



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

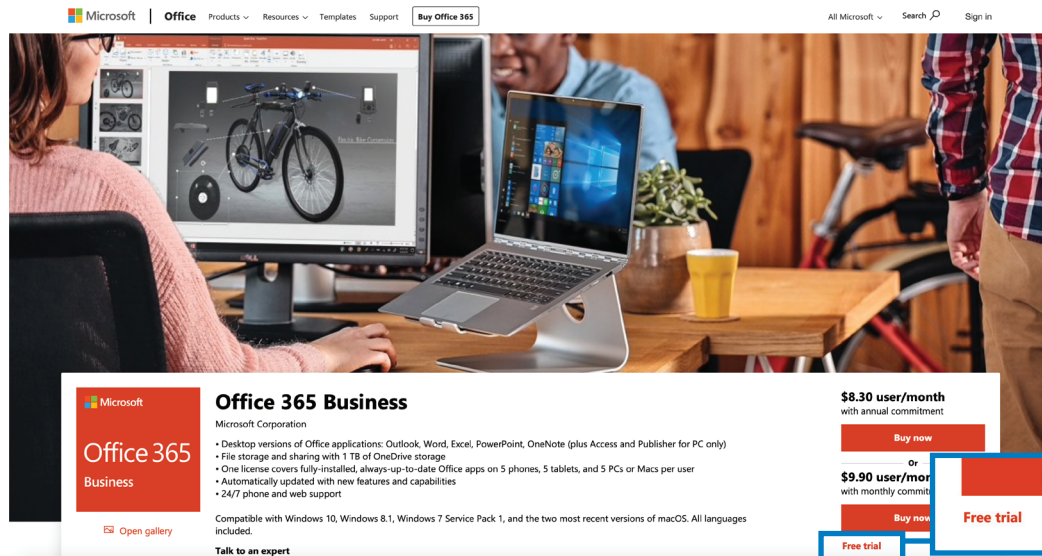
Section 1: Create an Office 365 Account	Page 4
This section covers creating an Office 365 account if you do not already have one as well as configuring a custom domain.	
Section 2: Create an Azure Account	Page 12
This section covers enabling Azure services from your Office 365 account.	
Section 3: Configure 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	Page 38
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 an Azure Group and Jamf Pro Groups for Admin Access to Jamf Pro	Page 58
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.



"Free Trial" is located 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.

Office 365 Business Trial

Want to add this to an existing subscription? [Sign in](#)

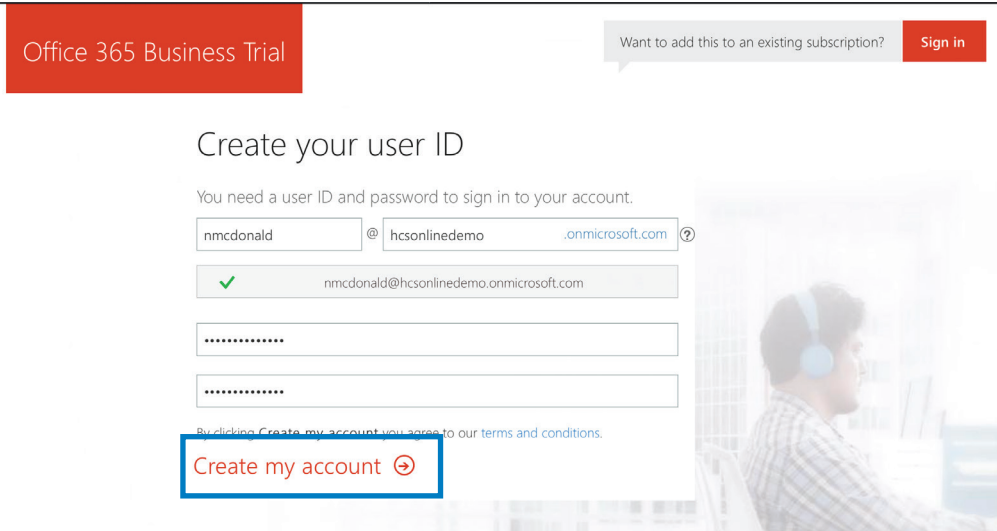
Welcome, let's get to know you

United States
This can't be changed after sign-up. Why not?

Nicholas McDonald

[Next](#)

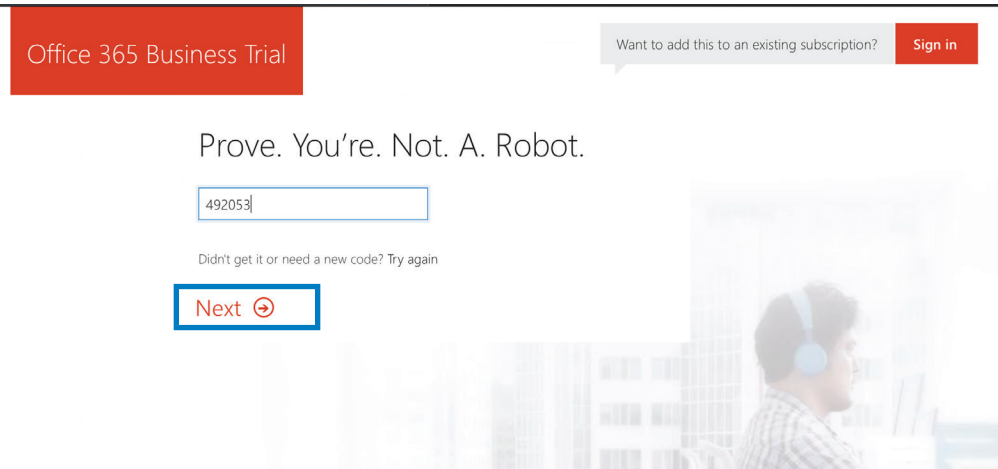
- 6. Create your first account as shown below.
- 7. Click "Create my account" when done.



- 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.



- 11. Enter the verification code Microsoft has given you, then click 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 Business Trial

Save this info. You'll need it later.

Sign-in page

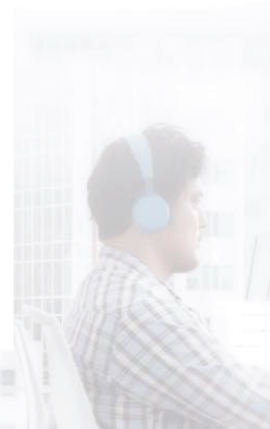
<https://portal.office.com/>

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.



Pick an account

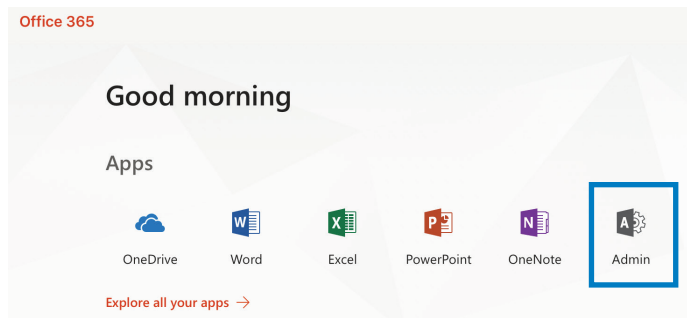


nmcdonald@hcs.jamfy.tech

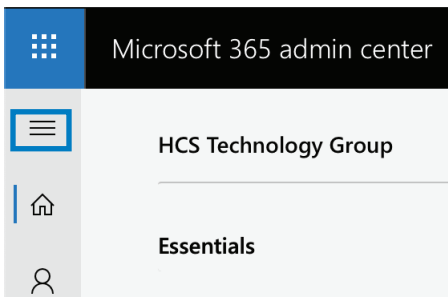


Use another account

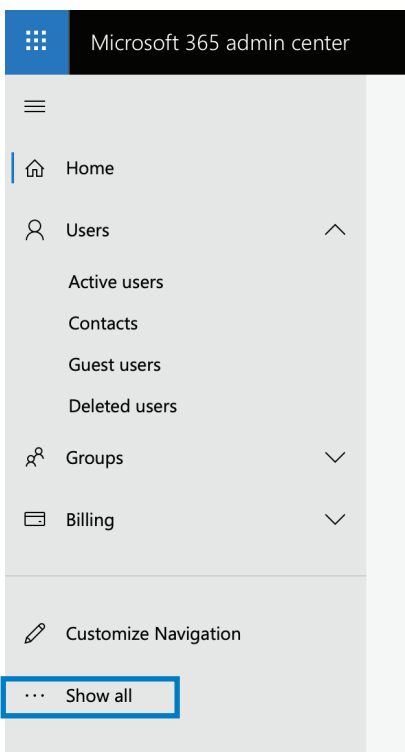
16. If you see a hints window, read or close the hints.
17. Click Admin.



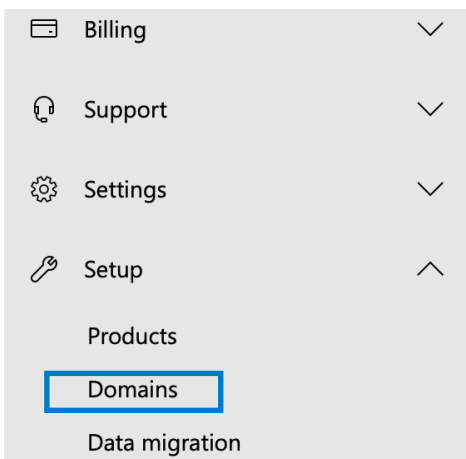
18. If necessary, in the sidebar, click the three lines to reveal a menu.



19. Click "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	Status
hcsonlineaddemo.onmicrosoft.com (Default)	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 [Close]

Add a domain • Verify domain • Set up your online servic... • Update DNS settings

Add a domain

Enter a domain you own.

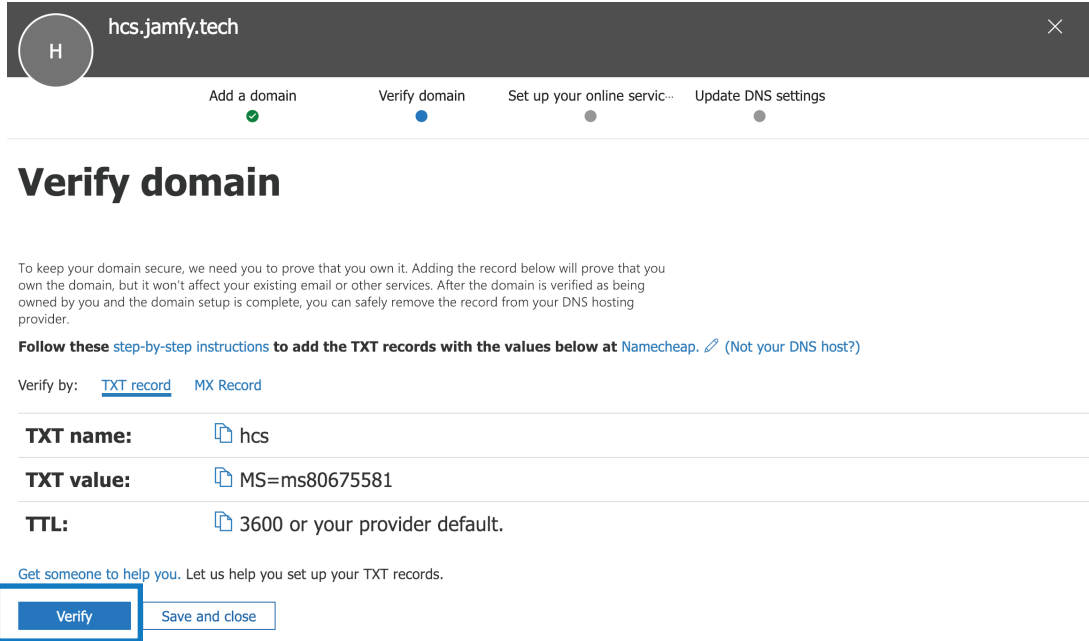
Your users' email addresses will look like this: username@hcs.jamfy.tech

Next Close

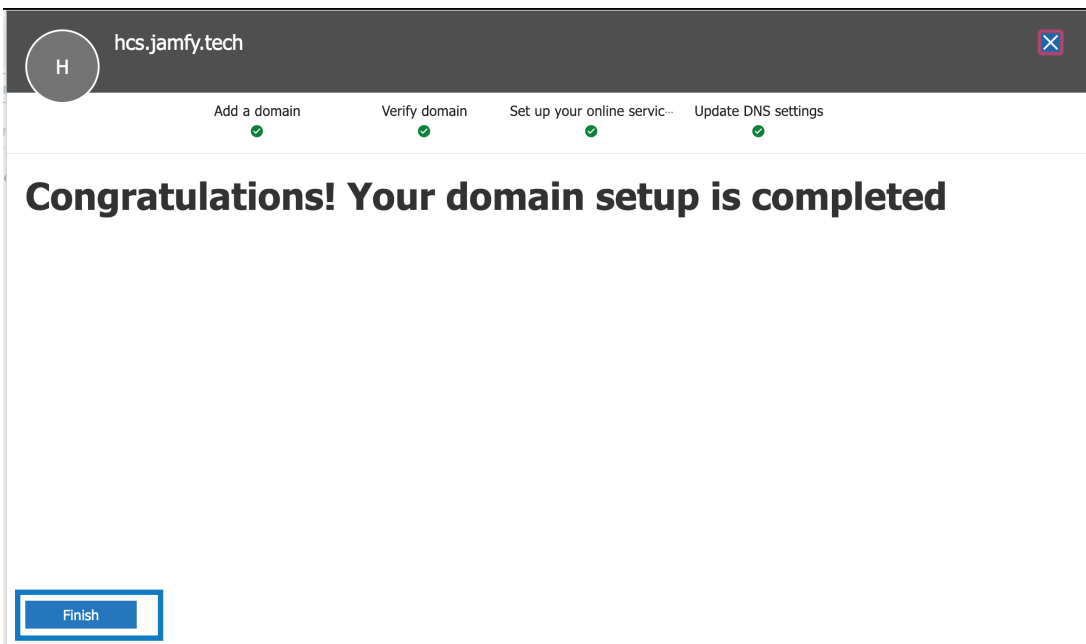
22. In the “Verify domain” window, add the requested DNS entries to your domain’s DNS provider. This process can vary between providers; contact your domain registrar or DNS provider for more information if necessary. After your DNS provider makes the required entries available on the Internet, click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

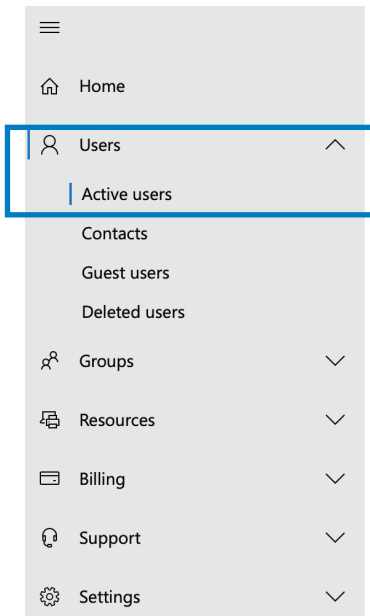


24. In the domain setup completion window, click Finish.





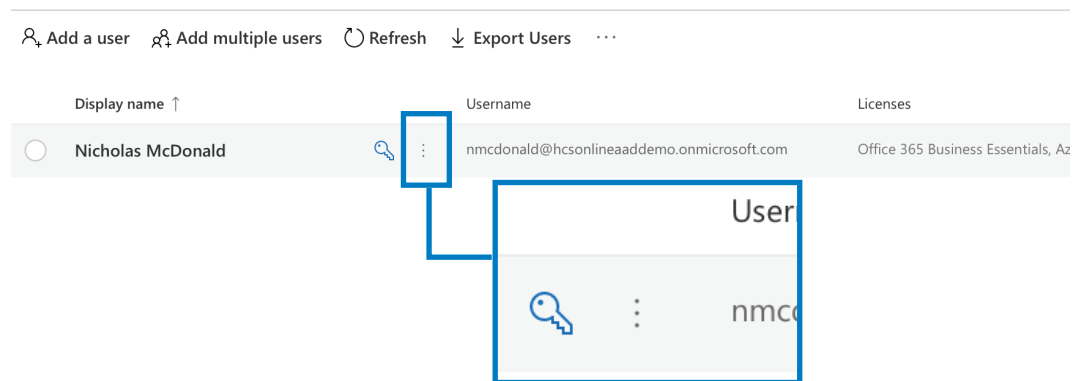
25. In the sidebar, click Users, then click Active Users.



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

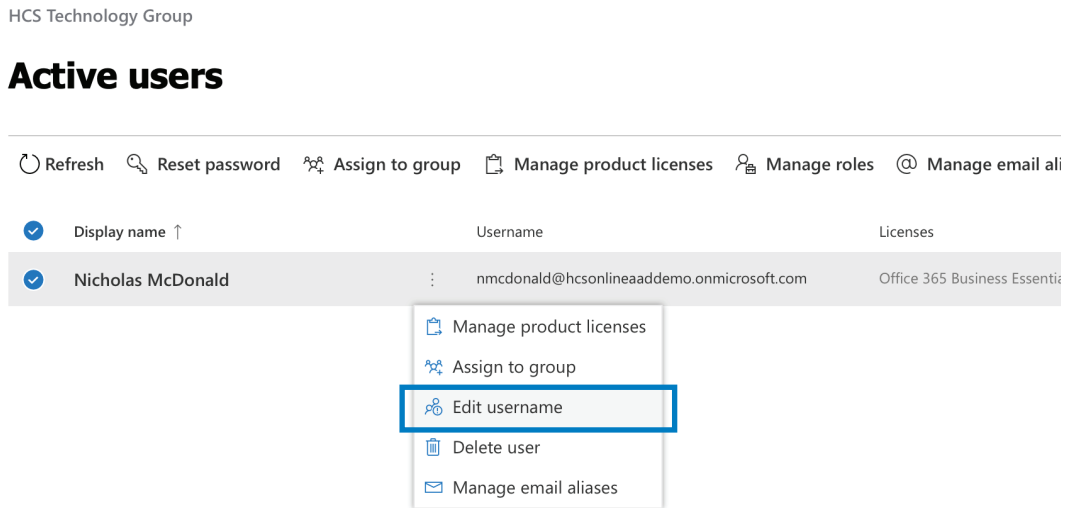
HCS Technology Group

Active users

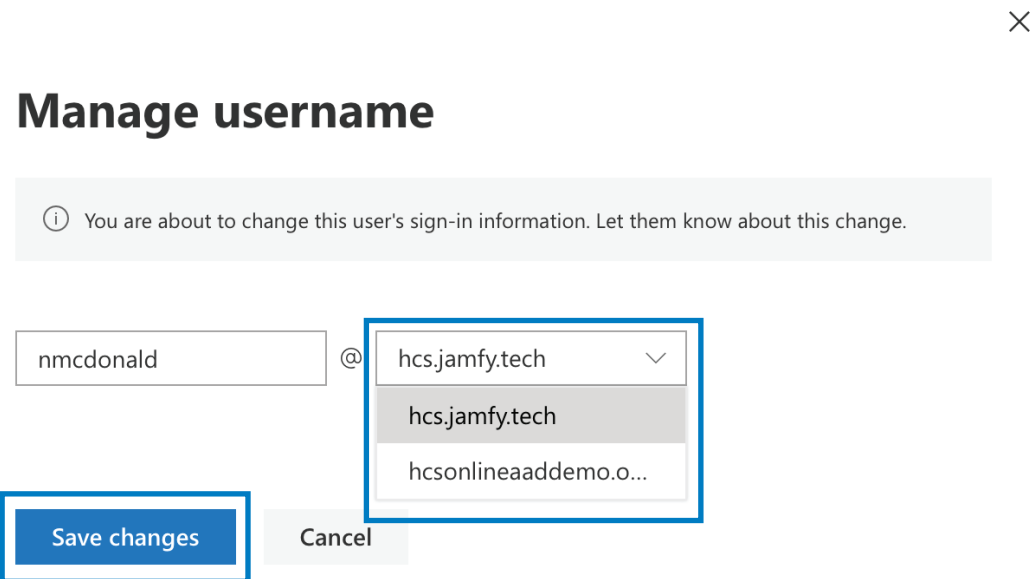


The three dots are located between the key icon and your username

27. In the options menu, choose “Edit username.”



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.

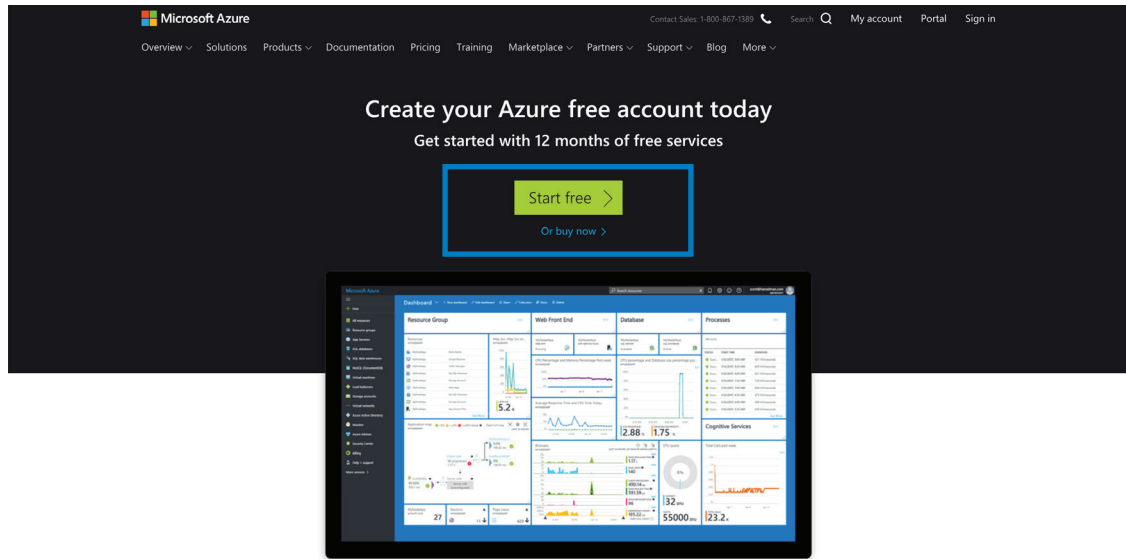




Section 2: Create an Azure Account

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 sign up.
2. Open <https://azure.microsoft.com/en-us/free/>.



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

Microsoft Azure nmcdonald@hconlineademo.onmicrosoft.com Sign out

Azure free account sign up
Start with a \$200 credit for 30 days, and keep going for free

1 About you ^

Country/Region ⓘ

First name

Last name

Email address ⓘ

Phone

By proceeding you acknowledge the [privacy statement](#) and [subscription agreement](#)

- 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

Phone number

- 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.

3 Identity verification by card ^

Why is credit card information necessary for a free account?

- To keep out spam and bots
- To verify your identity

You won't be charged unless you upgrade.



Card number

Expiration date CVV ⓘ

Name on card

Address line 1

Address line 2

City

State ZIP code

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

4 Agreement ^

I agree to the [subscription agreement](#), [offer details](#), and [privacy statement](#)

I will receive information, tips, and offers from Microsoft or selected partners about Azure, including Azure Newsletter, Pricing updates, and other Microsoft products and services.

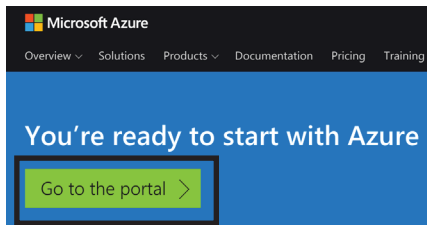


Section 3: Configure Azure Active Directory Domain Services

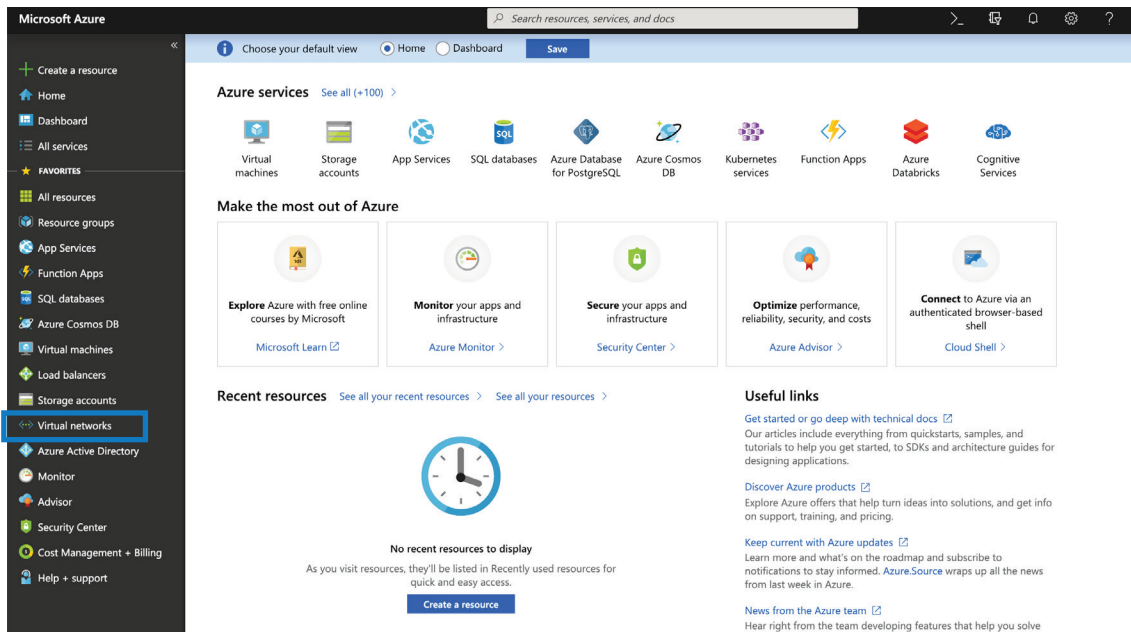
If AADDS is already active on your Azure account skip to step 7. Note: AADDS is a paid service within Azure, see <https://azure.microsoft.com/en-us/pricing/details/active-directory-ds/> for pricing information.

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.

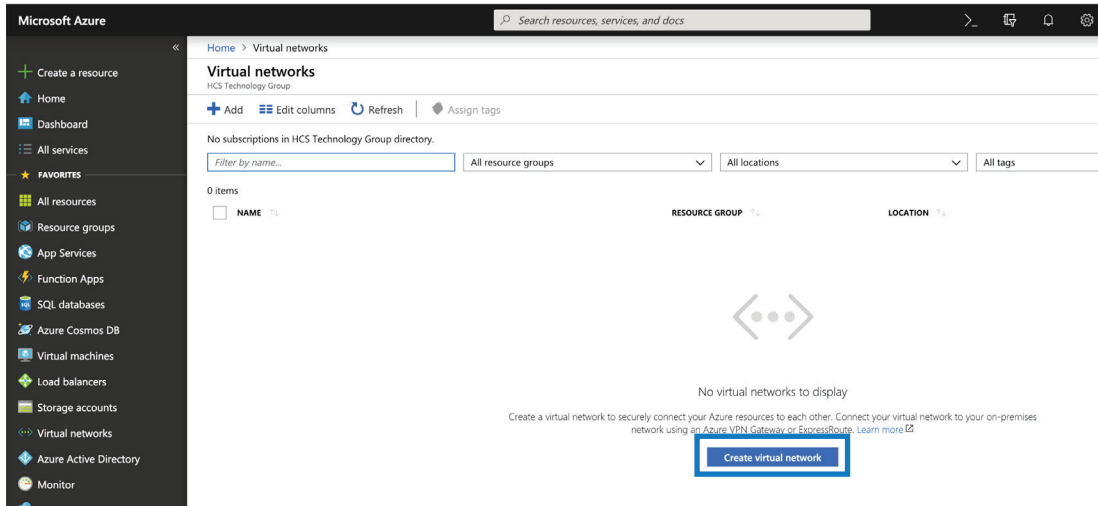
1. Navigate to the Azure Portal (<https://portal.azure.com/>) and sign in if requested. You may see “You’re ready to start with Azure” if this is your first time logging in. Click “Go to the portal.”



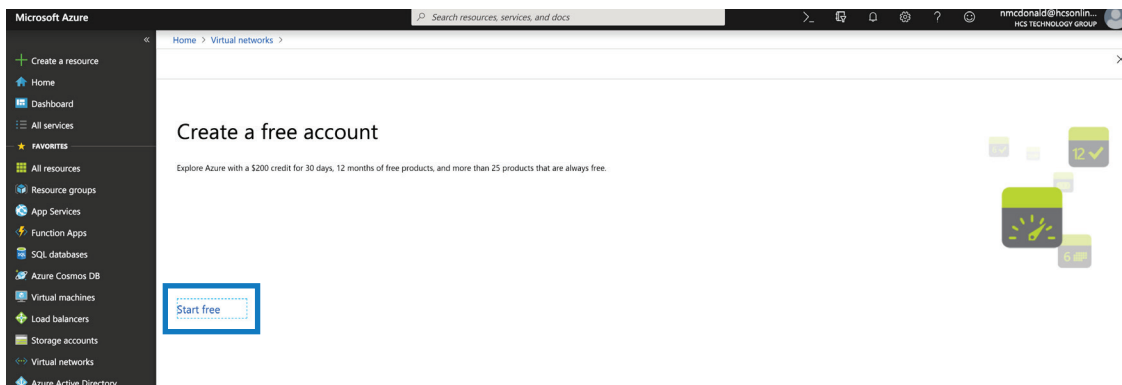
2. If you see the “Welcome to Microsoft Azure” dialog, click “Maybe later.”
3. If your organization already has a virtual network configured skip to step 9. A virtual network is required for AADDS to function.
4. From the sidebar, click “Virtual Networks.”



5. Click “Create virtual network.”



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.





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 addresses)

* Subscription
Free Trial ▾

* Resource group
(New) HCSnet ▾
[Create new](#)

* Location
West US ▾

Subnet

* Name
HCSnetSubnet1 ✓

* Address range ⓘ
10.1.0.0/24 ✓
10.1.0.0 - 10.1.0.255 (256 addresses)

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.

* Resource group
Select existing... ▾
[Create new](#)

A resource group is a container that holds related resources for an Azure solution.

* Name
HCSnet ✓

OK Cancel

Basic Standard

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).

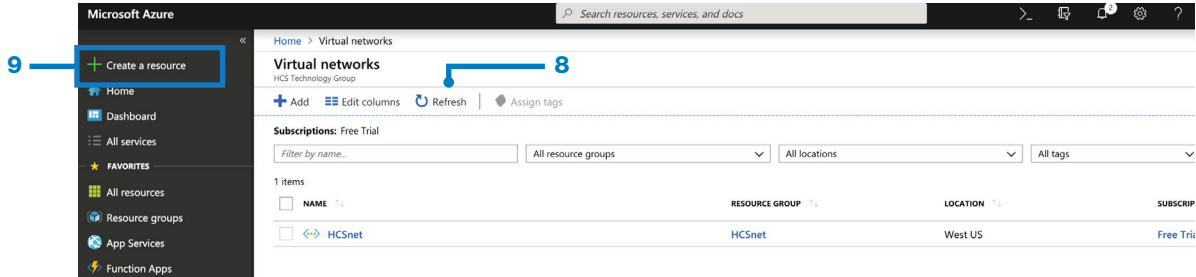
DDoS protection ⓘ
 Basic Standard

Service endpoints ⓘ
 Disabled Enabled

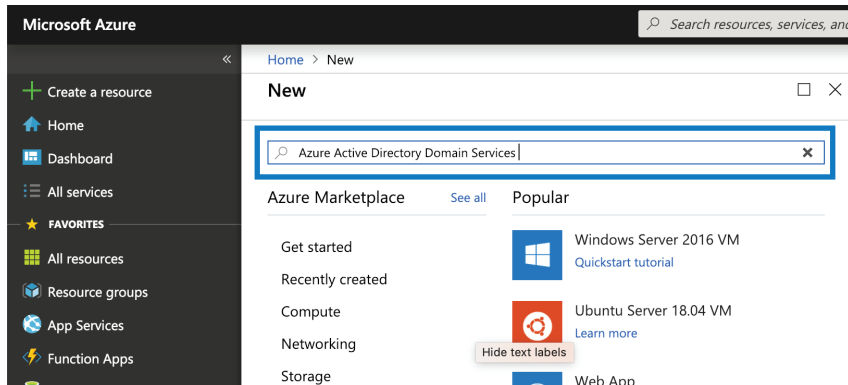
Firewall ⓘ
 Disabled Enabled

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

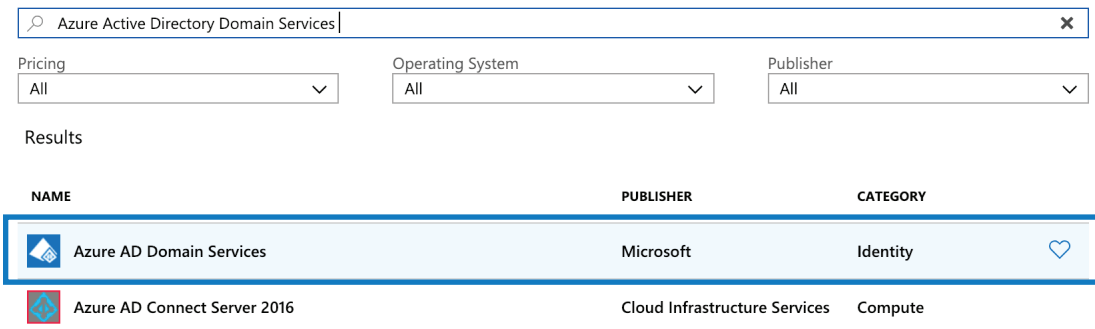
8. You should be brought back to the “Virtual networks” page. If your new virtual network is not yet listed, wait a moment, then click Refresh.
9. In the sidebar, click “Create a resource” to configure AADDS..



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



11. Select “Azure AD Domain Services” from the search results.





12. In the new panel click Create.

Azure AD Domain Services Microsoft

Azure Active Directory Domain Services lets you join Azure virtual machines to a domain without the need to deploy or manage domain controllers. Users sign in to these virtual machines using their corporate Active Directory credentials and can access resources seamlessly. Azure Active Directory Domain Services features domain join, LDAP, NTLM and Kerberos authentication are widely used in enterprises. Migrate legacy directory-aware applications running on premises to Azure without having to worry about identity requirements.

[Save for later](#)

PUBLISHER	Microsoft
USEFUL LINKS	Service overview Documentation Pricing

Create

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.

Basics

Directory name: HCS Technology Group **A**

* DNS domain name: hcs.jamfy.tech **B**

* Subscription: Free Trial **C**

* Resource group: HCSnet **D**

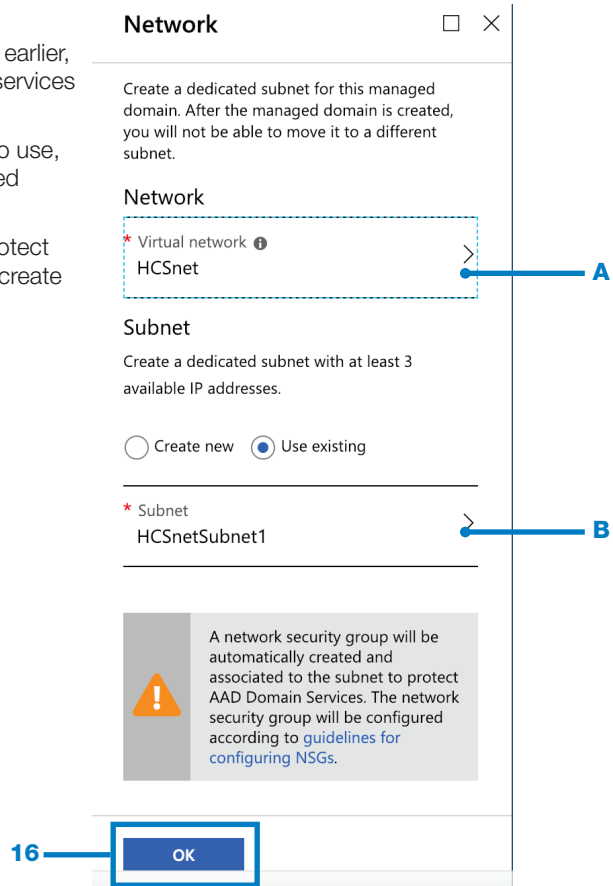
* Location: West US **E**

14. Confirm your settings then Click OK.

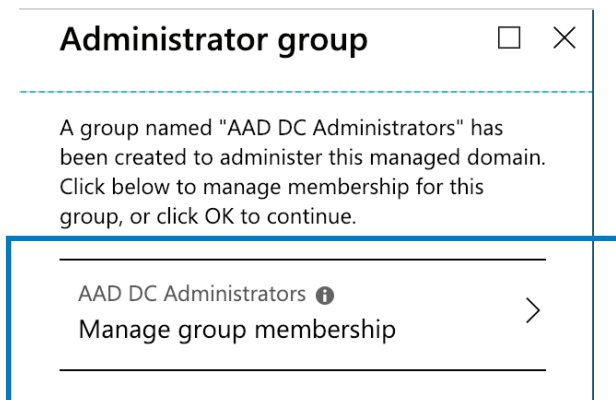
14 **OK**

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.



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.”





18. In the Members page, click “Add members.”

Home > New > Marketplace > Everything > Azure AD Domain Services > Enable Azure AD Domain Services > Administrator group > Members

Members

+ Add members Refresh

NAME	TYPE
No members have been 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.

Add members X

Select member or invite an external user ⓘ

nicholas mcdonald ✓

NM Nicholas McDonald
nmcdonald@hconlineaaddemo.onmicrosoft.com

Selected members:

NM Nicholas McDonald
nmcdonald@hconlineaaddemo.onmicrosoft... Remove

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.

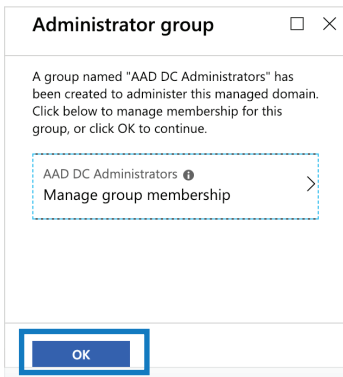
Home > New > Marketplace > Everything > Azure AD Domain Services > Enable Azure AD Domain Services > Administrator group > Members

Members

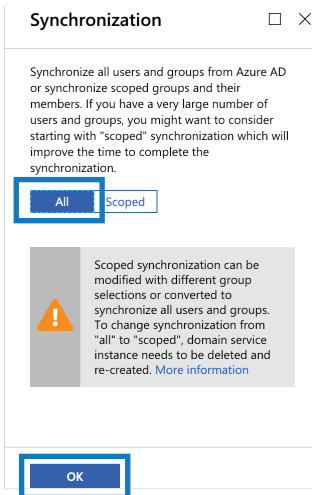
+ Add members Refresh

NAME	TYPE
NM Nicholas McDonald	User

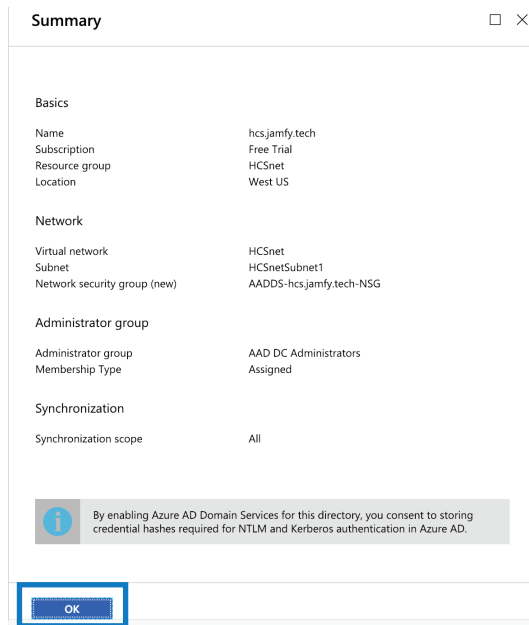
21. Click OK at the bottom of the “Administrator group” pane.



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

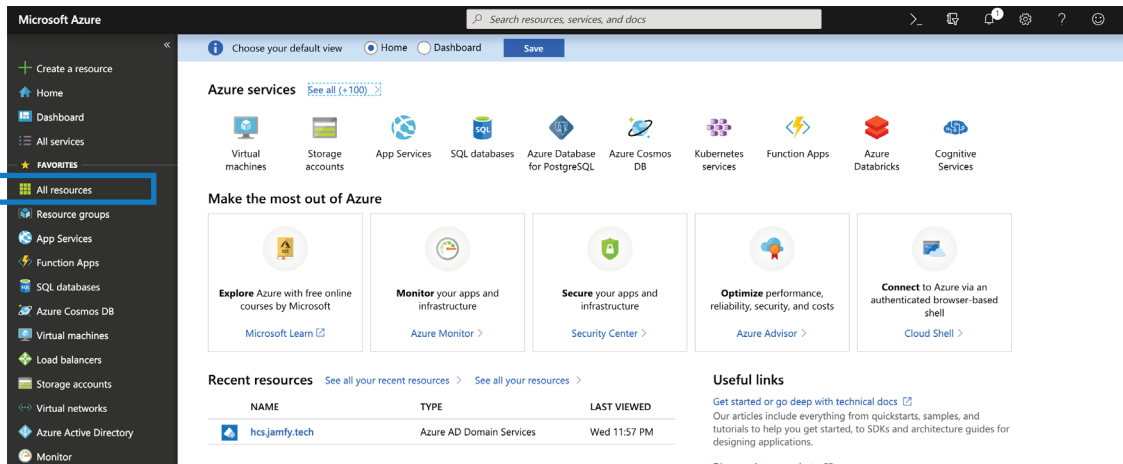


23. In the Summary screen, confirm your details, then click OK.

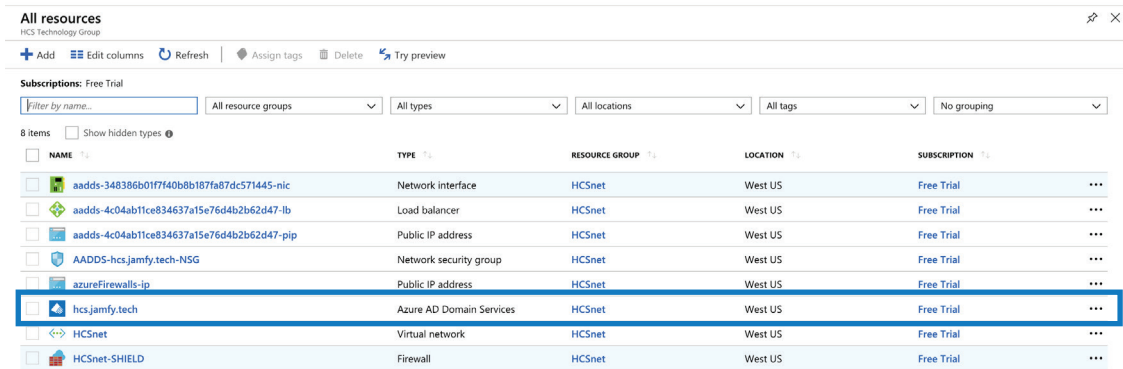




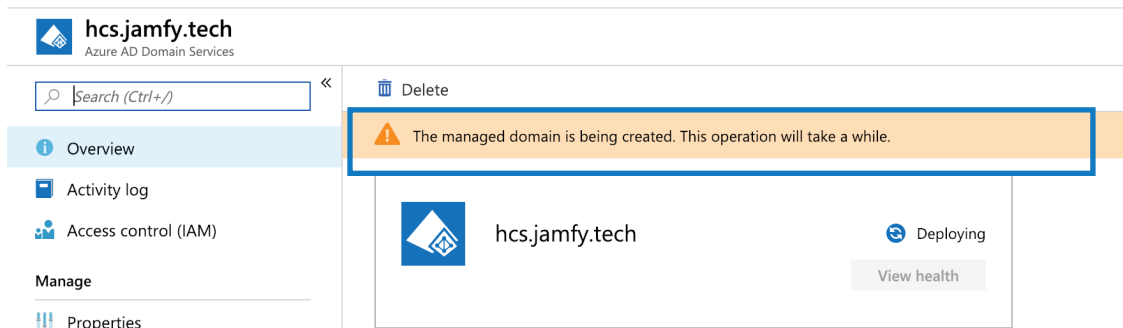
24. Confirm that your browser displays your Azure home page. In the sidebar, click “All resources.”



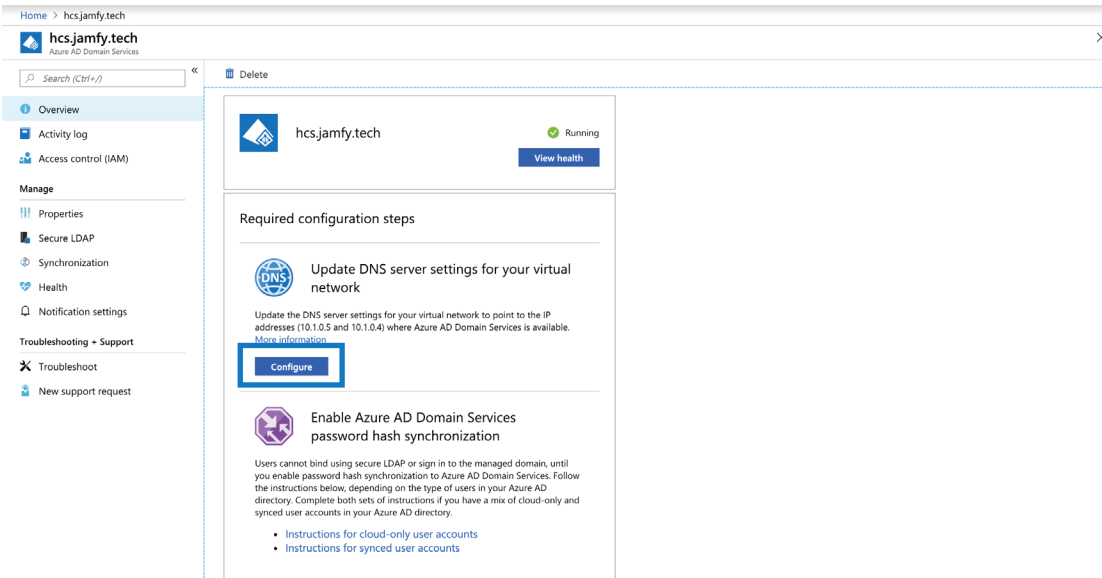
25. Click the hostname for your AADDS resource.



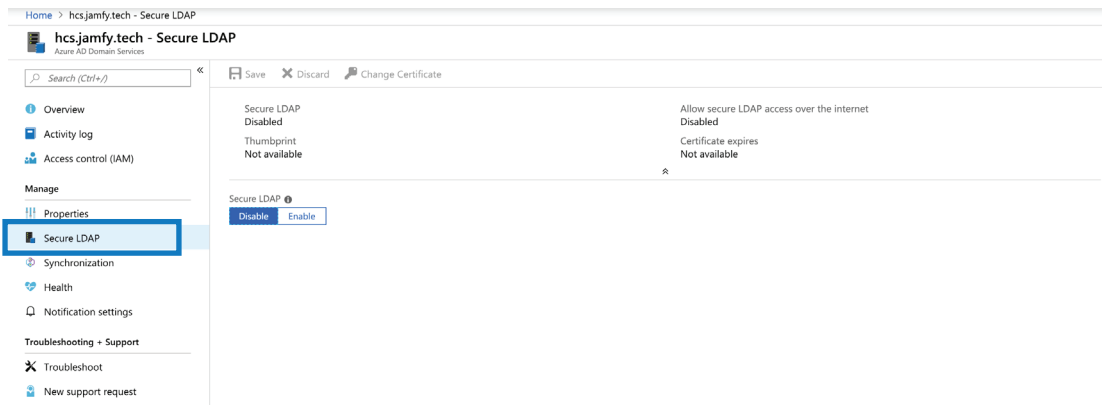
26. In the following page, if you see “The managed domain is being created. This operation will take a while,” this may take up to 1 hour to provision. Wait and refresh the page later.



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

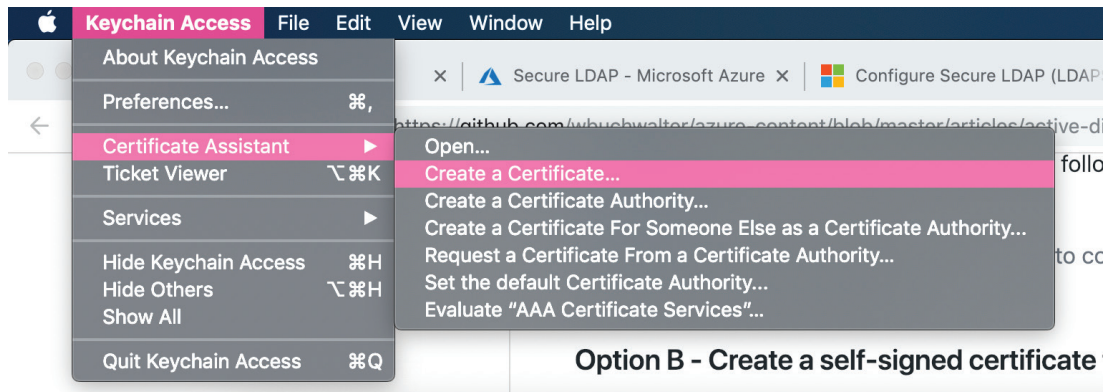


28. In the sidebar for the AADDS you just configured, click Secure LDAP and leave this window open. You will configure LDAPS to use a self-signed certificate.

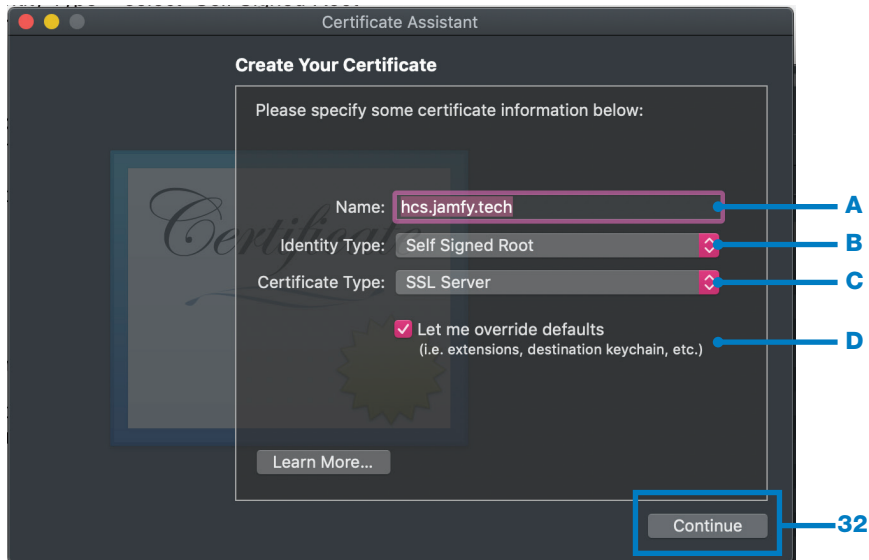




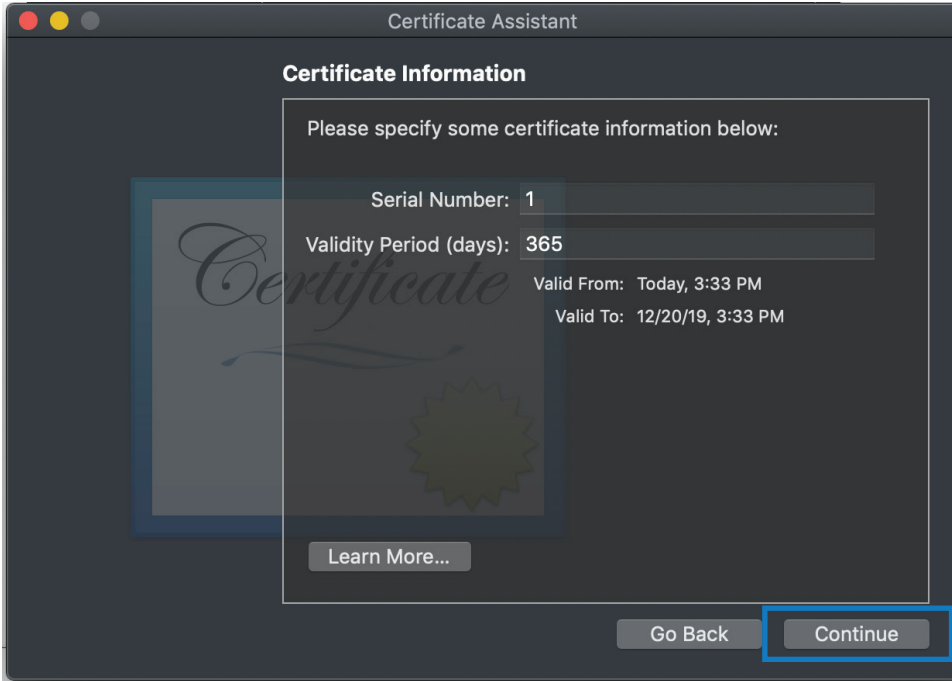
29. On your Mac, use Spotlight to open Keychain Access (or you can use Finder to open Applications>Utilities>Keychain Access). If you don't have a Mac, use the following steps:
 - A. If you don't have a Mac, create a certificate by using "Option B" in the following document: <https://docs.microsoft.com/en-us/azure/active-directory-domain-services/active-directory-ds-admin-guide-configure-secure-ldap>
 - 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-admin-guide-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.



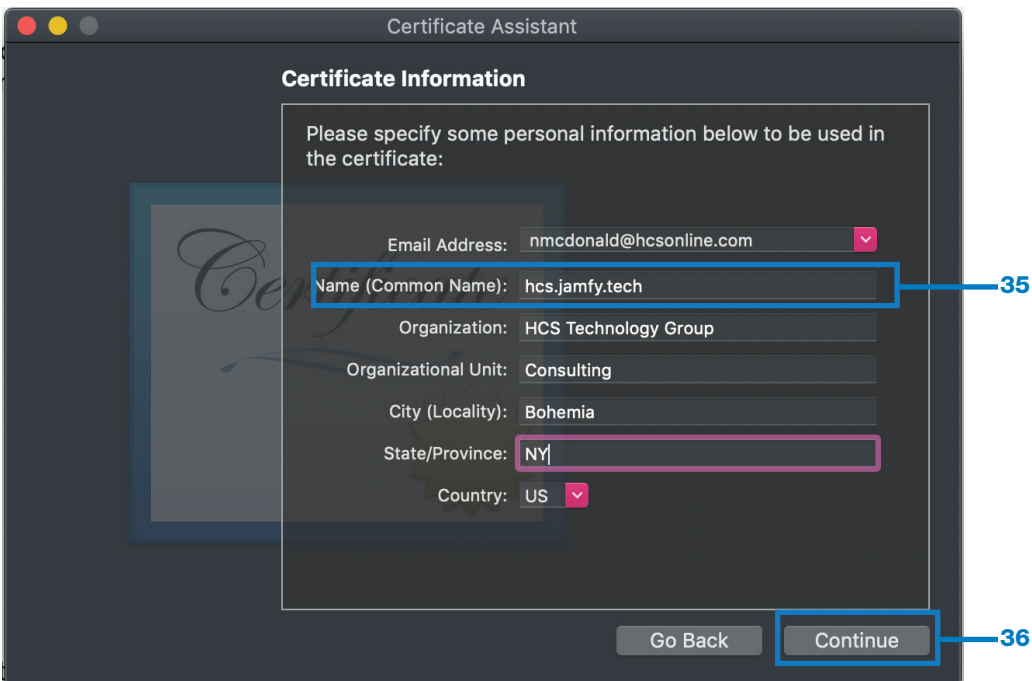
31. In the Certificate Assistant window, enter your details as follows.
 - A. Name - enter the DNS Name you selected in step 13-B.
 - B. Identity Type - choose Self Signed Root.
 - C. Certificate Type - choose SSL Server.
 - D. Select the option "Let me override defaults."
32. Confirm your settings then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



- 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.

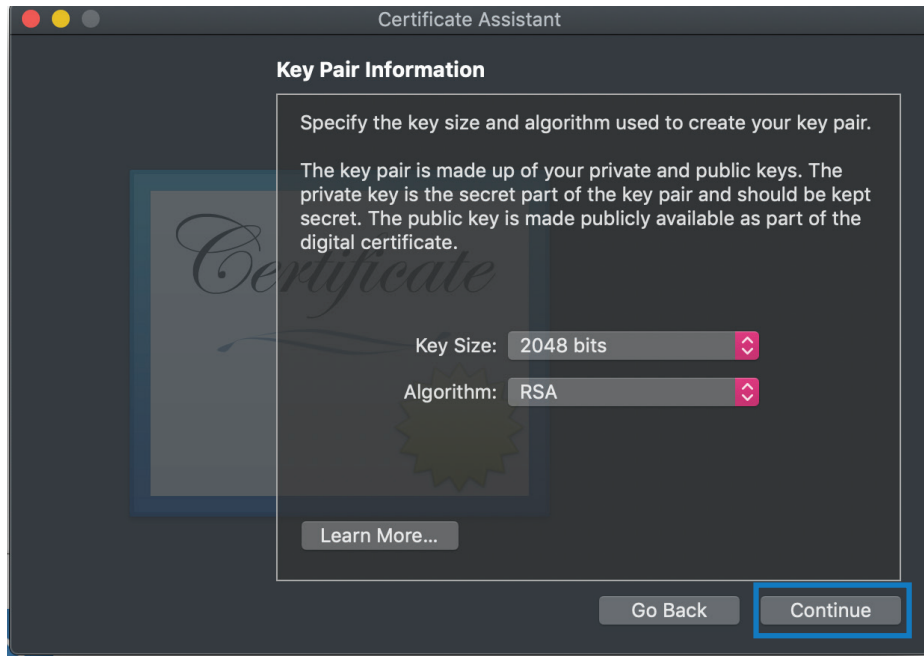


- 35. In the following screen, enter your organizational details. In the Name (Common Name) field enter the FQDN you selected in step 13-B.
- 36. Confirm your settings then click Continue.

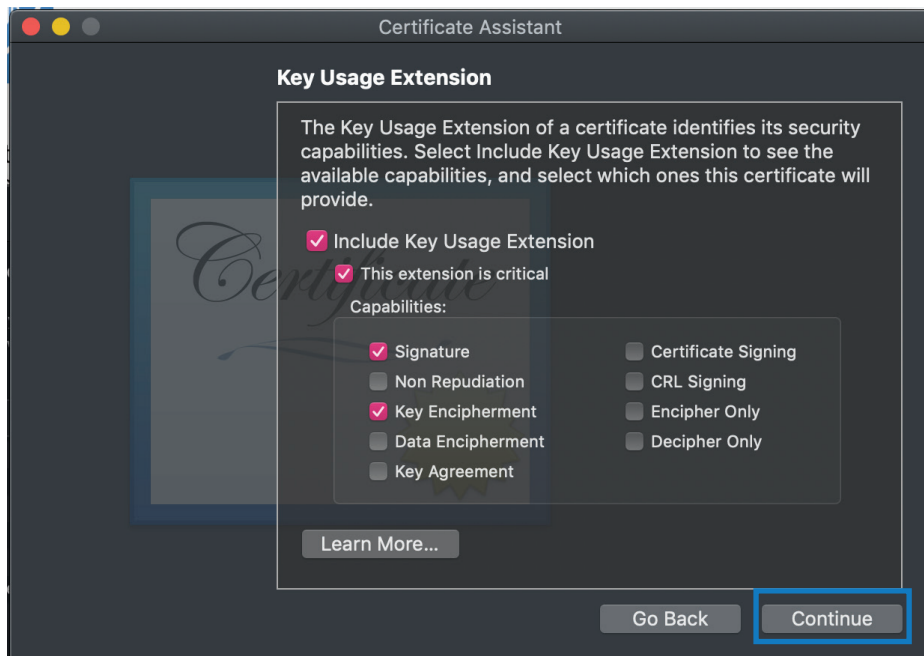




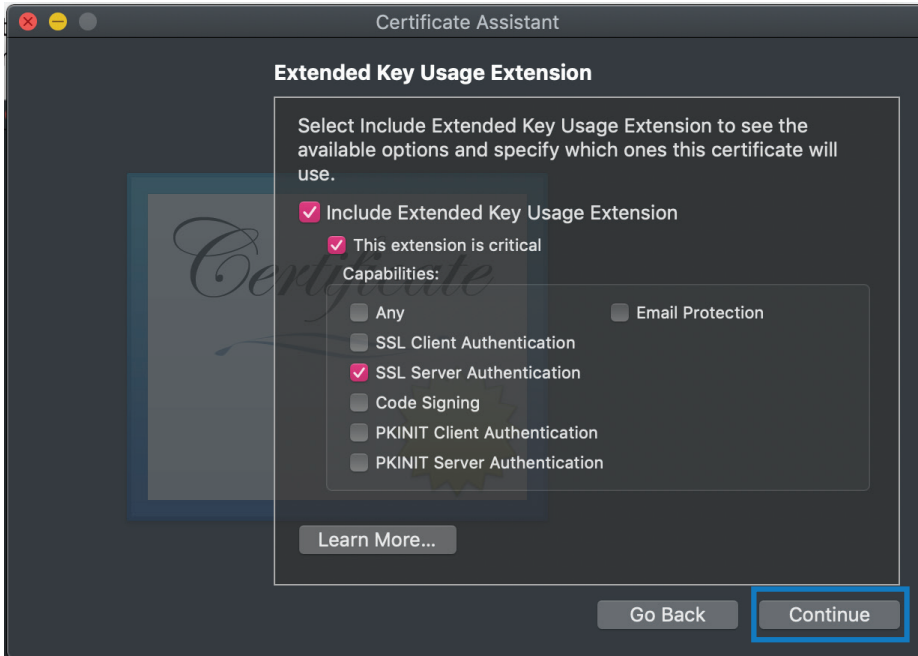
37. Leave the Key Pair Information at the default options then click



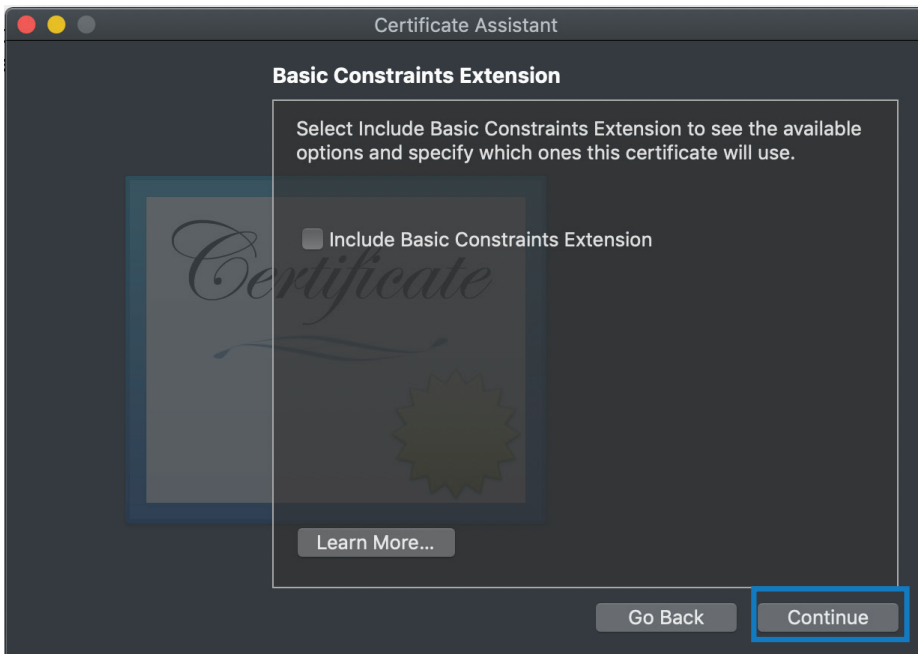
38. Leave the Key Usage Extension at the default options, then click Continue.



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

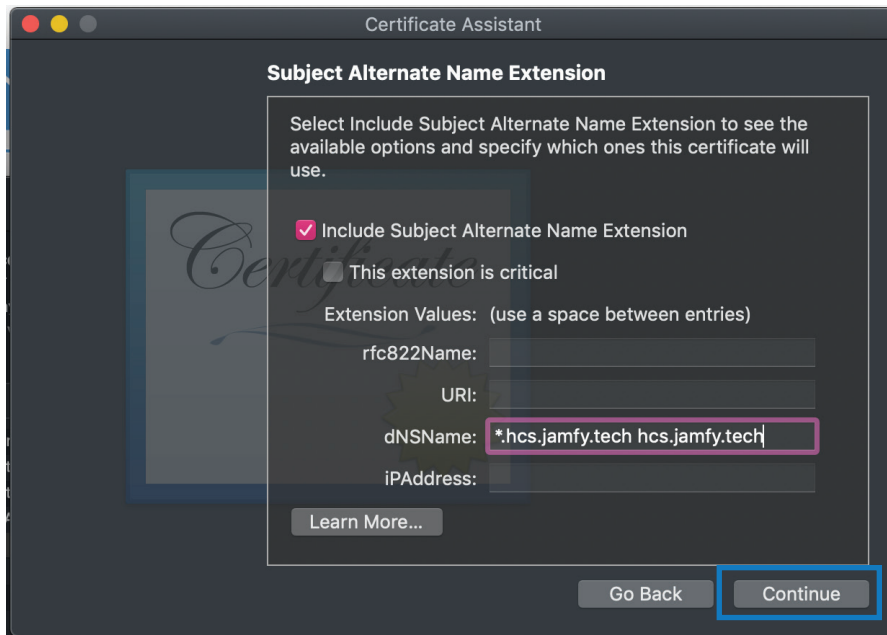


40. Leave the checkbox deselected for the Include Basic Constraints Extension option then click Continue.

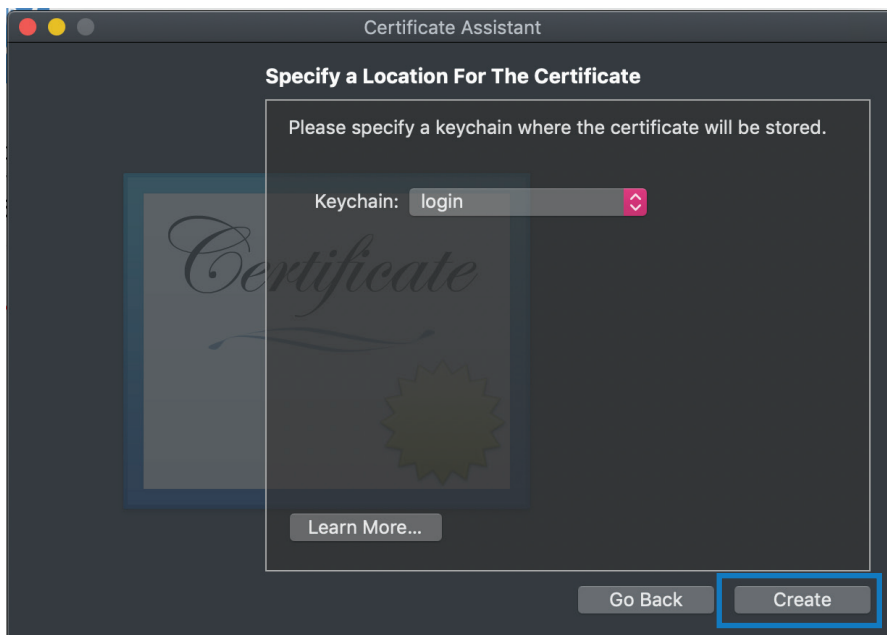




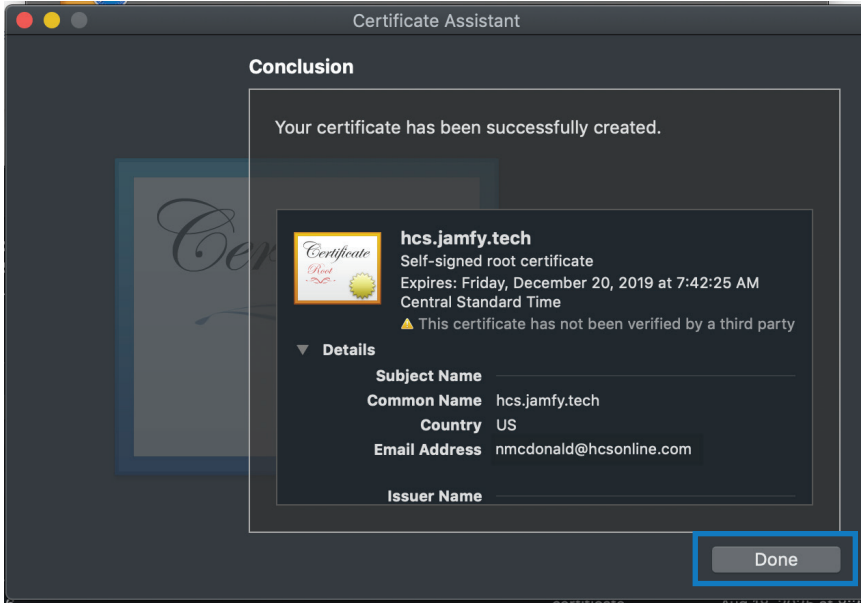
41. Configure the Subject Alternative Name Extension options as follows.
 - “dNSName:” - Enter an asterisk followed by your FQDN from step 13-B, then enter a Space character, then enter the FQDN from step 13-B (you must have a space between the two entries. For example, if your FQDN was aad.contoso.com, then enter *.aad.contoso.com aad.contoso.com.
 - “iPAddress:” - Clear all data from this field.
42. Confirm your settings then click Continue.



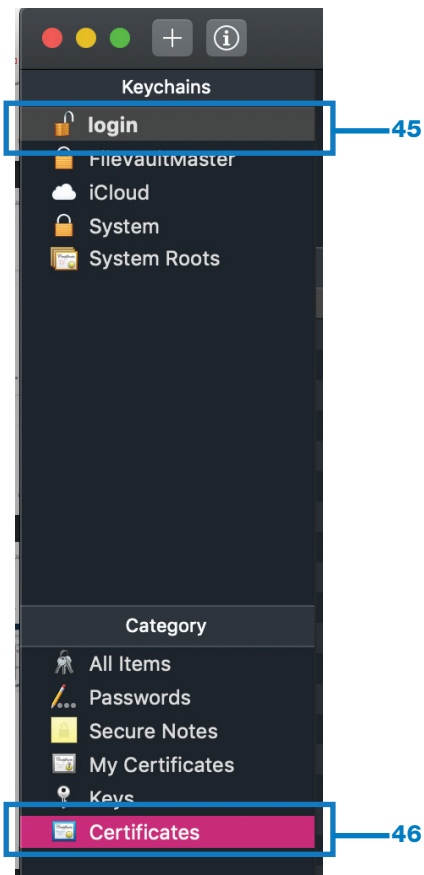
43. In the “Specify a Location For The Certificate” screen, leave the default as “login” and click Create.



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.

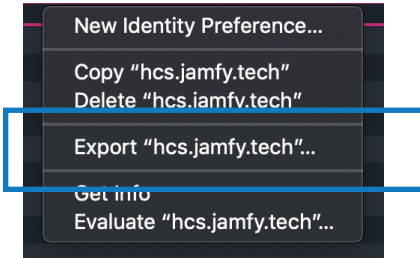




47. In the Certificates category, look for the certificate labeled with your FQDN from step 13-B.



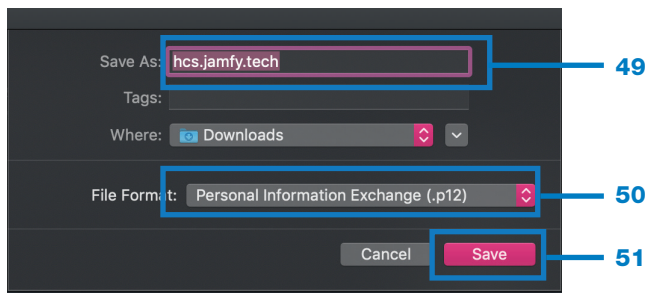
48. Right click your certificate then choose Export "your FQDN".



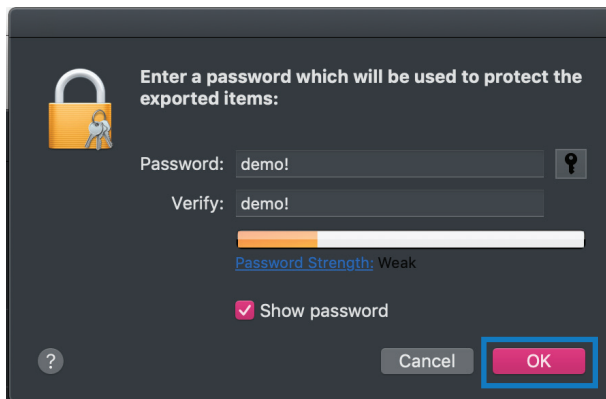
49. In the Save As field, enter something memorable, such as your FQDN.

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.

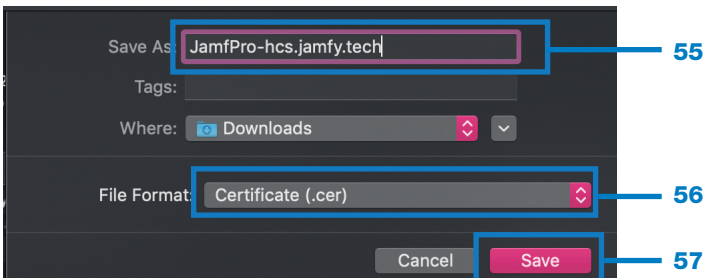


54. You will export the certificate again, this time with a different format. Right-click your certificate then choose Export "your FQDN".

55. In the Save As field, enter the same name you used in step 49, such as your FQDN.

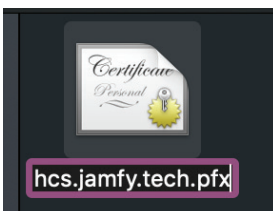
56. Click File Format and choose "Certificate (.cer)".

57. Click Save.

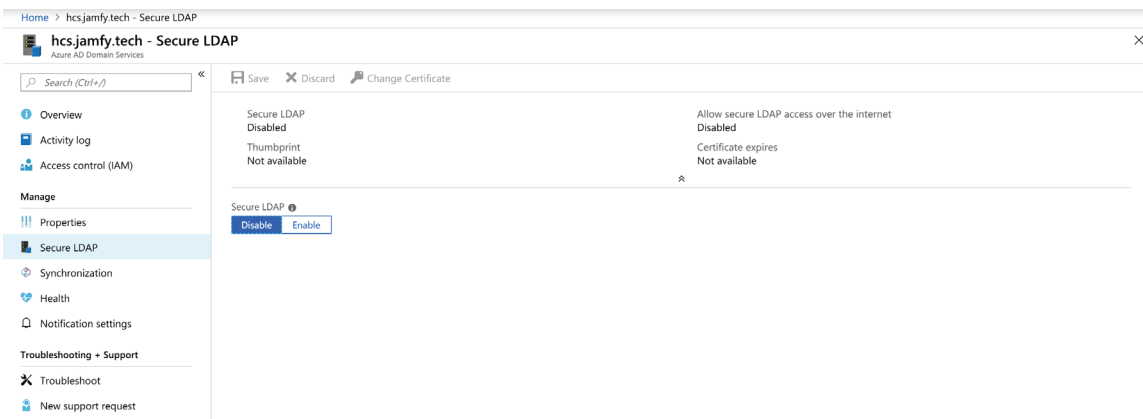


58. In the Finder, select the certificate you exported as a p12 file, then press Return to edit its name.

59. In the file name field, replace the extension .p12 with .pfx, then 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.





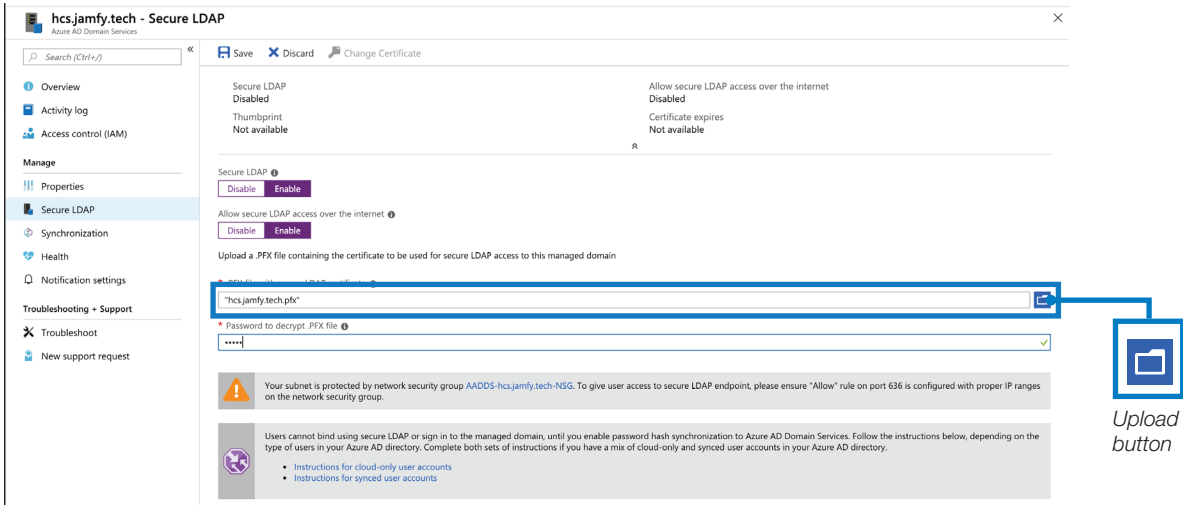
61. Near the Secure LDAP field, click Enable.

The screenshot shows the 'Secure LDAP' configuration page for 'hcs.jamfy.tech'. On the left, a navigation pane includes 'Overview', 'Activity log', 'Access control (IAM)', 'Properties', 'Secure LDAP', and 'Synchronization'. The main content area shows 'Secure LDAP' as 'Disabled' with a 'Thumbprint' of 'Not available'. To the right, 'Allow secure LDAP access over the internet' is also 'Disabled' with a 'Certificate expires' of 'Not available'. At the bottom, there are 'Disable' and 'Enable' buttons for the 'Secure LDAP' toggle, with the 'Enable' button highlighted by a blue box.

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

This screenshot shows the same 'Secure LDAP' configuration page. The 'Secure LDAP' toggle is now 'Enabled'. The 'Allow secure LDAP access over the internet' toggle is also 'Enabled' and highlighted with a blue box. Below the toggles, there are fields for uploading a '.PFX file containing the certificate' and a 'Password to decrypt .PFX file'. At the bottom, there are two informational messages: one about network security group settings and another about password hash synchronization requirements.

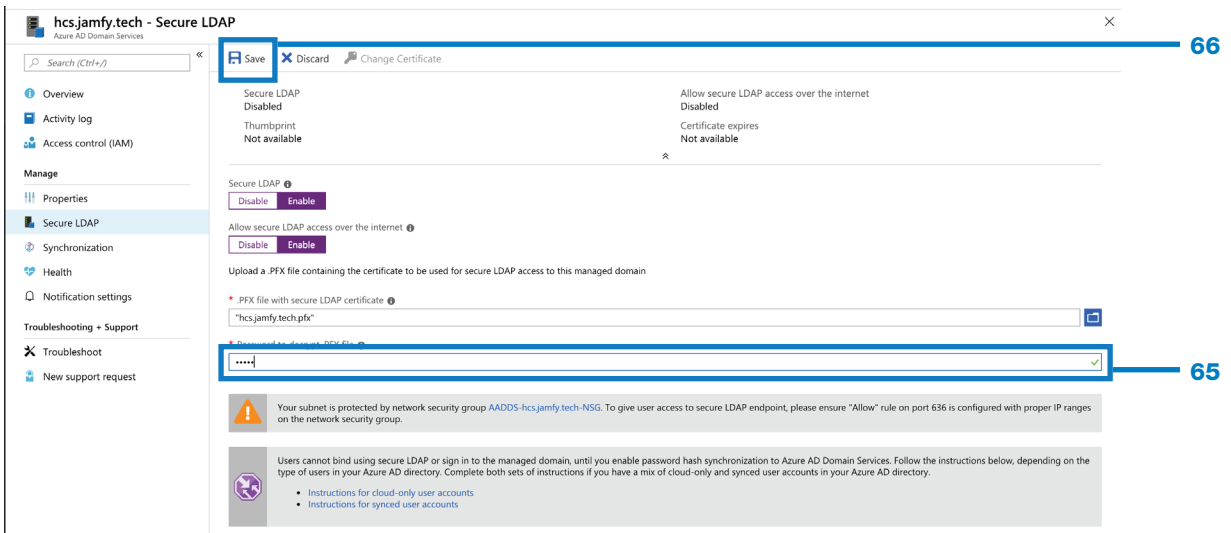
63. Next to the “.PFX file with secure LDAP certificate” field, click the Upload button (looks like a folder).



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.





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 LDAP

Search (Ctrl+F)

Save Discard Change Certificate

Configuring secure LDAP for the directory. This operation may take a while.

Essentials

Secure LDAP **Disable** Enable

Allow secure LDAP access over the internet **Disable** Enable

Upload a PFX file containing the certificate to be used for secure LDAP access to this managed domain

* PFX file with secure LDAP certificate

"hcs.jamfy.tech.pfx"

* Password to decrypt PFX file

Your subnet is protected by network security group AADD5-hcs.jamfy.tech-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.

- 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.

Home > hcs.jamfy.tech - Secure LDAP

hcs.jamfy.tech - Secure LDAP

Search (Ctrl+F)

Save Discard Change Certificate

Secure LDAP **Enabled**

Allow secure LDAP access over the internet **Enabled**

Thumbprint: 7696F18F26B4F089CCAEB7F257CFA573A7511138

Certificate expires: Fri, 20 Dec 2019 22:18:51 GMT

Secure LDAP **Disable** Enable

Allow secure LDAP access over the internet **Disable** Enable

Your subnet is protected by network security group AADD5-hcs.jamfy.tech-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.

- Instructions for cloud-only user accounts
- Instructions for synced user accounts

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 LDAP

Search (Ctrl+F)

Save Discard Change Certificate

Secure LDAP **Enabled**

Allow secure LDAP access over the internet **Enabled**

Thumbprint: 7696F18F26B4F089CCAEB7F257CFA573A7511138

Certificate expires: Fri, 20 Dec 2019 22:18:51 GMT

Secure LDAP **Disable** Enable

Allow secure LDAP access over the internet **Disable** Enable

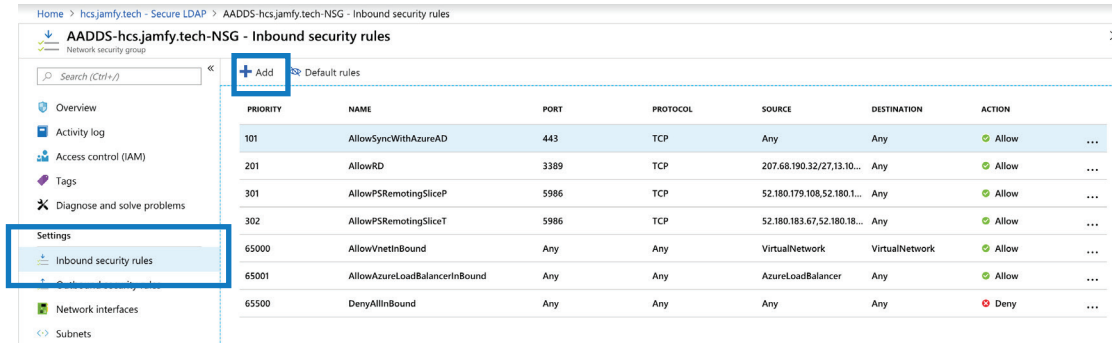
Your subnet is protected by network security group AADD5-hcs.jamfy.tech-NSG. To give user access to secure LDAP endpoint, please ensure "Allow" rule on port 636 is configured with proper IP ranges on the network security group.

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.

- Instructions for cloud-only user accounts
- Instructions for synced user accounts

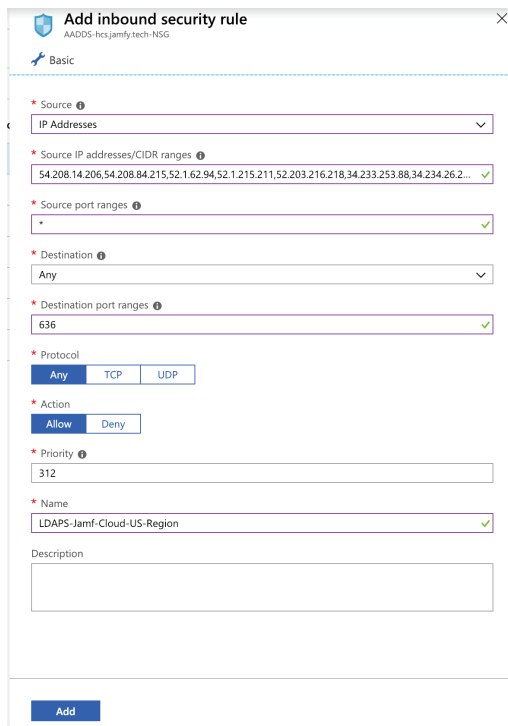
70. In the network security group screen, in the Settings column, click “Inbound security rules.”

71. Click Add to create a new firewall rule.



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.





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

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
101	AllowSyncWithAzureAD	443	TCP	Any	Any	Allow
201	AllowRD	3389	TCP	207.68.190.32/27.13.10...	Any	Allow
301	AllowPSRemotingSliceP	5986	TCP	52.180.179.108,52.180.1...	Any	Allow
302	AllowPSRemotingSliceT	5986	TCP	52.180.183.67,52.180.18...	Any	Allow
312	LDAP5-Jamf-Cloud-US-Region	636	Any	54.208.14.206,54.208.8...	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

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

Home > All resources > hcs.jamfy.tech - Secure LDAP > AADDs-hcs.jamfy.tech-NSG - Inbound security rules

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
101	AllowSyncWithAzureAD	443	TCP	Any	Any	Allow
201	AllowRD	3389	TCP	207.68.190.32/27.13.10...	Any	Allow
301	AllowPSRemotingSliceP	5986	TCP	52.180.179.108,52.180.1...	Any	Allow

75. In the sidebar, click Properties.

hcs.jamfy.tech - Secure LDAP

Secure LDAP Enabled

Thumbprint: 7696F18F26B4F089CCAEB7F257CFA573A7511138

Certificate expires: Fri, 20 Dec 2019 22:18:51 GMT

Secure LDAP:

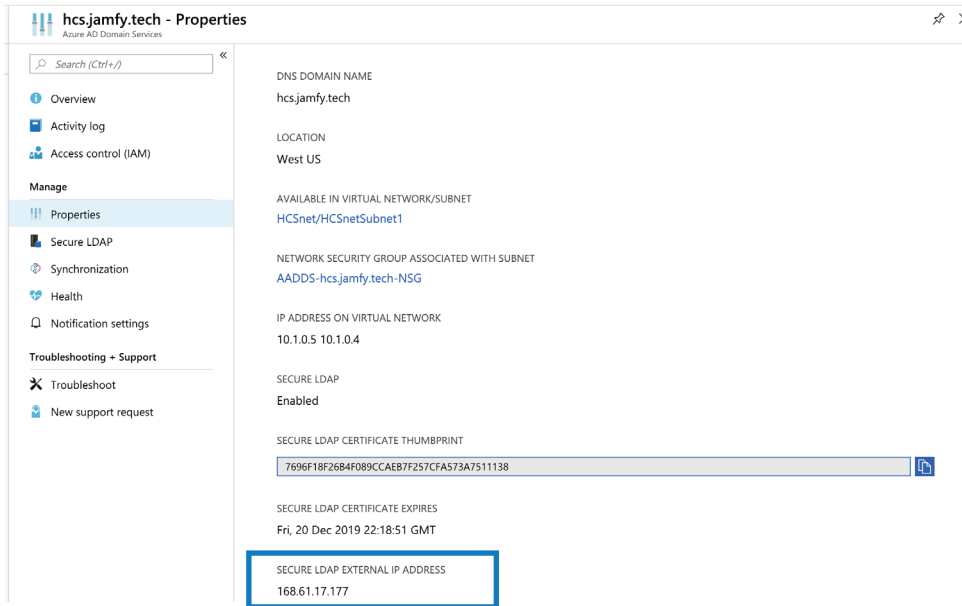
Allow secure LDAP access over the internet:

Your subnet is protected by network security group AADDs-hcs.jamfy.tech-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
- Instructions for synced user accounts

76. Make a note of the “Secure LDAP external IP address.”



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.



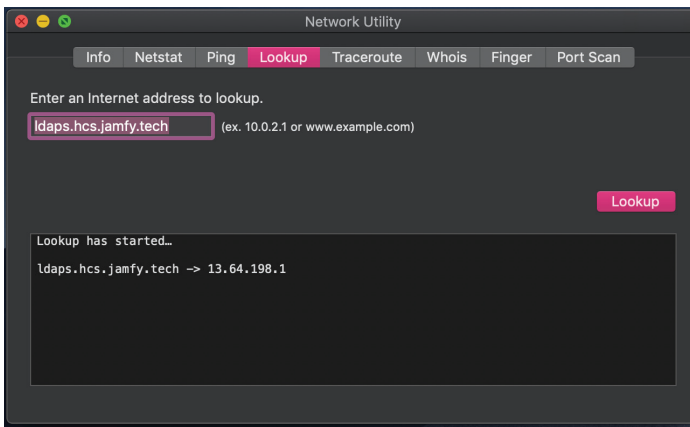
78. Use Spotlight to open Network Utility (it is located in /System/Library/CoreServices/Applications).

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.



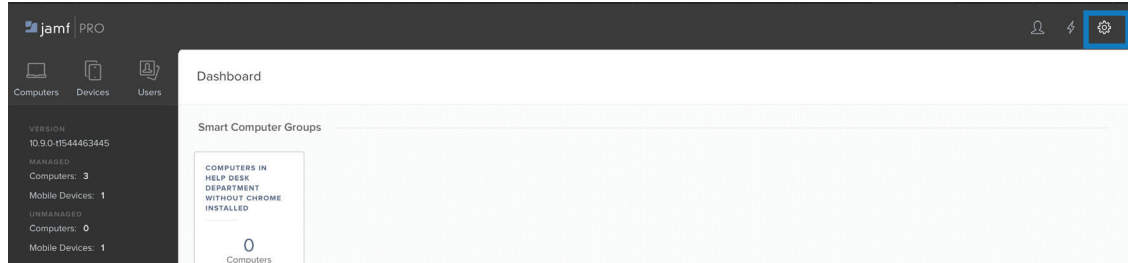
83. You have successfully configured Azure Active Directory Domain Services. You will use Jamf Pro in the next section to test the LDAPS service. Remember that the Azure firewall rule allows only LDAPS connections from the IP address or addresses you specified when you created the firewall rule.



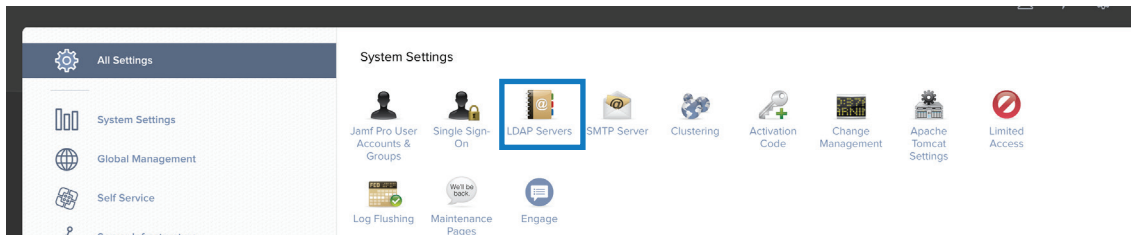
Section 4: Configure Jamf Pro for Azure AD Domain Services

This section covers connecting your AADDS Secure LDAP service to Jamf Pro

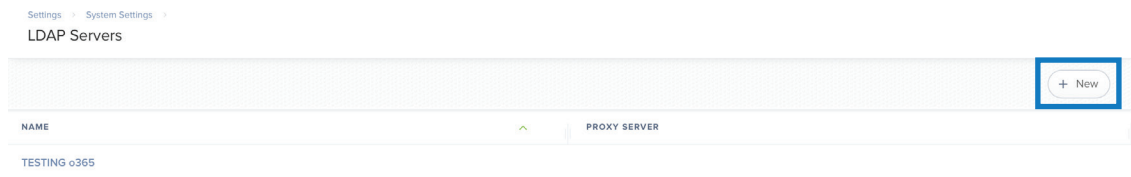
1. Log in to your Jamf Pro instance i.e. (<https://contoso.jamfcloud.com>)
2. In the upper-right corner, click Settings (looks like a gear).



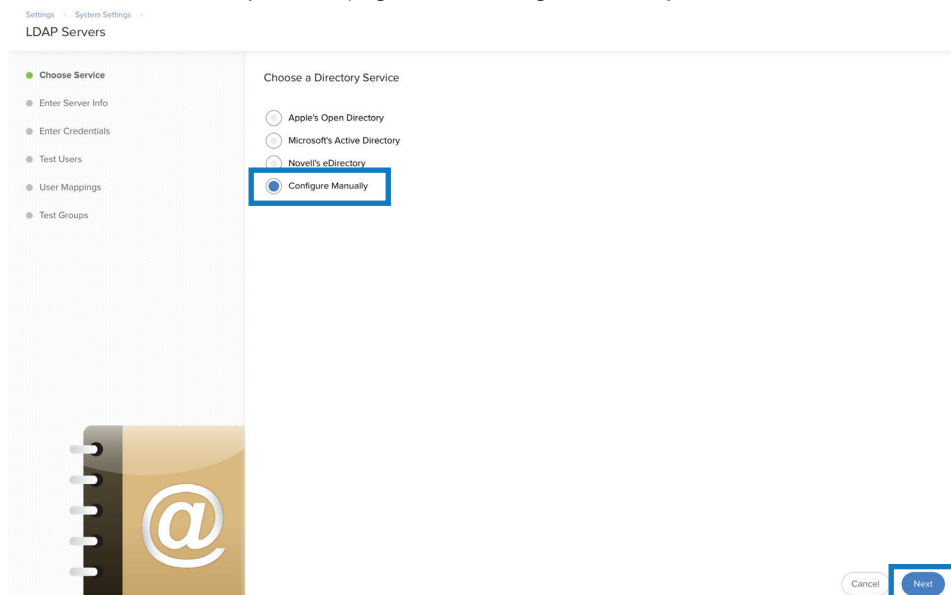
3. In the System Settings section, click LDAP Servers.



4. In the LDAP Servers page, click New.



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



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 ldaps.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.

Settings > System Settings > LDAP Servers > New LDAP Server

Connection Mappings

A **DISPLAY NAME** Display name for the LDAP server
Office 365

B **DIRECTORY SERVICE** Directory service to use for the LDAP server
Microsoft's Active Directory

C **SERVER AND PORT** Hostname or IP address, and port number of the LDAP server. Hostname is recommended if using SSL.
ldaps.hcs.jamfy.com 636

D **Enable LDAP Proxy Server** Configure LDAP proxy server settings to connect to the LDAP server.
PROXY SERVER: Select
PROXY BINDING ADDRESS AND PORT NUMBER:

E **Use SSL** Connect to the LDAP server over SSL. SSL must be enabled on the LDAP server for this to work.
JamfPro-hcs.jamfy.tech.cer

F **Upload Certificate**
Certificates to be shared across all LDAP connections.
Configuration Name: testing o365 Issuer: EMAILADDRESS=nmcdonald@hcsontline.com, L=Bohemia, C=US, ST=NY, OU=HCS Consulting *, O=HCS Technology Group *, CN=hcs.jamfy.tech

G **AUTHENTICATION TYPE** Type of authentication required to connect to the LDAP server
Simple

H **LDAP Server Account** Account to use to connect to the LDAP server. A service account is recommended
DISTINGUISHED USERNAME Distinguished name of the LDAP server account (e.g. "uid=authenticator,cn=users,dc=ods,dc=example,dc=com")
nmcdonald@hcs.jamfy.tech

I **PASSWORD**
.....
VERIFY PASSWORD
.....

J **CONNECTION TIMEOUT** Amount of time to wait before canceling an attempt to connect to the LDAP server
15 Seconds

K **SEARCH TIMEOUT** Amount of time to wait before canceling a search request sent to the LDAP server
60 Seconds

L **REFERRAL RESPONSE** Action to take when an LDAP server referral is received
Use default from LDAP service

M **Use Wildcards When Searching** Allow partial matches to be returned when searching the LDAP directory.
Use Wildcards When Searching



- 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.
- 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 Mappings

DISPLAY NAME Display name for the LDAP server
Office 365

- Click User Mappings.
- Configure the User Mappings settings as follows.
 - Object Class Limitation** Choose “All ObjectClass Values”
 - Object Class(es)** Enter “organizationalPerson, user”
 - Search Base** Enter your search base using this example “OU=AADDC Users, DC=contoso,DC=com”
 - Search Scope** Choose “All subtrees”
 - User ID** Enter “uSNCreated”
 - Username** Enter “userPrincipalName” or “mail”
 - Real Name** Enter “displayName”
 - Mail** Enter “mail”
 - Append to email results** - Leave blank unless needed
 - Department** Enter “department”
 - Building** Enter “streetAddress” (Or any other custom LDAP attribute)
 - Room** Enter “room”
 - Phone** Enter “mobile” (Or any other custom LDAP attribute)
 - Position** Enter “title”
 - User UUID** Leave “objectGUID”

User Mappings User Group Mappings User Group Membership Mappings

OBJECT CLASS LIMITATION Limitation to set for object classes in the Object Class field
A All ObjectClass Values

OBJECT CLASS(ES) Object class(es) to limit results to. Each object class must be separated by a comma
B organizationalPerson, user

SEARCH BASE Distinguished name of the search base
C OU=AADDC Users, DC=hcs,DC=jamfy,DC=tech

SEARCH SCOPE Hierarchical level to search below the search base
D All Subtrees

Attribute Mappings LDAP attribute mappings for Jamf Pro attributes

USER ID
E uSNCreated

USERNAME
F userPrincipalName

REAL NAME
G displayName

EMAIL ADDRESS
H mail

APPEND TO EMAIL RESULTS Text to append to email address results (e.g. "@mycompany.com")
I

DEPARTMENT
J department

BUILDING
K streetAddress

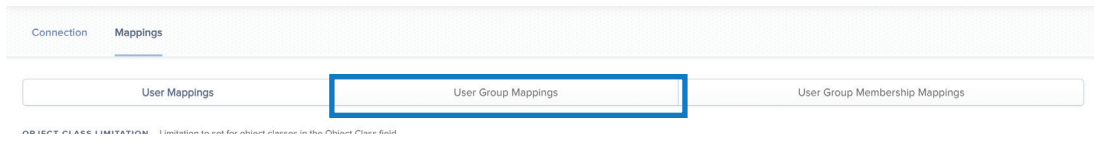
ROOM
L room

PHONE
M mobile

POSITION
N title

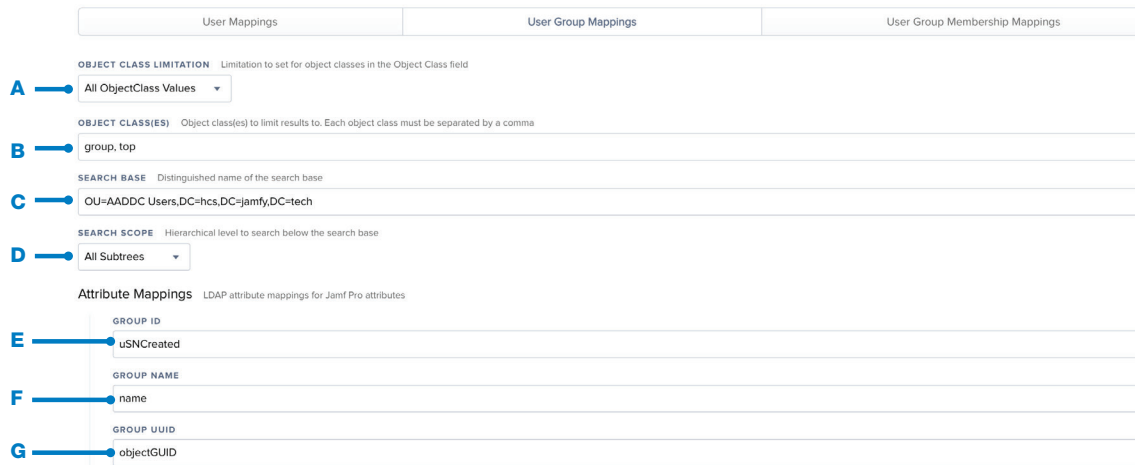
USER UUID
O objectGUID

11. Click User Group Mappings.

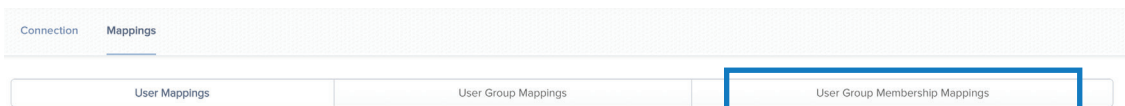


12. Configure the User Group Mappings settings as follows:

- 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”



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





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.

User Mappings | User Group Mappings | User Group Membership Mappings

MEMBERSHIP LOCATION The object where user group memberships are stored in the LDAP directory

A User Object

GROUP MEMBERSHIP MAPPING LDAP directory attribute to map group membership to

B memberOf

APPEND TO USERNAME WHEN SEARCHING Text to append to the username when searching the LDAP directory

C

D Use distinguished name of user groups when searching
Use distinguished name of user groups when searching the LDAP directory

E Use recursive group searches
Search groups that are members of user groups when searching the LDAP directory

Cancel Save

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 are stored in the LDAP directory

User Object

GROUP MEMBERSHIP MAPPING LDAP directory attribute to map group membership to

memberOf

APPEND TO USERNAME WHEN SEARCHING Text to append to the username when searching the LDAP directory

Use distinguished name of user groups when searching
Use distinguished name of user groups when searching the LDAP directory

Use recursive group searches
Search groups that are members of user groups when searching the LDAP directory

Done | History | Test | Clone | Delete | Edit

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 | User Group Membership Mapping

LOOK UP USERNAME

nmcdonald

Test

USERNAME	FULL NAME	EMAIL	PHONE	BUILDING	DEPARTMENT	ROOM	POSITION	UID
nmcdonald@hcs.jamfy.tech	Nicholas McDonald							20555

0.07 seconds

19. Click User Group Mappings.

The screenshot shows a navigation bar with three tabs: 'User Mappings', 'User Group Mappings' (which is highlighted with a blue box), and 'User Group Membership Mapping'. Below the navigation bar is a search field labeled '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.

The screenshot shows the 'User Group Mappings' tab selected. The search field 'LOOK UP USER GROUP' contains the text 'AAD DC Administrators'. Below the search field is a 'Test' button, which is highlighted with a blue box. Below the button is a table showing the search results.

GROUP NAME	GID
AAD DC Administrators	12768

0.21 seconds

21. Click User Group Membership Mappings.

The screenshot shows a navigation bar with three tabs: 'User Mappings', 'User Group Mappings', and 'User Group Membership Mapping' (which is highlighted with a blue box). Below the navigation bar is a search field labeled 'LOOK UP USERNAME' containing the text 'nmcdonald'. Below the search field is a 'Test' button. Below the button is a table showing user details.

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.

The screenshot shows the 'User Group Membership Mapping' tab selected. The 'CHECK IF USERNAME' field contains 'nmcdonald@hcs.jamfy.tech' and the 'IS A MEMBER OF USER GROUP' field contains 'AAD DC Administrators'. Below these fields is a 'Test' button, which is highlighted with a blue box. Below the button is a table showing the results of the membership check.

USERNAME	MEMBER
nmcdonald@hcs.jamfy.tech	Yes

0.07 seconds

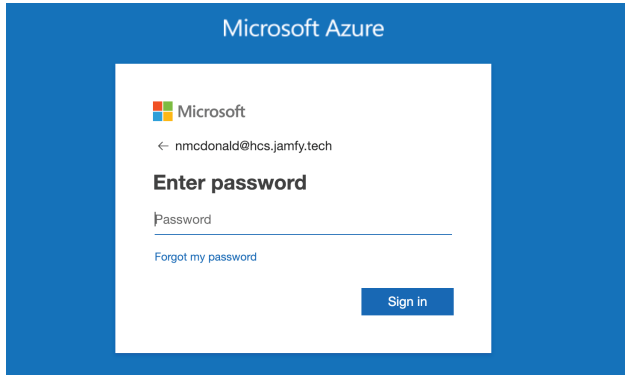
You have successfully configured Jamf Pro to integrate with Azure AD Domain Services - Secure LDAP service.



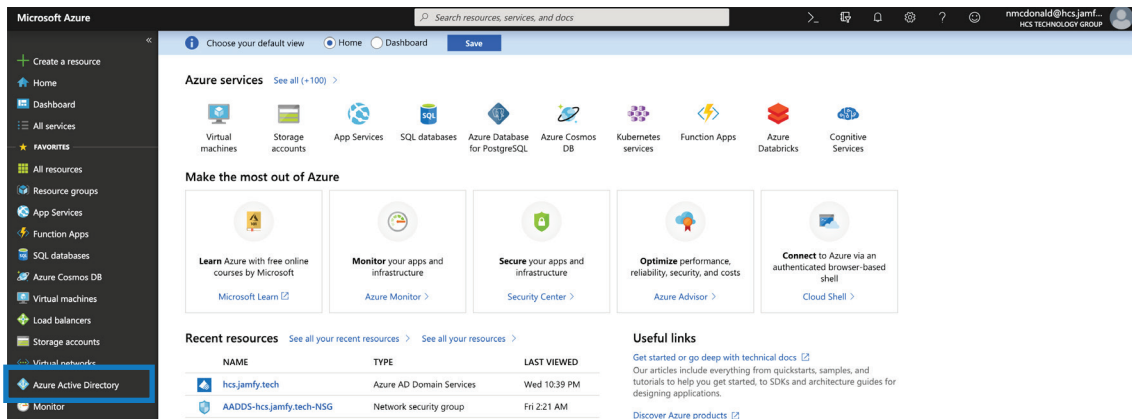
Section 5: Configure Azure Active Directory for Single Sign-On (SSO)

In this section you configure AADDS to support SSO with Jamf Pro.

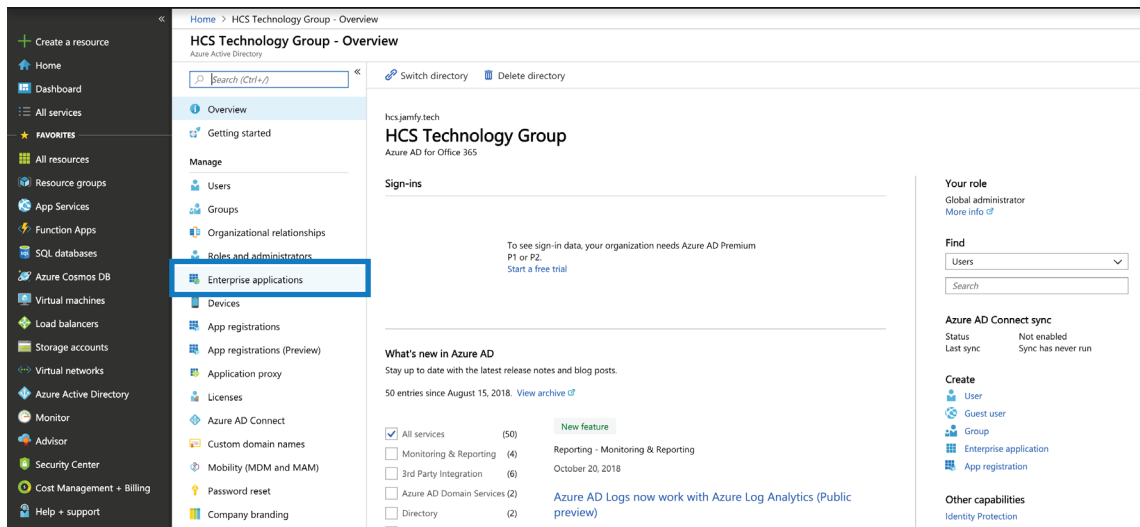
1. Use Firefox or Google Chrome to open portal.azure.com.
2. Log in with your Azure Admin credentials



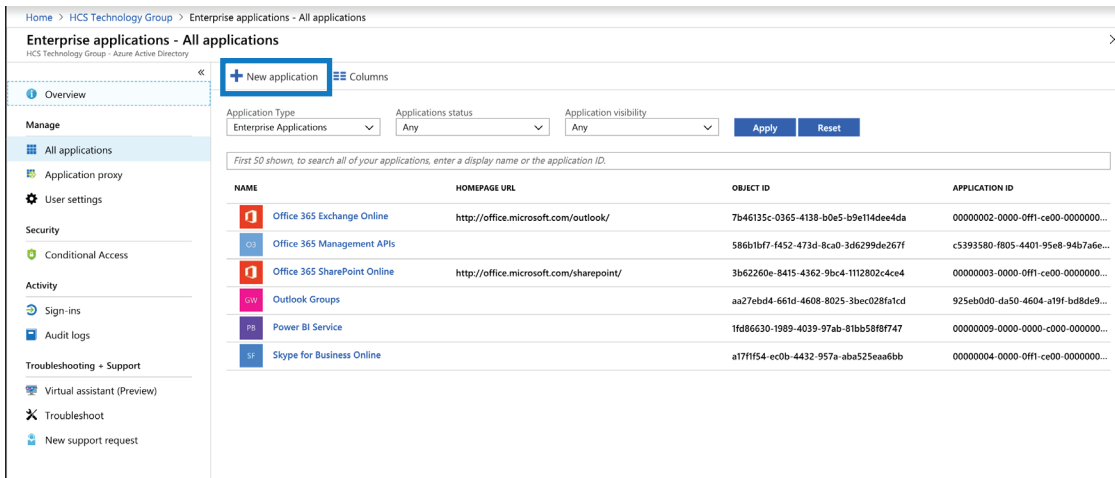
3. In the sidebar, click Azure Active Directory.



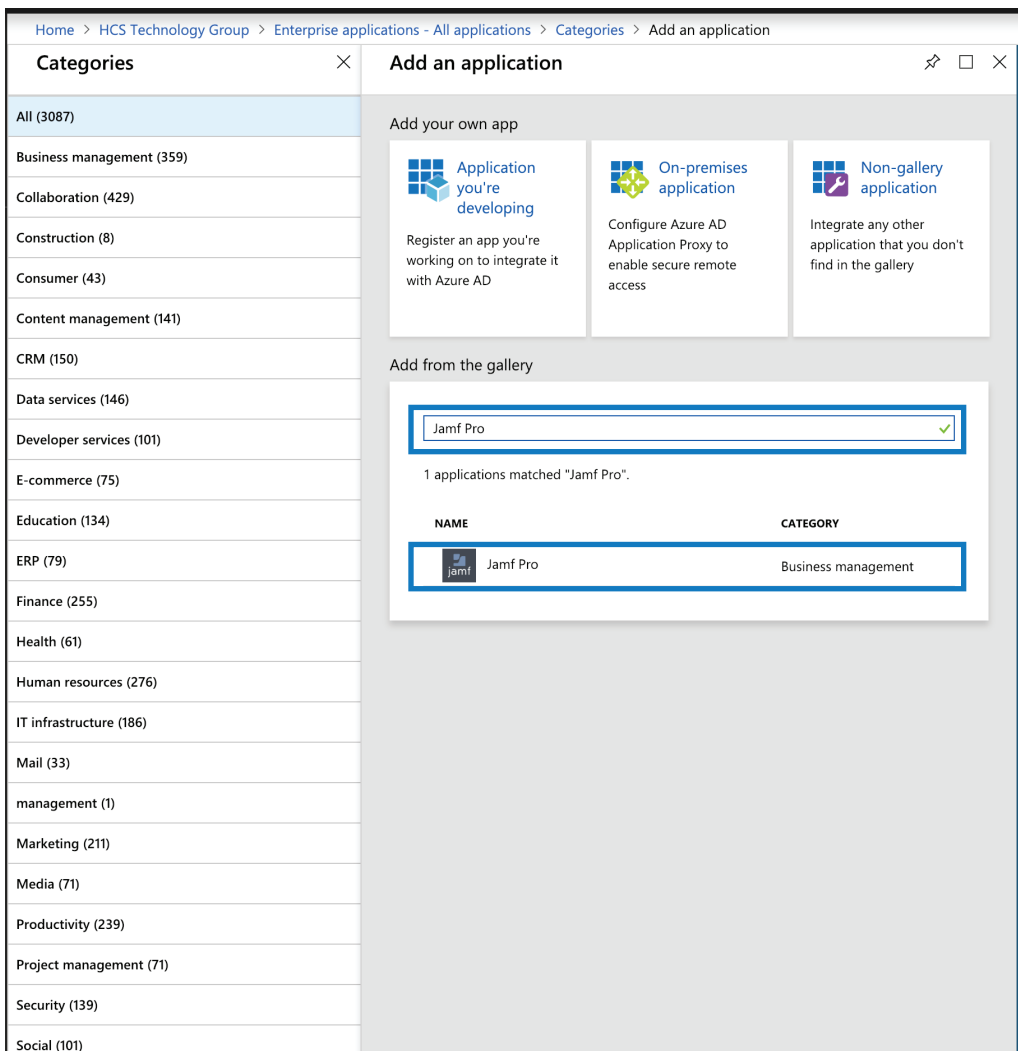
4. In the Manage section, click "Enterprise applications."



5. In the new window, click “New application.”

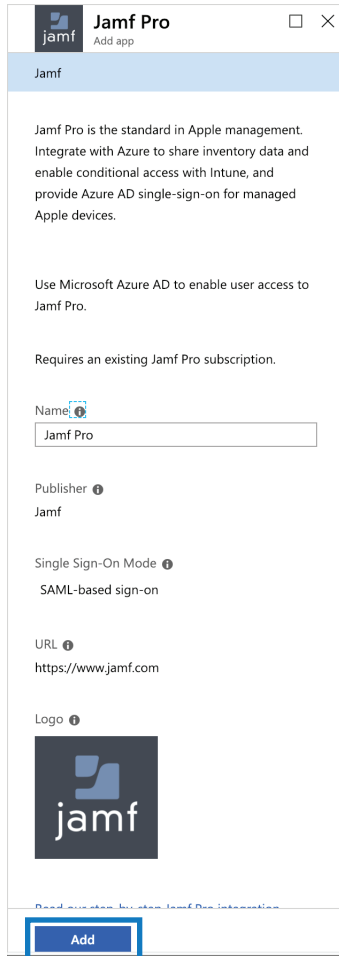


6. In the “Add from the gallery” section, enter “Jamf Pro”, then in the search results section, click Jamf Pro.



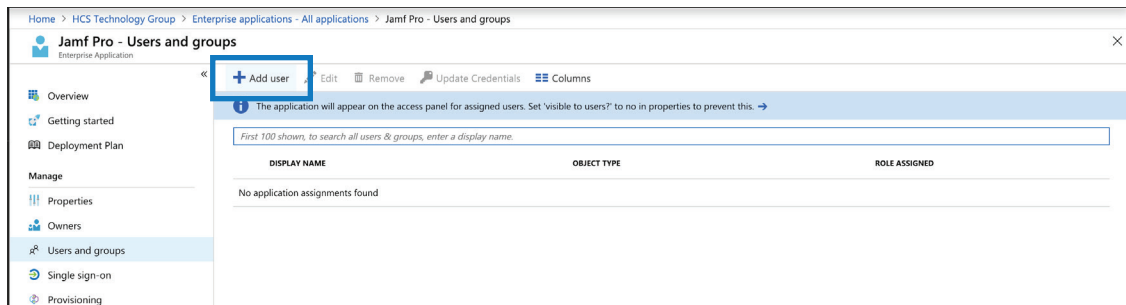


7. In the new panel, click Add.



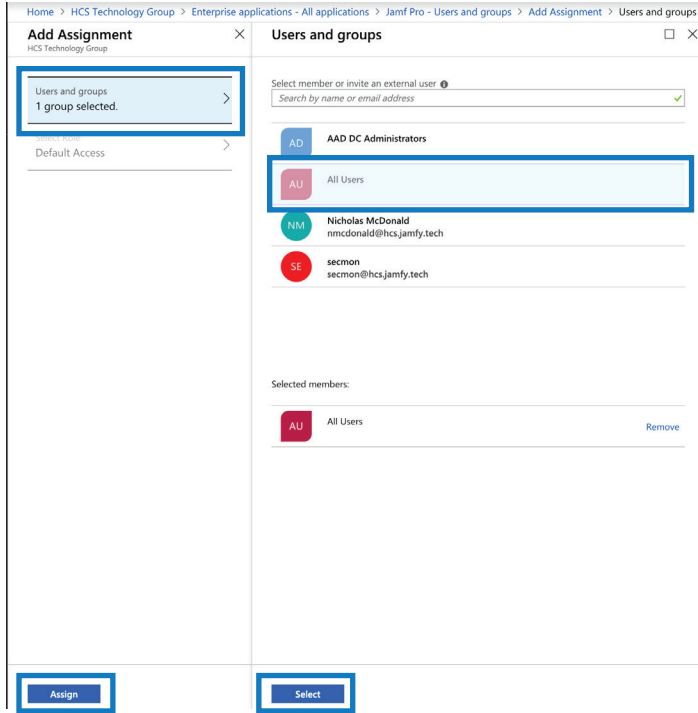
8. Click “Users and groups.”

9. Click “Add user.”

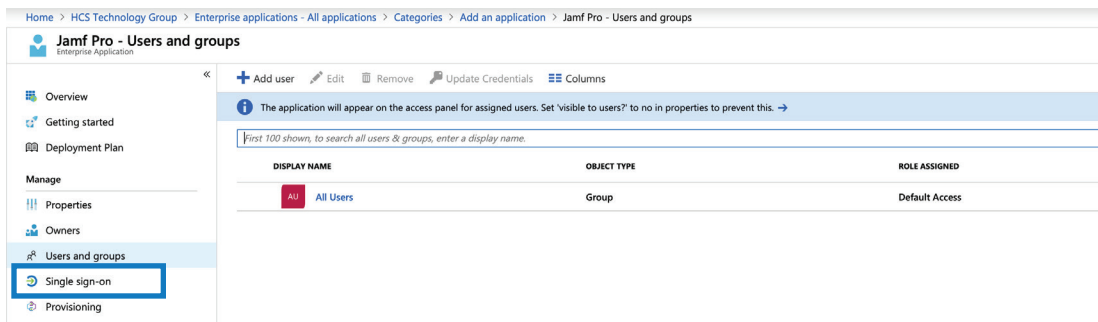


10. Click “Users and Groups.” If you see “Groups are not available for assignment due to your Active Directory plan level,” then for testing, you can continue with adding a user instead of a group.

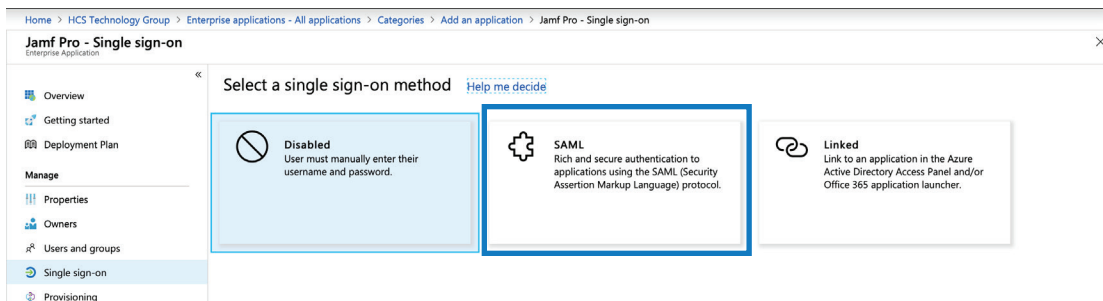
11. Select a user or group that should be able to access Jamf Pro. If you plan to allow users to use Azure AD to sign in to the User Initiated Enrollment window and Self Service, then select the All Users group. You can allow administrative access to the Jamf Pro web app to different groups or users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



13. Click "Single sign-on".



14. Select SAML.





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

Home > HCS Technology Group > Enterprise applications - All applications > Categories > Add an application > Jamf Pro - Single sign-on > SAML-based sign-on

Jamf Pro - SAML-based sign-on




Enterprise Application

Change single sign-on mode | Switch to the old experience

Welcome to the new experience for configuring SAML based SSO. Please click here to provide feedback →

Set up Single Sign-On with SAML - Preview

Read the [configuration guide](#) for help integrating Jamf Pro.

- Basic SAML Configuration** 
- User Attributes & Claims** 
- SAML Signing Certificate** 

Property	Value	Requirement
Identifier (Entity ID)		Required
Reply URL (Assertion Consumer Service URL)		Required
Sign on URL		Optional
Relay State		Optional
Logout URL		Optional


Property	Value
Givenname	user.givenname
Surname	user.surname
Emailaddress	user.mail
Name	user.userprincipalname
Unique User Identifier	user.userprincipalname

Property	Value
Status	Active
Thumbprint	E69647D0173CC451AD335CF66F4112772AE88C9D
Expiration	3/7/2022, 12:41:15 PM
Notification Email	nmcdonald@hcs.jamfy.tech
App Federation Metadata Url	https://login.microsoftonline.com/3a44480d-7f9e-4...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

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

 Upload metadata file

Identifier (Entity ID) (Required) ⓘ

Patterns: https://*.jamfcloud.com/saml/metadata

Reply URL (Assertion Consumer Service URL) (Required) ⓘ

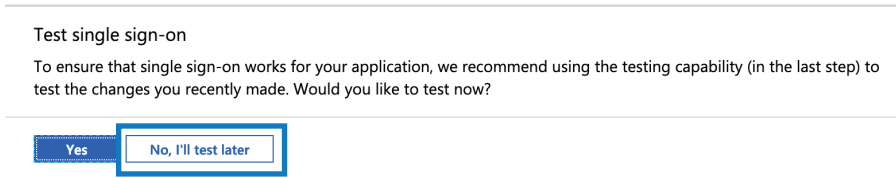
Patterns: https://*.jamfcloud.com/saml/SSO

Sign on URL (Optional) ⓘ

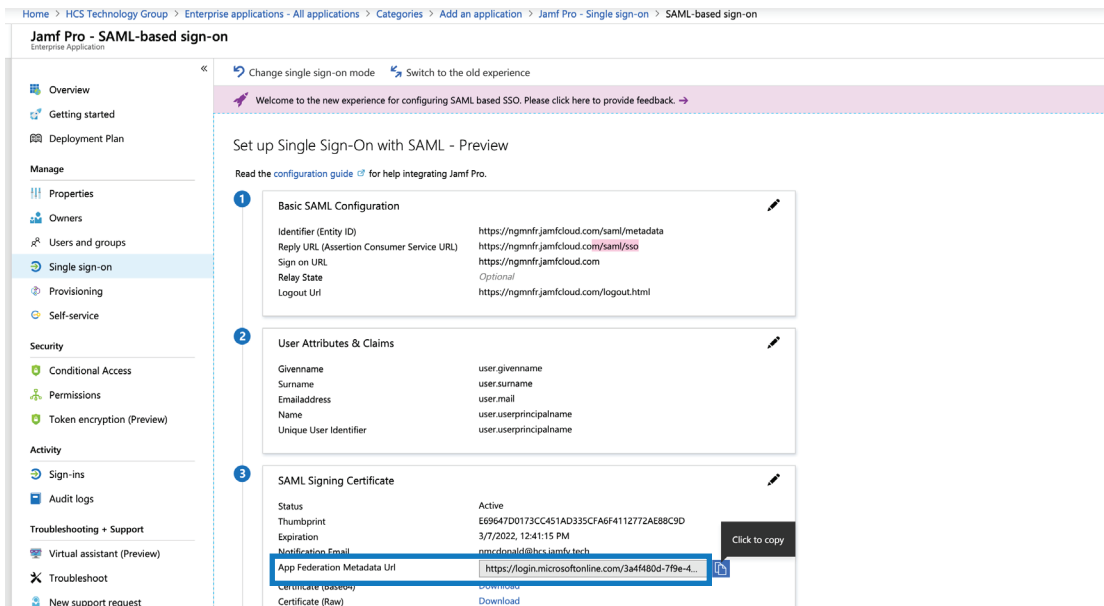
Relay State (Optional) ⓘ

Logout URL (Optional) ⓘ

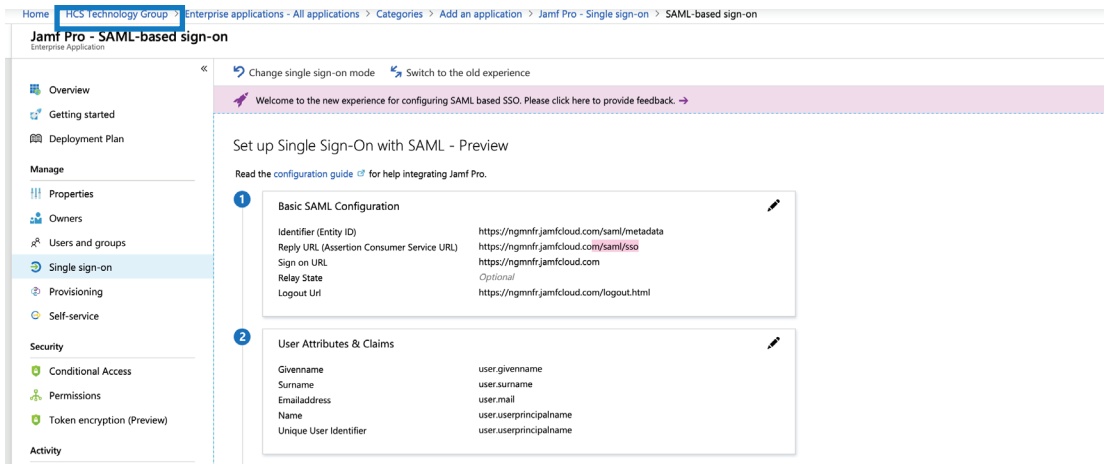
18. At the “Test single sign-on” message, click “No, I’ll test later.”



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 - Overview

HCS Technology Group - Overview

Azure Active Directory

Search (Ctrl+F)

Switch directory Delete directory

Overview

- Getting started
- Manage
 - Users
 - Groups
 - Organizational relationships
 - Roles and administrators
 - Enterprise applications
 - Devices
 - App registrations**
 - App registrations (Preview)
 - Application proxy
 - Licenses
 - Azure AD Connect
 - Custom domain names
 - Multi-tenant (M2M and M2M)

hcs.jamf.tech
HCS Technology Group
Azure AD Premium P1

Sign-ins

What's new in Azure AD

Stay up to date with the latest release notes and blog posts.

16 entries since November 15, 2018. [View archive](#)

All services (16) New feature

Access Control (2) App Proxy - Access Control

Your role
Global administrator
[More info](#)

Find

Users

Search

Azure AD Connect sync

Status Not enabled
Last sync Sync has never run

Create

- User
- Guest user
- Group
- Enterprise application
- App registration

22. Click “View all applications.”

Home > HCS Technology Group - App registrations

HCS Technology Group - App registrations

Azure Active Directory

Search (Ctrl+F)

New application registration Endpoints Troubleshoot

The preview experience for App registrations is available. Click this banner to launch the preview experience. →

Search by name or AppID My apps

DISPLAY NAME	APPLICATION TYPE	APPLICATION ID
You're not the owner of any applications in this directory.		

View all applications

23. After the window refreshes, select Jamf Pro.

Home > HCS Technology Group - App registrations

HCS Technology Group - App registrations

Azure Active Directory

Search (Ctrl+F)

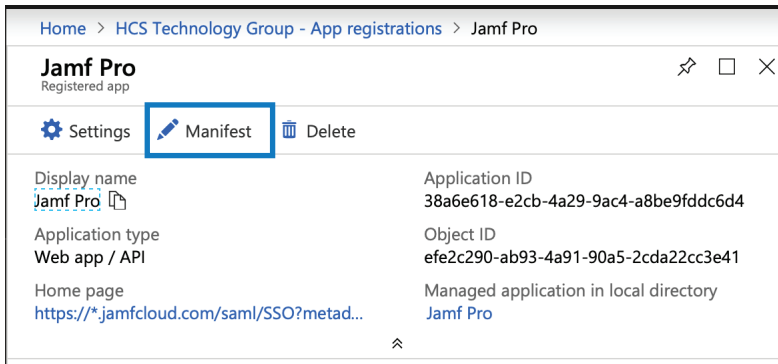
New application registration Endpoints Troubleshoot

The preview experience for App registrations is available. Click this banner to launch the preview experience. →

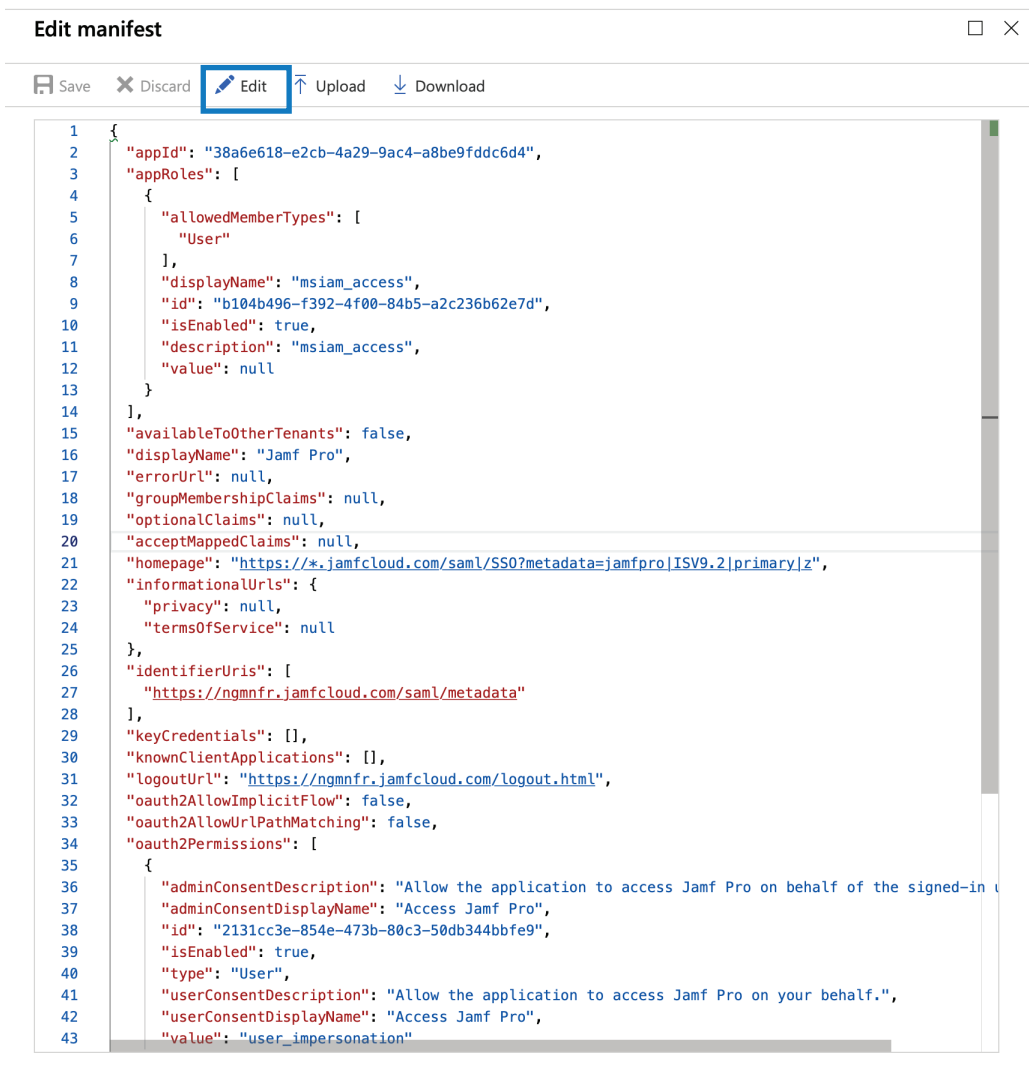
Search by name or AppID All apps

DISPLAY NAME	APPLICATION TYPE	APPLICATION ID
Azure AD Domain Services Sync	Web app / API	eec29ddb-eecd-4621-a268-50cd68b3f00f
Jamf Pro	Web app / API	38a6e618-e2cb-4a29-9ac4-a8be9fddc6d4

24. Click Manifest.



25. Click Edit.





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

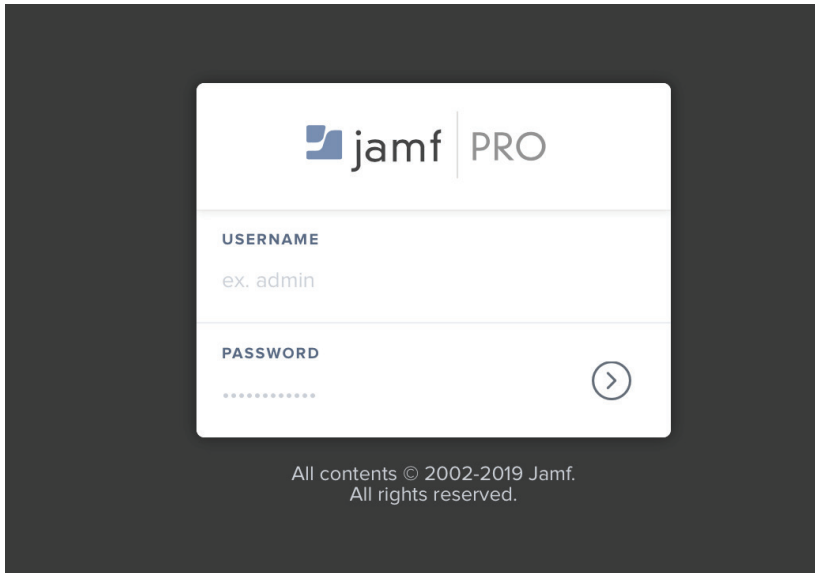
```
1 {
2   "appId": "38a6e618-e2cb-4a29-9ac4-a8be9fddc6d4",
3   "appRoles": [
4     {
5       "allowedMemberTypes": [
6         "User"
7       ],
8       "displayName": "msiam_access",
9       "id": "b104b496-f392-4f00-84b5-a2c236b62e7d",
10      "isEnabled": true,
11      "description": "msiam_access",
12      "value": null
13    }
14  ],
15  "availableToOtherTenants": false,
16  "displayName": "Jamf Pro",
17  "errorUrl": null,
18  "groupMembershipClaims": "All",
19  "optionalClaims": null,
20  "acceptMappedClaims": null,
21  "homepage": "https://*.jamfcloud.com/saml/SSO?metadata=jamfpro|ISV9.2|primary|z",
22  "informationalUrls": {
23    "privacy": null,
24    "termsOfService": null
25  },
26  "identifierUris": [
27    "https://ngmnfr.jamfcloud.com/saml/metadata"
28  ],
29  "keyCredentials": [],
30  "knownClientApplications": [],
31  "logoutUrl": "https://ngmnfr.jamfcloud.com/logout.html",
32  "oauth2AllowImplicitFlow": false,
33  "oauth2AllowUrlPathMatching": false,
34  "oauth2Permissions": [
35    {
36      "adminConsentDescription": "Allow the application to access Jamf Pro on behalf of the signed-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"
```

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

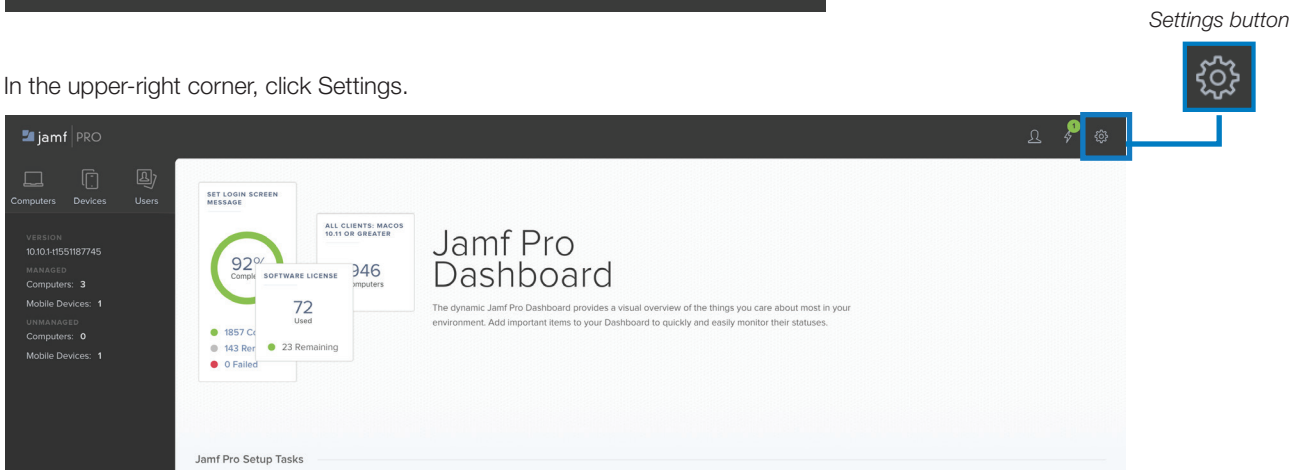
Section 6: Configure Jamf Pro for Azure AD - Single Sign-On

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.

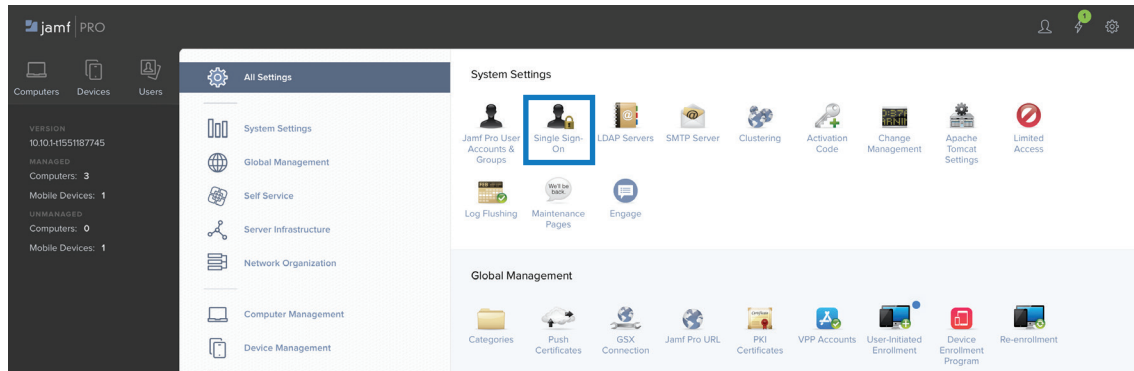


2. In the upper-right corner, click Settings.

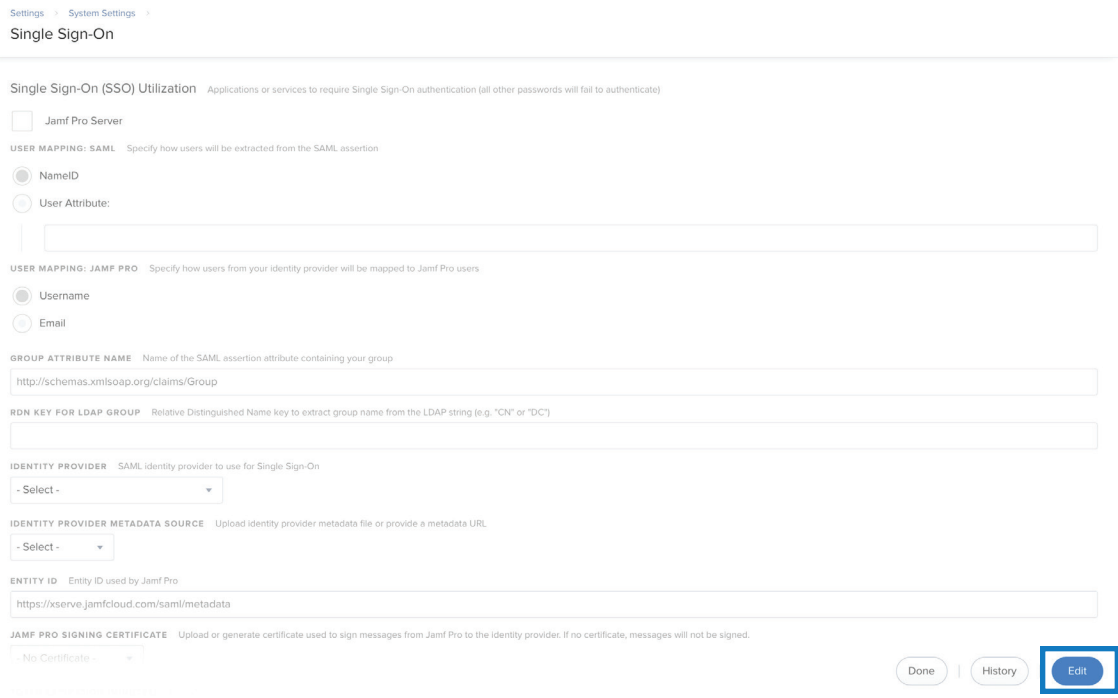




3. In the System Settings section, click Single Sign-On.

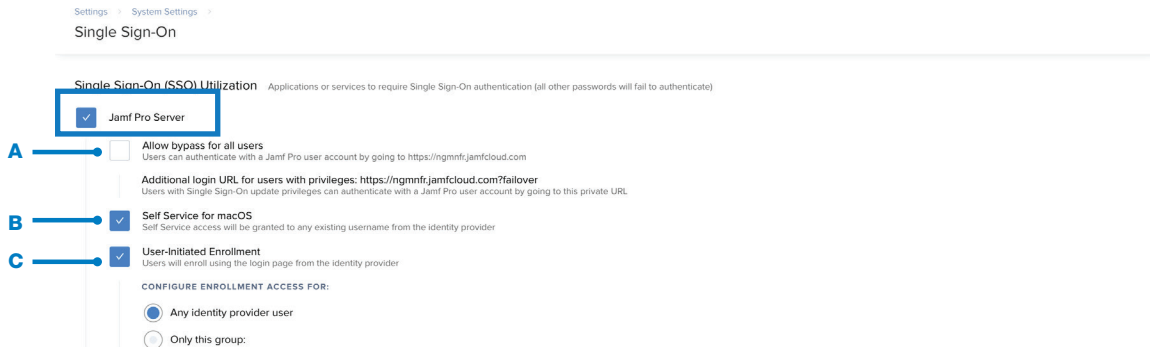


4. In the lower-right corner click Edit.

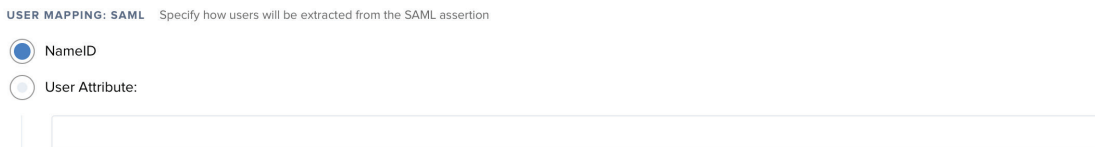


5. Select the checkbox “Jamf Pro Server”. Additional options are displayed.

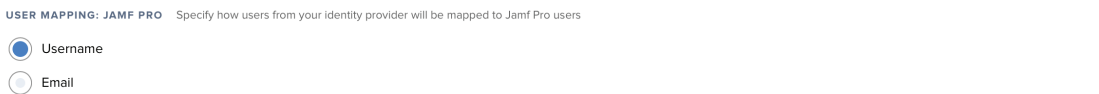
- A. Leave the checkbox deselected for the option “Allow bypass for all users.” When you leave this option disabled, administrators must use SSO to access the Jamf Pro web interface, unless they have “Single Sign-on” update privileges. In the next section of this guide you’ll create a group for administrators 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 enter the object ID of an Azure AD group; finding Group Object ID’s is covered on page 62 step 7.



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.



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.





- 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.

GROUP ATTRIBUTE NAME Name of the SAML assertion attribute containing your group

RDN KEY FOR LDAP GROUP Relative Distinguished Name key to extract group name from the LDAP string (e.g. "CN" or "DC")

- Click the Identity Provider menu, choose Other, and enter “Azure AD” in the Other Provider field.

IDENTITY PROVIDER SAML identity provider to use for Single Sign-On

Other

OTHER PROVIDER:

- 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

ENTITY ID Entity ID used by Jamf Pro

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.

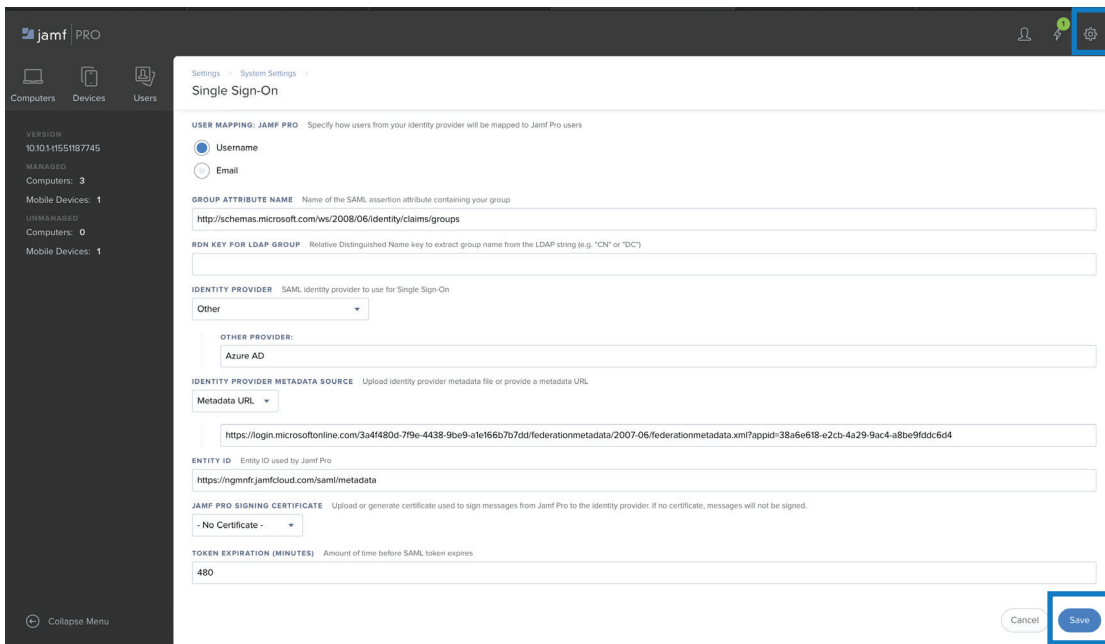
- No Certificate -

- Leave “Entity ID” and “Jamf Pro Signing Certificate” at their default values.
- 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).

TOKEN EXPIRATION (MINUTES) Amount of time before SAML token expires

12. In the lower-right corner click Save, then click Settings.

Settings button



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.

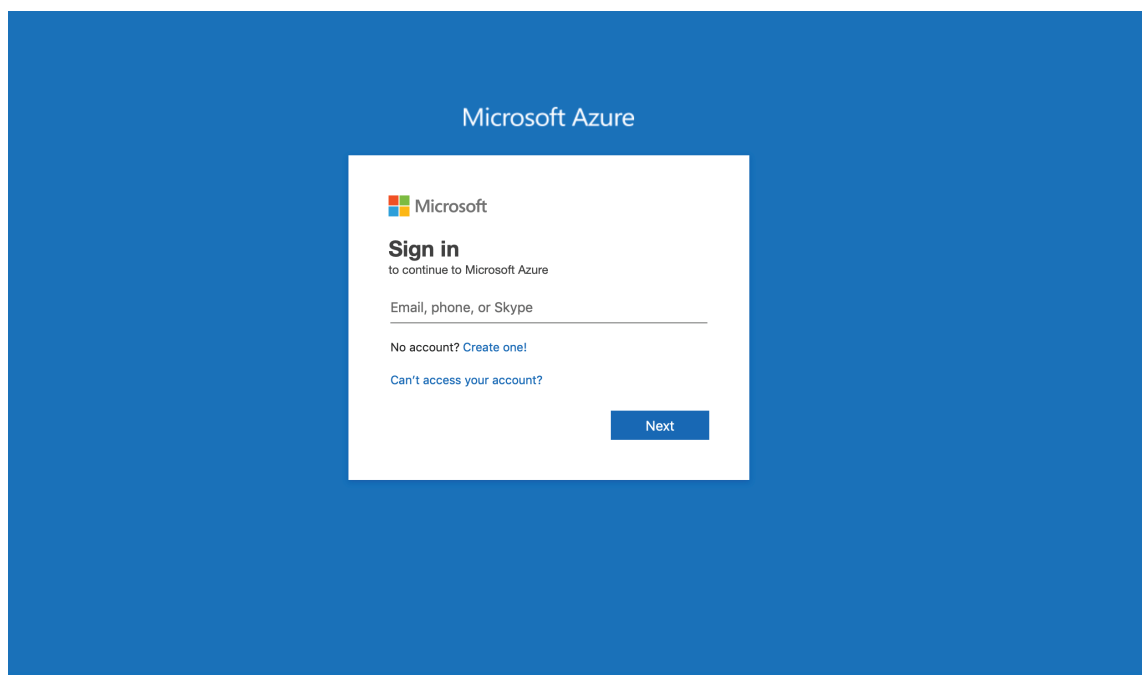
You'll create the following:

- 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

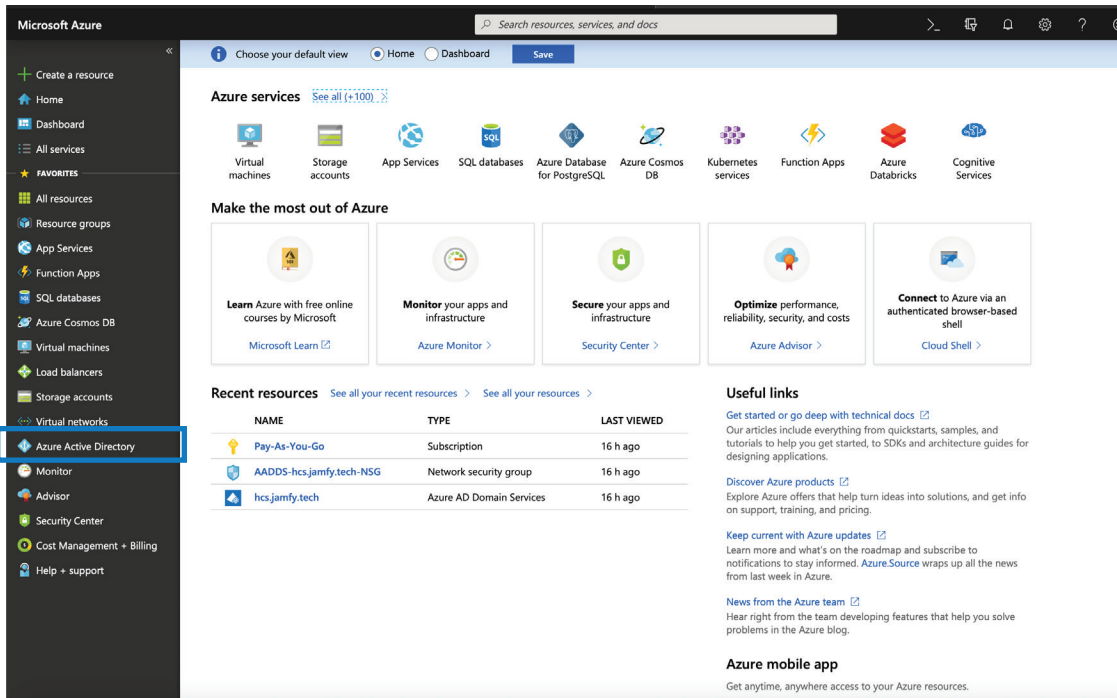
Do not perform this step for administrators that need to be able to use the Jamf Pro failover URL.

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

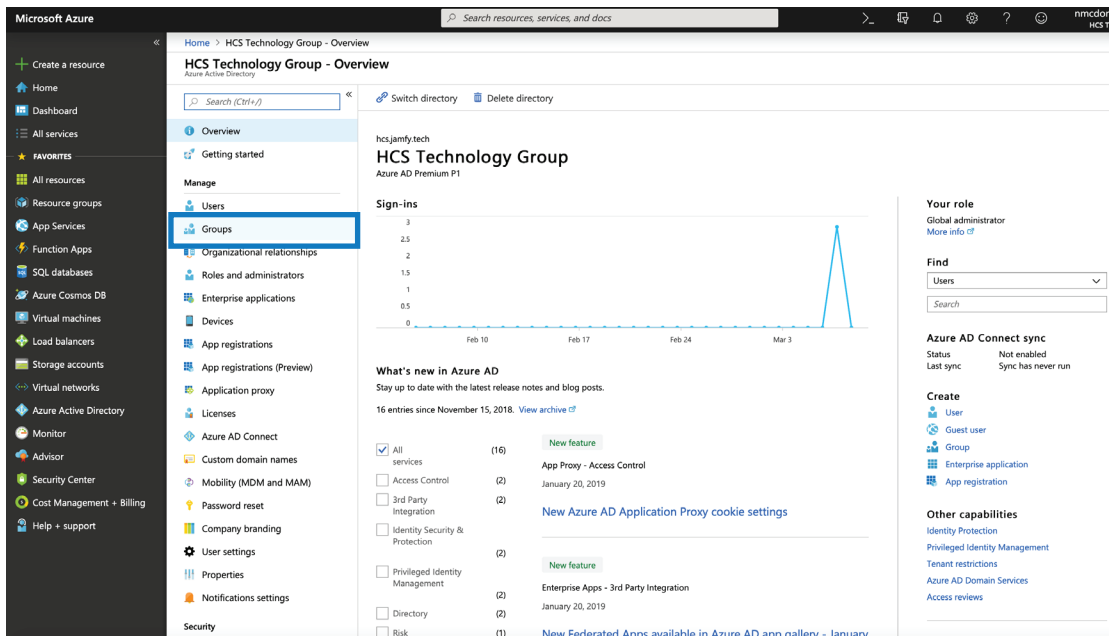
1. Use Firefox or Google Chrome to open portal.azure.com and sign in as an Azure AD admin.



2. In the sidebar, click Azure Active Directory.

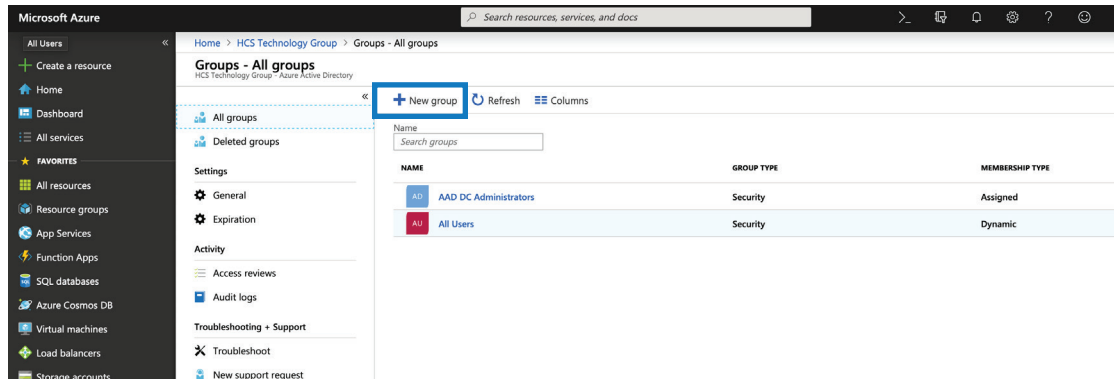


3. Click Groups.



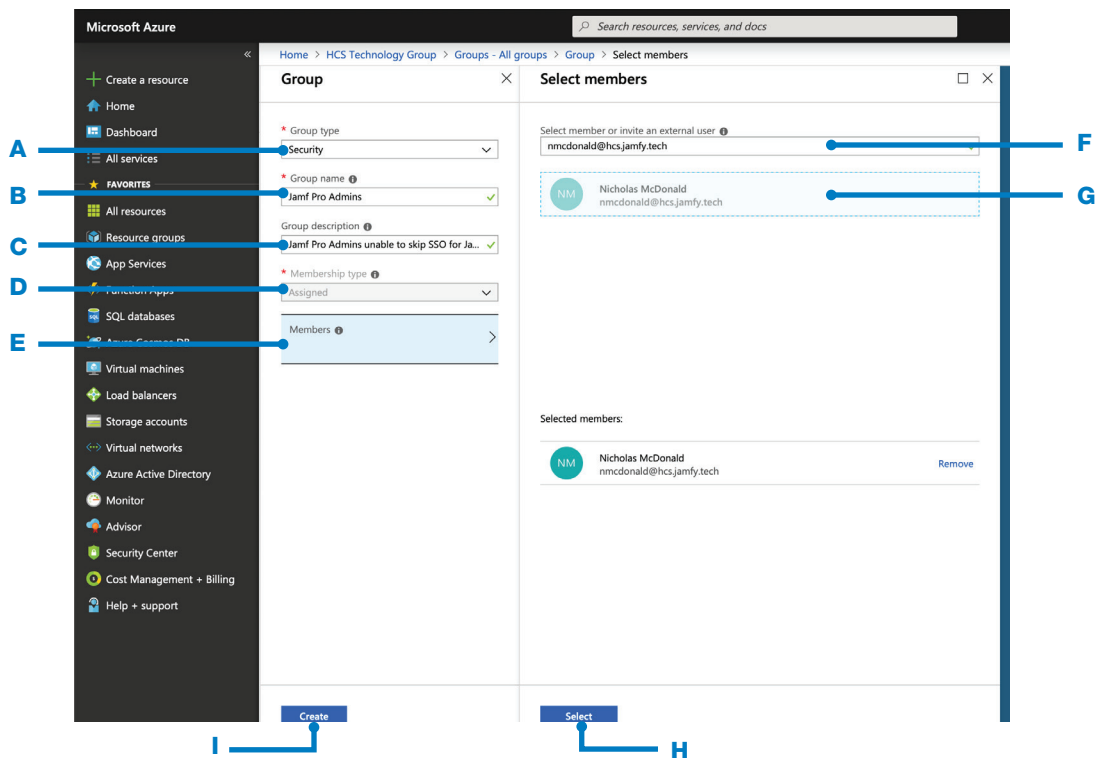


4. Click “New group.”

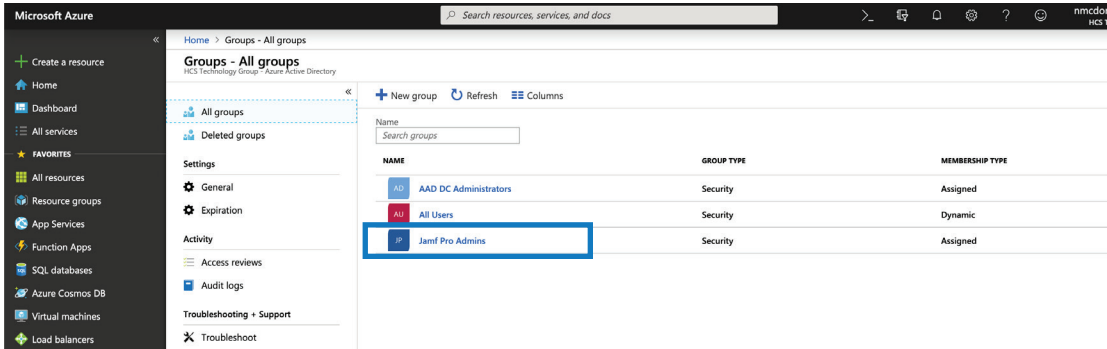


5. Configure the following options for the new group:

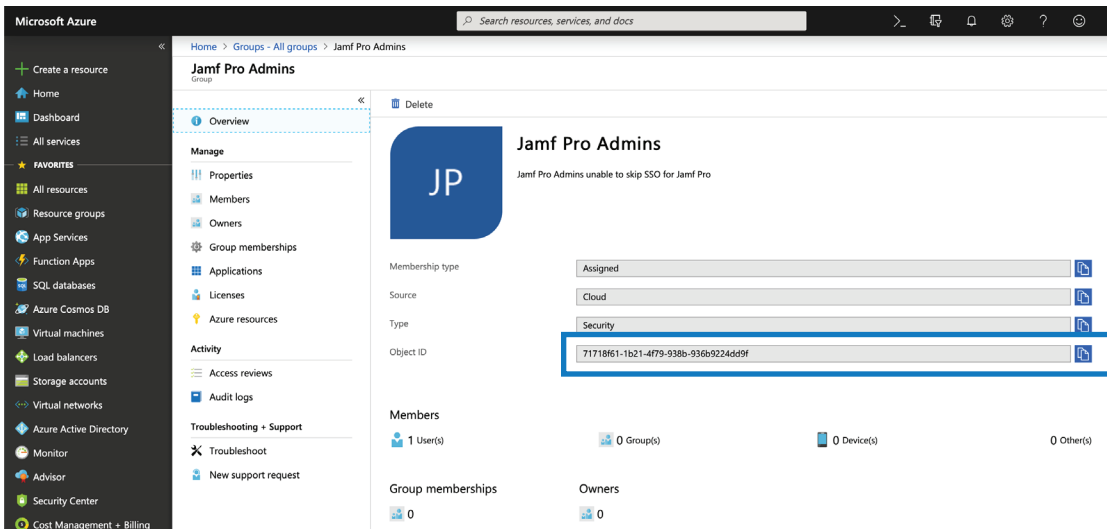
- A. Click “Group type” then choose “Security” (you could also use “Office 365”).
- B. In the Group Name field enter a name. This guide uses “Jamf Pro Admins” as an example.
- C. In the Group Description field enter a short description of the group This guide uses “Jamf Pro Admins unable to skip SSO 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.



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.



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.



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.”

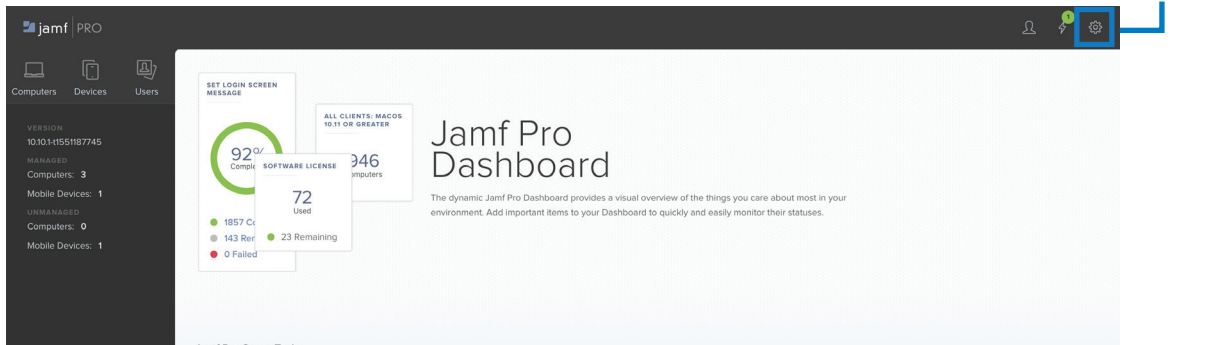


9. If you don't already have a window or tab open with your Jamf Pro web admin, you need to use your Jamf Pro failover URL (it follows the format of `https://YourJamfInstance.jamfcloud.com/?failover`) and log in.

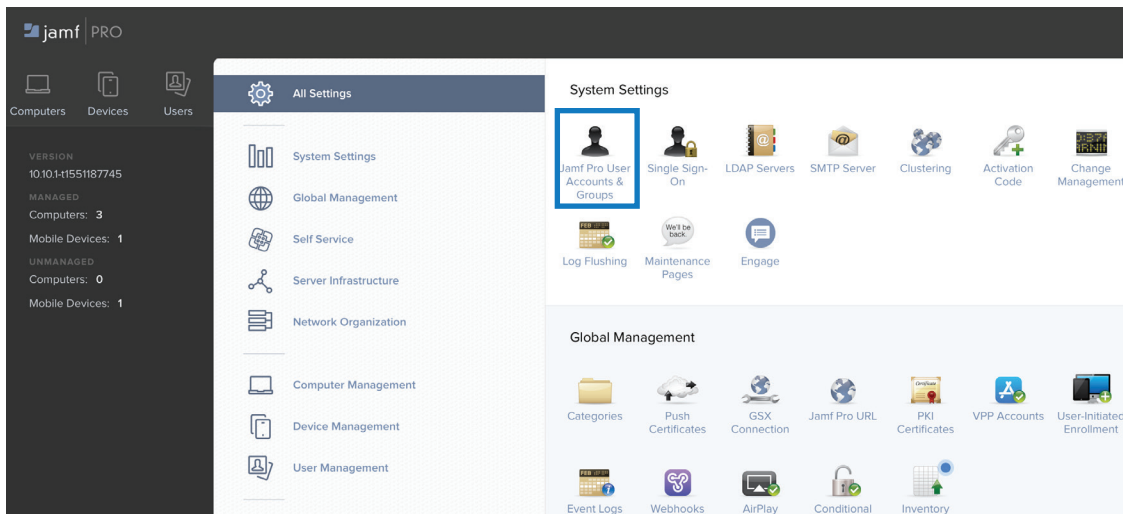


Settings button

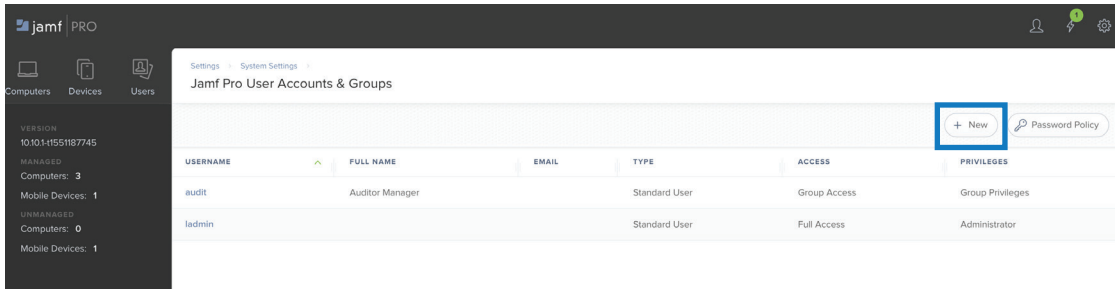
10. In the upper-right corner, click Settings.



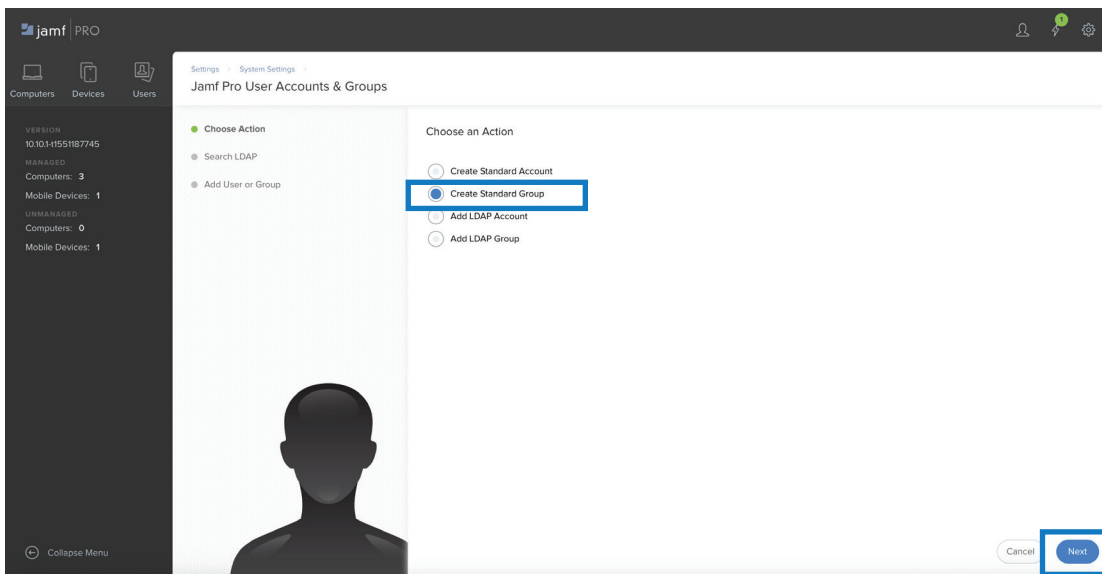
11. Click Jamf Pro User Accounts & Groups.



12. Click New.

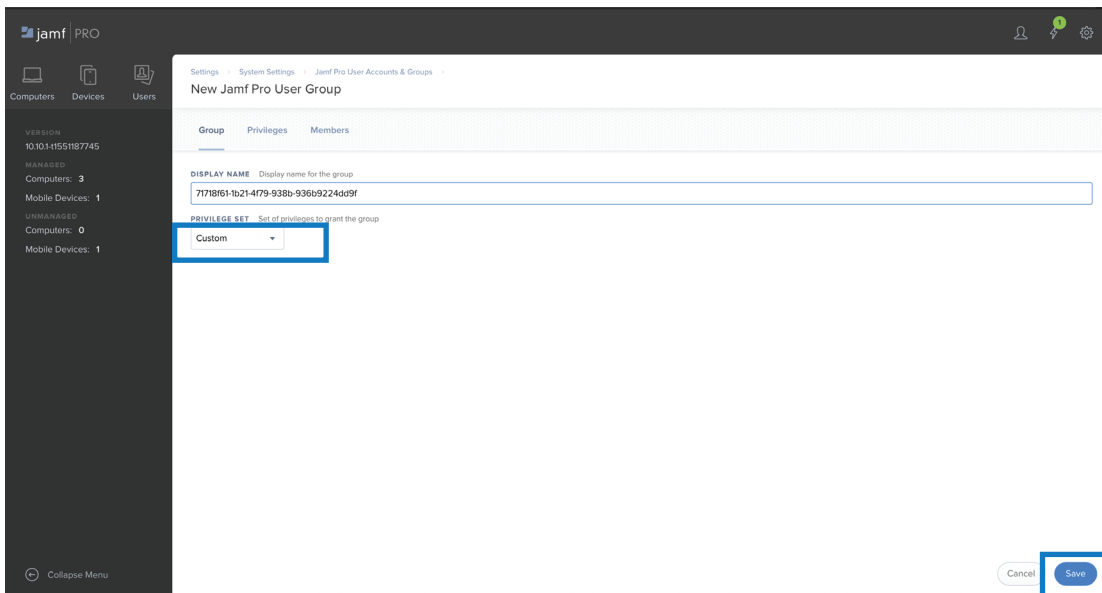


13. Select Create Standard Group then click Next.



14. For the "Display Name" enter the Object ID you collected in Step 7.

15. Click Privilege Set and choose Custom. Click Save.

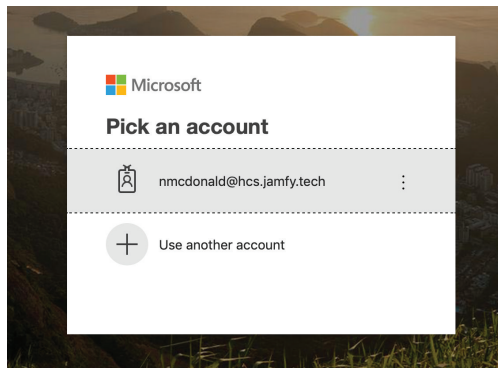




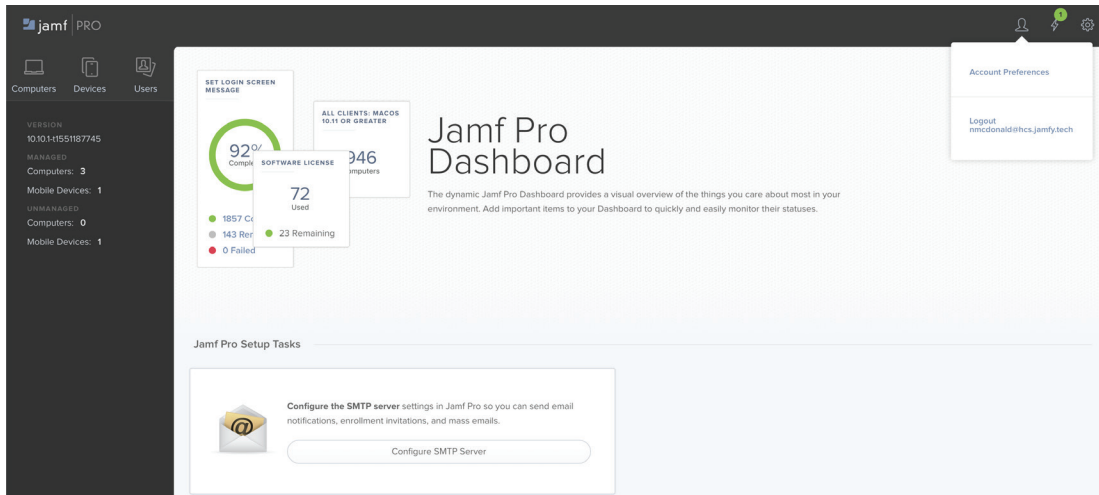
16. Click the Privileges tab.
17. Select Jamf Pro Server Objects.
 - A. Under the Create column, click All.
 - B. Under the Read column, click All.
 - C. Under the Update column, click All.
 - D. Under the Delete column, click All.
18. Select Jamf Pro Server Settings.
 - A. Under the Read column, click 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	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Security	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Self Service	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Self Service for iOS	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Single Sign-On	<input checked="" type="checkbox"/>	<input type="checkbox"/>
SMTP Server	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sso Settings	<input checked="" type="checkbox"/>	<input type="checkbox"/>
User-Initiated Enrollment	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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.



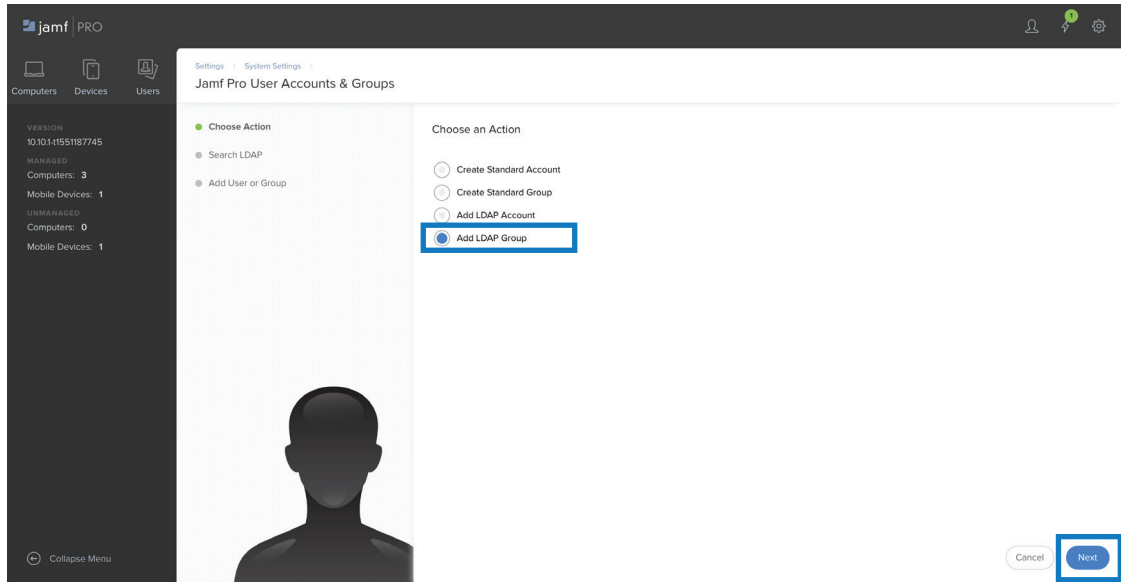
23. If your Azure AD account is displayed, select it. Otherwise, click “Use another account,” enter your Azure AD email address, click Next, enter your Azure AD password, then click “Sign in.” If your web browser offers to save your password, do not save the password.
24. Confirm that you see your Jamf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



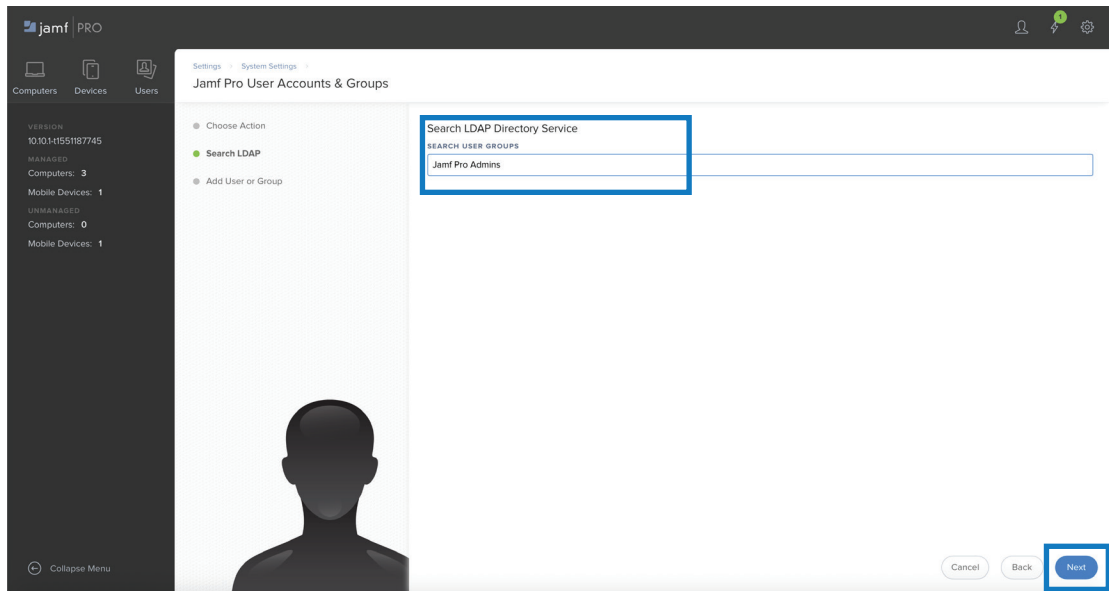
25. This is optional, but you can confirm that you can not yet use an Azure AD user to authenticate to Jamf Admin with the following outline:
 - A. Quit Jamf Admin if it's open.
 - B. In the Finder, open your Applications folder, then open the Jamf Pro folder.
 - C. Press and hold the Option key on your 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.



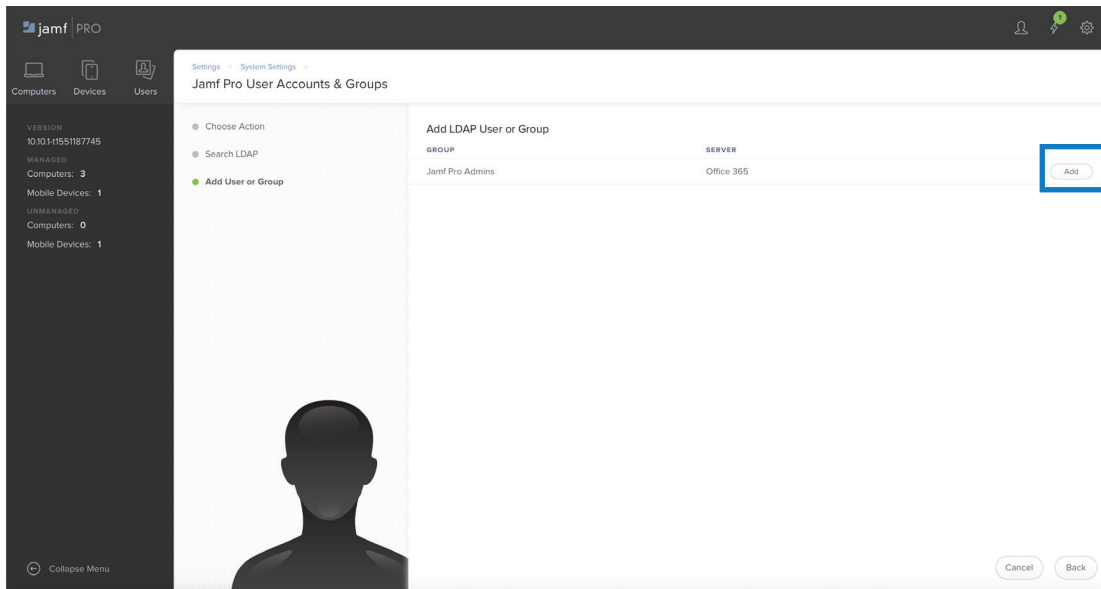
31. Select Add LDAP Group then click Next.



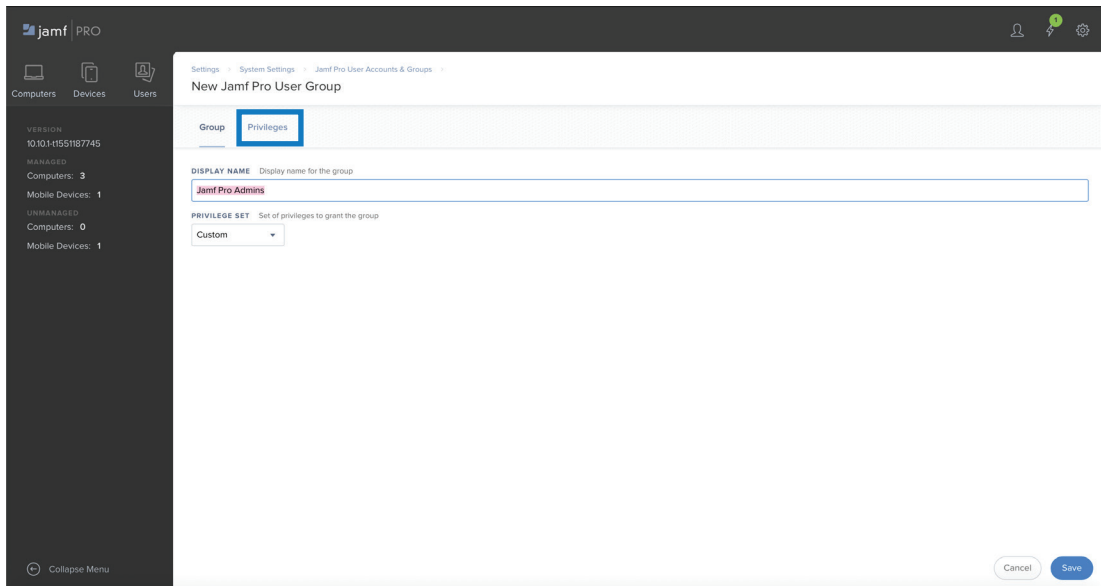
32. In the Search User Groups field, enter the name you gave your group in Azure (this guide uses “Jamf Pro Admins”), then click Next.



33. Next to the Azure group, click Add.



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





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	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Security	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Self Service	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Self Service for iOS	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Single Sign-On	<input checked="" type="checkbox"/>	<input type="checkbox"/>
SMTP Server	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sso Settings	<input checked="" type="checkbox"/>	<input type="checkbox"/>
User-Initiated Enrollment	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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:
- Quit Jamf Admin if it's open.
 - In the Finder, open your Applications folder, then open the Jamf Pro folder.
 - Press and hold the Option key on your keyboard, and double-click Jamf Admin.
 - Provide your Jamf Pro Server Address if prompted.
 - 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.
 - In the authentication dialog for Jamf Pro, leave the checkbox disabled for the option “Store in Keychain”.
 - Enter your Azure credentials, then click OK to log in.
 - Confirm that you see your expected Jamf Admin window.
 - 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

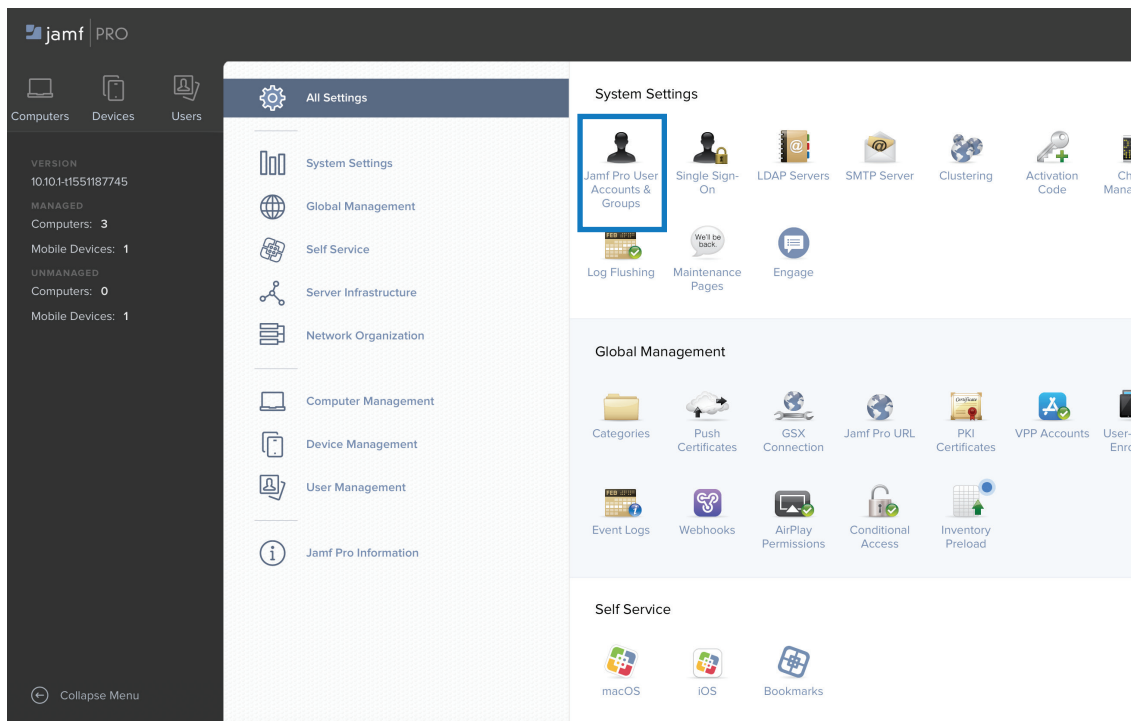
Perform this task only for someone that should be able to authenticate to the Jamf Pro failover URL with their Azure AD credentials. This account will be able to do the following:

- 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.

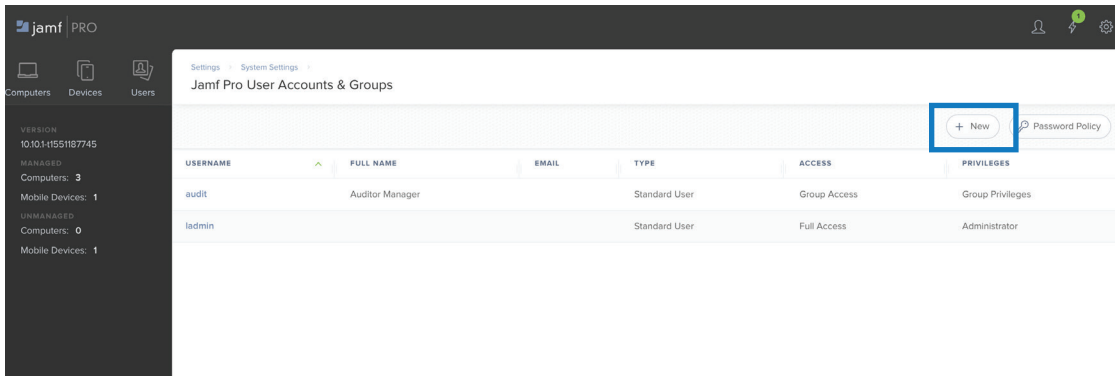
Do not perform this task for users that do not administer Jamf Pro.

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

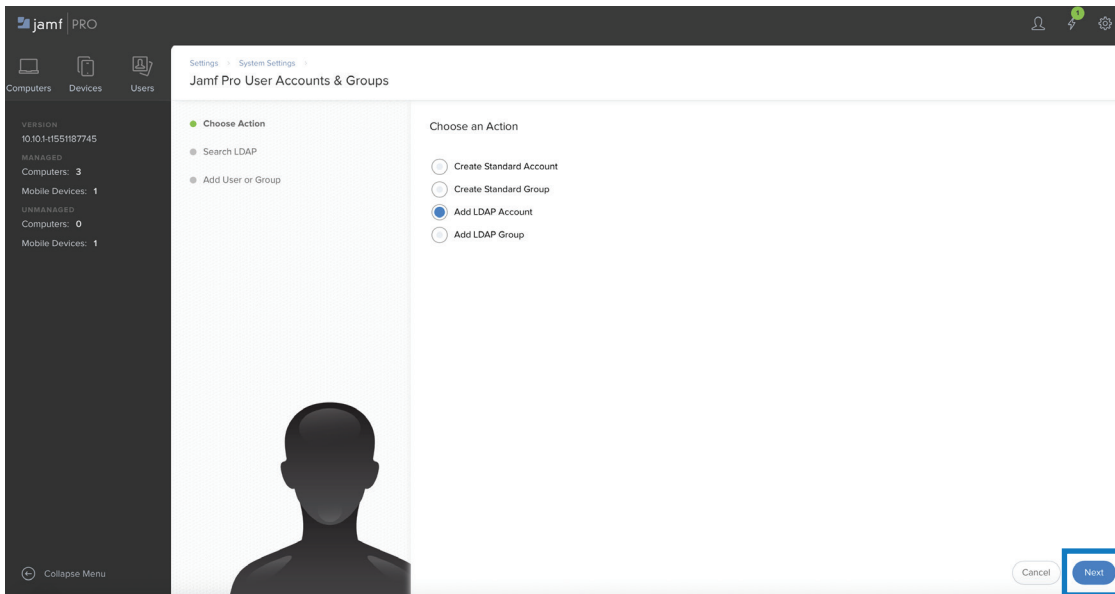
1. Click Jamf Pro User Accounts & Groups.



2. Click New.

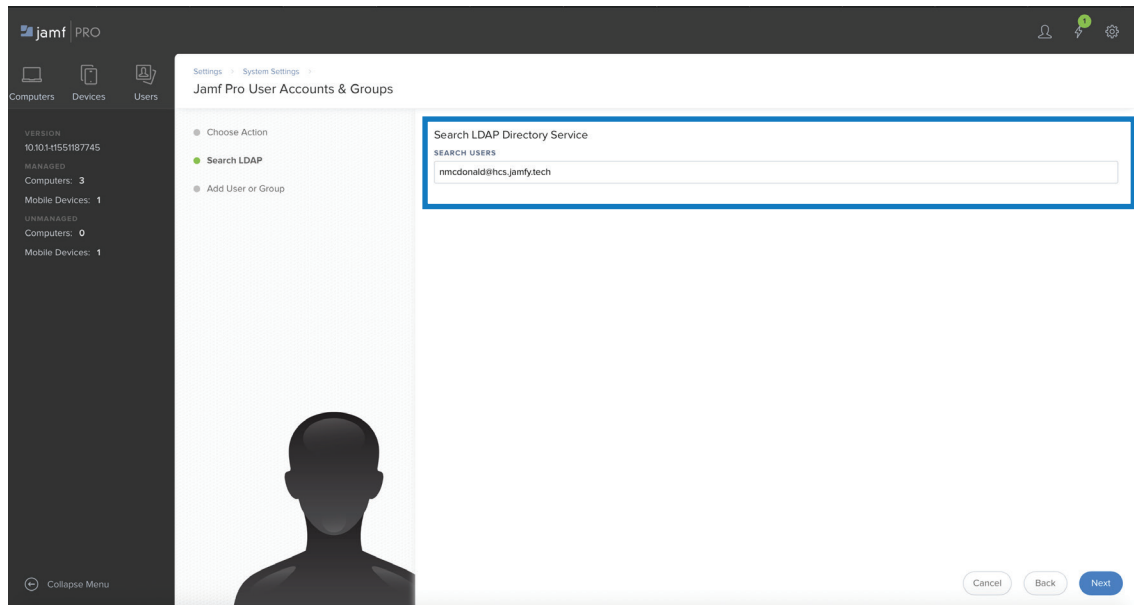


3. Select Add LDAP Account then click Next.

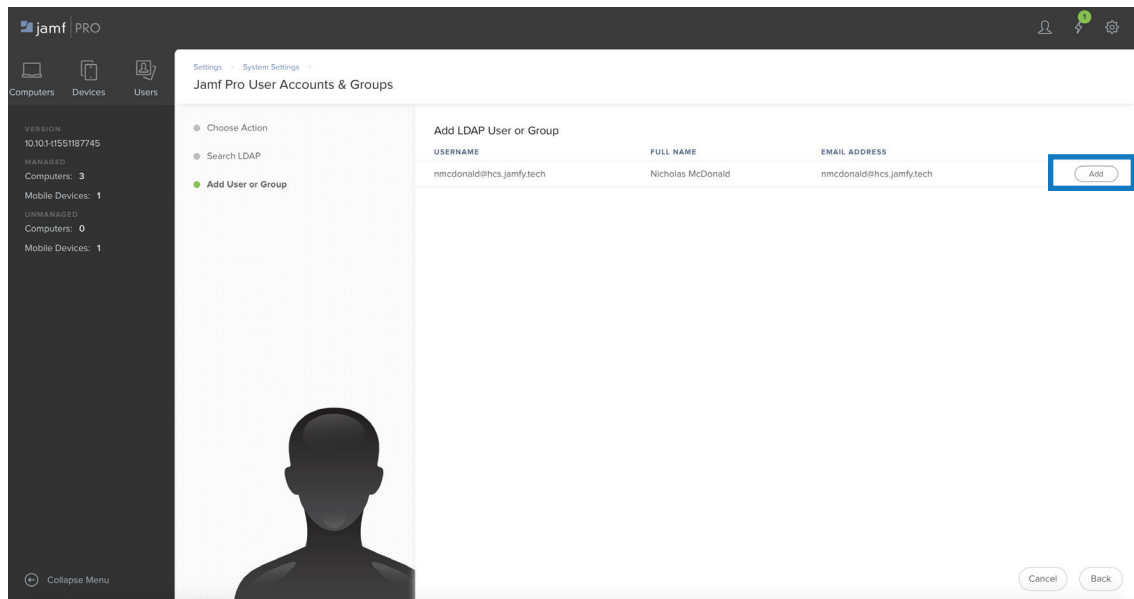




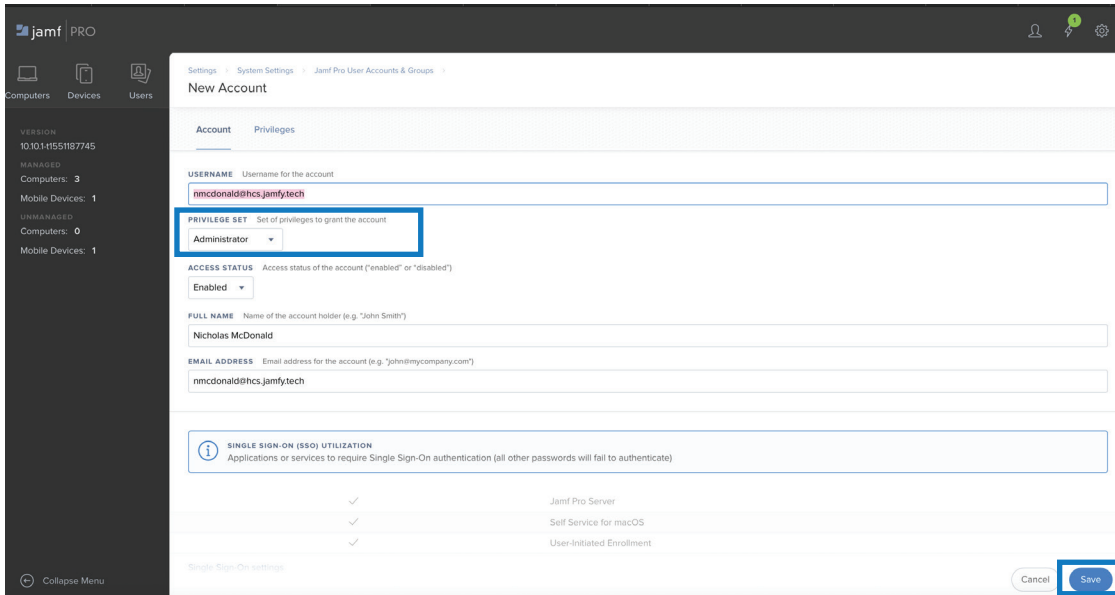
4. Enter the full username (email) of a user in Azure that you wish to add to Jamf Pro, then click Next.



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



6. Click Privilege Set, choose Administrator, then click Save.

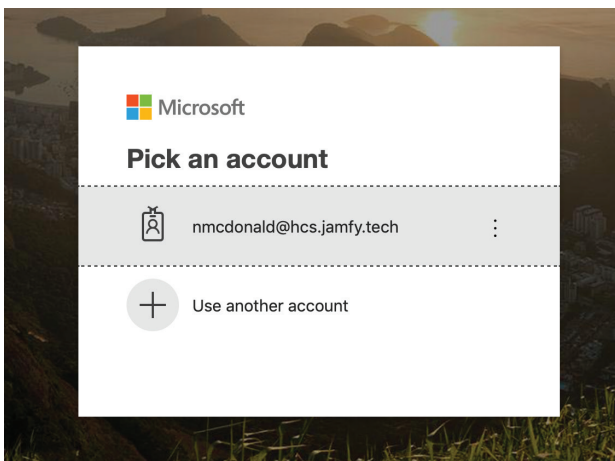


7. Test SSO access to Jamf Pro. In the upper-right corner, click the user silhouette, then choose Logout.

8. Close the web browser tab or window.

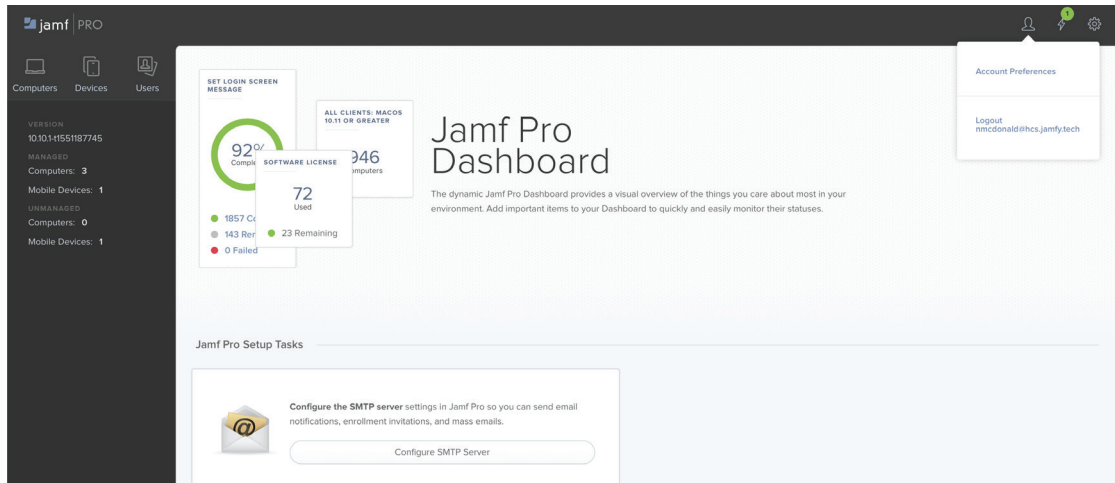
9. Open a new web browser window or tab, then open your Jamf Pro URL.

10. Confirm that the Microsoft account picker is displayed.

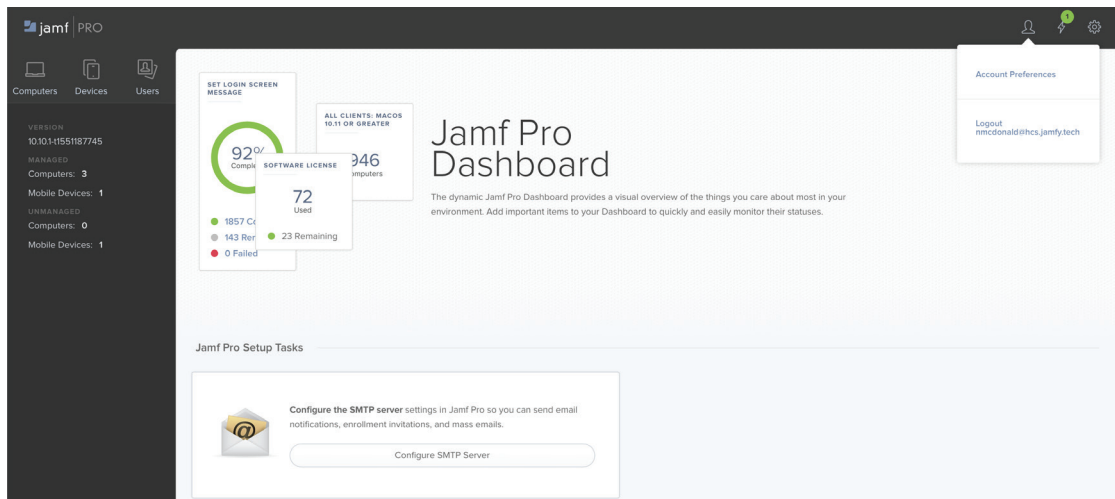




11. If your Azure AD account is displayed, select it. Otherwise, click “Use another account,” enter your Azure AD email address, click Next, enter your Azure AD password, then click “Sign in.” If your web browser offers to save your password, do not save the password.
12. Confirm that you see your Jamf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



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 use the Azure AD credentials to log in to Jamf Pro.



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