



Integrate and Configure Jamf Pro and Microsoft Intune for Conditional Access for macOS



# Contents

	Preface	.3
Section 1:	: Create Device Compliance Policy in Intune	.4
Section 2:	: Configure Conditional Access in Jamf Pro	.9
Section 3:	: Deploy the Microsoft Company Portal Application to Mac computers.	14
Section 4:	Register a Mac computer with Azure Active Directory	27
Section 5:	: Check macOS Device Compliance in Microsoft Intune	31



This guide provides step-by-step instructions to integrate your Jamf Pro with your Microsoft Intune. This allows Jamf Pro to pass along device information to Intune that can be used for Conditional Access. You will go through the process of creating a compliance policy in Intune, configuring Conditional Access in Jamf Pro, deploying the Microsoft Company Portal application to your Mac computers, registering a Mac computer with Azure Active Directory, and then experiencing how Jamf Pro gathers information and passes it to Intune.

#### **Resources:**

https://docs.jamf.com/technical-papers/jamf-pro/microsoft-intune/10.17.0/Introduction.html https://docs.jamf.com/10.19.0/jamf-pro/administrator-guide/Preface.html https://docs.microsoft.com/en-us/mem/intune/

Use this guide to configure Jamf Pro and Microsoft Intune to limit access to resources like Office365 to only compliant Mac computers. Jamf Pro reports information to Microsoft Intune, which uses that information to allow or deny access to resources.

Items needed to complete this task:

- Jamf Pro offers two methods to connect to Microsoft Intune. This guide uses the Cloud Connector method.
  - Manual connection: Jamf Pro 10.9.0 or later.
  - Cloud Connector: Jamf Pro 10.18.0 or later hosted in Jamf Cloud.
- Microsoft Enterprise Mobility + Security (specifically Microsoft AAD Premium and Microsoft Intune).
- A Jamf Pro user account with Conditional Access privileges.
- Microsoft Intune Company Portal app for macOS v1.1 or later.
- Computers with macOS 10.11 or later that are using a local or mobile account ( network accounts are not supported).

Depending on your environment, you may need to add the following domain names and ports as an exception or add them to your network firewall whitelist:

- login.microsoftonline.com
- graph.windows.net
- \*.manage.microsoft.com
- Port 80/443 (HTTP/HTTPS protocol)



# Section 1: Create Device Compliance Policy in Intune.

In this section, you'll create an Intune compliance policy for macOS. As an example, this guide uses a policy that includes, but is not limited to, the following requirements:

- System Integrity Protection is turned on.
- The version of macOS is at least 10.13.6.
- FileVault encryption is turned on.

The compliance policy you create may vary depending on your organization's needs.

Note: For testing purposes this guide uses a test Mac that has FileVault turned off, in order to get an immediate result. We recommend that you turn off FileVault on your test Mac so that it is included in the compliance policy report.

- 1. Open a new browser window or tab and navigate to https://devicemanagement.microsoft.com.
- 2. Log in with credentials for a global administrator or an Intune service administrator.
- 3. In the left blade, click Devices.

Microsoft Endpoint Manager a	dmin center
«	Home > Devices   Overview
1 Home	i Devices   Overview
묘 Dashboard	
E All services	Search (Cmd+/) « En
★ FAVORITES	(i) Overview
Devices	All devices
Аррз	Monitor
-	

4. In the middle blade, Click Compliance Policies.

Microsoft Endpoint Manager	admin center		
«	Home > Devices   Overview		
숚 Home	(i) Devices   Overview		
🗔 Dashboard			
Ⅲ All services	Search (Cmd+/) «	Enrollment status Enrollment alerts Cor	npliance status
★ FAVORITES	(i) Overview		Enrollm
Devices	All devices	Intune enrolled devices	100
Apps	Monitor	Platform Devices	80
🜏 Endpoint security	By platform	Android 0	60
Reports	Windows	iOS 0	00
💄 Users	iOS	macOS 0	40
A Groups	🖵 macOS	Windows 0	20
Tenant administration	Android	Windows Mobile 0	0
eta Troubleshooting + support	Device enrollment	Total 0	3/2 iOS
	Enroll devices		10
	Policy	Top enrollment failures this week	
	Compliance policies	No data to display	
	Conditional access		



#### 5. In the top of the window, Click Create Policy.

Microsoft Endpoint Manager a	admin center		
«	Home > Devices > Compliance policies   Pe	olicies	
🔒 Home	Compliance policies   Polic	cies	
🔚 Dashboard			V Filter () Pafrash J Evport
All services	р Бearch (Cmd+/) «		
<b>★</b> FAVORITES	Policies	✓ Search by name	
Devices	🐥 Notifications	Policy Name	$\uparrow_{\downarrow}$ Platform $\uparrow_{\downarrow}$
Apps	Retire Noncompliant Devices	macOS Security Policy	macOS
🛼 Endpoint security	Locations	Windows 10 Security	Windows 10 and later
Reports	铰 Compliance policy settings		
움 Users			
Sroups			

- 6. Enter a name for the policy. This guide uses "macOS Security Policy" as an example.
- 7. Optional: Enter a Description. This guide does not use the Description field.
- 8. Click the Platform menu and choose macOS.
- 9. Click the Settings section to configure Settings.
- 10. Click Device Health.
- 11. Next to "Require for system integrity protection," click Require.
- 12. Click OK

anager a	dmin center			Ę 🗳 ⊗	? 😊	dallen@pretendcolife.o PRETENDCO LIFE	
«	Home > Devices > Compliance policies   Policies           Create Policy         ×	> Create Policy > Mac compliance policy > De Mac compliance policy macOS	vice He	Device Health		□ ×	
	Name * macOS Security Policy  Description Inter a description Platform * macOS Settings Configure	Select a category to configure settings. Device Health 1 setting available Device Properties 4 settings available System Security 13 settings available	> - - -	Require system integrity protection ()	œ	equire Not configured	
port	Account for noncompanitive     >       1     configured       5     cope (Tags)       0     scope(s) selected	ОК		ок			



- 13. Click Device Properties.
- 14. In the "Minimum OS version" field, enter 10.13.6.
- 15. Click OK.

				4 *	PRETENDCO
«	Home > Devices > Compliance p	olicies   Policies	> Create Policy > Mac compliance policy > Device F	Properties	
Home	Create Policy	×	Mac compliance policy ×	Device Properties	
Dashboard	Name *		Select a category to configure settings.		
All services	macOS Security Policy	~		Operating System Version ①	1
FAVORITES	Description		Device Health >	Minimum OS version ①	10.13.6 🗸
Devices	Enter a description	~	Tor Facting computed	Maximum OS version ①	Not configured
Apps		13	4 settings available		
Endpoint security	Platform *			Minimum Os build version ()	Not configured
Reports	macOS	~	13 settings available	Maximum OS build version ①	Not configured
Jsers					
iroups	Settings	>			
enant administration	configure				
roubleshooting + support	Actions for noncompliance	>			
	T conligured				
	Scope (Tags)	>			
	o scope(s) selected				
	Create		OK	OK 15	

- 16. Click System Security.
- 17. Next to "Encryption of data storage on device," click Require."
- 18. Click OK.





- 19. Confirm that the window displays the Settings you configured in the Mac compliance policy section.
- 20. Click OK.
- 21. Click "Actions for noncompliance."
- 22. In the Actions section, leave the default values of "Mark device noncompliant" and "Immediately."

Note: This guide uses the "Mark device noncompliant" action as an example for testing. In a production environment, you could specify a different action that restricts access to resources for a noncompliant Mac, but this is outside the scope of this guide.

23. Click OK.

Microsoft Endpoint Manager a	dmin center			Ģ	٩	۲	?	٢	dallen@pretendcolife.o PRETENDCO LIFE
«	Home > Devices > Compliance policies   Policies	$\rightarrow$	Create Policy > Actions						
A Home	Create Policy ×		Actions Specify the sequence of actions on noncompliant devices		×				
I: Dahbard     I: All services     All services     Arworks     Arworks     Porices     Apps     Fradpoint security     Porion     Apps     Fradpoint security     Porion     Apps     Devices     Apps     Devices     Apps     Torupised the support	Name *       macOS Security Policy       Description       Enter a description       Platform *       macOS       7 configured       Actions for noncompliance       1 configured       Scope (rapi)       0 scope(s) selected	21	+ Add Action Schedule Message template Mark device noncomplant Immediately			22			
	Create	۵	ок 23						

- 24. Click Scope (Tags).
- 25. Click +Add.
- 26. Select the checkbox next to Default.
- 27. Click Select.
- 28. Click OK.
- 29. Click Create.

Microsoft Endpoint Manager ad	dmin center				G 🗳 🎯 ?	dallen@pretendcolife.o     PRETENDCO UFE
«	Home > Devices > Compliance policies   Policies Create Policy ×	> Create Policy > Tags > Select Tags	tags « ×	Select tags	□ ×	
Cashboard Cashb	Name * macOS Security Policy Description Enter a description Platform * macOS Settings 7 configured Actions for noncompliance	+ Add 25 Scope Tag No Tags	26	Select  Select  Search by name Search by name		
	1 configured       Scope (rags)       0 scope(s) selected	ок 28		selected Default	>	



- 30. In the overview page of the policy you just created, configure the following:
  - A. In the left blade, click Assignments.

	${\cal P}$ Search resources, services, and docs (G+/)		Σ	Q (	. ●	?	٢	dallen@pretendcolife.o PRETENDCO UFE
Home > Device compliance   F	olicies > macOS Security Policy							
macOS Security Policy	<b>y</b>							×
,	« 🗐 Delete							
<ol> <li>Overview</li> </ol>	Assign profile to at least one group. Click assignments.							
Manage III Properties	Profile type : Mac compliance policy Assign Platform supported : macOS Groups Groups excluded : 0 A	ed : No assigned : 0						
Monitor								
Device status	Policy assignment status — macOS devices Assigned to macOS dev	non-						
User status	Succeeded							
Per-setting status								

- B. Click the "Assign to" menu and choose "Selected Groups."
- C. In the "Select Groups to include," select the target group.
- D. Click Select.

	,₽ Search resources, services, and docs (G+/)	D 67	₽ ⊚	?   dallen@pretendcolife.o
Home > Device compliance   F	olicies > macOS Security Policy   Assignments			Select groups to include
A macOS Security	Policy   Assignments			Azure AD groups
Search (Cmd+/)	« 🗟 Save 🗙 Discard 🗸 Evaluate			Select  Search by name or email address
Overview	Include Exclude			Rata Tactare
Manage	Assign to			BT
Properties	Selected Groups V		С	EN Engineering
8 Assignments	Select proups to include			
Monitor				MU Mac Users
Device status	No assignments			MU Mobile Users
User status				
Per-setting status				
				Selected members: Mac Users Remove
				Select

#### E. Click Save.

=	Microsoft Azure	${\cal P}$ Search resources, services, and docs (G+/)		¢	۰		dallen@pretendcolife.o PRETENDCO UFE
н	ome > Device compliance   P	olicies > macOS Security Policy   Assignments					
3	A macOS Security I	Policy   Assignments					×
[		« 🔚 Save 🗙 Discard 🗸 Evaluate					
•	Overview	Include Exclude					
	Manage	Assign to					
1	Properties	Selected Groups					
- 8	Assignments	Select groups to include					
	Monitor	× · · · · · · · · · · · · · · · · · · ·					
	Device status	Mac Users ····					
	User status						
	Per-setting status						

Verify a save confirmation message appears in the upper right.



# Section 2: Configure Conditional Access in Jamf Pro

In this section, you'll configure the connection between Jamf Pro and Microsoft Intune so that Jamf Pro can send information about enrolled Mac computers to Intune.

- 1. In a new browser window or tab, navigate to your cloud-hosted Jamf Pro.
- 2. Log in with the credentials for a Jamf Pro administrator account.

🛥 jamf 🛛 PRO		
username dallen		
PASSWORD	$\bigcirc$	
All contents © 2002-2020 Jam All rights reserved.		

3. In the upper-right corner, click Settings (looks like a gear) to open All Settings.



4. In the middle column, click Global Management.

🖆 jamf 🛛 PRO										চ	\$ ٩
Computers Devices Use	<u>نې</u>	All Settings	Global Ma	anagement							
VERSION 10 201+11584039255	000	System Settings	Categories	Push	GSX	Jamf Pro URL	PKI	Volume	User-Initiated	Automated	
MANAGED Computers: 4		Global Management		Certificates	Connection		Certificates	Purchasing	Enrollment	Device Enrollment	
Mobile Devices: 2	Ð	Self Service			()	S	<b>L</b>	10	+	畦	
UNMANAGED Computers: 0	Å	Server Infrastructure	Apple Education Support	Re-enrollment	Event Logs	Webhooks	AirPlay Permissions	Conditional Access	Inventory Preload	Enrollment Customization	
Mobile Devices: 0	3	Network Organization									
		Computer Management									



5. Click Conditional Access.

🗖 jamf 🛛 PRO	х.										ß	\$ ŝ
Computers Devices U:	E) sers	ŝ	All Settings	Global Ma	inagement							
VERSION 10.20.1-t1584039255		000	System Settings	Categories	Push	GSX GSX	Jamf Pro URL	PKI	Volume	User-Initiated	Automated	
MANAGED Computers: 4	12		Global Management	_			-				Enrollment	
Mobile Devices: 2		Ð	Self Service	Apple	Re-enrollment	Event Logs	Webhooks	AirPlay	Conditional	A Inventory	Enrollment	
Computers: 0 Mobile Devices: 0		å	Server Infrastructure	Education Support				Permissions	Access	Preload	Customization	
		3	Network Organization									
			Computer Management									
		[]	Device Management									
		<b>D</b> )	User Management									
	1	i	Jamf Pro Information									

6. In the bottom-right corner, click Edit it.

🏜 jamf 🛛 PRO	L 👂 🕸	
Computers Devices	Settings : Global Management Conditional Access	
VERSION 10190 (1580394015 MANAGED Computers: 4 Mobile Devices: 2 UNMANAGED Computers: 0 Mobile Devices: 0		
	Application ID Jamf Client App ID from Microsoft Azure	
Collapse Menu	Landing Page For Computers Not Recognized By Microsoft Asure - Wintergradient and an effected of the computer is not applied with Asure AD or - Done   History	



- 7. Select the checkbox for the "Enable Intune Integration for macOS" option.
- 8. For the Connection Type, select Cloud Connector (configuring the connection type of Manual is outside the scope of this guide),
- 9. If necessary, click the Sovereign Cloud menu and choose the appropriate cloud from Microsoft.
- 10. Select the landing page for computers not recognized by Microsoft Azure. This guide uses "Default Jamf Pro Device Registration page" as an example.
- 11. Click Connect.

ଅ jamf   PRO	ይ 👂 🏟
Computers Devices Users	Settings : Global Management Conditional Access
VERSION 1013.0.11580334015 MANAGED Computer: 4 Mobile Devices: 2 UNMANAGED Computers: 0 Mobile Devices: 0	macOS Intune Integration                   chick mac Integration for macOS                    chick mac Integration for macOS Integrated with Active Active Directory                   chick mac Integration                   chick mac Integration </td
Collapse Menu	Cancel Connect

- 12. Confirm that you're redirected to the application registration page in Microsoft.
- 13. Log in again with a Microsoft Azure global administrator or an Intune service administrator account.





14. Read the application permissions that Jamf requests, then click Accept.



- 15. Log in again with a Microsoft Azure global administrator or an Intune service administrator account.
- 16. Confirm that you're redirected to the Application ID page.
- 17. Click "Copy and open Intune."

🎜 jamf   PRO		
	Application ID	
	Copy the Application ID below and paste it into the Jamf Azure Active Directory App ID field in your Intune Instance.	
	963a9494-54df-4554-97ac-2cb44007ff49 Copy and open Intune	
	Confirm	

- 18. Confirm that a new tab opens to the Microsoft "Partner device management" blade in Microsoft Azure.
- 19. Click the "Specify the Azure Active Directory App ID for Jamf" Field then paste the Application ID into the field.
- 20. Click Save.

≡ Microsoft Azure 🖉 Search	r resources, services, and docs (G+/)	Σ	Ŗ	0 🔅	§ ?	٢	dallen@pretendcolife.o
Home > Device compliance   Partner device	e management						
💻 Device compliance   Parti	ner device management						×
	🕐 Refresh						
0 Overview	Connection status Last connection						
Manage	😁 Not set up						
Policies	Compliance Connector for lamf						
Notifications	You can use Intune's compliance engine to evaluate Jamf-managed macQS devices in						
Image: Retire Noncompliant Devices	your organization. Set up the connection using the steps below. Find out more about						
Locations	Steps:						
Monitor	1. Authorize Jamf in Azure Active Directory.						
Noncompliant devices	Authorize Jamf to send device inventory information to Intune for compliance						
Devices without compliance pol	1 9 <sup>aluation.</sup>						
Setting compliance	2. Specify the Azure Active Directory App ID for Jamf. *						
Policy compliance	963a9494-54df-4554-97ac-2cb44007ff49						
Windows health attestation rep	Activate the connection between Intune and Iamf in the Iamf Pro console						
Threat agent status							
Setup	Connector Settings						
Compliance policy settings							
Ø Microsoft Defender ATP							
🕼 Mobile Threat Defense 🛛 🕇 🎖	Include Exclude						
Rartner device management	Assign to						



21. Navigate back to the Jamf tab with the Application ID and click Confirm.

🔄 jamf   PRO		
	Application ID	
	Are you sure you pasted the Application ID into Intune? Click Confirm to continue. Jam / Azure Active Directory App ID 963a9494-54df-4554-97ac-2cb44007ff49 Copy and open Intune	

- 22. Confirm that you're redirected to the Conditional Access page in Jamf Pro.
- 23. You may see a yellow "Establishing Connection" notification.

🗖 jamf 🔤	L 🖗 🕸
Computers Devices Users	Settings : Global Management Conditional Access
VERSION 10190-11580394015 MANAGED Computers: 4 Mobile Devices: 2 UMMANAGED Computers: 0	macOS Intune Integration           REGISTRATION REGULAR APPROVED           The connection with Microsoft Intune will be established momentarily.
Mobile Devices: 0	ESTABLISHING CONNECTION     The connection with Microsoft Intune is currently being established. If you have not consented to the permissions requested by the Jamf Azure application in     Microsoft, you must do so to complete the configuration. Open administrator consent URL     Sense Internet Integration for macOS     Sense Inventory information to Microsoft Intune for computer registered with Azure Active Directory.     Connection Type Connection Type In use for the macOS intune Integration

24. If you don't see a green "Connection Established" bar after a few minutes, reload the browser page.

🗖 jamf   PRO	L 🖗 🕸
Computers Devices Users	Settings : Global Management Conditional Access
VERSION 10.19.0-11580394015 MANAGED Computers: 4	mecOS Intune Integration
Mobile Devices: 2 UNMANAGED Computers: 0	CONNECTION ESTABLISHED
Mobile Devices: <b>0</b>	Emable Intune Integration for macOS Sends Inventory Information to Microsoft Intune for computers registered with Azure Active Directory Connection Type Connection type to use for the macOS Intune Integration
	Cloud Connector     Manual
	Severeign Cloud Location of the Severeign Cloud
	Update Intune Inventory Send an update of inventory attributes to intune outside of the standard communication Send Update
	Landing Page For Computers Not Recognized by Microsoft Azure Webpage where users are redirected to if their computer is not registered with Azure AD or not enrolled with Jamf Pro.
Collapse Menu	Done History Eat

25. Confirm you see a green "Connection Established" notification.



# Section 3: Deploy the Microsoft Company Portal Application to Mac computers.

Microsoft Intune helps organizations manage access to corporate apps, data, and resources. Company Portal is the app that lets you, as an employee of your company, securely access those resources. The Company Portal Application is used to register the user's device with Azure Active Directory.

You can download the company portal at: https://go.microsoft.com/fwlink/?linkid=862280 This link downloads a package so you can upload it directly to Jamf Pro.

In this section, you will upload the Microsoft Company Portal application package and create a Smart Computer Group in Jamf to install Company Portal on. You will then create a policy to install Company Portal. After this, you will create a Smart Computer Group in Jamf for computers with Company Portal installed and then create a policy for users to launch Company Portal from Self Service to register the device with Azure Active Directory.

#### Upload the Microsoft Company Portal Application Package

1. Log in to Jamf Pro and navigate to All Settings > Computer Management > Packages.



2. In the upper-right corner, click New.

🎜 jamf 🛛 PRO						L 👌 🏟
Computers Devices User	Settings : Computer Manageme ← Packages	nt				
VERSION 10.20.1-11584039255 MANAGED	NAME	∧ CATEGORY	PRIORITY	FUT	FEU	+ New
Computers: 4 Mobile Devices: 2 UNMANAGED	Google Chrome.pkg	No category assigned	10	No	No	No
Computers: <b>0</b> Mobile Devices: <b>0</b>						

Note: do not enter anything in the Display Name field yet because Jamf Pro automatically enters the name of the file after you complete the next two steps.



- 3. In the Filename section, click Choose File.
- 4. Select the package you just downloaded in the previous section. By default, Safari uses your Downloads folder, then click Choose.

Optional: Click the Category menu then choose an appropriate category. This guide uses Intune as an example category (to create a new category, you can navigate to All Settings > Global Management > Categories, click New, enter a name in the Display Name field, click Save, then go back to step 1).

- 5. Optional: In the Notes field, enter the URL from the beginning of this section.
- 6. Click Save.

🗖 jamf 🛛 PRO	٩	<b>P</b> &
Computers Devices Users	Settings : Computer Management > Packages ← New Package	
version 10.20.1-11584039255	General Options Limitations	
MANAGED Computers: 4	Display Name Display name for the package CompanyPortal 2.3 200201-Installer riko	
Mobile Devices: 2 UNMANAGED Computers: 0 Mobile Devices: 0	Category to add the package to Intune	
	Filename Filename of the package on the distribution point (e.g. %/Package dmg*) Change File CompanyPortal_2.3.200201-Installer.pkg	
	Manifest File	
	Upload Manifest File Info Information to display to the administrator when the package is deployed or uninstalled	
	Notes to display about the package (e.g. who built it and when it was built)	
	Company was downloaded from https://go.microsoft.com/fwiink/? <u>linkid</u> =862280	
Collapse Menu	Cancel	Save

#### Create a Smart Group to scope the installation of Company Portal app

1. In the upper-left corner, click Computers.

🛂 jam	f	
Computers	[ Devices	ل Users
VERSION 10.20.1-11 MANAGE Compute Mobile D UNMAN, Compute Mobile D	N 584039255 ED ers: 4 Nevices: 2 AGED ers: 0 Devices: 0	



2. In the sidebar, click Smart Computer Groups.



3. In the upper-right corner, click New.

🋂 jam	nf PRO		ይ	\$ ©
Computers		Computers Smart Computer Groups		
INVENTO				+ New
C Se	arch Inventory arch Volume Conten	NAME	^ COUNT	
Q. Lic		All Managed Clients	4	
	IT MANAGEMENT	All Managed Servers	0	
@, co		APFS Encryption FV2 is OFF	2	
🛞 Re		APFS Encryption FV2 is ON	2	
(A) Ma	ac App Store Apps	Computer WITH Microsoft Company Portal App	1	

4. In the Display Name field, enter a name for the Smart Group. This guide uses Computers WITHOUT Microsoft Company Portal App as an example.

🌌 jamf   PRO		<b>\$</b> 1	
Computers Devices Users	Computers : Smart Computer Groups ← New Smart Computer Group		
INVENTORY	Computer Group Criteria		
Search Volume Content	Display Name Display name for the smart computer group		
😞 Licensed Software	Computers WITHOUT Microsoft Compnay Portal App		
CONTENT MANAGEMENT	Send email notification on membership change When group membership changes, send an email notification to Jamf Pro users with email notifications enabled. An SMTP server must be set up in Jamf Pro for this to work	 	
Restricted Software			

5. Click the Criteria tab.

Computer Group	Criteria							
<u></u> -		-						
Display Name Display name for the smart computer group								
Computers WITHOUT Microsoft Company Portal App								



6. Click Add.

Computers : Smart Comput ← New Smart Com	er Groups nputer Group			
Computer Group Crite	eria			
AND/OR	CRITERIA	OPERATOR	VALUE	
				+ Add

7. Click Choose to the right of Application Title.

Computers : Smart Computer Groups ← New Smart Computer Group	
Computer Group Criteria	
NEW CRITERIA	Show Advanced Criteria
APFS Encryption Check	Choose
Application Title	Choose
Building	Choose
Computer Group	Choose

#### 8. Click the Operator menu and choose "Does Not Have."

Computer Group	Criteria					
AND/OR	Ŧ	CRITERIA Application Title	OPERATOR	VALUE		Delete
			has does not have			+ Add

#### 9. In the Value field, Enter Company Portal.app.

Computer Group	Criteria						
AND/OR		CRITERIA	OPERATOR	VALUE			
	•	Application Title	does not have 💌	Company Portal.app	••••	•	Delete
							4. 4.44

#### 10. Click Save.

VALUE
Company Portal.app
+ 4



#### Create a policy to install Company Portal app

- 1. In the sidebar, click Policies.
- 2. Click New.
- 3. In the General Payload configure the following settings:
  - A. In the Display Name field, enter a name. This guide uses Deploy Microsoft Company Portal.app as an example.
  - B. Optional: Click the Category menu and choose an appropriate category.
  - C. In the Trigger settings, select the checkbox for Enrollment Complete and for Recurring Check-in.
  - D. Click the Execution Frequency menu and choose "Once per computer."

<b>2</b> jamf   PRO	ይ 🖗 🕸
Computers Devices Users	
Computers         Devices         Users         Center Folicy           INVENTORY         Options         Scope         S           Search Inventory         Image: Contrast         Image: Contrast         Image: Contrast         Image: Contrast           Image: Contrast         Emage: Contrast         Image: Contrast<	If Service       User Interaction         If Service       General         Display Name       Display name for the policy         Display Name       Display name for the policy         Display Name       Display name for the policy         Display Name       Display Name         Image: Service       Display Name         Image: Service       Display Name         Image: Service       Display Name         Image: Service       Image: Service         Image: Service       Trigger         Image: Service       Image: Service         Image: Service       Image: Service         Image: Service       Service </th
Management Settings     EFI Password     Mac Configured     Restart Options     Configured	Custom At a custom event Execution Prequency at which to run the policy Once per computer Target Drive The drive on which to run the policy i.e. "VolumesRestore"). The policy runs on the boot drive by default

- 4. In the list of payloads, select Packages.
- 5. Click Configure.





6. Next to the Company Portal package, click Add.

Packages		Packages Settings
NAME	CATEGORY	
CompanyPortal_2.3.200201-Installer.pkg	Intune	Add
depnotify-with-installers.pkg	No category assigned	Add
Google Chrome.pkg	No category assigned	Add
		Cancel

- 7. Optional: Click the Distribution Point menu and choose an appropriate distribution point.
- 8. Leave the Action menu at its default value of Install.

🗖 jamf   PRO			D	چ چ
Computers Devices Users	omputers : Policies ← New Policy			
INVENTORY	Options Scope Self Service	User Interaction		
<ul> <li>Search Inventory</li> <li>Search Volume Content</li> </ul>	Packages > 1Pockage	Packages		
CONTENT MANAGEMENT	Software Updates Not Configured	Distribution Point Distribution point to download the package(s) from Each computer's default distribution point *		
Policies Configuration Profiles	Scripts 0 Scripts			
<ul> <li>Restricted Software</li> <li>PreStage Imaging</li> </ul>	Printers O Printers	CompanyPortal_2.3.200201-Installer.pkg Action Action to take on computers		× +
🛞 Mac App Store Apps	Disk Encryption Not Configured	Install		
eBooks	Dock Items 0 Dock Rems	Update Autorun data Add or remove the package from each computer's Autorun data		
Smart Computer Groups	Local Accounts			

- 9. Click the Maintenance payload.
- 10. Click Configure.

🛂 jamf   PRO				L 🍾 🏟
Computers Devices Users	Computers : Policies ← New Policy			
IVVENTORY  Search Inventory  Search Volume Content  Userrad Software  OTTENT VolumeContent  Configuration Profiles  Profiles Pensione Profiles  Profiles Profiles Profiles  Profiles Profiles  And App Store Apps  And App Store Apps  And App Store Apps  Configuration Profiles  Profiles  Content Profiles  Content Profiles  Profiles  Content Profiles  Profile	Options         Scope         Self Service           Solutions         Solutions         Solutions           Solutions         Printers         Solutions           Disk Encognition         Solutions         Solutions           Disk Encognition         Solutions         Solutions           Disk Encognition         Solutions         Solutions           Disk Encognition         Solutions         Solutions           Solutions         Solutions         Solutions	9	Configure Maintenance Under the update inventory, reset computer names, install all cached packages, and run common maintenance tasks. Configure 10	
Collapse Menu				Cancel Save



11. Confirm that the checkbox Update Inventory is selected.

🏜 jamf   PRO				
Computers Devices Users	Computers : Policies ← Deploy Microsoft Compar	nyPortal.app		
INVENTORY	Options Scope Self Service	User Interaction		
Search Volume Content	Scripts 0 Scripts	Maintenance		×
CONTENT MANAGEMENT	Printers 0 Printers	Force computers to submit updated inventory information to Jam Pro     Computer Name     Computer Name     Computer Name     Computer Name     Additional State State     S		
Configuration Profiles  Restricted Software  ProStage Imaging	Disk Encryption Not Configured	Install Cached Packages Install oackages cached by Janf Pro		

- 12. Click the Scope tab.
- 13. Leave the Target Computers menu at its default value of Specific Computers.
- 14. Next to Selected Deployment Targets, click Add.

🞜 jamf 🛛 PRO			L 🗞 🕸
Computers Devices Users	Computers : Policies ← New Policy		
INVENTORY	Options Scope Self Service User Interaction	I.	
Search Volume Content	Targets	Limitations	Exclusions
😞 Licensed Software	13		
CONTENT MANAGEMENT	Target Computers	Target Users	
Policies	Computers to deploy the policy to	Users to deploy the policy to	
Configuration Profiles	Specific Computers 👻	Specific Users 👻	
Restricted Software			14
PreStage Imaging			(C
Mac App Store Apps	Selected Deployment Targets		+ Add
Patch Management	TARGET	TYPE	
eBooks			
	No Targets		

- 15. Click the Computer Groups tab.
- 16. Next to the Smart Computer Group you just created, click Add
- 17. Next to Add Deployment Targets, click Done.
- 18. Click Save.

🗖 jamf 🛛 PRO					ይ \$ @
Computers Devices Users	Computers : Policies ← Deploy Microsoft CompanyPortal.app				
	Options Scope Self Service User Interaction	1			
	Targets	Limi	tations	Exclu	isions
					17
Policies     Configuration Drofiles	Add Deployment Targets				Done
Restricted Software	Computers Computer Group	s 15 Users	User Groups	Buildings	Departments
		10			
	Q Filter Re 1-9 of 9				
	GROUP NAME				
	All Managed Clients				Add
	Computer WITH Microsoft Company Portal App				Add
	All Managed Servers				Add
	Invalid or Unknown FV2 Recovery Key				Add
	APFS Encryption FV2 is OFF				Add
ProStage Earelmonte	Computers pat restarted within the last 45 days				A11
	compacto non restance manin are last 45 days				
Management Settings	FileVault Enabled				Add
	APFS Encryption FV2 is ON				16 Add
	Computers WITHOUT Microsoft Company Portal App				Add
	1 w b Show 100 w				Cancel Surg
Consepse Menu					Sure Sure



19. Confirm that the Target section displays the Smart Computer Group you created.

🖆 jamf 🛛 PRO			£ 🤌 🏟
Computers Devices Users	Computers : Policies		
INVENTORY	Options Scope Self Service User Interaction		Show in Jamf Pro Dashboard
Search Volume Content	Targets	Limitations	Exclusions
CONTENT MANAGEMENT Policies © Configuration Profiles	Target Computers Computers to deploy the policy to Specific Computers	Target Users Users to deploy the policy to Specific Users ~	
Restricted Software     PreStage Imaging     Mac App Store Apps		TYPE Second Communities Communi	
Patch Management     eBooks     GROUPS	Computers with OUT microsoft Compilary Portal App	arhart Computer Group	

#### Create a Smart Computer Group for computers with Company

- 1. If necessary, in the upper-left corner, click Computers.
- 2. In the sidebar, click Smart Computer Groups.
- 3. In the upper-right corner, click New.
- 4. In the Display Name field, enter a name. This guide uses Computers WITH Microsoft Company Portal App as an example.

🋂 jarr	nf PRO		\$ <sup>9</sup> ;	
Computers	[ Devices	Computers : Smart Computer Groups ← New Smart Computer Group		
	ORY	Computer Group Critteria		
🖂 Se		Display Name Display name for the smart computer group		
🔍 Lic	ensed Software	Computer WITH Microsoft Company Portal App		
CONTEN		Send email notification on membership change		
Po		When group membership changes, send an email notification to Jamf Pro users with email notifications enabled. An SMTP server must be set up in Jamf Pro for this to work		
🔍 Co				
🛞 Re				
📃 🔜 Pre	eStage Imaging			

#### 5. Click the Criteria tab.

Computer Group Criteria	
Display Name Display name for the smart computer group	
Computers WITH Microsoft Company Portal App	
Send email notification on membership change When group membership changes, send an email notification to Jamf Pro users with email notifications enabled. An SMTP server must be set up in Jamf Pro for this to work	

#### 6. Click Add.

Computer 0	Group Criteria				
AND/OR		CRITERIA	OPERATOR	VALUE	
	•	Application Title	has 💌	Company Portal.app	▼ Delete
					+ Add



7. Next to Application Title, click Choose.

Computer Group Criteria	
NEW CRITERIA	Show Advanced Criteria
APFS Encryption Check	Choose
Application Title	Choose
Building	Choose
Computer Group	Choose

8. Click the Operator menu and choose "Has."

Computer Group			
ND/OR		CRITERIA	is
	•	Application Title	is not ✓ has

9. In the Value field, enter **Company Portal.app**.

Computer Group	Criteria					
AND/OR		CRITERIA	OPERATOR	VALUE		
	•	Application Title	has 👻	Company Portal.app	-	Delete
						+ Add

#### 10. Click Save.

Computer Group Criteria				
AND/OR	CRITERIA	OPERATOR	VALUE	
<b>.</b>	Application Title	has 💌	Company Portal.app	▼ Delete
				+ Ad



# Create a policy for users to launch Company Portal from Jamf Self Service and register their device with Azure Active Directory.

A user must open the Company Portal app from Jamf Self Service to register their device with Azure Active Directory. Launching the Company Portal app manually (e.g., from the Applications or Downloads folder) will not register the device. If a user opens the Company Portal app manually, they will see an 'AccountNotOnboarded' warning message. Because of this, you'll create a policy for users to open Company Porta from Jamf Self Service.

- 1. If necessary, in the upper-left corner, click Computers.
- 2. In the sidebar, click Policies.
- 3. Click New.
- 4. In the General payload configure the following settings:
  - A. In the Display Name field, enter a name. This guide uses **Register Mac with Azure Active Directory via Company Portal.app Self Service** as an example.
  - B. Optional: Click the Category menu and choose an appropriate category.
  - C. In the Trigger section, leave all the checkboxes deselected (because this policy will be triggered only by Self Service).
  - D. Leave the Execution Frequency value at its default of "Once per computer."





5. Select the macOS Intune Integration payload then:

A. Click Config	gure.			
🔊 jamf 🛛 PRO				r 🍾 🕸
Computers Devices Users	Computers : Policies ← New Policy			
INVESTIGAT  Search Volume Content Search Volume Content Search Volume Content Subscreamed Search Volume Content  Policia Policia Policia Policia Software Policia Policia Software Policia Policia Policia Software Policia P	Options     Senti Senticiana       Sentinaria     Senti Senticiana       Sentinaria     Senti Senticiana       Senti Sentinaria     Senti Sentinaria       Senti Sentinaria     Senti SentiSeninaria       Senti Sentinaria	r Interaction	macOS Intune Integration Use this section to enable uses to register that devices with Acter Active Directory. Configure	
Collapse Menu				Cancel Save

b. Select the checkbox for the "Register computers with Azure Active Directory" option.

🏜 jamf 🛛 PRO		£ 🖗 🏟
Computers Devices Users	Computers : Policies ← New Policy	
INVENTORY	Options Scope Self Service	User Interaction
Q Search Inventory		
Search Volume Content	Scripts 0 Scripts	macOS Intune Integration ×
Q Licensed Software		
CONTENT MANAGEMENT	Printers 0 Printers	Register computers wan Azure Active Directory Launches the Company Portal app for users, enabling them to register computers with Azure Active Directory. Registered computers submit updated inventory to Jam Pro.
Policies		A The Microsoft Intune Company Portal and must be installed on computers in the scope of this policy prior to deploying the
Configuration Profiles	Disk Encryption Not Configured	policy to users.
Restricted Software		
PreStage Imaging	Dock Items 0 Dock Items	
Mac App Store Apps		
Patch Management	Local Accounts 0 Accounts	

6. Click the Scope tab.

Options Scope Self Service	User Interaction
General	macOS Intune Integration
Packages 0 Packages	Register computers with Azure Active Directory Launches the Company Portal app for users, enabling them to register computers with Azure Active Directory. Registered computers submit updated inventory to Jam Pro.
Software Updates Not Configured	The Microsoft Intune Company Portal app must be installed on computers in the scope of this policy prior to deploying the policy to users.
Scripts 0 Scripts	

7. Leave the Target Computers menu at its default value of Specific Computers.

Options Scope Self Service User Interaction		
Targets	Limitations	Exclusions
Target Computers Computers to deploy the policy to	Target Users Users to deploy the policy to	
Specific Computers	Specific Users	



### 8. Click Add.

Options Scope Self Service User Interaction		
Targets	Limitations	Exclusions
Target Computers Computers to deploy the policy to	Target Users Users to deploy the policy to	
Specific Computers *	Specific Users •	
Selected Deployment Targets		+ Add
TARGET	TYPE	

#### 9. Click the Computer Groups tab.

Options Scope Self	Service User Interaction				
Targ	gets	Limitat	ions	Excl	usions
Add Deployment Targets					Done
Computers	Computer Groups	Users	User Groups	Buildings	Departments
Q Filter Re 1 - 9 of 9		]			

#### 10. Next to the Smart Group you created, click Add.

Options Scope Self Service User Interaction				
Targets	Limitat	lons	Exclu	isions
Add Deployment Targets				Done
Computers Computer Groups	Users	User Groups	Buildings	Departments
Q Filter Re 1-9 of 9				
GROUP NAME				
All Managed Clients				Add
Computer WITH Microsoft Company Portal App				Add
All Managed Servers				Add



- 11. Click the Self Service Tab.
- 12. Select the checkbox for the "Make the policy available in Self Service" option.
- 13. In the Self Service Display Name, enter Register Your Computer.

14. In the Button Name field, enter Register.

🛂 jamf 🛛 PRO		L 🍾 🏟
Computers Devices Users	Computers : Policies ← New Policy 12	
	Options Scope Self Service User Interaction	
	Self Service Display Name Divide name for the policy in Self Service (Self Service 30.0 or later)	
Policies     Configuration Profiles     Destricted Software	14 Register Vour Company many temperature on any party of a set of	
	15 Register	
	Description Description to display for the policy in Self Service Type your description here	
	Force eases to view the description before the paticy runs	
	Notification Display notifications for the policy	
	Icon I conto display for the policy. It is recommended that you use a file with the GIF or PNG format. The recommended size is 512x512 pixels. AzureLogo.png Upload Icon	
	Select Existing Icon	Cancel Save

- 15. Optional: Assign a Category.
- 16. Configure the rest of the Self Service tab as you'd like.

Note: We recommend that you use an engaging icon for each Self Service policy. This is beyond the scope of this document, but we have provided resources below:

Resources:

https://www.flaticon.com/free-icons/self-service

https://www.jamf.com/resources/videos/self-service-with-jamf-pro/

https://docs.jamf.com/10.20.0/jamf-pro/administrator-guide/About\_Jamf\_Self\_Service\_for\_macOS.html

17. Click Save.



# Section 4: Register a Mac computer with Azure Active Directory

In this section, you'll register a test Mac with Azure Active Directory by using an app called JamfAAD. JamfAAD sends the token with the Azure AD information to Jamf Pro. Jamf Pro sends computer inventory information to Microsoft Intune and the computer record is created in Intune after compliance is calculated for the first time. The Azure AD information is stored in the device\_aad\_information table in the Jamf Pro database.

- 1. On a Mac that's enrolled with Jamf Pro, log in with a local or mobile account.
- 2. Open Jamf Self Service.
- 3. For the "Register Your Computer" item, click Register.

Q Search			لے Activity		Log In	¢
Self Service						
Home					Sort AZ	٢
All Intune Security/FileVault	Encrypt Me New	Register Your C Register	omputer			

- 4. Confirm that the Company Portal app opens and prompts the user to sign in.
- 5. Click Sign In.





6. Enter a valid Azure Active Directory username and click Next.

•••			
Microsoft Intune			
Microsoft			
dallen@pretendcolife.onmicrosoft.com	_		
Can't access your account? Sign in from another device			
Next			
Cancel sign-in	Terms of us	se Privacy & cookies	

7. Enter your password and click "Sign in."

	Microsoft Intune			
	<ul> <li>Microsoft</li> <li>dallen@pretendcolife.onmicrosoft.com</li> <li>Enter password</li> <li>Forgot my password</li> <li>Sign in</li> </ul>			
	Terms	of use	Privacy & cookies	
Cancel sign-in				



8. Confirm that the Company Portal app displays a window with a progress bar and a message that the company is being contacted:

A. Once the company is contacted, it displays "Registering your Mac..."



B. Once finished, it displays "You're all set!" Click Done.

Pretendco Life
You're all set!
You should now have access to your email, devices, Wi-Fi, and apps for work.
Done



- 11. Follow the prompts for the JamfAAD app. Depending on your environment, the user is asked to do one of the following:
  - A. If your environment has Azure AD federation configured, the user is prompted to enter their authentication credentials for a second time and accept a multi-factor authentication prompt if configured.
  - B. If your environment only uses Azure AD accounts, the user is prompted to enter their password again and accept a multi-factor authentication prompt if configured.

Microsoft
MICrosoft
dallen@pretendcolife.onmicrosoft.com
Enter password
Forgot my password
Sign in with another account
Sign in
Terms of use Privacy & cookies ····

15. When you are prompted to unlock the login keychain in Keychain Access to grant permissions, enter your login password, then click Allow.

$\bigcirc$	JamfAAD wants to access key "Microsoft Workplace Join Key" in your keychain.								
To allow this, enter the "login" keychain password.									
	Password:								
?	Always Allow Deny Allow								

r



# Section 5: Check macOS Device Compliance in Microsoft Intune

- 1. Open a new browser window or tab and navigate to https://portal.azure.com.
- 2. Log in to Microsoft Azure with a global administrator or an Intune service administrator account
- 3. If Azure displays Device Compliance, click Device Compliance.

=	Microsoft Azure	𝒫 Search resources, serv	vices, and docs (G+/)					E	r (* o	? 😊	dallen@pretendcolife.o PRETENDCO UFE
		Azure services									
		+   🛛	6	<u>e</u>	۲		SQL	Ŧ	<b>8</b>	$\rightarrow$	
		Create a Dev resource comp	Nice Azure Activ Diance Directory	e Virtual machines	App Services	Storage accounts	SQL databases	Azure Database for PostgreS	Azure Cosmos DB	More services	
		Navigate	Device com	oliance 🛪							
		📍 Subscriptic 👁	View			All resourc		Da	shboard		
		Usef Tools Over Price Microsoft Learn of Learn Azure with fr training from Micro	ful links nyiew (2 Started (2 ng (2 ree online cosoft	Azure Monitor Monitor your apps i Infrastructure	and	Security C Secure you infrastruct	enter ur apps and ure	s c Al d	ost Management nalyze and optimiz oud spend for free	e your	
		Useful links						Azure r	nobile app		
		Technical Documentation D Azure Migration Tools	⊰" Azure Find a	Services @" n Azure expert		Recent Azure Upda Quickstart Center	ites d'	É App	o Store	500gle Play	

4. If Azure does not display Device Compliance, then in the search bar at the top of the Azure portal page, enter device compliance then choose "Device compliance."

= Microsoft Azure			×								
	Services	M	larketplace	1 m							
	. Device compliance		No results were found.								
L	Devices	Dr	ocumentation See all	$\rightarrow$							
	Device configuration	0	Conditional Access - Require compliant devices - Azure	atabase Azure Cosmos More services							
	C Device enrollment	a	Conditional Access require managed device - Azure Active	greS DB							
	Oevice Provisioning Services	A	Idmin role descriptions and permissions - Azure AD								
	StorSimple Device Managers	w	What is device identity in Azure Active Directory								
	Resources	Re	esource Groups								
	No results were fo	und.	No results were found.	Dashboard							
	Searching all subscriptions. Charge										
	Tools										
	Learn Azure with free online training from Microsoft		ind Security Center Secure your apps and Infrastructure	Cost Management Analyze and optimize your cloud spend for free							
	Useful links		4	Azure mobile app							
	Technical Documentation (2) Azure Migration Tools	Azure Services ©" Find an Azure expert	Recent Azure Updates 😅 Quickstart Center	App Store Google Play							



5. Confirm that the Overview blade displays a summary of Compliant devices and Noncompliant devices.

Note: To refresh the data, click Sync Report at the top-left corner of the Device Compliance blade.

■ Microsoft Azure	n resources, services, and docs	(G+/)							0		dallen@pretendcolife.o PRETENDCO LIFE
Home > Device compliance											
Device compliance											×
✓ Search (Cmd+/) «	Sync Report										
0 Overview	1 Data in this view was la	ist refreshed on 03/30/20 at 2:5	58:17 PM.								
Manage	Tenant name : pretend	co.life		Ð	MDM au	thority : M	icrosoft	Intune			
Policies	Tenant location :				Account	status : A	tive				
Notifications						1					
I Retire Noncompliant Devices	Devices without	Policy compliance									
Locations		Policy	Compliant devices	Noncompliant	devices						
Monitor	0.	macOS Security Policy	0	1							
Noncompliant devices	•••										
Devices without compliance pol											
Setting compliance											
Policy compliance											
Windows health attestation rep											
Threat agent status											
Setup											
Compliance policy settings	Setting compliance										
Ø Microsoft Defender ATP	Setting	Platform	Noncompliant devic								
Mobile Threat Defense	Minimum password le	ength macOS	1								
Partner device management	Encryption of data sto	rage on macOS	1								
Help and support	Allow apps download	ed from macOS	0								
Help and support	Minimum OS version	macOS	0								
	Require a password to	unlock macOS	0								
	Require system integr	ity prot macOS	0								
	Design and the star										

6. From the Policy compliance tile, click the policy you created in section 1 of this guide (this guide uses "macOS Security Policy" as an example).

E Microsoft Azure Search	resources, services, and docs (	G+/)				Q 🖗	•	? 😊	dallen@pretendcolife.o PRETENDCO LIFE		
Home > Device compliance											
<b>i</b> Device compliance									×		
, ♀ Search (Cmd+/) ≪	💍 Sync Report										
() Overview	Data in this view was las	t refreshed on 03/30/20 at 2	:58:17 PM.								
Manage	Tenant name : pretendo	o.life		D MDM a	uthority : Microsoft	t Intune					
Policies	renant location :			Account status : Active							
Notifications	Devices without	Policy compliance			\$						
Retire Noncompliant Devices		Policy	Compliant devices	Ioncompliant devices	<b>_</b>						
ey cocations	•	macOS Security Policy	0								
Noncompliant devices	U				1						
<ul> <li>Devices without compliance pol</li> </ul>											
Setting compliance											
Policy compliance											
Windows health attestation rep											
Threat agent status											
Setup									1		
Compliance policy settings	Setting compliance										
Microsoft Defender ATP	Setting	Platform	Noncompliant devic								
Restrict device management	Minimum password ler	ngth macOS	1								
Help and support	Encryption of data stor	age on macOS	1								
A Help and support	Allow apps downloade	a from macOS	0								
	Require a password to	unlock macOS	0								
	Require system integrit	ty prot macOS	0								



7. Confirm that the Device Compliance blade displays all devices with that policy assigned and if they are compliant or not compliant.

Ξ	Microsoft Azure	℅ Search resources, services, and docs (G+/)		۶.	Ģ	Ø	۲	?	۲	dallen@pretendcolife.o PRETENDCO LIFE			
÷	Home > Device compliance   Policy compliance > Device status												
	Device status									×			
	≡≡ Columns 🛓 Export												
	Data in this view is live.												
_	₽ Filter items												
Γ	Device	User Principal Name	Compliance status			Last	status i	update					
	13" MacBook Pro	dallen@pretendcolife.onmicrosoft.com	😵 Not Compliant			3/30/	20, 2:4	5 PM					
L													

8. To view the details for your test Mac, click its entry.

😑 Microsoft Azure 🔎 Sear	ch resources, services, and	docs (G+/)				D G	0	۲	?	٢	dallen@pretendcolife.o PRETENDCO LIFE
Home > Device compliance   Policy comp	pliance > Device status >	13" MacBook Pro									
13" MacBook Pro											×
✓ Search (Cmd+/) «	📋 Delete										
0 Overview	Device name	: 13" MacBook Pro			Primary user (preview	v) : None					
Manage	Management na	ime :			Enrolled by						
III Properties	Ownership	: Corporate			Compliance	: Not Co	mpliant				
Marilan	Serial number	: C02MW0B8FH05			Operating system	: Mac O	5 X				
Monitor	Phone number	:			Device model	: 13+inci	i Ketina N	ласвооя	( Pro (i	Late 2013	0
Hardware	See more			*							
Discovered apps											
bevice compliance	Device actions sta	itus									
Device configuration	Action	Status		Date/Time	Error						
App configuration	No data										
Endpoint security configuration											
B→ Recovery keys											
👶 Managed Apps											
						-					
X C manage A V F	righlight All Match Case	Match Diacritics Whole V	words 1 of 2 matches								



9. In the left blade, click "Device compliance."

≡	Microsoft Azure	₽ Search	resources, services, and docs (G+/)				2	G	¢ @	?	٢	dallen@pretendcolife.o PRETENDCO LIFE	
Ho	Home > 13* MacBook Pro   Device compliance												
13	13" MacBook Pro   Device compliance ×												
2	Search (Cmd+/)	«	↓ Export										
0	Overview		✓ Filter by name										
			Policy	τţ	User Principal Name		$\uparrow_{\downarrow}$	State				↑↓	
	Burnetin		macOS Security Policy		dallen@pretendcolife.onmicrosoft.com	m		😮 N	ot Compli	ant			
141	Properties		Built-in Device Compliance Policy		None			Not e	evaluated				
Mo	onitor												
6	Hardware												
d	Discovered apps												
Ľ,	Device compliance												
Ц	Device configuration												
1	App configuration												
•	Endpoint security configu	ration											
≜⇒	Recovery keys												
	Managed Apps												

10. Confirm that the Device compliance blade displays the list of policies that apply to your test Mac, along with the state of compliance for each policy.

Microsoft Azure     P Search resources, services, and docs (0)	i+/)	D 🗣 🗘 🎯 ? (	dallen@pretendcolife.o PRETENDCO LIFE								
Home > 13' MacBook Pro   Device compliance > macOS Security Policy											
macOS Security Policy Policy settings	×										
🞍 Export											
P Filter by name											
Setting	↑↓ State	↑↓ State Details	$\uparrow_{\downarrow}$								
Require system integrity protection	Compliant										
Minimum password length	Not Compliant										
Allow apps downloaded from these locations	Compliant										
Minimum OS version	Compliant										
Encryption of data storage on device.	8 Not Compliant										
Require a password to unlock devices.	Compliant										
		]									

- 11. Click the policy with a non-compliant state.
- 12. Confirm that the "macOS Security Policy" section displays a list of each setting and its state of compliance.

If you'd like help implementing the solution in this white paper, we are ready to help; contact us at info@hcsonline.com or (866) 518-9672.

If you have corrections please send them to info@hcsonline.com.

For more white papers, visit https://hcsonline.com/support/white-papers.

For more information about HCS, visit https://hcsonline.com.