

How to Configure Jamf Pro and Intune Company Portal for macOS Platform SSO Integration



# Contents

Preface	3
Section 1: Configure MFA in Microsoft Entra	6
Section 2: Creating a smart computer group	21
Section 3: Creating Configuration Profiles in Jamf Pro	24
Section 4: Deploying Microsoft Intune Company Portal with Jamf Pro	40
Section 5: Register a Mac using Microsoft Intune Company Portal App and Test Microsoft PSSO.	43
Section 6: Configuring Microsoft Entra for use with Jamf Connect and PSSO	52



## Preface

### What is Platform SSO

Platform SSO is a framework introduced in macOS 13 that enables single sign-on (SSO) at a system level, allowing users to authenticate once and then seamlessly access multiple apps and services without needing to re-enter credentials. Platform SSO integrates with identity providers (IdPs) like Microsoft Entra ID enabling organizations to streamline authentication across apps and services within their enterprise environment.

When integrated with Microsoft Entra ID, Platform single sign-on for macOS (Platform SSO) allows end users to authenticate to their computers using a smart card or their Entra ID credentials. Alternatively, it can be configured to create a secure, hardware-bound, non-phishable authentication factor used by Entra ID to access organization resources. In this "Secure Enclave Key" mode, the local account credentials are unchanged and knowledge of the local account password fulfills the need for multiple factors for conditional access policies.

This configuration qualifies as multi-factor authentication (MFA) because it combines two distinct types of authentication factors. When a user signs in with their local username and password along with the Secure Enclave–backed key, it satisfies "something you know" (the password) and "something you have" (the hardware-bound key stored in the Secure Enclave). Alternatively, if Touch ID is used along with the Secure Enclave key, it satisfies "something you are" (the biometric fingerprint) and "something you have" (the Secure Enclave key, it satisfies "something you are" (the password) and requirements.

#### Key Features of Platform SSO

System-wide SSO After a user authenticates via an Identity Provider their session is maintained across multiple apps and services allowing them to access resources without re-authentication.

**Integration with Enterprise SSO Plugin** macOS supports the Microsoft Enterprise SSO plugin, which works with Microsoft's identity services such as Microsoft 365 and other supported enterprise services to allow smooth authentication without needing separate app logins.

Login Window SSO In some configurations, Platform SSO can work directly from the macOS login screen, allowing users to authenticate to their device using their enterprise credentials and access services without additional prompts. Platform SSO, when configured in password mode, supports user authentication with a newly updated password directly from the FileVault login screen or the standard macOS login window. When a user logs in with their updated Entra ID password and does not recall their previous local password, this workflow can initiate an automatic keychain reset. This helps maintain access continuity while reducing the need for manual keychain troubleshooting or IT intervention.



**Device Compliance** If integrated with Microsoft Intune or another MDM like Jamf Pro, Platform SSO can ensure that devices comply with organizational security policies before granting access to resources.

Platform SSO supports the following authentication methods:

- Password
- Secure Enclave
- Smart Card

Microsoft highly recommends using Secure Enclave as the authentication method when configuring Platform SSO. If using Platform SSO on a shared Mac, Password is the recommended authentication method by Microsoft over the Secure Enclave method as all users may not have a way to use multi factor authentication.

For more information on shared devices, go here:

https://learn.microsoft.com/en-us/entra/identity/devices/device-join-macos-platform-single-signon-multi-user-device

Feature	Secure Enclave	Smart Card	Password
Passwordless (phishing resistant)			×
TouchID supported for unlock			
Can be used as passkey		×	×
MFA mandatory for setup			×
Multifactor authentication (MFA) is always recommended			
Local Mac password synced with Entra ID	×	×	
Supported on macOS 13.x +		×	
Supported on macOS 14.x +			
Optionally, allow new users to log in with Entra ID credentials (macOS 14.x +)			

#### TLS Inspection and Apple's SSO Framework

The number one support call at Microsoft for macOS SSO not functioning properly is due to TLS Inspection not being allowed access to the URL's below:

https://app-site-association.cdn-apple.com

https://app-site-association.cdn-apple.com

Microsoft recommends allowing the above URL's or preferably adding wildcards in your firewall for:

\*.cdn-apple.com

\*.networking.apple



## What Platform SSO is NOT

- Not "Windows Hello for Business" for Macs.
- Not a replacement for passwords. Apple states, "Passcodes and passwords are essential to the security of Apple devices."
- Does not support FIDO2 authenticators at login or FileVault screens.
- Does not deploy automatically via zero-touch onboarding; an admin must register the device interactively for just-in-time account creation.
- Does not replace the FileVault authentication screen. On Apple Silicon, only a password or SecureCard linked to a local user can decrypt FileVault.
- Does not enforce Multi-Factor Authentication (MFA) for macOS, including FileVault decryption, login, or admin authorization prompts.
- Not a password-less login method. SmartCards remain the only macOS-native password-less option. However, Platform SSO allows SmartCard-based cloud identity account creation in macOS Sonoma.
- It does not support VisionOS, iOS, iPadOS, or tvOS. It is exclusive to macOS.
- Does not create MDM-enabled users or allow user-level configuration profiles.
- Does not allow password changes at the login window.
- Does not support RADIUS 802.1x

#### Requirements for Platform SSO with Microsoft Entra ID

This guide will use Microsoft Entra ID as the IdP and macOS 15 for the lessons in the guide. As of this writing, Microsoft Platform Single Sign-on is in public preview so please keep that in mind when following the lessons in this guide.

Get more information on Platform SSO features at the link below:

https://learn.microsoft.com/en-us/mem/intune/configuration/platform-sso-macos

Special thanks to the following individuals for making this guide possible:

- Christos Drosos
- John Hutchison
- Michael Epping
- Michael Lopez
- Sean Rabbitt
- Yash Patel



# Section 1: Configure MFA in Microsoft Entra

#### What You'll Need:

Learn what hardware, software, and information you'll need to complete the tutorials in this section.

#### Hardware and Software:

Requirements for following along with this section:

- An authentication method policy in Microsoft Entra with Microsoft Authenticator and Passkey (FIDO2) enabled
- An active user account in Microsoft Entra
- Access to an iPhone or iPad running iOS 16 or later with the Microsoft Authenticator app installed
- A Personal Identification Device (PIV) This guide will use a Yubikey (Optional)

In this section, we will configure multi-factor authentication (MFA) settings in Microsoft Entra to utilize a Passkey stored on your iPhone and a YubiKey personal identification device. Both of these methods enable password-less authentication for your Mac while providing phishing-resistant credentials for WebAuthn challenges.

 This step is a prerequisite. You cannot continue with the lessons in this guide without proper authentication methods in place on your Microsoft Entra tenant. Your Microsoft Entra Authentication method policy must have Microsoft Authenticator and Passkey (FIDO2) enabled and scoped to a target group of your choosing. This guide will use the All users group for simplicity. Administrative privileges on your Microsoft Entra tenant are required to configure these settings. Follow these steps below:

A. Log into Microsoft Entra with administrative privileges. <u>https://entra.microsoft.com</u>

- B. Select Protection.
- C. Select Authentication methods.
- D. Select Passkey (FIDO2) and enable it with a Target of your choosing and save.
- E. Select Microsoft Authenticator and enable it with a Target of your choosing and save.

		Home		Home > Devices   All devices >				1
		Diagnose & solve problems		Authentication met	hods   Policies		×	
	*	Favorites	$\sim$	Search « Manage	+ Add external method	(Preview) 💍 Refresl	이 🔗 Got feedback?	
	۵	Identity	$\sim$	<ul> <li>Policies</li> <li>Password protection</li> </ul>	Authentication metho Use authentication method may register and use. If a u	od policies ds policies to configure t user is in scope for a me	he authentication methods your users thod, they may use it to authenticate and	
в —	*	Protection	^	<ul> <li>Registration campaign</li> <li>Authentication strengths</li> </ul>	Method	Target	Enabled	
	•	Identity Protection Conditional Access		<ul> <li>Addicinication strengths</li> <li>Settings</li> </ul>	✓ Built-In Passkey (FIDO2)	All users	Yes	
с—	43	Authentication methods		Monitoring	Microsoft Authenticator	All users	Yes	
	E	Password reset Custom security attributes		<ul> <li>User registration details</li> <li>Registration and reset events</li> </ul>	SMS Temporary Access Pass	All users	Yes	
	20	Risky activities		Bulk operation results	Hardware OATH tokens	All users	No Yes	
		Show more			Voice call	All	No	
	۲	Identity Governance	$\sim$		Certificate-based authe	All users	No	
		Verified ID	$\checkmark$		QR code (Preview)		No	ļ



- 2. Users must be able to join devices in Microsoft Entra.
  - A. Click Devices.
  - B. Click All devices.
  - C. Select Device settings.
  - D. Under Users may join devices to Microsoft Entra, select how users join their device to connect to Microsoft Entra. This guide will select All.

		Home		Home > Devices	
		nome		رَيْ <b>Devices</b>   Device sett	ings
	×	Diagnose & solve problems		HCS Training - Microsoft Entra ID	
	_	Foundation		×	🔜 Save 🔀 Discard   🔗 Got feedback?
	×	Favorites	~	Overview	
	4	Identity	~	All devices	Microsoft Entra join and registration settings
				Manage C	, , , , , , , , , , , , , , , , , , , ,
	0	Overview			Users may join devices to Microsoft Entra ①
	8	Users	$\sim$	🖏 Enterprise State Roaming	
	°24ª	Groups	$\sim$	₽ BitLocker keys (Preview)	Selected No member selected
Α—	٩.	Devices	^	Local administrator password recovery	
		Overview		Activity	Users may register their devices with Microsoft Entra
в —		All devices		Audit logs	

3. Using a web browser of your choosing, go to

https://mysignins.microsoft.com

4. Sign in with your Microsoft user account.

Microsoft	
Pick an account	
keith@hcstraining.net	:
kmitnick@hcsonline.com	:
+ Use another account	

- 5. Enter your password.
- 6. Click Sign in.





7. Select the option of reducing the number of times you are asked to sign in. This guide will select Yes.

Microsoft		
keith@hcstraining.r	net	
Stay signed	l in?	
Do this to reduce th to sign in.	ne number of time	es you are asked
Don't show thi	s again	
	No	<u>Yes</u>

- 8. Click Security info.
- 9. Click Add sign-in method (+).

	🗰 My Sign-Ins 🗸					
8 —	R Overview	Security info These are the methods you use to sign into your a You're using the most advisable sign-in method	ccount or reset your password. where it applies.			
	Devices     Sign-in method when most advisable is unavailable: Microsoft Authenticator - notification Change					
	S Password 9					
	Organizations	& Phone	+1 6319026911	Change	Delete	
	🔒 Settings & Privacy	••• Password	Last updated: 5 months ago	Change		

10.Select Microsoft Authenticator.

Add a	Add a sign-in method $ imes$					
Ŷ	Passkey in Microsoft Authenticator Sign in with your face, fingerprint, PIN					
Ö	Security key Sign in using a USB, Bluetooth, or NFC device					
٢	Microsoft Authenticator Approve sign-in requests or use one-time codes					
123	Hardware token Sign in with a code from a hardware token					
C	Office phone Get a call to sign in with a code					
	Email Receive a code to reset your password					



11.If you need to download the Microsoft Authenticator app on your device, click Download now, otherwise click Next.

Microsoft	Authenticator	×	
	Start by getting the app		
	On your phone, install the Microsoft Authenticator app. Download now		need to obtain the Microsoft
	After you install the Microsoft Authenticator app on your device, choose "Next".		Authenticator app
	I want to use a different authenticator app		
	Cancel	t	

### 12.Click Next.

Microsoft	Authenticator	×
):::::::::::::::::::::::::::::::::::::	Set up your account If prompted, allow notifications. Then add an account, and select "Work or school". Back	đ

13.Scan the QR code with your device.

## 14.Click Next.

Microsoft Authenticator	×
Scan the QR code	
Use the Microsoft Authenticator app to scan the QR code. This will connect the Microsof app with your account.	t Authenticator
After you scan the QR code, choose "Next".	
Can't scan image?	Nevt
Back	Next

15. Enter the code in the Microsoft Authenticator app on your device.

Microsoft	Authenticator	×
	Let's try it out	
	Approve the notification we're sending to your app by entering the number shown bel	OW.
L-J	23	
	Back Ne	



## 16.Click Next.

Microsoft Authenticator	×
Notification approved	
	Next

## 17. Confirm Microsoft Authenticator shows in the list below.

Security info						
These	These are the methods you use to sign into your account or reset your password.					
You're Sign-in m	You're using the most advisable sign-in method where it applies. Sign-in method when most advisable is unavailable: Microsoft Authenticator - notification Change					
+ A	dd sign-in method					
S	Phone	+1 € 1	Change	Delete		
	Password	Last updated: 5 months ago	Change			
\$	Microsoft Authenticator Push multi-factor authentication (MFA)	iPhone 14 Pro Max		Delete		

18.Open the Authenticator app on your device and tap your account.





## 19. Tap Create a passkey.

3:20 all 5	? 🗆 `
<	
HCS Training keith@hcstraining.net	
WAYS TO SIGN IN OR VERIFY	
Bign-in notifications Approve a sign-in request on your	ohone
One-time password code	o
OTHER WAYS TO SIGN IN	
Create a passkey	>
Set up passwordless sign- in requests	>
MANAGE	
Change password	C
Update security info	C
Review recent activity	C

# 20.Tap Sign in.

3:21 .il 중 ➡>
Let's create
your passkey
It takes less than a minute to help secure your account with a passkey. Once set up, you can sign in faster and more securely with your face, fingerprint, or PIN. First, sign in with your <b>keith@hcstraining.net</b> account to verify your identity.
Sign in



21.Confirm the app needs to approve your sign in request with a number.



22.Enter the number.

23.Tap Yes.





## 24. Tap Done.

3:22 .
V
<b>Passkey created</b>
You can now use your passkey with Authenticator. Your passkey is called: Authenticator - iOS
TO SIGN IN WITH YOUR PASSKEY:
Select Face, fingerprint, or PIN.
Make sure Authenticator is turned on as a passkey provider.
How to use your passkey
Done

25.Let's test the passkey. Using a web browser of your choosing, go to <u>https://mysignins.microsoft.com</u>

Click on your account in the upper-right corner

26. Click Sign out.



27.Select the account you want to sign out of.

Mi	crosoft	
Pick	an account	
Which a	account do you want to sign out o	ıf?
à	Keith Mitnick keith@hcstraining.net Signed in	

28.Confirm you have signed out of your account.





29. Select an account to sign in with.

Pick	crosoft an account		
à	keith@hcstraining.net	:	
à	kmitnick@hcsonline.com	÷	
+	Use another account		

30. At the password login screen, select Use your face, fingerprint, PIN, or security key instead.

← keith@hcstraining.net	
Enter password	
••••••	
Forgot my password	
	coourity key instead

31. A QR code will appear. Scan this with the Camera.app on your device.





32. On your device, Tap Sign in with a passkey.



33. On your device, Tap Continue.



34. Select the option of reducing the number of times you are asked to sign in. This guide will select Yes.

Microsoft				
keith@hcstraining.net	keith@hcstraining.net			
Stay signed	Stay signed in?			
Do this to reduce the number of times you are asked to sign in.				
Don't show this again				
	No	Yes		



35. Click Security Info, and confirm your Passkey shows in the list.

🗰 My Sign-Ins 🗸					
<ul> <li>Overview</li> <li>Security info</li> <li>Devices</li> </ul>	Security info These are the methods you use to sign into You're using the most advisable sign-in m Sign-in method when most advisable is unavailable Microsof	o your account or reset your password. nethod where it applies. t Authenticator - notification Change			
Password Organizations	+ Add sign-in method	+1 6 1	Change	Delete	
A Settings & Privacy	Password	Last updated: 5 months ago	Change		
Recent activity	Microsoft Authenticator Push multi-factor authentication (MFA)	iPhone 14 Pro Max		Delete	
	Passkey Microsoft Authenticator	Authenticator - iOS iOS device		Delete	~

The next steps are optional and require a Personal Identification Device (PIV) This guide will use a Security Key (Yubikey shown below). You can skip these steps if they are not required by your organization.



36.Click Add sing-in method.

$\blacksquare$ My Sign-Ins $\lor$					
8 Overview	Security info				
𝒫 Security info	These are the methods you use to sign into your account or reset your password.				
💻 Devices	You're using the most advisable sign-in method where it applies. Sign-in method when most advisable is unavailable: Microsoft Authenticator - notification Grange				
🔍 Password	+ Add sign-in method				
Organizations	& Phone	+1 6 1	Change	Delete	
A Settings & Privacy	••• Password	Last updated: 5 months ago	Change		
Recent activity	Microsoft Authenticator     Push multi-factor authentication (MFA)	iPhone 14 Pro Max		Delete	
	Passkey Microsoft Authenticator	Authenticator - iOS iOS device		Delete	~



### 37. Select Security key.



38. Select your security key type. This guide will select USB device.

Security key	×
Choose the type of security key that you have.	
■ NFC device	
	Cancel

#### 39.Click Next.





40.Connect your security key and activate the security key. NOTE: Follow the instructions on how to activate your security key.



- 41. Enter your PIN for your security key if prompted.
- 42. Click Next.



43. Activate your security key.





## 44.Enter a name your security key.

45.Click Next.



### 46.Click Done.

Security key	×
You're all set!	
You can use your security key instead of a username and passwo the next time you sign in.	rd
Be sure to follow your security key manufacturer's guidance to perform any additional setup tasks such as registering your fingerprint.	
Dor	1e

47.Confirm your security key shows in the list. It will show as Passkey with the name you provided for your key.

Sec These You're <sup>Sign-in m</sup>	curity info are the methods you use to sign into your a using the most advisable sign-in method ethod when most advisable is unavailable: Microsoft Authentic	ccount or reset your password. where it applies. ator - notification Change			
+ A	dd sign-in method				
S	Phone	+1 ( 1	Change	Delete	
	Password	Last updated: 5 months ago	Change		
\$	Microsoft Authenticator Push multi-factor authentication (MFA)	iPhone 14 Pro Max		Delete	
ු	Passkey	Keith's Yubikey		Delete	×
ු	Passkey Microsoft Authenticator	Authenticator - iOS iOS device		Delete	~



48. In the step above, the Security key showed up as a Passkey. This will change once you sign in to your Microsoft account with your security key. It will show up in the list as Security key going forward.

Se These You're	curity info e are the methods you use to sign into your a using the most advisable sign-in method nethod when most advisable is unavailable: Microsoft Authenti-	ccount or reset your password. where it applies. cator - notification Change					
+ 4	+ Add sign-in method						
S	Phone	+1 1	Change	Delete			
	Password	Last updated: 5 months ago	Change				
\$	Microsoft Authenticator Push multi-factor authentication (MFA)	iPhone 14 Pro Max		Delete			
Ö	Security key Security Key	Keith's Yubikey		Delete	~		
ු	Passkey Microsoft Authenticator	Authenticator - iOS iOS device		Delete	~		

This completes this section. In the next section, we will create a smart computer group in Jamf Pro to find all Mac computers running macOS 14.5 or later. While macOS 13 supports Platform SSO, it is recommended to use macOS 14.5 or later to leverage the latest enhancements and features.



# Section 2: Creating a smart computer group

#### What You'll Need:

Learn what hardware, software, and information you'll need to complete the tutorials in this section.

#### Hardware and Software:

Requirements for following along with this section:

• Administrative access to your Jamf Pro server.

In this section, we will create a smart computer group in Jamf Pro to find all Mac computers running macOS 14.5 or later. While macOS 13 supports Platform SSO, it is recommended to use macOS 14.5 or later to leverage the latest enhancements and features. We will use this smart computer group as a scope to install the Intune Company Portal application in a later section of this guide.

1. Log into your Jamf Pro server with administrative credentials.

P P	Pro
Username	
Required	
Password	
	Ø
Required	

- 2. Select Computers.
- 3. Smart Computer Groups.
- 4. Click New.





- 5. Click Computer Group if not already selected.
- 6. Enter Macs running macOS 14.5 or later for the Display Name.
- 7. Click Criteria.



8. Click Add.

Computer Group	Criteria			
AND/OR	CRITERIA	OPERATOR	VALUE	

9. Select Choose for Operating System Version.

Computers: Smart Computer Groups ← New Smart Computer Gr	oup
Last Inventory Update	Choose
Model	Choose
Model Identifier	Choose
Number of Available Updates	Choose
Operating System	Choose
Operating System Version	Choose

- 10.Select greater than or equal to for the Operator.
- 11.Enter 14.5 for the Value.
- 12.Click Save.

Computer Group	Criteria			
AND/OR	CRITERIA	OPERATOR	VALUE	
	Operating System Version	greater than or equal	• 14.5	 Delete
	1	0		(
				(T Add



## 13.Click Previous.

Computers :	Smart Computer Groups
 ← Ma	cs running macOS 14.5 or later

14. Confirm the smart computer group named Macs running 14.5 or later shows up in the list.

Computers Smart Computer Groups	
macOS_Sequoia_CIL_LVL2_NotCompliant	2
macOS_Sequoia_CIS_LVL2_Compliant	1
Macs Eligible for macOS Ventura Upgrade	0
Macs Enrolled with Baseline Mac Deployment PreStage	1
Macs Enrolled with Jamf Setup Manager PreStage	0
Macs Enrolled With Universal Mac Deployment PreStage	0
Macs running macOS 14.5 or later	4

This completes this section. In the next section, we will create configuration profiles in Jamf Pro to manage background notifications, Microsoft messages, and Microsoft PSSO settings.



# Section 3: Creating Configuration Profiles in Jamf Pro

#### What You'll Need:

Learn what hardware, software, and information you'll need to complete the tutorials in this section.

#### Hardware and Software:

Requirements for following along with this section:

- Administrative access to your Jamf Pro server
  - Download the customPSSO.plist: https://hcsonline.com/images/files/customPSSO.plist.zip

In this section, we will create the following configuration profiles in Jamf Pro:

- Managed Background Item Notifications
- Managed Microsoft Messages
- Microsoft Platform SSO Extension

The Managed Background Item Notifications and Managed Microsoft Messages configuration profiles control the messages shown below so end users won't need to take action or make decisions based on them.

мистовот клизирани	Managed Login Items Added Your organization added items that can run in the background. You can view these in Login Items & Extensions.
ň	Background Items Added Microsoft AutoUpdate* added items that can run in the background. You can manage these in Lozin Items & Extensions.
Required Data Notice	
Microsoft AutoUpdate helps update your Microsoft applications for Mac. We collect required diagnostic data to keep Microsoft AutoUpdate secure, up-to-date and performing as expected on the device it is installed on. This date naties to the basic functioning of Microsoft	
Autolopade and does not include your name, file contents or information about pape unrelated to the Microsoft Apollosiane. It helps keep up-to-date. The applications Microsoft Autolopade services may privide you with an option to send optional abgenetic data to Microsoft, if you opt-in to sending optional disposito data that choice will also apply to Microsoft Autolopade.	

1. If necessary, Log into your Jamf Pro server with administrative credentials.

Username	
Required	
Password	
	Ø



- 2. Click Computers.
- 3. Click Configuration Profiles.
- 4. Click New.

	2	Pro							۵ 🗘
	8	□ Computers	Computers Configuration	Profiles			_		
	G	Inventory	C Filter Profiles	0 - 0 of 0			+ New	Upload	:= 88
	8	Search Inventory	NAME	业 LOGS	I COMPLETED	I PENDING	I FAILED	I SCOPE	ф
	٢	Licensed Software	No data available in table						
		Content Management							
		Policies							
3 —		Configuration Profiles							
		Software Updates							
l		Postricted Software							

- 5. Click General, if not already selected.
- 6. Enter Managed background item Notifications for the Name.
- 7. Select a category of your choosing. This guide will use PSSO

	Pro		Ģ	8
88	Computers	Computers : Configuration Profiles		
	Inventory Search Inventory Search Volume Content Licensed Software	Options     Scope     5       Q     Search     General       Image: Comparison of the profile     Name       Image: Comparison of the profile     Managed background item Notifications	•	
0	Content Management Policies Configuration Profiles	ACME Certificate     Not configured     ACME Certificate     Acmediate     Acmediat     Acmediate     Acmedia		
	Software Updates Restricted Software	AD Certificate     Not configured     Category     Category to add the profile to		
	Mac Apps Patch Management eBooks	App-To-Per-App VPN Apping Not configured App-to-Per-App VPN Level Level Level at which to apply the profile Computer Level		
		Application &		



- 8. Scroll down and select Notifications.
- 9. Click Add (+).



10. Enter Managed Background Items for the App Name.

11.Enter com.apple.btmnotificationagent for the Bundle ID.

12. Enable Notifications.

- 13.Select Disable.
- 14.Click Scope





## 15.Click Targets.

16.Select Specific Computers.

17.Click Add (+).

***	Pro			Q 8
	Computers	computers : Configuration Profiles ← Managed backgro	ound item Notification	IS
G	Inventory	Options Scope	15	
8	Search Inventory	Targets	Limitations	Exclusions
	Search Volume Content			
÷	Licensed Software	Target Computers	Target Users	
9		Computers to assign the profile to	Users to distribute the profile to	
	Content Management	Specific Computers 🔻	Specific Users	
2	Policies		16	
	Configuration Profiles	Selected Deployment Targets		+ Add
	Software Updates			
	Restricted Software	TARGET	TYPE	
	Mac Apps	No Targets		
	•	»)		

18.Click Computer Groups.

19.Enter **14.5** in the search field.

20.Click Add for Macs running macOS 14.5 or later.

Targets	Limitat	ions	Exclusions
Add Deployment Targe	ts	—18	Done
Computers	Computer Groups	Users	User Groups
Bui	dings	Depa	artments
Q 14.5	<del></del> 19		
GROUP NAME			



21.Click Save.

laigets	Limitation	ns	Exclusions
Add Deployment Target	S		Done
Computers	Computer Groups	Users	User Groups
Bu	ildings	Depa	rtments
Q 14.5	1 - 1 of <b>1</b>		
GROUP NAME			

## 22.Click Previous (←).

Computers :	Configuration Profiles
_← Ma	nage Background Item Notifications

23.Click New.

2	Pro							₽ 8
88	Computers	Computers Configuratio	n Profiles					
Co	Inventory	Q Filter Profiles	0 - 0 of 0			+ New	🖞 Upload	:= 88
8	Search Inventory Search Volume Content	NAME	ili LOGS	I COMPLETED	I PENDING	I FAILED	I SCOPE	ψ



24. Click General if it's not already selected.

25.Enter Managed Microsoft Messages for the Name.

26.Select a category of your choosing. This guide will use PSSO.



27.Scroll down and click Application & Custom Settings.

28.Click Upload.

29.Click Add (+).

	Pro Pro			Q 8	
	Computers	computers : Configuratio ← New mac	n Profiles		-
∎ 	Inventory Search Inventory Search Volume Content Licensed Software Content Management Policies Configuration Profiles Software Updates	Options     Scope       Q. Search     ArrPlay Not configured       App-To-Per-App VPN Mapping Not configured       Application & Custom Settings Not configured       Jamf Applications	Upload Use this section to define generic settings for preference domains.	Remove all + Add	- 29
	Restricted Software Mac Apps Patch Management	External Applications Upload	- 28		



30.Enter com.microsoft.autoupdate2 for the name of the Preference Domain.

31.Enter the XML below Into the Property List field.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/
DTDs/PropertyList-1.0.dtd">
<plist version="1.0"> <dict> <key>AcknowledgedDataCollectionPolicy</key>
<string>RequiredDataOnly</string> </dict>
```

#### </plist>

32.Click Scope.





## 33.Click Targets.

34.Select Specific Computers.

35.Click Add (+).

🗄 🎽 Pro			Ç L
Computers	computers : Configuration Profiles ← Managed backgr	ound item Notifications	6
Inventory	Options Scope	33	
Search Inventory	Targets	Limitations	Exclusions
Search Volume Content	-		
Licensed Software	Target Computers	Target Users	
	Computers to assign the profile to	Users to distribute the profile to	
Content Management	Specific Computers -	Specific Users •	
Policies		34	
Configuration Profiles	Selected Deployment Targets		+ Add
Software Updates			
Restricted Software	TARGET	ТҮРЕ	
Mac Apps	No Targets		
Batah Managamant	•		

36.Click Computer Groups.

37.Enter **14.5** in the search field.

38.Click Add for Macs running macOS 14.5 or later.

Targets	Limitati	ans	Evolucione
Talgata	LIIIILUU		Exclusions
Add Deployment Target	5		Done
Computers	Computer Groups	— 36 Users	User Groups
Build	lings	Depa	rtments
Q 14.5	<del>⊔1•</del> 67		
CROURNAME			
GROUP NAME			



39.Click Save.

Targets	Limit	ations	Exclusions	
Add Deployment Target	's		Done	
Computers	Computer Groups	Users	User Groups	
Bu	ildings	Departments		
<b>Q</b> 14.5	1 - 1 of <b>1</b>			
GROUP NAME				

40.Click Previous (←).

Computers :	Configuration Profiles	
← Ma	naged Microsoft Messag	jes

41.Click New.

2	Pro							<b>1</b> 8
88	Computers	Computers Configuratio	n Profiles					
G	Inventory	C Filter Profiles	0 - 0 of 0			+ New	🖞 Upload	.≡ 88
8	Search Inventory Search Volume Content	NAME	小 LOGS	I COMPLETED	I PENDING	I FAILED	I SCOPE	ф



42. Enter Microsoft Platform SSO Extension for the Name.

43. Select a category of your choosing. This guide will use PSSO.

44.Leave the rest of the settings at their defaults.



45.Scroll down Select Single Sign-On Extension payload.

46.Click Add.





- 47.Select SSO for the Payload Type.
- 48. Enter com.microsoft.CompanyPortalMac.ssoextension for Extension Identifier
- 49.Enter UBF8T346G9 for Team Identifier.
- 50. Select Redirect.
- 51. Enter https://login.microsoftonline.com for the URL.
- 52.Click Add.





53.Enter the next two URLs:

- https://login.microsoft.com
- https://sts.windows.net

These URL's are optional and only required if you're using sovereign cloud domains: This guide will add them.

- https://login.partner.microsoftonline.cn

- https://login.partie.imclosoftonime.
  https://login.microsoftonline.us
  https://login-us.microsoftonline.com

	Pro			Ą	8	
88	□ Computers	computers : Configuration Pro ← New macO	Riles S Configuration Profile	nfiguration Profile		
		Options Scope			-	
G	Inventory Search Inventory	Q Search	The team identifier of the app extension that performs single sign-on			-
8		-	UBF8T346G9			
*	Search Volume Content	Received Not configured	Sign-on Type			
0	Licensed Software	Restrictions     Not configured	Sign-on authorization type Credential Redirect			
•	Content Management		URLs			
	Policies	SCEP Not configured	URLs of identity providers where the app performs single sign-on. The URLs must begin with http:// or https:// and be unique for all configured Single Sign-			
	Configuration Profiles	Coourity and	On Extensions payloads. Query parameters and URL fragments are not allower	d.		
	Software Updates	Privacy ~ Not configured	https://login.microsoftonline.com		Û	
	Restricted Software		https://login.microsoft.com		<u> </u>	
	Mac Apps	Single Sign-On Extensions				- 53
	Patch Management	1 payload configured	https://sts.windows.net	<del>] .</del>	<u>-</u>	
	eBooks	B Smart Card Not configured	https://login.partner.microsoftonline.cn		Û	
	Groups	Software Update	https://login.chinacloudapi.cn	, (	Û	
	Smart Computer Groups			5		Optional entries
		System Migration	https://login.microsoftonline.us	_ '	Û	
	Groups				<b>⊕</b>	
	Classes	System Extensions Not configured	https://ogin-us.nierosoftoninie.com		Ш	
	Enrollment	Time Machine     Not configured		+ Add	d	
	Enrollment Invitations		Setting	Includ	е	
	PreStage Enrollments	VPN Not configured	Use Platform SSO		)	
			Allow the user to sign in once at the login window and then automatically			/



54. Scroll Down and Enable Use Platform SSO.

55. Select User Secure Enclave Key under Authentication Method.

56. Enable Registration Token.

57.Enter the following in the field {{DEVICEREGISTRATION}}

58.Enable Use Shared Device Keys.




59. Scroll down and enable Authentication when screen is locked.

60.Select Do not handle.

61.Enable Custom Configuration.

62.Upload the file named customPSSO.plist (This was download at the beginning of this section) 63.Click Scope.





## 64.Click Targets.

65.Select Specific Computers.

66.Click Add (+).

🗄 🖌 Pro			Q 8
😐 Compute	rs ← Managed back	ground item Notifications	5
Inventory	Options Scope	64	
Search Inventor	Targets	Limitations	Exclusions
Search Volume	Content		
Licensed Softw	re Target Computers	Target Users	
	Computers to assign the profile to	Users to distribute the profile to	
Content Managen	ant Specific Computers	▼ ) (Specific Users ▼ )	
Policies		65	
Configuration F	ofiles Selected Deployment Targets		+ Add
Software Updat	·S		
Restricted Softw	are TARGET	TYPE	
Mac Apps	No Targets		
Patch Managem	int		

67.Click Computer Groups.

68.Enter **14.5** in the search field.

69.Click Add for Macs running macOS 14.5 or later.

Targets	Limitatio	ns	Exclusions	
Add Deployment Targets		.67	Done	-
Computers	Computer Groups	Users	User Groups	
Buildings		Depa	rtments	
Q 14.5	<del>~~+</del> 68			
GROUP NAME				



70.Click Save.

Targets	Limita	tions	Exclusions
Add Deployment Targe	ts		Done
Computers	Computer Groups	Users	User Groups
В	uildings	Depa	rtments
Q 14.5	1 - 1 of <b>1</b>		
GROUP NAME			

71.Click Previous (←).



72. Confirm all three configuration profiles were created.

	Pro						Q 8
88	Computers	Computers Configuratio	n Profil	es			
G	Inventory	C G Filter results	1 - 26 o	f 26		+ New	Upload 📃 🐯
ő	Search Inventory Search Volume Content	NAME	4 LOGS	I COMPLETED	+ PENDING	I FAILED	ι  SCOPE ι ι
≆	Licensed Software	> Network					
٥	Content Management Policies	~ PSSO					
	Configuration Profiles	Managed background item Notifications	View	0	2	0	Macs running macOS 14.5
	Restricted Software	Managed Microsoft Messages	View	0	2	0	Macs running macOS 14.5
	Mac Apps Patch Management	Microsoft Platform SSO Extension	View	0	2	0	Macs running macOS 14.5

This completes this section. In the next section, we will deploy the Microsoft Intune Company Portal application using the Jamf app catalog.



# Section 4: Deploying Microsoft Intune Company Portal with Jamf Pro

#### What You'll Need:

Learn what hardware, software, and information you'll need to complete the tutorials in this section.

#### Hardware and Software:

Requirements for following along with this section:

• Administrative access to your Jamf Pro server.

NOTE: Users in Microsoft Entra ID must have a strong authentication method, such as MFA, Federated MFA, FIDO, or a Temporary Access Pass. Additionally, they must have permission to join devices to Microsoft Entra ID. Ensure that this setting is not blocked in Microsoft Entra ID as discussed in section one of this guide.

1. If necessary, Log into your Jamf Pro server with administrative credentials.

	Pro Pro	
Username		
Required		
Password		
ſ		Ø
l		
Required		

- 2. Click Computers.
- 3. Mac Apps.
- 4. Click New.

	Pro		Q 8
80	Computers	Computers Mac Apps	+ New
	Inventory	Jamf App Catalog App Store	
	Search Inventory	Q Search filterable columns $\leftarrow$ 1 $\rightarrow$ 1 - 2 of 2	÷ •
Čě.	Search Volume Content	□ NAME ↑ ♀ □ DEPLOYMENT STATUS □ VERSION DEPLOYED ♀ □ TARGET GROUP	UPDATE METHOD
*	Licensed Software	Adobe Creative Cl () Not installed 6.5.0.348 macOS Sonoma - Curren	Automatic
0	Content Management	Adobe Photoshop ③ Not installed 25.12.2 Notebooks	Automatic
0	Policies		
	Configuration Profiles		
	Software Updates		
	Restricted Software		
	Mac Apps		
	Patch Management		



- 5. Select Jamf App Catalog.
- 6. Click Next.

Mac Apps	
Select App Source	App Source Mac App Store Mar App Catalog Mart App Catalog Relies on Jamf App Installers for updates 5

- 7. In the search field, enter **company portal**.
- 8. Click Add.

2	Pro				₽ 8 Ì
:: 	Computers	Computers Mac Apps			
© © # © ⊕	Inventory Search Inventory Search Volume Content Licensed Software Content Management Policies Configuration Profiles Software Updates Restricted Software Mac Apps Patch Management eBooks	<ul> <li>Select App Source</li> <li>Select App</li> </ul>	Select App Installers software title	7 1 → 1 - 1 of 1 √ ↓ LATEST VERSION 5.2502.1	Cadd



- 9. Select a category of your choosing. This guide will use PSSO.
- 10. Select Macs running macOS 14.5 or later for the Target Group.
- 11.Select an install method that works for you. This guide will choose Install Automatically.
- 12. Select Automatic to allow Jamf to automatically install the latest version.
- 13. Select the checkbox for Log event notifications for this app.
- 14. Select the checkbox for Install supporting configuration profiles.
- 15.Click Save.

1

1 1

1

Use the switch to enable deployment	of this app	De
onfiguration settings Deployment st	tatus Self Service End user experience	
Settings		
Display Name Display name (up to 255 characters) f	for the app	
Microsoft Intune Company Portal		
Required		
Site		
NONE		
NONE		
Category Category to add the app to		
PSSO		
Target Group		
Macs running macos 14.5 of later		
nitial distribution method	a ann to a computer for the initial installation	
Install automatically	app to a compater for the mitial installation.	
Make available in Self Service		
Undate method		
The method to use for all future app u	pdates, regardless of the initial distribution method.	
Automatic Allow Jamf to automatic	cally install the latest version.	
Manual Allows you to decide when	n to install a newer version.	
Log event notifications for this ap Opt in to receiving notifications for	p or certain events including app updates and installa	ation failures.
<ol> <li>You must select specific events</li> </ol>	s in your Account Notification settings to receive not	tifications.
Configuration profiles for additio	nal settings	
Install supporting configuration pr Allows Jamf to automatically inst	ofiles all necessary configuration profiles to support this	App Installer
<ol> <li>When unselected, you may nee More information </li> </ol>	ed to create configuration profiles for some software	titles.
App Installer metadata		
Application name	Installer package hash	Media source
	2d88f6164238e1ad1a8b1e64	Jamf server
Microsoft Intune Company Portal	508dc052	
Microsoft Intune Company Portal Publisher	508dc052 Installer package hash type	Media source URL

This completes this section. In the next section, we will register a Mac computer using Microsoft Intune Company Portal.



# Section 5: Register a Mac using Microsoft Intune Company Portal App and Test Microsoft PSSO.

## What You'll Need:

Learn what hardware, software, and information you'll need to complete the tutorials in this section.

#### Hardware and Software:

Requirements for following along with this section:

- A non production Mac computer running macOS 14.5 or later enrolled in Jamf Pro
- Google Chrome with the Microsoft single sign-on extension installed

In this section, we will register a Mac computer using the Microsoft Intune Company Portal App and test the Microsoft PSSO Extension by signing into Microsoft services using Safari and Google Chrome web browsers. This section will cover installing the Microsoft single sign-on extension for Google Chrome on versions prior to 136. Google Chrome version 136 added built in support for single sign-on. If you're using version 136, you can skip steps 25-31.

1. Log into your non production Mac computer.



2. Confirm you get a Registration Required notification. Click Register.



3. Click Continue.





- 4. Enter your administrative credentials.
- 5. Click Unlock.

Platform SSO	
Register your macOS account with your identity provider.	
Enter your password to allow this.	
keith	
Password	
Cancel Unlock	

- 6. Enter your Microsoft Entra account.
- 7. Click Next.

NOTE: Your sign in authentication steps may be different if you are using a passkey, security key., or Microsoft Authenticator.

	Register your device with Microsoft Entra	
	Microsoft Sign in keth@hcstraining.net No account? Create one! Can't access your account? Next	• 6
	🔍 Sign-in options	
	Terms of use Privacy & cookies ••••	
(i) More information	Close	



- 8. Enter your password.
- 9. Click Sign in.

	Register your device with Microsoft Entra			
	Register your device with Microsoft Entra			8
		Terms of use	Privacy & cookies ••••	
(i) More information			Close	

10. Enter the MFA code in your Microsoft Authenticator app.



![](_page_45_Picture_0.jpeg)

11.Click Open System Settings.

<b>•</b>
Enable your Entra ID passkey
To use your Entra ID passkey, you must enable Company Portal as a Passkey Provider.
To complete this action, open the System Settings app and navigate to: General > Autofill & Passwords > Autofill from > Enable Company Portal.
AutoFill Passwords and Passkeys Automatically suggest passwords, passkeys, and verification codes when signing in to apps and websites.
AutoFill from
Passwords C
Company Portal
Open System Settings
Dismiss

12.Enable Company Portal.

•••	< > AutoFill & Passwords
Q Search	All Your Passwords in One Place         ×           Passwords, passkeys, and verification codes are safely stored in the new Passwords app and are available to use in Safari and other apps.
Image Creation Tools Are Here	Open Passwords
<ul> <li>Wi-Fi</li> <li>Bluetooth</li> <li>Network</li> </ul>	AutoFill Passwords and Passkeys Automatically suggest passwords, passkeys, and verification codes when signing in to apps and websites.
Battery	AutoFill from
<ul> <li>Ceneral</li> <li>Accessibility</li> <li>Appearance</li> <li>Apple Intelligence &amp; Siri</li> </ul>	Passwords Passkeys, passwords, and codes     Image: Company Portal Passkeys
Control Center Desktop & Dock Displays	Verification Codes Delete After Use Automatically delete verification codes in Messages and Mail after they are used.
Spotlight By Wallpaper	Set Up Codes In Passwords will be used to open links for setting up verification codes and QR codes.

## 13.Click Close.

ſ	Microsoft Entra ID
	Successfully configured your Entra ID passkey.
	Close

![](_page_46_Picture_0.jpeg)

#### 14.Click Close.

![](_page_46_Picture_2.jpeg)

15. Let's check our registration and tokens. Open System Settings.

![](_page_46_Picture_4.jpeg)

16.Click Users & Groups.

17.Click on info((i)) next to your user name.

![](_page_46_Picture_7.jpeg)

![](_page_47_Picture_0.jpeg)

18.Look at the information in the Platform Single Sign-on section. Confirm the following:A. Login: Shows your user account in Microsoft Entra.

- B. Method: Secure Enclave.C. Registration: Shows as Registered.
- D. Tokens: SSO tokens are present.

## 19.Click OK.

User na	ime	keith
Passwo	rd	Change
Allow the You can	nis user to administer this computer not remove yourself from administrators.	
Platfor	m Single Sign-on	
Login		keith@hcstraining.net 🖛
Method	I	Secure enclave key 👇
Registre Regist	ation ered	Repair
Tokens	nkens present	Authenticate

#### 20.Click Edit.

	< > Users & Groups	
Q Search	keith Admin	(j)
Spotlight		
🛞 Wallpaper	Guest User	(j)
Notifications		Add Group Add User
🚺 Sound		
C Focus	Automatically log in as	Off C
Screen Time		
Lock Screen	Network account server	Edit
🕛 Privacy & Security		
Touch ID & Password		?
LUSERS & Groups		

21. This will show the Mac SSO Extension as Registered. Click Done.

	No Servers	
+ -		
Platform Single Sign-o	n	
Mac SSO Extensi • Registered	ion	Repair

22. Open Terminal.app located in /Applications/Utilities.

![](_page_47_Picture_13.jpeg)

Terminal

![](_page_48_Picture_0.jpeg)

## 23.Run the following command:

![](_page_48_Figure_2.jpeg)

24. You will see a lot of information on the screen. Scroll to the bottom to view the SSO Token and Expiration information.

![](_page_48_Picture_4.jpeg)

25.Let's test out the Microsoft Platform SSO Extension. Open Google Chrome.

![](_page_48_Picture_6.jpeg)

## 26.Go to:

https://chromewebstore.google.com/detail/microsoft-single-sign-on/ ppnbnpeolgkicgegkbkbjmhlideopiji?hl=en

## 27.Click Add to Chrome.

chrome web store	Q Search extensions and themes	: ::
Discover Extensions Themes		
Microsoft Single Sig	n On	Add to Chrome
2.5 ★ (761 ratings) < Share		
Extension Workflow & Planning 34,000,000 users		

#### 28.Click Add extension.

Add "Microsoft Single Sign On"?
It can:
Read and change all your data on all websites
Communicate with cooperating native applications
Cancel Add extension

## 29. Click Close (X).

![](_page_48_Picture_14.jpeg)

![](_page_49_Picture_0.jpeg)

- 30. To test the Microsoft Single Sign on Google Chrome Extension. Go to: <u>https://mysignins.microsoft.com/security-info</u>
- 31.Confirm you were not prompted to sign in. This is because your Mac computer has a Platform SSO token.

My Sign-Ins   Sec	urity Info   M × +				<b>`</b>
$\leftrightarrow$ $\rightarrow$ C $\sim$ mysigning	.microsoft.com/security-info			☆	Ď∣© :
000000000000000000000000000000000000					Р. ? (КМ)
<ul> <li>Q Overview</li> <li>𝑘 Security info</li> <li>□ Devices</li> </ul>	Security info These are the methods you use to sign into y You're using the most advisable sign-in me Sign-in method when most advisable is unavilable. Microsoft A	rour account or reset your password. thod where it applies. uthenticator notification Change			
💫 Password	+ Add sign-in method				
Organizations	S Phone	+1 1	Change	Delete	
🔒 Settings & Privacy	••• Password	Last updated: 5 months ago	Change		
🕚 Recent activity	<ul> <li>Microsoft Authenticator</li> <li>Push multi-factor authentication (MFA)</li> </ul>	iPhone 14 Pro Max		Delete	
	Security key Security Key	Keith's Yubikey		Delete	~
	Passkey Microsoft Authenticator	Authenticator - iOS iOS device		Delete	~
	Lost device? Sign out everywhere				

- 32. To test using Safari, sign into a different Microsoft service which has native support for Microsoft Platform SSO, Open Safari.
- 33.Go to: https://www.office.com
- 34.Click Sign in.

![](_page_49_Picture_7.jpeg)

![](_page_50_Picture_0.jpeg)

35. Make a selection of your choosing. This guide will select Allow.

![](_page_50_Picture_2.jpeg)

36. You will not be prompted to sign in as your Mac computer has a Platform SSO token.

![](_page_50_Picture_4.jpeg)

This completes this section. In the next section, we will use Jamf Connect with the Microsoft PSSO Extension to show how they can work together to provide a solution to Password syncing while using the Secure Enclave authentication method.

![](_page_51_Picture_0.jpeg)

# Section 6: Configuring Microsoft Entra for use with Jamf Connect and PSSO

## What You'll Need:

Learn what hardware, software, and information you'll need to complete the tutorials in this section.

#### Hardware and Software:

Requirements for following along with this section:

- A Mac Computer with the Jamf Connect Configuration app installed. This guide will use version 2.45.1
- Administrative privileges in Microsoft Entra

To ensure Microsoft Authenticator is used instead of FIDO2 authentication methods with Jamf Connect, specific configuration in Microsoft Entra ID is required due to how Jamf Connect operates. Jamf Connect uses WebKit, the macOS-native rendering engine, at the login window which is not a full browser. This presents limitations when handling advanced authentication methods like FIDO2, which rely on features not supported in WebKit such as browser extensions or certain redirect behaviors.

Because of these limitations, Microsoft recommends enforcing the use of Microsoft Authenticator or password-based methods instead of FIDO2 for Jamf Connect when the secure enclave method is used and password syncing is required. This is achieved by:

- Configuring Conditional Access Policies in Microsoft Entra ID to target a specific cloud app.
- Modifying Jamf Connect's App Registration to support Conditional Access scenarios where only compatible authentication methods like Microsoft Authenticator are allowed.
- Avoiding FIDO2 because it may not complete successfully within the WebKit-based login window used by Jamf Connect.

This configuration ensures a smoother and more secure user experience during macOS login while maintaining compliance with organizational authentication policies. It also allows local account password syncing when using Jamf Connect with the secure enclave method.

In this section, we will configure the following:

- Configure an administrative account in Microsoft Entra with the required roles to create a custom security attribute for MFA exceptions.
- Create a custom security attribute for MFA exceptions.
- Create an application registration with a custom API.
- Create an application registration to call a custom scope.
- Apply the custom security attribute to Jamf Connect Enterprise application.
- Create a conditional access authentication strength to specify which combinations of authentication methods can be used to access Jamf Connect.
- Create a conditional access policy to enforce rules on the Jamf Connect application.
- Create a Jamf Connect configuration profile with conditional access settings.

While not required, Jamf recommends creating new application registrations for Jamf Connect instead of modifying existing application registrations. This will help prevent unexpected errors or conflicts during deployment to your organization. We recommend using a Microsoft Entra development server to test the steps in this section before using it in production. This guide will create all the app registrations needed for Jamf Connect.

This section discusses a topic that is often brought up by organizations when using the Secure Enclave method with Jamf connect to provide password syncing. Keep in mind, Microsoft's long term vision is to move organizations away from password syncing and recommends the guidance below.

Microsoft does not recommend using the Resource Owner Password Credential (ROPC) flow to synchronize the local macOS password with the user's Entra ID password. While authentication at the macOS login window via the OIDC (OpenID Connect) flow, such as with an authenticator app or Jamf Connect is supported, Microsoft's long-term vision is for organizations to treat the local Mac password similarly to the Windows Hello for Business (WHfB) PIN.

From Microsoft's perspective, tools like Jamf Connect at the macOS login window are acceptable for federated authentication, but password synchronization should be avoided as part of a broader security modernization effort. If organizations continue to implement password sync today, it is

![](_page_52_Picture_0.jpeg)

recommended that they consider deprecating it in the medium to long term. This aligns with current Microsoft guidance for Windows environments, where passwordless and non-synced credential models (e.g., WHfB, FIDO2, and certificate-based auth) are becoming the standard.

For more information on what we are configuring in this section, see the official Jamf documentation at the links below:

https://learn.jamf.com/en-US/bundle/jamf-connect-documentation-current/page/Entra\_ID\_ Conditional Access and All Cloud Apps.html

https://learn.jamf.com/en-US/bundle/jamf-connect-documentation-current/page/Modifying\_Jamf\_ Connect\_for\_Conditional\_Access\_Polices.html

Here is a video from JNUC 2023 that explains conditional access with Jamf Connect. <u>https://www.youtube.com/watch?v=D9-4miD-3pM</u>

- 1. To add the required roles to your account, log into Microsoft Entra.
- 2. Click Users.
- 3. Click All Users.
- 4. Select your user account.

A Home ✓ What's new		Home > Users HCS Training	
Diagnose & solve problems		🚨 All users	≪ + New user ∨ ⊘ Edit (Pre
★ Favorites	$\sim$	Audit logs	Azure Active Directory is now     Search
Identity	^	<ul> <li>Sign-in logs</li> <li>Diagnose and solve problems</li> </ul>	2 users found
() Overview		💰 Deleted users	Display name ↑
8 Users	~	📍 Password reset	CC Craig Cohen
		User settings	KM Keith Mitnick
All users		👶 Bulk operation results	

- 5. Click Assigned roles.
- 6. Confirm you have the following roles:
  - Attribute assignment administrator
  - Attribute assignment reader
  - Attribute definition administrator
  - Attribute definition reader

NOTE: Having Global Administrator rights are not enough, you must assign the roles above to your Global Administrator account.

7. If the above roles are not assigned to you, Click Add assignments (+). You cannot continue with this section without having the above roles assigned to your account.

<ul> <li>Home</li> <li>What's new</li> </ul>	··· > Password reset   Properties > S Keith Mitnick   Assi User	security profiles > Conditional Access   Policies > Jamf Connect - Require Multifactor Authentication
Diagnose & solve problems		$+$ Add assignments 💍 Refresh $\mid  otic R P$ Got feedback?
★ Favorites	<ul> <li>Vverview</li> <li>Audit logs</li> </ul>	Eligible assignments Active assignments Expired assignments
Identity	<ul> <li>Sign-in logs</li> <li>Diagnose and solve problems</li> </ul>	Y Search by role       Role     ↑↓     Principal name     Scope
(i) Overview	Custom security attributes	Attribute Definition Administrator keith@hcstraining.net Directory
8 Users	Assigned roles	Attribute Assignment Administrator keith@hcstraining.net Directory
	Administrative units	Attribute Definition Reader keith@hcstraining.net Directory
All users	A Groups	Attribute Assignment Reader keith@hcstraining.net Directory
Deleted users	Applications	Global Administrator keith@hcstraining.net Directory
5		

![](_page_53_Picture_0.jpeg)

- 8. To create a custom security attribute, click Protection.
- 9. Click Custom security attributes.
- 10.Click Add attribute set.

![](_page_53_Picture_4.jpeg)

- 11.Enter JamfConnectAttributes for Attribute set name (The name cannot contain more than 32 characters, spaces, or special characters.)
- 12. Enter Jamf Connect Security Attributes for the Description.
- 13.Enter 25 for Maximum number of attributes.
- 14.Click Add.

Add an attribute set to group a security attributes must be a pa	nd manage related custom security attributes. All rt of an attribute set. Learn more	custom
Attribute set name * 🛈	JamfConnectAttributes	ו
Description ①	Jamf Connect Security Attributes	~
Maximum number of attributes	① 25	•

![](_page_54_Picture_0.jpeg)

15.Click on JamfConnectAttributes to open it.

Home > Custom attribu	ites		×
+ Add attribute set	Refresh   🛱 Got feedback?		
Search attribute set nan	ne	]	
Attribute set name	$\uparrow_{\downarrow}$ Description	Maximum number of attributes	
JamfConnectAttributes	Jamf Connect Security Attri	butes 25	

## 16.Click Add attribute (+).

Home > Custom attributes >			
📀 JamfConnectAttril	outes   Active attributes		
<ul> <li>Active attributes</li> </ul>	Add attribute 🗇 Deactivate att	ribute   💍 Refresh   🖗 Go	t feedback?
Deactivated attributes	٩	dal avota na avoita e attribu	
Roles and administrators	Custom define ar users or	ecurity attributes are key-value pair ad assign to Microsoft Entra objects, applications. Learn more	s that you such as
	≋≡	<b>\$</b>	2.
	1. Define attributes	2. Manage attributes	3. Assign attributes
	Add custom security attributes to your directory.	Specify who can define and assign custom security attributes.	Assign custom security attributes to Microsoft Entr objects for your scenario.
		Add attribute	

17.Enter JamfConnectExemptCA for the Attribute name.

18. Enter Jamf Connect Exempt Conditional Access for the Description.

- 19.Select String for Description.
- 20.Select No for Allow multiples values to be assigned.
- 21.Select Yes for Only allow predefined values to be assigned.
- 22.Click Add Value.

Home > Custom attributes > JamfConnect	Attributes   Active attributes >	
New attribute	×	
Add a custom security attribute (key-value pair) more	to your directory that you can later assign to Microsoft Entra objects, such as users or applications. Learn	
Attribute name * ()	JamfConnectExemptCA	—17
Description ()	Jamf Connect Exempt Conditional Access	
Data type *	String	
Allow multiple values to be assigned $\bigcirc$	○ Yes ● No ●	<u> </u>
Only allow predefined values to be assigned	• Yes No	<u> </u>
Predefined values ①	+ Add value	
	Value 1 1 Is active?	

![](_page_55_Picture_0.jpeg)

- 23.Enter **Exempt** for the Value.
- 24.Select the checkbox for Is active?.
- 25.Click Add.
- 26.Click Save.

26

New attribute			
		Add a single predefined value of the selected data type.	
Add a custom security attribute (key-value pair) to more	your directory that you can later assign to Micros	Value *	
Attribute name * 🕕	JamfConnectExemptCA	Is active?	
Description ①	Jamf Connect Exempt Conditional Access		
Data type *	String		
Allow multiple values to be assigned ①	🔿 Yes 💿 No		
Only allow predefined values to be assigned ①	● Yes ○ No		
Predefined values	+ Add value		
	Value		
	No results		

27.Confirm the active attribute shows in the list.

Home > Custom attributes >					
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	+ Add attribute 😑 Deactivate attribute 🛛 💍 Refresh 🔰 🔗 Got feedback?				
<ul> <li>Active attributes</li> </ul>					
Ø Deactivated attributes	Search attribute name				
<ol> <li>Roles and administrators</li> </ol>	Attribute name ↑↓ Description	Data type	Predefined values		
	JamfConnectExemptCA Jamf Connect Exempt Conditional Access	String	Exempt		
l					

- 28. To create an app registration with a custom API, click Applications.
- 29.Select App registrations.
- 30. Click New registration (+).

![](_page_55_Picture_11.jpeg)

![](_page_56_Picture_0.jpeg)

- 31. Enter Jamf Connect Conditional Access Policy API for the Name.
- 32.Select the Radio Button for Accounts in this organizational directory only (<Company Name> only Single tenant). [HCS Training is used for the company name in this example].
- 33.Click Register.

Home > Custom attributes > App registrations > Enterprise applications   All applications > App registrations >
Register an application
* Name
The user-facing display name for this application (this can be changed later).
Jamf Connect - Conditional Access Policy AP
Supported account types
Who can use this application or access this API?
Accounts in this organizational directory only (HCS Training only - Single tenant)
O Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)
<ul> <li>Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)</li> </ul>
O Personal Microsoft accounts only
Help me choose
Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.
Select a platform V e.g. https://example.com/auth
Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from Enterprise applications.

![](_page_57_Picture_0.jpeg)

34. Click API permissions.

35. Click Grant admin consent for <Company Name>. (HCS Training is used in the example)

![](_page_57_Picture_3.jpeg)

#### 36.Click Yes.

ſ	Grant admin consent confirmation.
	Do you want to grant consent for the requested permissions for all accounts in HCS Training? This will update any existing admin consent records this application already has to match what is listed below.
l	Yes No

- 37.Under Status, confirm "Granted for <Company Name>" is active. This is indicated with a ♥ (HCS Training is used for the company name in the example)
- 38.In the sidebar, click Expose an API.

Home > Custom attributes > App regist	rations > Enterprise applications   All applications > App registrations > Jamf Connect - Conditional Access Policy API ditional Access Policy API   API permissions  * ···· C) Refresh   R Got feedback?	×
<ul> <li>Overview</li> <li>Quickstart</li> <li>Integration assistant</li> </ul>	Successfully granted admin consent for the requested permissions.	×
Manage     Branding & properties	Granting tenant-wide consent may revoke permissions that have already been granted tenant-wide for that application. Permissions that users have already granted on their own behalf aren't affected. Learn more	×
Authentication     Certificates & secrets	The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. Learn more Configured permissions	
API permissions     Expose an API	Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of confi permissions should include all the permissions the application needs. Learn more about permissions and consent + Add a permission $\checkmark$ Grant admin consent for HCS Training	gured
App roles       App roles       App roles       App roles	API / Permissions na Type Description Admin consent req Status	
Koles and administrators     Manifest     Support + Troubleshooting	User.Read Delegated Sign in and read user profile No Strand for HCS Training	
New support request		

![](_page_58_Picture_0.jpeg)

39.In the Application ID URI section, click Add.

Н	ome > Custom attributes > App regist	rations > Enterprise applications   All applications > App registrations > Jamf Connect - Conditional Access Policy API					
	👩 Jamf Connect - Conditional Access Policy API   Expose an API 🔗 😁						
	C Search «	R Got feedback?					
	Overview						
4	Quickstart						

40.Confirm the Application ID URI. Leave it at it's default value.

41.Click Save.

Edit application ID URI	×	
The globally unique URI used to identify this web API. It is the prefix for scope tokens, it is the value of the audience claim. Also referred to as an identifier UI	s and in access RI.	
Application ID URI		
api://b0127250-c527-4514-a87f-cca50fda6a4c	•	—
Save Discard		
	J	

## 42.Click Add a scope (+).

41

Home > Custom attributes > App regis	trations > Enterprise applica	tions   All a	API   Expose a	istrations > Jamf Connect n API ☆ …	: - Conditional Access Po	olicy API
✓ Search «	🔗 Got feedback?					
<ul> <li>Overview</li> <li>Quickstart</li> </ul>	Application ID URI : api://	b0127250-	c527-4514-a87f-cca50fda	6a4c 🗈 Edit		
<ul> <li>Integration assistant</li> <li>Diagnose and solve problems</li> <li>Manage</li> </ul>	Scopes defined by this Define custom scopes to res API can request that a user c	API trict access r admin coi	to data and functionality nsent to one or more of t	protected by the API. An app hese.	plication that requires acc	ess to parts of this
Branding & properties	Adding a scope here creates assignable to application typ	only delega e. Go to Ap	ated permissions. If you a proles.	re looking to create applicat	ion-only scopes, use 'App	roles' and define app roles
<ul> <li>Authentication</li> <li>Certificates &amp; secrets</li> </ul>	+ Add a scope		42			
Token configuration	Scopes		Who can consent	Admin consent disp	User consent displa	State
->- API permissions	No scopes have been defin	ed				
🙆 Expose an API						
App roles Owners	Authorized client applie Authorizing a client applicati this API.	ations	s that this API trusts the a	pplication and users should	not be asked to consent v	when the client calls

![](_page_59_Picture_0.jpeg)

43. Enter **jamfconnect** for the Scope name.

44. Set who can consent. This guide will use Admins only.

45.Enter **Read user files** for Admin consent display name.

46.Enter Allows the app to read the signed in users files for Admin consent description.

47.Set the State to Enabled.

### 48.Click Add Scope.

NOTE: We are not actually reading the users files, we are reading the users information in Entra. For more info on this, go here: https://learn.microsoft.com/en-us/graph/permissions-reference#userread

	Add a scope	×	
	Scope name * ①		
	jamfconnect	•	<b>—</b> 43
	api://b0 :/jamfconnect		
	Who can consent? () Admins and users Admins only		
	Admin consent display name * ①		
	Read user files	•	<b>— 4</b> 5
	Admin consent description * ①		
	Allows the app to read the signed in users files	•	<b>— 46</b>
	User consent display name		
	e.g. Read your files		
	e.g. Allows the app to read your files.		
17	State ()		
4/—	Enabled		
19			

## 49. Confirm the Application ID URI and Scope were created.

Home > Custom attributes > App reg	gistrations > Enterprise applications   Al	applications > App regi	strations > Jamf Connect	- Conditional Access Pol	licy API
🙆 Jamf Connect - Co	nditional Access Policy	API   Expose a	n API 🛷 …		×
Search «	🛜 Got feedback?				
Overview					
n Quickstart	Got a second to give us some feet	dback? $\rightarrow$			~
<ul> <li>Integration assistant</li> <li>Diagnose and solve problems</li> </ul>	Application ID URI : api://b01	<527 4514 all <sup>27</sup> cubillia	🗈 Edit		
Manage	Scopes defined by this API				
Branding & properties	Define custom scopes to restrict acces	s to data and functionality r	protected by the APL An apr	lication that requires acce	ss to parts of this
Authentication	API can request that a user or admin o	onsent to one or more of th	iese.		
🕈 Certificates & secrets	Adding a scope here creates only dele	gated permissions. If you ar	e looking to create applicati	on-only scopes, use 'App	roles' and define app roles
Token configuration	assignable to application type. Go to A	pp roles.			
<ul> <li>API permissions</li> </ul>	+ Add a scope				
<ul> <li>Expose an API</li> </ul>	Scopes	Who can consent	Admin consent disp	User consent displa	State
App roles	api://b :	Admins only	Read user files		Enabled
🔉 Owners	L				
Roles and administrators	Authorized client applications				

![](_page_60_Picture_0.jpeg)

50.Let's create an app registration to call a custom scope. Click Applications.

51.Select App registrations.

52. Click New registration (+).

![](_page_60_Picture_4.jpeg)

53. Enter Jamf Connect - OIDC Endpoint for the Name.

- 54.Select the radio button for Accounts in this organizational directory only (<Company Name> only Single tenant) [HCS Training is used for the company name in the example].
- 55. Select Public client/native (mobile) under Redirect URI.
- 56.Click Register.

![](_page_60_Picture_9.jpeg)

![](_page_61_Picture_0.jpeg)

- 57.Click Authentication.
- 58. Select Yes for Allow public client flows.
- 59.Click Save.

![](_page_61_Picture_4.jpeg)

- 60. Click API permissions.
- 61. Click Grant admin consent for <Company Name> (HCS Training is used in the example).

		ations > App registrations > Jamf Connect - OIDC Endpoint   Expose an API > App registrations > Jamf Connect - OIDC Endpoint <b>C Endpoint   API permissions</b> $\not\approx$	×			
	Search «					
	<ul> <li>Quickstart</li> <li>Integration assistant</li> <li>Diagnose and solve problems</li> <li>Manage</li> <li>Branding &amp; properties</li> </ul>	Granting tenant-wide consent may revoke permissions that have already been granted tenant-wide for that application. Permissions that users have already granted on their own behalf aren't affected. Learn more	×			
60		The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. Learn more				
	Authentication     Configured permissions     Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of consent permissions should include all the permissions the application needs. Learn more about permissions and consent     Add a permission     Add a permission     Add a permission     Grant admin consent for HCS Training     G1					
	<ul> <li>Expose an API</li> <li>Expose an API</li> </ul>	API / Permissions name Type Description Admin consent req Status				
	App roles     Owners	User.Read Delegated Sign in and read user profile No				
	<ul> <li>Roles and administrators</li> <li>Manifest</li> </ul>	To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try Enterprise applications.				
	Support + Troubleshooting					

![](_page_62_Picture_0.jpeg)

## 62.Click Yes.

Grant admin consent confirmation.
Do you want to grant consent for the requested permissions for all accounts in HCS Training? This will update any existing admin consent records this application already has to match what is listed below.
Yes No

# 63.Click Add a permission (+).

··· > Enterprise applications   All appli	cations > App registrations > Jamf	Connect - OIDC Endpoint   Expose an API	> App registrations > Jar	nf Connect - OIDC Endpoint	
Jamf Connect - OID	C Endpoint   API pern	nissions 🖈 …			$\times$
	💍 Refresh   🐬 Got feedback	?			
Overview	<ol> <li>Successfully granted admin cons</li> </ol>	sent for the requested permissions.			
📣 Quickstart					
🚀 Integration assistant					
X Diagnose and solve problems	Granting tenant-wide consent m have already granted on their ov	ay revoke permissions that have already been gr vn behalf aren't affected. <u>Learn more</u>	ranted tenant-wide for that app	lication. Permissions that users	×
Manage					
Branding & properties	The "Admin consent required" or	olumn shows the default value for an organizatio	n However user consent can h	e customized per permission use	×
Authentication	or app. This column may not refl	lect the value in your organization, or in organiza	ations where this app will be use	ed. Learn more	· ·
📍 Certificates & secrets	Configured normissions				
Token configuration	Applications are authorized to call AP	Ne when they are granted permissions by use	re admine as part of the con	sent process. The list of configu	rad
API permissions	permissions should include all the pe	rmissions the application needs. Learn more	about permissions and conse	ent	leu
🔷 Expose an API	$+$ Add a permission $\checkmark$ Grant a	admin consent for HCS Training			
App roles	API / Permissions name Type	Description	Admin consent req	Status	
A Owners	✓ Microsoft Graph (1)				
Roles and administrators	User Read Delegate	ed Sign in and read user profile	No	Granted for HCS Training	
10 Manifest	Delegan			-	
Support + Troubleshooting	To view and manage consented perm	nissions for individual apps, as well as your te	nant's consent settings, try E	nterprise applications.	
New support request					

- 64. Click APIs my organization uses.
- 65.In the search field, enter Jamf Connect.
- 66.Select Jamf Connect Conditional Access Policy API.

Request API permissions	×	
Select an API64		
Microsoft APIs APIs my organization uses My APIs		
Apps in your directory that expose APIs are shown below		
Name	Application (client) ID	
Jamf Connect - Conditional Access Policy API	b	

![](_page_63_Picture_0.jpeg)

- 67.Select Delegated permissions.
- 68.Select the checkbox for jamfconnect under Permissions.
- 69.Click Add permissions.

	Request API permissions	Х
	All APIs Jamf Connect - Conditional Access Policy API api://b0127250-c527-4514-a87f-cca50fda6a4c What type of permissions does your application require?	
7—	Delegated permissions Your application needs to access the API as the signed-in user.	
	Application permissions Your application runs as a background service or daemon without a signed-in user.	
	Select permissions	expand all
	The "Admin consent required" column shows the default value for an organization permission, user, or app. This column may not reflect the value in your organization more	n. However, user consent can be customized per $$\times$$ on, or in organizations where this app will be used. Learn
	Permission	Admin consent required
	✓ Permissions (1)	
В——	jamfconnect ① Read user files	Yes
9——	Add permissions Discard	

70. Click Grant admin consent for <Comapny Name> (HCS Training is used in the example).

> Enterprise applications   All applications > App registrations > Jamf Connect - OIDC Endpoint   Expose an API > App registrations > Jamf Connect - OIDC Endpoint									
Jamf Connect - OID	Imf Connect - OIDC Endpoint   API permissions 🖉 🖤								
	🖔 Refresh 🛛 🕅 Got	feedback?							
👯 Overview	🛕 You are editing permi	ission(s) to you	r application, users will have to conse	nt even if they've already done so prev	riously.				
🏜 Quickstart									
🚀 Integration assistant									
✗ Diagnose and solve problems	Granting tenant-wide have already granted	consent may r on their own b	evoke permissions that have already ehalf aren't affected. <u>Learn more</u>	been granted tenant-wide for that app	lication. Permissions that users	×			
Manage									
💳 Branding & properties	The "Admin consent r	equired" colun	nn shows the default value for an org	anization. However, user consent can b	e customized per permission, us	er, ×			
Authentication	or app. This column n	nay not reflect	the value in your organization, or in c	rganizations where this app will be use	ed. Learn more				
📍 Certificates & secrets	Configurad parmission	26							
Token configuration	Applications are authorized	to call APIs v	when they are granted permissions	by users/admins as part of the con	sent process. The list of config	ured			
<ul> <li>API permissions</li> </ul>	permissions should include	all the permi	ssions the application needs. Learn	more about permissions and conse	ent	Jicu			
Expose an API	+ Add a permission	<ul> <li>Grant adm</li> </ul>	in consent for HCS Training						
App roles	API / Permissions name	Туре	Description	Admin consent req	Status				
A Owners	V Jamf Connect - Conditi								
Roles and administrators	jamfconnect	Delegated	Read user files	Yes	Not granted for HCS Tra.	•••			
🔟 Manifest	V Microsoft Graph (1)								
Support + Troubleshooting	User.Read	Delegated	Sign in and read user profile	No	Granted for HCS Training				
New support request									

![](_page_64_Picture_0.jpeg)

#### 71.Click Yes.

Grant admin consent confirmation.
Do you want to grant consent for the requested permissions for all accounts in HCS Training? This will update any existing admin consent records this application already has to match what is listed below.
Yes No

72. In the Status section, confirm Granted for <Company Name> is active for both entries. This is indicated with a Ø (HCS Training is used for the company name in the example).

NOTE: Roles can be added to this app registration if required but we will not configure them in this guide. Roles allow a user that logs in with Jamf Connect, to query Microsoft Entra and if the user is an administrator in Entra, they will be created or converted to an administrator on their Mac. If they are a standard user in Microsoft Entra, they will be created or converted to a standard user on their Mac. To add roles to this app registration, follow the instructions for optional roles here: <a href="https://learn.jamf.com/en-US/bundle/jamf-connect-documentation-current/page/Modifying\_Jamf\_Connect\_for\_Conditional\_Access\_Polices.html#ariaid-title3">https://learn.jamf.con/en-US/bundle/jamf-connect-documentation-current/page/Modifying\_Jamf\_Connect\_for\_Conditional\_Access\_Polices.html#ariaid-title3</a>

![](_page_64_Picture_5.jpeg)

- 73. Let's apply the custom security attribute to the Jamf Connect Enterprise application. From the sidebar, Click Enterprise applications.
- 74. Click Jamf Connect Conditional Access Policy API.

		Homo		··· > Jamf Connect - OIDC Endpoint   B	Expose an API > App registrations > Jamf Connect - O			
	-	What's new		Enterprise applications   All applications				
		Diagnose & solve problems		« Overview	+ New application 💍 Refresh 🞍 Download (Ex			
	*	Favorites	$\sim$	Overview	View, filter, and search applications in your organization t			
	4	Identity	^	Manage	Search by application name or object ID			
	0	Overview		All applications	Application type == Enterprise Applications $\times$			
	8	Users	$\sim$	Private Network connectors	3 applications found			
	<sup>9</sup> 29	Groups	$\sim$	<ul> <li>User settings</li> <li>App launchers</li> </ul>	Name JC Jamf Connect - OIDC Endpoint			
	-63	Devices	$\sim$	Custom authentication extensions	JC Jamf Connect - Conditional Access Policy API			
	₩,	Applications	^	Security	JP Jamf Pro Entra ID Connector			
73—	-0	Enterprise applications		💺 Conditional Access				

![](_page_65_Picture_0.jpeg)

75.Click Custom security attributes.

> Jamf Connect - Conditional Acc	> Jamf Connect - Conditional Access Policy API   Properties > Enterprise applications   All applications									
Enterprise Application	nditional Access Policy API   Overview									
iii Overview	Properties									
Deployment Plan	Name ①									
🗙 Diagnose and solve problems	Jamf Connect - Conditional 🗈									
Manage	Application ID ()									
Properties	Object ID ①									
A Owners	aa2cff83-a2a7-4272-b284-f4 🗈									
Roles and administrators	Getting Started									
Users and groups										
➔ Single sign-on										
Provisioning	1. Assign users and groups									
Application proxy	Provide specific users and groups access to the applications									
Self-service	Assign users and groups									
75 Custom security attributes										

76.Click Add assignment.

··· > Enterprise applications   All a         Image: Second state of the second state of	applica onc	itions > Jamf Connect -	Conditional Access Policy	API JStom security a	attr ×		
👪 Overview	~	🖫 Save 🗙 Discard	+ Add assignment	× Remove assignment	🖗 Got feedback?		
Deployment Plan			es or values	+ <sub>▼</sub> Add filters			
X Diagnose and solve problems		Attribute set	Attribute name	Attribute descrip	Data type		
Manage No attributes assigned to this application yet. You can add one now.							
Properties		Add assignment					

77.Under Attribute set, from the menu, select JamfConnectAttributes.

78. Under Attribute Name, from the menu, select JamfConnectExemptCA.

79.Under Assigned Value, select Exempt.

80.Click Save.

81.Confirm the settings as shown below.

> App registrations > Enterprise applications > Iamf Connect - Conditional Access Policy API   Properties > Enterprise applications   All applications > Jamf Connect - Conditional Access Policy API								
Jamf Connect - Conditional Access Policy API   Custom security attributes								
80	Save X Discard   + Add assignment	t X Remove assignment	R Got feedback?					
Deployment Plan	Search attribute names or values	+ <sub>▼</sub> Add filters						
× Diagnose and solve problems	Attribute set	Attribute name	Attribute description	Data type	Multi-valued	Assigned values		
Manage	JamfConnectAttributes	JamfConnectExemptCA	Jamf Connect Exempt Co	String	No	Exempt	~	
7778								

![](_page_66_Picture_0.jpeg)

- 82.Let's create a conditional access authentication strength to specify which combinations of authentication methods can be used to access Jamf Connect. From the sidebar, click Protection.
- 83.Click Authentication methods.
- 84. Click Policies and view the different authentication methods that are enabled.
- 85.Click Authentication strengths.

When there are multiple authentication method policies enabled, some methods like Passkey FIDO2 and other FIDO2 methods will not work at the Jamf Connect Login window. A conditional access authentication strength will allow us to force authentication methods that are supported by Jamf Connect at the login window like Microsoft Authenticator.

![](_page_66_Picture_6.jpeg)

86.Click New authentication strength.

··· > Jamf Connect - Conditional Acc	ess Policy API   Custom security attributes >	Conditional Access	Policies > Jamf Connect - Require Multifactor Au	thentication > Authentication me
Authentication met HCS Training - Microsoft Entra ID Secur	thods   Authentication stre	engths		
	+ New authentication strength 💍 Ref	fresh		
Manage	Authentication strengths determine the com	bination of authenticat	tion methods that can be used.	
Policies	Learn more 🖸	_		
Password protection	Type: All Authentication methods: All	₩ Reset filters		
📙 Registration campaign				
Q Authentication strengths	Authentication strength	Type Authe	entication methods	Conditional access policies

![](_page_67_Picture_0.jpeg)

- 87.Enter JamfConnect Authenticator ONLY for the Name.
- 88. Enter Only Microsoft Authenticator is used for MFA with Jamf Connect for the Description.
- 89. In the Multifactor authentication section, select the checkbox for Password + Microsoft Authenticator (Push Notifications).
- 90. Click Next.

Configure	Review	
Name *		
JamfConn	ect Authenticator ONLY	
Description		
Only Micro	osoft Authenticator is used for MFA with Jamf Connect	
Searc	h authentication combinations	
	Phishing-resistant MFA (3)	
	Passwordless MFA (1)	
	<ul> <li>Multifactor authentication (13)</li> </ul>	
	Temporary Access Pass (One-time use)	
	Temporary Access Pass (Multi-use)	
-	Password + Microsoft Authenticator (Push Notification)	
	Password + Software OATH token	
	Password + Hardware OATH token	
	Password + SMS	
	Password + Voice	

91.Click Create.

New authentication strength	×
Configure Review	
During sign in, users will be required to authenticate using one of the following:	
Password + Microsoft Authenticator (Push Notification)	
Previous Create	

![](_page_68_Picture_0.jpeg)

92.Confirm the authentication strength shows in the list.

Search     Samf Connect - Conditional Acces     Authentication meth     HCS Training - Microsoft Entra ID Security     Search     «	s Policy API   Custom security attributes nods   Authentication str y + New authentication strength () 6	> Conditional ) rengths	Access   Policies > Jamf Connect - Require Multifactor # 	uthentication > Authentication methods	
Manage Policies Password protection Registration campaign	Authentication strengths determine the co Learn more (2 Type: All Authentication methods: All Authentication strength	ombination of au	thentication methods that can be used. Authentication methods	Conditional access policies	
Authentication strengths     Settings     Monitoring	JamfConnect Authenticator ONLY	Custom	Password + Microsoft Authenticator (Push Notifica	Not configured in any policy yet	
mi     Activity       Image: Contract of the second	Multifactor authentication	Built-in	Windows Hello For Business / Platform Credential	Not configured in any policy yet	
Registration and reset events	Passwordless MFA Phishing-resistant MFA	Built-in Built-in	Windows Hello For Business / Platform Credential Windows Hello For Business / Platform Credential	Not configured in any policy yet	

- 93.Let's create a conditional access policy and assign the authentication strength we just created to it. From the sidebar, select Protection.
- 94. Click Conditional access.
- 95.Click Policies.

96.Click New policy (+).

	Microsoft Entra admin center			ervices, and docs (G+/)	
	Diagnose & solve problems		··· > Jamf Connect - Conditional Acce	ss Policy API   Properti	
	★ Favorites	$\sim$	Econditional Access	Policies	
	Identity	$\sim$	<ul> <li>Overview</li> </ul>	+ New policy	- 90
93 —	• 🕹 Protection	^	Policies 95	What is Condition	
	Identity Protection		🗙 Diagnose and solve problems	Learn more 🛛	
94 —	Conditional Access		Manage	Conditions	

- 97. Enter Jamf Connect Require Multifactor Authentication for the Name.
- 98. Users: Click the users and groups selected link.

![](_page_68_Figure_10.jpeg)

![](_page_69_Picture_0.jpeg)

99.Click Include.

- 100. Select the Radio button for Select users and groups.
- 101. Enable Users and groups.

$\cdots$ > Enterprise applications   All application	ns > Jamf Connect - Conditional Access Policy AP	
New		
Conditional Access policy		
Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more c	Control access based on who the policy will apply to, such as users and groups, workload identities, directory roles, or external guests. Learn more C <sup>a</sup>	
Name *	Include Exclude	- 99
Assignments	None     All users	
Users 🕕	<ul> <li>Select users and groups</li> </ul>	- 100
Specific users included	Guest or external users ①	
Select users and groups" must be configured	Directory roles ①	
Target resources ①	Users and groups	- 101
No target resources selected		
Network NEW ①		
Not configured		
Conditions (j)		
0 conditions selected		
Access controls		
Grant ①		
0 controls selected		
Session ()		
0 controls selected		
Enable policy		
Report-only On Off		
Create		
		J

- 102. Select the appropriate Users or Groups. This guide will select one user for simplicity.
- 103. Click Select.

	<ol> <li>Try cha</li> </ol>	anging or adding filters if you don	't see what you're looking	for.
	Search	ind		
	All Users	s Groups		
		Name	Туре	Details
		Craig Cohen	User	craig@hcstraining.net
		HCS Executives	Group	
2 —		Keith Mitnick	User	keith@hcstraining.net

![](_page_70_Picture_0.jpeg)

104. Confirm your users or groups show in the list.

105. Under Target resources, click the link, No target resources selected.

ſ	··· > Enterprise applications   All applications	> Jamf Connect - Conditional Access Policy API   C	
	New		
	Conditional Access policy		
	Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more of	Control access based on who the policy will apply to, such as users and groups, workload identities, directory roles, or external guests. Learn more c	
	Name *	Include Exclude	
	Jamf Connect - Require Multifactor Authe 🗸		
	Assignments	All users	
	Users ①	<ul> <li>Select users and groups</li> </ul>	
	Specific users included	Guest or external users ①	
	Target resources ①	Directory roles ①	
105 —	No target resources selected	Users and groups	
	Network NEW ①		
	Not configured	Select	
	Conditions ①	1 user	
	0 conditions selected	KM Keith Mitnick 104	4
	Access controls		
	Grant ①		

- 106. Click Include.
- 107. Select the radio button for Select resources.
- 108. Under Select, click None.

New		
Conditional Access policy		
Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more c <sup>3</sup> Name *	Control access based on all or specific apps, internet resources, actions, or authentication context. Learn more C <sup>*</sup> Select what this policy applies to Resources (formerly cloud apps)	
Jamf Connect - Require Multifactor Authe 🗸		—106
Assignments	Include Exclude	
Specific users included	All internet resources with Global Secure	
Target resources (i)	All resources (formerly 'All cloud apps')	407
No target resources selected	Select resources	-107
Select resources" must be configured	Edit filter	
Network NEW ①	None	
Not configured	Select	
Conditions ① 0 conditions selected	None	—108
Access controls	To create a Conditional Access policy targeting members in your tenant with	
Grant 🛈	Global Secure Access (GSA) as a resource, make sure GSA is deployed in	
0 controls selected	your tenant. Learn more 2	
Session ①		
0 controls selected		

![](_page_71_Picture_0.jpeg)

- 109. Perform the following: In the search field, enter **jamf connect**.
- 110. Select the checkbox for Jamf Connect Conditional Access Policy API.
- 111. Click Select.

![](_page_71_Picture_4.jpeg)

- 112. Confirm Jamf Connect Conditional Access Policy API shows in the list.
- 113. Under Grant, Click 0 Controls selected.

	··· > Enterprise applications   All application	s > Jamf Connect - Conditional Access Policy API	Custom se
	New		
	Conditional Access policy		
	Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more c	Control access based on all or specific apps, internet resources, actions, or authentication context. Learn more c <sup>3</sup>	
	Name *	Resources (formerly cloud apps)	
	Jamf Connect - Require Multifactor Authe 🗸		
	Assignments	Include Exclude	
	Users ①	O None	
	Specific users included	<ul> <li>All internet resources with Global Secure Access</li> </ul>	
	Target resources ①	<ul> <li>All resources (formerly 'All cloud apps')</li> </ul>	
	1 resource included	<ul> <li>Select resources</li> </ul>	
	Network NEW ①	Edit filter	
	Not configured	None	
	Conditions ①	Select	
	0 conditions selected	Jamf Connect - Conditional Access Policy API	
	Access controls Grant ①	JC Jamf Connect - Conditional Ac b0127250-c527-4514-a87f-cca50fda6a4c	112
113 —	0 controls selected Session ① 0 controls selected	↑ To create a Conditional Access policy targeting members in your tenant with Global Secure Access (GSA) as a resource, make sure GSA is deployed in your tenant. <u>Learn more</u> 3	
	Enable policy Report-only On Off Create		


- 114. Enable Grant access.
- 115. Select JamfConnect Authenticator ONLY under Require authentication strength.
- 116. Click Select.



- 117. Select On for Enable Policy.
- 118. Click Create.

	New	
	Conditional Access policy	
	Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more C	
	Name *	
	Jamf Connect - Require Multifactor Authe $\checkmark$	
	Assignments	
	Users ①	
	Specific users included	
	Target resources ①	
	1 resource included	
	Network NEW ①	
	Not configured	
	Conditions ①	
	0 conditions selected	
	Access controls	
	Grant ①	
	1 control selected	
	Session ①	
	0 controls selected	
		_
	Enable policy	+ 11
	Report-only On Off	
18	Create	



119. Confirm the policy shows in the list and the State is On.

Home > Conditional Access   Policies	> Authentication method	ods   Authentication strengths > Condi	tional Access   Policie	s > App regist	rations > Jamf Connect -	OIDC Endpoint > Conditional	Access
	Policies						
«	+ New policy	New policy from template 🕴 Upload	d policy file 🛛 🔍 What	t if 🕐 Refrest	n 🛛 🕞 Preview features	Rot feedback?	
<ol> <li>Overview</li> </ol>	Microsoft Entra Conc	litional Access policies are used to apply a	case controls to keep	our organizatio	p recure Learn more 12		
I Policies	wild osoft Entra conc	intonal Access policies are used to apply a	cess controls to keep y	our organizatio	n secure. Learn more La		
Insights and reporting	All policies	Microsoft-managed policies					
	1	<b>9</b> 0					
<ul> <li>Diagnose and solve problems</li> </ul>	Total	out of 1					
Manage				1			
Named locations	Search			Add filter	r		
Custom controls (Preview)	1 out of 1 policy fou	ind					
😽 Terms of use	Policy name		SI	ate	Creation date	Modified date	
VPN connectivity	Jamf Connect - Rec	quire Multifactor Authentication	0	n	4/17/2025, 10:02:58 PM	4/17/2025, 10:16:35 PM	
Authentication contexts	1						

- 120. Let's create a TextEdit document to gather all the ID's needed to configure Jamf Connect settings. Open Text Edit.
- 121. Name the document, Jamf Connect ID's.
- 122. Enter the following info in the document:
  - Directory (tenant) ID:
  - Jamf Connect Conditional Access Policy API Application ID URI:
  - Jamf Connect OIDC Endpoint Client ID:
- 123. Save the document to your Desktop.



- 124. Switch back to Microsoft Entra. In the sidebar, Select Applications.
- 125. Select App registrations.
- 126. Select All applications.
- 127. Select the Jamf Connect Conditional Access Policy API.





- 128. Copy the Application ID URI and paste the URI to the Application ID URI section of the Jamf Connect ID's document.
- 129. Copy the Directory (tenant) ID and paste this ID to the Directory (tenant) ID section of the Jamf Connect ID's document.

··· > Jamf Connect - Conditional Access	Policy API $>$ App registrations $>$ Jamf Connect - OIDC Endpoint $>$ App	registrations >	
Jamf Connect - Cond	ditional Access Policy API 🛷 …		
	📋 Delete 🜐 Endpoints 💀 Preview features		
R Overview	1 Got a second? We would love your feedback on Microsoft identity platform (	previously Azure AD for developer). $ ightarrow$	
🗳 Quickstart			
🚀 Integration assistant	↑ Essentials		
X Diagnose and solve problems	Display name Jamf Connect - Conditional Access Policy API	Client credentials Add a certificate or secret	
Manage	Application (client) ID	Redirect URIs	
Branding & properties	Object ID		
Authentication	9b e83	api://b( ida6a4c 🕳	<u> </u>
Certificates & secrets	Directory (tenant) ID d4 15530 - 129	Managed application in local directory Jamf Connect - Conditional Access Policy API	
Token configuration	Supported account types		
API permissions	My organization only		

- 130. In the sidebar, Select Applications.
- 131. Select All applications.
- 132. Select App registrations.
- 133. Select the Jamf Connect OIDC Endpoint.





- 134. Copy the Application (client) ID and paste this ID to the Client ID section of the Jamf Connect ID's document.
- 135. Save the changes to the Jamf Connect ID's document.

··· > App registrations > Jamf Connect	- OIDC Endpoint > App registrations > Jamf Connect - Conditional Acc	ess Policy API > App registrations >
Jamf Connect - OIDC	CEndpoint 💉 …	
<mark>∕⊃ β</mark> earch ≪	🛍 Delete 🌐 Endpoints 🗔 Preview features	
R Overview	Got a second? We would love your feedback on Microsoft identity platform (	previously Azure AD for developer). $ ightarrow$
🗳 Quickstart		
🚀 Integration assistant		
X Diagnose and solve problems	Display name Jamf Connect - OIDC Endpoint	Client credentials Add a certificate or secret
Manage	Application (client) ID	Redirect URIs
🧮 Branding & properties	58c if6d7 - 134	<u>0 web, 0 spa, 1 public client</u>
Authentication	Object ID Of db8ea	Application ID URI Add an Application ID URI
📍 Certificates & secrets	Directory (tenant) ID d4 530	Managed application in local directory Jamf Connect - OIDC Endpoint
Token configuration	Supported account types	
API permissions	My organization only	

136. Confirm your Jamf Connect ID's document looks similar to the picture below.



137. Let's create a Jamf Connect configuration profile with conditional access settings using the Jamf Connect Configuration App. Open the Jamf Connect Configuration App. NOTE: We will only test OIDC and ROPG connections using the Jamf Connect Configuration app. This guide will not cover configuring a Jamf Connect profile for production use.





138. Enter a name for your profile. This guide will use JC PSSO.

- 139. If necessary, click Identity provider.
- 140. Select Microsoft Entra ID for Identity Provider.
- 141. Copy the Client ID from the Jamf Connect ID's file on your Desktop and paste it into the field for OIDC client ID.
- 142. Copy the Client ID from the Jamf Connect ID's file on your Desktop and paste it into the field for ROPG client ID.
- 143. Copy the Directory (tenant) ID from the Jamf Connect ID's file on your Desktop and paste it into the field for Tenant.
- 144. Copy the Application ID URI from the Jamf Connect ID's file on your Desktop and paste it into the field for OpenID connect scopes. Add this to the end: /jamfconnect+openid+email+profile
- 145. Enter https://127.0.0.1/jamfconnect for OIDC redirect URL.
- 146. Click Test

<b>C PSSO</b> 4/18/2025	137		
	Required		
	Identity provider:	Microsoft Entra ID	-140
	OIDC client ID:	5- id7	1
	ROPG client ID:	58c <sup>6</sup> 6d7	-142
	Tenant:	d4 5530	<b></b> 1
	OpenID connect scopes:	api://b0127250- ia6a4c/jamfconnect+openid+email+profile	
	Token caching:	Ignore cookies	
	Client secret:	JCCyfVL7YWtP6gudLljbRZV_N0dW4f3xETilxqtokEAZ6FAsBtgylq0MpU1uQ7Jid	
	OIDC redirect URI:	https://127.0.0.1/jamfconnect	1
	Discovery URL:	https://identity-provider-example-address.com/.well-known/openid-configuration	
	Change password URL:	https://www.passwordchangeexample.com	
	Choose licence	lamf Connect operators in trial mode without a license	

## 147. Select OIDC.

	Okta Classic	
	Okta OIE	
	OIDC	
	ROPG	
	FIDO2	
Jamf	Connect License	
		-
¢		
Save	Test	



148. Enter your Microsoft Entra account name.



150. Enter your password.

151. Click Sign in.

		Preview	
150	<ul> <li>← keith@hcstraining.net</li> <li>Enter password</li> </ul>		Auth endpoint: Token endpoint: User info endpoint: Access token:
150-	Forgot my password	Sign in 151	Refresh token:
	Terms of use Privacy & cookies		Supported scopes:



152. Enter the code into Microsoft Authenticator on your device.



153. Confirm OIDC Login was successful. Click Close (⊗).





155. Select ROPG.





- 156. Enter your Microsoft Entra account name.
- 157. Enter your password.

158. Click Sign in.



159. Confirm ROPG Login was successful.



NOTE: When testing to make sure your Microsoft Entra credentials work, we only need to test OIDC and ROPG connections using the Jamf Connect Configuration app. This guide will not cover configuring a Jamf Connect profile for production use.

160. There is a bug in the Jamf Connect Configuration application that will sometimes show an error message. If you see any of the errors listed below, as long as you see a tokens were granted, the connection was successful. Jamf is aware of this product issue.

• •	Preview	
Inable to load your identity rovider	Auth endpoint: https://login.microsoftonline.com/d4cb5287-2584-484e-9ab9-b37607cd5530/oauth2/y2.0/author/ze Tokan endpoint: https://login.microsoftonline.com/d4cb5287-2584-484e-9ab9-b37607cd5530/oauth2/y2.0/tokan Usar info endpoint: https://graph.microsoft.com/oidc/usarinfo	
e identity provider for your system is unable to be contacted. Check network tings or contact technical support.	Access token: eyJ&xAUOLIXYIOLICJ:hbGolOUSUJ1Nilsing1dCl6ikNOdjBPSTNSd3FsSEZFVm5hb018c2hDSDJYRSIsImipZCl6ikNOc Refresh token: ID token: eyJ&xAUOLIXYIOLICJ:hbGolOUSUJ1NilsimipZCl6ikNOdjBPSTNSd3FsSEZFVm5hb018c2hDSDJYRSJ8.eyJhdWOjOlT at 1744790770 to 4x450877.204-464.esb4b370707cd5S0 to 4x450877.204.esb4b370707cd5S0 to 4x45087	Confirm tokens grante
	Supported scopes: ["openid", "profile", "email", "offline_access"] Save	
•	Preview	
Microsoft	Auth endpoint: https://login.microsoftonline.com/id4ob5287-2584-484e-9ab9-b37607cd5530/oauth2/v2.0/authorize Token endpoint: https://login.microsoftonline.com/id4ob5287-2584-484e-9ab9-b37607cd5530/oauth2/v2.0/token User info endpoint: https://graph.microsoft.com/id6/userinfo	
Sorry, but we're having trouble signing you in.	Access token:	Confin
AADSTS900561: The endpoint only accepts POST requests. Received a GET request.	eyJ0eXAIOLKVIQI.C.hbGciOUSUz11Nilsing1dCi6ikNOdjBPSTNSd3FsSEZFVm5hb01Bc2hDSDJYRSisimtpZCi6ikNOC Refresh token:	tokens grante
	ID token: eyJoxXA/OUKY/QILCJhbGciOUSUz11NiisimtpZCI6lkNOdjBPSTNSd3FsSEZFVm6hb01Bc2hDSDJYRSJ8.eyJhdWQiOir	
	Int 174497803.0 site 016 Decomment: Leafle Decomments and the Decomment site 00500-900-20146-014-014948484 out - 44007149-2480-4492-5830-3094exc20400 motion: LOBOCCI 5630-3764-847-172EEDEOPTPED Intel Control C	l
Request Id: 3e819eb3-ecfa-4574-90b2-2274f3066600         ×           Correlation Id: 08914dd4-4e70-4291-affc-9c1fc1ab46d6         Timestamp: 2025-04-1811141:54Z	Supported scopes:	
message: AAUS I SYUUSDI: The endpoint only accepts POST	Coherent house' aussidiances 1	
	SAVA	