



How to Configure Account-Driven Enrollment and Enroll a Personal Device in Jamf Pro



Contents

Preface	3
Section 1: Setting Up the Discovery URL	4
Section 2: Configuring Account-driven User Enrollment in Jamf Pro	9
Section 3: Enrolling an iOS or iPadOS Device	12

Preface

Account-driven User Enrollment Explained

Account-driven User Enrollment is designed for organizations that need personal devices enrolled into Mobile Device Management. This method of enrollment supports Bring Your Own Devices (BYOD) scenarios, where the user owns the device but need access to the organization's resources. This provides for a combination of security for the organization, and privacy for the user.

What are the core components of Account-driven User Enrollment?

- A Managed Apple ID An Apple ID managed by the organization.
- Data separation A secure APFS volume to keep organizational data separate from personal.
- Limited management capabilities Limited management capabilities due to user ownership.

Requirements:

- Access to organization's web host
- An MDM solution (in this guide, we will use Jamf Pro)
- An unsupervised iOS/iPadOS device



Section 1: Setting Up the Discovery URL

You will need an application to create your JSON file in. Although this can be done in a text editor, it would be recommended to use an application that can verify your input. This guide will use JSON Editor, which is available for free from the App Store.

https://apps.apple.com/us/app/json-editor/id567740330?mt=12

1. Open JSON Editor.



2. Hover over the Root key and click Add (•) to create a new item.

Untitled	Cutline Text	Add Duplicate Edit Value	Delete Sort
Кеу	Туре	Value	
✓ Root	Object	🗘 (0 items)	



3. Label the object, Servers.

• • • Untitled Edited	Cutline Text	H D Image: Constraint of the second	>>
Кеу	Туре	Value	
∨ Root	Object	✿ (1 item)	
Servers	String	\$	
Servers	String	Ÿ	

4. Click the Type menu (≎) to the right of the Servers string.

• • • Untitled Edited	Outline Text	H Image: Constraint of the state of the
Кеу	Туре	Value
✓ Root	Object	
Servers	String	\$

5. Select Array from the menu

• • • Untitled Edited	Outline Text	+ Image: Constraint of the state of the
Кеу	Туре	Value
✓ Root	Object	✿ (1 item)
Servers	Array Object ✓ String Null Number Boolean	



•••	com.apple.rem	✓ 🔚 Outline	 + Add	Duplicate	Edit Value	Delete	↑↓ Sort	>>
Key		Туре		Value				
∨ Root	0	Object	٥	(3 items)				
> Servers		Array	٥	(0 items)				
Version		String	٥					
BaseURL		String	٢					

6. Create two new additional String objects below Servers and label them Version and BaseURL.

7. In the Value column for Version, enter mdm-byod.

8. In the value for BaseURL, enter the following: https://[Your-MDM-URL]/servicediscoveryenrollment/v1/userenroll (ie. https://myfakedomain.jamfcloud.com/servicediscoveryenrollment/v1/userenroll)

Outline Text Add Duplicate Edit Value Delete Sort Key Type Value Value Value Root Object \$ (3 items) > Servers Array \$ (0 items) Version String \$ mdm-byod BaseURL String \$ https://myfakedomain.jamfcloud.com/ servicediscovervenrollment/v1/userenroll	• • • Untitled		
Key Type Value Root Object \$ (3 items) > Servers Array \$ (0 items) Version String \$ mdm-byod BaseURL String \$ https://myfakedomain.jamfcloud.com/ servicediscoveryenrollment/v1/userenroll	Luited	Outline Text	Add Duplicate Edit Value Delete Sort
Root Object \$ (3 items) > Servers Array \$ (0 items) Version String mdm-byod BaseURL String https://myfakedomain.jamfcloud.com/ servicediscovervenrollment/v1/userenroll	Кеу	Туре	Value
> Servers Array © (0 items) Version String mdm-byod BaseURL String https://myfakedomain.jamfcloud.com/ servicediscoveryenrollment/v1/userenroll	Root	Object	(3 items)
Version String mdm-byod BaseURL String https://myfakedomain.jamfcloud.com/ servicediscoveryenrollment/v1/userenroll	> Servers	Array	(0 items)
BaseURL String https://myfakedomain.jamfcloud.com/ servicediscovervenrollment/v1/userenroll	Version	String	≎ mdm-byod
	BaseURL	String	https://myfakedomain.jamfcloud.com/ servicediscoveryenrollment/v1/userenroll



9. Save with the specific file name of com.apple.remotemanagement. IMPORTANT: This file name is critical since it is what the enrollment process will look for.

• • • Untitled Edited	Outline Text	│┼│
Кеу	Туре	Value
∨ Root	Object	♦ (3 items)
> Servers	Array	✿ (0 items)
Version	String	mdm-byod
BaseURL	String	https://myfakedomain.jamfcloud.com/ servicediscoveryenrollment/v1/userenroll)
	Save As: com.apple.	remotemanagement
	Tags:	
	Where: HCS	
	File Format: JSON	O
		Cancel Save
No selection		

10. Upload this file to your domain host in this specific location:

https://YOUR-WEB-SERVER-FQDN-HERE/.well-known/com.apple.remotemanagement

NOTE: The steps to upload your JSON file will differ based on the entity that hosts your domain services.

😢 HCS		+ =
<pre>\$ public_html > .well-known</pre>		↑☆(…)
Name ^	Size	Date
> 🛅 Old_FILE	-	5/13/22, 12:00 A
> 🚞 acme-challenge	-	8/29/20, 12:00
> 🛅 oldJSON	166 bytes	8/28/23, 11:02 P
> 🚞 pki-validation	-	8/28/23, 4:18 A
htaccess	98 bytes	5/16/22, 12:00 A
apple-developer-merchantid-domain-asso	9 KB	8/29/20, 12:00
com.apple.remotemanagement	166 bytes	5/16/22, 12:00 A



11. Open Terminal from /Applications.



12. Enter the following command:

curl -I https://YOUR-WEB-SERVER-FQDN-HERE/.well-known/com.apple.remotemanagement

(ie. curl -l https://hcstechgroup.com/.well-known/com.apple.remotemanagement)

13. Verify the response shows OK and Content-Type is application/json.





Section 2: Configuring Account-driven User Enrollment in Jamf Pro

The steps detailed in this section are specific to Jamf Pro. Check with your MDM vendor for steps on how to enable Account-driven User Enrollment.

1. Log into Your Jamf Pro Server.

	iamf PRO	
USERNAME ex. admin		
PASSWORD		\bigcirc
All co	ntents © 2002-2023 Jamf. All rights reserved.	

- 2. On the top-right corner, click Settings (🚱).
- 3. Click Global.
- 4. Click User-initiated Enrollment.





5. Click Edit.

🖆 jamf 🛛 PRO		L 🏓 🕸
Computers Devices Users	Settings : Global ← User-initiated enrollment	
VERSON No.Active Computers - 3 Mobile Devices - 2 UNINAARDES Computers - 9 Mobile Devices - 9	General Messaging m.cod G.G. Access Image: A decision of method decision of the access of the complexity of the access of the access of the complexity of the access of the access of the complexity of the access of the access of the complexity of the access of the a	
Collapse Menu		13 History Edit

6. Click iOS

7. Under Account-Driven User Enrollment, select the checkbox for personally owned devices.

		R	¢ <mark>ب</mark>
	Settings : Global ← User-Initiated enrollment		
6 —	Construit Macranico muno. OS Access		
	Profile-Driven Enrollment via URL Allow users to enroll by going to https://AMM_FRO_URL.jumfcloud.com/enroll (hosted in Jamf Cloud) or https://JAMF_FRO_URL.com/8443/enroll (hosted on-premixe)		
	Enable for institutionally owned devices		
	Enrollment Method		
	User Enrollment Personal data on devices enrolled via User Enrollment is retained when the MDM potile is removed, IOS 131 or later, PacOS 131 or later) Personal Device Profiles Personal data on devices enrolled via personal device profiles may be deleted when the MDM potile is removed, IOS 13 or later, PacOS 13]		
	Account-Driven User Enrollment Adva users to enoit by system of its their device using a Managed Apple ID		
7 —	Enable for personally owned devices Personal data on devices enrolled via Account Driver Diser Enrollment is retained when the MDM profile is removed, (JOS 15 or later, IPadOS 15 of later)		

- 8. Click Access.
- 9. Click Edit (🗹)

Settings : Global ← User-initiated enrolln	ient		
General Messaging macOS	iOS Access	8	
Directory Service Groups	Directory Service groups to configure enrollment acce	ess for	+ Add Group Access
Group	Profile-Driven	Account-Driven	
All Directory Service Users	Institutional	No	Ŭ



- 10. Select the checkbox for Allow group to enroll personally owned devices via Account-Driven User Enrollment.
- 11. Click Save.



12. Click Save.

NOTE: The ability to allow directory service users to participate in Account-driven User Enrollment is due to previously configuring Cloud Identity Providers within Jamf. For more details, please see our guide on Microsoft Azure Active Directory with Jamf Pro.

https://hcsonline.com/support/white-papers/a-guide-to-integrate-azure-active-directory-with-jamf-pro

요) Users	Settings : Global			
	General Messaging macOS iOS Access			
	Directory Service Groups Directory Service groups	o configure enrollment access for		+ Add Group Access
	Group	Profile-Driven	Account-Driven	
	All Directory Service Users	Institutional	Yes	ľ
				Cancel Save



Section 3: Enrolling an iOS or iPadOS Device

Before enrolling BYOD into an MDM solution, it is important to know what functions are possible on a personally owned device:

MDM can	MDM can't
 Configure accounts Configure Per App VPN Install and configure apps Require a passcode on iPhone or iPad Enforce certain restrictions Access inventory of work apps Remove work data only 	 See personal information, usage data or logs Access inventory of personal apps Remove any personal data Take over management of a personal app Require a complex iPhone and iPad passcode Remotely wipe the entire device Access unique device identifiers Access device location Manage Activation Lock Access roaming status Turn on Lost Mode

1. On your iPad, tap Settings.

2. Tap General

3. Tap VPN & Device Management.

	Sattings	General
		About
	Apple ID, iCloud, Media & Purchases	Software Update >
	Airplane Mode	AirDrop
	S Wi-Fi Mobius	AirPlay & Handoff >
	8 Bluetooth On	Picture in Picture >
	_	
	Notifications	iPad Storage
	Sounds	Background App Refresh
	C Focus	
	Screen Time	Date & Time
		Keyboard
2 —	😥 General	Gestures
	Control Center	Fonts
	AA Display & Brightness	Language & Region >
	Home Screen & Multitasking	Dictionary
	(f) Accessibility	
	Wallpaper	VPN & Device Management
	Siri & Search	Legal & Regulatory
	Apple Pencil	
	Touch ID & Passcode	Transfer or Reset iPad >
	Battery	Shut Down
	Privacy & Security	
	👗 App Store 🗕	



2. Tap Sign In to Work or School Account.

4:31 PM Mon Aug 28	Ceneral VPN & Device Management	奈 100% ■
Settings		
User One Apple ID, iCloud, Media & Purchases	VPN Not Co	onnected
	Sign In to Work or School Account	
Airplane Mode		
🛜 Wi-Fi Mobius		

- 3. Enter your Managed Apple ID.
- 4. Tap Continue.





5. Tap Next.

NOTE: This can be a built-in Jamf Pro account or you can connect Jamf Pro with your Identity Provider. This guide uses Managed Apple ID federation with Microsoft Azure.

4:33 PM Mon Aug 28	1 Cor	VDN & Dovice	Aanagamant	 ≎ 100% ■
0.11	(Ger		vianagement	
Setting	🔒 login.mi	crosoftonline.com	5 AA	Connected
A 8	Microsoft			
Airpla	Sign in			
wi-Fi	svalencia@hcstechgroup	p.com		
Bluet	Can't access your account?	?		
Notifi		Next		
Sound				
C Focu:	Sign-in option	s		
Scree				
Gene				
Contr Terms of	use Privacy & cookies			
AA Displi	>		Û	
Home Screen &				

- 6. Enter your password.
- 7. Tap Sign in.





- 8. Enter the code displayed in the authenticator app on your mobile device.
- 9. Tap Verify.



10. Tap Sign In to iCloud.





11. Tap Continue to proceed to Microsoft Online to enter federated credentials. NOTE: Alternatively, this can be a standard Managed Apple ID and password.



- 12. Enter your password.
- 13. Tap Sign in.





- 14. Enter the code displayed in the authenticator app on your mobile device.
- 15. Tap Verify.

4:34 PM Mon Aug 28	< General	VPN & Device Managen	nent	奈 100% ■	
Setting	🔒 login.microsofton	line.com AA	S	Connected	
Airple	Microsoft svalencia@hcstechgroup.com Enter code				
* Bluet	Enter the code displayed in the your mobile device	authenticator app on			-14
Soun Focu:	More information	Verify			—15
Scree					
Contr Terms of u	se Privacy & cookies		Û		
Home Screen &					

16. Tap Allow Remote Management.





17. Enter your device passcode.







19. The iCloud settings for your Managed Apple ID will appear.

4:44 PM Mon Aug 28		중 100% ■
	Apple ID	
Settinas		
Q Search		
	EDT Com Valencia	
Apple ID, iCloud, Media & Purchases	Sam valencia svalencia@hcstechgroup.com	
	Name & Email	>
InstructUs LLC svalencia@hcstechgroup.com	Password & Security	>
Examplane Mode	Profiles & Device Management	>
ᅙ Wi-Fi Mobius		
Bluetooth On	iCloud	5 GB > 🗲
Notifications	User's iPad This iPad	>
Sounds		
C Focus	Sign Out	
Screen Time		
General		
Control Center		
AA Display & Brightness		
Home Screen & Multitasking		
(i) Accessibility		
🛞 Wallpaper		
Siri & Search		
Apple Pencil		
Touch ID & Passcode		