jamf

Microsoft Intune

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

HCS TECHNOLOGY GROUP

Contents

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.

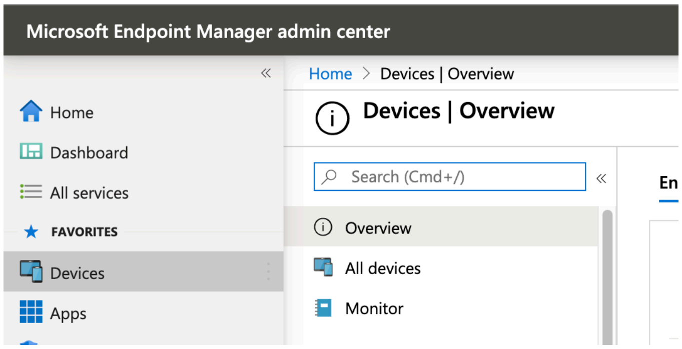
The compliance policy you create may vary depending on your organization's needs.

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.

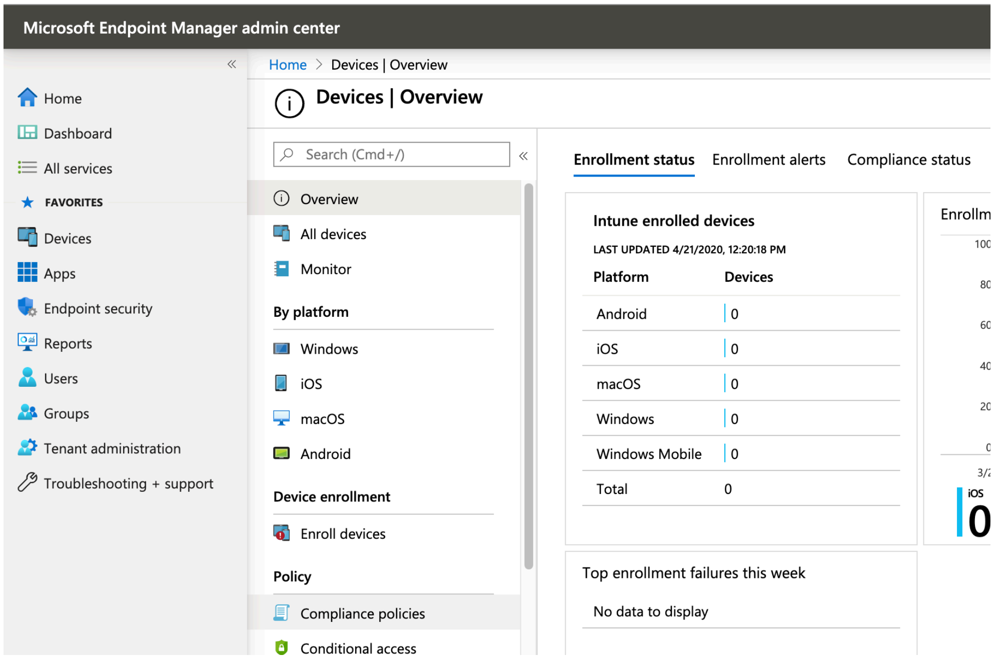
1. Open a new browser window or tab and navigate to https://devicemanagement.microsoft.com.

2. Log in with credentials for a global administrator or an Intune service administrator.

3. In the left blade, click Devices.



4. In the middle blade, Click Compliance Policies.



Intune enrolled devices

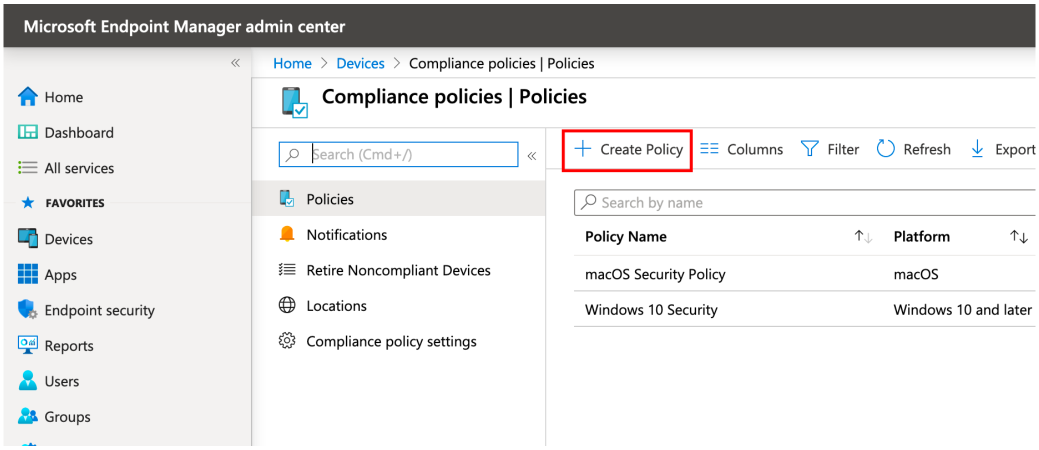
LAST UPDATED 4/21/2020, 12:20:18 PM

Platform	Devices
Android	0
iOS	0
macOS	0
Windows	0
Windows Mobile	0
Total	0

Top enrollment failures this week

No data to display

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



Policy Name	Platform
macOS Security Policy	macOS
Windows 10 Security	Windows 10 and later

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.

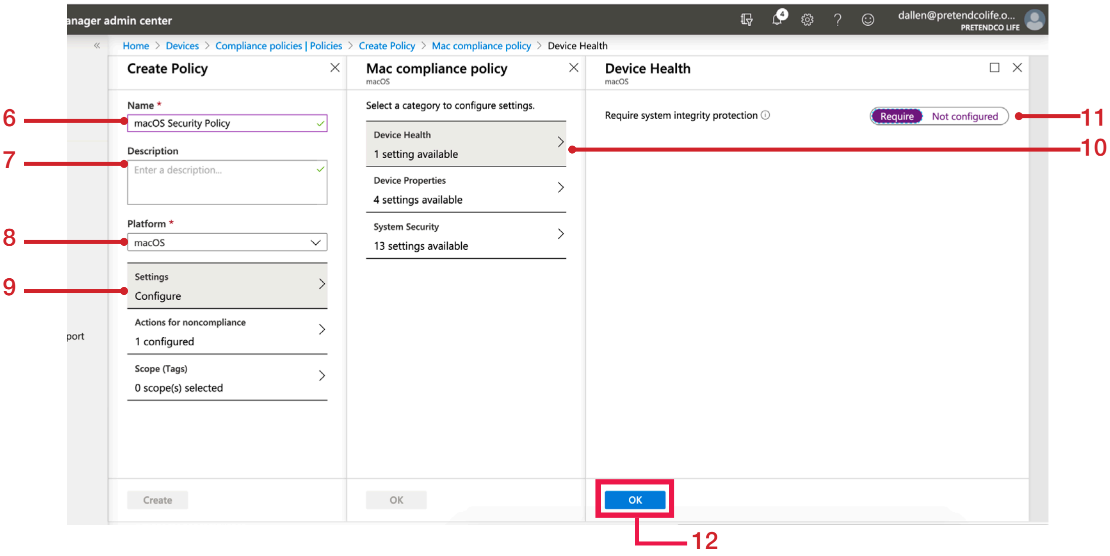
8. Click the Platform menu and choose macOS.

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



Name *: macOS Security Policy

Description: Enter a description...

Platform *: macOS

Settings: Configure

Actions for noncompliance: 1 configured

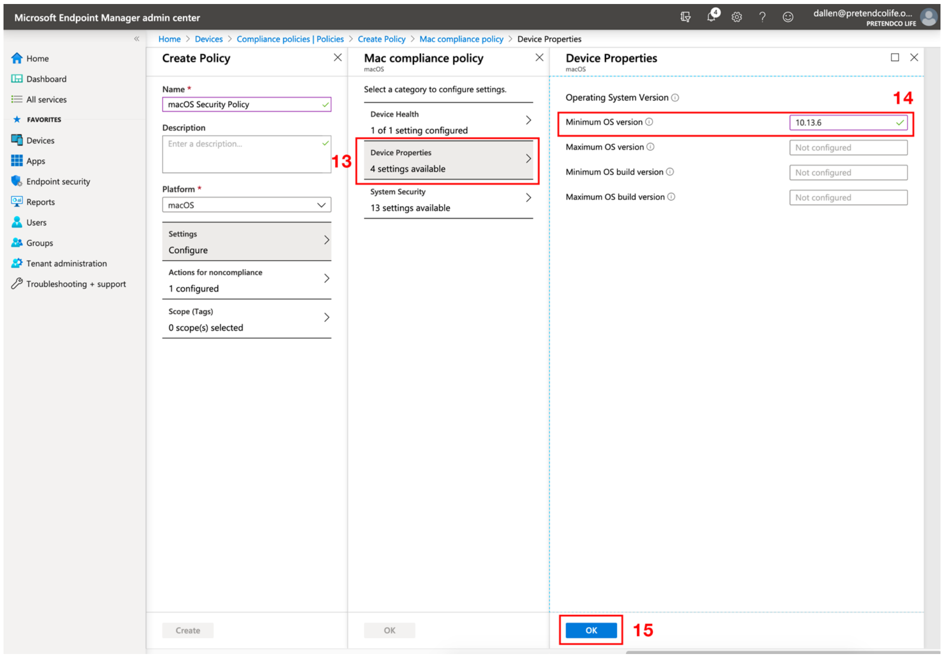
Scope (Tags): 0 scope(s) selected

Require system integrity protection: Require | Not configured

13. Click Device Properties.

14. In the “Minimum OS version” field, enter 10.13.6.

15. Click OK.


Microsoft Endpoint Manager admin center
dallen@pretendcolife.o...
PRETENDCO LIFE
Home > Devices > Compliance policies | Policies > Create Policy > Mac compliance policy > Device Properties
Home
Dashboard
All services
FAVORITES
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
13
14
15
Create
OK
OK

Create Policy

Name * macOS Security Policy

Description Enter a description...

Platform * macOS

Settings: Configure

Actions for noncompliance: 1 configured

Scope (Tags): 0 scope(s) selected

Mac compliance policy (macOS)

Select a category to configure settings.

Device Health: 1 of 1 setting configured

Device Properties: 4 settings available

System Security: 13 settings available

Device Properties (macOS)

Operating System Version

Minimum OS version: 10.13.6

Maximum OS version: Not configured

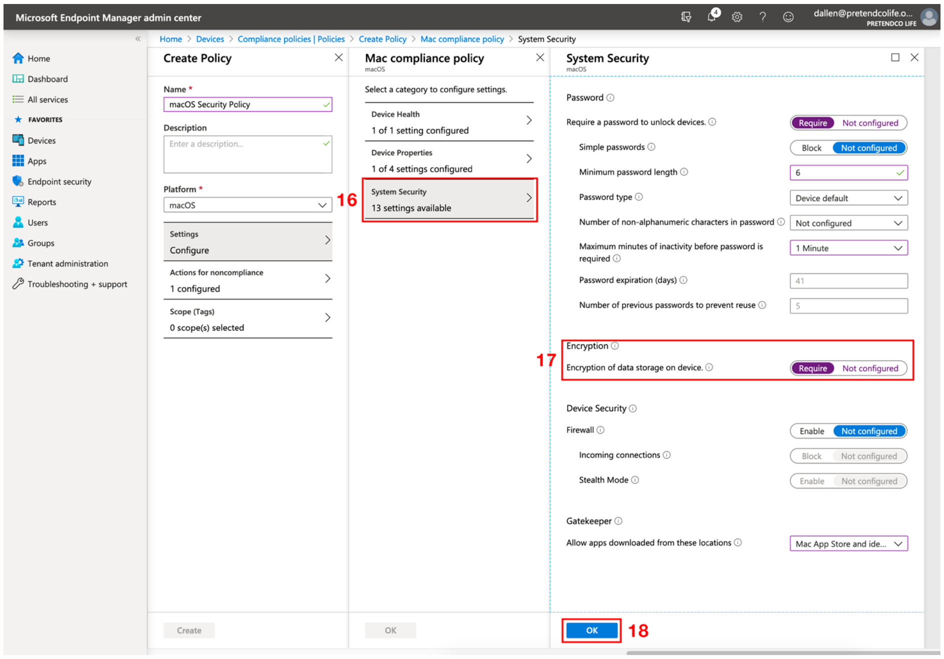
Minimum OS build version: Not configured

Maximum OS build version: Not configured

16. Click System Security.

17. Next to “Encryption of data storage on device,” click Require.”

18. Click OK.


Microsoft Endpoint Manager admin center
dallen@pretendcolife.o...
PRETENDCO LIFE
Home > Devices > Compliance policies | Policies > Create Policy > Mac compliance policy > System Security
Home
Dashboard
All services
FAVORITES
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
16
17
18
Create
OK
OK

Create Policy

Name * macOS Security Policy

Description Enter a description...

Platform * macOS

Settings: Configure

Actions for noncompliance: 1 configured

Scope (Tags): 0 scope(s) selected

Mac compliance policy (macOS)

Select a category to configure settings.

Device Health: 1 of 1 setting configured

Device Properties: 1 of 4 settings configured

System Security: 13 settings available

System Security (macOS)

Password

Require a password to unlock devices: [✓ Require] Not configured

Simple passwords: Block [✓ Not configured]

Minimum password length: 6

Password type: Device default

Number of non-alphanumeric characters in password: Not configured

Maximum minutes of inactivity before password is required: 1 Minute

Password expiration (days): 41

Number of previous passwords to prevent reuse: 5

Encryption

Encryption of data storage on device: [✓ Require] Not configured

Device Security

Firewall: Enable [✓ Not configured]

Incoming connections: Block Not configured

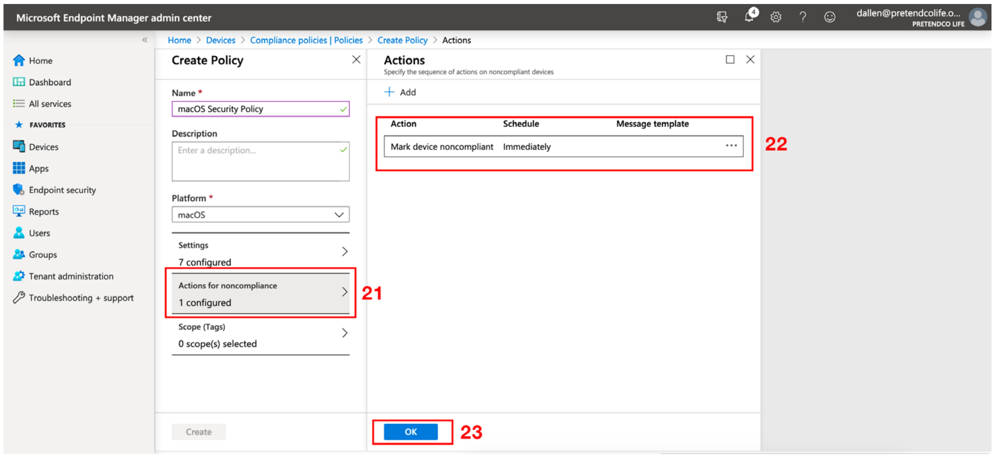
Stealth Mode: Enable Not configured

Gatekeeper

Allow apps downloaded from these locations: Mac App Store and ide...

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 admin center
dallen@pretendcolife.o...
PRETENDCO LIFE
Home > Devices > Compliance policies | Policies > Create Policy > Actions
Home
Dashboard
All services
FAVORITES
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Create Policy
Actions
Specify the sequence of actions on noncompliant devices
+ Add
Create
OK
21
22
23

Name * macOS Security Policy

Description Enter a description...

Platform * macOS

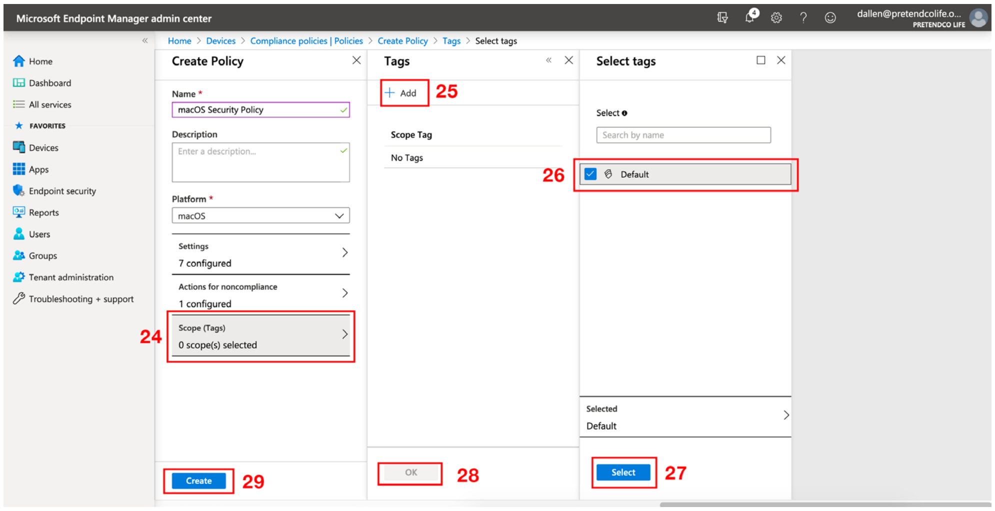
Settings 7 configured

Actions for noncompliance 1 configured

Scope (Tags) 0 scope(s) selected

Action	Schedule	Message template
Mark device noncompliant	Immediately	···

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



Name * macOS Security Policy

Description Enter a description...

Platform * macOS

Settings 7 configured

Actions for noncompliance 1 configured

Scope (Tags) 0 scope(s) selected

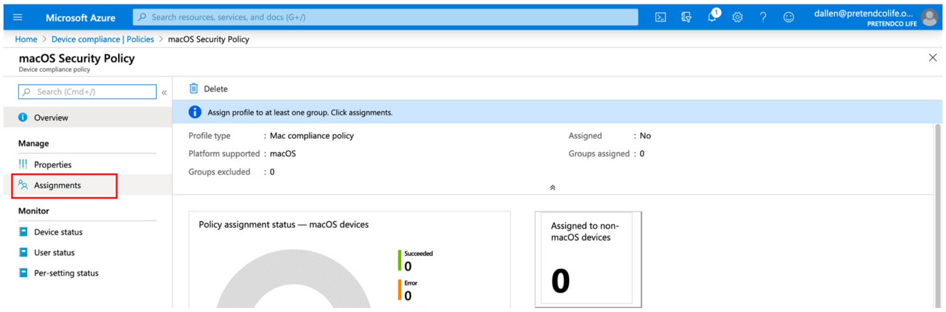
Scope Tag
No Tags

☑ Default

Selected Default

30. In the overview page of the policy you just created, configure the following:

A. In the left blade, click Assignments.



Assign profile to at least one group. Click assignments.

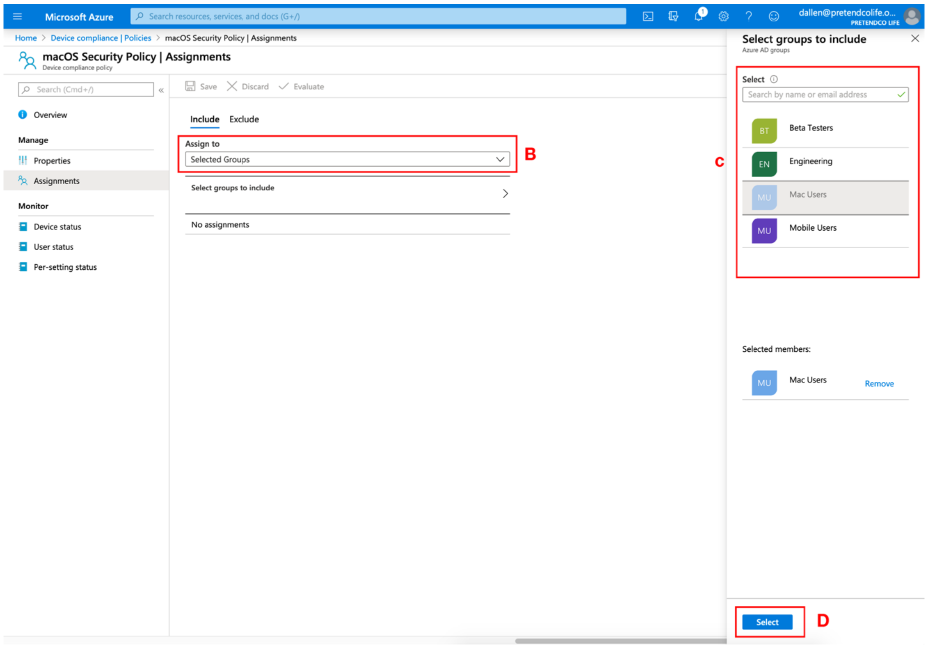
Profile type : Mac compliance policy
Platform supported : macOS
Groups excluded : 0
Assigned : No
Groups assigned : 0

Microsoft Azure
Search resources, services, and docs (G+/)
dallen@pretendcolife.o...
PRETENDCO LIFE
Home > Device compliance | Policies > macOS Security Policy
macOS Security Policy
Device compliance policy
Search (Cmd+/)
Delete
Overview
Manage
Properties
Assignments
Monitor
Device status
User status
Per-setting status
Policy assignment status — macOS devices
Succeeded
0
Error
0
Assigned to non-macOS devices
0

B. Click the “Assign to” menu and choose “Selected Groups.”

C. In the “Select Groups to include,” select the target group.

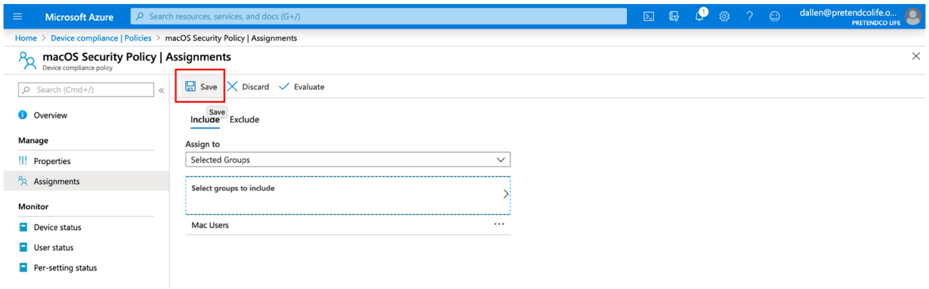
D. Click Select.



Assign to: Selected Groups

Selected members: Mac Users

E. Click Save.



Assign to: Selected Groups

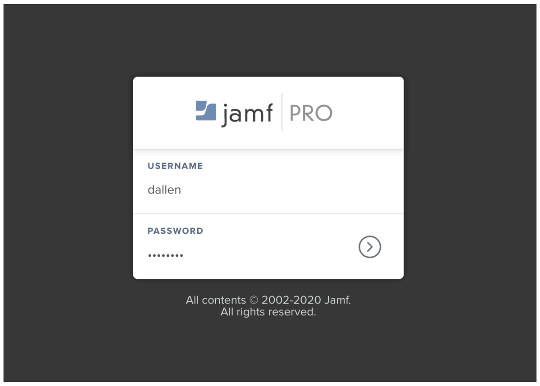
Mac Users

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.

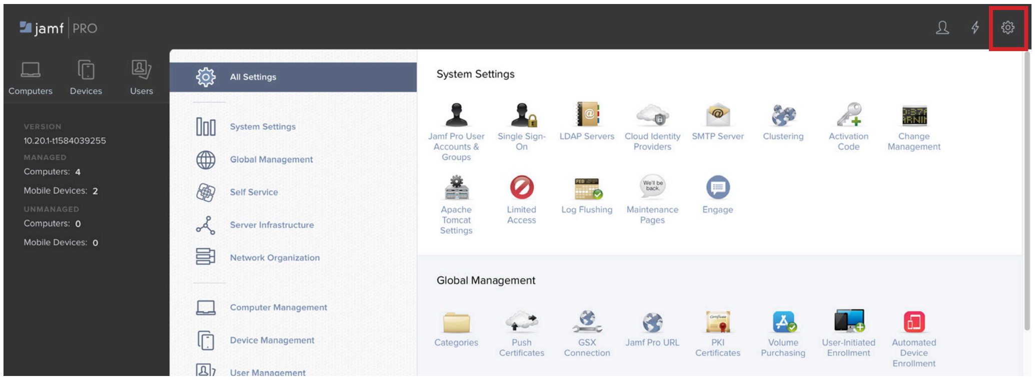


USERNAME
dallen

PASSWORD
••••••••

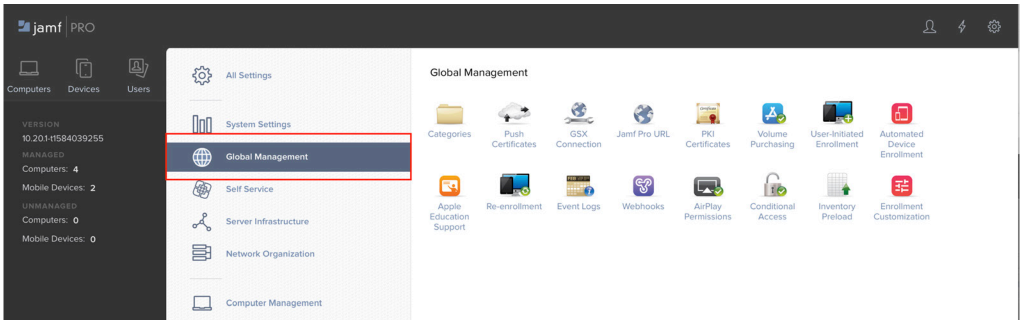
All contents © 2002-2020 Jamf.
All rights reserved.

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



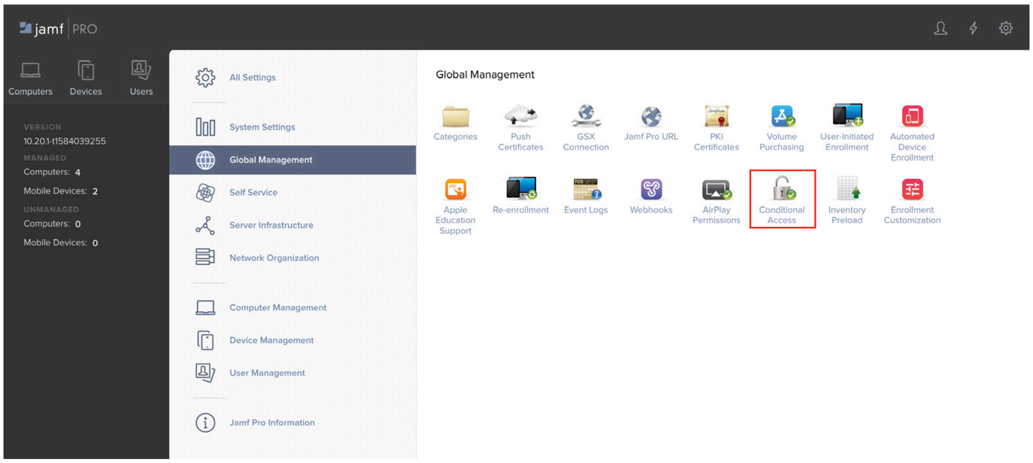
VERSION
10.20.1-t1584039255
MANAGED
Computers: 4
Mobile Devices: 2
UNMANAGED
Computers: 0
Mobile Devices: 0

4. In the middle column, click Global Management.



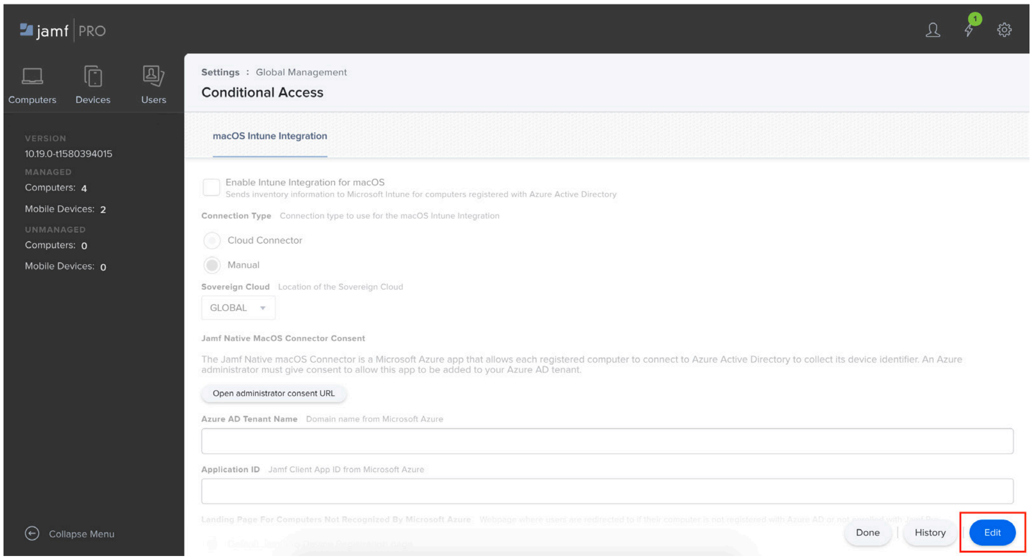
VERSION
10.20.1-t1584039255
MANAGED
Computers: 4
Mobile Devices: 2
UNMANAGED
Computers: 0
Mobile Devices: 0

5. Click Conditional Access.



VERSION
10.20.1-t1584039255
MANAGED
Computers: 4
Mobile Devices: 2
UNMANAGED
Computers: 0
Mobile Devices: 0

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



VERSION
10.19.0-t1580394015
MANAGED
Computers: 4
Mobile Devices: 2
UNMANAGED
Computers: 0
Mobile Devices: 0

Conditional Access

□ Enable 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

Sovereign Cloud Location of the Sovereign Cloud

GLOBAL

Jamf Native MacOS Connector Consent

The Jamf Native macOS Connector is a Microsoft Azure app that allows each registered computer to connect to Azure Active Directory to collect its device identifier. An Azure administrator must give consent to allow this app to be added to your Azure AD tenant.

Azure AD Tenant Name Domain name from Microsoft Azure

Application ID Jamf Client App ID from Microsoft Azure

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

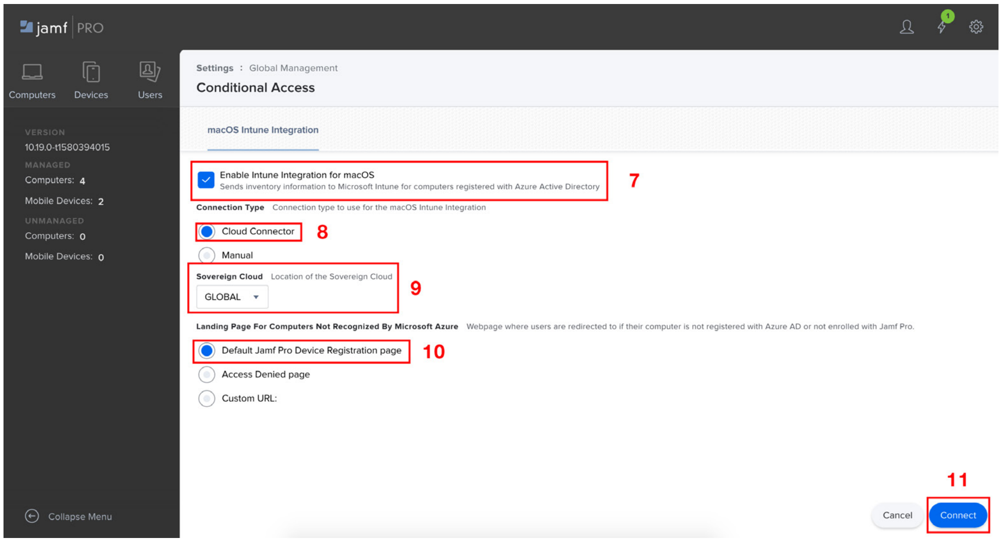
7. Select the checkbox for the “Enable Intune Integration for macOS” option.

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.



VERSION
10.19.0-t1580394015
MANAGED
Computers: 4
Mobile Devices: 2
UNMANAGED
Computers: 0
Mobile Devices: 0

Settings : Global Management

Conditional Access

macOS Intune Integration

☑ Enable Intune Integration for macOS
Sends inventory information to Microsoft Intune for computers registered with Azure Active Directory

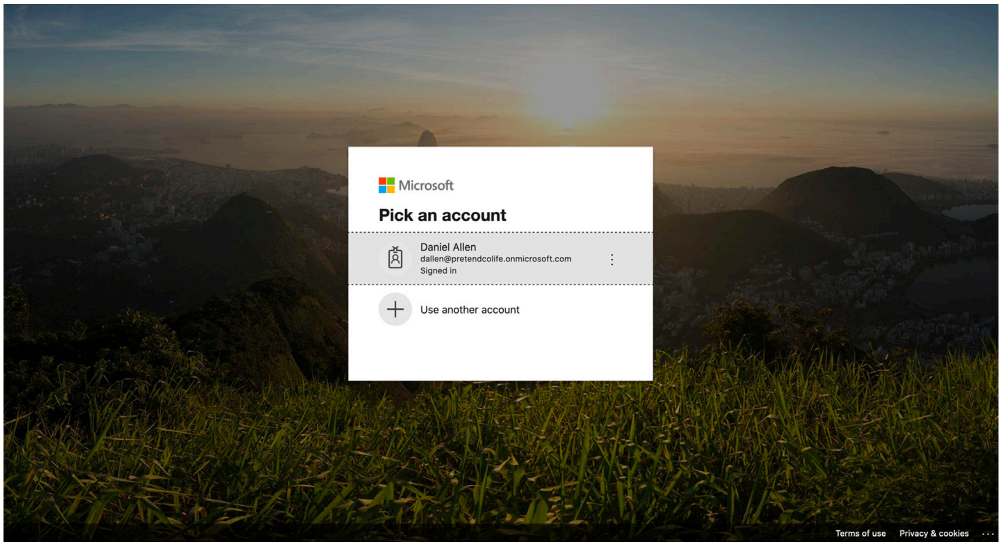
Connection Type Connection type to use for the macOS Intune Integration
● Cloud Connector
○ Manual

Sovereign Cloud Location of the Sovereign Cloud
GLOBAL ▾

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.
● Default Jamf Pro Device Registration page
○ Access Denied page
○ Custom URL:

12. Confirm that you’re redirected to the application registration page in Microsoft.

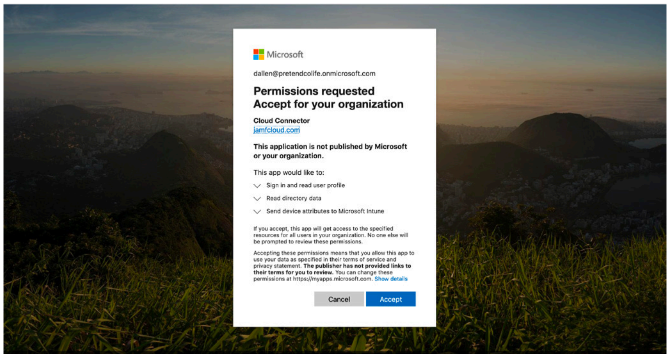
13. Log in again with a Microsoft Azure global administrator or an Intune service administrator account.



Pick an account

Daniel Allen
dallen@pretendcolife.onmicrosoft.com
Signed in

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



dallen@pretendcolife.onmicrosoft.com

Permissions requested
Accept for your organization

Cloud Connector
jamfcloud.com

This application is not published by Microsoft or your organization.

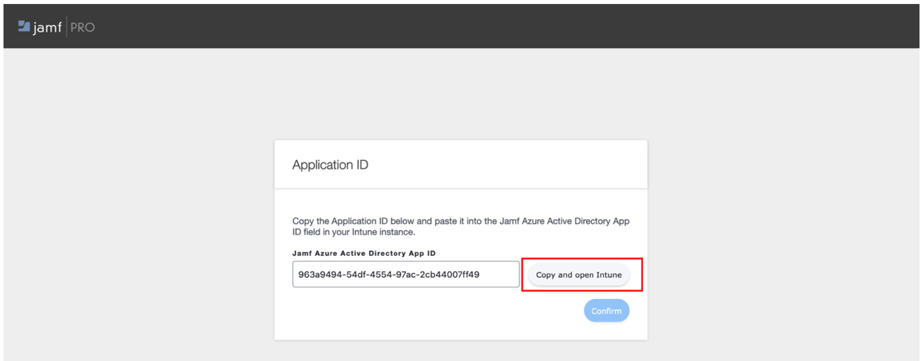
This app would like to:

- Sign in and read user profile
- Read directory data
- Send device attributes to Microsoft Intune

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at https://myapps.microsoft.com. Show details

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."

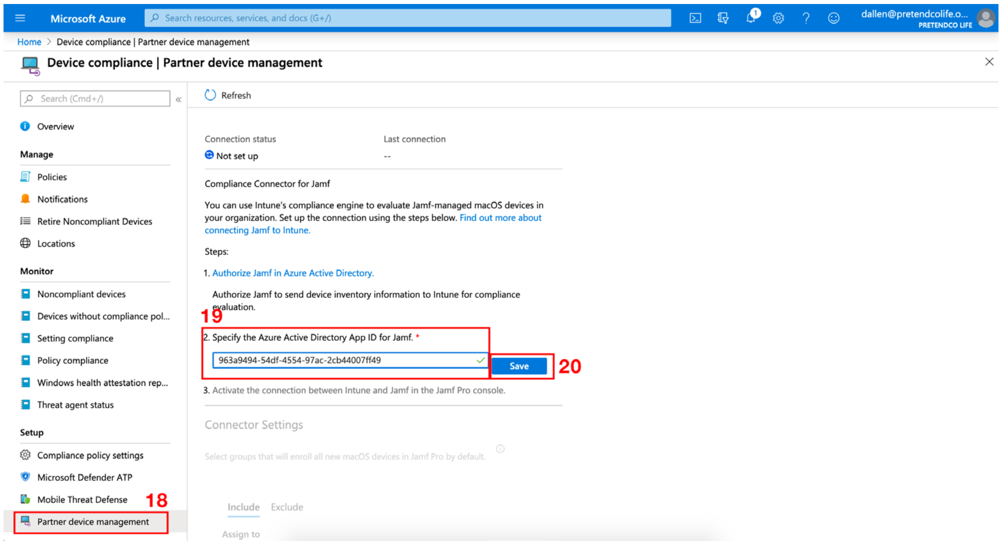


Application ID

Copy the Application ID below and paste it into the Jamf Azure Active Directory App ID field in your Intune instance.

Jamf Azure Active Directory App ID: 963a9494-54df-4554-97ac-2cb44007ff49

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 resources, services, and docs (G+/)
dallen@pretendcolife.o...
PRETENDCO LIFE
Home > Device compliance | Partner device management

Device compliance | Partner device management

Search (Cmd+/)
Overview
Manage
Policies
Notifications
Retire Noncompliant Devices
Locations
Monitor
Noncompliant devices
Devices without compliance pol...
Setting compliance
Policy compliance
Windows health attestation rep...
Threat agent status
Setup
Compliance policy settings
Microsoft Defender ATP
Mobile Threat Defense
18
Partner device management
Refresh

Connection status: Not set up
Last connection: --

Compliance Connector for Jamf

You can use Intune's compliance engine to evaluate Jamf-managed macOS devices in your organization. Set up the connection using the steps below. Find out more about connecting Jamf to Intune.

Steps:

1. Authorize Jamf in Azure Active Directory.

   Authorize Jamf to send device inventory information to Intune for compliance evaluation.

2. Specify the Azure Active Directory App ID for Jamf. *

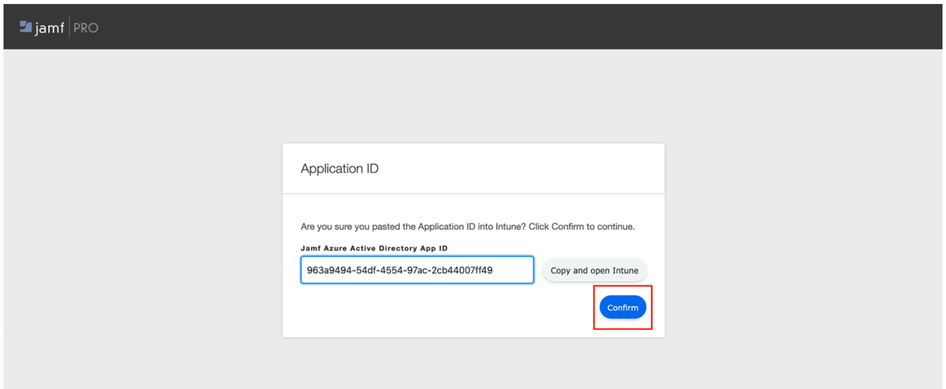
   963a9494-54df-4554-97ac-2cb44007ff49

3. Activate the connection between Intune and Jamf in the Jamf Pro console.

Connector Settings

Select groups that will enroll all new macOS devices in Jamf Pro by default.

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



Application ID

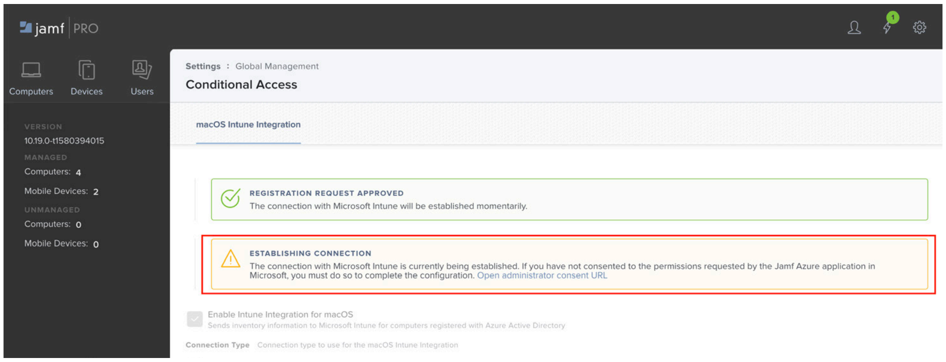
Are you sure you pasted the Application ID into Intune? Click Confirm to continue.

Jamf Azure Active Directory App ID

963a9494-54df-4554-97ac-2cb44007ff49

22. Confirm that you're redirected to the Conditional Access page in Jamf Pro.

23. You may see a yellow “Establishing Connection” notification.



VERSION
10.19.0-t1580394015
MANAGED
Computers: 4
Mobile Devices: 2
UNMANAGED
Computers: 0
Mobile Devices: 0

Conditional Access

REGISTRATION REQUEST APPROVED
The connection with Microsoft Intune will be established momentarily.

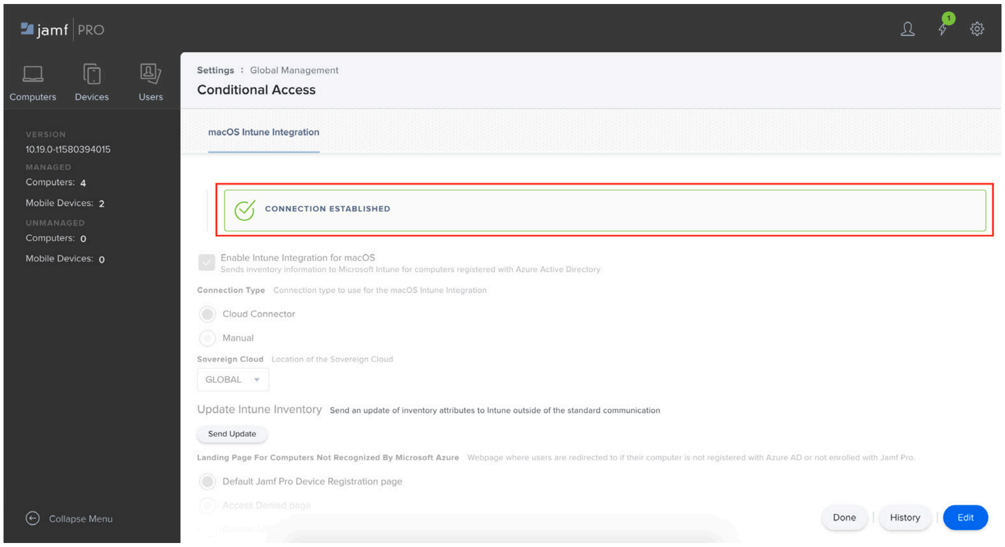
ESTABLISHING CONNECTION
The connection with Microsoft Intune is currently being established. If you have not consented to the permissions requested by the Jamf Azure application in Microsoft, you must do so to complete the configuration. Open administrator consent URL

☑ Enable 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

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

25. Confirm you see a green “Connection Established” notification.



VERSION
10.19.0-t1580394015
MANAGED
Computers: 4
Mobile Devices: 2
UNMANAGED
Computers: 0
Mobile Devices: 0

Conditional Access

CONNECTION ESTABLISHED

☑ Enable 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

Sovereign Cloud Location of the Sovereign Cloud

GLOBAL

Update Intune Inventory Send an update of inventory attributes to Intune outside of the standard communication

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.

● Default Jamf Pro Device Registration page
○ Access Denied page

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

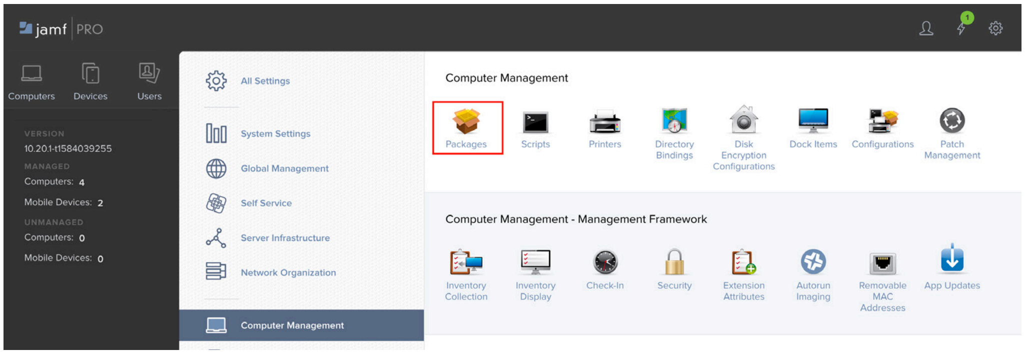
Microsoft Intune helps organizations manage access to corporate apps, data, and resources. Company Portal is the app that lets you, as an employee of your company, securely access those resources. The Company Portal Application is used to register the user's device with Azure Active Directory.

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.

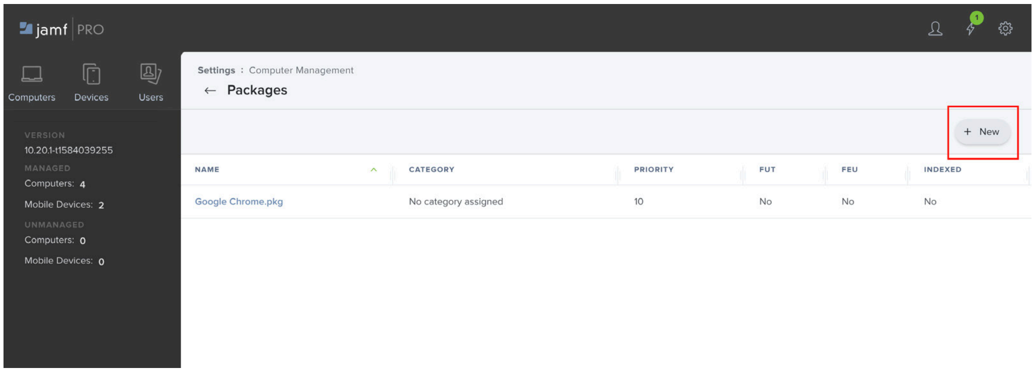
Upload the Microsoft Company Portal Application Package

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



VERSION
10.20.1-t1584039255
MANAGED
Computers: 4
Mobile Devices: 2
UNMANAGED
Computers: 0
Mobile Devices: 0

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



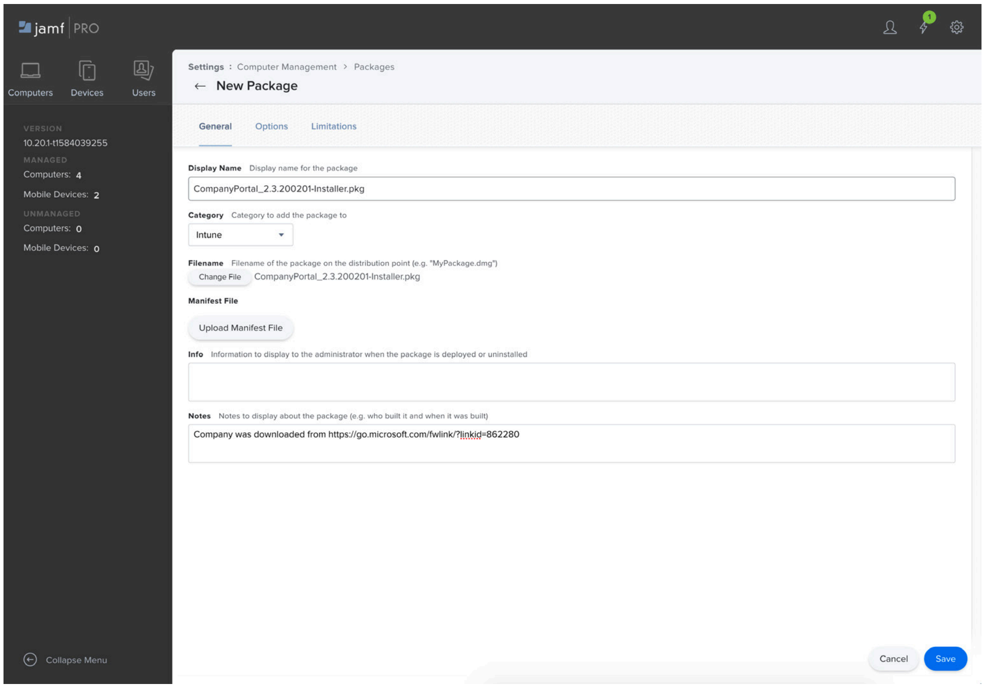
VERSION
10.20.1-t1584039255
MANAGED
Computers: 4
Mobile Devices: 2
UNMANAGED
Computers: 0
Mobile Devices: 0

NAME	CATEGORY	PRIORITY	FUT	FEU	INDEXED
Google Chrome.pkg	No category assigned	10	No	No	No

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.



Display Name Display name for the package
CompanyPortal_2.3.200201-Installer.pkg

Category Category to add the package to
Intune

Filename Filename of the package on the distribution point (e.g. "MyPackage.dmg")
Change File CompanyPortal_2.3.200201-Installer.pkg

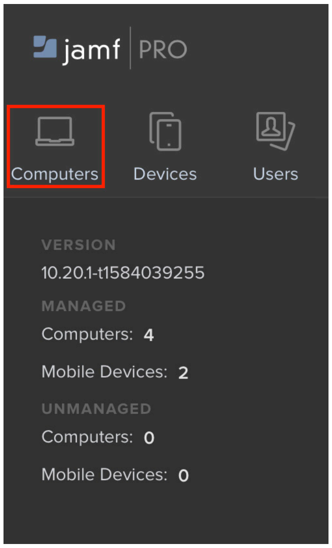
Manifest File
Upload Manifest File

Info Information to display to the administrator when the package is deployed or uninstalled

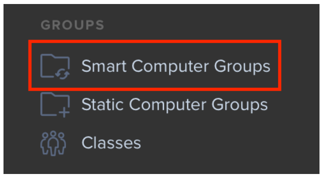
Notes Notes to display about the package (e.g. who built it and when it was built)
Company was downloaded from https://go.microsoft.com/fwlink/?linkid=862280

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

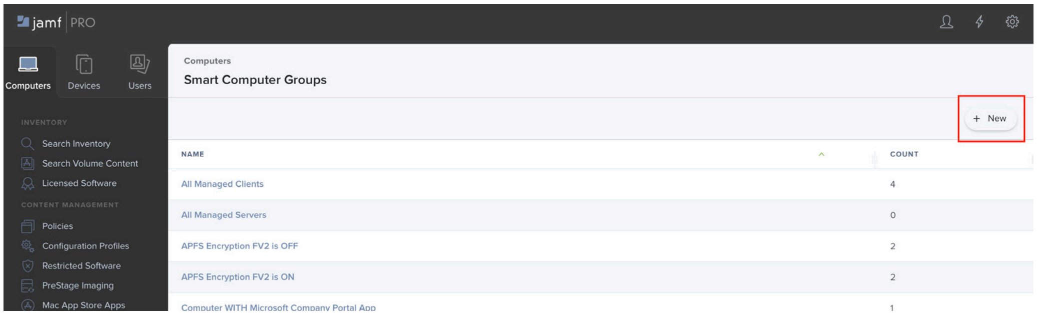
1. In the upper-left corner, click Computers.



2. In the sidebar, click Smart Computer Groups.

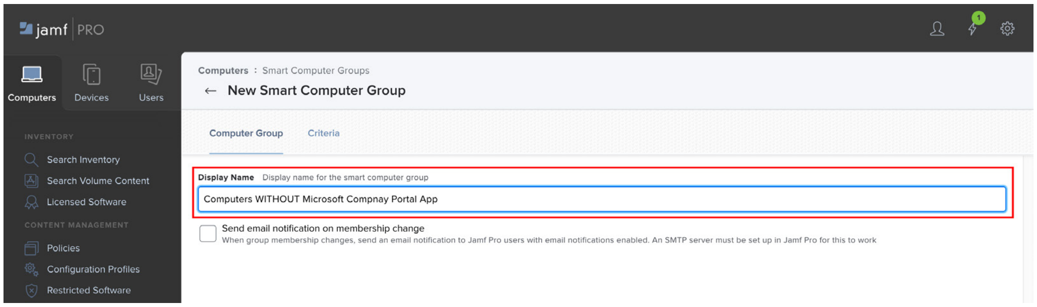


3. In the upper-right corner, click New.



NAME	COUNT
All Managed Clients	4
All Managed Servers	0
APFS Encryption FV2 is OFF	2
APFS Encryption FV2 is ON	2
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.

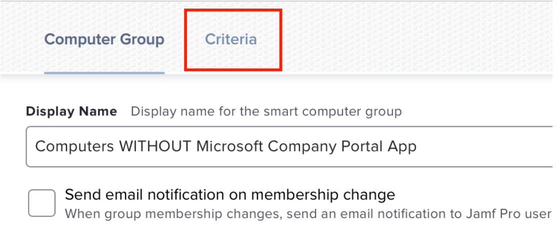


Display Name Display name for the smart computer group

Computers WITHOUT Microsoft Compnay 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

5. Click the Criteria tab.

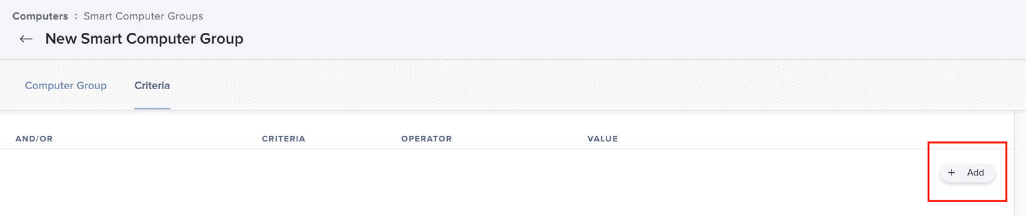


Display Name Display name for the smart computer group

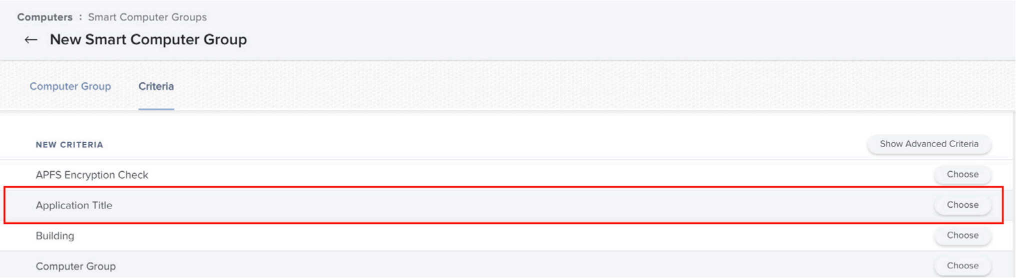
Computers WITHOUT Microsoft Company Portal App

□ Send email notification on membership change
When group membership changes, send an email notification to Jamf Pro user

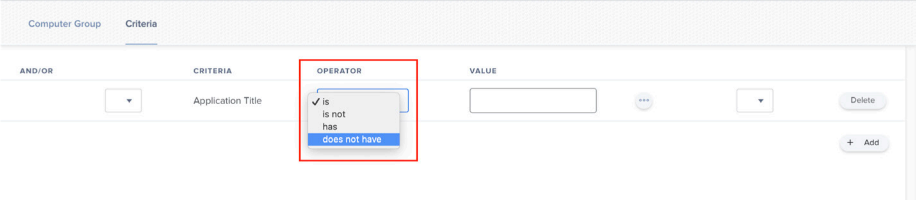
6. Click Add.



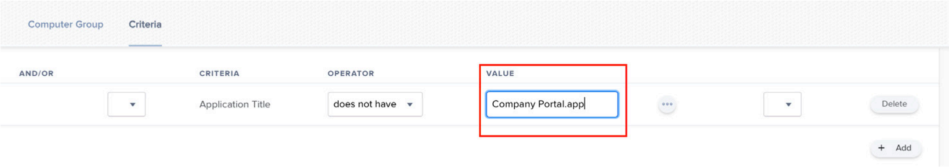
7. Click Choose to the right of Application Title.



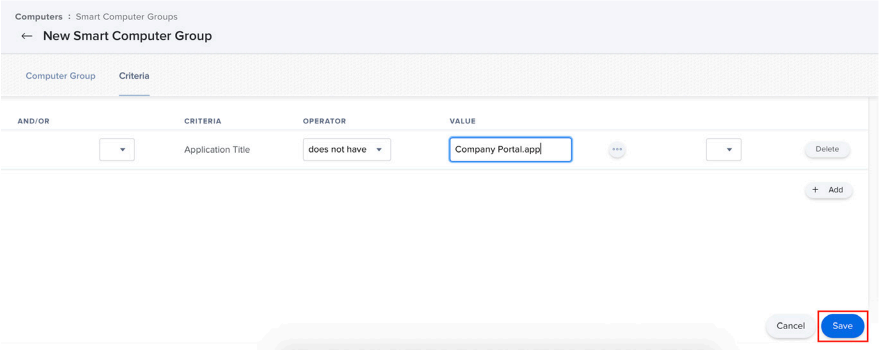
8. Click the Operator menu and choose “Does Not Have.”



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



10. Click Save.

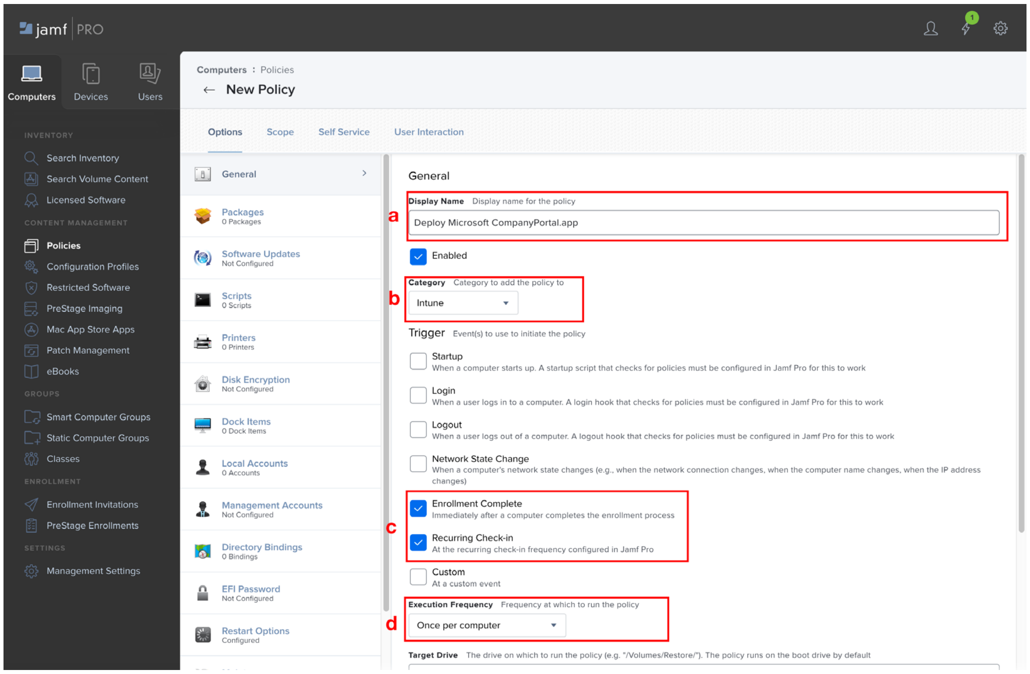


Create a policy to install Company Portal app

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.”



General

Display Name Display name for the policy
Deploy Microsoft CompanyPortal.app

☑ Enabled

Category Category to add the policy to
Intune

Trigger Event(s) to use to initiate the policy

☐ Startup
When a computer starts up. A startup script that checks for policies must be configured in Jamf Pro for this to work

☐ Login
When a user logs in to a computer. A login hook that checks for policies must be configured in Jamf Pro for this to work

☐ Logout
When a user logs out of a computer. A logout hook that checks for policies must be configured in Jamf Pro for this to work

☐ Network State Change
When a computer's network state changes (e.g., when the network connection changes, when the computer name changes, when the IP address changes)

☑ Enrollment Complete
Immediately after a computer completes the enrollment process

☑ Recurring Check-in
At the recurring check-in frequency configured in Jamf Pro

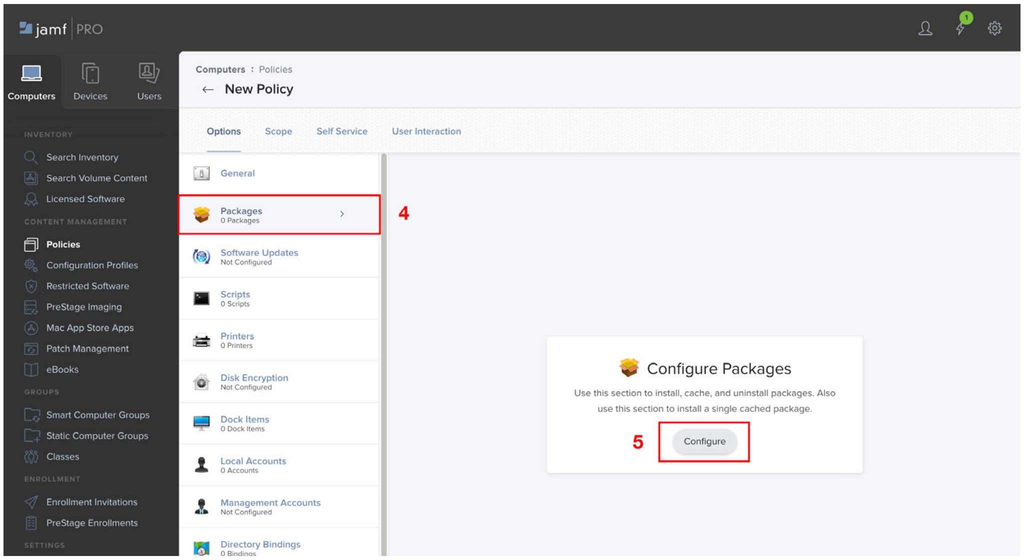
☐ Custom
At a custom event

Execution Frequency Frequency at which to run the policy
Once per computer

Target Drive The drive on which to run the policy (e.g. "/Volumes/Restore/"). The policy runs on the boot drive by default

4. In the list of payloads, select Packages.

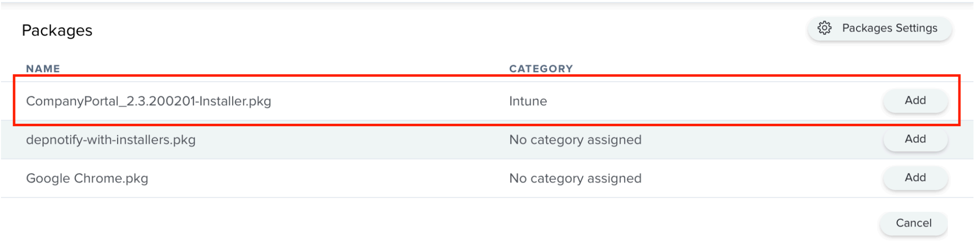
5. Click Configure.



Configure Packages

Use this section to install, cache, and uninstall packages. Also use this section to install a single cached package.

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

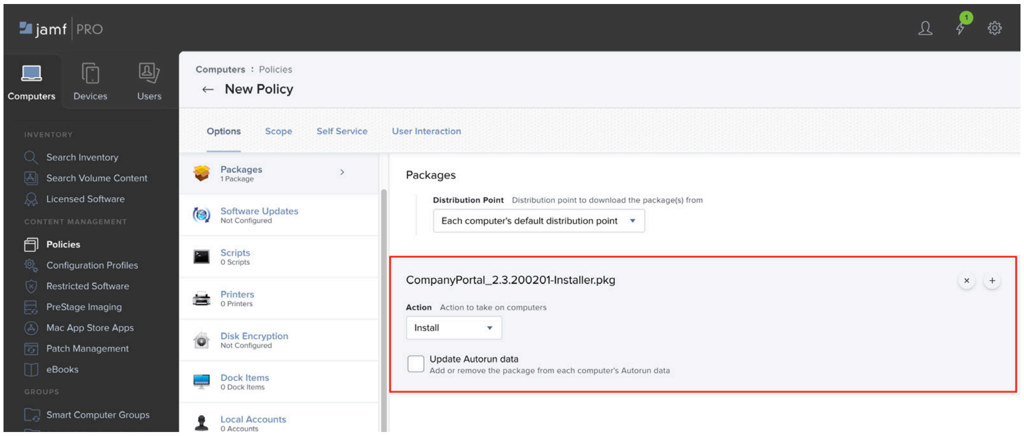


Packages

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

7. Optional: Click the Distribution Point menu and choose an appropriate distribution point.

8. Leave the Action menu at its default value of Install.



Computers : Policies

New Policy

Packages

Distribution Point — Distribution point to download the package(s) from: Each computer's default distribution point

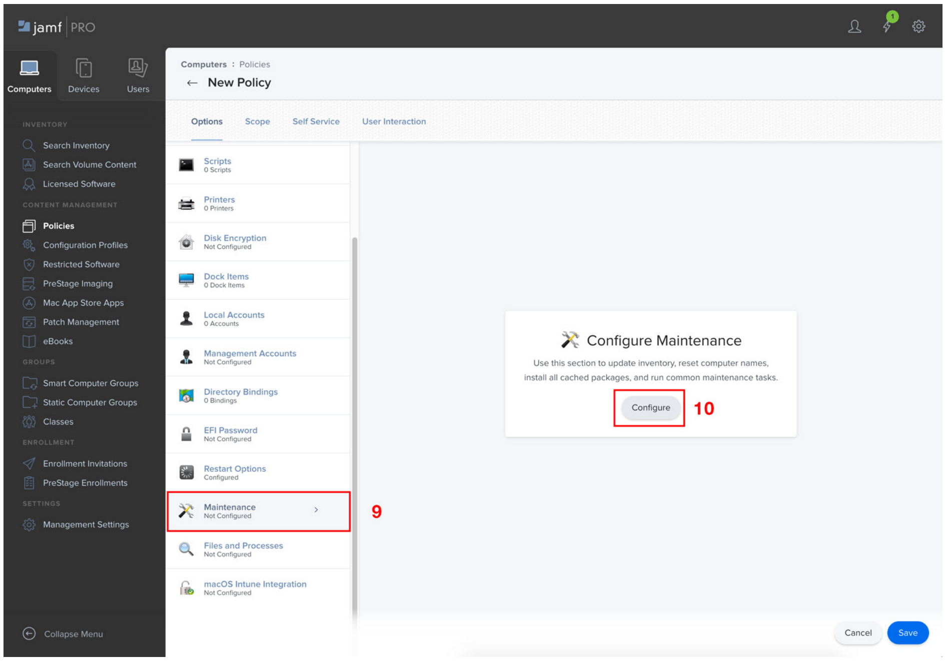
CompanyPortal_2.3.200201-Installer.pkg

Action — Action to take on computers: Install

☐ Update Autorun data
Add or remove the package from each computer's Autorun data

9. Click the Maintenance payload.

10. Click Configure.



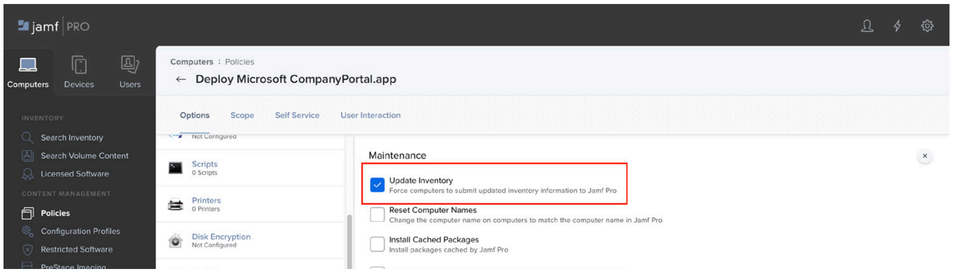
Computers : Policies

New Policy

Configure Maintenance

Use this section to update inventory, reset computer names, install all cached packages, and run common maintenance tasks.

11. Confirm that the checkbox Update Inventory is selected.

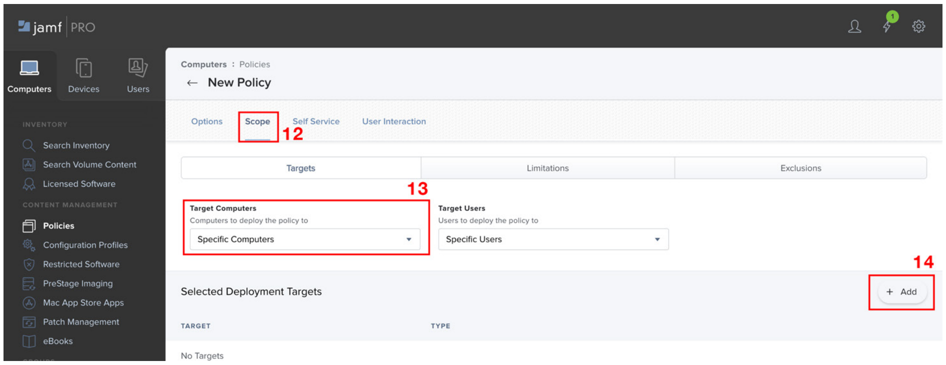


☑ Update Inventory
Force computers to submit updated inventory information to Jamf Pro

□ Reset Computer Names
Change the computer name on computers to match the computer name in Jamf Pro

□ Install Cached Packages
Install packages cached by Jamf Pro

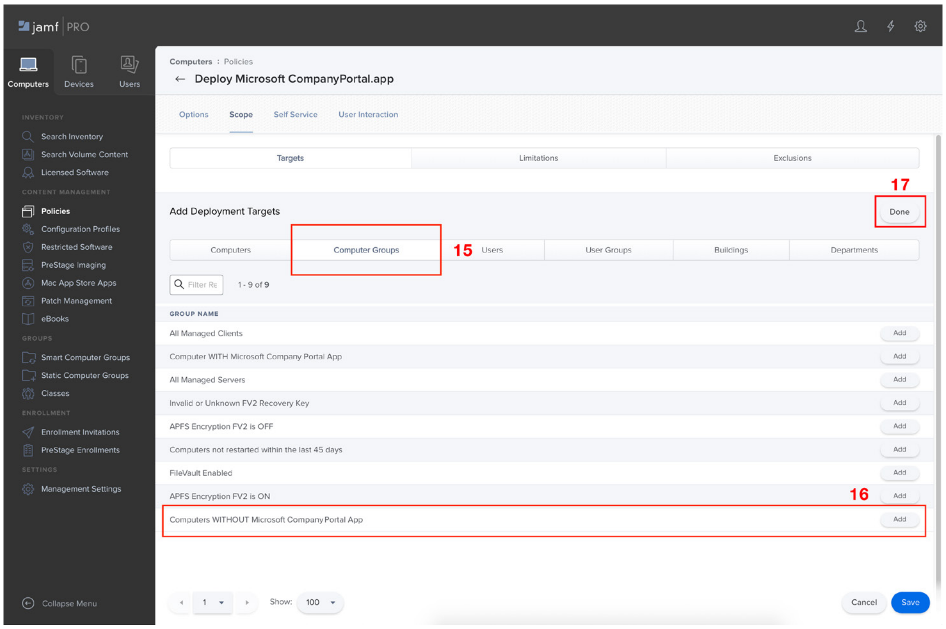
12. Click the Scope tab.
13. Leave the Target Computers menu at its default value of Specific Computers.
14. Next to Selected Deployment Targets, click Add.



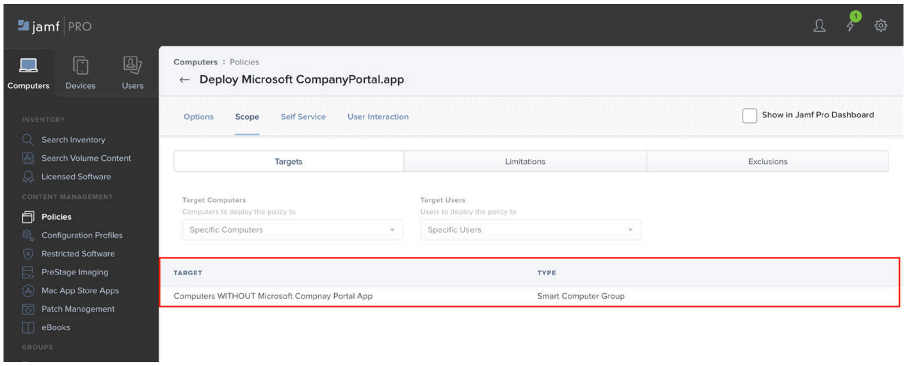
Target Computers
Computers to deploy the policy to
Specific Computers

Target Users
Users to deploy the policy to
Specific Users

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.



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



← Deploy Microsoft CompanyPortal.app

□ Show in Jamf Pro Dashboard

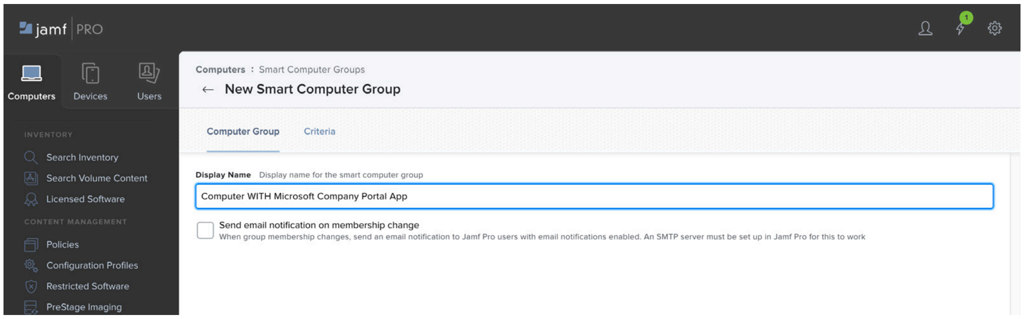
Target Computers: Specific Computers

Target Users: Specific Users

TARGET	TYPE
Computers WITHOUT Microsoft Compnay Portal App	Smart 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.

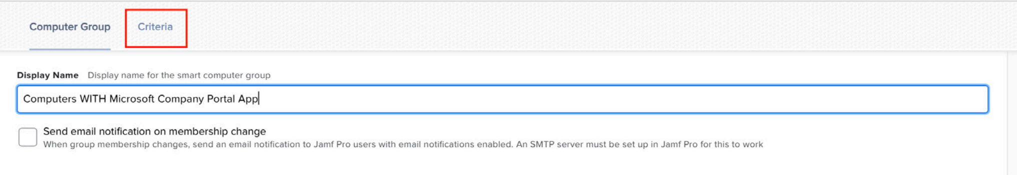


← New Smart Computer Group

Display Name: Computer 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

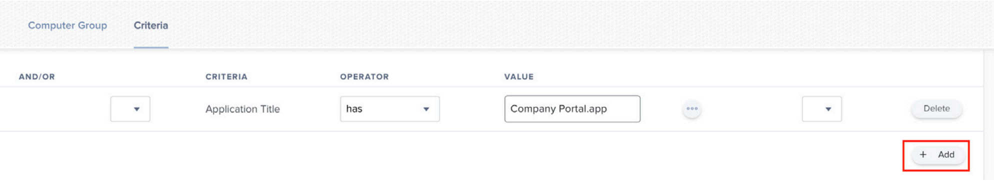
5. Click the Criteria tab.



Display Name: Computers WITH Microsoft Company Portal App

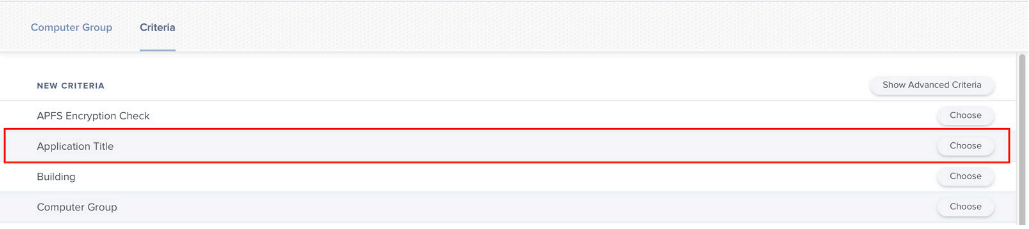
□ Send email notification on membership change
When group membership changes, send an email notification to Jamf Pro users with email notifications enabled. An SMTP server must be set up in Jamf Pro for this to work

6. Click Add.



AND/OR	CRITERIA	OPERATOR	VALUE
	Application Title	has	Company Portal.app

7. Next to Application Title, click Choose.

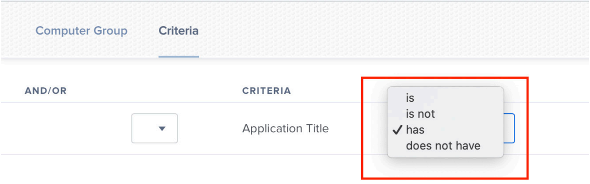


Computer Group | Criteria

NEW CRITERIA — Show Advanced Criteria

APFS Encryption Check	Choose
Application Title	Choose
Building	Choose
Computer Group	Choose

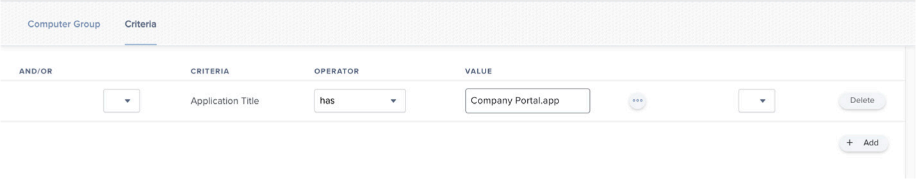
8. Click the Operator menu and choose “Has.”



Computer Group | Criteria

AND/OR	CRITERIA	
▾	Application Title	is is not ✓ has does not have

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

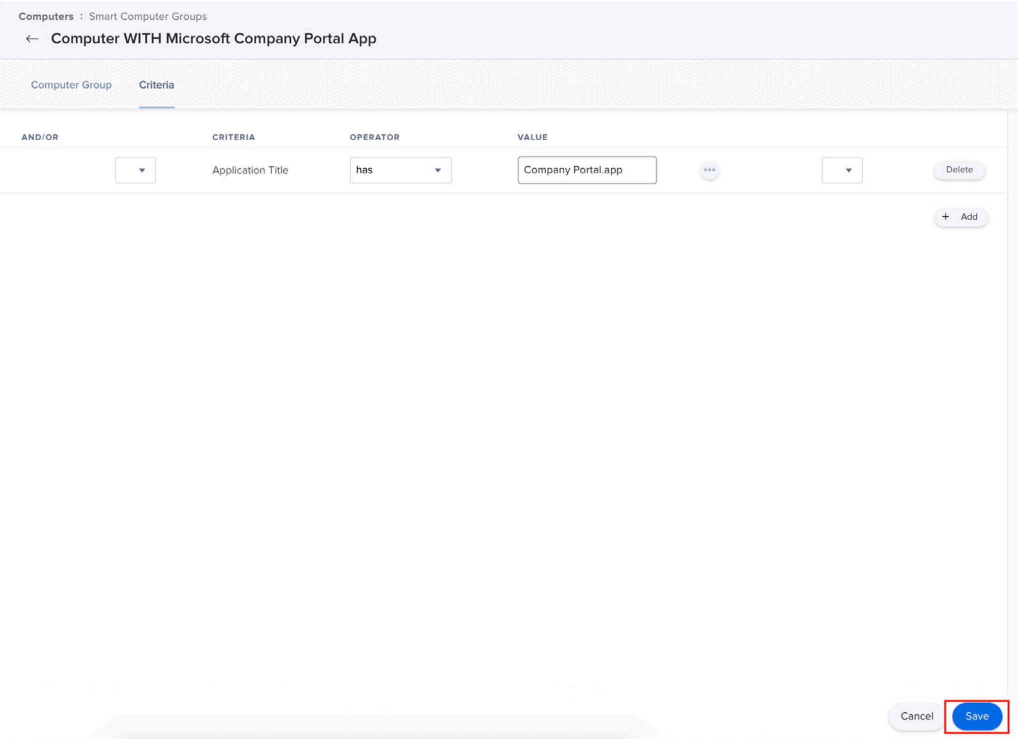


Computer Group | Criteria

AND/OR	CRITERIA	OPERATOR	VALUE			
▾	Application Title	has ▾	Company Portal.app	•••	▾	Delete

+ Add

10. Click Save.



Computers : Smart Computer Groups

← Computer WITH Microsoft Company Portal App

Computer Group | Criteria

AND/OR	CRITERIA	OPERATOR	VALUE			
▾	Application Title	has ▾	Company Portal.app	•••	▾	Delete

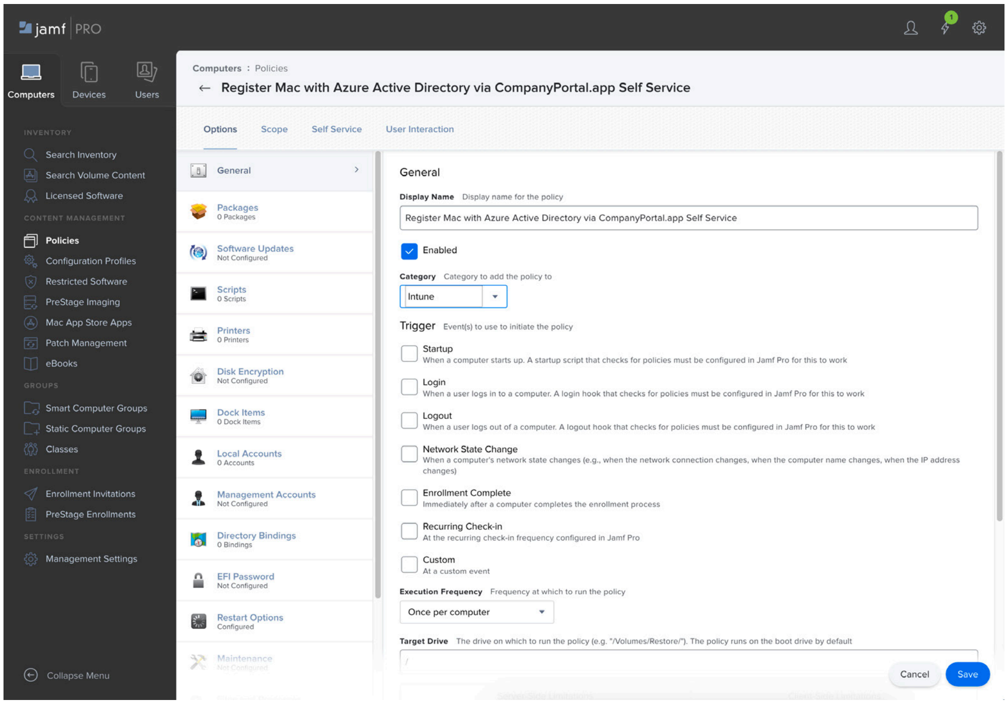
+ Add

Cancel | Save

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."



← Register Mac with Azure Active Directory via CompanyPortal.app Self Service

General

Display Name Display name for the policy

Register Mac with Azure Active Directory via CompanyPortal.app Self Service

☑ Enabled

Category Category to add the policy to

Intune

Trigger Event(s) to use to initiate the policy

☐ Startup
When a computer starts up. A startup script that checks for policies must be configured in Jamf Pro for this to work

☐ Login
When a user logs in to a computer. A login hook that checks for policies must be configured in Jamf Pro for this to work

☐ Logout
When a user logs out of a computer. A logout hook that checks for policies must be configured in Jamf Pro for this to work

☐ Network State Change
When a computer's network state changes (e.g., when the network connection changes, when the computer name changes, when the IP address changes)

☐ Enrollment Complete
Immediately after a computer completes the enrollment process

☐ Recurring Check-in
At the recurring check-in frequency configured in Jamf Pro

☐ Custom
At a custom event

Execution Frequency Frequency at which to run the policy

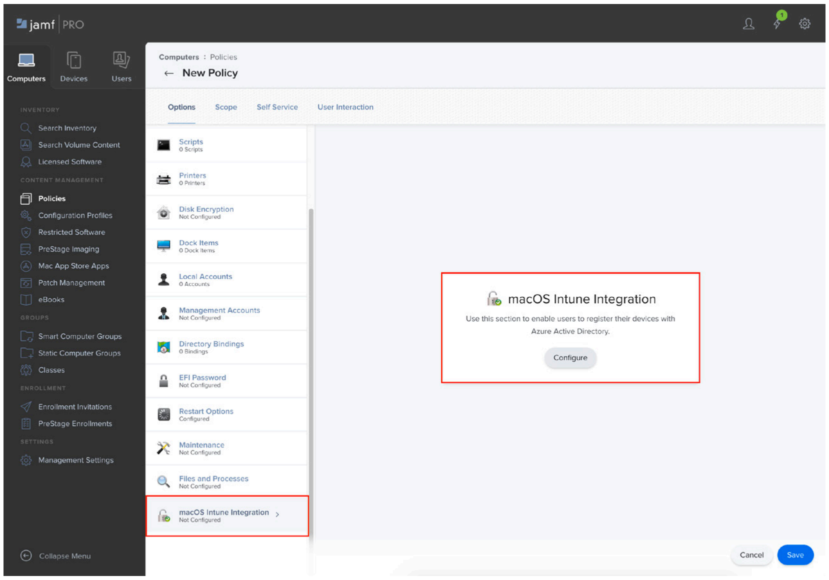
Once per computer

Target Drive The drive on which to run the policy (e.g. "/Volumes/Restore/"). The policy runs on the boot drive by default

/

5. Select the macOS Intune Integration payload then:

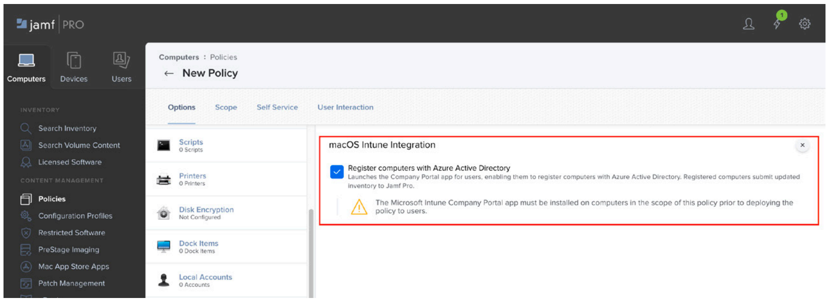
A. Click Configure.



macOS Intune Integration

Use this section to enable users to register their devices with Azure Active Directory.

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

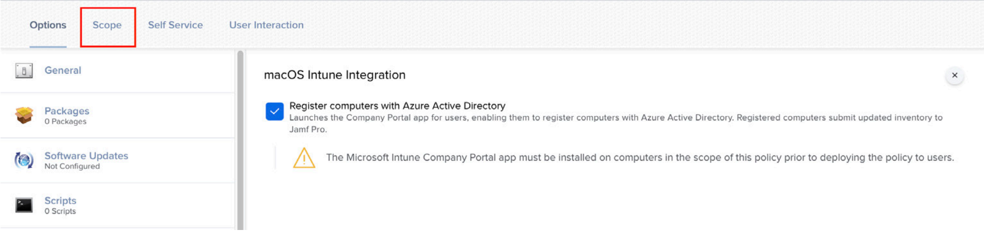


macOS Intune Integration

☑ 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 Jamf Pro.

⚠ The Microsoft Intune Company Portal app must be installed on computers in the scope of this policy prior to deploying the policy to users.

6. Click the Scope tab.

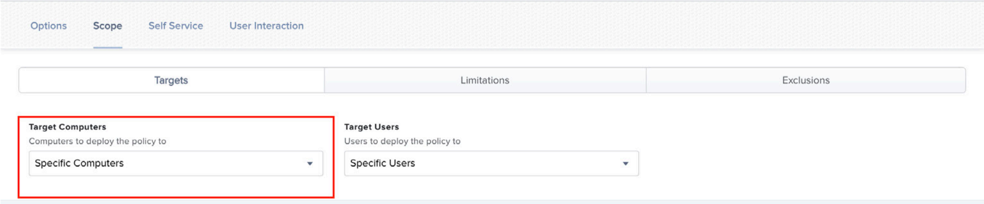


macOS Intune Integration

☑ 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 Jamf Pro.

⚠ The Microsoft Intune Company Portal app must be installed on computers in the scope of this policy prior to deploying the policy to users.

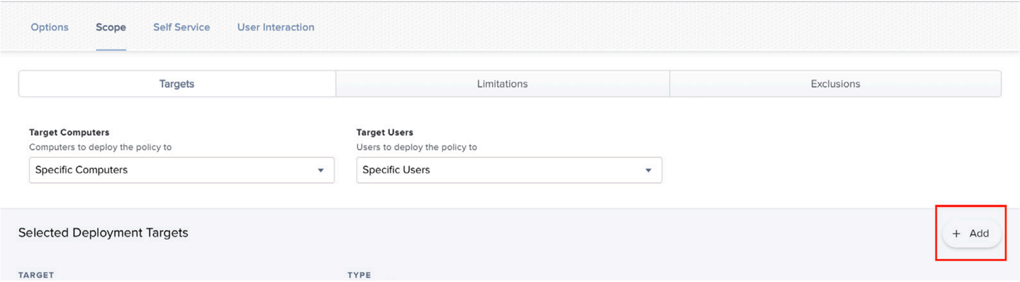
7. Leave the Target Computers menu at its default value of Specific Computers.



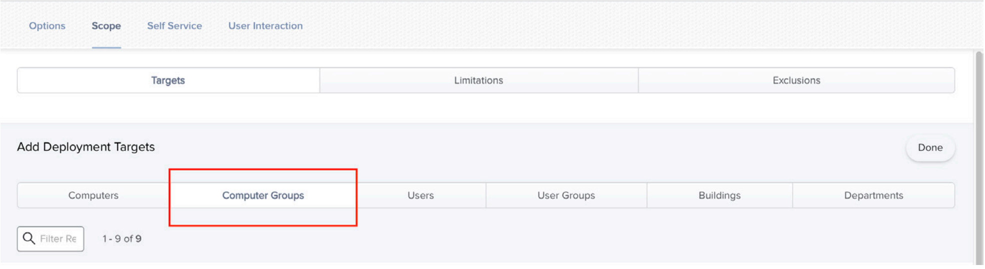
Target Computers
Computers to deploy the policy to
Specific Computers

Target Users
Users to deploy the policy to
Specific Users

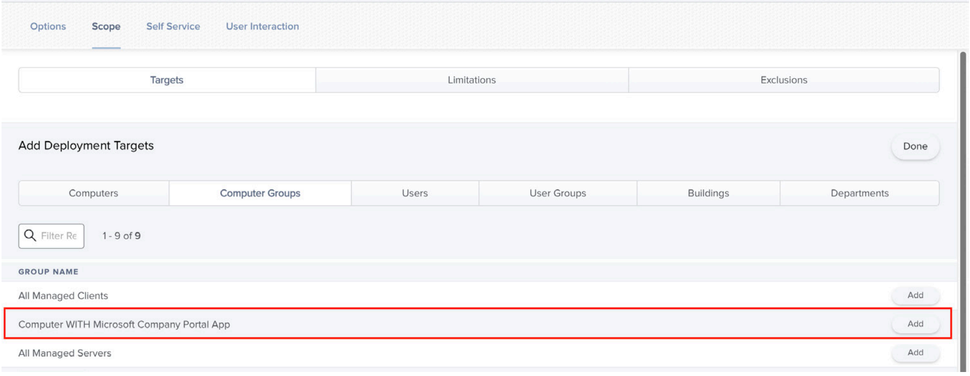
8. Click Add.



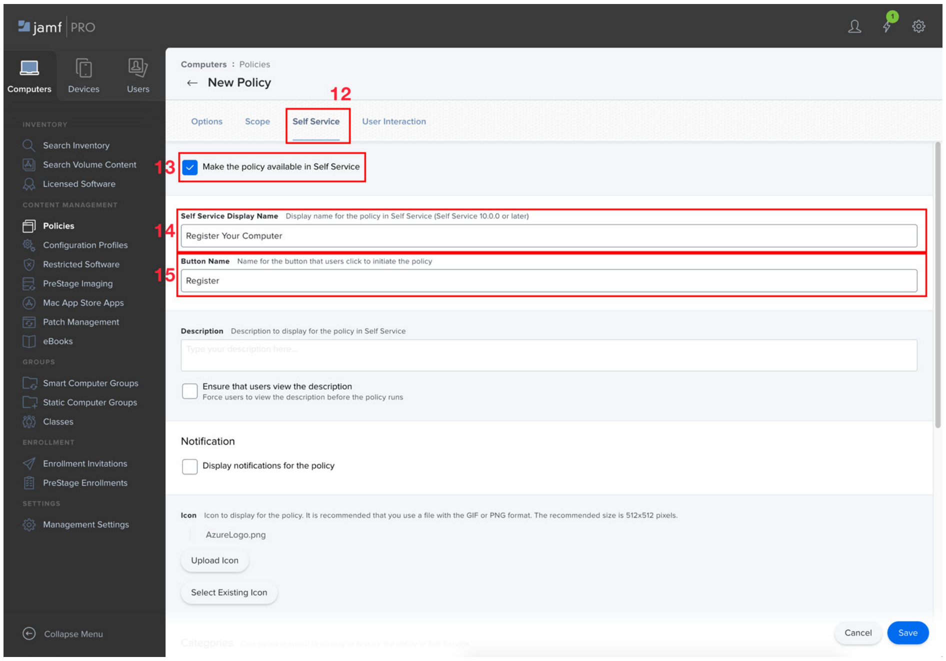
9. Click the Computer Groups tab.



10. Next to the Smart Group you created, click 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**.



☑ Make the policy available in Self Service

Self Service Display Name Display name for the policy in Self Service (Self Service 10.0.0 or later)
Register Your Computer

Button Name Name for the button that users click to initiate the policy
Register

Description Description to display for the policy in Self Service
Type your description here...

□ Ensure that users view the description
Force users to view the description before the policy runs

Notification

□ Display notifications for the policy

Icon Icon to 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

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.

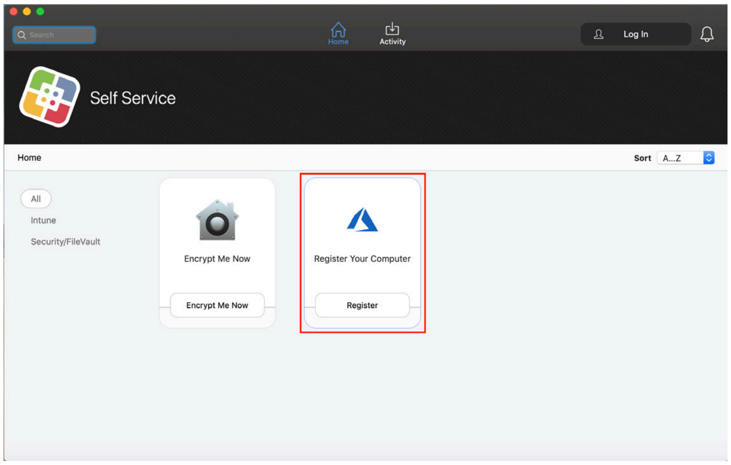
Section 4: Register a Mac computer with Azure Active Directory

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.

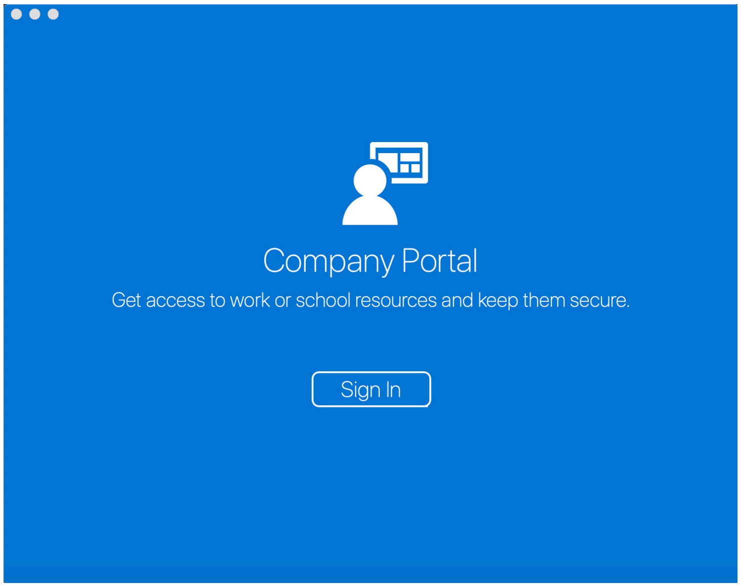
2. Open Jamf Self Service.

3. For the "Register Your Computer" item, click Register.

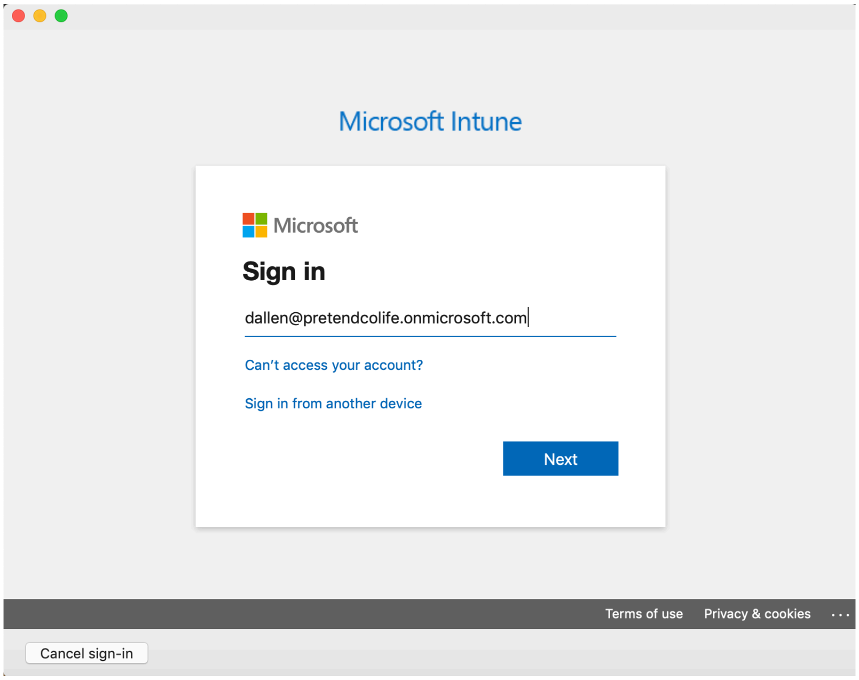


4. Confirm that the Company Portal app opens and prompts the user to sign in.

5. Click Sign In.


Company Portal
Get access to work or school resources and keep them secure.
Sign In

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



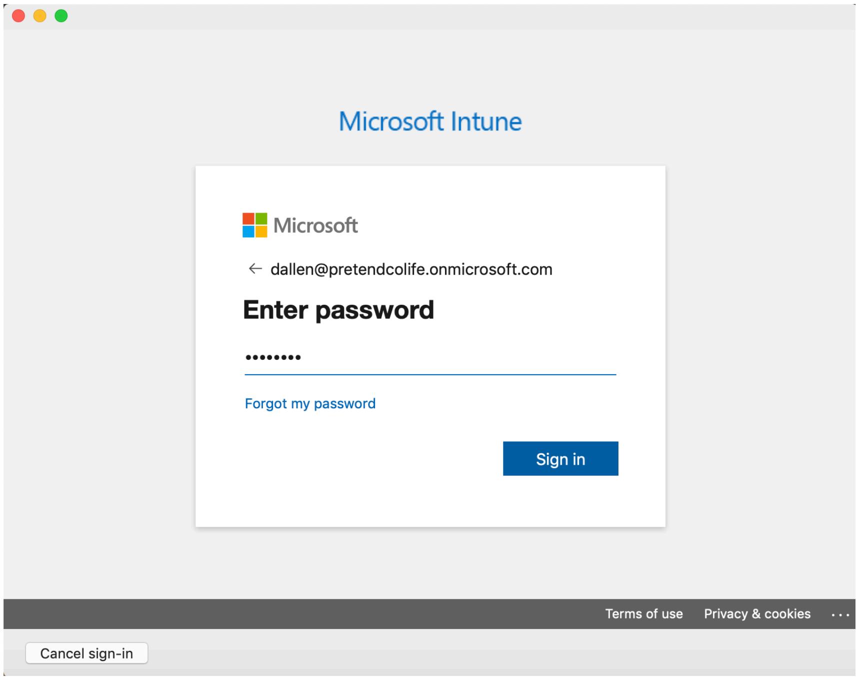
Microsoft Intune

Microsoft

Sign in

dallen@pretendcolife.onmicrosoft.com

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



Microsoft Intune

Microsoft

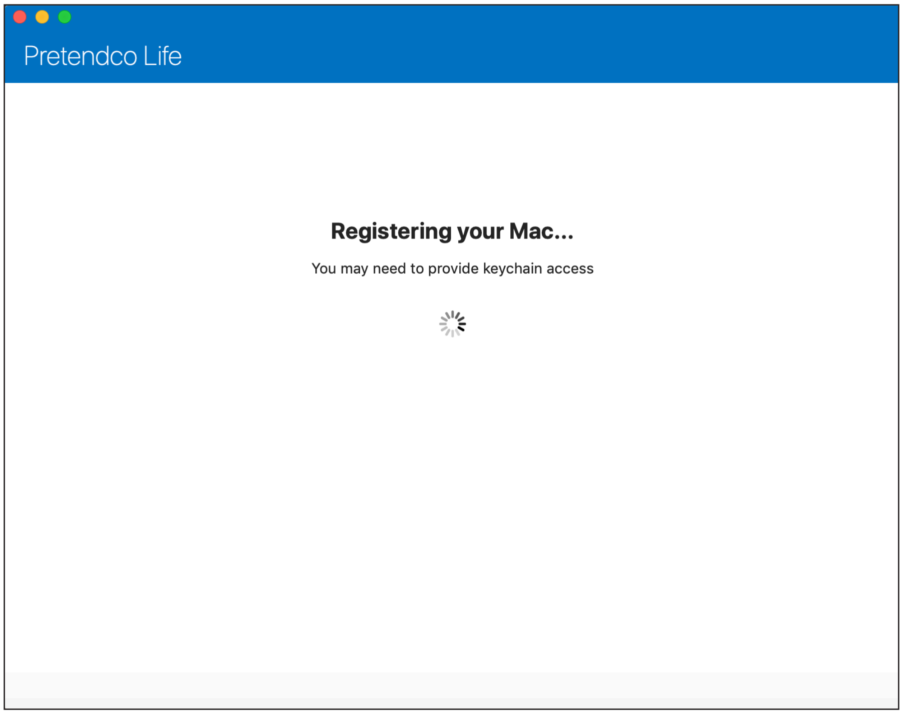
← dallen@pretendcolife.onmicrosoft.com

Enter password

••••••••

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…"

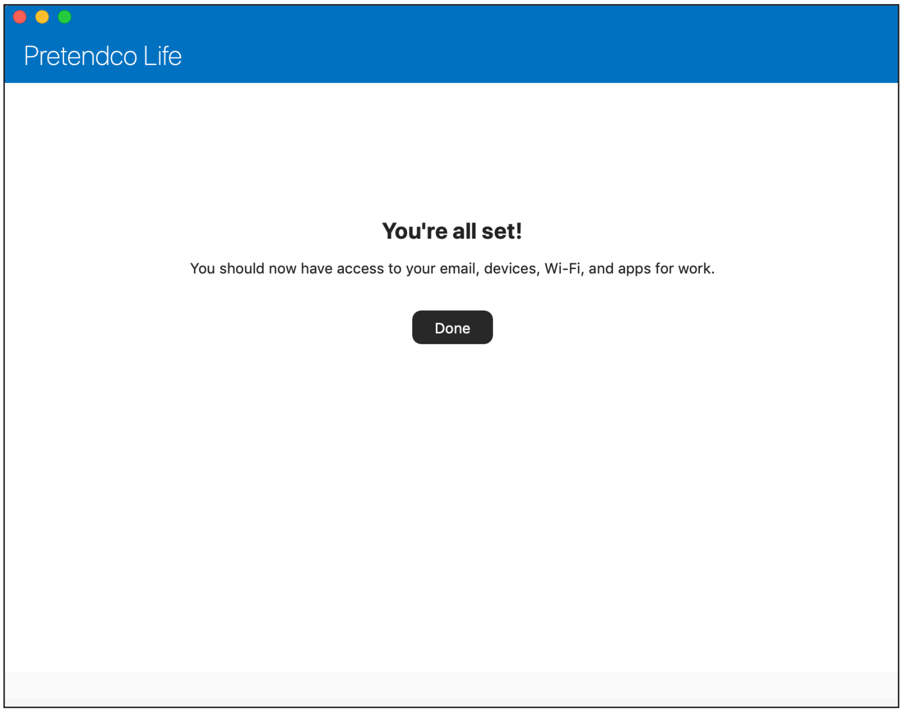


Pretendco Life

Registering your Mac...

You may need to provide keychain access

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

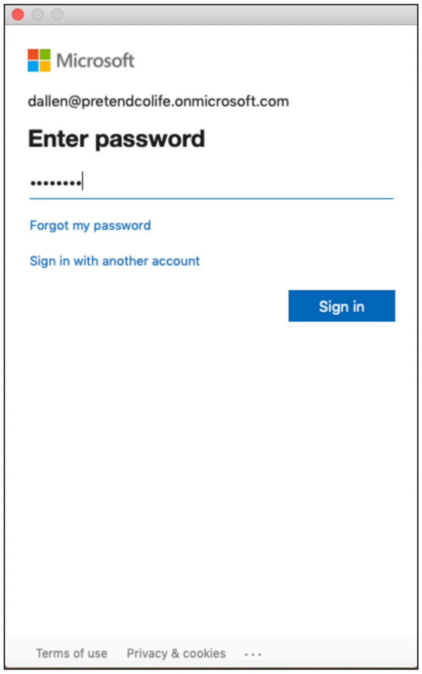


Pretendco Life

You're all set!

You should now have access to your email, devices, Wi-Fi, and apps for work.

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.



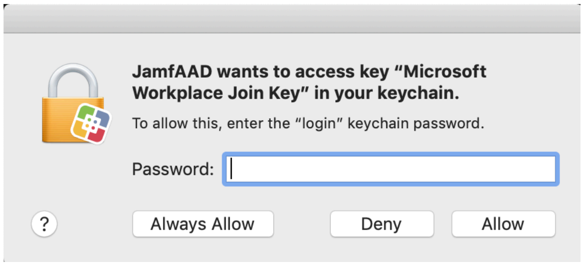
Microsoft

dallen@pretendcolife.onmicrosoft.com

Enter password

••••••••

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



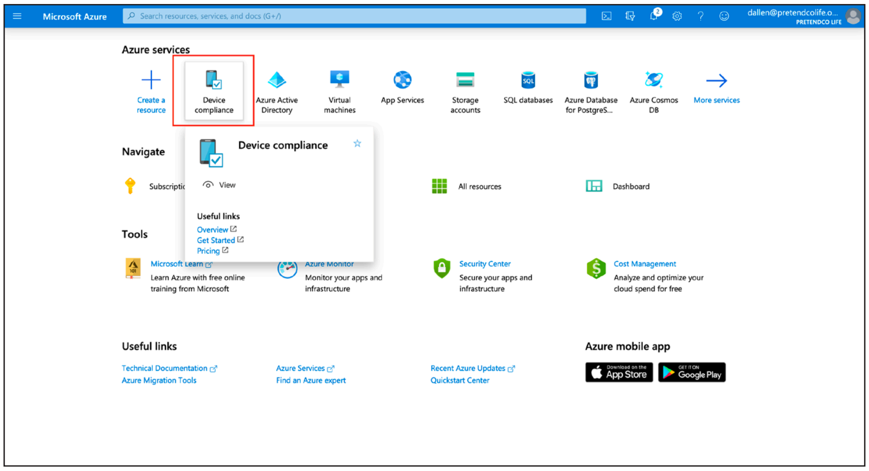
JamfAAD wants to access key "Microsoft Workplace Join Key" in your keychain.

To allow this, enter the "login" keychain password.

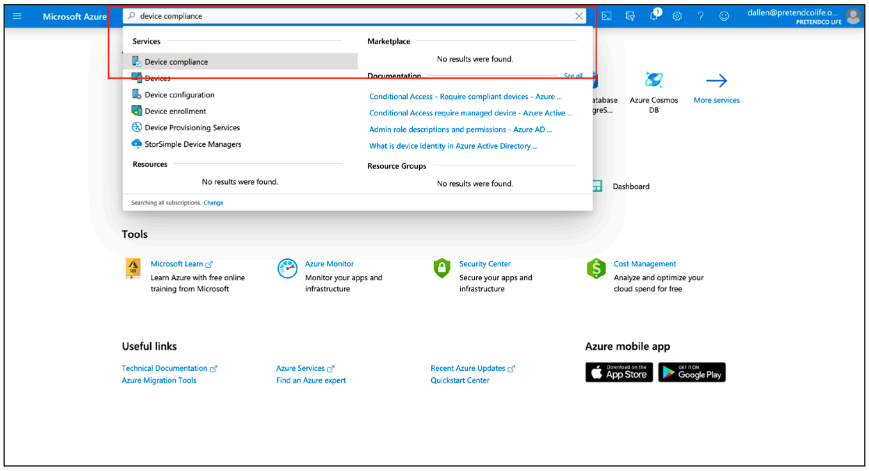
Password:

Section 5: Check macOS Device Compliance in Microsoft Intune

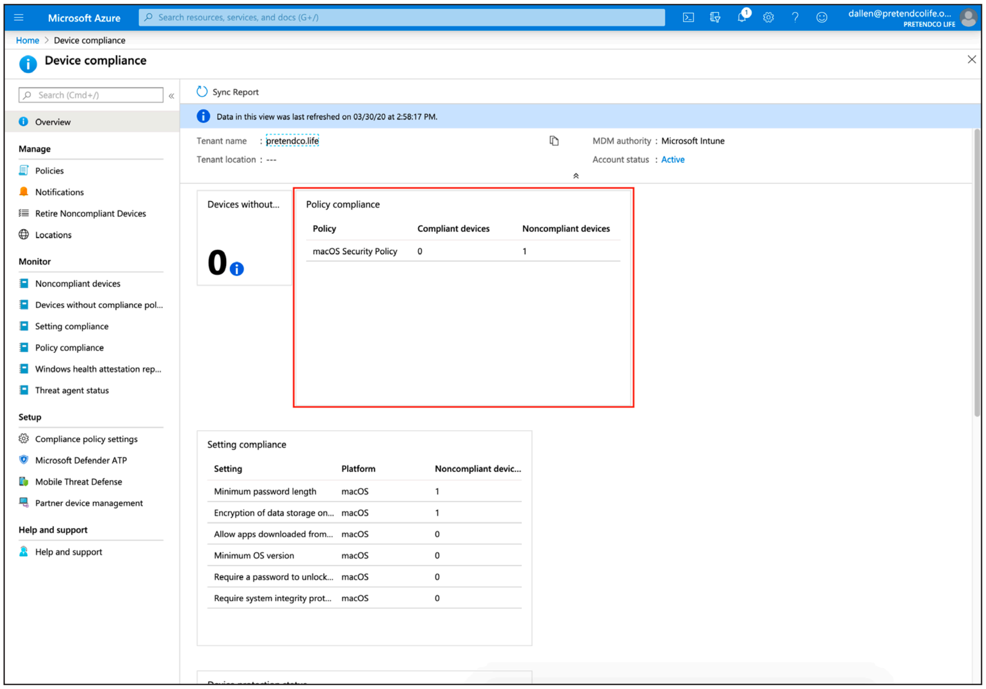
1. Open a new browser window or tab and navigate to https://portal.azure.com.
2. Log in to Microsoft Azure with a global administrator or an Intune service administrator account
3. If Azure displays Device Compliance, click Device Compliance.



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
device compliance
dallen@pretendcolife.o...
PRETENDCO LIFE
Services
Device compliance
Devices
Device configuration
Device enrollment
Device Provisioning Services
StorSimple Device Managers
Resources
No results were found.
Marketplace
No results were found.
Documentation
See all
Conditional Access - Require compliant devices - Azure ...
Conditional Access require managed device - Azure Active ...
Admin role descriptions and permissions - Azure AD ...
What is device identity in Azure Active Directory ...
Resource Groups
No results were found.
Searching all subscriptions. Change
Azure Cosmos DB
More services
Dashboard
Tools
Microsoft Learn
Learn Azure with free online training from Microsoft
Azure Monitor
Monitor your apps and infrastructure
Security Center
Secure your apps and infrastructure
Cost Management
Analyze and optimize your cloud spend for free
Useful links
Technical Documentation
Azure Migration Tools
Azure Services
Find an Azure expert
Recent Azure Updates
Quickstart Center
Azure mobile app
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.



Data in this view was last refreshed on 03/30/20 at 2:58:17 PM.

Tenant name : pretendco.life
Tenant location : ---
MDM authority : Microsoft Intune
Account status : Active

Devices without...

0

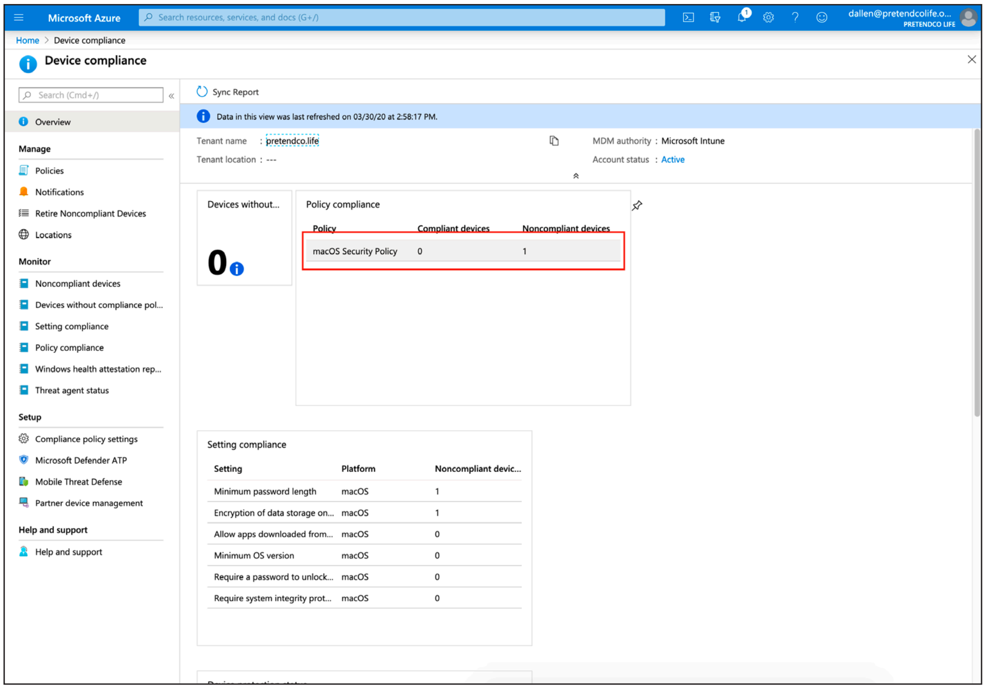
Policy compliance

Policy	Compliant devices	Noncompliant devices
macOS Security Policy	0	1

Setting compliance

Setting	Platform	Noncompliant devic...
Minimum password length	macOS	1
Encryption of data storage on...	macOS	1
Allow apps downloaded from...	macOS	0
Minimum OS version	macOS	0
Require a password to unlock...	macOS	0
Require system integrity prot...	macOS	0

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).


Data in this view was last refreshed on 03/30/20 at 2:58:17 PM.

Tenant name : pretendco.life
Tenant location : ---
MDM authority : Microsoft Intune
Account status : Active

Devices without...

0

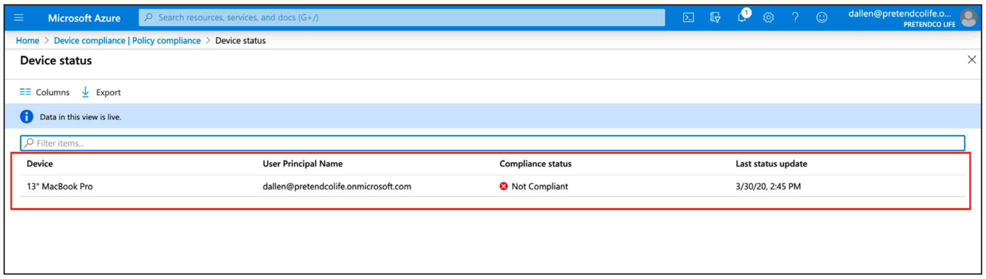
Policy compliance

Policy	Compliant devices	Noncompliant devices
macOS Security Policy	0	1

Setting compliance

Setting	Platform	Noncompliant devic...
Minimum password length	macOS	1
Encryption of data storage on...	macOS	1
Allow apps downloaded from...	macOS	0
Minimum OS version	macOS	0
Require a password to unlock...	macOS	0
Require system integrity 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.



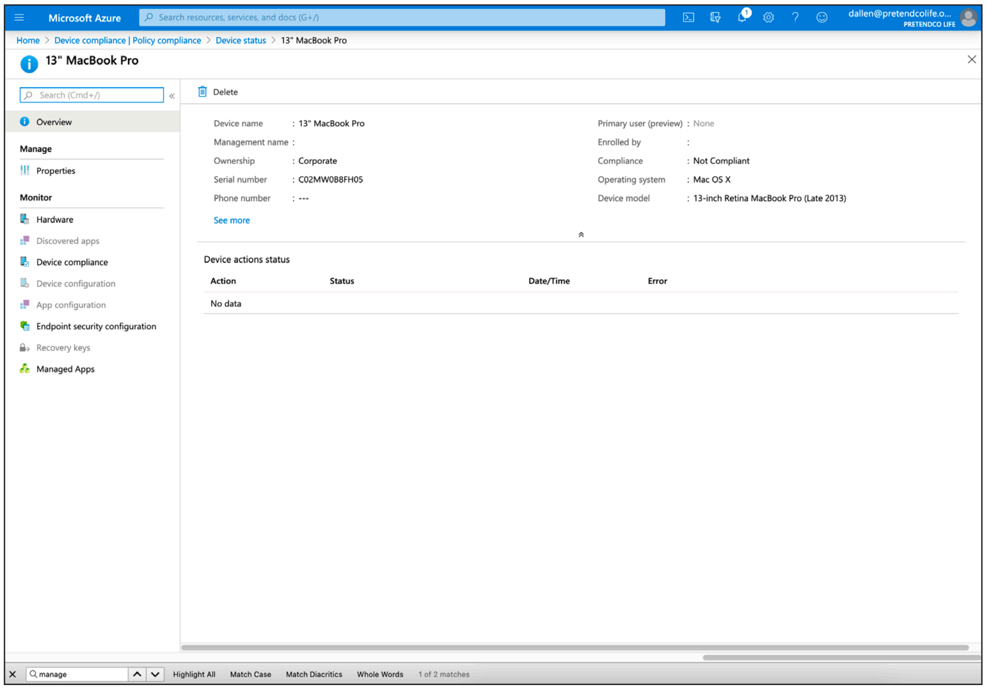
Microsoft Azure
Search resources, services, and docs (G+/)
dallen@pretendcolife.o...
PRETENDCO LIFE
Home > Device compliance | Policy compliance > Device status
Columns
Export
Filter items...

Device status

Data in this view is live.

Device	User Principal Name	Compliance status	Last status update
13" MacBook Pro	dallen@pretendcolife.onmicrosoft.com	✖ Not Compliant	3/30/20, 2:45 PM

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



13" MacBook Pro

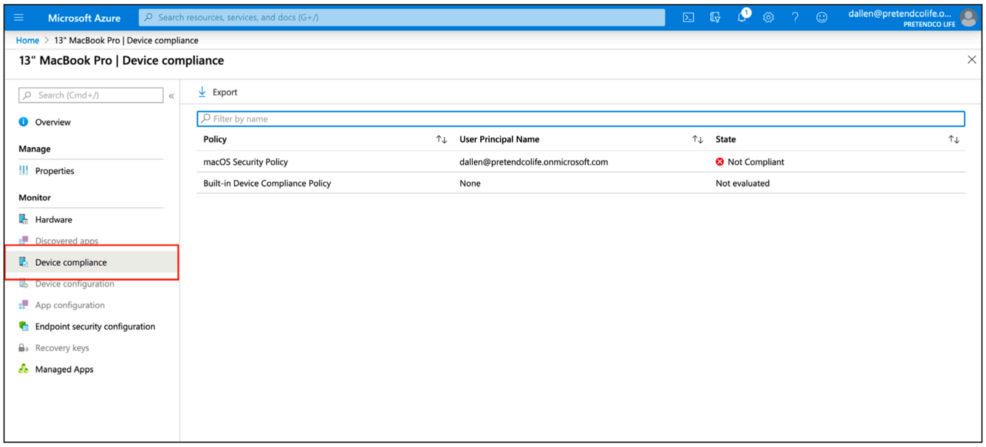
Device name : 13" MacBook Pro
Management name :
Ownership : Corporate
Serial number : C02MW0B8FH05
Phone number : ---

Primary user (preview) : None
Enrolled by :
Compliance : Not Compliant
Operating system : Mac OS X
Device model : 13-inch Retina MacBook Pro (Late 2013)

Device actions status

Action	Status	Date/Time	Error
No data			

9. In the left blade, click “Device compliance.”

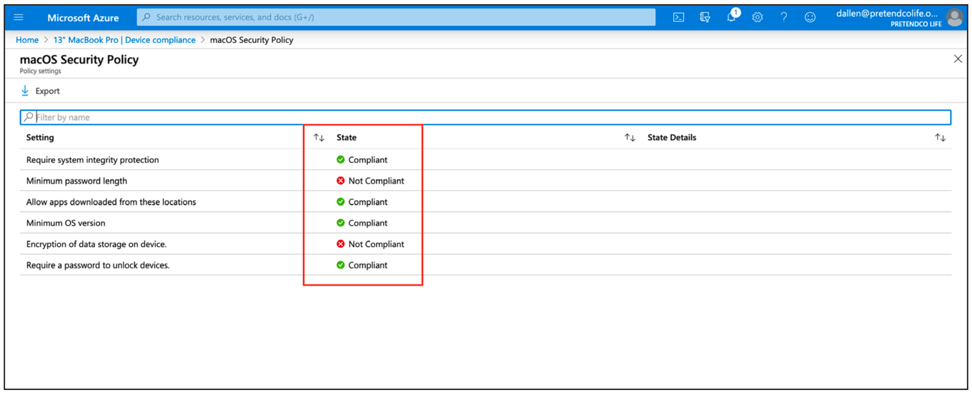


Home > 13" MacBook Pro | Device compliance

13" MacBook Pro | Device compliance

Policy	User Principal Name	State
macOS Security Policy	dallen@pretendcolife.onmicrosoft.com	☒ Not Compliant
Built-in Device Compliance Policy	None	Not evaluated

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
Search resources, services, and docs (G+/)
dallen@pretendcolife.o...
PRETENDCO LIFE
Export
Filter by name

Home > 13" MacBook Pro | Device compliance > macOS Security Policy

macOS Security Policy

Policy settings

Setting	State	State Details
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.	☒ 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.