

A Guide to Integrate Azure Active Directory with Jamf Pro





This guide was created using the following:

- An Office 365 Business License
- Jamf Pro 10.10.1 or later
- An Azure Active Directory Managed Domain Services Subscription & Enterprise Mobility + Security E5 level or the Azure AD Premium P2 level (to support certain group types).

Requirements

- Any Office 365 Business License
- A Jamf Pro Server
- Google Chrome or Firefox
- The following ports must be open for on an on premise Jamf Pro server: LDAPS 636
- It may take several hours to complete the tasks in this guide, due to the length and creation of DNS entries

Acronyms and Definitions

- AAD Azure Active Directory
- SSO Single Sign-On
- TLS Transport Layer Security, commonly referred to as SSL (Secure Sockets Layer)
- LDAP Lightweight Directory Access Protocol
- LDAPS Lightweight Directory Access Protocol (over SSL), Secure version of LDAP that works on port 636
- AADDS Azure Active Directory Domain Services
- Office 365 A cloud productivity offering from Microsoft
- Azure Active Directory SSO and Directory solution from Microsoft, included in most Office 365 plans
- Azure Active Directory Domain Services Securely-managed AD domain hosted by Microsoft that allows traditional AD features such as LDAP/LDAPS and binding machines (specifically Virtual Machines in the Azure Cloud) to the domain.
- DNS Domain Name System A system that provides translation from a domain host name like www. google.com to an IP address
- FQDN Fully Qualified Domain Name, A real domain name, for example, www.google.com

Sections

Section 1: Create an Office 365 Account Page 4
This section covers creating an Office 365 account if you do not already have one
as well as configuring a custom domain.
Section 2: Create an Azure Account Page 12
This section covers enabling Azure services from your Office 365 account.
Section 3: Configure Azure Active Directory Domain Services Page 14
This section covers configuring Azure AD Domain Services
Section 4: Configure Jamf Pro for Azure AD Domain Services
This section covers connecting your new Azure AD Domain Secure LDAP service to Jamf Pro
Section 5: Configure Azure AD for Single Sign-On (SSO) Page 44
This section covers configuring Azure AD for SSO
Section 6: Configure Jamf Pro for SSO with AAD Page 53
This section covers integration Azure AD for Single Sign-On in Jamf Pro
Section 7: Create on Azura Group and Jamf Pro Groups for Admin Access to Jamf Pro
Section 7. Greate an Azure Group and Jami Fro Groups for Admin Access to Jami Fro
Section 8: Configure an Individual Azure User for Jamf Pro Admin Access Page 70



Section 1 Create an Office 365 account

If you already have an Office 365 account, skip to the next section, "Create an Azure Account."

- 1. Open Firefox or Google Chrome; Safari is not compatible.
- 2. Open https://products.office.com/en-us/business/office-365-business and select "Free Trial" as shown below.



the "Buy Now" button

- 3. If you see the screen, "It looks like you already have an account," then click "No, I'll sign up for a new account."
- 4. Enter your organization's information.
- 5. Complete all fields, then click Next.

Of

e 365 l	Business Trial	Want to add this to an existing subscription? Sign	in
	Welcome, let's get to know y	′OU	
	United States		
	Nicholas		
	nmcdonald@hcsonline.com		
	(866) 518-9672		
	HCS Technology Group		
	(25-49 people		
	Next Θ		

- 6. Create your first account as shown below.
- 7. Click "Create my account" when done.

Office 365 Business Tria		Want to ad	dd this to an existing subscription?	Sign in
Create	e your user ID			
You need a	user ID and password to sign in t	o your account.	0	
~	nmcdonald@hcsonlinedemo.onmi	crosoft.com		
By disking Create m	ate my account you acces to our terms any account ⊖	and conditions.		

- 8. Select Call Me or Text Me.
- 9. Enter your telephone number, then click Call Me or Text me.
- 10. Wait for Microsoft to text or call the provided number with a 6 digit code.

Office 365 Business Trial		Want to add this to an existing subscription?	Sign in
Prove. You ○ Text me (+1) ♥ Phone nu We don't save this opport Call me ●	U're. Not. A. Robot. Call me Imber In number or use it for any other purpose.	1 ~	

11. Enter the verification code Microsoft has given you, then click Next.

Office 365 Business Trial	Want to add this to an existing subscription?	Sign in
Prove. You're. Not. A. Robot.		
492053		
Didn't get it or need a new code? Try again		
Next 😔		



- 12. Wait a moment until you see the account creation confirmation page.
- 13. Write down your user ID.
- 14. Click "You're ready to go."

Office 365 Bus	iness Trial
	Save this info. You'll need it later.
	Sign-in page https://portal.office.com/
	Your user ID nmcdonald@hcsonlinedemo.onmicrosoft.com
	You're ready to go ⊖
	Do not refresh this page

15. If you are prompted to sign in to Office 365 again, select your user account and sign in.



- 16. If you see a hints window, read or close the hints.
- 17. Click Admin.

Office 365	5						
	Good m	orning					
	Apps						
	6	w]	x	P	N	A 33	
	OneDrive	Word	Excel	PowerPoint	OneNote	Admin	
	Explore all your	apps $ ightarrow$					

18. If necessary, in the sidebar, click the three lines to reveal a menu.



19. Click "Show all."

	Microsoft 365 admin center	
≡		
	Home	
8	Users ^	
	Active users	
	Contacts	
	Guest users	
	Deleted users	
Ŕ	Groups 🗸	
	Billing \lor	
ß	Customize Navigation	
V		
	Show all	

20. In the Setup section, click Domains.





21. Click "Add domain".

Home	> Domains						HCS Technolo
	+ Add domain	+ Buy domain	View	All domains	*	Search domains	
	Domain name	8			St	atus	
	hcsonlineaad	demo.onmicrosoft.co	om (Defa	ault)	S	Setup complete	

22. In the new "Add a domain" window, enter a domain or subdomain that you control and want to use with Office 365 (this guide uses hcs.jamfy.tech as an example. Your user accounts will have this domain appended, for example, nmcdonald@hcs.jamfy.tech), then click Next.

New Domain						
	Add a domain	Verify domain	Set up your online servic…	Update DNS settings		
Add a d	lomain					
Enter a domain you	own.					
hcs.jamfy.tech						
Your users' email addre	esses will look like this: username	@hcs.jamfy.tech				
Next	Close					

22. In the "Verify domain" window, add the requested DNS entries to your domain's DNS provider. This process can vary between providers; contact your domain registrar or DNS provider for more information if necessary. After your DNS provider makes the required entries available on the Internet, click Verify.

This step is required for Microsoft to verify you own the domain you are trying to use. Note: DNS Records may take up to 72 hours to propagate.

(H) hcs.	jamfy.tech				×
	Add a domain	Verify domain	Set up your online servic…	Update DNS settings	
Verify	domain				
To keep your domain own the domain, but i owned by you and the provider.	secure, we need you to prove that t won't affect your existing email o e domain setup is complete, you ca	: you own it. Adding the r or other services. After the an safely remove the reco	ecord below will prove that you e domain is verified as being rd from your DNS hosting		
Follow these step-	by-step instructions to add th	e TXT records with t	he values below at Nameche	ap. 🖉 (Not your DNS host?)	
verity by: IXI re	COTO MX RECORD				
TXT name:	hcs				
TXT value:	🗅 MS=ms806	75581			
TTL:	🗅 3600 or you	ur provider defau	lt.		
Get someone to help	o you. Let us help you set up y	our TXT records.			
Verify	Save and close				

24. In the domain setup completion window, click Finish.

H hcs.jam	fy.tech				×
	Add a domain	Verify domain	Set up your online servic…	Update DNS settings	
Congrati	lations	Your do	main setu	n is comple	eted
congrad					
Finish					



25. In the sidebar, click Users, then click Active Users.

	≡		
	ŵ	Home	
Γ	8	Users	\sim
		Active users	
		Contacts	
		Guest users	
		Deleted users	
	٨	Groups	\sim
	母	Resources	\sim
		Billing	\sim
	Ç	Support	\sim
	£33	Settings	\sim

26. Click the three dots next to your user account.

HCS Technology Group

Active users



The three dots are located between the key icon and your username

27. In the options menu, choose "Edit username."

HCS Technology Group

Active users

Nicholas McDonald

Assign to group

Manage product licenses

Nicholas McDonald

Image product licenses

Manage product licenses

Manage product licenses

Manage product licenses

Assign to group

Edit username

Delete user

Manage email aliases

28. Click the domain menu, choose your new domain, then click Save. If you are not automatically signed out, sign out then sign in with your new username.

Manage username						
i You are about to c	nange this user's sign-in information. Let them know about this change					
nmcdonald	@ hcs.jamfy.tech \checkmark					
	hcs.jamfy.tech					
	hcsonlineaaddemo.o					
Save changes	Cancel					

 \times



Section 2: Create an Azure Account

If your organization has already created your Azure account, skip to the next section, to "Configure Azure Active Directory Domain Services."

- 1. With Firefox or Google Chrome, sign into office.com as an Office 365 admin; this allows Microsoft to match the Office 365 Tenant correctly for signup.
- 2. Open https://azure.microsoft.com/en-us/free/.

Hicrosoft Azure	Contact Sales: 1-600-667-1389 📞 Search: Q My account Portal Sign in
Overview \sim Solutions Products \sim	Documentation Pricing Training Marketplace - Partners - Support - Blog More -
	Create your Azure free account today
	Get started with 12 months of free services
	Start free Or buy now >
	A model and mode

3. Enter your organization's details and click Next.

	Microsoft Azure	nmcdonald@hcsonlineaaddemo.onmicrosoft.com	Sign out
	Azure free account sign (Start with a \$200 credit for 30 days, and	JD keep going for free	
1	About you		^
	Country/Region 0		
	United States	÷	
	First name		
	Nicholas		
	Last name		
	McDonald		
	Email address 0		
	nmcdonald@hcsonline.com		
	Phone		
	(337) 476-2776		
	By proceeding you acknowledge the <u>privacy statement</u> and <u>subscription</u>	ution agreement	

4. Complete the phone verification process with either Call Me or Text Me, enter the provided 6-digit code, then click Next.

2	Identity verification by phone	^
	Country code	
	United States (+1)	
	Phone number	
	(337) 476-2776	
	Text me Call me	

5. Enter a credit card for identity verification then Select Next. If your organization does not have access to a credit card or P-card, have your organization reach out to Microsoft sales to complete the verification process.

 $\overline{}$

//y is credit card information necessary for a free account? To keep out spam and bots To verify your identity ou won't be charged unless you upgrade. ISA Image: I	
To keep out spam and bots To verify your identity Dou won't be charged unless you upgrade. ISA To the charged unless you upgrade. ISA To the charged unless you upgrade. ISA To the charged unless you upgrade. ISA To the charged unless you upgrade. ISA To the charged unless you upgrade. ISA To the charged unless you upgrade. ISA To the charged unless you upgrade. ISA To the charged unless you upgrade. ISA To the charged unless you upgrade. ISA To the charged unless you upgrade. ISA To the charged unless you upgrade. ISA To the charged unless you upgrade. ISA To	
To verify your identity Do won't be charged unless you upgrade.	
To venty your identity Sou won't be charged unless you upgrade. SA SA SA SA CVV Arriter CVV Arr	
uwon't be charged unless you upgrade. ISA Isa <td></td>	
ISA Image: I	
ard number	
xpiration date CW • Aonth • Year • arme on card ddress line 1 ddress line 2 Optional -	
Aprication date CW Adonth CW Adonth CW	
kpiration date CVV • Aonth • Year • arme on card iddress line 1 iddress line 2 Optional -	
Annth Year American Year American Year American Year American American Year	
ame on card ddress line 1 ddress line 2 Optional -	
ddress line 1 ddress line 2 Optional -	
ddress line 1 ddress line 2 Optional -	
ddress line 1 ddress line 2 Optional -	
ddress line 2 Optional -	
ddress line 2 Optional -	
ddress line 2 Optional -	
Optional -	
ty	
zate ZIP code	
\$	

Sign up

6. Confirm you have the legal authority to accept this agreement on behalf of your organization. Accept the agreement and click "Sign up."

4	Agreement	^
ſ	✓ I agree to the <u>subscription agreement</u> , <u>offer details</u> , and <u>privacy statement</u>	
1	l will receive information, tips, and offers from Microsoft or selected partners ab Newsletter, Pricing updates, and other Microsoft products and services.	out Azure, including Azure



Section 3: Configure Azure Active Directory Domain Services

If AADDS is already active on your Azure account skip to step 7. Note: AADDS is a paid service within Azure, see https://azure.microsoft.com/en-us/pricing/details/active-directory-ds/ for pricing information.

Important Note: In order for users to authenticate against the secure LDAPS service included in AADDS, each user needs to change their password after you create and configure the AD Domain service, so Microsoft can store the hash of the password in a way that AADDS can use. If you are already using Azure AD Connect, then your users' passwords are already hashed with Microsoft.

1. Navigate to the Azure Portal (https://portal.azure.com/) and sign in if requested. You may see "You're ready to start with Azure" if this is your first time logging in. Click "Go to the portal."



- 2. If you see the "Welcome to Microsoft Azure" dialog, click "Maybe later."
- 3. If your organization already has a virtual network configured skip to step 9. A virtual network is required for AADDS to function.
- 4. From the sidebar, click "Virtual Networks."



5. Click "Create virtual network."

Microsoft Azure		\wp Search resources, services, and docs				Ş	Q	0
«	Home > Virtual networks							
+ Create a resource	Virtual networks							
🛧 Home	+ Add EE Edit columns () Refresh	ssian tans						
🖪 Dashboard		ang						
Ξ All services	No subscriptions in HCS Technology Group directory.	All seconds	All locations			tage		
	riter by name	All resource groups	All locations	~	All	tags		
All resources	0 items		CROUP (LOCATION .				
📦 Resource groups	NAME 10	RESOURCE	GROOP	LOCATION				
🔇 App Services								
Function Apps								
👼 SQL databases			1					
😹 Azure Cosmos DB			<"> </th <th></th> <th></th> <th></th> <th></th> <th></th>					
Virtual machines								
💠 Load balancers		No	wittual potworks to display					
🧮 Storage accounts		Create a virtual network to securely connect your A	Trine resources to each other. Connect	your virtual network tr	NOUR OF	unremise	к	
Virtual networks		network using an Az	zure VPN Gateway or ExpressRoute. Lea	arn more 🖄	your on	prentise		
Azure Active Directory			Create virtual network					
Monitor		_						

6. If your organization has not used Azure services before you may be prompted with a "Free Trial" offer. If you see this screen please reference the above section "Create an Azure account," and contact Microsoft directly for pricing information.

Microsoft Azure	⊘ Search resources, services, and docs	>_	₽ Q	\ & ?	٢	nmcdonald@hcsonlin HCS TECHNOLOGY GROUP
*	Home > Virtual networks >					
+ Create a resource						×
🛧 Home						
🖪 Dashboard						
i≡ All services	Create a free account					
🕂 🛧 FAVORITES						6V - 12 V
III resources	Explore Azure with a \$200 credit for 30 days, 12 months of free products, and more than 25 products that are always free.					
Resource groups						
🔇 App Services						
inction Apps						2 12
🗟 SQL databases						6 💷
😹 Azure Cosmos DB						
Virtual machines						
🚸 Load balancers	Start free					
Storage accounts						
Virtual networks						
Azure Active Directory						



7. Enter your virtual network details, then click Create. If you are unsure how to configure this section, ask your network administrator, or see the example in the figure below.

Create virtual network		×
* Name		
HCSnet	~]
* Address space 🚯		
10.1.0.0/16	~]
10.1.0.0 - 10.1.255.255 (65536 add	resses)
* Subscription		-
Free Trial	\sim	
* Resource group		
(New) HCSnet	\sim]
Create new		
* Location		
West US	\sim	
Subnet		-
* Name		-
HCSnetSubnet1	 ✓ 	
* Address range 🚯		
10.1.0.0/24	~	
10.1.0.0 - 10.1.0.255 (256 add	resses)
DDoS protection		
• Basic Standard		

A. If you don't have an existing resource group to put your virtual network into, then below the Resource group field, click "Create new," enter a name, then click OK.

Select existing		\sim		
eate new				
	group is a container th	at holds	related	
A resource resources	group is a container th or an Azure solution.	nat holds	related	
A resource resources	group is a container th or an Azure solution.	hat holds	related	
A resource resources t	group is a container th or an Azure solution.	hat holds	related	
A resource resources t * Name HCSnet	group is a container th or an Azure solution.	hat holds	related	
A resources resources * Name HCSnet	group is a container th	hat holds	related	
A resources resources * Name HCSnet	group is a container th or an Azure solution.	hat holds	related	

B. Leave "DDoS protection" set to Basic, and leave "Service endpoints" and Firewall as Disabled (you do not need to enable the firewall because AADDS has its own network security group for firewall rules).

DDoS prote	ction 🚯			
Basic	Standard			
0	0			
Service end	points 🚯			
Disabled	Enabled			
Firewall				
Disabled	Enabled			

C. Important: Note your Location because you need to create the AADDS resource in the same location later.

- 8. You should be brought back to the "Virtual networks" page. If your new virtual network is not yet listed, wait a moment, then click Refresh.
- 9. In the sidebar, click "Create a resource" to configure AADDS..

	Microsoft Azure			rvices, and docs		>	- Q	Ĺ3	©	?
	«	Home > Virtual networks								
9 —	+ Create a resource	Virtual networks	8							
	1 Home	+ Add == Edit columns () Refresh	Assign tags							
	🛅 Dashboard		• roogr ago							
	i≡ All services	Subscriptions: Free Trial								
	- 🛨 FAVORITES	Filter by name	All resource groups	✓ All	locations	~	All tags			~
	III resources	1 items		RESOURCE GROUI	p ↑.				\$	IBSCRIP
	📦 Resource groups									
	S App Services	HCSnet		HCSnet		West US			F	ree Tria
	Function Apps									

10. In the New pane, in the search field, enter "Azure Active Directory Domain Services" and press Enter.

Microsoft Azure			${\cal P}$ Search resources, services, and
«	Home > New		
+ Create a resource	New		\Box ×
🛧 Home			
🛄 Dashboard	Azure Active Directory Do	main Services	×
≣ All services	Azure Marketplace	See all Popula	r
— 🛨 FAVORITES ————————————————————————————————————			Windows Server 2016 VM
All resources	Get started		Quickstart tutorial
📦 Resource groups	Recently created		
🔇 App Services	Compute	0	Ubuntu Server 18.04 VM
Function Apps	Networking	Hide text labels	Learn more
	Storage		Web App

11. Select "Azure AD Domain Services" from the search results.

Azure Active Directory Domain Services	s			×
Pricing All ~	Operating System All	Publisher ✓ All		~
Results				
NAME		PUBLISHER	CATEGORY	
Azure AD Domain Services		Microsoft	Identity	\heartsuit
Azure AD Connect Server 2016		Cloud Infrastructure Services	Compute	



12. In the new panel click Create.

Azure AD Doma Microsoft	in Services	\$ 🗆 ×
Azure Active Directory D need to deploy or manager corporate Active Directo Domain Services feature	omain Services lets you join Azure virtual machines ge domain controllers. Users sign in to these virtual ry credentials and can access reources seamlessly. A s domain join, LDAP, NTLM and Kerberos authentic	to a domain without the machines using their Azure Active Directory ation are widely used in
enterprises. Migrate lega having to worry about id	acy directory-aware applications running on premise lentity requirements.	es to Azure without
enterprises. Migrate lega having to worry about id Save for later PUBLISHER	acy directory-aware applications running on premise lentity requirements. Microsoft	es to Azure without
enterprises. Migrate lega having to worry about id Save for later PUBLISHER	acy directory-aware applications running on premise lentity requirements. Microsoft Service overview	es to Azure without
enterprises. Migrate lege having to worry about id Save for later PUBLISHER USEFUL LINKS	acy directory-aware applications running on premise lentity requirements. Microsoft Service overview Documentation	es to Azure without



- 13. In the resulting setup screen, configure the Basics with the following settings:
 - A. Confirm that "Directory name" is automatically populated based on information from your Azure Active Directory data.
 - B. For "DNS domain name" enter a FQDN that you control, ideally something like "aad. contoso.com". This is especially important if you use a 3rd party signed secure LDAP certificate. You must be able to edit DNS records for this domain. Currently AADDS does not support FQDNs over 15 characters. This guide uses hcs.jamfy.tech as an example.
 - C. For "Subscription" select whatever subscription your Azure admin has configured for you (this guide uses "Free Trial").
 - D. For "Resource group" select the resource group that your Virtual Network is in. This is not required but simplifies organization.
 - E. For "Location" select the location that your Virtual Network is in.
- 14. Confirm your settings then Click OK.





- 15. In the Network section, configure the following settings:
 - A. For "Virtual network" select the network you created earlier, or whatever Virtual Network you want your AADDS services to be located in.
 - B. For "Subnet" select a pre-existing subnet you wish to use, or create a new one. This subnet should be dedicated exclusively for AADDS services.

Note: A network security group will be created to protect AADDS; this network security group will be used to create firewall rules for your LDAP service.

16. Confirm your settings then click OK.

earlier.	Network 🗆 ×	
ervices	Create a dedicated subnet for this managed domain. After the managed domain is created, you will not be able to move it to a different subnet.	
a	Network	
otect create	* Virtual network HCSnet	A
	Subnet	
	Create a dedicated subnet with at least 3 available IP addresses.	
	Create new	
	* Subnet HCSnetSubnet1	В
	A network security group will be automatically created and associated to the subnet to protect AAD Domain Services. The network security group will be configured according to guidelines for configuring NSGs.	
16—	ОК	

17. In the "Administrator group" section, confirm that Azure automatically created a new group for you called AAD DC Administrators. This group is created to administer the domain. You will need to add at least 1 administrator to this group. Click "Manage group membership."

Administrator group	
A group named "AAD DC Administrate been created to administer this manag Click below to manage membership fo group, or click OK to continue.	ors" has ged domain. or this
AAD DC Administrators 🚯	



18. In the Members page, click "Add members."

Home > New > Ma	Aarketplace > Everything > Azure AD Domain Services > Enable Azure AD Dor	nain Services > Administrator group > Members
Members		
🕂 Add members	U Refresh	
NAME	-	ТУРЕ
No members have be	peen found	

19. In the "Select member or invite an external user field" enter at least one user's name, (ideally this would be your own account), click the user in the search results, then click Select.



20. Confirm you are back at the Members screen. Click Refresh and confirm you see at least one user. Click the Close button (x) in the upper-right corner.

Home > New > Marketplace > Everything > Azure AD Domain Services > Enal	ble Azure AD Domain Services > Adu	ninistrator group > Members	
Members AAD DC Administrate			×
+ Add member : O Refresh			
NAME	түре		
M Nicholas McDonald	User		

21. Click OK at the bottom of the "Administrator group" pane.



22. In the Synchronization pane, click All then click OK.



23. In the Summary screen, confirm your details, then click OK.

Summary		Δ×
Basics		
Name	hcs.jamfy.tech	
Subscription	Free Trial	
Resource group	HCSnet	
Location	West US	
Network		
Virtual network	HCSnet	
Subnet	HCSnetSubnet1	
Network security group (new)	AADDS-hcs.jamfy.tech-NSG	
Administrator group		
Administrator group	AAD DC Administrators	
Membership Type	Assigned	
Synchronization		
Synchronization scope	All	
By enabling Azure AD Dom credential hashes required	ain Services for this directory, you consent to storing for NTLM and Kerberos authentication in Azure AD.	
ОК		



24. Confirm that your browser displays your Azure home page. In the sidebar, click "All resources."



25. Click the hostname for your AADDS resource.

All resources HCS Technology Group					☆ ×
+ Add	Try preview				
Subscriptions: Free Trial					
Filter by name All resource groups	All types 🗸 🗸	All locations	✓ All tags	V No grouping	\sim
8 items Show hidden types 💿					
NAME	ТҮРЕ 🗘	RESOURCE GROUP	LOCATION	SUBSCRIPTION	
aadds-348386b01f7f40b8b187fa87dc571445-nic	Network interface	HCSnet	West US	Free Trial	
aadds-4c04ab11ce834637a15e76d4b2b62d47-lb	Load balancer	HCSnet	West US	Free Trial	
aadds-4c04ab11ce834637a15e76d4b2b62d47-pip	Public IP address	HCSnet	West US	Free Trial	
AADDS-hcs.jamfy.tech-NSG	Network security group	HCSnet	West US	Free Trial	
azureFirewalls-ip	Public IP address	HCSnet	West US	Free Trial	
hcs.jamfy.tech	Azure AD Domain Services	HCSnet	West US	Free Trial	
HCSnet	Virtual network	HCSnet	West US	Free Trial	
HCSnet-SHIELD	Firewall	HCSnet	West US	Free Trial	

26. In the following page, if you see "The managed domain is being created. This operation will take a while," this may take up to 1 hour to provision. Wait and refresh the page later.



27. In the "Required configuration steps" section, under "Update DNS server settings for your virtual network," click Configure.



28. In the sidebar for the AADDS you just configured, click Secure LDAP and leave this window open. You will configure LDAPS to use a self-signed certificate.





- 29. On your Mac, use Spotlight to open Keychain Access (or you can use Finder to open Applications>Utilities>Keychain Access). If you don't have a Mac, use the following steps:
 - A. If you don't have a Mac, create a certificate by using "Option B" in the following document: https://docs.microsoft.com/en-us/azure/active-directory-domain-services/active-directory-ds-adminguide-configure-secure-Idap
 - B. If you don't have a Mac, export the certificate using the following document: https://docs.microsoft.com/en-us/azure/active-directory-domain-services/active-directory-ds-adminguide-configure-secure-ldap-export-pfx
 - C. If you don't have a Mac, skip to step 60.
- 30. In Keychain Access, go to the menu bar, click Keychain Access, choose Certificate Assistant, then choose Create a Certificate.

Ś	Keychain Access File	Edit	View	Window	Help	
	About Keychain Access		×	🔥 Secu	ıre LDAP - Microsoft Azure 🗙 🕴 Configure Secure LDAP (L	DAP
6	Preferences	ж,	https://	aithub co	m/wbuchwalter/azuro_content/blob/master/articles/activ	ve-di
	Certificate Assistant		Ор	en		
	Ticket Viewer	∼ະສκ	Cre	ate a Cert	ificate	tollo
	Services	►	Cre Cre	ate a Cert ate a Cert	ificate Authority ificate For Someone Else as a Certificate Authority	
	Hide Keychain Access Hide Others Show All	出発 日第ブ	Rec Set Eva	quest a Ce the defau luate "AAA	rtificate From a Certificate Authority It Certificate Authority A Certificate Services"	o cc
	Quit Keychain Access	жQ			Option B - Create a self-signed certifica	ate

- 31. In the Certificate Assistant window, enter your details as follows.
 - A. Name enter the DNS Name you selected in step 13-B.
 - B. Identity Type choose Self Signed Root.
 - C. Certificate Type choose SSL Server.
 - D. Select the option "Let me override defaults."
- 32. Confirm your settings then click Continue.

Certificate Assistant	
Create Your Certificate	
Please specify some certificate information below:	
Name: hcs.jamfy.tech	- A
C C C Identity Type: Self Signed Root	- B
Certificate Type: SSL Server	- C
Let me override defaults (i.e. extensions, destination keychain, etc.)	- D
Learn More	
Continue	-32

- 33. At the dialog that "You are about to create a self-signed certificate," click Continue.
- 34. In the following screen, enter a Serial Number (you can leave the default of "1") and a Validity period (you can leave the default of 365 days but you must renew before it expires), then click Continue.

Certificate Assistant
Certificate Information
 Please specify some certificate information below:
Serial Number: 1
Validity Period (days): 365
Valid From: Today, 3:33 PM Valid To: 12/20/19, 3:33 PM
Learn More
 Go Back Continue

- 35. In the following screen, enter your organizational details. In the Name (Common Name) field enter the FQDN you selected in step 13-B.
- 36. Confirm your settings then click Continue.

	Certificate Assistant		
Certificate Information			
	Please specify some personal information below to be used in the certificate:		
	Email Address: nmcdonald@hcsonline.com		
	Vame (Common Name): hcs.jamfy.tech	— 35	
	Organization: HCS Technology Group		
	Organizational Unit: Consulting		
	City (Locality): Bohemia		
	State/Province: NY		
	Country: US		
t	Go Back Continue	—36	



37. Leave the Key Pair Information at the default options then click

	Certificate Assistant		
Key Pair Information			
Ce	Specify the key size and algorithm used to create your key pair. The key pair is made up of your private and public keys. The private key is the secret part of the key pair and should be kept secret. The public key is made publicly available as part of the digital certificate.		
	Key Size: 2048 bits 😂		
	Algorithm: RSA		
	Learn More		
	Go Back Continue		

38. Leave the Key Usage Extension at the default options, then click Continue.

	Certificate Assistant		
Key Usage Extension			
_	The Key Usage Extension of a certificate identifies its security capabilities. Select Include Key Usage Extension to see the available capabilities, and select which ones this certificate will provide.		
C	 Include Key Usage Extension This extension is critical Capabilities: 	n	
	 Signature Non Repudiation Key Encipherment Data Encipherment Key Agreement 	Certificate Signing CRL Signing Encipher Only Decipher Only	
	Learn More		
		Go Back Continue	

😣 😑 🔵 Certificate Assistant			
Extended Key Usage Extension			
	Select Include Extended Key Usage Extension to see the available options and specify which ones this certificate will use.		
Ce	 Include Extended Key Usage Extension This extension is critical Capabilities: 		
	 Any Email Protection SSL Client Authentication SSL Server Authentication Code Signing 		
	PKINIT Client Authentication PKINIT Server Authentication		
	Learn More		
	Go Back Continue		

39. Leave the Extended Key Usage Extension at the default options then click Continue.

40. Leave the checkbox deselected for the Include Basic Constraints Extension option then click Continue.

	Certificate Assistant	
Basic Constraints Extension		
	Select Include Basic Constraints Extension to see the available options and specify which ones this certificate will use.	
Ce	Include Basic Constraints Extension	
	Learn More	
	Go Back Continue	



41. Configure the Subject Alternative Name Extension options as follows.

"dNSName:" - Enter an asterisk followed by your FQDN from step 13-B, then enter a Space character, then enter the FQDN from step 13-B (you must have a space between the two entries. For example, if your FQDN was aad.contoso.com, then enter *.aad.contoso.com aad.contoso.com. "iPAddress:" - Clear all data from this field.

42. Confirm your settings then click Continue.

Certificate Assistant				
Subject Alternate Name Extension				
Select Include Subject Alternate Name Extension to see the available options and specify which ones this certificate will use.				
. Ce	Include Subject Alternate Name Extension			
	Extension Values: (use a space between entries)			
rfc822Name:				
r	dNSName: *.hcs.jamfy.tech hcs.jamfy.tech			
	iPAddress:			
6	Learn More			
	Go Back Continue			

43. In the "Specify a Location For The Certificate" screen, leave the default as "login" and click Create.

🔴 🕘 Certificate Assistant			
Specify a Location For The Certificate			
	Please specify a keychain where the certificate will be stored.		
	Keychain: login		
	E THE REAL PROPERTY AND A DECEMBER OF A DECE		
	Learn More		
	Go Back Create		



44. In the Conclusion screen click Done. The certificate and private key have been created in your "login" keychain.

- 45. In the Keychain Access sidebar, select login.
- 46. In the Category section of the Keychain Access sidebar, select Certificates.





47. In the Certificates category, look for the certificate labeled with your FQDN from step 13-B.

▶ 🗑 hcs.jamfy.tech certificate Dec 20, 2019 at 7:42:25... login

48. Right click your certificate then choose Export "your FQDN".



- 49. In the Save As field, enter something memorable, such as your FQDN.
- 50. Leave the File Format as Personal Information Exchange (.p12).
- 51. Click Save.



52. In the new window, enter a password to protect the exported certificate and private key, then click OK. The figure in this guide includes the cleartext of the password for illustration.



53. In the new window, enter your login keychain password (this should be the same as your Mac password) to allow the export then click Allow.

	Keychain Access wants to export key "hcs.jamfy.tech" from your keychain. To allow this, enter the "login" keychain password.	
	Password:	
?	Always Allow Deny Allow	

- 54. You will export the certificate again, this time with a different format. Right-click your certificate then choose Export "your FQDN".
- 55. In the Save As field, enter the same name you used in step 49, such as your FQDN.
- 56. Click File Format and choose "Certificate (.cer)".
- 57. Click Save.

Save As JamfPro-hcs.jamfy.tech	- 55
Tags: Where: 🔯 Downloads 🔗 🗸	
File Format Certificate (.cer)	— 56
Cancel	- 57

58. In the Finder, select the certificate you exported as a p12 file, then press Return to edit its name.

59. In the file name field, replace the extension .p12 with .pfx, the press Return to save the name change.



60. Open your browser window that still displays the Secure LDAP configuration screen you left open in step 28.

Home > hcsjamfytech - Secure LDAP			
hcs.jamfy.tech - Secure LE	DAP	×	
	📙 Save 🗙 Discard 🔑 Change Certificate		
Overview	Secure LDAP Disabled	Allow secure LDAP access over the internet Disabled	
Activity log	Thumbprint	Certificate expires	
Access control (IAM)	Not available	Not available	
Manage	Comm 1040 a		
Properties	Disable Enable		
Secure LDAP			
Synchronization			
💝 Health			
Q Notification settings			
Troubleshooting + Support			
🗙 Troubleshoot			
New support request			



61. Near the Secure LDAP field, click Enable.

Home > hrsiamfytech - Secure I DAP			
kcs.jamfy.tech - Secure LDAP kare Abomin Swites			
	🕀 Save 🛛 🗙 Discard 🖉 Change Certificate		
1 Overview	Secure LDAP Disabled	Allow secure LDAP access over the internet	
Activity log	Thumbprint	Certificate expires	
Access control (IAM)	Not available	Not available	
Manage	Secure LD	*	
Properties	Disable Enable		
Secure LDAP			
Synchronization			

62. Near "Allow secure LDAP access over the internet," click Enable.

Home > hcs.jamfy.tech - Secure LDAP		
hcs.jamfy.tech - Secure LD Azure AD Domain Services	DAP	
	🕂 Save 🗙 Discard 🔎 Change Certificate	
Overview Activity log Access control (IAM)	Secure LDAP Disabled Thumbprint Not available	Allow secure LDAP access over the internet Disabled Certificate expires Not available
Manage		
Properties	Disable Enable	
Secure LDAP	Allow secil	
Synchronization	Disable Enable	
😌 Health	Upload a .PFX file containing the certificate to be used for secure LDAP access to this managed domain	
Q Notification settings	* .PFX file with secure LDAP certificate 🚯	
Troubleshooting + Support	Select a file	
X Troubleshoot	* Password to decrypt .PFX file 📵	
New support request		
	Your subnet is protected by network security group AADDS-hcsjamfy.tech-NSG. To give user a on the network security group.	access to secure LDAP endpoint, please ensure "Allow" ru
	Users cannot bind using secure LDAP or sign in to the managed domain, until you enable pass type of users in your Azure AD directory. Complete both sets of instructions if you have a mix of Instructions for cloud-only user accounts Instructions for synced user accounts	word hash synchronization to Azure AD Domain Services of cloud-only and synced user accounts in your Azure AD

Azure AD Domain Services		
,> Search (Ctrl+/)	Save X Discard P Change Certificate	
Overview Activity log Access control (IAM)	Secure LDAP Allow secure LDAP access over the internet Disabled Disabled Thumbprint Certificate expires Not available	
Manage	- Secure LDAP 🛛	
Properties	Disable Enable	
Secure LDAP	Allow secure LDAP access over the internet	
Synchronization	Disable Enable	
💔 Health	Upload a .PFX file containing the certificate to be used for secure LDAP access to this managed domain	
Q Notification settings		
Troubleshooting + Support	"hsjantly.tech.pbr"	
X Troubleshoot	* Password to decrypt. PFX file 💿	
New support request	·····	
	Your subnet is protected by network security group AADDS-hcsjamfytech-NIGC. To give user access to secure LDAP endpoint, please ensure "Allow" rule on port 636 is configured with proper IP ranges on the network security group.	
	Users cannot bind using secure LDAP or sign in to the managed domain, until you enable password hash synchronization to Azure AD Domain Services. Follow the instructions below, depending on the type of users in your Azure AD directory. Complete both sets of instructions if you have a mix of cloud-only and synced user accounts in your Azure AD directory. Instructions for cloud-only user accounts Instructions for yourd azure accounts Instructions for synced user accounts Instructions for synced user accounts Instructions for yourd azure AD directory.	Up bu

63. Next to the ".PFX file with secure LDAP certificate" field, click the Upload button (looks like a folder).

64. Select the file with the .pfx filename extension you renamed in step 59 then click Open.

65. In the "Password to decrypt .PFX file" field, enter the password you used in step 52.

66. Click Save.

hcs.jamfy.tech - Secu Azure AD Domain Services	re LDAP	< C(
	Save Save Certificate	- 66
Overview Activity log Access control (IAM)	Secure LDAP Allow secure LDAP access over the internet Disabled Disabled Certificate expires Not available Not available Not available	
Manage	8 Server 1040 6	
Properties	Disable Enable	
Secure LDAP	Allow secure LDAP access over the internet	
Synchronization	Disable Enable	
P Health	Upload a .PFX file containing the certificate to be used for secure LDAP access to this managed domain	
Notification settings	* .PFX file with secure LDAP certificate 👩	
Troubleshooting + Support	"hcsjamfytech.pfr"	
 Troubleshoot New support request 	Annual as despt. DOC 61.0	65
	Your subnet is protected by network security group AADDS-hccjamfytech-NSG. To give user access to secure LDAP endpoint, please ensure "Allow" rule on port 636 is configured with proper IP ranges on the network security group.	
	Users cannot bind using secure LDAP or sign in to the managed domain, until you enable password hash synchronization to Azure AD Domain Services. Follow the instructions below, depending on the type of users in your Azure AD directory. Complete both sets of instructions if you have a mix of cloud-only and synced user accounts in your Azure AD directory. Instructions for cloud-only user accounts	



67. You will see the following screen notifying you that the secure LDAP service is being configured. Leave the window open until the configuration is complete.

Home > hcs.jamfy.tech - Secure LDAP	
hcs.jamfy.tech - Secure LD	AP ×
	🕂 Save 🗶 Discard 🔑 Change Certificate
1 Overview	Configuring secure LDAP for the directory. This operation may take a while.
Activity log	Essentials ×
Access control (IAM)	Secure LDAP 0
Manage	nyadua Cuadua
Properties	Allow secure LDAP access over the internet
Secure LDAP	Level at EX file containing the certificate to be used for service IDAP access to this managed domain
Synchronization	opose a si vi ne consensity un certificate to le decti on secure core access to tins managere domain
💔 Health	PKR lie with secure LDAP certificate Control Contron Control Control Control Control Control Control Control Control
Q Notification settings	* Password to decrypt. PFX file 🕐
Troubleshooting + Support	····
★ Troubleshoot	
New support request	Your submet is protected by network security group AADDS-hcs jamfytech-NSG. To give user access to secure LDAP endpoint, please ensure "Allow" rule on port 636 is configured with proper IP ranges on the network security group.
	Uses cannot bind using secure LDAP or sign in to the managed domain, until you enable password hash synchronization to Azure AD Domain Services. Follow the instructions below, depending on the type of users in your Azure AD directory. Instructions for cloud-only user accounts Instructions for synced user accounts

68. After about 10 minutes the window should refresh and you should see "Enabled" under Secure LDAP.



69. Next to the notification icon (looks like an exclamation mark inside a yellow triangle) click the link to your network security group.

Home > hcs.jamfy.tech - Secure LDAP		
hcs.jamfy.tech - Secure Ll	DAP	>
	戻 Save 🔀 Discard 🏓 Change Certificate	
Overview Activity log	Secure LDAP Enabled Thumbprint	Allow secure LDAP access over the internet Enabled Certificate expires
Access control (IAM)	7696F18F26B4F089CCAEB7F257CFA573A7511138	Fri, 20 Dec 2019 22:18:51 GMT
Manage	Serure I DAP	
Properties	Disable Enable	
Secure LDAP	Allow secure LDAP access over the internet 🚯	
Synchronization	Disable Enable	
 Health Q Notification settings 	Your subnet is protected by network security gro AADDS-hcsjamfy.tech-NSG on the network security group.	o give user access to secure LDAP endpoint; please ensure "Allow" rule on port 636 is configured with proper IP ranges
Troubleshooting + Support X Troubleshoot Image: Support request Image: Support request	Users cannot bind using secure LDAP or sign in to the managed domain, until y type of users in your Azure AD directory. Complete both sets of instructions if y . Instructions for doud-only user accounts . Instructions for synced user accounts	su enable password hash synchronization to Azure AD Domain Services. Follow the instructions below, depending on the un have a mix of cloud-only and synced user accounts in your Azure AD directory.

- 70. In the network security group screen, in the Settings column, click "Inbound security rules."
- 71. Click Add to create a new firewall rule.

AADDS-hcs.jamfy.tech-N Network security group	NSG - Inbound s	ecurity rules						
Search (Ctrl+/)	🕂 Add 🔍 De	efault rules						
Overview	PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION	
Activity log	101	AllowSyncWithAzureAD	443	ТСР	Any	Any	Allow	
Access control (IAM)	201	AllowRD	3389	тср	207.68.190.32/27,13.10	Any	Allow	
Tags	301	AllowPSRemotingSliceP	5986	ТСР	52.180.179.108,52.180.1	Any	Ø Allow	
Diagnose and solve problems	302	AllowPSRemotingSliceT	5986	TCP	52.180.183.67,52.180.18.	. Any	Allow	
ttings	65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow	
Inbound security rules	65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow	
Naturalk interfaces	65500	DenyAllInBound	Any	Any	Any	Any	O Deny	

72. In the new "Add Inbound security rule" panel, enter these details as follows.

- Source Choose IP Addresses
- Source IP addresses/CIDR ranges Enter every IP address listed for your Jamf Cloud region, separated by a comma. If you use an on-prem Jamf Pro Server, then enter its public IP address. A list of Jamf Cloud public IP addresses for your region is at https://www.jamf.com/jamf-nation/articles/409/permitting-inbound-outbound-traffic-with-jamf-cloud. For illustration, this guide uses the IP addresses for the US Region; at the time of publication, the field contains "54.208.14.206,54.208. 84.215,52.1.62.94,52.1.215.211,52.203.216.218,34.233.253.88,34.234.26.211,52.72.152.43"
- Source port ranges Leave the default setting of "*"
- Destination Leave the default setting of Any
- Destination Port Ranges Enter 636
- Protocol Leave the default setting of Any
- Action Leave the default setting of Allow
- Priority Leave the default setting
- Name Enter a memorable name; this guide uses "LDAPS-Jamf-Cloud-US-Region"
- Description Leave blank or enter a description, like the URL you used for the "Source IP addresses/ CIDR ranges" field
- Review your settings then click Add.

* Source 🚯		
IP Addresse	S	V
* Source IP a	ddresses/CIDR ranges 🚯	
54.208.14.2)6,54.208.84.215,52.1.62.94,52.1.215.211,52.203.216.218,34.233.253.88,34.234.26.2	~
Source por	t ranges 🚯	
٠		v
Destination	θ	
Any		v
Destination	port ranges 🚯	
636		~
Protocol		
Any	TCP UDP	
Action		
Allow	Deny	
Priority 🚯		
312		
* Name		
LDAPS-Jam	-Cloud-US-Region	~
Description		



73. You should now see your new Inbound security rule in the rules list.

AADDS-hcs.jamfy.tech-NSG	- Inbound secur	ity rules						×
	🕂 Add 🔌 Default i	rules						
🎯 Overview	PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION	
Activity log	101	AllowSyncWithAzureAD	443	тср	Any	Any	Allow	
Access control (IAM)	201	AllowRD	3389	тср	207.68.190.32/27,13.10	Any	Allow	
 Tags Diagnose and solve problems 	301	AllowPSRemotingSliceP	5986	тср	52.180.179.108,52.180.1	Any	Allow	
Cottings	302	AllowPSRemotingSliceT	5986	тср	52.180.183.67,52.180.18	Any	Allow	
Inbound security rules	312	LDAPS-Jamf-Cloud-US-Region	636	Any	54.208.14.206,54.208.8	Any	Allow	
Outbound security rules	65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow	
Network interfaces	65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow	
Subnets	65500	DenyAllInBound	Any	Any	Any	Any	O Deny	

74. In the breadcrumbs bar, select your AADDS object.

Н	ome > All resource > hcs.jamfy.tech - Se	ture LDA	P > AADDS-h	cs.jamfy.tech-NSG - Inbound se	curity rules					
5	AADDS-hcs.jamfy.tech-NSC	i - Inb	ound secu	rity rules						×
	Search (Ctrl+/)	🕂 Add	🕸 Default	rules						
0	Overview	PRIORI	ſY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION	
-	Activity log	101		AllowSyncWithAzureAD	443	тср	Any	Any	Allow	
20	Access control (IAM)	201		AllowRD	3389	тср	207.68.190.32/27,13.10	Any	Allow	
4	Tags	301		AllowPSRemotingSliceP	5986	тср	52.180.179.108,52.180.1	Any	Allow	
~	plagnose and solve problems									

75. In the sidebar, click Properties.

Azure AD Domain Services		
	🕞 Save 🗙 Discard 🔑 Change Certificate	
Overview	Secure LDAP Enabled	Allow secure LDAP access over the internet Enabled
Activity log	Thumbprint 7696F18F26B4F089CCAEB7F257CFA573A7511138	Certificate expires Fri, 20 Dec 2019 22:18:51 GMT
		*
lanage	Server LDAD @	
Properties	Disable Enable	
Secure LDAP	Allow secure LDAP access over the internet ()	
Synchronization	Disable Enable	
Health		
O Notification settings	Your subnet is protected by network security group AADI "Allow" rule on port 636 is configured with proper IP range	DS-hcsjamfy.tech-NSG. To give user access to secure LDAP endpoint, please ensure ges on the network security group.
roubleshooting + Support		
K Troubleshoot	Users cannot bind using secure LDAP or sign in to the ma Domain Services. Follow the instructions below, dependir instructions if you have a mix of cloud-only and surged u	anaged domain, until you enable password hash synchronization to Azure AD g on the type of users in your Azure AD directory. Complete both sets of ser accounts in your Azure AD directory.
New support request	Instructions for cloud-only user accounts Instructions for synced user accounts	de accounte in your realier to ancecory.
76. Make a note of the "Secure LDAP external IP address."

hcs.jamfy.tech - Propertie	s	Ŷ
	DNS DOMAIN NAME	
1 Overview	hcs.jamfy.tech	
 Activity log Access control (IAM) 	LOCATION West US	
Manage	AVAILABLE IN VIRTUAL NETWORK/SUBNET	
Secure LDAP Synchronization Health	NEWORK SECURITY GROUP ASSOCIATED WITH SUBNET AADDS-hcs.jamfy.tech-NSG	
Notification settings Troubleshooting + Support	IP ADDRESS ON VIRTUAL NETWORK 10.1.0.5 10.1.0.4	
 X Troubleshoot New support request 	SECURE LDAP Enabled	
	SECURE LDAP CERTIFICATE THUMBPRINT 7696F18F2684F089CCAEB7F257CFA573A7511138	Đ
	SECURE LDAP CERTIFICATE EXPIRES Fri, 20 Dec 2019 22:18:51 GMT	
	SECURE LDAP EXTERNAL IP ADDRESS 168.61.17.177	

77. Create a DNS A record with your DNS provider to resolve to the IP address of the "Secure LDAP external IP address" you gathered in the previous step. Because you created a wildcard self-signed certificate earlier, you can use any subdomain of the "Domain" you created earlier. This guide uses ldaps.hcs.jamfy.tech as an example, and the following figure illustrates the A record displayed at the DNS provider namecheap.com.

Note: This may take up to 72 hours to propagate.

A Record Idaps.hcs 168.61.17.177	Automatic	Ê
----------------------------------	-----------	---

- 78. Use Spotlight to open Network Utility (it is located in /System/Library/CoreServices/Applications).
- 79. Click Lookup.
- 80. Enter the name of the DNS A record you created in step 59.
- 81. Click Lookup.
- 82. Confirm that the lookup query returned the IP address of the "Secure LDAP external IP address" you gathered in step 76.



83. You have successfully configured Azure Active Directory Domain Services. You will use Jamf Pro in the next section to test the LDAPS service. Remember that the Azure firewall rule allows only LDAPS connections from the IP address or addresses you specified when you created the firewall rule.



Section 4: Configure Jamf Pro for Azure AD Domain Services This section covers connecting your AADDS Secure LDAP service to Jamf Pro

- 1. Log in to your Jamf Pro instance i.e. (https://contoso.jamfcloud.com)
- 2. In the upper-right corner, click Settings (looks like a gear).

🖬 jamf 🛛 PRO		L 🖇 🔯
Computers Devices Users	Dashboard	
VERSION 10.30-0154463445 MARAGED Computers: 3 Mobile Devices: 1 URMARAGED Computers: 0 Mobile Devices: 1	Smart Computer Groups	

3. In the System Settings section, click LDAP Servers.

ŝ	All Settings	System Set	tings							
000	System Settings	Jamf Pro User	Single Sign-	LDAP Servers	SMTP Server	Clustering	Activation	Change	Apache	Limited
	Global Management	Accounts & Groups	On		·		Code	Management	Tomcat Settings	Access
圈	Self Service		We'll be back.							
8	Sonvor Infractivicture	Log Flushing	Maintenance Pages	Engage						

4. In the LDAP Servers page, click New.

Settings >> System Settings >> LDAP Servers			
			+ New
NAME	^	PROXY SERVER	
TESTING 0365			

5. In the Chose a Directory Service page, select Configure Manually, then click Next.

AP Servers		
Choose Service	Choose a Directory Service	
Enter Server Info	Apple's Onen Directory	
Enter Credentials	Microsoft's Active Directory	
Test Users	Novell's eDirectory	
User Mappings	Configure Manually	
Test Groups		
		Cancel

- 6. Configure the Connection settings using the following information:
 - A. Display Name Set this to any preferred display name i.e. "Office 365".
 - B. Directory Service Choose "Microsoft's Active Directory."
 - C. Server and Port Enter your LDAPS FQDN created earlier, for example Idaps.contoso.com, then in the Port field enter "636".
 - D. Enable LDAP Proxy Server Leave this option deselected.
 - E. Use SSL Select this option.
 - F. **Upload Certificate** Click Upload Certificate, then in the CA Certificate dialog click Choose File, navigate to the .cer certificate you created in the previous section, then click Upload.
 - G. Authentication Type Set this to Simple.
 - H. **Distinguished Username** Enter an active Azure AD username, preferably a service account, that is a member of the "AAD DC Administrators" group. Instead of the recommended format, enter the username in the form of an email address. This guide uses nmcdonald@hcs.jamfy.tech, which is not a service account, for illustration.
 - I. Password Enter the account password for the previous step's account .
 - J. Connection Timeout Leave as default.
 - K. Search Timeout Leave as default.
 - L. Referral Response Leave as default.
 - M. Use Wildcards When Searching Leave as default.

ISPLAY NAME Display name for	he LDAP server	
Office 365		
DIRECTORY SERVICE Directory s	rvice to use for the LDAP server	
Microsoft's Active Directory		
	Paddores and not number of the LDAD renser Mostname is recommended if usion SSI	
daps.hcs.jamfy.com	a dearcos, and por nameer of the control incommended in damy dec.	: 636
Configure LDAP proxy Server	r settings to connect to the LDAP server.	
PROXY SERVER		
Select 🔻		
PROXY BINDING ADDRES	AND PORT NUMBER	
Upload Certificate		
Upload Certificate Certificates to be shared Configuration Name testing 0365 EA AUTHENTICATION TYPE Type of Simple T	scross all LDAP connections; Issuer AlLADDRESS=nmcdonald@hcsonline.com, L=Bohemia, C=US, ST=NY, OU=*Consulting *, O=*HCS Technolog uuthentication required to connect to the LDAP server	y Group ", CN=hcs.jamfytech
Upload Certificate Certificates to be shared Configuration Name testing 0365 EA AUTHENTICATION TYPE Type of Simple • LDAP Server Account	Incross all LDAP connections. Issuer All.ADDRESS=nmcdonald@hcsonline.com, L=Bohemia, C=US, ST=NY, OU=*Consulting *, O=*HCS Technolog authentication required to connect to the LDAP server Account to use to connect to the LDAP server. A service account is recommended Define without any of the IDAP server account is no "without bottor account do account is accounted account is accounted account in the total account in the total account is account in the total account in the total account is accounted account in the total account in the total account is accounted accounted account in the total account in the total account is accounted accounted account in the total account is accounted	y Group ", CN=hcs.jamfytech
Upload Certificate Certificates to be shared Configuration Name testing 0365 EA UTHENTICATION TYPE Type of Simple • LDAP Server Accound DISTINGUISHED USERNA medonald@rcs.iamk	Incross all LDAP connections. Issuer All.ADDRESS=nmcdonald@hcsonline.com, L=Bohemia, C=US, ST=NY, OU=*Consulting *, O=*HCS Technolog authentication required to connect to the LDAP server Account to use to connect to the LDAP server. A service account is recommended Account to use to connect to the LDAP server account (e.g.*uid=authenticator.cn=users.dc=ods.dc=example.dc=com*) Cohemication	y Group ", CN=hcs.jamfytech
Upload Certificate Certificates to be shared Configuration Name tasting o365 EA NUTHENTICATION TYPE Type of Simple • LDAP Server Account DISTINGUISHED USERNA Intraduald@hcs.jamfy	scross all LDAP connections: Issuer AILADDRESS=nmcdonald@hcsonline.com, L=Bohemia, C=US, ST=NY, OU="Consulting *, O="HCS Technolog authentication required to connect to the LDAP server Account to use to connect to the LDAP server. A service account is recommended A Count to use to connect to the LDAP server. A service account is recommended ME Distinguished name of the LDAP server account (e.g. "uid=authenticator.cn=users.dc=ods.dc=example.dc=com") tech	ty Group *, CN=hcs.jamfy.tech
Upload Certificate Certificates to be shared Configuration Name testing 0365 EA AUTHENTICATION TYPE Type of Simple • LDAP Server Accound DISTINGUISHED USERNA MICHAINER USERNA PASSWORD	Issuer AILADDRESS=nmcdonald@hcsonline.com, L=Bohemia, C=US, ST=NY, OU=*Consulting *, O=*HCS Technolog authentication required to connect to the LDAP server AL Account to use to connect to the LDAP server. A service account is recommended ME Distinguished name of the LDAP server account (e.g.*uid=authenticator.cn=usen.dc=ods.dc=example.dc=com*) tech	y Group ", CN=hcs.jamfytech
Upload Certificate Certificates to be shared Configuration Name testing 0365 EA NUTHENTICATION TYPE Type of Simple UDAP Server Account DISTINGUISHED USERNU MICONALGREA, Jamfy PASSWORD UERICY PASSWORD	Issuer AILADDRESS=nmcdonald@hcsonline.com, L=Bohemia, C=US, ST=NY, OU=*Consulting *, O=*HCS Technolog authentication required to connect to the LDAP server It Account to use to connect to the LDAP server. A service account is recommended ME Distinguished name of the LDAP server account (e.g.*uid=authenticator.cn=users.dc=ods.dc=example.dc=com*) tech	y Group ", CN=hcs.jamfytech
Upload Certificate Certificates to be shared Configuration Name testing 0365 EA NUTHENTICATION TYPE Type of Simple UDAP Server Accou DISTINGUISHED USERNI mcGonald@hcs.jamfy PASSWORD URITY PASSWORD	Issuer AILADDRESS=nmcdonald@hcsonline.com, L=Bohemia, C=US, ST=NY, OU=*Consulting *, O=*HCS Technolog authentication required to connect to the LDAP server It Account to use to connect to the LDAP server. A service account is recommended ME Distinguished name of the LDAP server account (e.g., "uid=authenticator.cn=users.dc=ods.dc=example.dc=com") tech	y Group ", CN=hcs.jamfytech
Upload Certificate Certificates to be shared Configuration Name testing 0365 EA NUTHENTICATION TYPE Type of Simple UDAP Server Accou DISTINGUISHED USERN mcdonald@hcsjamfy FASSWORD VERIFY PASSWORD	Issuer AILADDRESS=nmcdonald@hcsonline.com, L=Bohemia, C=US, ST=NY, OU=*Consulting *, O=*HCS Technolog authentication required to connect to the LDAP server AIL Account to use to connect to the LDAP server. A service account is recommended ME Distinguished name of the LDAP server account (e.g., "uid=authenticator.cn=usen.dc=ods.dc=example.dc=com") Istech Inf time to wait hefere carcelling an attempt to connect to the LDAP server	y Group ", CN=hcs.jamfytech
Upload Certificate Certificates to be shared Configuration Name testing 0365 EA UTHENTICATION TYPE Type of Simple • LDAP Server Accou DISTINGUISHED USERN MICHONAIGIBHCS Jamfy PASSWORD VERIFY PASSWORD	scross all LDAP connections: Issuer AlLADDRESS=nmcdonald@hcsonline.com, L=Bohemia, C=US, ST=NY, OU=*Consulting *, O=*HCS Technolog udhentication required to connect to the LDAP server Account to use to connect to the LDAP server. A service account is recommended ME Distinguished name of the LDAP server account (e.g.*Lid=authenticator.cn=users.dc=ods.dc=example.dc=com*) tech t of time to wait before canceling an attempt to connect to the LDAP server ds	y Group ", CN=hcs.jamfytech
Upload Certificate Certificates to be shared Configuration Name testing 0365 EA UUTHENTICATION TYPE Type of Simple UDAP Server Accou DISTINGUISHED USERN MINICANAIGABIABACSJAMY VERIFY PASSWORD VERIFY PASSWORD CONNECTION TIMEOUT Amou 15 Secon	Issuer AILADDRESS=nmcdonald@hcsonline.com, L=Bohemia, C=US, ST=NY, OU="Consulting *, O="HCS Technolog uuthentication required to connect to the LDAP server It Account to use to connect to the LDAP server. A service account is recommended ME Distinguished name of the LDAP server account (e.g., "uid=authenticator.cm=users.dc=ods.dc=example.dc=com") tech to filme to wait before canceling an attempt to connect to the LDAP server ds	y Group ", CN=hcs.jamfy.tech
Upload Certificate Certificates to be shared Configuration Name testing 0365 EA UUTHENTICATION TYPE Type of Simple • LDAP Server Accou DISTINGUISHED USERN MICHONAId@hcsjamfy VERIFY PASSWORD VERIFY PASSWORD SEARCH TIMEOUT Amount of the SEARCH TIMEOUT Amount of the	Issuer AlLADDRESS=nmcdonald@hcsonline.com, L=Bohemia, C=US, ST=NY, OU="Consulting *, O="HCS Technolog uuthentication required to connect to the LDAP server It Account to use to connect to the LDAP server. A service account is recommended ME Distinguished name of the LDAP server account (e.g., "uid=authenticator.cm=users.dc=ods.dc=example.dc=com") Itech It of time to wait before canceling an attempt to connect to the LDAP server ds to to the UbAP server account to the LDAP server d=	y Group ", CN=hcs.jamfy.tech
Upload Certificate Certificates to be shared Configuration Name testing 0365 EA UUTHENTICATION TYPE Type of Simple UDAP Server Accou DISTINGUISHED USERN Inconald@hcs.jamfy VERIFY PASSWORD CONNECTION TIMEOUT Amou 15 Secon SEARCH TIMEOUT Amount of ti , 60 Secon	Issuer AlLADDRESS=nmcdonald@hcsonline.com, L=Bohemia, C=US, ST=NY, OU="Consulting *, O="HCS Technolog unthentication required to connect to the LDAP server It Account to use to connect to the LDAP server. A service account is recommended ME Distinguished name of the LDAP server account (e.g., "uid=authenticator.cn=users.dc=ods.dc=example.dc=com") It is to wait before canceling an attempt to connect to the LDAP server ds	ny Group ", CN=hcs.jamfy.tech



- 7. In the lower-right corner click Save. If you see the message, "Unable to communicate with the LDAP server," then double-check your LDAP server settings, the DNS record for the FDQN of the LDAPS service, and the certificate.
- 8. If you don't see an error message, click Edit, then click Mappings in the top bar.

Settings > System Settings > LDAP Servers > Office 365	
Connection	
DISPLAY NAME Display name for the LDAP server Office 365	

9. Click User Mappings.

10. Configure the User Mappings settings as follows.

- A. Object Class Limitation Choose "All ObjectClass Values"
- B. Object Class(es) Enter "organizationalPerson, user"
- C. Search Base Enter your search base using this example "OU=AADDC Users, DC=contoso, DC=com"
- D. Search Scope Choose "All subtrees"
- E. User ID Enter "uSNCreated"
- F. Username Enter "userPrincipalName" or "mail"
- G. Real Name Enter "displayName"
- H. Mail Enter "mail"
- I. Append to email results" Leave blank unless needed
- J. Department Enter "department"
- K. Building Enter "streetAddress" (Or any other custom LDAP attribute)
- L. Room Enter "room"
- M. Phone Enter "mobile" (Or any other custom LDAP attribute)
- N. Position Enter "title"
- O. User UUID Leave "objectGUID"

	User Mappings	User Group Mappings	User Group Membership Mappings					
	OR JECT CLASS LIMITATION Limitation to set for object classes in the	Direct Class field						
A	All ObjectClass Values 👻							
~ _	OR IECT CLASSIES) Object classies to limit results to Each object class	must be consisted by a comma						
B	organizationalPerson, user	must be separated by a comma						
	SEARCH BASE Distinguished name of the search base							
c —	OU=AADDC Users, DC=hcs,DC=jamfy,DC=tech							
•	SEAPY STORE Harmshall and search hate							
D	All Subtrees V							
	······							
	Attribute Mappings LDAP attribute mappings for Jamf Pro attribut	es						
E	SNCreated							
	UCEDNANE							
F	SerPrincipalName							
G —	displayName							
	EMAIL ADDRESS							
н ——	mail							
	ADDEND TO EMAIL DESULTS Taxt to annead to email address	rasulis la n. "Reminomany com"						
I —		raamin (e.g. grof earliperi fearli (
	DEPARTMENT							
J —	department							
•	BUILDING							
к —	streetAddress							
	ROOM							
L —	pom							
	PHONE							
M ——	Chobile							
	POSITION							
	litte							
	USER UUID							
o <u> </u>	bjectGUID							
0	BlectGOID							

11. Click User Group Mappings.

Connection Map	pings		
	User Mappings	User Group Mappings	User Group Membership Mappings
	Imitation to ent for object classes in the C	blast Class field	

- 12. Configure the User Group Mappings settings as follows:
 - A. Object Class Limitation Leave at "All ObjectClass Values"
 - B. Object Class(es) Enter "group, top"
 - C. Search Base Enter your search base using this example "OU=AADDC Users, DC=contoso, DC=com"
 - D. Search Scope Select "All subtrees"
 - E. Group ID Enter "uSNCreated"
 - F. Group Name Enter "name"
 - G. Group UUID Leave at "objectGUID"

OBJECT CLASS LIMITATION Limitation to set for object classes in the Object Class field All ObjectClass Values						
a comma						
uSNCreated						
GROUP NAME						
name						
	a comma					

13. Click User Group Membership Mappings in the top bar.

Connection Mappings		
User Mappings	User Group Mappings	User Group Membership Mappings



- 14. Configure the User Group Membership Mappings settings as follows:
 - A. Membership Location Choose "User Object"
 - B. Group Membership Matching Enter "memberOf"
 - C. Append to username when searching Leave blank
 - D. Use distinguished name of user groups when searching Select this option
 - E. Use recursive group searches Select this option
- 15. Click Save.

oser mappings	User Group Mappings	User Group Membership Mappings				
MEMBERSHIP LOCATION The object where user group memberships are stored in the LDAP directory						
User Object 🔹						
GROUP MEMBERSHIP MAPPING LDAP directory attribute to m	ap group membership to					
memberOf						
APPEND TO USERNAME WHEN SEARCHING Text to append	o the username when searching the LDAP directory					
						
-						
Use distinguished name of user groups when searn Use distinguished name of user groups when searching the	LDAP directory					
Use distinguished name of user groups when searching the Use distinguished name of user groups when searching the	hing LDAP directory					

16. In the lower-right corner, click Test.

Connection Mappings							
User Mappings	User Group Mappings	User Group Membership Mappings					
MEMBERSHIP LOCATION The object where user group memberships an User Object * GROUP MEMBERSHIP MAPPING LDAP directory attribute to member/of	e stored in the LDAP directory p group membership to						
APPEND TO USERNAME WHEN SEARCHING Text to append to	APPEND TO USERNAME WHEN SEARCHING Text to append to the username when searching the LDAP directory Ika distinguished name of user arguing when searching						
Use distinguished name of user groups when searching the Use recursive group searches Search groups that are members of user groups when search	LDAP directory						



- 17. Click User Mappings.
- 18. Enter a known username and click Test. If you see the username listed then Jamf Pro can make a connection to the LDAPS service, and your User Mappings settings are configured correctly.

User	Mappings		User	Group Mappings		Use	r Group Membersh	ip Mapping	
LOOK UP USERNAME									
nmcdonald									
Test	FULL NAM	E	EMAIL	PHONE	BUILDING	DEPARTMENT	ROOM	POSITION	UID
nmcdonald@hcs.jamfy.tech	Nicholas N	McDonald							20565
0.07 seconds									

19. Click User Group Mappings.

1 11 0		
User Mappings	User Group Mappings	User Group Membership Mapping
LOOK UP USER GROUP		

20. Enter a known User Group and click Test. This guide uses AAD DC Administrators as an example known group. If you see the Group Name listed then User Group Mappings is configured correctly.

User Mappings	User Group Mappings	User Group Membership Mapping
LOOK UP USER GROUP		
AAD DC Administrators		
Test		
GROUP NAME		GID
AAD DC Administrators		12768
0.21 seconds		

21. Click User Group Membership Mappings.

User Mappi	ngs	U	ser Group Mappings	5		User Group Memb	ership Mapping	
LOOK UP USERNAME								
nmcdonald								
Test								
USERNAME	FULL NAME	EMAIL	PHONE	BUILDING	DEPARTMENT	ROOM	POSITION	UID
nmcdonald@hcs.jamfy.tech	Nicholas McDonald							20565
0.07 seconds								

22. In the Check If Username field, enter a known user; in the Is A Member Of User Group field, enter a group the user is a member of (your own account should be in AAD DC Administrators) then click Test. If you see Yes in the Member column, then User Group Membership Mapping is configured correctly.

User Mappings	User Group Mappings	User Group Membership Mapping	
CHECK IF USERNAME			
nmcdonald@hcs.jamfy.tech			
IS A MEMBER OF USER GROUP			
AAD DC Administrators			
Test			
USERNAME		MEMBER	
nmcdonald@hcs.jamfy.tech		Yes	
0.07 seconds			

You have successfully configured Jamf Pro to integrate with Azure AD Domain Services - Secure LDAP service.



Section 5: Configure Azure Active Directory for Single Sign-On (SSO) In this section you configure AADDS to support SSO with Jamf Pro.

- 1. Use Firefox or Google Chrome to open portal.azure.com.
- 2. Log in with your Azure Admin credentials

Microsoft Azure			
 Microsoft ← nmcdonald@hcs.jamfy.tech Enter password Password 			
Forgot my password			

3. In the sidebar, click Azure Active Directory.

Microsoft Azure		, <i>P</i> Search	h resources, services, and docs		>_ 💀 Q 🕴	? O nmcdonald@hcs.jamf
«	Choose your default view	Home Dashboard	Save			
Create a resource Home	Azure services See all (+10)) >				
Dashboard	_	·			•	
i≡ All services	<u> </u>	SQL SQL	I D		* 49	
+ FAVORITES	Virtual Storage machines accounts	App Services SQL databases	Azure Database Azure Cosmos for PostgreSQL DB	Kubernetes Function Apps services	Azure Cognitive Databricks Services	
III resources	Make the most out of Az	ure				
Resource groups						
S App Services	4		0			
Function Apps	-					
SQL databases	Learn Azure with free online courses by Microsoft	Monitor your apps and infrastructure	Secure your apps and infrastructure	Optimize performance, reliability, security, and cost	Connect to Azure via an authenticated browser-based	
Virtual machines	Microsoft Learn 🗹	Azure Monitor >	Security Center >	Azure Advisor >	Cloud Shell >	
Load balancers						
Storage accounts	Recent resources See all y	our recent resources $>$ See all yo	ur resources >	Useful links		
··· Virtual notworks	NAME	TYPE	LAST VIEWED	Get started or go deep with Our articles include everyth	h technical docs 🗹 hing from quickstarts, samples, and	
Azure Active Directory	hcs.jamfy.tech	Azure AD Domain Sen	vices Wed 10:39 PM	tutorials to help you get sta designing applications.	arted, to SDKs and architecture guides for	
C Monitor	AADDS-hcs.jamfy.tech-N	SG Network security grou	p Fri 2:21 AM	Discover Azure products	a	

4. In the Manage section, click "Enterprise applications."

«	Home > HCS Technology Group - Overvi	6.M			
+ Create a resource	HCS Technology Group - Ove	rview			
🛧 Home	Azure Active Directory				
🛄 Dashboard	.> Search (Ctrl+/)	Switch directory			
∃ All services	 Overview 	heeiamfutach			
— 🛧 FAVORITES —————	💕 Getting started	HCS Technology Group			
All resources	Manage	Azure AD for Office 365			
📦 Resource groups	users	Sign-ins	Your role		
🔕 App Services	🗳 Groups		Global administrator		
Function Apps	Organizational relationships				
👼 SQL databases	Boles and administrators	To see sign-in data, your organization needs Azure AD Premium P1 or P2.	Find		
😹 Azure Cosmos DB	Enterprise applications	Start a free trial	Courth		
🧕 Virtual machines	Devices		Search		
🚸 Load balancers	App registrations		Azure AD Connect sync		
Storage accounts	App registrations (Preview)	What's new in Azure AD	Status Not enabled Last sync Sync has never run		
🐡 Virtual networks	Application proxy	Stay up to date with the latest release notes and blog posts.	Create		
Azure Active Directory	🔓 Licenses	50 entries since August 15, 2018. View archive C	🔓 User		
🕒 Monitor	Azure AD Connect	Manufacture	Suest user		
🐢 Advisor	Custom domain names	All services (50)	Group		
Security Center	Mobility (MDM and MAM)	Monitoring & Reporting (4) Reporting - Monitoring & Reporting	App registration		
O Cost Management + Billing	Password reset	3rd Party Integration (6)			
Help + support	Company branding	Azure AD Logs now work with Azure Log Analytics (Public Directory (2) preview)	Other capabilities		
	 company branding 		Identity Protection		

5. In the new window, click "New application."

HCS Technology Group - Azure Active Directory				
0 Overview	New application	15		
Manage	Application Type Enterprise Applications	Application status Application visibility Any V Any	✓ Apply Reset	
All applications	First 50 shown to search all of your	applications, enter a display name or the application ID		
Application proxy	This bo shown, to search an or your	applications, enter a display name or the application rb.		
User settings	NAME	HOMEPAGE URL	OBJECT ID	APPLICATION ID
Security	Office 365 Exchange Onlir	http://office.microsoft.com/outlook/	7b46135c-0365-4138-b0e5-b9e114dee4da	00000002-0000-0ff1-ce00-00000
Conditional Access	Office 365 Management A	.PIs	586b1bf7-f452-473d-8ca0-3d6299de267f	c5393580-f805-4401-95e8-94b7a
	Office 365 SharePoint Onl	ine http://office.microsoft.com/sharepoint/	3b62260e-8415-4362-9bc4-1112802c4ce4	00000003-0000-0ff1-ce00-00000
Activity	GW Outlook Groups		aa27ebd4-661d-4608-8025-3bec028fa1cd	925eb0d0-da50-4604-a19f-bd8d
Sign-ins	P8 Power BI Service		1fd86630-1989-4039-97ab-81bb58f8f747	00000009-0000-0000-c000-0000
Troubleshooting + Support	SF Skype for Business Online		a17f1f54-ec0b-4432-957a-aba525eaa6bb	00000004-0000-0ff1-ce00-00000
👳 Virtual assistant (Preview)				
X Troubleshoot				
New support request				

6. In the "Add from the gallery" section, enter "Jamf Pro", then in the search results section, click Jamf Pro.

Home > HCs rechnology Group > Enterprise appl	ications - All applications / Cate		
Categories ×	Add an application		x ⊔ x
All (3087)	Add your own app		
Business management (359)	Application	On-premises	Non-gallery
Collaboration (429)	developing	Configure Azure AD	Integrate any other
Construction (8)	Register an app you're working on to integrate it	Application Proxy to enable secure remote	application that you don't find in the gallery
Consumer (43)	with Azure AD	access	
Content management (141)			
CRM (150)	Add from the gallery		
Data services (146)			
Developer services (101)	Jamf Pro		~
E-commerce (75)	1 applications matched "Ja	mf Pro".	
Education (134)	NAME		CATEGORY
ERP (79)	jamf Jamf Pro		Business management
Finance (255)			
Health (61)			
Human resources (276)			
IT infrastructure (186)			
Mail (33)			
management (1)			
Marketing (211)			
Media (71)			
Productivity (239)			
Project management (71)			
Security (139)			
Social (101)			



7. In the new panel, click Add.

jam <u>f</u>	Jamf Pro			\times
Jamf	Add upp			
Jamf Pro Integrate enable co provide A Apple de	is the standard in Apple with Azure to share inv onditional access with In uzure AD single-sign-on vices.	manageme entory data tune, and for manage	ent. and ed	
Use Micr Jamf Pro	osoft Azure AD to enabl	e user acce	ss to	
Requires	an existing Jamf Pro sul	oscription.		
Name 👩 Jamf Pr	0			
Publisher Jamf	blisher 🕜 mf			
Single Sig SAML-b	gn-On Mode 🚯 ased sign-on			
URL 🔀 https://w	ww.jamf.com			
ja	mf			
Ad	d			

- 8. Click "Users and groups."
- 9. Click "Add user."

Jamf Pro - Users	and groups			>
Overview Getting started	 Citic Control Contro Control Control Control Control Control Control Control Cont	Update Credentials EE Columns ess panel for assigned users. Set 'visible to users?' to no in properties to prevent	this. ➔	
Getting started	First 100 shown, to search all users & gro	ups, enter a display name.		
Manage	DISPLAY NAME	OBJECT TYPE	ROLE ASSIGNED	
Properties	No application assignments found			
🍰 Owners				
x ^R Users and groups				
Single sign-on				
Provisioning				

10. Click "Users and Groups." If you see "Groups are not available for assignment due to your Active Directory plan level," then for testing, you can continue with adding a user instead of a group.

11. Select a user or group that should be able to access Jamf Pro. If you plan to allow users to use Azure AD to sign in to the User Initiated Enrollment window and Self Service, then select the All Users group. You can allow administrative access to the Jamf Pro web app to different groups or users later in the document.

HCS Technology Group	×	Users and groups	
Users and groups 1 group selected.	>	Select member or invite an external user O Search by name or email address	~
Select Kole Default Access	>	AD AAD DC Administrators	
		AU All Users	
		NM Nicholas McDonald nmcdonald@hcs.jamfy.tech	
		SE secmon secmon@hcs.jamfy.tech	
		Selected members:	
		AU All Users	Remove

13. Click "Single sign-on".

Home > HCS Technology Group > Enterprise applications - All applications > Categories > Add an application > Jamf Pro - Users and groups				
Jamf Pro - Users and groups				
	« 🕂 Add user 🖋 Edit 🛅 Remov	e 🎾 Update Credentials 🛛 🗮 Columns		
Overview Getting started	The application will appear on the a	ccess panel for assigned users. Set 'visible to users?' to no in properties to preven	it this. \rightarrow	
Deployment Plan	First 100 shown, to search all users & g	oups, enter a display name.		
Manage	DISPLAY NAME	OBJECT TYPE	ROLE ASSIGNED	
tit Properties	AU All Users	Group	Default Access	
🔐 Owners				
ศ ^R Users and groups				
Single sign-on				
Provisioning				

14. Select SAML.





15. Next to Basic SAML Configuration, click Edit (looks like a pencil).

Jamf Pro - SAML-based sig	gn-on			
Overview	 Change single sign-on mode Switch Welcome to the new experience for configure 	to the old experience ing SAML based SSO. Please click here to provide feedback. $ imes$		
Getting started Deployment Plan Manage	Set up Single Sign-On with SAM	1L - Preview		
 Properties Owners χ⁰ Users and groups 	Basic SAML Configuration Identifier (Entity ID) Renk (IB) (Acception Consumer Service)	Required		
Single sign-on Provisioning Salf-service	Sign on URL Relay State Logout Url	Optional Optional Optional		
Security	2 User Attributes & Claims		/	
 Conditional Access Permissions Token encryption (Preview) Activity 	Girenname Sumame Emailaddress Name Unique User Identifier	user givenname user sumame user mail user userprincipalname user userprincipalname		
Sign-insAudit logs	3 SAML Signing Certificate Status Thumborint	Active 66964700173CC451AD333CFA6F4112772AE88C9D	1	
Troubleshooting + Support Virtual assistant (Preview) X Troubleshoot New support request	Expiration Notification Email App Federation Metadata Url Certificate (Base64) Certificate (Raw)	3/7/2022, 12:41:15 PM nmcdonald@hcs.jamfy.tech https://ogin.microsoftonline.com/3a4f480d-7f9e-4 Download Download	I	

- 16. Configure the following options as shown below (replace "YourJamfInstance.jamfcloud.com" with your Jamf Pro URL) then click Save.
- 17. In the upper-right corner click Close (X).

Basic SAML Configuration	
R Save ↑ Upload metadata file	
ldentifier (Entity ID) (Required) 👩	
https://YourJamfInstance.jamfcloud.com/saml/metadata	✓ ···
Patterns: https://*.jamfcloud.com/saml/metadata	
Reply URL (Assertion Consumer Service URL) (Required) $_{m 0}$	
https://YourJamfinstance.jamfcloud.com/saml/sso	 ✓ ····
Patterns: https://*jamfcloud.com/saml/SSO	
Sign on URL (Optional) 👩	
https:///www.lawefile.tagasi.comfale.cd	×
https:// YourJaminstance.jamicioud.com	-
Relay State (Optional) 🕤	`
Relay State (Optional) Enter a relay state	· · · · · · · · · · · · · · · · · · ·
Relay State (Optional) Enter a relay state Logout URL (Optional)	· · · · · · · · · · · · · · · · · · ·

18. At the "Test single sign-on" message, click "No, I'll test later."



19. In the SAML Signing Certificate section, next to App Federation Metadata URL, click Copy (looks like two documents). Paste the URL into another document (such as in the Notes app), and keep it in your paste buffer for use in the next section.



20. In the breadcrumb bar, click your organization's Azure AD name.





21. In the Manage sidebar, click "App Registrations."

Home > HCS Technology Group - Overvie	w	
HCS Technology Group - Over Azure Active Directory	view	>
,> Search (Ctrl+/) «	Switch directory 📋 Delete directory	
() Overview	hcs.jamfy.tech	
g ^{er} Getting started	HCS Technology Group Azure AD Premium P1	
Users Groups Groups Groanizational relationships	Sign-ins	Your role Global administrator Noce info ゴ
Roles and administrators Constraints Roles and administrators Devices	06 04 02 0	Find Users V Search
Rep registrations	Feb 10 Feb 17 Feb 24 Mar 3	Azure AD Connect sync Status Not enabled
App registrations (Preview) Application proxy	What's new in Azure AD Suy up to date with the latest release notes and blog posts.	Last sync Sync has never run Create
Licenses Azure AD Connect	To entries since November 15, 2018. View archive C	🎽 User 🐼 Guest user 🔐 Group
Custom domain names	services App Proxy - Access Control Access Control 20 20 20 20 20 20 20 20 20 20 20 20 20	Enterprise application

22. Click "View all applications."

Home > HCS Technology Group - App re	egistrations			
HCS Technology Group - App Azure Active Directory	o registrations			\$ ×
	+ New application registration 🗄 Endpoints 🗙 Troubleshoot			
1 Overview	\checkmark The preview experience for App registrations is available. Click this banner to	launch the preview experience. $ ightarrow$		
getting started	Search by name or ApplD Vy apps V			
Manage	DISPLAY NAME	APPLICATION TYPE	APPLICATION ID	
🔮 Users	Yau	're not the sumer of any applications in this direct	ton.	
🝰 Groups	You re not the owner of any applications in this directory.			
Organizational relationships		view an applications		
• ••• • • • • • •				

23. After the window refreshes, select Jamf Pro.



24. Click Manifest.

Jamf Pro Registered app	\$
Settings 🖍 Manifest 🛱 Deler	e
Display name	Application ID
Jamf Pro 🗈	38a6e618-e2cb-4a29-9ac4-a8be9fddc6d
Application type	Object ID
Web app / API	efe2c290-ab93-4a91-90a5-2cda22cc3e41
Home page	Managed application in local directory
https://*.jamfcloud.com/saml/SSO?meta	d Jamf Pro
	\$

25. Click Edit.

Edit ma	nifest	
R Save	🗙 Discard 📝 Edit 🗍 T Upload 🖳 Download	
1		
2	} "appTd", "28a6a618_a2ch_4a20_0ac4_a8ha0fddc6d4"	- 8
2		
4		
5	l "allovedMemberTypes". [
6		
7		
8	J, "dienlawName", "msiam access"	
0	UISPLOSMAILE - INSTAIL_ACCESS , UISPLOSMAILE - INSTAIL_ACCESS , UISPLOSMAILE - INSTAIL_ACCESS ,	
10	"icFabled", true	
11		
12	uescription: instan_access,	
12		
14		
14	J, NewsilshieTeOtherTeocotell, feloe	_
15	"avaitable lootnerienants": Taise,	
10	"olsplaywame": "Jamt Pro",	
1/	"errorurt": null,	
18	"groupmembershipt talms": nutt,	
19	"optionallaims": null,	_
20	"acceptMappedLaims": null,	_
21	"nomepage": "nttps://*.jamtcloud.com/samt/SSU/metadata=jamtprojiSV9.2[primary]2",	
22	"informationalUrls": {	
23	"privacy": null,	
24	"termsOfService": null	
25	<i>}</i> ,	
26	"IdentifierUris": [
27	" <u>https://ngmnfr.jamfcloud.com/saml/metadata</u> "	
28	1,	
29	"keyCredentials": [],	
30	"knownClientApplications": [],	
31	"logoutUrl": " <u>https://ngmnfr.jamfcloud.com/logout.html</u> ",	
32	"oauth2AllowImplicitFlow": false,	
33	"oauth2AllowUrlPathMatching": false,	
34	"oauth2Permissions": [
35	{	
36	"adminConsentDescription": "Allow the application to access Jamf Pro on behalf of the sign	ned-in u
37	"adminConsentDisplayName": "Access Jamf Pro",	
38	"id": "2131cc3e-854e-473b-80c3-50db344bbfe9",	
39	"isEnabled": true,	
40	"type": "User",	
41	"userConsentDescription": "Allow the application to access Jamf Pro on your behalf.",	
42	"userConsentDisplayName": "Access Jamf Pro",	
43	"value": "user_impersonation"	



26. In the "groupMembershipClaims" line, change the word null to "All", then click Save.

Edit r	nanifest	
R Save	🗙 Discard 🖍 Edit 🕂 Upload 🞍 Download	
1	-	
2	* "appId": "38a6e618-e2cb-4a29-9ac4-a8be9fddc6d4".	
3	"appRoles": [
4		
5	"allowedMemberTypes": [
6	"User"	
7		
8	"displayName": "msiam access".	
9	"id": "b104b496-f392-4f00-84b5-a2c236b62e7d".	
10	"isEnabled": true.	
11	"description": "msiam access".	
12	"value": null	
13		_
14	1.	
15	"availableToOtherTenants": false.	
16	"displayName": "Jamf Pro".	
17	"errorUrl": null.	
18	"groupMembershipClaims": "All".	
19	optionattiaims : nutt.	
20	"acceptMappedClaims": null.	
21	<pre>"homepage": "https://*.jamfcloud.com/saml/SSO?metadata=jamfpro/ISV9.2/primary/z".</pre>	
22	"informationalUrls": {	
23	"privacy": null,	
24	"termsOfService": null	
25	},	
26	"identifierUris": [
27	"https://ngmnfr.jamfcloud.com/saml/metadata"	
28	1,	
29	<pre>"keyCredentials": [],</pre>	
30	<pre>"knownClientApplications": [],</pre>	
31	<pre>"logoutUrl": "https://ngmnfr.jamfcloud.com/logout.html",</pre>	
32	<pre>"oauth2AllowImplicitFlow": false,</pre>	
33	<pre>"oauth2AllowUrlPathMatching": false,</pre>	
34	"oauth2Permissions": [
35	{	
36	"adminConsentDescription": "Allow the application to access Jamf Pro on behalf of the signed	l-in ι
37	"adminConsentDisplayName": "Access Jamf Pro",	
38	"id": "2131cc3e-854e-473b-80c3-50db344bbfe9",	
39	"isEnabled": true,	
40	"type": "User",	
41	"userConsentDescription": "Allow the application to access Jamf Pro on your behalf.",	
42	"userConsentDisplayName": "Access Jamf Pro",	
43	"value": "user_impersonation"	

You have successfully configured Azure AD for Single Sign-On (SSO).

Section 6: Configure Jamf Pro for Azure AD - Single Sign-On In this section you configure Jamf Pro to support SSO with Azure AD.

1. Navigate to your Jamf Pro instance and log in with administrator credentials.

🛂 jamf 🛛 PRO		
USERNAME ex. admin		
PASSWORD	\bigcirc	
All contents © 2002-2019 Jamf. All rights reserved.		

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

🖆 jamf PRO		£ 🖗 🏟
Computers Devices Users VERSION VERSION VERSION VERSION Computers 3 Mobile Devices: 1 Version Versio	Arree 6 6 7 8 8 9 9 9 9 9 9 9 9 9 9 9 9 9	

Settings button



3. In the System Settings section, click Single Sign-On.

🛂 jamf 🛛 PRO											ይ	¢ 🖗
Computers Devices Users	錼	All Settings	System Se	ttings								
	000	System Settings	Jamf Pro User	Single Sign-	@ LDAP Servers	SMTP Server	Clustering	Activation	Change	Apache	Limited	
		Global Management	Groups	01				couc	management	Settings	Access	
	B	Self Service	Log Flushing	Maintenance	Engage							
Computers: 0 Mobile Devices: 1	Å	Server Infrastructure		Pages								
	글	Network Organization	Global Mar	nagement								
		Computer Management		\Leftrightarrow	<u></u>	3	Complexer	,×,		6		
	Ē	Device Management	Categories	Push Certificates	GSX Connection	Jamf Pro URL	PKI Certificates	VPP Accounts	User-Initiated Enrollment	Device Enrollment Program	Re-enrollment	

4. In the lower-right corner click Edit.

Settings > System Settings > Single Sign-On	
Single Sign-On (SSO) Utilization Applications or services to require Single Sign-On authentication (all other passwords will fail to authenticate)	
Jamf Pro Server	
USER MAPPING: SAML Specify how users will be extracted from the SAML assertion	
NamelD	
User Attribute:	
USER MAPPING: JAMF PRO Specify how users from your identity provider will be mapped to Jamf Pro users	
Username	
Email	
GROUP ATTRIBUTE NAME Name of the SAML assertion attribute containing your group	
http://schemas.xmlsoap.org/claims/Group	
RDN KEY FOR LDAP GROUP Relative Distinguished Name key to extract group name from the LDAP string (e.g. "CN" or "DC")	
IDENTITY PROVIDER SAML identity provider to use for Single Sign-On	
- Select - v	
IDENTITY PROVIDER METADATA SOURCE Upload identity provider metadata file or provide a metadata URL	
- Select - *	
ENTITY ID Entitly ID used by Jamf Pro	
https://xserve.jamfcloud.com/sami/metadata	
JAMF PRO SIGNING CERTIFICATE Upload or generate certificate used to sign messages from Jamf Pro to the identity provider. If no certificate, messages will not be signed.	
	Done History Edit

- 5. Select the checkbox "Jamf Pro Server". Additional options are displayed.
 - A. Leave the checkbox deselected for the option "Allow bypass for all users." When you leave this option disabled, administrators must use SSO to access the Jamf Pro web interface, unless they have "Single Sign-on" update privileges. In the next section of this guide you'll create a group for administrators that do not have Single Sign-on update privileges, so they cannot bypass SSO. Be sure that you always have at least one Jamf Pro standard account with Administrator privileges that can access your Jamf Pro failover URL in case there is a problem with SSO, so you can log in to Jamf Pro and update your Single Sign-on configuration.
 - B. Select the checkbox "Self Service for macOS" to enable SSO authentication for Self Service for macOS. Note, for this option to have an effect, under Settings > Self Service > macOS, you must enable the option "Enable Self Service User Login", then choose either "Allow users to log in to view items available to them" or "Require login."
 - C. Select the checkbox "User-Initiated Enrollment" to enable users enrolling devices at your web enrollment portal to authenticate with SSO. Note: to enable only certain groups to be able to enroll devices with your web enrollment portal, select "Only this group" and and enter the object ID of an Azure AD group; finding Group Object ID's is covered on page 62 step 7.

	Settings > System Settings > Single Sign-On
	Sincle Sign-On (SSO) Utilization Applications or services to require Single Sign-On authentication (all other passwords will fail to authenticate) Jamf Pro Server
A —	Allow bypass for all users Users can authenticate with a Jamf Pro user account by going to https://ngmnfr/jamfcloud.com
	Additional login URL for users with privileges: https://ngmnfr.jamfcloud.com?failover Users with Single Sign-On update privileges can authenticate with a Jamf Pro user account by going to this private URL
в —	Self Service for macOS Self Service access will be granted to any existing username from the identity provider
c —	Users will erroll using the login page from the identity provider
	CONFIGURE ENROLLMENT ACCESS FOR:
	Any identity provider user
	Only this group:

6. Leave User Mapping: SAML at its default configuration; Jamf Pro will use the UPN from Azure to match to a user in Jamf Pro. An example user from this guide is nmcdonald@hcs.jamfy.tech.

USER MAI	PPING: SAML	Specify how users will be extracted from the SAML assertion
Nar	meID	
Use	er Attribute:	

Leave User Mapping: Jamf Pro at its default configuration, unless you configured Azure such that a user's UPN does not match the Jamf Pro user's username (this guide uses the example Jamf Pro user name nmcdonald@hcs.jamfy.tech, which matches the example Azure UPN). Change this to Email if that is a better fit for your environment. If you use groups to control access this is somewhat irrelevant as you will not be creating single users to match to.

USER MAPPING: JAMF PRO Specify how users from your identity provider will be mapped to Jamf Pro users





7. In the Group Attribute Name field, enter: http://schemas.microsoft.com/ws/2008/06/identity/claims/groups. This tells Jamf Pro what SAML attribute to use group membership. Leave the "RDN Key for LDAP Group" field blank.

8. Click the Identity Provider menu, choose Other, and enter "Azure AD" in the Other Provider field.

IDENTI	TY PROVIDER SAML identity provider	to use for Single Sign-On
Other		
	OTHER PROVIDER:	
	Azure AD	

9. Click the Identity Provider Metadata Source menu, choose Metadata URL, and enter the URL you copied earlier in the previous section, step 19 (you can find the Metadata URL in your Azure portal > Azure Active Directory > Enterprise applications > Jamf Pro > Single Sign-On > SAML Signing Certificate > App Federation Metadata URL).

IDENTITY PROVIDER METADATA SOURCE Upload identity provider metadata file or provide a metadata URL Metadata URL *
https://login.microsoftonline.com/3a4/480d-7/9e-4438-9be9-a1e166b7b7dd/federationmetadata/2007-06/federationmetadata.xml?appld=c2aff364-f00a-46b6-a15b-9c33tee438cc
ENTITY ID Entity ID used by Jamif Pro
https://ngmnfr.jamfcloud.com/sami/metadata
JAMF PRO SIGNING CERTIFICATE Upload or generate certificate used to sign messages from Jamf Pro to the identity provider. If no certificate, messages will not be signed. No Certificate

- 10. Leave "Entity ID" and "Jamf Pro Signing Certificate" at their default values.
- 11. Set the Token Expiration field to whatever value in minutes you would like; after a token expires you will be logged out. Think of this as a session timeout value. The default value is 480 minutes (8 hours).



		Settings b
n the lower-rigl	nt corner click Save, then click Settings.	۲Ç۶
🗖 jamf PRO	ې ۵ کې کې د د د د د د د د د د د د د د د د د	
Devices Users	Settings > System Settings > Single Sign-On	-
	USER MAPPING: JAMP PRO Specify how users from your identity provider will be mapped to Jamf Pro users	
10.10.1+t1551187745 MANAGED Computers: 3	Email	
	GROUP ATTRIBUTE NAME Name of the SAML assertion attribute containing your group	
	http://schemas.microsoft.com/ws/2008/06/identity/claims/groups	
Computers: 0 Mobile Devices: 1	RDN KEY FOR LDAP GROUP Relative Distinguished Name key to extract group name from the LDAP string (e.g. "CN" or "DC")	
	IDENTITY PROVIDER SAML identity provider to use for Single Sign On Other	
	OTHER PROVIDER:	
	Azure AD	
	IDENTITY PROVIDER METADATA SOURCE Upload identity provider metadata file or provider metadata UR.	
	Metadata URL 👻	
	https://login.microsoftonline.com/3a/1480d-7/9e-4438-9be9-a1e166b7b7b7dd/federationmetadata/2007-06/federationmetadata.xml?appid=38a6e618-d2cb-4a29-9ac4-a8be9/fddc6d4	
	ENTITY ID Entity ID used by Jamf Pro	
	https://ngmnfrjamfcloud.com/sami/metadata	
	JAMP PRO SIGNING CERTIFICATE Upload or generate certificate used to sign messages from Jamf Pio to the identity provider. If no certificate, messages will not be signed.	
	TOKEN EXPIRATION (MINUTES) Amount of time before SAML token expires 480	
	Corret	

You are done configuring the Jamf Pro Single Sign-On settings. You will test these settings in the next section.



Section 7: Create an Azure Group and Jamf Pro Groups for Administrator Access to Jamf Pro

In this section you'll configure a group of administrators that can administer Jamf Pro but cannot use the Jamf Pro failover URL; these administrators must use SSO to log in to Jamf Pro.

When you attempt to use SSO to authenticate to Jamf Pro, your browser sends an SAML assertion (Statement) from Azure to your Jamf Pro server.

Jamf Pro attempts to match the username asserted (Stated) to either a Jamf Pro Standard Account or a Jamf Pro LDAP Account.

Other Identity Providers (IdPs) include an assertion that includes the names of groups that the authenticated user is a member of, so Jamf Pro can attempt to match that user to a Jamf Pro LDAP or standard group. The Azure AD assertion does not include the plain text names of groups the authenticated user is a member of, so Jamf Pro cannot match an authenticating SSO user to a Jamf Pro LDAP group. However, the Azure AD assertion does include the OID of groups a user is a member of. So you'll create a Jamf Pro Standard group whose name matches the OID of the Azure AD group.

But what about portions of Jamf Pro that do not use SSO? You will create a Jamf Pro LDAP Group that matches the Azure AD group, so an administrator can use their Azure AD credentials to authenticate to portions of Jamf Pro that do not support SSO, such as Jamf Admin, Recon, and Jamf Imaging.

If at any point Jamf Pro shows "Single Sign On Error" go to office.com and sign out of your Office 365 account, then close and re-open your browser.

You'll create the following:

- An Azure AD group
- A Jamf Pro standard group whose name matches the LDAP group's Azure OID. This allows Jamf Pro to match SSO group membership assertions to authenticate to the Jamf Pro web interface.
- A Jamf Pro LDAP group that matches the Azure AD group to authenticate to the portions of Jamf Pro that do not use SSO

Do not perform this step for administrators that need to be able to use the Jamf Pro failover URL.

Do not perform this step for users who do not administer Jamf Pro.

1. Use Firefox or Google Chrome to open portal.azure.com and sign in as an Azure AD admin.

	Microsoft		
Sig	gn in		
Ema	ail, phone, or Skype		
No a	account? Create one!		
Can	't access your account?		
		Next	

2. In the sidebar, click Azure Active Directory.



3. Click Groups.

Microsoft Azure		,≏ Se	arch resource	es, services, and docs	– ttp D @ ? ☺ nmcda на					
	Home > HCS Technology Group - Overv	view								
+ Create a resource	HCS Technology Group - Overview									
🛧 Home	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	Culture allocations	n Delete di							
🔟 Dashboard	,> Search (Ctrl+/)	& switch directory	Delete di							
∃ All services	 Overview 	hcs.jamfy.tech	hcsjamfytech							
* FAVORITES	💅 Getting started	HCS Techno	HCS Technology Group							
All resources	Manage	Azure AD Premium P1								
📦 Resource groups	🔓 Users	Sign-ins			Your role					
🔇 App Services	🝰 Groups	3		I	Global administrator More info @					
🎸 Function Apps	Organizational relationships	2.5								
🗃 SQL databases	Roles and administrators	1.5			Find					
🐼 Azure Cosmos DB	Enterprise applications	1		Cearch						
🐖 Virtual machines	Devices	0.5			Search					
💠 Load balancers	App registrations	Fi	10 to	Feb 17 Feb 24 Mar 3	Azure AD Connect sync					
Storage accounts	App registrations (Preview)	What's new in Azu	e AD		Status Not enabled Last sync Sync has never run					
Virtual networks	Application proxy	Stay up to date with the I	atest release r	otes and blog posts.	Greate					
Azure Active Directory	🔓 Licenses	16 entries since Novemb	er 15, 2018. V	ew archive 🕫	Ser User					
Monitor	Azure AD Connect			Newforkers	🔕 Guest user					
🗣 Advisor	🕫 Custom domain names	✓ All services	(16)	New reature	Group					
Security Center	Ø Mobility (MDM and MAM)	Access Control	(2)	January 20, 2019	App registration					
Ost Management + Billing	Password reset	3rd Party	(2)	New Amure AD Application Prove cookin acting						
Page Help + support	Company branding	Identity Security &		New Azure AD Application Proxy COOkle settings	Other capabilities					
	User settings	Protection	(2)		Privileged Identity Management					
	Properties	Privileged Identity		New feature	Tenant restrictions					
	Notifications settings	Management	(2)	Azure AD Domain Services Access reviews						
		Directory	(2)	January 20, 2019						
	security	Risk	(1)	New Federated Apps available in Azure AD app gallery - January						



4. Click "New group."

Microsoft Azure		\mathcal{P} Search resources, services, and docs		>_ 🖓	p @ ? ☺
All Users «	Home > HCS Technology Group > Groups	- All groups			
+ Create a resource	Groups - All groups HCS Technology Group - Azure Active Directory				
🛧 Home	« [+ New group			
🔚 Dashboard	🝰 All groups				
E All services	🔐 Deleted groups	Search groups			
+ FAVORITES	Sattings	NAME	GROUP TYPE		MEMBERSHIP TYPE
III resources	A General		for the		
📦 Resource groups		AD DC Administrators	security		Assigned
🔇 App Services		AU All Users	Security		Dynamic
Function Apps	Activity				
🥃 SQL databases	Access reviews				
🥖 Azure Cosmos DB	Audit logs				
Virtual machines	Troubleshooting + Support				
🚸 Load balancers	X Troubleshoot				
Storage accounts	New support request				

- 5. Configure the following options for the new group:
 - A. Click "Group type" then choose "Security" (you could also use "Office 365").
 - B. In the Group Name field enter a name. This guide uses "Jamf Pro Admins" as an example.
 - C. In the Group Description field enter a short description of the group This guide uses "Jamf Pro Admins unable to skip SSO for Jamf Pro" as an example.
 - D. Click "Member type" then choose Assigned.
 - E. Click Members.
 - F. In the "Select member or invite an external user" field, enter an Azure AD User, then press Return.
 - G. Select the user.
 - H. In the lower-left corner click Select.
 - I. Review the settings for the new group then click Create.

Microsoft Azure			$ \mathcal{P} $ Search resources, services, and docs	
	Home > HCS Technology Gr	roup > Groups - All gr	oups > Group > Select members	
+ Create a resource	Group	×	Select members	\Box ×
🛧 Home				
🛄 Dashboard	* Group type		Select member or invite an external user ()	
E All services	Security	~	nmcdonald@hcs.jamfy.tech	
+ FAVORITES	* Group name 🔀		Nicholas McDonald	
All resources	Jamf Pro Admins	~	nmcdonald@hcs.jamfy.tech	
📦 Resource groups	Group description	1 550 ft 1		
App Services	Damt Pro Admins unable to se	ap SSO for Ja 🗸		
	* Membership type 🕤			
	Assigned	•		
	Members 😗	>		
No. of the second second				
virtuai machines				
Load balancers				
Storage accounts			Selected members:	
Virtual networks			Nicholas McDonald	Remove
Azure Active Directory			nmcdonald@hcs.jamfy.tech	
😁 Monitor				
📫 Advisor				
Security Center				
Cost Management + Billing				
Help + support				
	Create		Select	

6. Select the group you just created (this guide uses the example "Jamf Pro Admins"). If you don't see your new group, wait a moment and refresh the page.

Microsoft Azure			5	17				© nmcd нс
	Home > Groups - All groups							
+ Create a resource	Groups - All groups							
🛧 Home	**************************************	► New group C) Refresh EE Columns						
🛄 Dashboard	🝰 All groups	Normal States						
∃ All services	🝰 Deleted groups	Search groups						
🛨 FAVORITES	Settings	NAME	GROUP TYPE		ME	MBERSHIP	TYPE	
All resources	General	AD AAD DC Administrators	Security		As	sianed		
📦 Resource groups	Expiration	All Lisers	Security		Du	namic		
🔇 App Services			Secondy		.,			
🦘 Function Apps	Activity	JP Jamf Pro Admins	Security		As	signed		
🧧 SQL databases	Access reviews							
🥭 Azure Cosmos DB	Audit logs							
🧕 Virtual machines	Troubleshooting + Support							
🚸 Load balancers	X Troubleshoot							

7. Copy the Object ID and paste this information into a text file or the Notes app, because you will need it in a later step.

Microsoft Azure	.> Search resources, services, and docs					>_ 🛱	Ð	ŝ	?	© '
«	Home > Groups - All groups > Jamf Pr	o Admins								
+ Create a resource	Jamf Pro Admins									
🛧 Home	«	m Delete								
🛄 Dashboard	 Overview 	Derete								
i≡ All services	Manage		Jamf P	ro Admins						
— 🛨 FAVORITES ————————————————————————————————————	111 Properties		Jamf Pro Adm	ins unable to skip SSO for Jamf Pro						
III resources	Members	JP								
📦 Resource groups	Owners									
🔇 App Services	Group memberships									
Inction Apps	Applications	Membership type		Assigned						Ē.
👼 SQL databases		Source		Cloud						
🧟 Azure Cosmos DB		-		cloud						40
👰 Virtual machines	- Address	Туре		Security						L L
🚸 Load balancers	Activity	Object ID		71718f61-1b21-4f79-938b-936b922	4dd9f					Ð
🧱 Storage accounts	Access reviews									_
↔ Virtual networks	Audit logs	Momborg								
Azure Active Directory	Troubleshooting + Support	• 1 units							0.0	
😁 Monitor	🗙 Troubleshoot	M T User(s)		U Group(s)	U Device()			00)ther(s)
🗣 Advisor	New support request	Course and and have been		0						
Security Center		Group memberships		Owners						
O Cost Management + Billing		0		<u></u>						

8. Make a note of the time. You can complete several more steps now, but you need to wait about 30 minutes before you continue with the steps that have you create a Jamf Pro LDAP Group. At the time of this publication, https://docs.microsoft.com/en-us/azure/active-directory-domain-services/active-directory-ds-synchronization states, "After initial synchronization completes, it takes about 20-30 minutes for changes that are made in Azure AD to be updated in your managed domain."



9. If you don't already have a window or tab open with your Jamf Pro web admin, you need to use your Jamf Pro failover URL (it follows the format of https://YourJamfInstance.jamfcloud.com/?failover) and log in.

		1	
🚄 jamf PRO			
USERNAME ex. admin			
PASSWORD	\bigcirc		
All contents © 2002-2019 Jan All rights reserved.	nf.		

10. In the upper-right corner, click Settings.

I jamf PRO		ম	£	
Computers 2 VERSION COMPUTERS 12 Computers 3 Mobile Devices 1 Mobile Devices 1	amf Pro ashboard namic Jami Pro Dashboard provides a visual overview of the things you care about most in your iment. Add important items to your Dashboard to quickly and easily monitor their statuses.			

Settings button

11. Click Jamf Pro User Accounts & Groups.

🛂 jamf PRO		
Computers Devices Users	ද්රාදි All Settings	System Settings
VERSION 10.10.1+t1551187745	00 System Settings	Jamf Pro User Accounts & On
MANAGED Computers: 3	Global Management	Groups (WTb)
Mobile Devices: 1	Self Service	Log Flushing Maintenance Engage
Computers: 0 Mobile Devices: 1	Server Infrastructure	- aggest
		Global Management
	Computer Management	😑 😅 🌋 🍪 🔚 🛃
	Device Management	Categories Push GSX Jamt Pro UKL PKI VPP Accounts User-Initiate Certificates Connection Certificates Enrollment
	User Management	
		Event Logs Webhooks Airriay Conditional Inventory

12. Click New.

🜌 jamf PRO							L 🖗 🕸
Computers Devices Users	Settings System Settings Jamf Pro User Acco	ounts	& Groups				
VERSION 10.10.1+t1551187745							+ New Password Policy
MANAGED Computers: 3	USERNAME	^	FULL NAME	EMAIL	ТҮРЕ	ACCESS	PRIVILEGES
Mobile Devices: 1	audit		Auditor Manager		Standard User	Group Access	Group Privileges
UNMANAGED Computers: 0	ladmin				Standard User	Full Access	Administrator
Mobile Devices: 1							

13. Select Create Standard Group then click Next.



- 14. For the "Display Name" enter the Object ID you collected in Step 7.
- 15. Click Privilege Set and choose Custom. Cick Save.

🏜 jamf 🛛 PRO		ম	چ چ
Computers Devices Users	Settings > System Settings > Jamf Pro User Accounts & Groups > New Jamf Pro User Group		
version 10.10.1-11551187745	Group Privileges Members		
MANAGED Computers: 3	DISPLAY NAME Display name for the group		
Mobile Devices: 1	777/8/6/1/b214/79-938b-936b9224dd9f		
Computers: 0	Custom •		
mobile Devices, 1			
Collapse Menu		Cancel	Save



- 16. Click the Privileges tab.
- 17. Select Jamf Pro Server Objects.
 - A. Under the Create column, click All.
 - B. Under the Read column, click All.
 - C. Under the Update column, click All.
 - D. Under the Delete column, click All.
- 18. Select Jamf Pro Server Settings.
 - A. Under the Read column, click All.
 - B. Under the Update column, click All.
 - C. Next to Single-Sign On, deselect the Update checkbox.
 - D. Next to SSO Settings, deselect the Update checkbox.

Re-enrollment		
Security	\checkmark	
Self Service		
Self Service for iOS	\checkmark	
Single Sign-On		
SMTP Server		
Sso Settings	\checkmark	
User-Initiated Enrollment		

- Cancel Save
- 19. Select Jamf Pro Server Actions, then click All. You don't need to update the permissions for Recon, Jamf Admin, Jamf Remote, or Jamf Imaging, because you cannot use SSO to authenticate to these tools. If your administrators need to use those tools, you will create an LDAP group later in this section.
- 20. Click Save. In the upper-right corner, click the user silhouette, then choose Logout.
- 21. Test SSO access to Jamf Pro. Open a new web browser window or tab, then open your Jamf Pro URL.
- 22. Confirm that the Microsoft account picker is displayed.



- 23. If your Azure AD account is displayed, select it. Otherwise, click "Use another account," enter your Azure AD email address, click Next, enter your Azure AD password, then click "Sign in." If your web browser offers to save your password, do not save the password.
- 24. Confirm that you see your Jamf Pro administration interface.

⊿ jamf PRO	<u> </u>
Computers Devices Users Missage	Account Preferences
VERSION NO. NO. 1555187745	Logout nmcdonald@hcs.jamfy.tech
Complexes 3 Complexes Software License 240 Dasnboard	
Mobile Devices: 1 72 The dynamic Jamf Pro Dashboard provides a visual overview of the things you care about most in your UNMANAGED Used environment. Add Important items to your Dashboard to quickly and easily monitor their statuses.	
Computers 0 0 23 Remaining Mobile Devices: 1 0 143 Rev 0 23 Remaining 0 Falled	
Jamf Pro Setup Tasks	
Configure the SMTP server settings in Jamf Pro so you can send email notifications, enrollment invitations, and mass emails.	
Configure SMTP Server	

- 25. This is optional, but you can confirm that you can not yet use an Azure AD user to authenticate to Jamf Admin with the following outline:
 - A. Quit Jamf Admin if it's open.
 - B. In the Finder, open your Applications folder, then open the Jamf Pro folder.
 - C. Press and hold the Option key on your keyboard, and double-click Jamf Admin.
 - D. Provide your Jamf Pro Server Address if prompted.
 - E. If you see the dialog that starts with "Jamf Admin wants to use your confidential information..." then click Deny. You will see this dialog for each item you have named Jamf Software Server in your keychain; click Deny for each dialog.
 - F. In the authentication dialog for Jamf Pro, leave the checkbox disabled for the option "Store in Keychain".
 - G. Enter your Azure credentials, then click OK to log in.
 - H. Confirm that Jamf Pro displays an authentication error.
 - I. Quit Jamf Admin.
- 26. If your administrators do not need to use the portions of Jamf Pro that do not use SSO, you can skip the rest of the steps in this section.
- 27. Log in to your Jamf Pro web admin interface.
- 28. In the upper-right corner, click Settings.
- 29. Click Jamf Pro User Accounts & Groups.
- 30. Click New.



31. Select Add LDAP Group then click Next.



32. In the Search User Groups field, enter the name you gave your group in Azure (this guide uses "Jamf Pro Admins"), then click Next.



33. Next to the Azure group, click Add.

🗖 jamf 🛛 PRO				ম	چ 🏓
Computers Devices Users	Settings : System Settings : Jamf Pro User Accounts & Groups				
VERSION 10.03.1155187745 MARAGED Computer: 3 Mobile Devices: 1 UMMARAGED Mobile Devices: 1	 Choose Action Search LDAP Add User or Group 	Add LDAP User or Group anoue Jamf Pro Admins	server Office 365		Add
Collopse Menu	2			Cancel	Back

34. Leave Privilege Set at Custom, then click the Privileges tab.

🗖 jamf 🛛 PRO		چ چ
Computers Devices	Gentings Spatient Settings Just Physical Settings New Jamf Pro User Group Users New Jamf Pro User Group New Jamf Pro User Group New Jamf Pro User Group	
	Group Privileges	
	DISPLAY NAME Display name for the group	
	Jam Pro Admins	
Computers: 0	PRIVILEGE SET Set of privileges to grant the group	
	custom +	
	Cancel	Save



- 35. Select Jamf Pro Server Objects.
 - A. Under the Create column, click All.
 - B. Under the Read column, click All.
 - C. Under the Update column, click All.
 - D. Under the Delete column, click All.
- 36. Select Jamf Pro Server Settings.
 - A. Under the Read column, click All.
 - B. Under the Update column, click All.
 - C. Next to Single-Sign On, deselect the Update checkbox. Even though this LDAP group is for portions of Jamf Pro that do not use SSO, if you configure the group to be able to update this option, Jamf Pro will automatically enable Update for "SSO Settings".
 - D. Next to SSO Settings, deselect the Update checkbox.

Re-enrollment		
Security	\checkmark	
Self Service		
Self Service for iOS	\checkmark	
Single Sign-On		
SMTP Server		
Sso Settings		
User-Initiated Enrollment		

Cancel

Save

- 37. Select Jamf Pro Server Actions, then click All.
- 38. Select Recon, then click All.
- 39. Select Jamf Admin, then click All.
- 40. Select Jamf Remote, then click All.
- 41. Select Jamf Imaging, then click All.
- 42. Click Save.

43. Confirm that you cannot authenticate using the Jamf Pro failover URL. In a new web browser window or tab, enter your Jamf Pro failover URL (it follows the format of https://YourJamfInstance.jamfcloud. com/?failover).



- 44. Enter the credentials for an Azure AD user in the Azure AD group that should not have the ability to use the Jamf Pro failover URL, then press Return or click the right arrow.
- 45. Confirm that Jamf Pro displays "Access Denied."



Access Denied

Contact your administrator to request access to the Jamf Pro server.

- 46. Close the browser window or tab.
- 47. This is optional, but you can confirm that you can use an Azure AD user to authenticate to Jamf Admin with the following outline:
 - A. Quit Jamf Admin if it's open.
 - B. In the Finder, open your Applications folder, then open the Jamf Pro folder.
 - C. Press and hold the Option key on your keyboard, and double-click Jamf Admin.
 - D. Provide your Jamf Pro Server Address if prompted.
 - E. If you see the dialog that starts with "Jamf Admin wants to use your confidential information..." then click Deny. You will see this dialog for each item you have named Jamf Software Server in your keychain; click Deny for each dialog.
 - F. In the authentication dialog for Jamf Pro, leave the checkbox disabled for the option "Store in Keychain".
 - G. Enter your Azure credentials, then click OK to log in.
 - H. Confirm that you see your expected Jamf Admin window.
 - I. Quit Jamf Admin.

You have now successfully configured Jamf Pro to use an AD Azure Group to authenticate to administer Jamf Pro.



Section 8: Configure an Individual Azure User for Jamf Pro Admin Access

Perform this task only for someone that should be able to authenticate to the Jamf Pro failover URL with their Azure AD credentials. This account will be able to do the following:

- use SSO to log in to the Jamf Pro web interface
- use the Jamf Pro failover URL to log in to the Jamf Pro web interface
- use their username and password to administer Jamf Pro with the Jamf Pro apps for Mac.

Do not perform this task for users that do not administer Jamf Pro.

Do not perform this task for administrators that should not be able to use Jamf Pro failover URL.

1. Click Jamf Pro User Accounts & Groups.

🗖 jamf 🛛 PRO		
	ද්රා All Settings	System Settings
VERSION 10.10.1-1551187745 MANAGED Computers: 3 Mobile Devices: 1 UMMANAGED Computers: 0	Global Management	Image: Single Sign- LDAP Servers Image: Single Sign- LDAP Servers Image: Single Sign- LDAP Servers Image: Single Sign- Charactering Image: Single Single Sign- Charactering Image: Single Si
Mobile Devices: 1	Network Organization	Global Management
	Computer Management	Categories Push Certificates Connection Certificates Connection
	User Management	Event Logs Webbooks AirPlay Conditional Inventory Preload
		Self Service
Collapse Menu		macOS IOS Bookmarks

2. Click New.

🞜 jamf 🛛 PRO					£ 🖗 🕸
Computers Devices User	Settings System Jamf Pro Use	er Accounts & Groups			
VERSION 10.10.1-11551187745					+ New Password Policy
MANAGED	USERNAME	A FULL NAME	EMAIL	YPE AC	CESS PRIVILEGES
Mobile Devices: 1	audit	Auditor Manager	s	itandard User Gro	aup Access Group Privileges
UNMANAGED Computers: 0	ladmin		S	itandard User Ful	Administrator
Mobile Devices: 1					

3. Select Add LDAP Account then click Next.





4. Enter the full username (email) of a user in Azure that you wish to add to Jamf Pro, then click Next.

🗾 jamf PRO		ß	\$
Computers Devices Users	Settings > System Settings > Jamf Pro User Accounts & Groups		
VERSION 10.10.11551187745 MANAGED Computers: 3 Mobile Devices: 1	Choose Action Search LDAP Directory Service StaticH USERS Inncdonald@hcs.jamfytech		
UNMANAGED Computers: 0 Mobile Devices: 1			
 Collapse Menu 		Cancel Back	Next

5. Next to the appropriate LDAP user, click Add.

🖆 jamf 🛛 PRO					L 🍾 🕸
Computers Devices Users	Settings > System Settings > Jamf Pro User Accounts & Groups				
VERSION 10.10.1-11551187745 MANAGED	Choose Action Search LDAP	Add LDAP User or Group	FULL NAME	EMAIL ADDRESS	
Computers: 3 Mobile Devices: 1 UNMANAGED Computers: 0	Add User or Group	nmcdonaio@ncs.jamy.tecn	NICHOIAS MCDONAId	nmcdonaioi¤ncs.jamty.tecn	Add
Mobile Devices: 1					
Collapse Menu					Cancel Back
6. Click Privilege Set, choose Administrator, then click Save.

🜌 jamf PRO			L 🍾 🏟	
Computers Devices Users	Settings: Exystem Settings: Exystem Settings: New Accounts & Groups: Experimental Section Settings: Experimental Section Secti			
version 10.10.1+11551187745	Account Privileges			
MANAGED Computers: 3	USERNAME Username for the account			
Mobile Devices: 1	nmcdonaldthcsJamfyttech			
UNMANAGED Computers: 0 Mobile Devices: 1	PRIVILEGE SET Set of privileges to grant the account Administrator			
	ACCESS STATUS Access status of the account ("enabled" or "disabled") Enabled			
	FULL NAME Name of the account holder (e.g. "John Smith")			
	Nicholas McDonald			
	EMAIL ADDRESS Email address for the account (e.g. "johntimycompany.com")			
	mccdonaldBhcs.jamfytech			
	Applications or services to require Single Sign-On authentication (all other particular)	swords will fail to authenticate)		
		land Day Deven		
	~			
	· · · · · · · · · · · · · · · · · · ·	User-Initiated Enrollment		
Collapse Menu			Cancel	

- 7. Test SSO access to Jamf Pro. In the upper-right corner, click the user silhouette, then choose Logout.
- 8. Close the web browser tab or window.
- 9. Open a new web browser window or tab, then open your Jamf Pro URL.
- 10. Confirm that the Microsoft account picker is displayed.





- 11. If your Azure AD account is displayed, select it. Otherwise, click "Use another account," enter your Azure AD email address, click Next, enter your Azure AD password, then click "Sign in." If your web browser offers to save your password, do not save the password.
- 12. Confirm that you see your Jamf Pro administration interface.

™jamf PRO	<u>A</u> 🖗 🐡
Computers Devices Users MISSAGE	Account Preferences
VERSION 10/0/MISSIS/7/45 920 10/0/ December 2000 10/0/December 2000 10/0/December 2000 10/0/December 2000	Logout nmcdonald@hcs.jamfy.tech
Computers: 3 Compress: 1 72	
UNMANAGED Used environment. Add important items to your Dashboard to quickly and easily monitor their statuses.	
Mobile Devices: 1 A 143 Ref 23 Remaining 0 Failed	
Jamf Pro Setup Tasks	
Configure the SMTP server settings in Jami Pro so you can send email	
notifications, enrollment invitations, and mass emails.	
Configure SMTP Server	

- 13. Confirm that you can use this LDAP account to bypass SSO to log in to the Jamf Pro web interface. In the upper-right corner, click the user silhouette, then choose Logout.
- 14. Close the web browser tab or window.
- 15. Open a new web browser window or tab, then open your Jamf Pro failover URL (which follows the format of https://YourJamfInstance.jamfcloud.com/?failover).
- 16. Confirm that your browser displays the Jamf Pro username and password fields, not the Microsoft account picker.
- 17. Confirm that you can user the Azure AD credentials to log in to Jamf Pro.

™ jam f PRO	<u>र</u> 🗞 🕸
Computers Devices Users Stream	Account Preferences
VERSION 10/10/155/187745 MAIMATO	Logout nmcdonald@hcs.jamfy.tech
Computers: 3 Computers: 3 Mobile Devices: 1 To dynamic Jamif Pro Dashboard provides a visual overview of the things you care about most in your	
UNMANAGED Used environment. Add important items to your Dashboard to quickly and easily monitor their statuses.	
Mobile Devices: 1	
Jamf Pro Setup Tasks	
Configure the SMTP server settings in Jami Pro so you can send email notifications, enrollment invitations, and mass emails.	
Configure SMTP Server	

You have successfully added an individual SSO/LDAP User to Jamf Pro