assignments ④ Review + create
Name *	
Description	
Upload profile file *	Select an iOS provisioning profile
Expiration Date *	8/13/2021, 5:08:51 PM

- 4. Proceed to **Scope tags**, **Assignments and Review + create** sections as described above (for Android platform configuration). After that, you can see the profile you just uploaded in the list.
- From the left panel, Select Apps → All apps, click [Add] button. In the Select app type panel, click on App type, scroll down to select IOS store app, and click [Select] button at the bottom of the panel.
- 6. When the "Add App" page shows up, click on the Search the App Store button and search for the workspace booking app...

6	Home > Apps >	Search the App Store		0
Home	Add App	the second s		
Dashboard	IOS store app	P workspace booking	> United States (default) V
All services	App information Scope Tags Assignments Assignments Assignments	Name	Publisher	74
* PRIVORITES		ranje	1. Puulsie	
Devices	Select app * () Search the App Store	31 Google Calendar: Get Organized	Google LLC	
Apps		and the second se		
Endpoint security		Expansive Workspace Client App	Level Office Management LLC	
Reports				
Users		Regus: Offices & Meeting Rooms.	Regus	
Groups				
Tenant administration		Peerspace - Book Unique Venues	PeerSpace	
Troubleshooting + support				
		Workspace Booking	Add-On Products	
		Flow Hotel & Workspace by Hour	Flow Entertainment Limited	
		SR. WorkSpace	Solutionreach, Inc.	
		• spaces. Spaces: Creative workspaces	Spacesworks	
		File Manager: Music; POF; Text	Salix	
		Workspors LLC	WORKSPOTS LLC	
	Freedom Next	-		
		Select		

... and select it. The app's info is displayed.



~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	Home > Apps >	
合 Home ☑ Dashboard	Add App ···	
All services	App information ② Scope	tags (3) Assignments (4) Review + create
★ FAVORITES	<u> </u>	
Devices	Select app * 🕕	Search the App Store
Apps	Name * 🕡	Workspace Booking
🔩 Endpoint security 🟆 Reports	Description * 🕧	Workspace is a mobile app that provides an easy way to book Microsoft Office 365 and on-premise resources e.g. meeting rooms and hot-desks.
Lusers	Publisher * 🛈	Add-On Products
Groups Tenant administration	Appstore URL	https://apps.apple.com/us/app/workspace-booking/id1480198282?uo=4
Troubleshooting + support	Minimum operating system * 💿	ios 8.0 V
	Applicable device type * 🕕	2 selected V
	Category 🕠	0 selected V
	Show this as a featured app in the Company Portal ①	Yes No
	Information URL ①	Enter a valid url
	Privacy URL	Enter a valid url
	Developer (i)	
	Owner (i)	
	Notes ①	
	Logo 🕕	Change image
	Previous Next	

Fill in necessary details and click [Next].

7. Proceed to Scope tags, Assignments and Review + create sections by clicking [Next] → [Create].

#### Create app configuration policies

1. On the left panel, select Apps  $\rightarrow$  App configuration policies. Click [Add]  $\rightarrow$  Managed devices.



~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	Home > Apps	
숚 Home	Apps App configura	ation policies
🖾 Dashboard		
E All services		+ Add \sim
★ FAVORITES	Overview	Managed devices
Devices	All apps	Managed apps Platform ↑↓
Apps	Monitor	Config for Zoom iOS
Endpoint security	By platform	ManagedAppConfig c Android
Reports	Windows	Test app config policy
Lusers	iOS/iPadOS	Test WSARestriction Android
A Groups	🖵 macOS	Workspace Booking In Android
Tenant administration	Android	Workspace Booking In iOS
🗙 Troubleshooting + support	Policy	WSA configuration po Android
	App protection policies	4
	App configuration policies	
	iOS app provisioning profiles	

- 2. Fill in details for the configuration policy \rightarrow **Basics** section:
- Enter configuration policy name
- Platform: iOS/iPadOS
- Targeted app: Click to select the created app (WSA) in the Associated app panel and click [OK] → [Next].

*	Home > Apps > Workspace configurat	ion IOS >	
1 Home	Edit app configuration policy		
🕮 Dashboard			
E All services			
★ FAVORITES	Basics 2 Review + save		
Devices	Name *	Workspace configuration IOS	
Apps	Description		
뤇 Endpoint security			
Reports			
🚨 Users			
🖧 Groups			
Tenant administration	Device enrollment type	Managed devices	\sim
🗙 Troubleshooting + support	Platform ()	iOS/iPadOS	\sim
	Targeted app * 🔅	Workspace Booking	

3. In Settings section, select Use configuration designer for Configuration settings format label, then enter value for 2 keys: Server URL and Workspace Secret.

A Home	Edit app configuration	policy		
🖾 Dashboard				
E All services				
★ FAVORITES	Settings (2) Review + save			
Devices	Configuration settings format 🔅	Use configuration desi	gner	\sim
Apps				
🔩 Endpoint security	Once the policy is created, the forma	at cannot be changed		
Reports				
🔒 Users	Enter values for the XML property list. Th	e values in the list will vary	depending on the app you are configuring. Contact the	3
🎎 Groups	supplier of the app to learn the values yo	bu can use.		
🍰 Tenant administration	Learn more about XML property lists			
X Troubleshooting + support	Configuration key	Value type	Configuration value	
	workspace_server_url	String	dssclients.aod.vn	•••
	workspace_secret	String	71d84fa3-2f1f-49e0-bd1a-80b067f	•••
		Select one		

- a. workspace_server_url: Automatically establish server address on login panel of workspace app which was installed from MS Intune.
- **b.** workspace_secret: This is a security key. When this key is similar to the key on DS Server (parameter: Workspace.Secret), DS Server only allows Workspace with this key to connect.

Then click [Review + save].

- 4. The Scope tags can be optionally established, then click [Next].
- 5. In Assignments section, you can add groups, users and devices, then click [Next].
- 6. Proceed to **Review + create** section and click [**Create**] to finish. The "WSA configuration policy" is created and displayed in the list of **App configuration policies**.

Create app protection policies

1. On the left panel, select Apps \rightarrow App protection policies. Click [Create policy] \rightarrow iOS/iPadOS.



Microsoft Endpoint Manager admin center			
Microsoft Endpoint Manager a « Home Dashboard All services FAVORITES Devices Apps Endpoint security Reports Users Users Groups Tenant administration Troubleshooting + support	Home > Apps Apps App protection policies … Search (Ctrl+/) Overview All apps Monitor By platform Windows iOS/iPadOS macOS Android Policy		
	App protection policies App configuration policies		

- Fill in details for the protection policy → Basics section:
 Enter protection policy name
 Platform: iOS/iPadOS

Home > Apps > Create policy			
Basics Apps) Data protection ④ Access requirements ⑤ Conditional launch ⑥ Scope tags		
Name *	Workspace Booking App Protection Policy		
Description			
Platform	iOS/iPadOS 🗸		

Then click [Next] to proceed.In Apps section, configure as in the following figure:

Home > Apps >			
Create policy			
Sasics 2 Apps 3 Data p	rotection ④ Access requirements	5 Conditional launch	6 Scope tage
Choose how you want to apply this policy	to apps on different devices. Then add at	least one app.	
Target to apps on all device types ①	Yes	No	
Device types 🕠	0 selected		\sim
Target policy to	Selected apps		\sim
Public apps	Remove		
Microsoft Edge	Remove		
+ Select public apps			
Custom apps	Remove		
com.addonproducts.dssworkspace	Remove		
+ Select custom apps			

NOTE: To setup Custom apps, click [+ Select custom apps] to open Select apps to target:

	Add-On Products		
Δ	Digital	Sign	Service

lome > Apps >		Select apps to target
Create policy		
		Search by Bundle ID 🗸
Sasics 2 Apps 3 Data	protection ④ Access requirements ⑤ Conditional launch ⑥ Scope tags ⑦ Assignmen	
Choose how you want to apply this polic	y to apps on different devices. Then add at least one app.	Bundle ID com.contoso.app
Target to apps on all device types 🕕	Ves No	concontosoapp
		Add
Device types (i)	0 selected V	
Target policy to	Selected apps	
Dublic const	Demons	
Public apps	Remove	
Microsoft Edge	Remove	
+ Select public apps		
Custom apps	Remove	
No custom apps selected		
+ Select custom apps		
		Selected Apps:
		Selected Apps.
		No Apps selected
Previous Next		

In **More apps** → **Bundle ID**, enter "com.addonproducts.dssworkspace" then click [Add]:

Δ	Add-On Products	Sign	Service
	9	9	

lome > Apps >		Select apps to target
Create policy		
		Search by Bundle ID 🗸
Sasics 2 Apps 3 Data	protection ④ Access requirements ⑤ Conditional launch ⑥ Scope tags	Assignments More apps Bundle ID
Choose how you want to apply this polic	cy to apps on different devices. Then add at least one app.	com.contoso.app
Target to apps on all device types 🕕	Yes No	
Device types ①	0 selected V	Add
Target policy to	Selected apps	com.addonproducts.dssworkspace
Public apps	Remove	
Microsoft Edge	Remove	
+ Select public apps		
Custom apps	Remove	
No custom apps selected		
+ Select custom apps		
		Selected Apps:
		com.addonproducts.dssworks Remove

Finally, select the "com.addonproducts.dssworkspace" app that you have added and click [Select]. This app will now appear in your list of **Custom apps**.

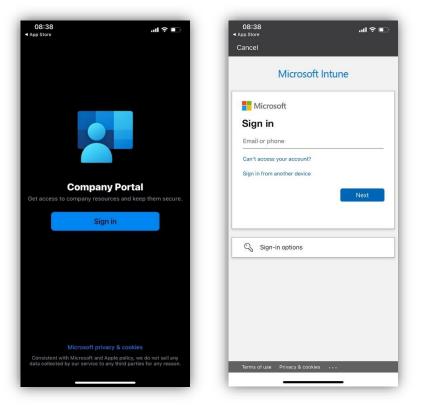
Then click [Next] to proceed.

- 4. Keep the default configuration for **Data protection**, **Access requirements**, **Condition launch** sections, and proceed.
- 5. The Scope tags can be optionally established, then click [Next].
- 6. In Assignments section, you can add groups, then click [Next].
- 7. Proceed to **Review + create** section and click [**Create**] to finish. The "Workspace Booking App protection policy" is created and displayed in the list of **App protection policies**.

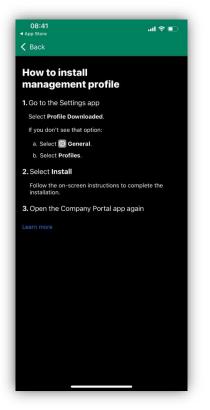
Configuration on iOS/iPad OS device

- 1. In your device, go to App Store, search for the key word "company portal"
- 2. Install and sign in with the account that was used to do the configuration in Microsoft Intune in the previous section



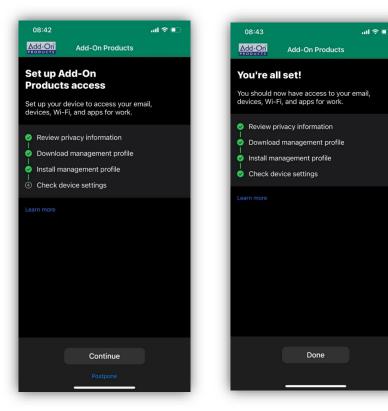


3. After signing in, proceed with setting up the work profile (keep clicking **Continue** to proceed) until the following screen shows up:



4. Follow the instruction on the "How to install management profile" screen, then go back to the app:





5. Click [Done] and proceed to install the app.



6. After installation, open the app, fill in the server address (similar to the URL you entered when creating the **configuration policy** in the previous section) to sign in. You might encounter the following warning message:





7. In this case, you need to go to DSS web backend, create parameter **Workspace.Secret** and enter the secret key (that you entered when creating the **configuration policy** in the previous section) in Value field.

DS Service	Edit Parameter - "Workspace.Secret"	
DASHBOARD	BACK SAVE	
V DAILY TASKS	* Key	Create Date
✓ REPORTS	Workspace.Secret	Dec 20, 2021 17:00:54
SYSTEM	Value	Last Update Date
License	71d84fa3-2f1f-49e0-bd1a-80b067f1ef35	Dec 20, 2021 10:35:25
Connections	Description	
Settings	Used in conjunction with Microsoft Intune to restrict server acces for Microsoft Intune deployed Workspace Booking app	S
Outputs		
Categories		
Parameters		

Click [Save] to finish.