Integrate Azure Active Directory with Jamf Pro - A Cloud Only Approach

This guide was created using the following:

- Jamf Pro 10.16 or later
- An Azure Active Directory Managed Domain Services Subscription. If you want use the All Users group, an Azure P1 or P2 license is required.

Requirements

- **A Microsoft Azure Subscription with an administrative account.**
- **A public registered domain name under 15 characters. Microsoft will truncate any domain name over 15 characters.**
- **Access to your domain registrars website to create DNS A and TXT records.**
- **For best results use the Google Chrome web browser.**

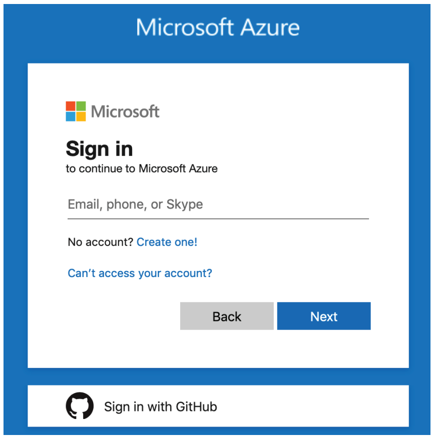
Acronyms and Definitions

- **AAD** Azure Active Directory
- **SSO** Single Sign-On
- **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
- **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

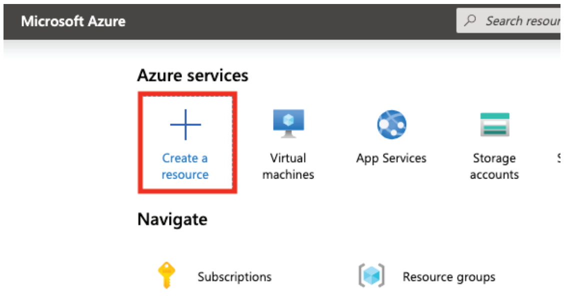
Sections

Section 1 Creating an Azure Active Directory Domain

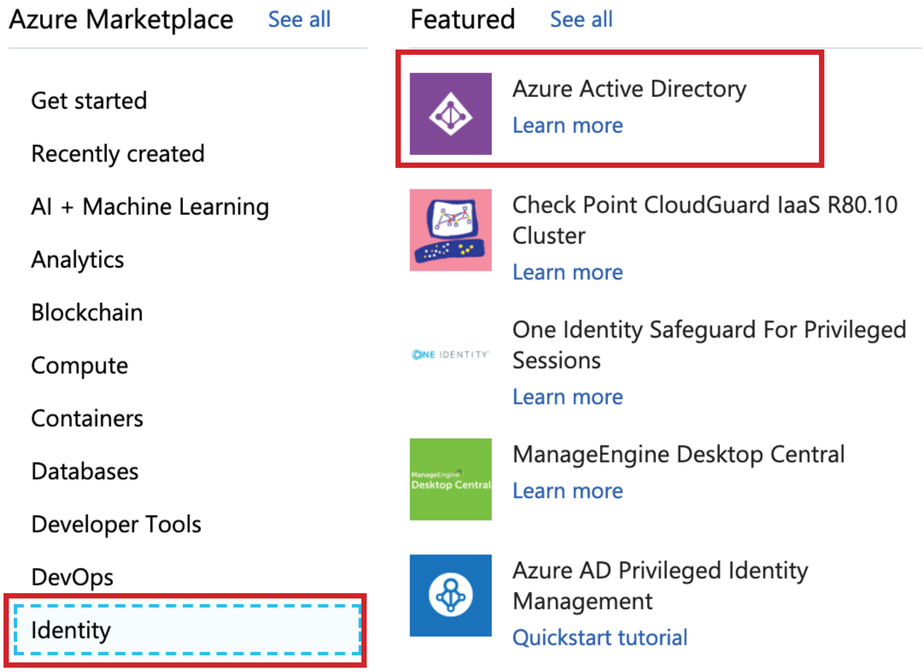
1. Sign in to your Microsoft Azure account here: https://portal.azure.com.



2. Click Create a resource.

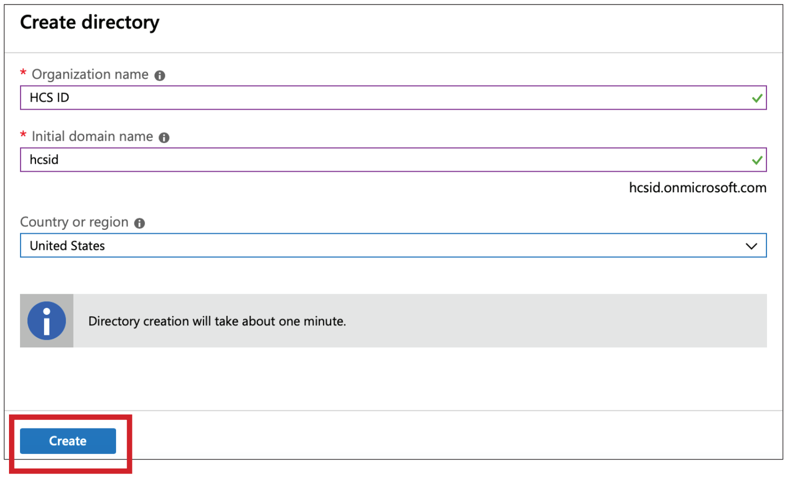


3. Select Identity, then select Azure Active directory.



4. Enter you identity information then click Create. This process will take about a minute to complete.

   NOTE: In this example, the initial creation of the domain name will be hcsid.onmicrosoft.com. We will create a custom domain in a later step so hcsid.com can be used instead of hcsid.onmicrosoft.com. The onmicrosoft.com is required and cannot be deleted.



Create directory

* Organization name: HCS ID

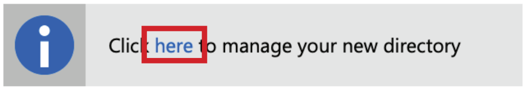
* Initial domain name: hcsid

hcsid.onmicrosoft.com

Country or region: United States

Directory creation will take about one minute.

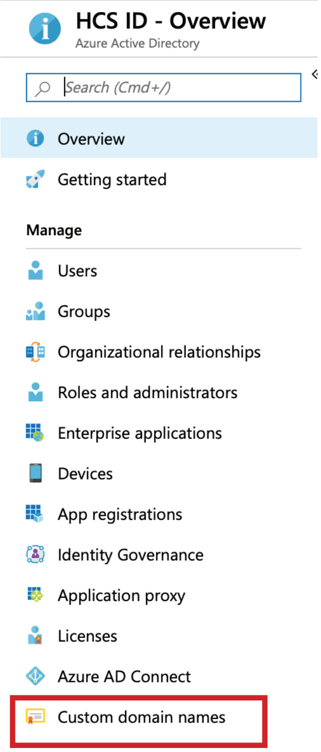
5. Click here to mange your new directory. It may take a few minutes for the directory page to show. Please be patient.



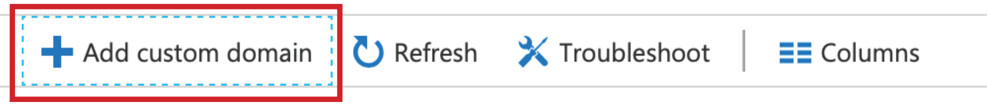
Click here to manage your new directory

6. You will be on the Overview page for your Azure Active Directory Server. Click Custom domain names.

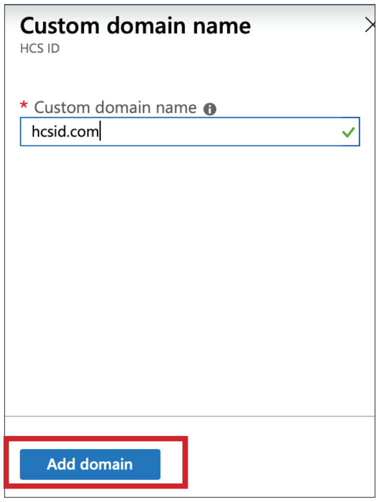
   NOTE: This requires a publicly accessible registered domain.



7. Click Add Custom Domain.



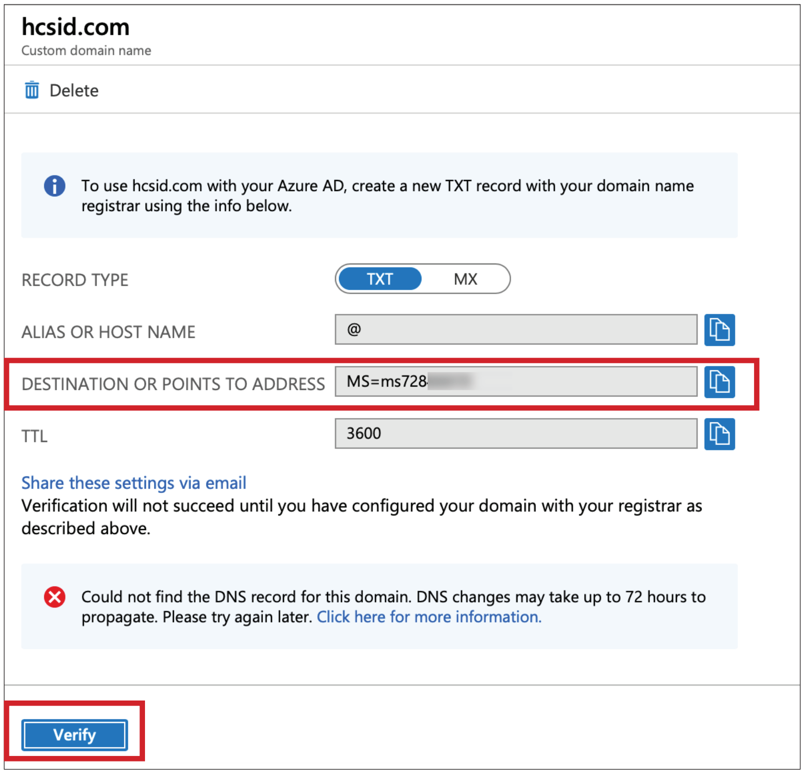
8. Enter your domain name, then click Add Domain.


Custom domain name
HCS ID

* Custom domain name: hcsid.com

9. This step requires you to create a DNS TXT record at your domain registrar. I.E. Hostmonster, GoDaddy, etc. Use the information listed below when creating the DNS TXT record on your domain registrars web site. Select Verify after you complete step 10.

NOTE: If you click Verify and see the error message with the red x below, this means DNS has not propagated yet. It can take up to 72 hrs for this to happen but normally it's ready in about an hour.


hcsid.com
Custom domain name

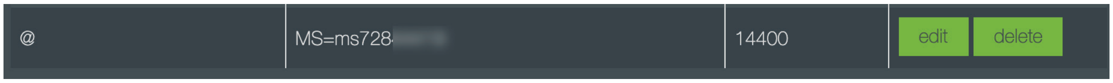
To use hcsid.com with your Azure AD, create a new TXT record with your domain name registrar using the info below.

RECORD TYPE: TXT [✓] MX
ALIAS OR HOST NAME: @
DESTINATION OR POINTS TO ADDRESS: MS=ms728[redacted]
TTL: 3600

Share these settings via email
Verification will not succeed until you have configured your domain with your registrar as described above.

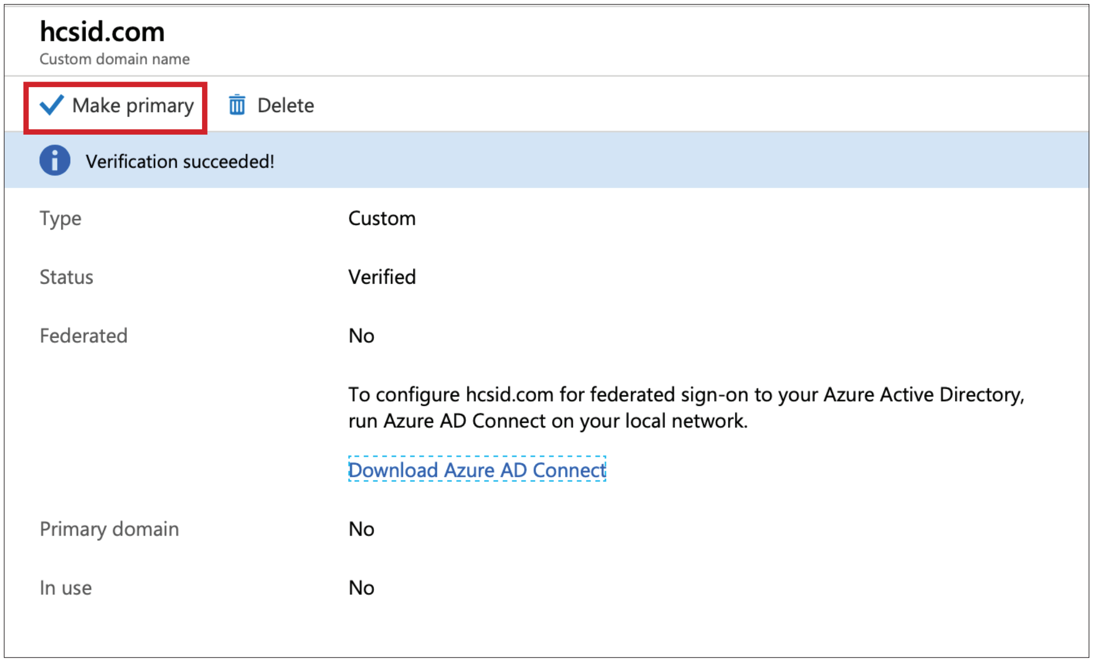
Could not find the DNS record for this domain. DNS changes may take up to 72 hours to propagate. Please try again later. Click here for more information.

10. In this step, I will create a DNS TXT record using my domain registrar account. You will need to do the same on your domain registrars web site.



@	MS=ms728[redacted]	14400	edit delete

11. Once verification is successful, click Make Primary.

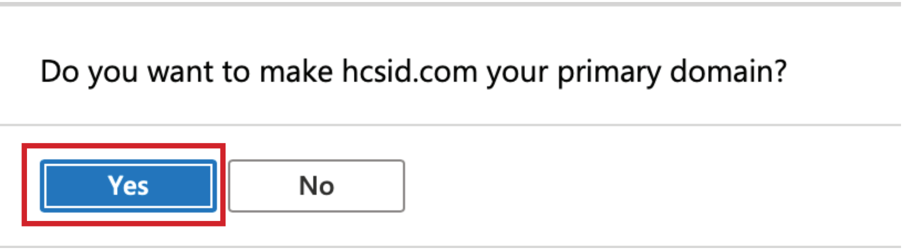


hcsid.com
Custom domain name

Verification succeeded!

Type	Custom
Status	Verified
Federated	No
	To configure hcsid.com for federated sign-on to your Azure Active Directory, run Azure AD Connect on your local network. Download Azure AD Connect
Primary domain	No
In use	No

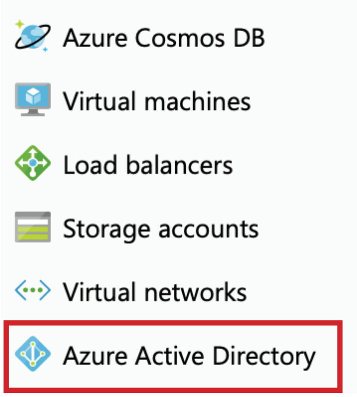
12. Click Yes. This will make your custom domain the primary domain going forward so when you create users they will have the custom domain name instead of the .onmicrosoft.com domain. E.G. kmitnick@hcsid.com. instead of kmitnick@hcsid.onmicrosoft.com. This completes this section



Do you want to make hcsid.com your primary domain?

Section 2: Create User Accounts

1. Click Azure Active Directory.



Azure Cosmos DB

Virtual machines

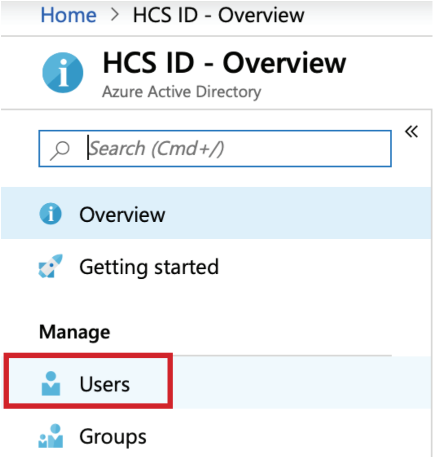
Load balancers

Storage accounts

Virtual networks

Azure Active Directory

2. Click Users.

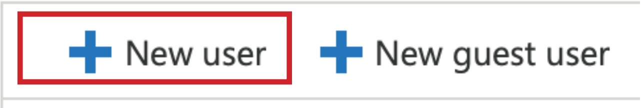


Home > HCS ID - Overview

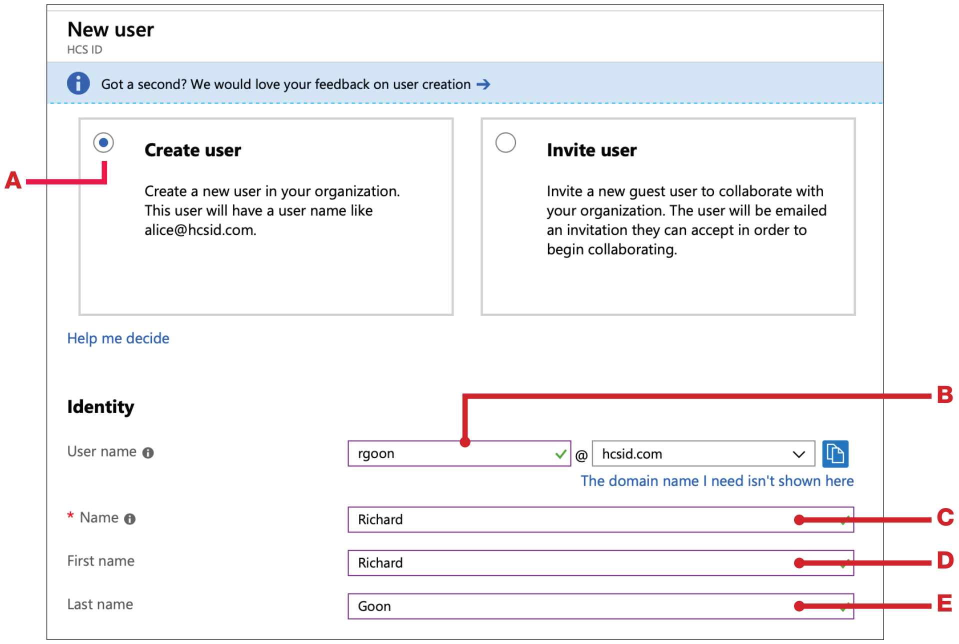
HCS ID - Overview

Azure Active Directory

3. Click New user.



4. Do the following:
    - A. Select Create user
    - B. Add a user Name and make sure the custom domain name is selected from drop down menu.
    - C. Add a Name
    - D. Add a First Name
    - E. Add a Last Name
    - F. Initial Password: Check the Show password box then copy the password. You will need this to login.
    - G. Click Create.



New user
HCS ID

Got a second? We would love your feedback on user creation →

● **Create user**

Create a new user in your organization. This user will have a user name like alice@hcsid.com.

○ **Invite user**

Invite a new guest user to collaborate with your organization. The user will be emailed an invitation they can accept in order to begin collaborating.

Help me decide

Identity

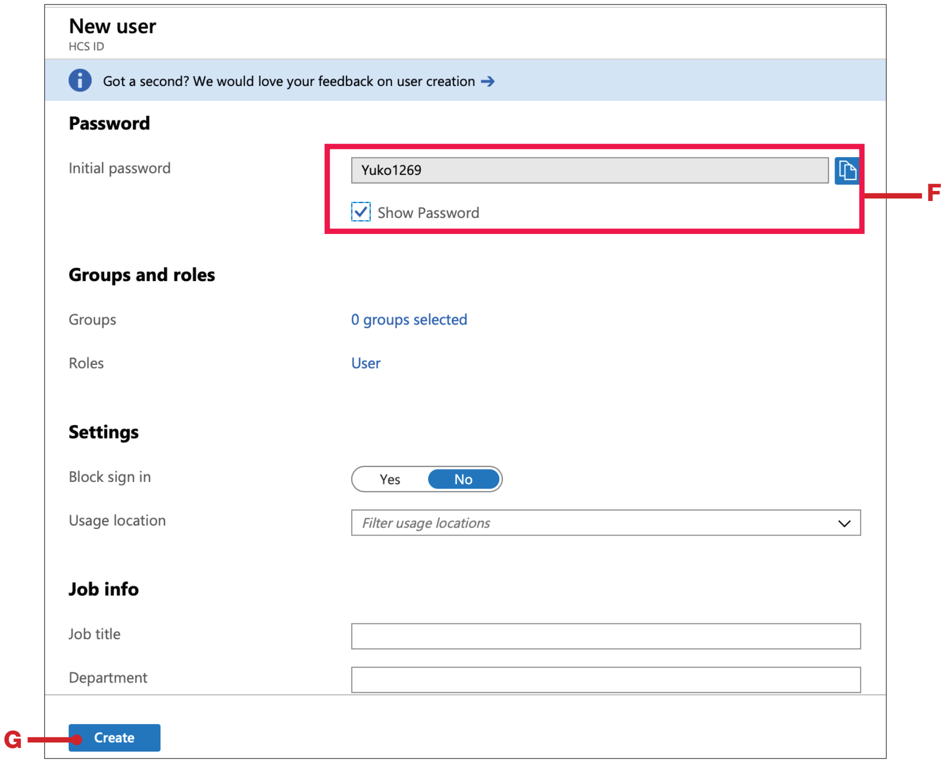
User name: rgoon @ hcsid.com

The domain name I need isn't shown here

* Name: Richard

First name: Richard

Last name: Goon



New user
HCS ID

Got a second? We would love your feedback on user creation →

Password

Initial password: Yuko1269

☑ Show Password

Groups and roles

Groups: 0 groups selected

Roles: User

Settings

Block sign in: Yes [✓ No]

Usage location: *Filter usage locations*

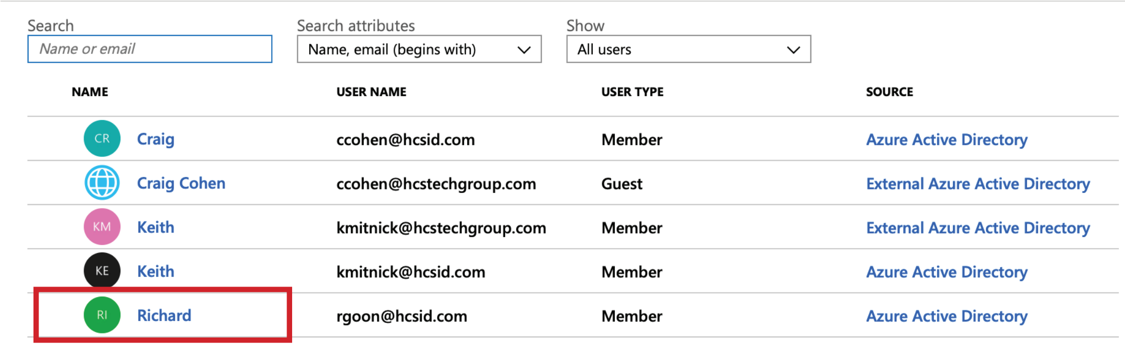
Job info

Job title:

Department:

Create

5. Select the newly created user by clicking on the name. In this example, the new user is Richard.



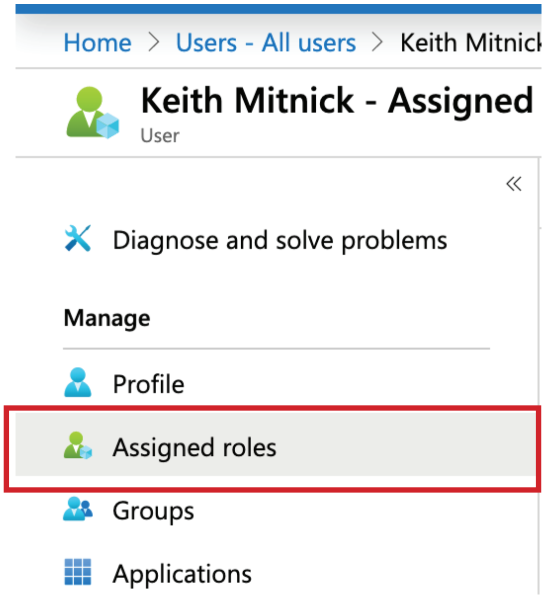
Search: Name or email

Search attributes: Name, email (begins with)

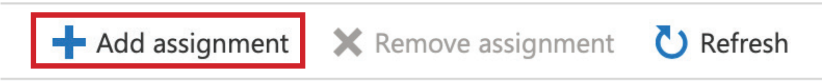
Show: All users

NAME	USER NAME	USER TYPE	SOURCE
CR Craig	ccohen@hcsid.com	Member	Azure Active Directory
Craig Cohen	ccohen@hcstechgroup.com	Guest	External Azure Active Directory
KM Keith	kmitnick@hcstechgroup.com	Member	External Azure Active Directory
KE Keith	kmitnick@hcsid.com	Member	Azure Active Directory
RI Richard	rgoon@hcsid.com	Member	Azure Active Directory

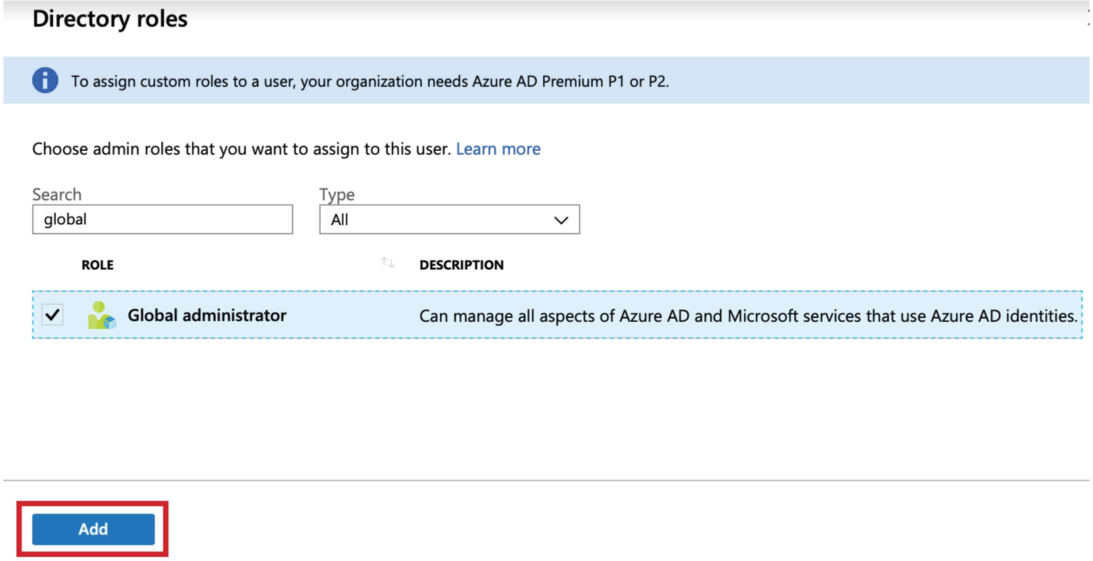
6. Click Assinged role.



7. Click Add assignment.



8. In the search field, enter the required role for the user. Select the user role checkbox, then click Add. This completes this section.



Directory roles

To assign custom roles to a user, your organization needs Azure AD Premium P1 or P2.

Choose admin roles that you want to assign to this user. Learn more

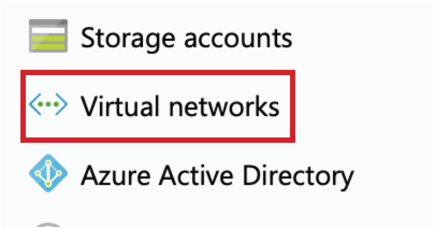
Search: global

Type: All

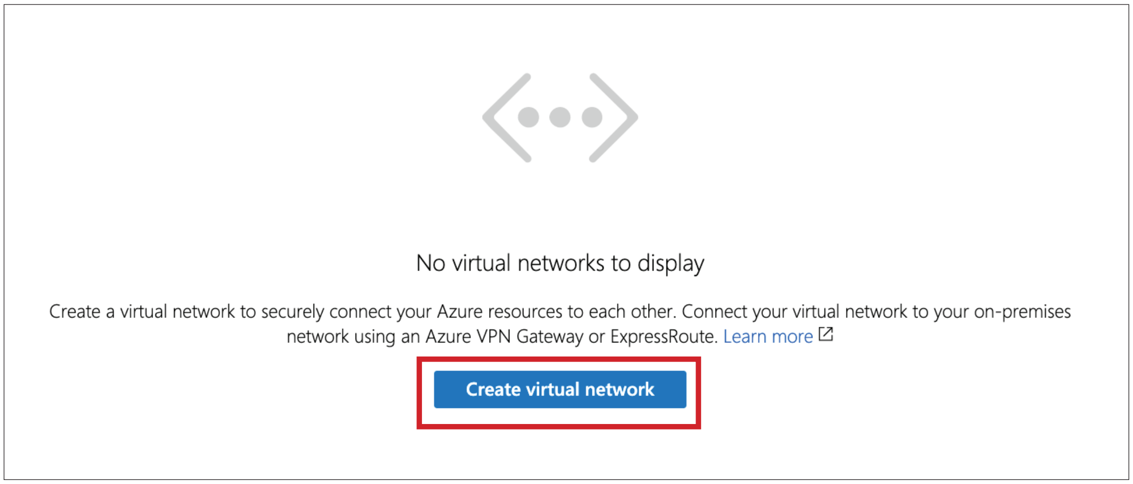
	ROLE	DESCRIPTION
☑	Global administrator	Can manage all aspects of Azure AD and Microsoft services that use Azure AD identities.

Section 3: Configure a Virtual Network and Secure LDAP

1. Click Virtual networks from the sidebar.



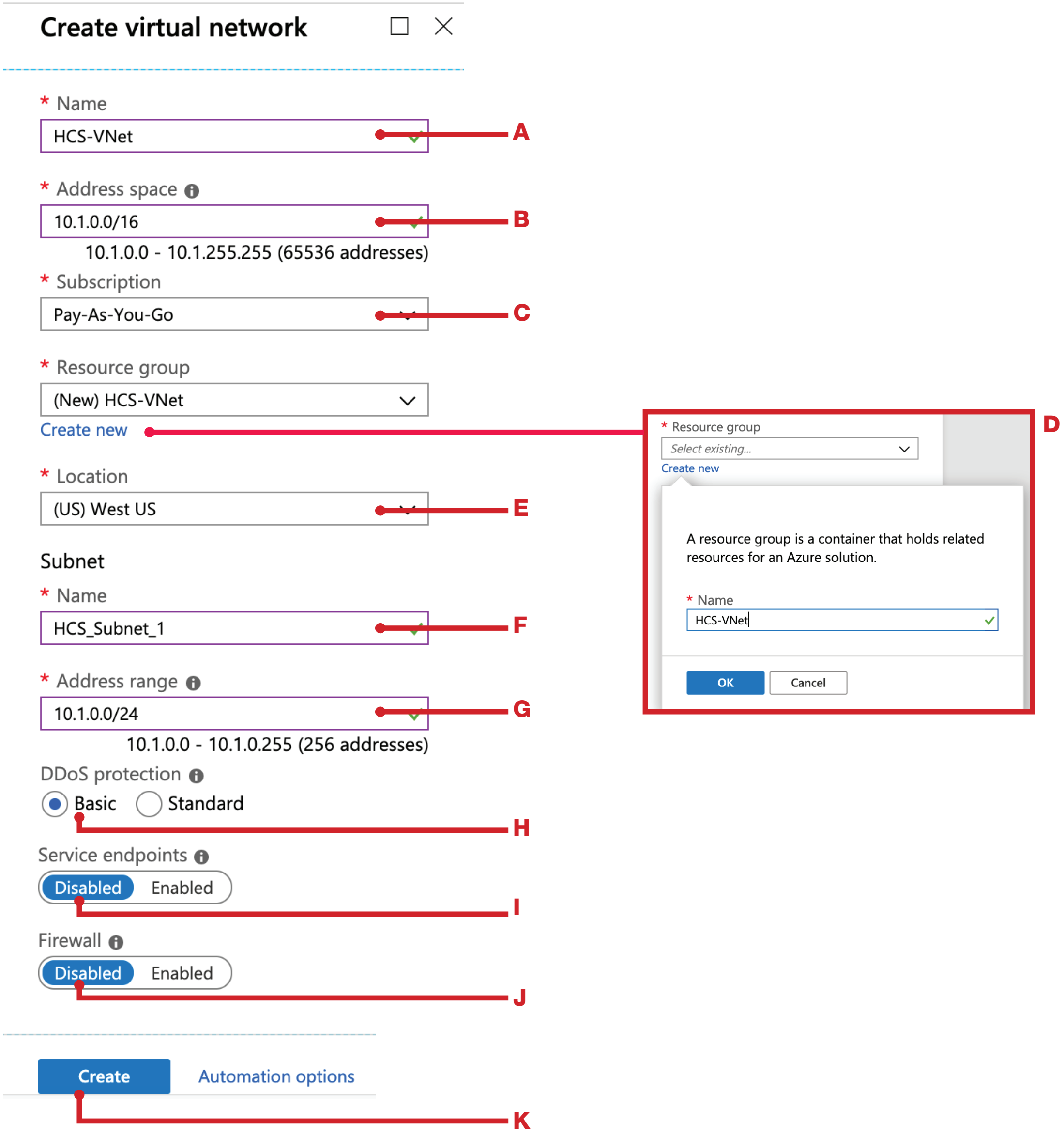
2. Click Create virtual network


No virtual networks to display

Create a virtual network to securely connect your Azure resources to each other. Connect your virtual network to your on-premises network using an Azure VPN Gateway or ExpressRoute. Learn more

3. Enter the following:

   A. Provide a Name for your network.
   B. Address Space
   C. Select your subscription
   D. Create a new resource group if needed.
   E. Location - take note of the location. We will need it in a later step.
   F. Subnet Name
   G. Subnet Address Range
   H. DDoS protection - set to Basic
   I. Service Endpoints - Disabled
   J. Firewall - Disabled
   K. Click Create.



Create virtual network

* Name
HCS-VNet

* Address space
10.1.0.0/16
10.1.0.0 - 10.1.255.255 (65536 addresses)

* Subscription
Pay-As-You-Go

* Resource group
(New) HCS-VNet
Create new

* Location
(US) West US

Subnet

* Name
HCS_Subnet_1

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

DDoS protection
● Basic ○ Standard

Service endpoints
Disabled | Enabled

Firewall
Disabled | Enabled

Create | Automation options

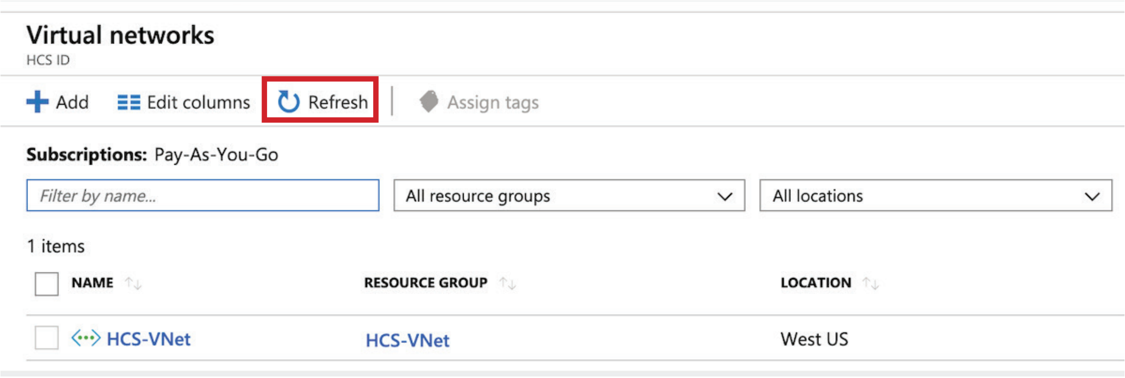
* Resource group
Select existing...
Create new

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

* Name
HCS-VNet

OK | Cancel

4. It can take a few minutes to setup the virtual network. Click the refresh button if necessary.



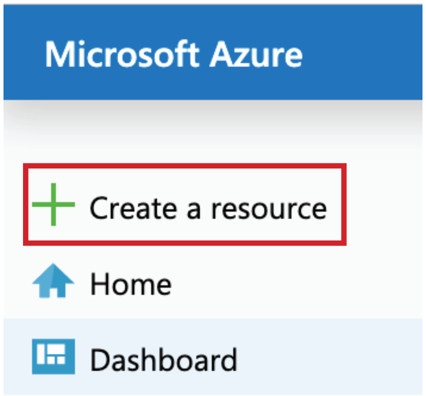
Subscriptions: Pay-As-You-Go

Filter by name...

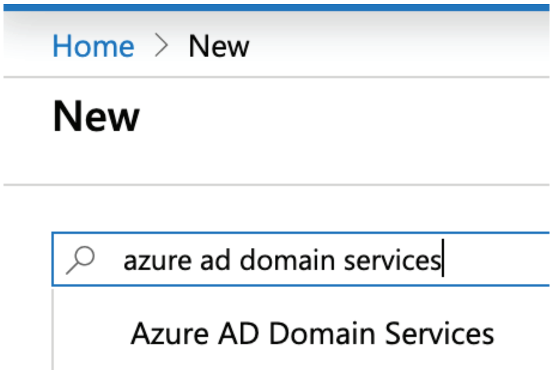
1 items

NAME	RESOURCE GROUP	LOCATION
HCS-VNet	HCS-VNet	West US

5. Click Create a resources from the sidebar.



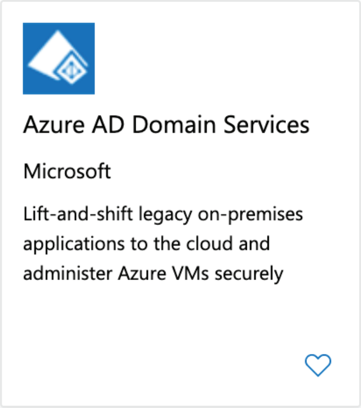
6. In the search field, enter Azure AD Domain Services then press enter.



azure ad domain services

Azure AD Domain Services

7. Select Azure AD Domain Services.

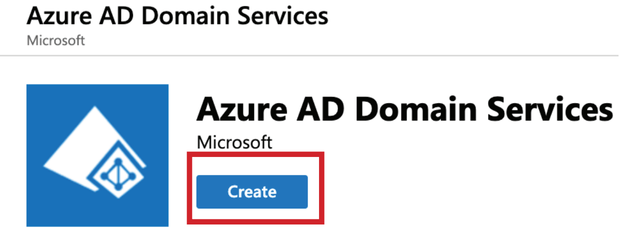


Azure AD Domain Services

Microsoft

Lift-and-shift legacy on-premises applications to the cloud and administer Azure VMs securely

8. Click Create.



Azure AD Domain Services

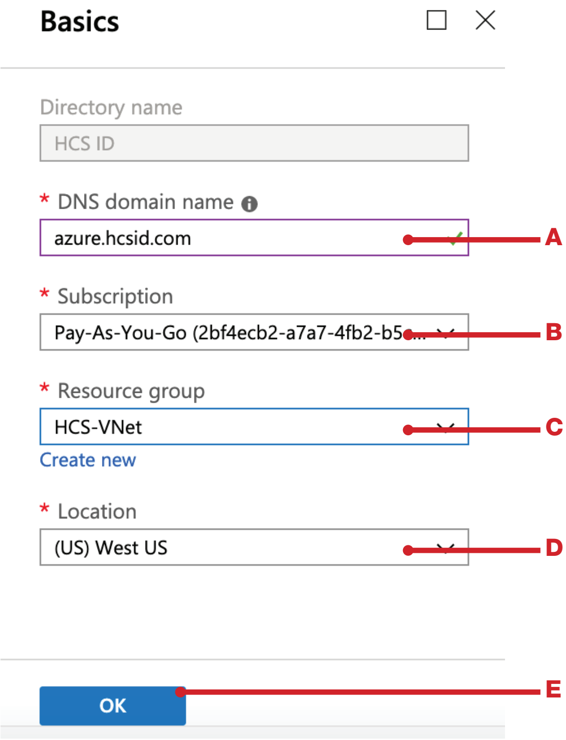
Microsoft

Azure AD Domain Services

Microsoft

9. Enter the following:

A. DNS domain name: Enter a fully qualified domain name. *NOTE: A subdomain is NOT required. You can use hcsid.com in this field.*
B. Subscription: Select your subscription type
C. Resource group: Select your resource group
D. Location: Select your location. Make sure to choose the same location as shown in step 3.
E. Click OK.



Basics

Directory name: HCS ID

* DNS domain name: azure.hcsid.com

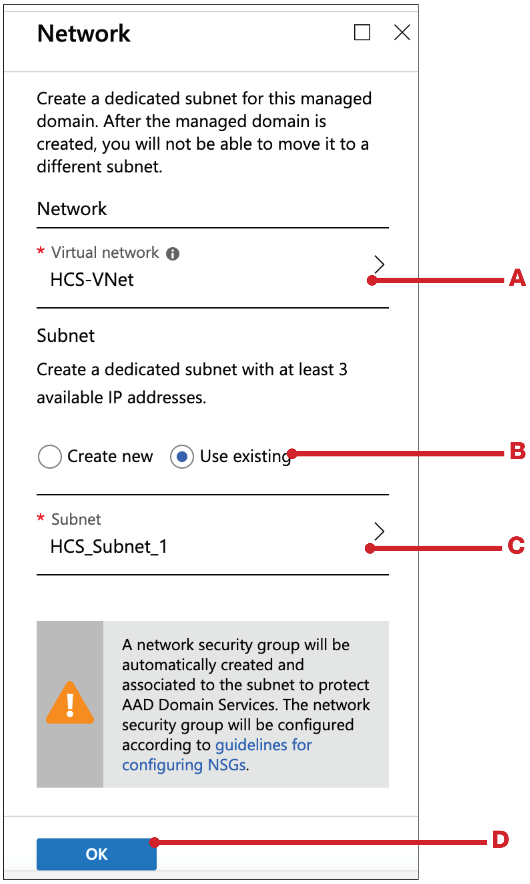
* Subscription: Pay-As-You-Go (2bf4ecb2-a7a7-4fb2-b5...

* Resource group: HCS-VNet

* Location: (US) West US

10. Enter the following:

    A. Network: Select your Virtual network
    B. Subnet: Select Use existing
    C. Subnet: Select your subnet
    D. Select OK



Network

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.

Network

* Virtual network: HCS-VNet

Subnet

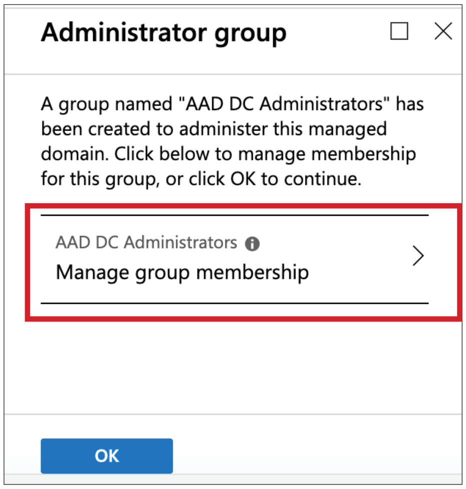
Create a dedicated subnet with at least 3 available IP addresses.

○ Create new ● Use existing

* Subnet: HCS_Subnet_1

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.

11. Select Manage group membership.



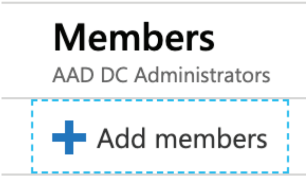
Administrator group

A group named "AAD DC Administrators" has been created to administer this managed domain. Click below to manage membership for this group, or click OK to continue.

AAD DC Administrators

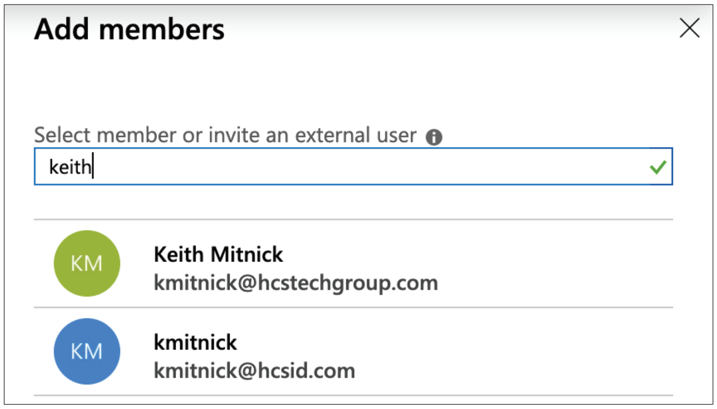
Manage group membership

12. Select Add members.


Members

AAD DC Administrators

13. Search for a user, then select the user.


Add members

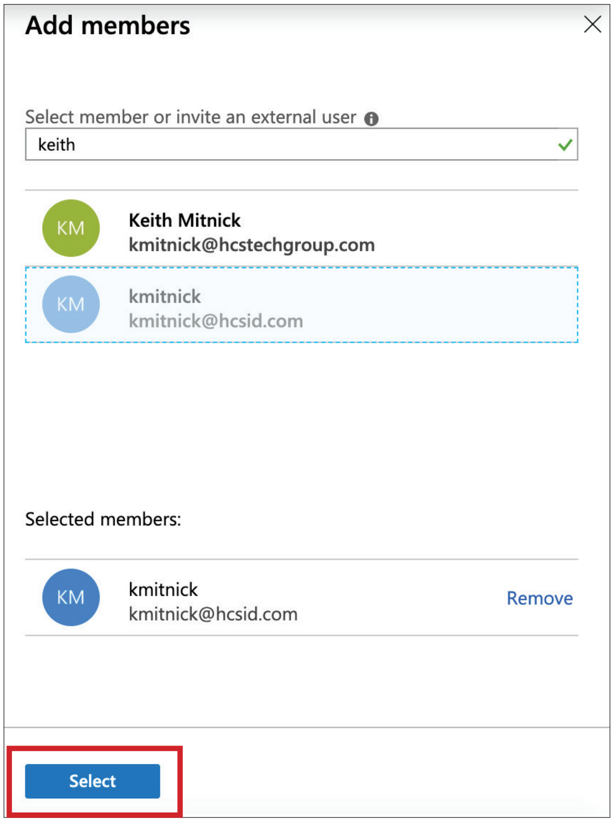
Select member or invite an external user

keith

KM Keith Mitnick
kmitnick@hcstechgroup.com

KM kmitnick
kmitnick@hcsid.com

14. Press Select button.


Add members

Select member or invite an external user

keith

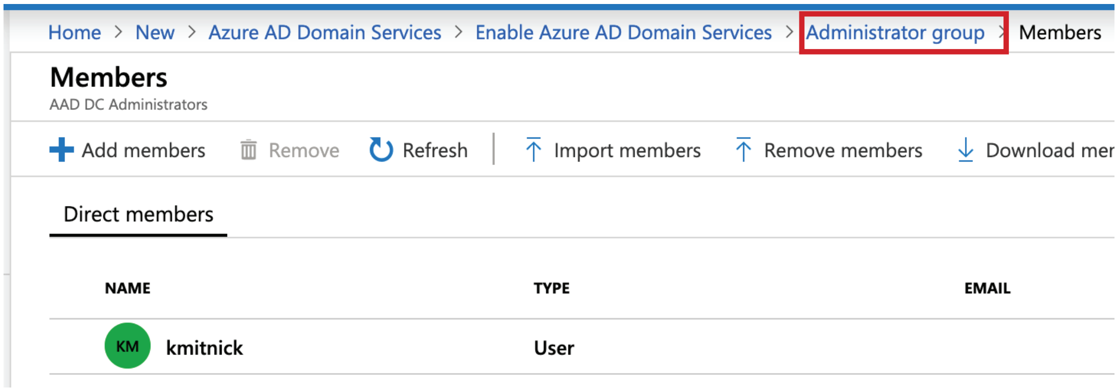
KM Keith Mitnick
kmitnick@hcstechgroup.com

KM kmitnick
kmitnick@hcsid.com

Selected members:

KM kmitnick
kmitnick@hcsid.com

15. The user will show up in the member section. Select the Administrator group breadcrumb.

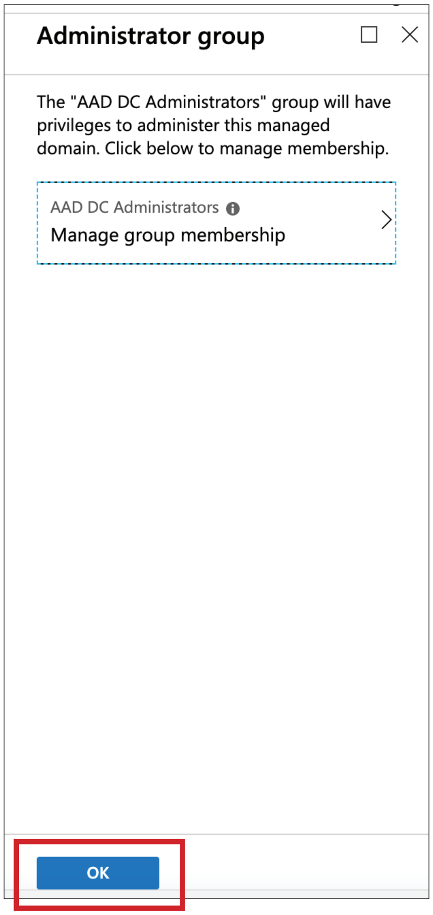

Home > New > Azure AD Domain Services > Enable Azure AD Domain Services > Administrator group > Members
Add members
Remove
Refresh
Import members
Remove members
Download mer
Direct members

Members

AAD DC Administrators

NAME	TYPE	EMAIL
KM kmitnick	User	

16. Select OK.



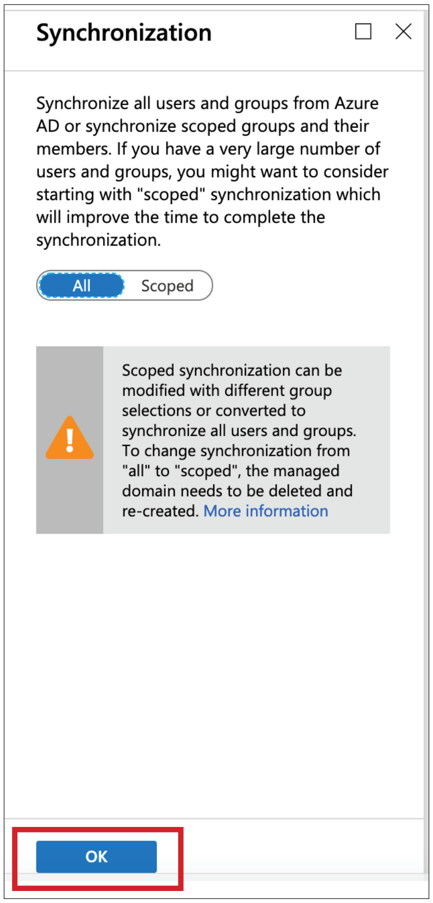
Administrator group

The "AAD DC Administrators" group will have privileges to administer this managed domain. Click below to manage membership.

AAD DC Administrators

Manage group membership

17. Select All, then select OK.

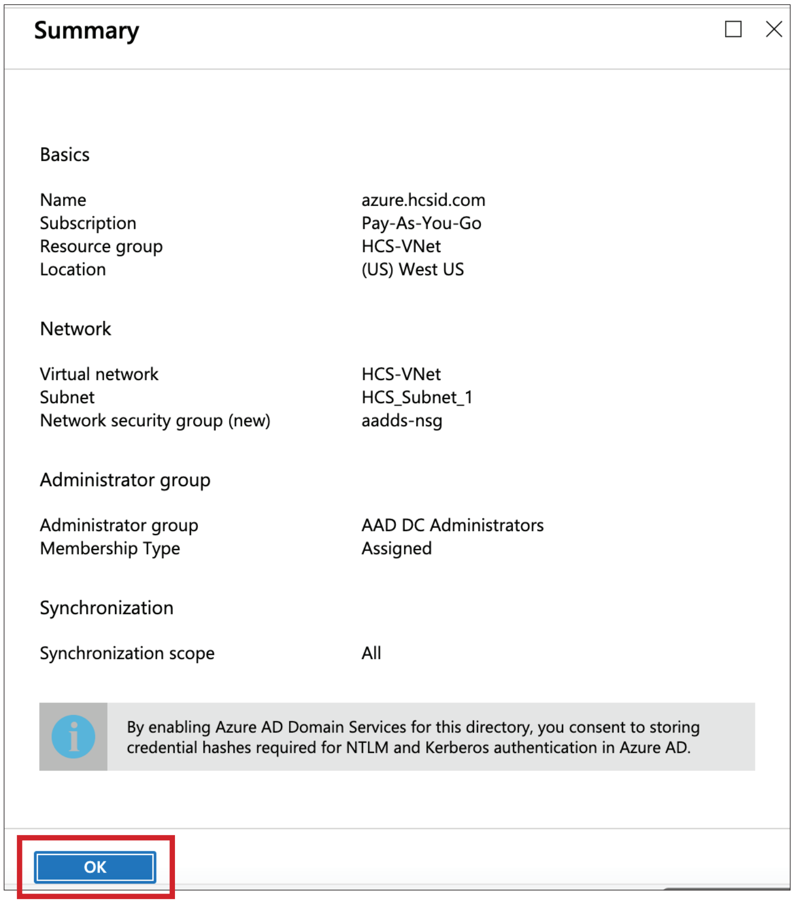


Synchronization

Synchronize all users and groups from Azure AD or synchronize scoped groups and their members. If you have a very large number of users and groups, you might want to consider starting with "scoped" synchronization which will improve the time to complete the synchronization.

Scoped synchronization can be modified with different group selections or converted to synchronize all users and groups. To change synchronization from "all" to "scoped", the managed domain needs to be deleted and re-created. More information

18. Make sure everything looks correct in the summary, then select OK.



Summary

Basics

Name	azure.hcsid.com
Subscription	Pay-As-You-Go
Resource group	HCS-VNet
Location	(US) West US

Network

Virtual network	HCS-VNet
Subnet	HCS_Subnet_1
Network security group (new)	aadds-nsg

Administrator group

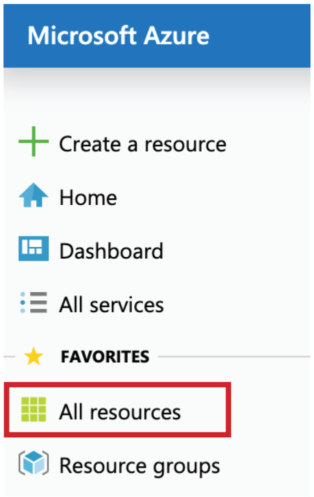
Administrator group	AAD DC Administrators
Membership Type	Assigned

Synchronization

Synchronization scope	All

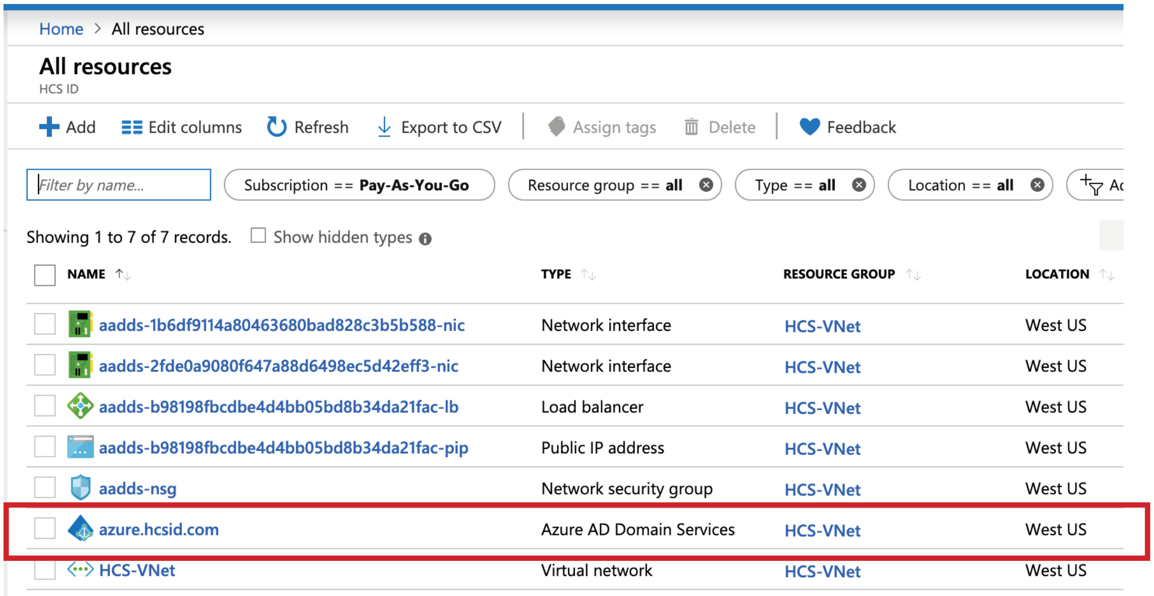
By enabling Azure AD Domain Services for this directory, you consent to storing credential hashes required for NTLM and Kerberos authentication in Azure AD.

19. Select All resources from the sidebar.



20. Select the hostname for your Azure AD Domain Service. E.G. azure.hcsid.com.

NOTE: It can take up to 1 hour for all resources to show up in the list. Please be patient.



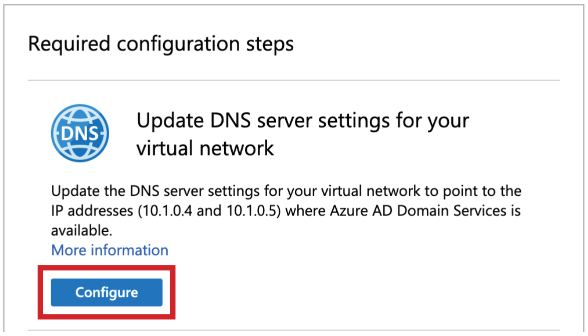
All resources
HCS ID

Filter by name...   Subscription == **Pay-As-You-Go**   Resource group == **all**   Type == **all**   Location == **all**

Showing 1 to 7 of 7 records.   □ Show hidden types

□	NAME	TYPE	RESOURCE GROUP	LOCATION
□	aadds-1b6df9114a80463680bad828c3b5b588-nic	Network interface	HCS-VNet	West US
□	aadds-2fde0a9080f647a88d6498ec5d42eff3-nic	Network interface	HCS-VNet	West US
□	aadds-b98198fbcdbe4d4bb05bd8b34da21fac-lb	Load balancer	HCS-VNet	West US
□	aadds-b98198fbcdbe4d4bb05bd8b34da21fac-pip	Public IP address	HCS-VNet	West US
□	aadds-nsg	Network security group	HCS-VNet	West US
□	azure.hcsid.com	Azure AD Domain Services	HCS-VNet	West US
□	HCS-VNet	Virtual network	HCS-VNet	West US

21. In the Required configuration steps section, select Configure.



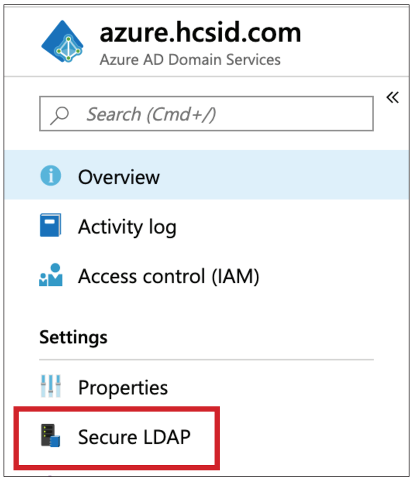
Required configuration steps

Update DNS server settings for your virtual network

Update the DNS server settings for your virtual network to point to the IP addresses (10.1.0.4 and 10.1.0.5) where Azure AD Domain Services is available.
More information

22. From the sidebar, select Secure LDAP.

NOTE: Keep this browser page open as we will need it in a later step.

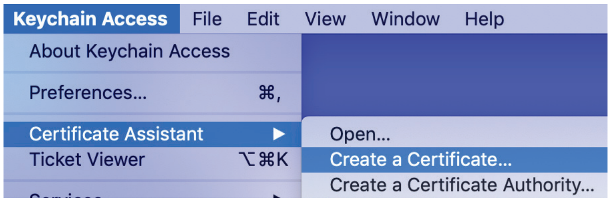


azure.hcsid.com
Azure AD Domain Services

23. In this step we will create a certificate on your Mac to use with secure LDAP in Azure. Open Keychain Access, located in /Applications/Utilities.

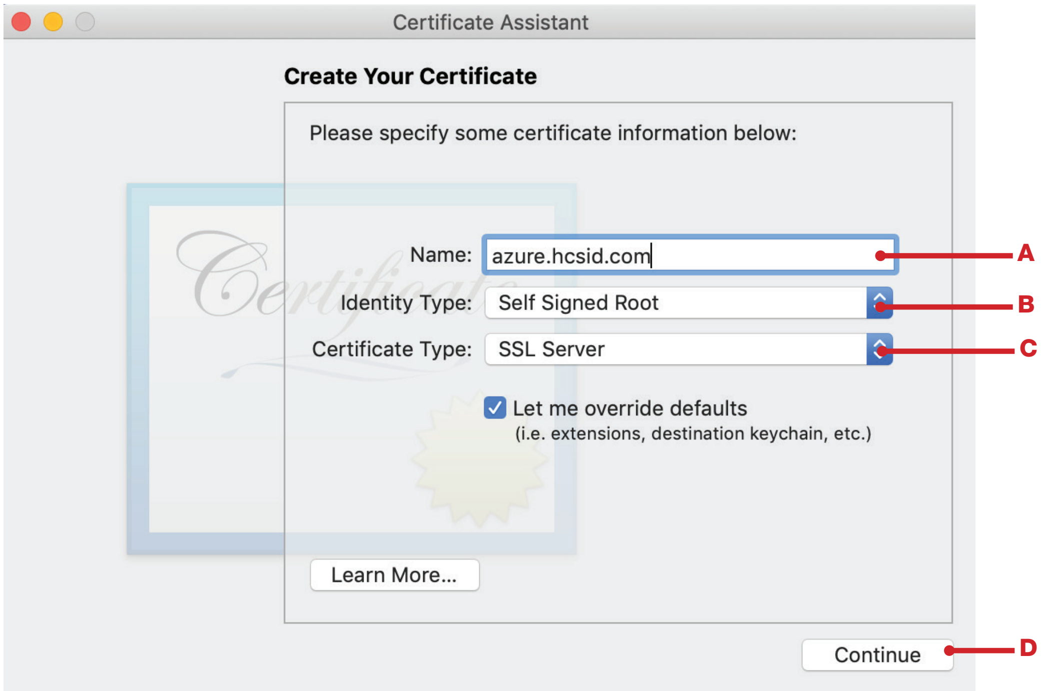
Keychain Access

24. From the Keychain Access menu, select Certificate Assistant, then select Create a Certificate.



25. In the Certificate Assistant window, enter the following:

A. Name - Enter your DNS Name. E.G. azure.hcsid.com
B. Identity Type - choose Self Signed Root.
C. Certificate Type - choose SSL Server.
D. Select the option Let me override defaults.
E. Select Continue.


Certificate Assistant

Create Your Certificate

Please specify some certificate information below:

Name: azure.hcsid.com

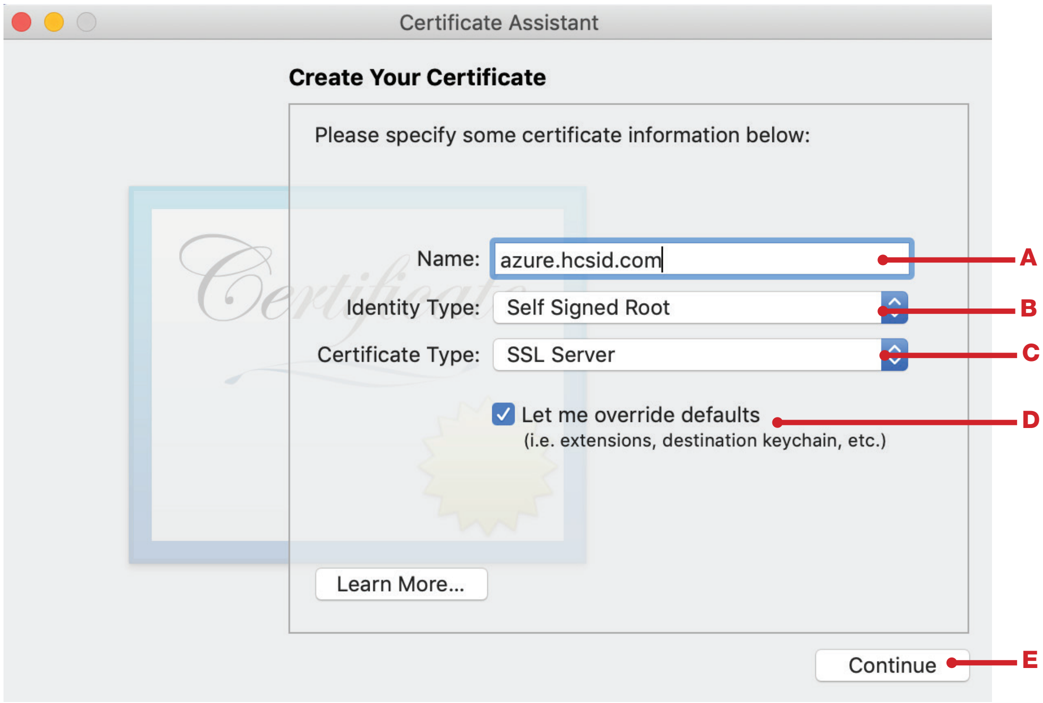
Identity Type: Self Signed Root

Certificate Type: SSL Server

☑ Let me override defaults
(i.e. extensions, destination keychain, etc.)

26. In the Certificate Assistant window, enter the following:

A. Name - Enter your DNS Name. E.G. azure.hcsid.com
B. Identity Type - choose Self Signed Root.
C. Certificate Type - choose SSL Server.
D. Select the option Let me override defaults.
E. Select Continue.



Please specify some certificate information below:

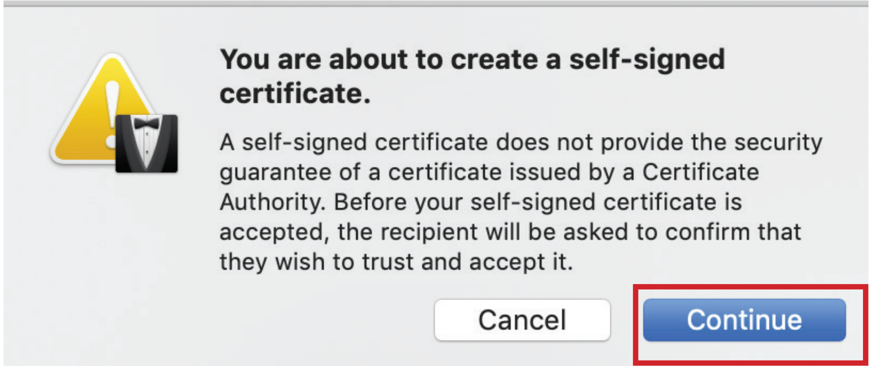
Name: azure.hcsid.com

Identity Type: Self Signed Root

Certificate Type: SSL Server

☑ Let me override defaults
(i.e. extensions, destination keychain, etc.)

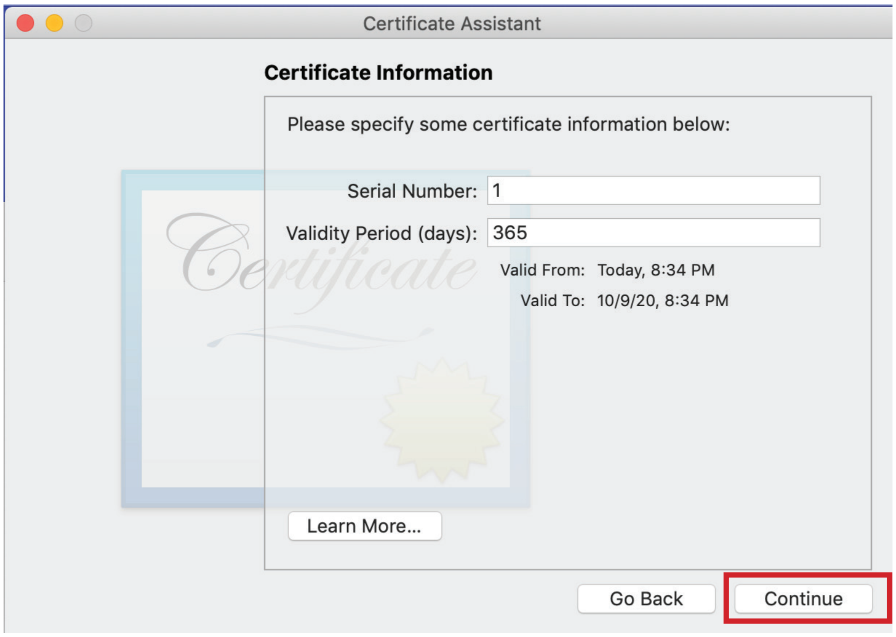
27. Select Continue.



You are about to create a self-signed certificate.

A self-signed certificate does not provide the security guarantee of a certificate issued by a Certificate Authority. Before your self-signed certificate is accepted, the recipient will be asked to confirm that they wish to trust and accept it.

28. Leave the default settings, then select Continue.



Certificate Information

Please specify some certificate information below:

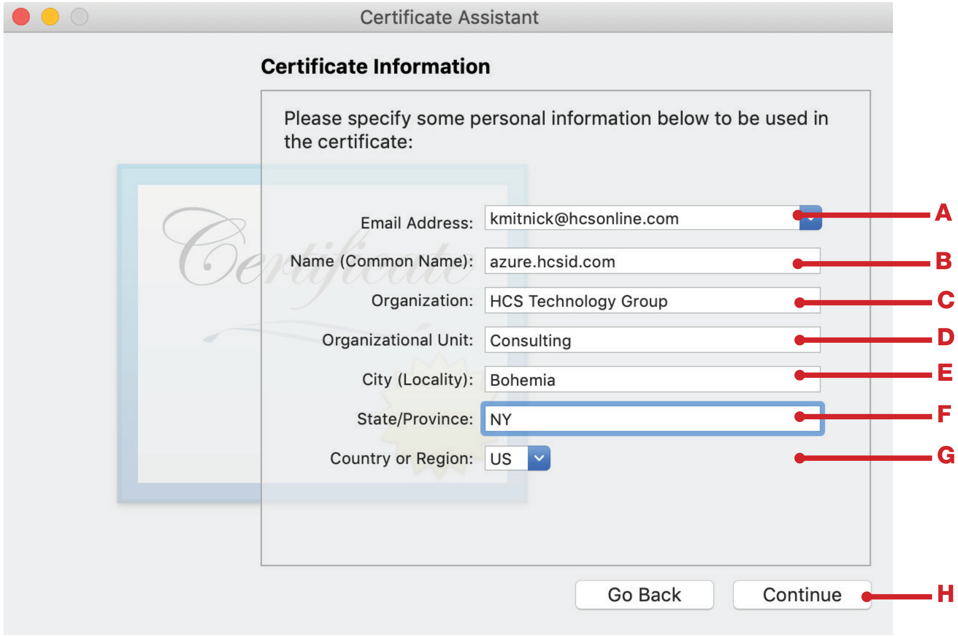
Serial Number: 1

Validity Period (days): 365

Valid From: Today, 8:34 PM

Valid To: 10/9/20, 8:34 PM

29. In the Certificate Information window, enter the following:
    A. Email Address - Enter your email address.
    B. Name - Enter your hostname. E.G. azure.hcsid.com
    C. Organization- Enter your organization name.
    D. Organizational Unit - Enter your Organizational Unit.
    E. City - Enter your city.
    F. State - Enter your state.
    G. Country - Enter your country.
    H. Select Continue.



Certificate Information

Please specify some personal information below to be used in the certificate:

Email Address: kmitnick@hcsonline.com

Name (Common Name): azure.hcsid.com

Organization: HCS Technology Group

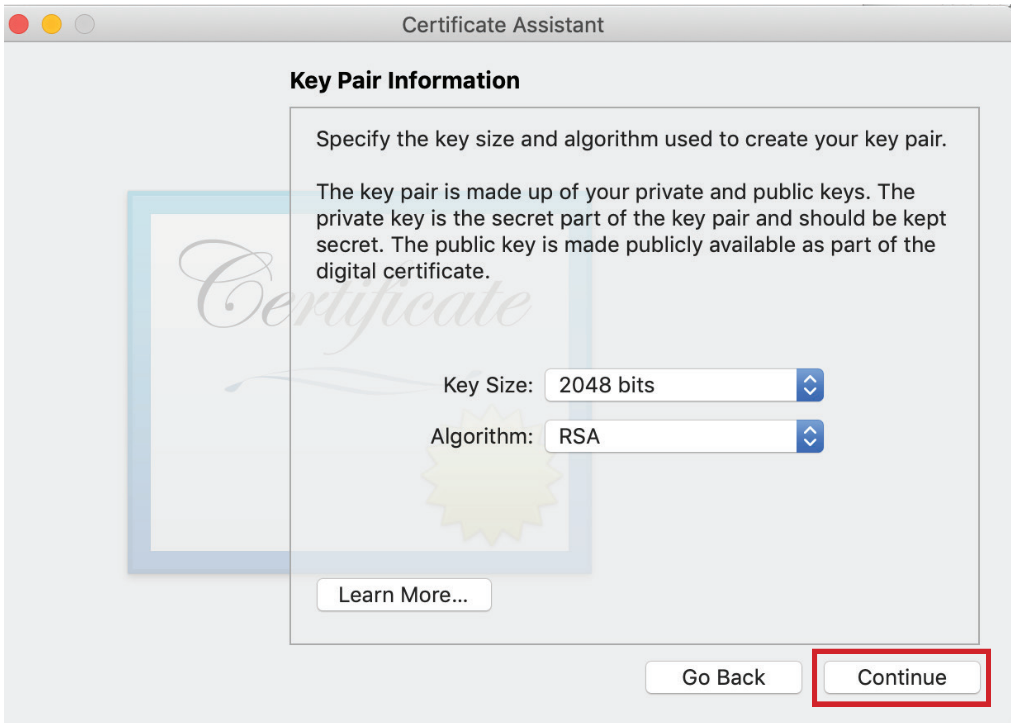
Organizational Unit: Consulting

City (Locality): Bohemia

State/Province: NY

Country or Region: US

30.Leave the default settings, then select Continue.



Certificate Assistant

Key Pair Information

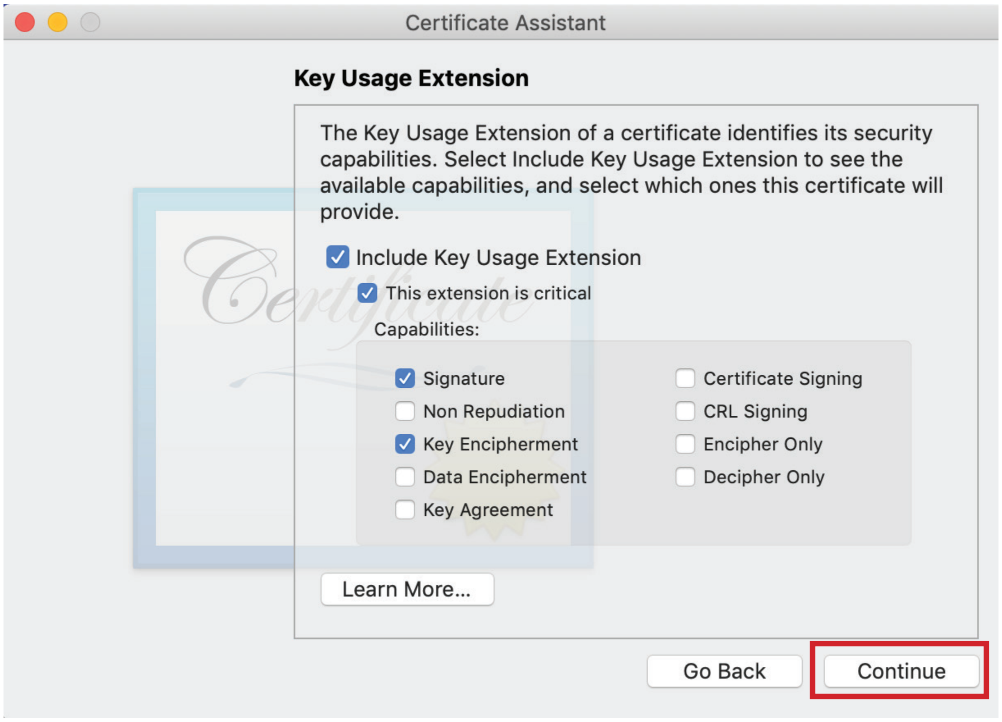
Specify the key size and algorithm used to create your key pair.

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

31. Leave the default settings, then select 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.

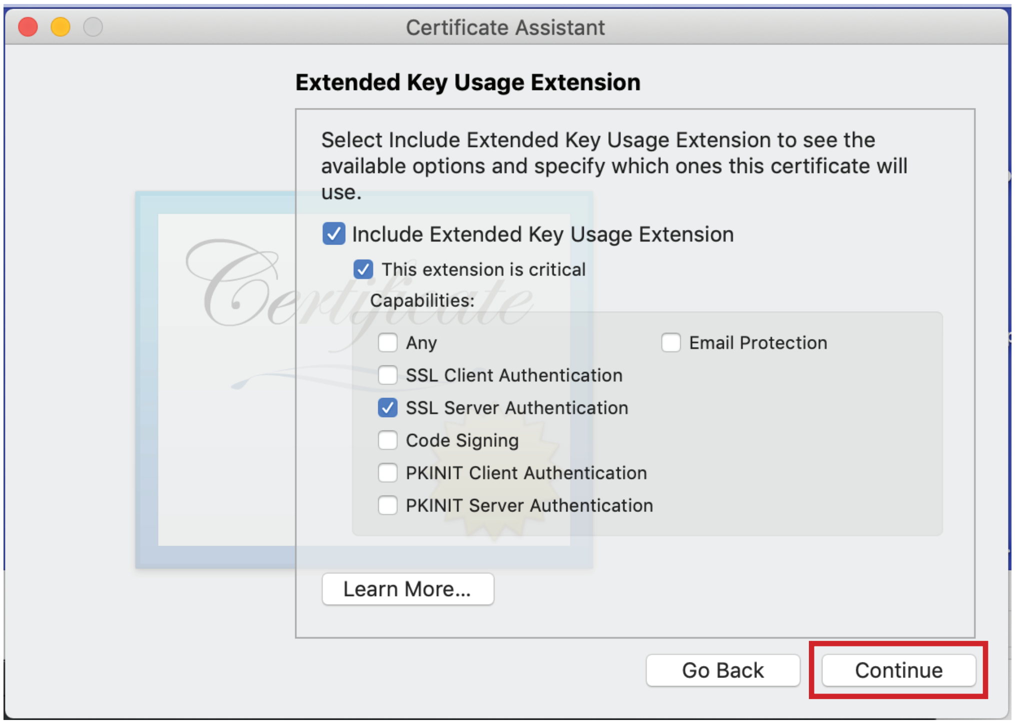
☑ Include Key Usage Extension

☑ This extension is critical

Capabilities:

☑ Signature
□ Non Repudiation
☑ Key Encipherment
□ Data Encipherment
□ Key Agreement
□ Certificate Signing
□ CRL Signing
□ Encipher Only
□ Decipher Only

32. Leave the default settings, then select Continue.



Extended Key Usage Extension

Select Include Extended Key Usage Extension to see the available options and specify which ones this certificate will use.

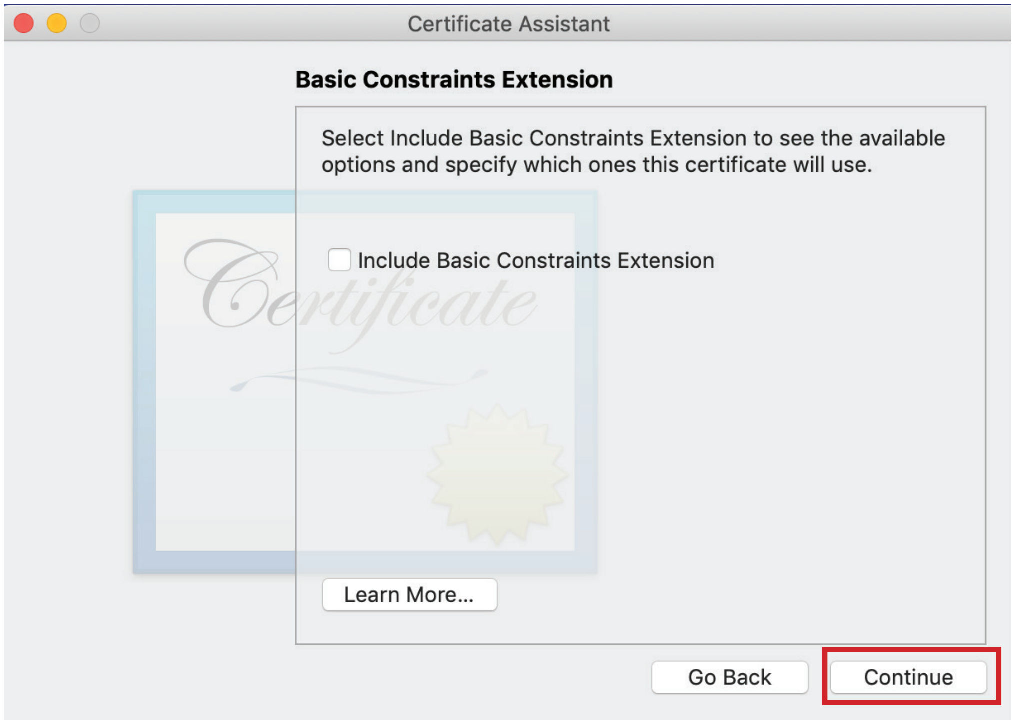
☑ Include Extended Key Usage Extension

☑ This extension is critical

Capabilities:

- ☐ Any
- ☐ Email Protection
- ☐ SSL Client Authentication
- ☑ SSL Server Authentication
- ☐ Code Signing
- ☐ PKINIT Client Authentication
- ☐ PKINIT Server Authentication

33. Leave the default settings, then select Continue.



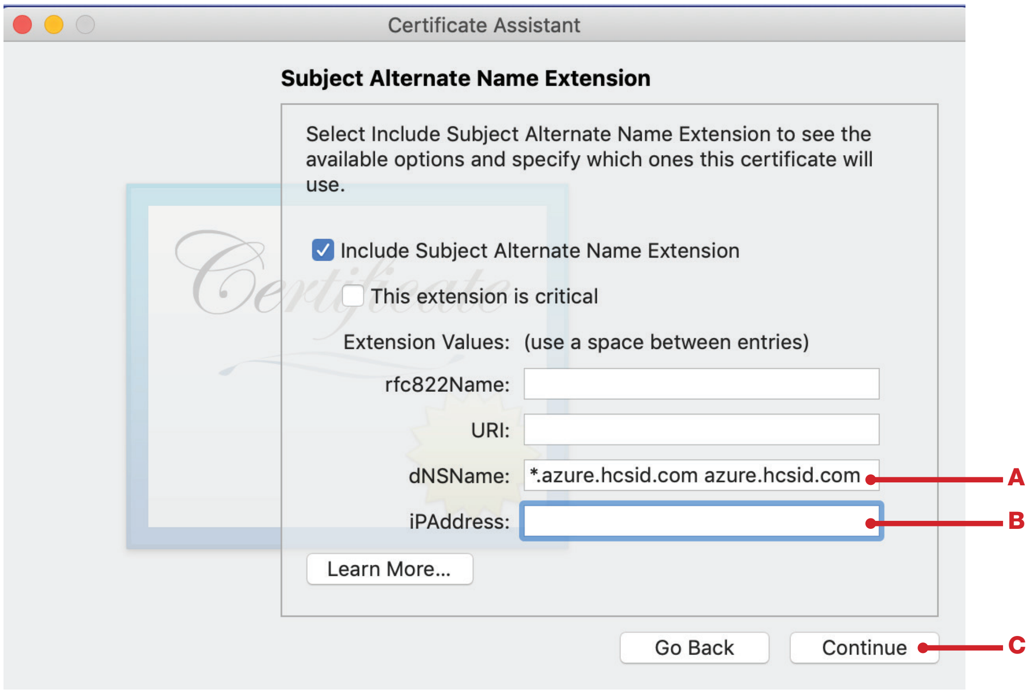
Basic Constraints Extension

Select Include Basic Constraints Extension to see the available options and specify which ones this certificate will use.

☐ Include Basic Constraints Extension

34. Configure the following:

A. dNSName: Enter YOUR dns hostname as shown in the picture. There MUST be a space between the two entries.
B. iPAddress: Clear all data from this field.
C. Select Continue.



Subject Alternate Name Extension

Select Include Subject Alternate Name Extension to see the available options and specify which ones this certificate will use.

☑ Include Subject Alternate Name Extension

□ This extension is critical

Extension Values: (use a space between entries)

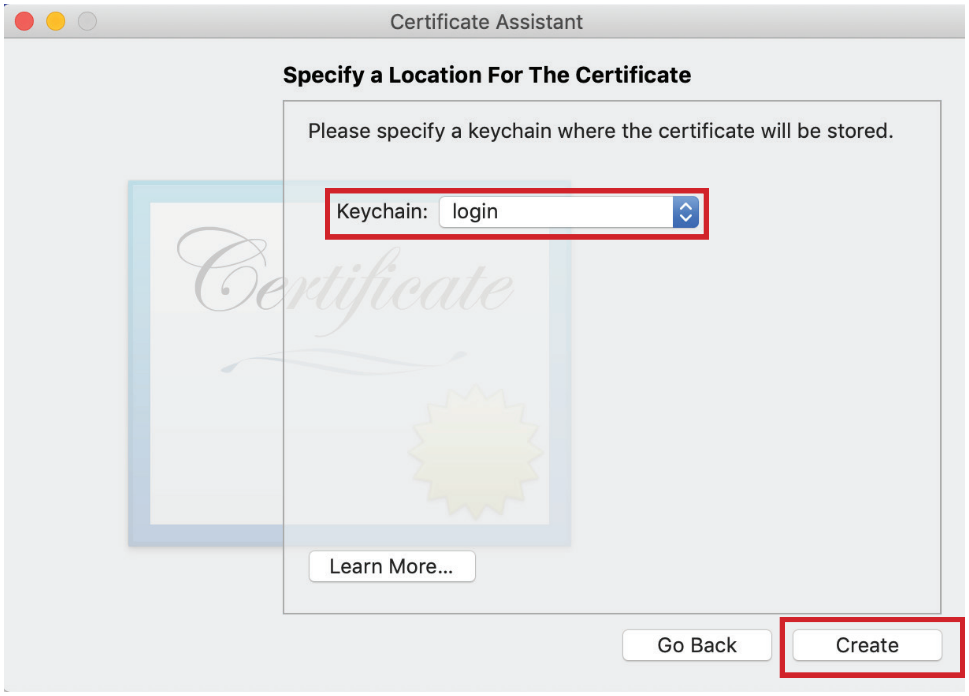
rfc822Name:

URI:

dNSName: *.azure.hcsid.com azure.hcsid.com

iPAddress:

35. Make sure login is set in the dropdown menu, then click Create.

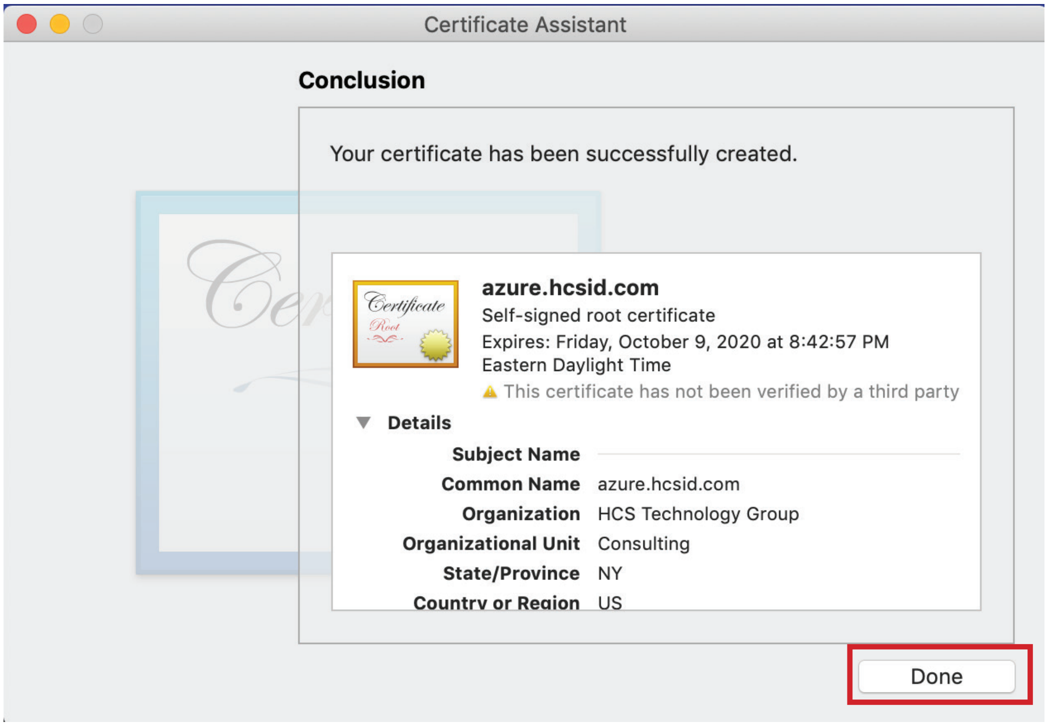


Specify a Location For The Certificate

Please specify a keychain where the certificate will be stored.

Keychain: login

36. Select Done.



Conclusion

Your certificate has been successfully created.

azure.hcsid.com

Self-signed root certificate

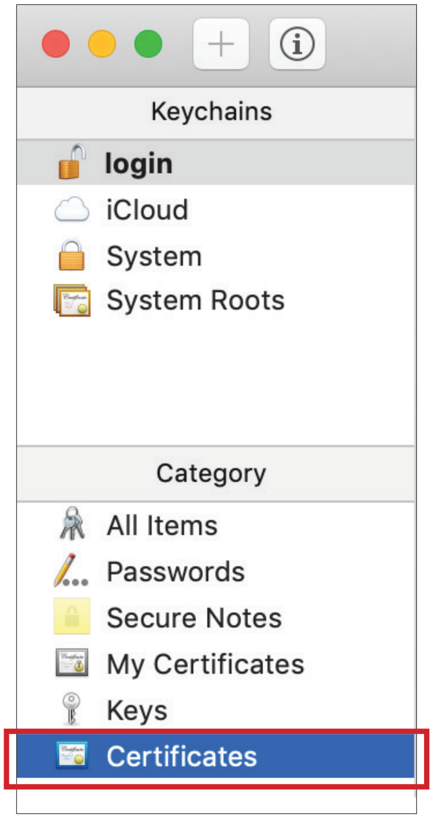
Expires: Friday, October 9, 2020 at 8:42:57 PM Eastern Daylight Time

⚠ This certificate has not been verified by a third party

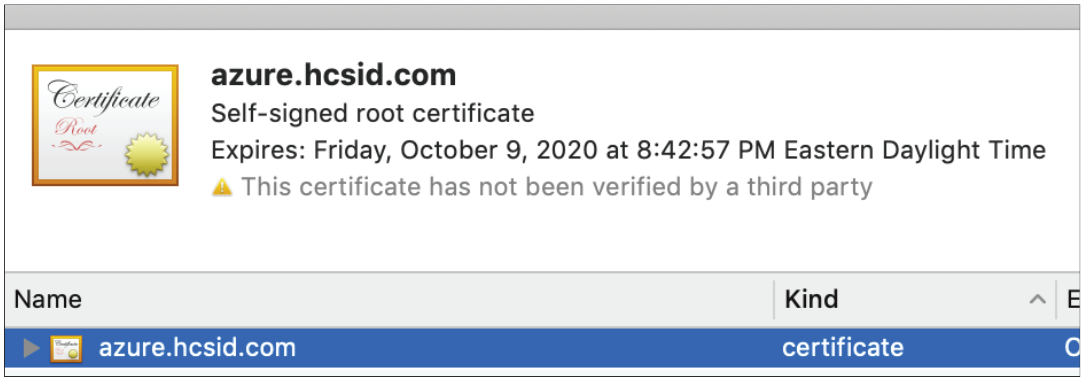
Details

Subject Name	
Common Name	azure.hcsid.com
Organization	HCS Technology Group
Organizational Unit	Consulting
State/Province	NY
Country or Region	US

37. In the Keychain Access side bar, select login, then select Certificates.



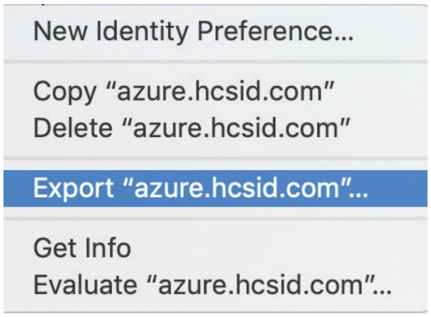
38. Look for the certificate with your dns name. IE. azure.hcsid.com. Right click on the certificate.



azure.hcsid.com
Self-signed root certificate
Expires: Friday, October 9, 2020 at 8:42:57 PM Eastern Daylight Time
⚠ This certificate has not been verified by a third party

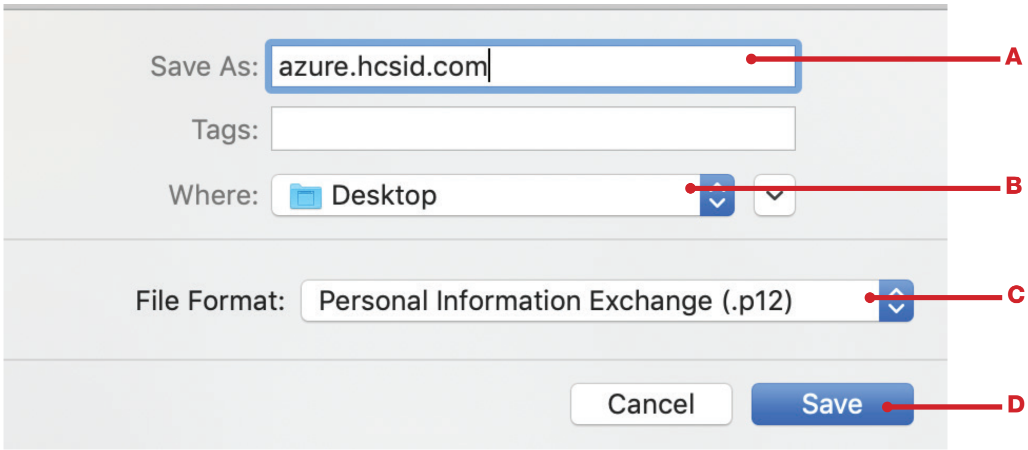
Name	Kind	E
azure.hcsid.com	certificate	C

39. Select Export.


New Identity Preference...
Copy "azure.hcsid.com"
Delete "azure.hcsid.com"
Export "azure.hcsid.com"...
Get Info
Evaluate "azure.hcsid.com"...

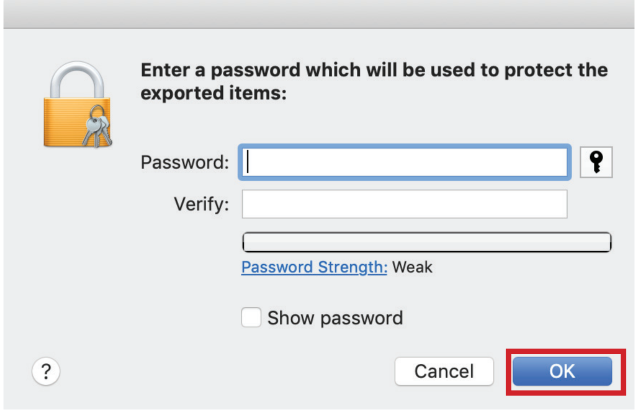
40. Enter the following:

A. Save As: Enter the DNS hostname.
B. Where: Save to Desktop
C. File Format: Personal Information Exchange (.p12)
D. Select Save.



Save As: azure.hcsid.com
Tags:
Where: Desktop
File Format: Personal Information Exchange (.p12)

41. Enter a password, then select OK.



Enter a password which will be used to protect the exported items:

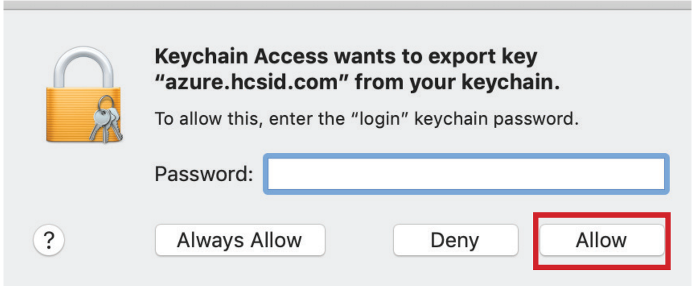
Password:

Verify:

Password Strength: Weak

□ Show password

42. Enter your login password, then select Allow.

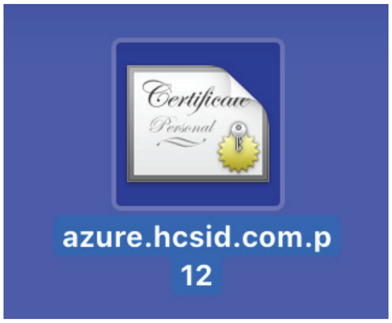


Keychain Access wants to export key "azure.hcsid.com" from your keychain.

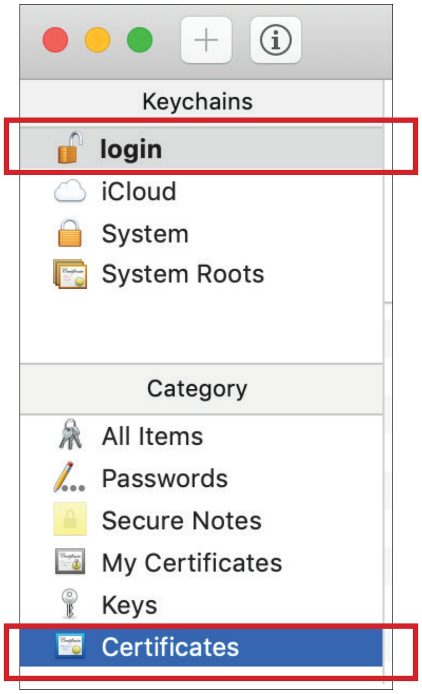
To allow this, enter the "login" keychain password.

Password:

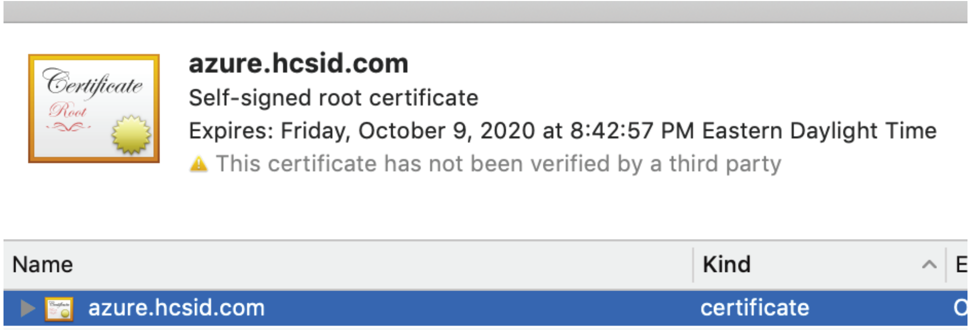
43. The certificate will be saved to your Desktop.



44. We need a second export of the certificate in a different format. In the Keychain Access side bar, select login, then select Certificates.



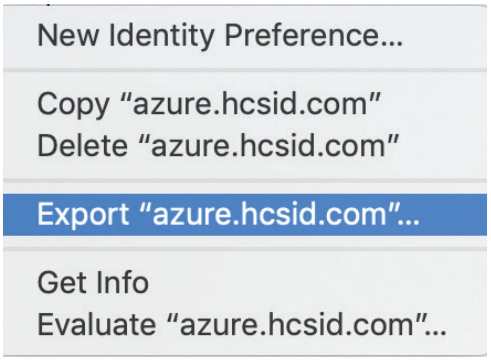
45. Look for the certificate with your dns name. IE. azure.hcsid.com. Right click on the certificate.



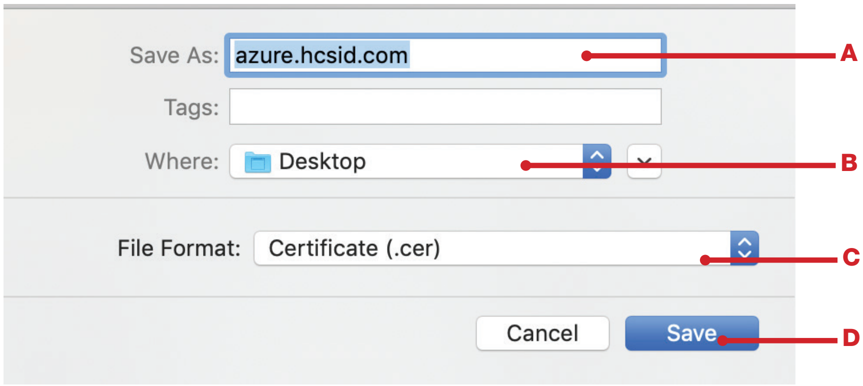
azure.hcsid.com
Self-signed root certificate
Expires: Friday, October 9, 2020 at 8:42:57 PM Eastern Daylight Time
⚠ This certificate has not been verified by a third party

Name	Kind	E
azure.hcsid.com	certificate	C

46. Select Export.



47. Enter the following:
    A. Save As: Enter the DNS hostname.
    B. Where: Save to Desktop
    C. File Format: Certificate (.cer)
    D. Select Save.



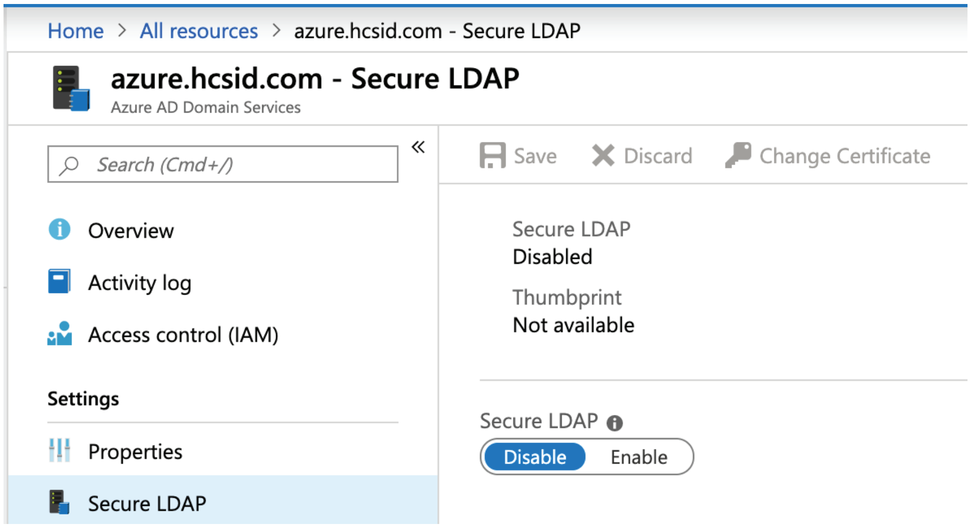
Save As: azure.hcsid.com
Tags:
Where: Desktop
File Format: Certificate (.cer)

48. On the Desktop, select the certificate with the .p12 extension. Change the .p12 extension to .pfx.

azure.hcsid.com.p12

azure.hcsid.com.pfx

49. Open your browser window that still displays the Secure LDAP configuration screen that was left open in step 22.



Home > All resources > azure.hcsid.com - Secure LDAP

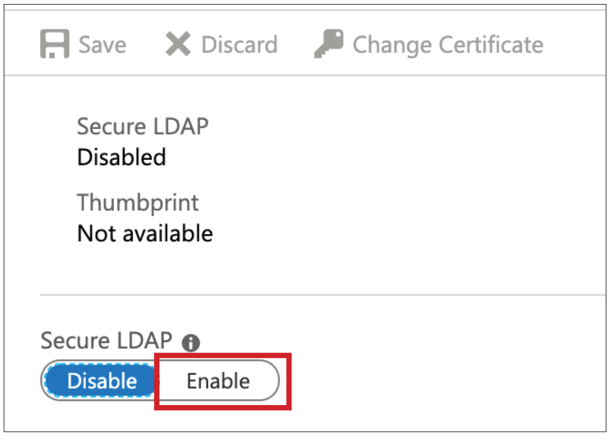
azure.hcsid.com - Secure LDAP
Azure AD Domain Services

Secure LDAP
Disabled

Thumbprint
Not available

Secure LDAP
○ Disable ● Enable

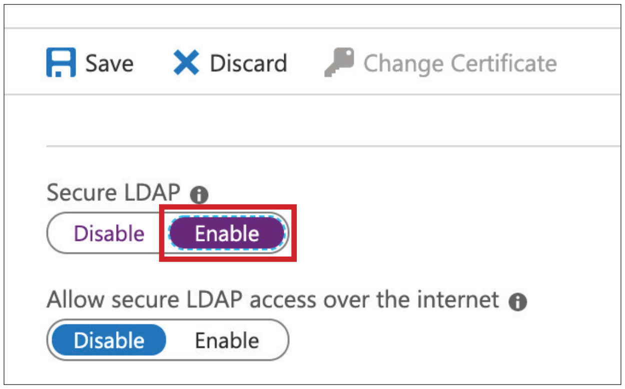
50. Secure LDAP, Select Enable.



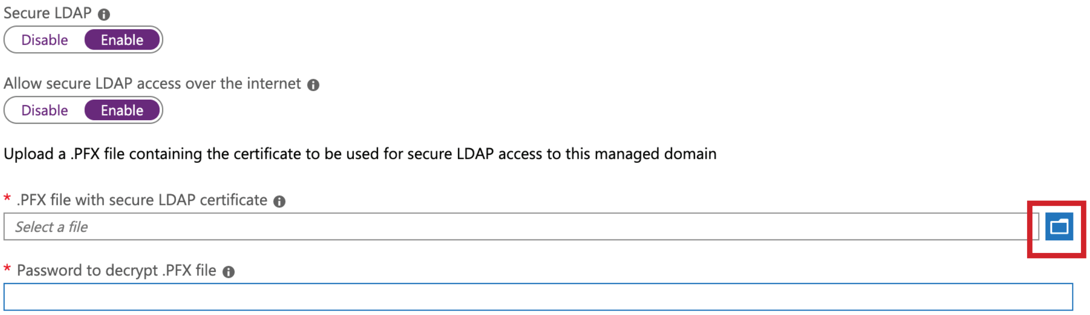
Secure LDAP
Disabled

Thumbprint
Not available

51. Allow secure LDAP access over the internet, Select Enable.



52. In the .PFX file with secure LDAP Certificate section, select the blue folder icon and navigate to the .pfx certificate that you saved to the Desktop in step 47. Enter the decryption password. This is the password you used in step 40.



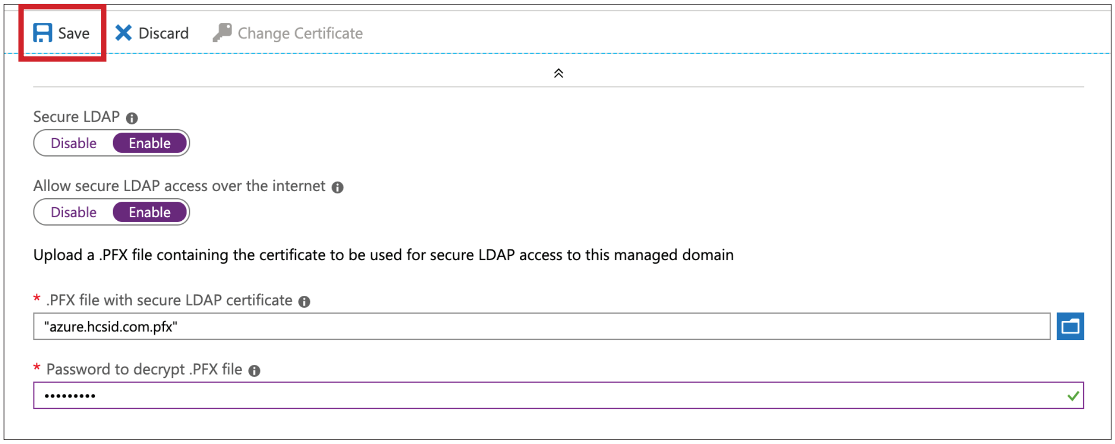
Upload a .PFX file containing the certificate to be used for secure LDAP access to this managed domain

* .PFX file with secure LDAP certificate

Select a file

* Password to decrypt .PFX file

53. Select Save. It will take a few minutes for Azure to configure secure LDAP. Please be patient.



Secure LDAP: Disable | **Enable**

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

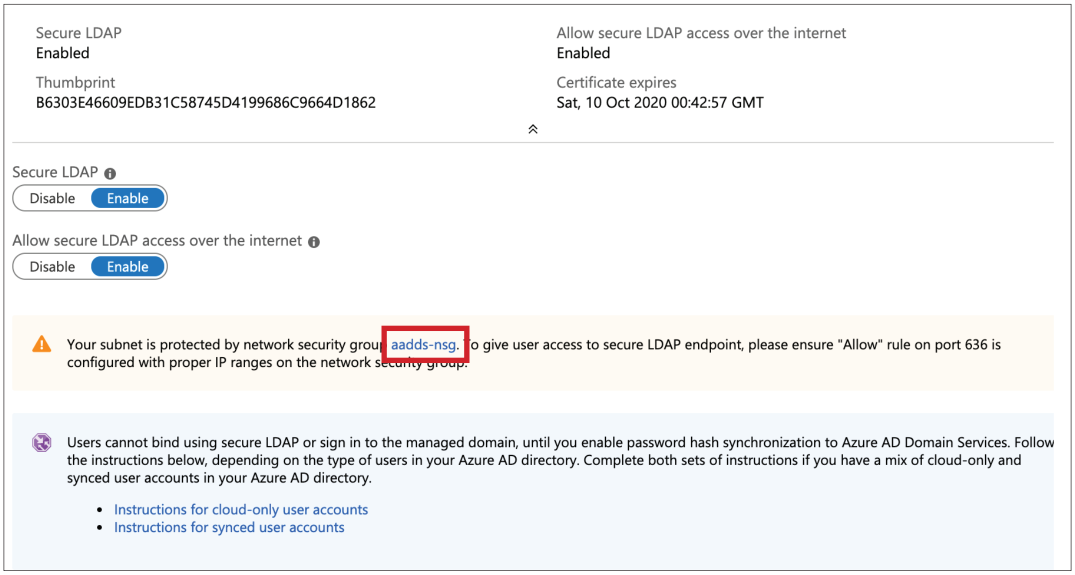
Upload a .PFX file containing the certificate to be used for secure LDAP access to this managed domain

* .PFX file with secure LDAP certificate: "azure.hcsid.com.pfx"

* Password to decrypt .PFX file: •••••••••

54. Once secure LDAP is configured, you will be brought to the screen below that shows the status as Enabled. Next to the notification icon (looks like an exclamation mark inside a yellow triangle) click the link to your network security group. E.G. aadds-nsg

NOTE: It may take a few minutes for Azure to show the network security group items. Please be patient



Secure LDAP
Enabled

Allow secure LDAP access over the internet
Enabled

Thumbprint
B6303E46609EDB31C58745D4199686C9664D1862

Certificate expires
Sat, 10 Oct 2020 00:42:57 GMT

Secure LDAP: Disable | **Enable**

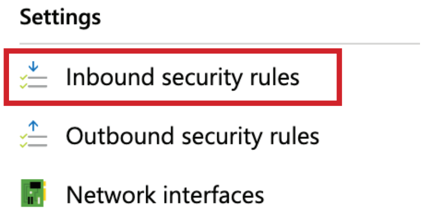
Allow secure LDAP access over the internet: Disable | **Enable**

⚠ Your subnet is protected by network security group aadds-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

55. Select Inbound security rules from the sidebar.



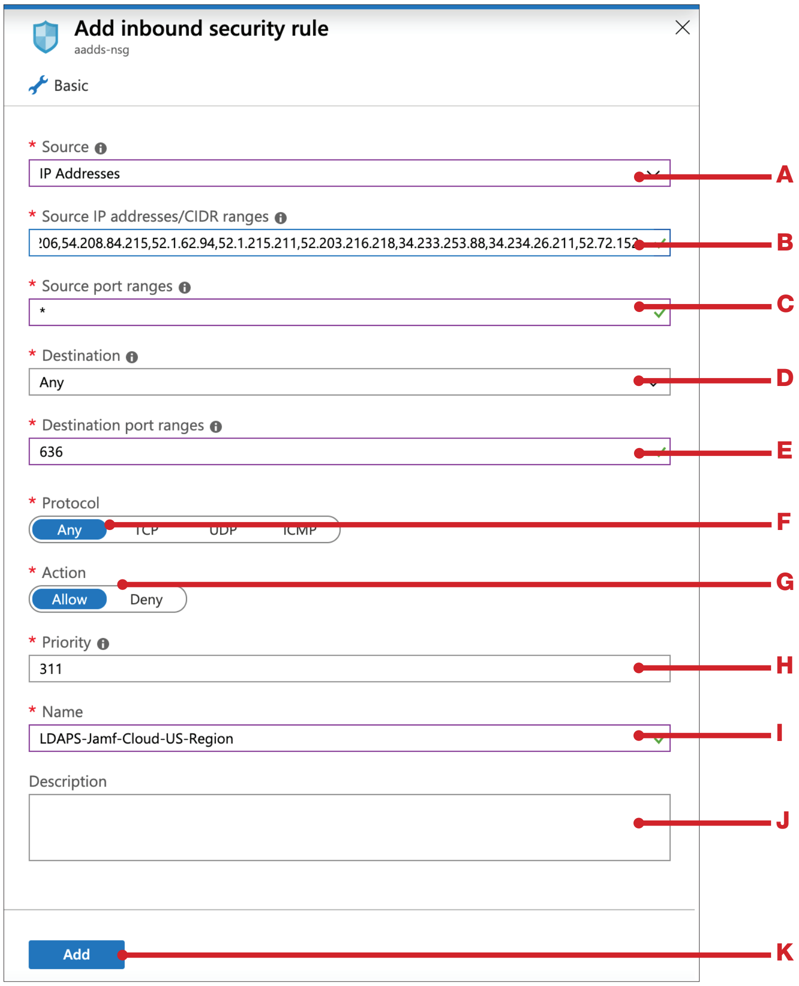
56. In the new Add Inbound security rule panel, enter the following:

NOTE: Step B: 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 located at:

https://www.jamf.com/jamf-nation/articles/409/permitting-inbound-outbound-traffic-with-jamf-cloud

This guide will use the IP address for the US Cloud Region. You may want to add the public IP address for you company to the list as it will be helpful for troubleshooting any issues with LDAPS from your computer. If you don't add it, then only jamf cloud servers will be able to connect to LDAPS and not your computer for troubleshooting.

A. Source: Choose IP Addresses
B. Source IP addresses/CIDR ranges:
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
C. Source port ranges Leave the default setting of * (star)
D. Destination: Leave the default setting of Any
E. Destination Port Ranges: Enter 636
F. Protocol: Leave the default setting of Any
G. Action: Leave the default setting of Allow
H. Priority: Leave the default setting
I. Name: Enter whatever you want. E.G. LDAPS-Jamf-Cloud-US-Region
J. Description: Leave blank or enter a description if you choose.
K. Review your settings then click Add.



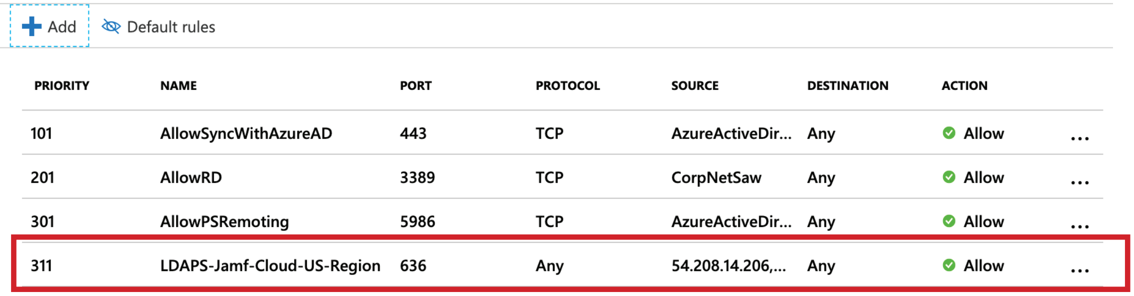
Add inbound security rule
aadds-nsg

Basic

* Source: IP Addresses
* Source IP addresses/CIDR ranges: 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
* Source port ranges: *
* Destination: Any
* Destination port ranges: 636
* Protocol: Any | TCP | UDP | ICMP
* Action: Allow | Deny
* Priority: 311
* Name: LDAPS-Jamf-Cloud-US-Region

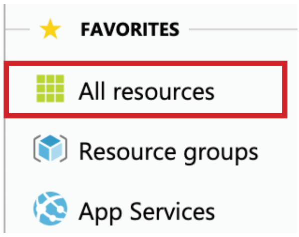
Description:

57. Confirm you see the rule you just created in the list. E.G. LDAPS-Jamf-Cloud-US-Region.

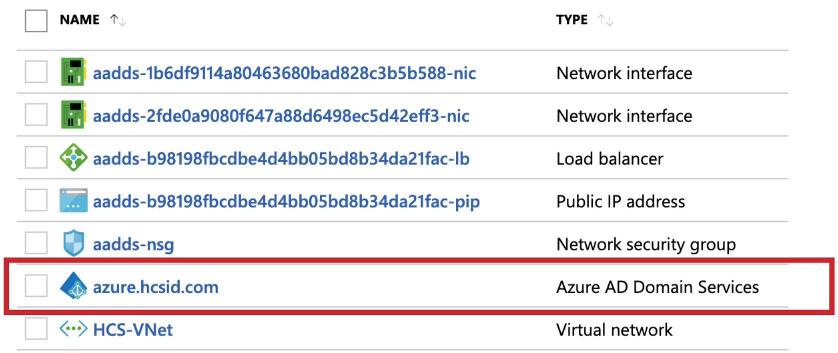


PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION	
101	AllowSyncWithAzureAD	443	TCP	AzureActiveDir...	Any	✓ Allow	...
201	AllowRD	3389	TCP	CorpNetSaw	Any	✓ Allow	...
301	AllowPSRemoting	5986	TCP	AzureActiveDir...	Any	✓ Allow	...
311	LDAPS-Jamf-Cloud-US-Region	636	Any	54.208.14.206,...	Any	✓ Allow	...

58. Select All resources from the sidebar.

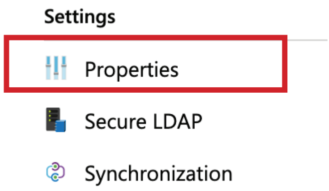


59. Select your Azure AD Domain. E.G. azure.hcsid.com

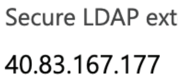


□ NAME ↑↓	TYPE ↑↓
□ aadds-1b6df9114a80463680bad828c3b5b588-nic	Network interface
□ aadds-2fde0a9080f647a88d6498ec5d42eff3-nic	Network interface
□ aadds-b98198fbcdbe4d4bb05bd8b34da21fac-lb	Load balancer
□ aadds-b98198fbcdbe4d4bb05bd8b34da21fac-pip	Public IP address
□ aadds-nsg	Network security group
□ azure.hcsid.com	Azure AD Domain Services
□ HCS-VNet	Virtual network

60. Select Properties.



61. Copy the Secure LDAP external IP address. We will need this IP address to create an external DNS A record in the next step.

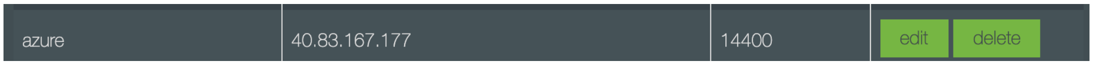


Secure LDAP external IP address

40.83.167.177

62. In this step, I will create a DNS A record using my domain registrar account. You will need to do the same on your domain registrars web site.

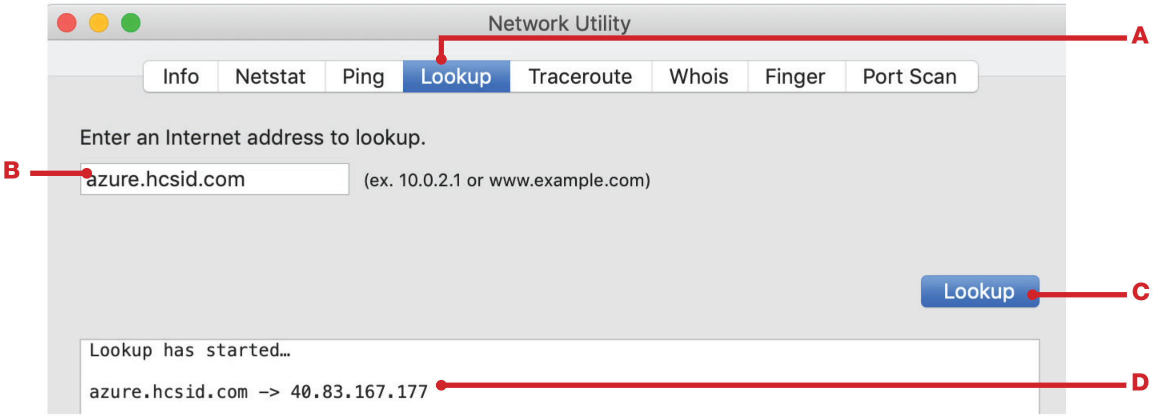
NOTE: It can take up to 72 hrs for the A record to propagate across the internet.



azure	40.83.167.177	14400	edit delete

63. Open Network Utility located in /Applications/Utilities.

A. Select the Lookup tab.
B. Enter the name of the DNS recored you created in step 62.
C. Click the Lookup button.
D. If all went well, the lookup will provide the name to address mapping shown below.
E.G. azure.hcsid.com -> 40.83.167.177
E. Quit Network Utility. This completes this section.



Enter an Internet address to lookup.

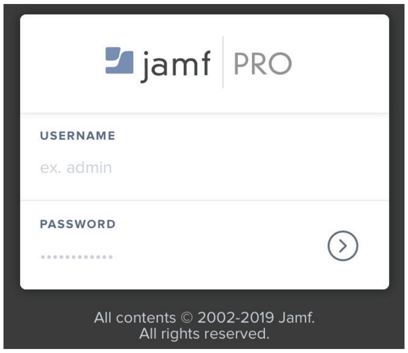
azure.hcsid.com (ex. 10.0.2.1 or www.example.com)

```
Lookup has started…

azure.hcsid.com -> 40.83.167.177
```

Section 4: Configure Jamf Pro with Azure Secure LDAP

1. If necessary, Login to your Jamf Pro server.



jamf | PRO

USERNAME

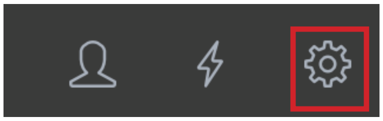
ex. admin

PASSWORD

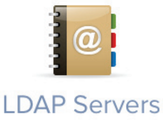
••••••••••••

All contents © 2002-2019 Jamf.
All rights reserved.

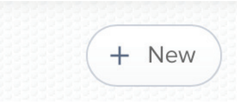
2. Select Settings in the upper right corner.



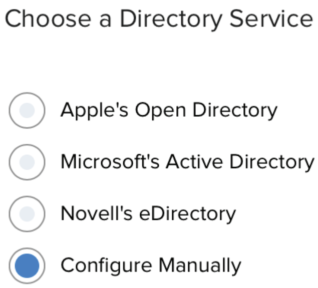
3. Select LDAP Servers.



4. Select New.



5. Select Configure Manually.



Choose a Directory Service

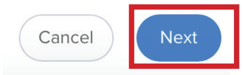
○ Apple's Open Directory

○ Microsoft's Active Directory

○ Novell's eDirectory

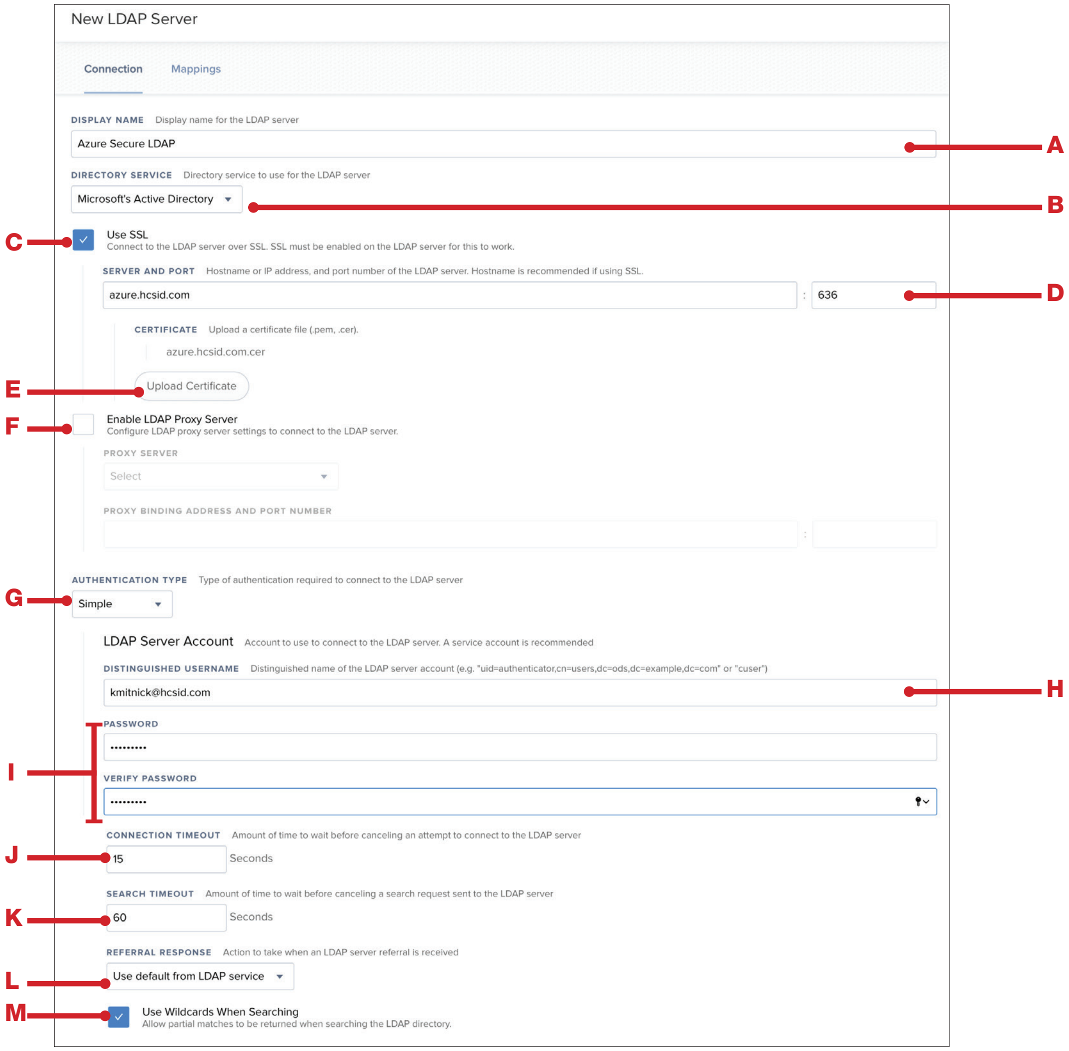
● Configure Manually

6. Click Next.



7. Select the Connection tab, the configure the following:

A. Display Name: Enter a name of your choosing
B. Directory Service: Select Microsoft's Active Directory
C. Use SSL: Make sure this is checked
D. Server and Port: Enter your azure secure LDAP name and set the port to 636.
E.G. azure.hcsid.com
E. Select the Upload Certificate button and navigate to the certificate you saved on your desktop ending in .cer E.G. azure.hcsid.com.cer
F. Enable LDAP Proxy Server: Make sure this is NOT checked
G. Authentication Type: Set this to Simple
H. Distinguished Name: Enter an Azure account that is part of the AAD DC Administrators group. Best practice is to use a service only account. Enter the name in the form of an email address.
E.G. kmitnick@hcsid.com
I. Enter the password for the account and verify it.
J. Connection timeout: Leave at default
K. Search timeout: Leave at default
L. Referral Response:Leave at default
M. Use Wildcards when Searching: Leave at default



New LDAP Server

DISPLAY NAME Display name for the LDAP server
Azure Secure LDAP

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

☑ Use SSL
Connect to the LDAP server over SSL. SSL must be enabled on the LDAP server for this to work.

SERVER AND PORT Hostname or IP address, and port number of the LDAP server. Hostname is recommended if using SSL.
azure.hcsid.com : 636

CERTIFICATE Upload a certificate file (.pem, .cer).
azure.hcsid.com.cer

□ Enable LDAP Proxy Server
Configure LDAP proxy server settings to connect to the LDAP server.

PROXY SERVER
Select

PROXY BINDING ADDRESS AND PORT NUMBER

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

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" or "cuser")
kmitnick@hcsid.com

PASSWORD
•••••••••

VERIFY PASSWORD
•••••••••

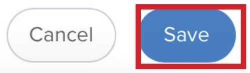
CONNECTION TIMEOUT Amount of time to wait before canceling an attempt to connect to the LDAP server
15 Seconds

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

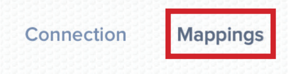
REFERRAL RESPONSE Action to take when an LDAP server referral is received
Use default from LDAP service

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

8. Select Save.

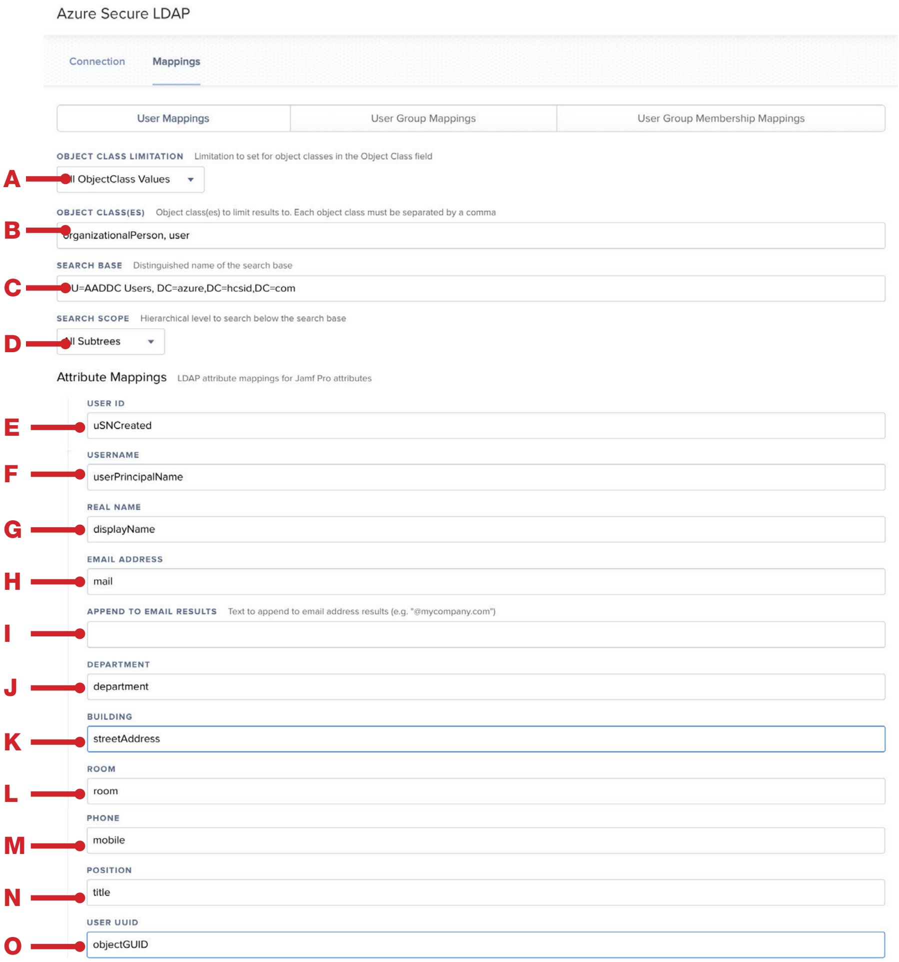


9. Select Mappings.



10. Select the User Mappings tab, then configure the following:

    A. Object Class Limitation: Select All ObjectClass Values
    B. Object Class(es): Enter organizationalPerson, user
    C. Search Base: Enter your search base using this example OU=AADDC Users, DC=azure, DC=hcsid,DC=com
    D. Search Scope: Select All Subtrees
    E. User ID: Enter uSNCreated
    F. Username: Enter userPrincipalName
    G. Real Name: Enter displayName
    H. Email Address: Enter mail
    I. Append to Email Results: Leave blank unless you require it.
    J. Department: Enter department
    K. Building: Enter streetAddress
    L. Room: Enter room
    M. Phone: Enter mobile
    N. Position: Enter title
    O. User UUID: Leave objectGUID



Azure Secure LDAP

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

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

SEARCH BASE Distinguished name of the search base
U=AADDC Users, DC=azure,DC=hcsid,DC=com

SEARCH SCOPE Hierarchical level to search below the search base
ll Subtrees

Attribute Mappings LDAP attribute mappings for Jamf Pro attributes

USER ID
uSNCreated

USERNAME
userPrincipalName

REAL NAME
displayName

EMAIL ADDRESS
mail

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

DEPARTMENT
department

BUILDING
streetAddress

ROOM
room

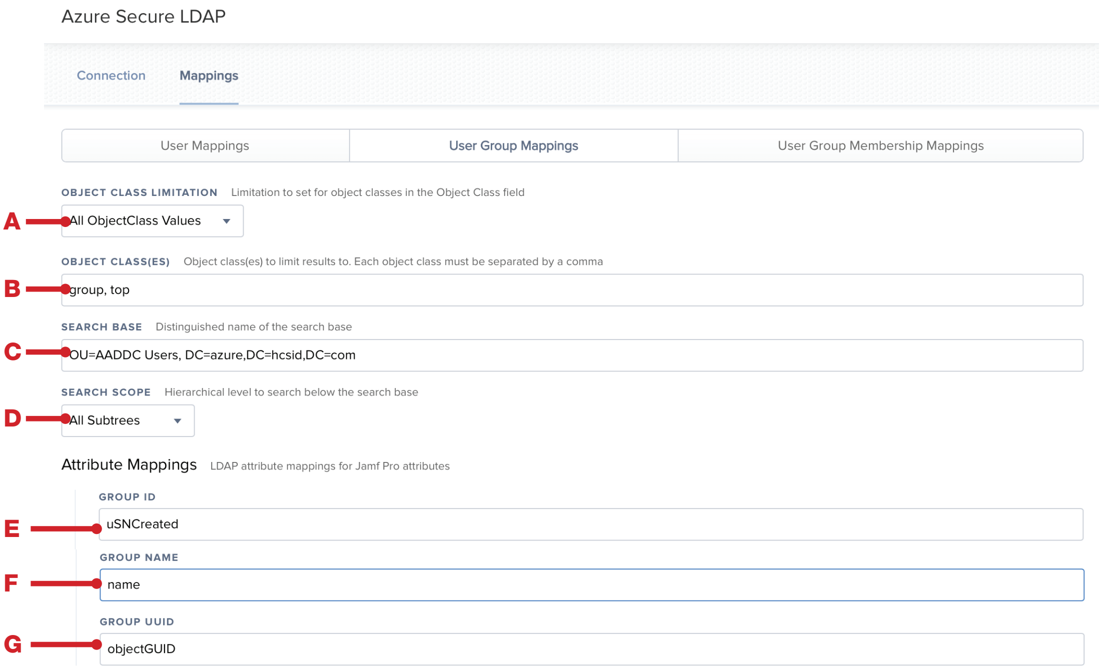
PHONE
mobile

POSITION
title

USER UUID
objectGUID

11. Select the User Group Mappings tab, then configure the following:

    A. Object Class Limitation: Leave All ObjectClass Values
    B. Object Class(es): Enter group, top
    C. Search Base: Enter your search base using this example OU=AADDC Users, DC=azure, DC=hcsid,DC=com
    D. Search Scope: Select All subtrees
    E. Group ID: Enter uSNCreated
    F. Group Name: Enter name
    G. Group UUID: Leave at objectGUID



Azure Secure LDAP

Connection | **Mappings**

User Mappings | **User Group Mappings** | User Group Membership Mappings

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

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

SEARCH BASE Distinguished name of the search base
OU=AADDC Users, DC=azure,DC=hcsid,DC=com

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

Attribute Mappings LDAP attribute mappings for Jamf Pro attributes

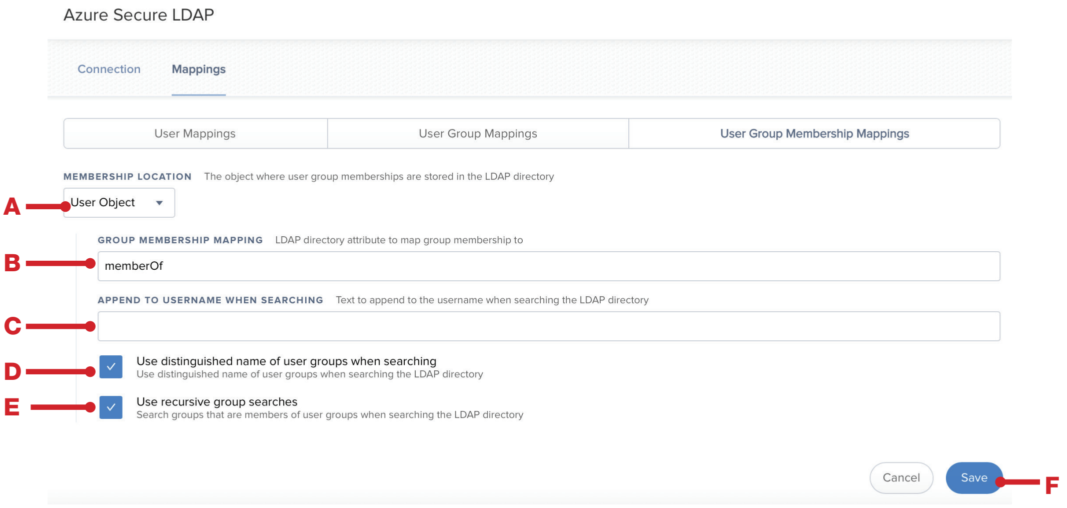
GROUP ID
uSNCreated

GROUP NAME
name

GROUP UUID
objectGUID

12. Select the User Group Membership Mappings tab, then configure the following:

    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
    F. Click Save



Azure Secure LDAP

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

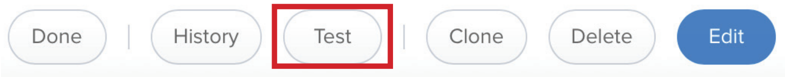
GROUP MEMBERSHIP MAPPING LDAP directory attribute to map group membership to
memberOf

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

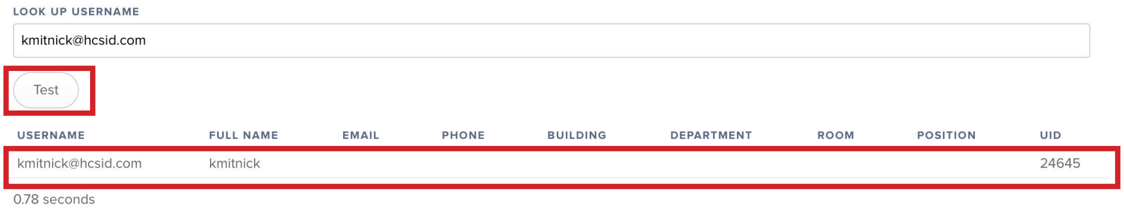
13. Select Test.



14. Select User Mappings, then enter a name from your Azure Active Directory to lookup in the Look up Username field. Click Test. If all went well, you will see the results of your user lookup.

    NOTE: If you're not seeing the results below it could be an issue with your mapping settings. A great tool to use for troubleshooting LDAP connections is LDAP Browser. Get it here: http://www.ldapbrowsermac.com

    In order to use LDAP Browser from your computer, the public IP for you company must be in the trusted IP list as described in section 3, step 56 of this guide.



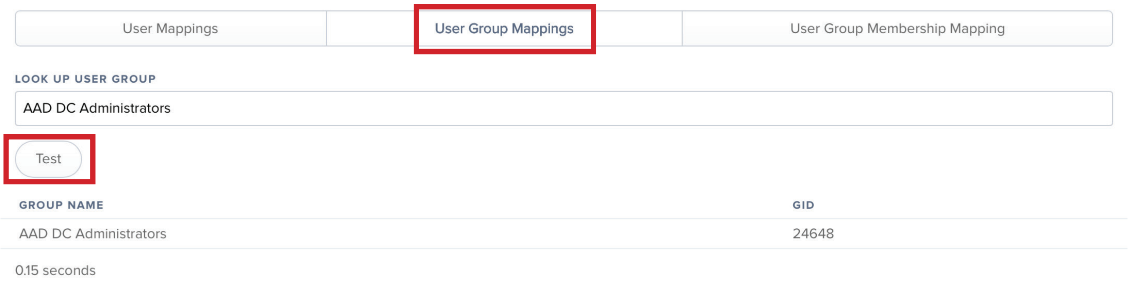
LOOK UP USERNAME

kmitnick@hcsid.com

USERNAME	FULL NAME	EMAIL	PHONE	BUILDING	DEPARTMENT	ROOM	POSITION	UID
kmitnick@hcsid.com	kmitnick							24645

0.78 seconds

15. Select User Group Mappings then enter AAD DC Administrators in the Look up User Group Field. Click Test.If all went well, you will see the results of your user group lookup.



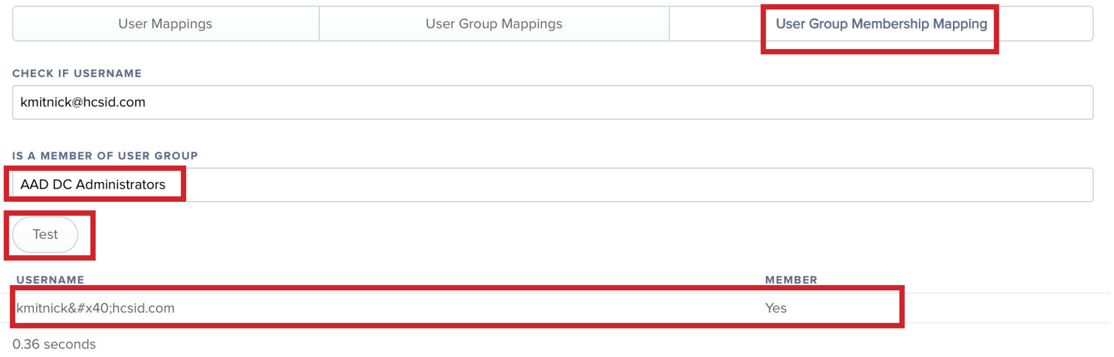
LOOK UP USER GROUP

AAD DC Administrators

GROUP NAME	GID
AAD DC Administrators	24648

0.15 seconds

16. Select User Group Membership Mapping then enter a user account in the Check if Username Field. Enter AAD DC Administrators in the If a Member of User Group field. Click Test.If all went well, you will see the results of your user group membership mapping lookup.



CHECK IF USERNAME

kmitnick@hcsid.com

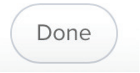
IS A MEMBER OF USER GROUP

AAD DC Administrators

USERNAME	MEMBER
kmitnick&#x40;hcsid.com	Yes

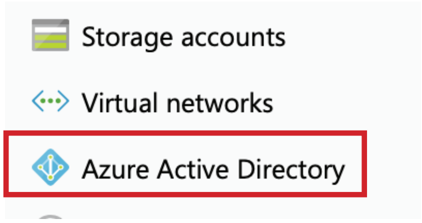
0.36 seconds

17. Click Done. You have successfully configured Jamf Pro to integrate with Azure AD via Secure LDAP.This completes this section.

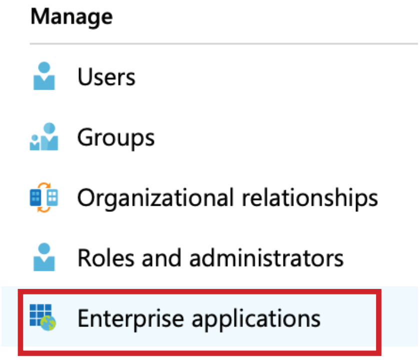


Section 5: Configure Azure Active Directory for Single Sign-On (SSO) with Jamf Pro

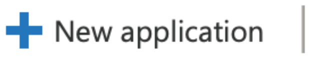
1. Select Azure Active Directory from the sidebar.



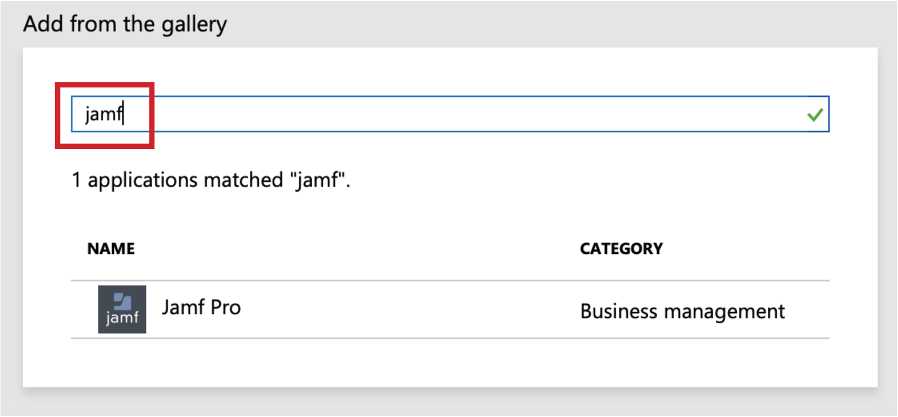
2. Select Enterprise applications.



3. Select New application.



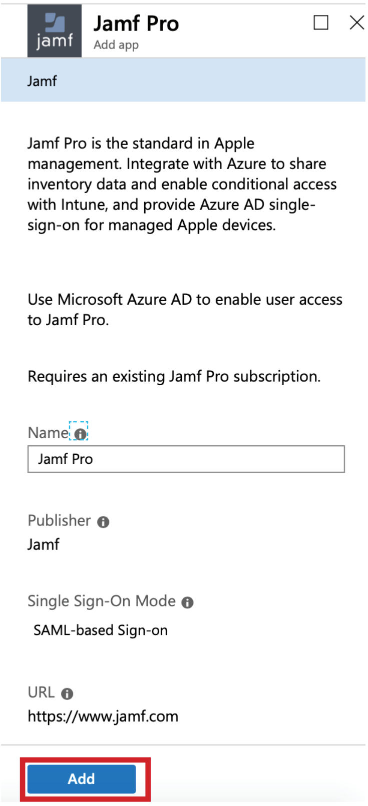
4. In the Add from the gallery section, enter jamf in the search field then click on Jamf Pro .



1 applications matched "jamf".

NAME	CATEGORY
Jamf Pro	Business management

5. Click Add.



Jamf Pro
Add app

Jamf

Jamf Pro is the standard in Apple management. Integrate with Azure to share inventory data and enable conditional access with Intune, and provide Azure AD single-sign-on for managed Apple devices.

Use Microsoft Azure AD to enable user access to Jamf Pro.

Requires an existing Jamf Pro subscription.

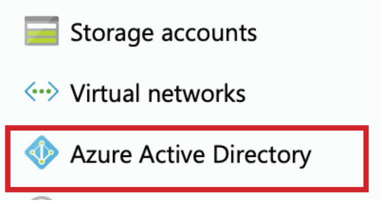
Name: Jamf Pro

Publisher: Jamf

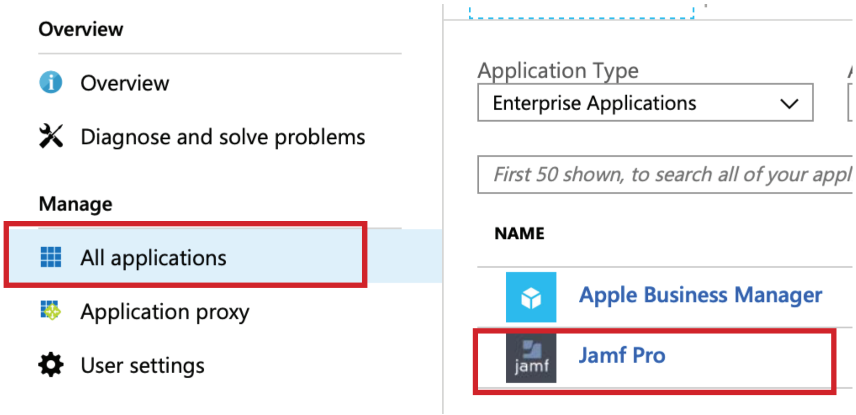
Single Sign-On Mode: SAML-based Sign-on

URL: https://www.jamf.com

6. Select Azure Active Directory from the sidebar.



7. Select All applications, then click on Jamf Pro.

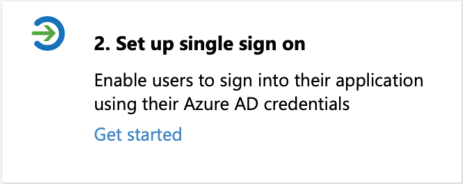


Application Type: Enterprise Applications

First 50 shown, to search all of your appl

NAME
Apple Business Manager
Jamf Pro

8. Select Set up single sign on.

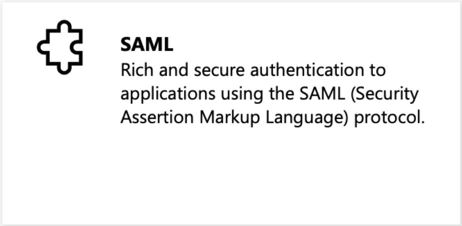


2. Set up single sign on

Enable users to sign into their application using their Azure AD credentials

Get started

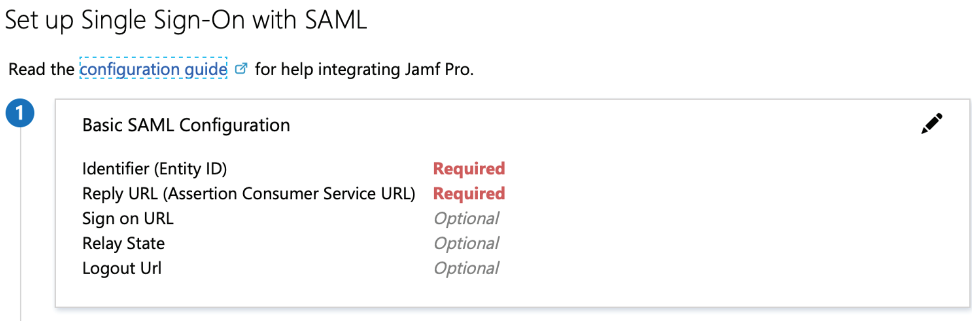
9. Select SAML.



SAML

Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

10. In section 1, Basic SAML Configuration, we need the Identifier and Reply URL. This information comes from Jamf Pro and we will get that in the next steps.



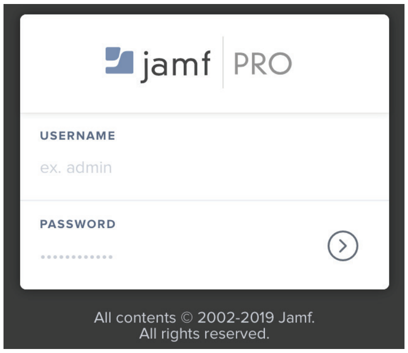
Set up Single Sign-On with SAML

Read the configuration guide for help integrating Jamf Pro.

1 Basic SAML Configuration

Identifier (Entity ID)	**Required**
Reply URL (Assertion Consumer Service URL)	**Required**
Sign on URL	*Optional*
Relay State	*Optional*
Logout Url	*Optional*

11. Open a new tab in your web browser, and navigate to your Jamf Pro server. Login with admin credentials.



USERNAME

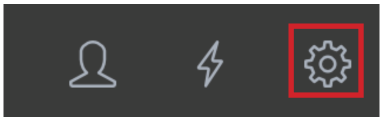
ex. admin

PASSWORD

············

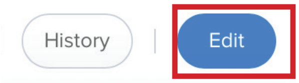
All contents © 2002-2019 Jamf.
All rights reserved.

12. Select the Settings in the upper right corner.

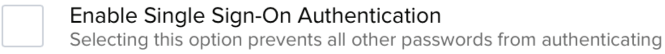


13. Select Single Sign-On.

14. Click Edit.

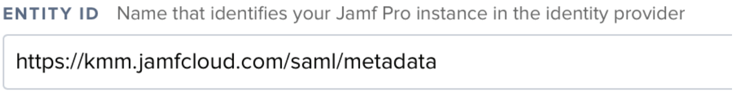


15. Enable Single Sign-On Authentication.



□ Enable Single Sign-On Authentication
Selecting this option prevents all other passwords from authenticating

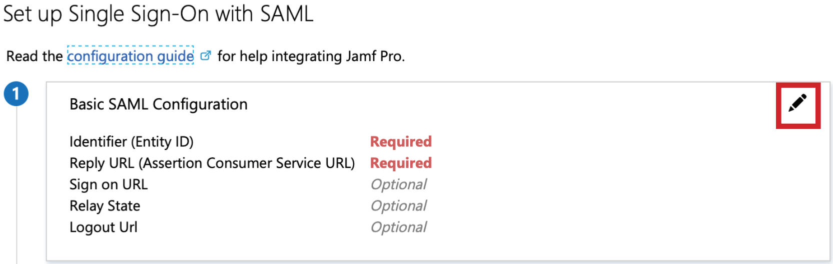
16. Copy the Entity ID, then cancel out of this setup page.



ENTITY ID Name that identifies your Jamf Pro instance in the identity provider

https://kmm.jamfcloud.com/saml/metadata

17. Switch back to your Azure portal. In section 1, click the pencil icon to edit the settings.



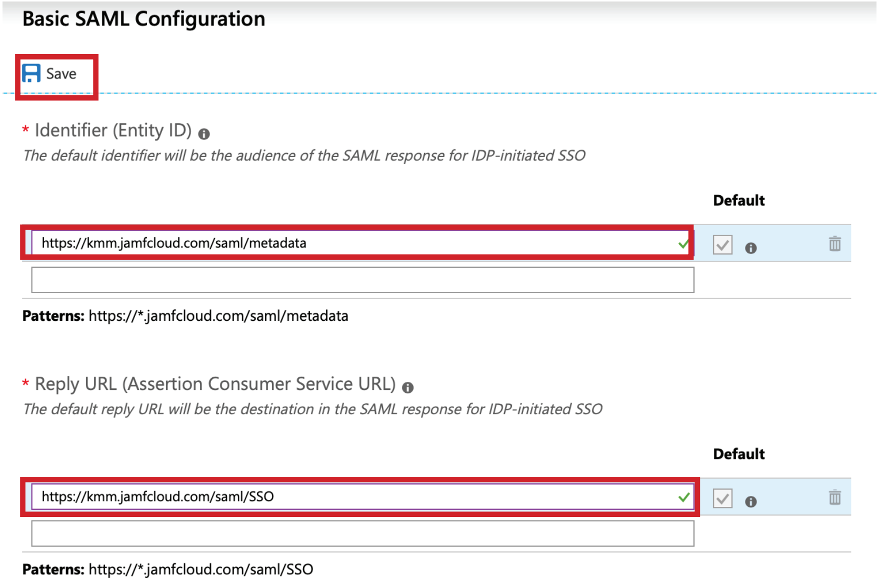
Set up Single Sign-On with SAML

Read the configuration guide for help integrating Jamf Pro.

1 Basic SAML Configuration

Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	*Optional*
Relay State	*Optional*
Logout Url	*Optional*

18. Enter the Identifier (Entity ID) in the field, then enter the same information in the Reply URL field but remove the metadata from the url and replace it with SSO. Select Save.



Basic SAML Configuration

Save

* Identifier (Entity ID)
The default identifier will be the audience of the SAML response for IDP-initiated SSO

	Default
https://kmm.jamfcloud.com/saml/metadata ✓	☑

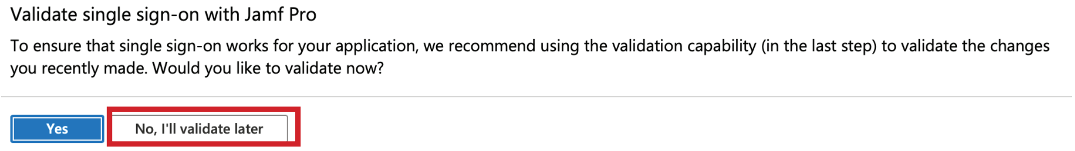
Patterns: https://*.jamfcloud.com/saml/metadata

* Reply URL (Assertion Consumer Service URL)
The default reply URL will be the destination in the SAML response for IDP-initiated SSO

	Default
https://kmm.jamfcloud.com/saml/SSO ✓	☑

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

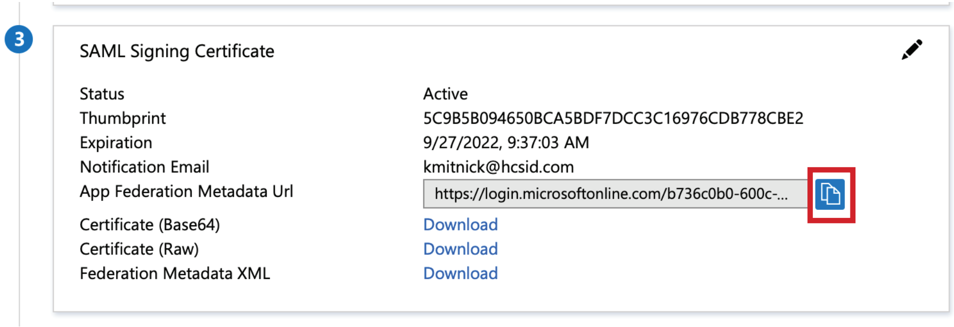
19. At the message below, select No, I'll validate later.



Validate single sign-on with Jamf Pro

To ensure that single sign-on works for your application, we recommend using the validation capability (in the last step) to validate the changes you recently made. Would you like to validate now?

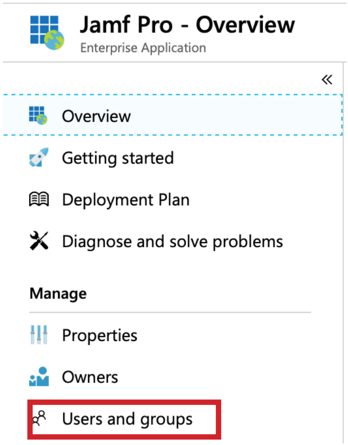
20. In section 3, SAML Signing Certificate, copy the App Federation Metadata URL. We will need this in a later step. You can click the blue icon next to it to copy it.



SAML Signing Certificate

Status	Active
Thumbprint	5C9B5B094650BCA5BDF7DCC3C16976CDB778CBE2
Expiration	9/27/2022, 9:37:03 AM
Notification Email	kmitnick@hcsid.com
App Federation Metadata Url	https://login.microsoftonline.com/b736c0b0-600c-...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

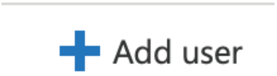
21. Select Users and Groups.



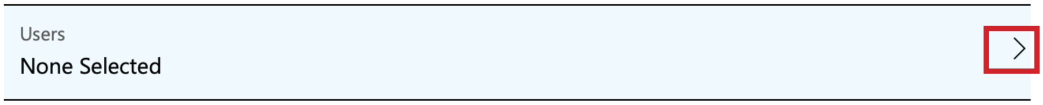
Jamf Pro - Overview

Enterprise Application

22. Select Add User.



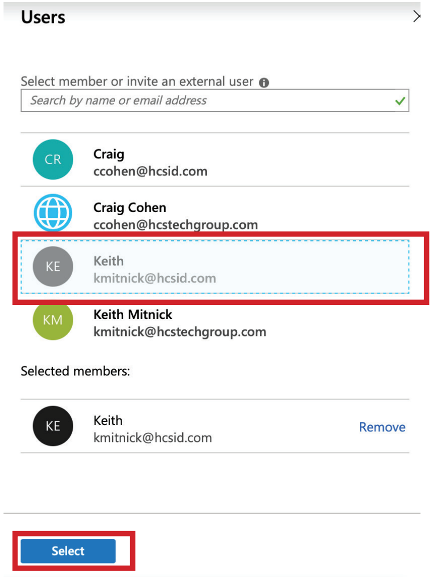
23. In the Users section, click on the Arrow on the right side.



Users

None Selected

24. Select a user then click the Select button.



Users

Select member or invite an external user

Search by name or email address

CR Craig
ccohen@hcsid.com

Craig Cohen
ccohen@hcstechgroup.com

KE Keith
kmitnick@hcsid.com

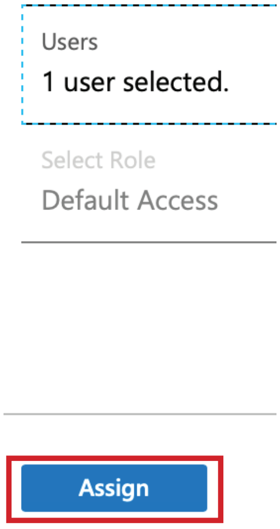
KM Keith Mitnick
kmitnick@hcstechgroup.com

Selected members:

KE Keith
kmitnick@hcsid.com Remove

Select

25. Select Assign.

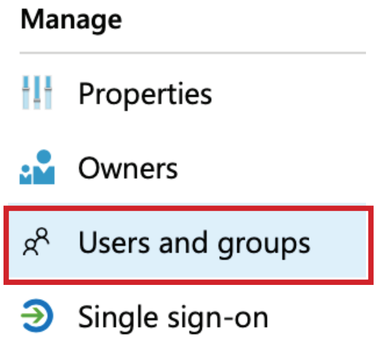


Users
1 user selected.

Select Role
Default Access

Assign

26. Select Single Sign-On.



Manage

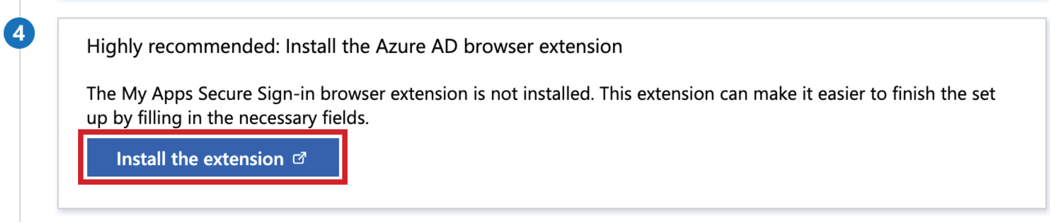
Properties

Owners

Users and groups

Single sign-on

27. In section 4, click Install the extension.

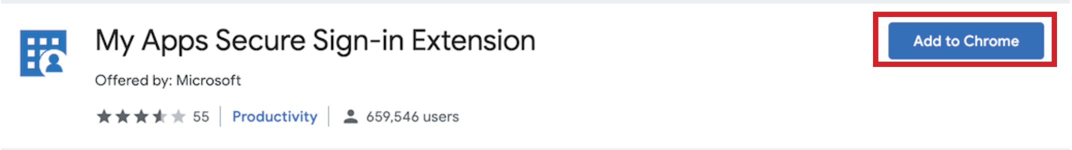


4

Highly recommended: Install the Azure AD browser extension

The My Apps Secure Sign-in browser extension is not installed. This extension can make it easier to finish the set up by filling in the necessary fields.

28. Select Add to Chrome.

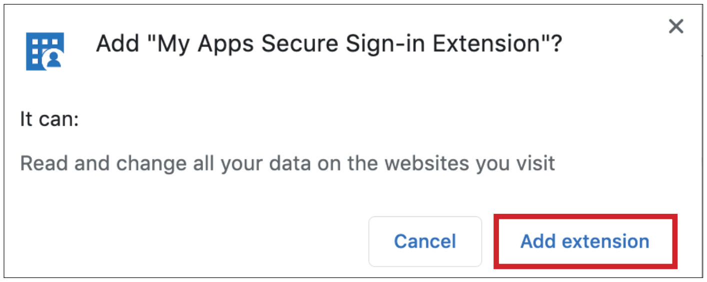


My Apps Secure Sign-in Extension

Offered by: Microsoft

★★★★☆ 55 | Productivity | 659,546 users

29. Select Add extension. Then switch back to Azure.

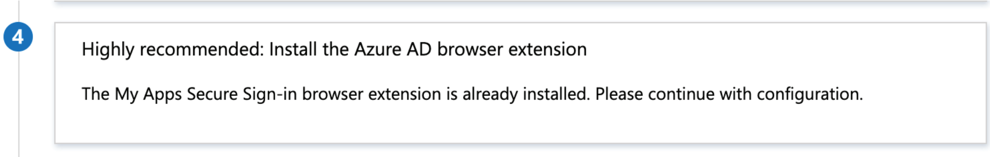


Add "My Apps Secure Sign-in Extension"?

It can:

Read and change all your data on the websites you visit

30. The extension is successfully installed.

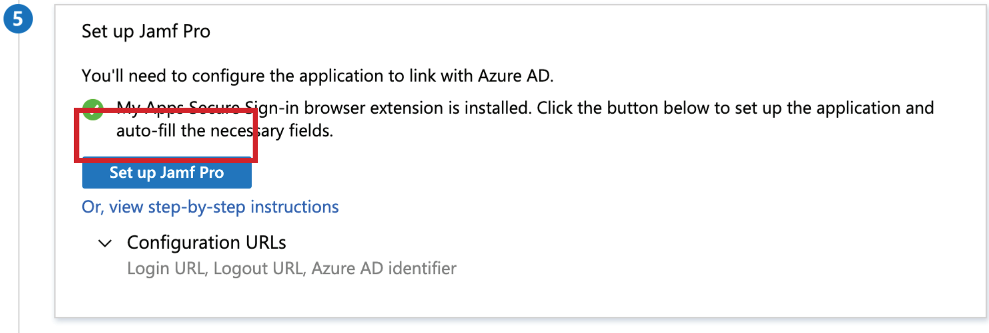


4

Highly recommended: Install the Azure AD browser extension

The My Apps Secure Sign-in browser extension is already installed. Please continue with configuration.

31. In section 5, Set up Jamf Pro, Select Set up Jamf Pro.
NOTE: You may need to clear your browser cache for this step to work properly.



5

Set up Jamf Pro

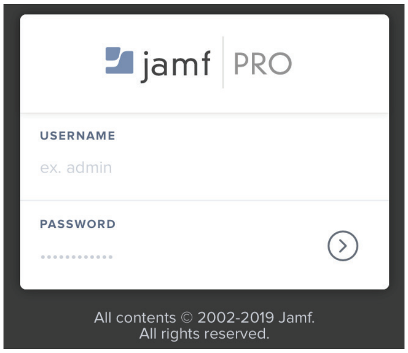
You'll need to configure the application to link with Azure AD.

✓ My Apps Secure Sign-in browser extension is installed. Click the button below to set up the application and auto-fill the necessary fields.

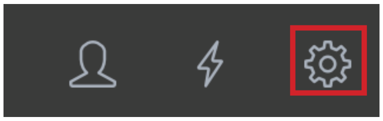
Or, view step-by-step instructions

Configuration URLs
Login URL, Logout URL, Azure AD identifier

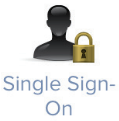
32. If not already logged in, Log into Jamf Pro with an admin account.



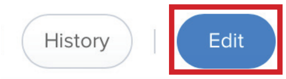
33. Select the Settings in the upper right corner.



34. Select Single Sign-On. Click Edit.

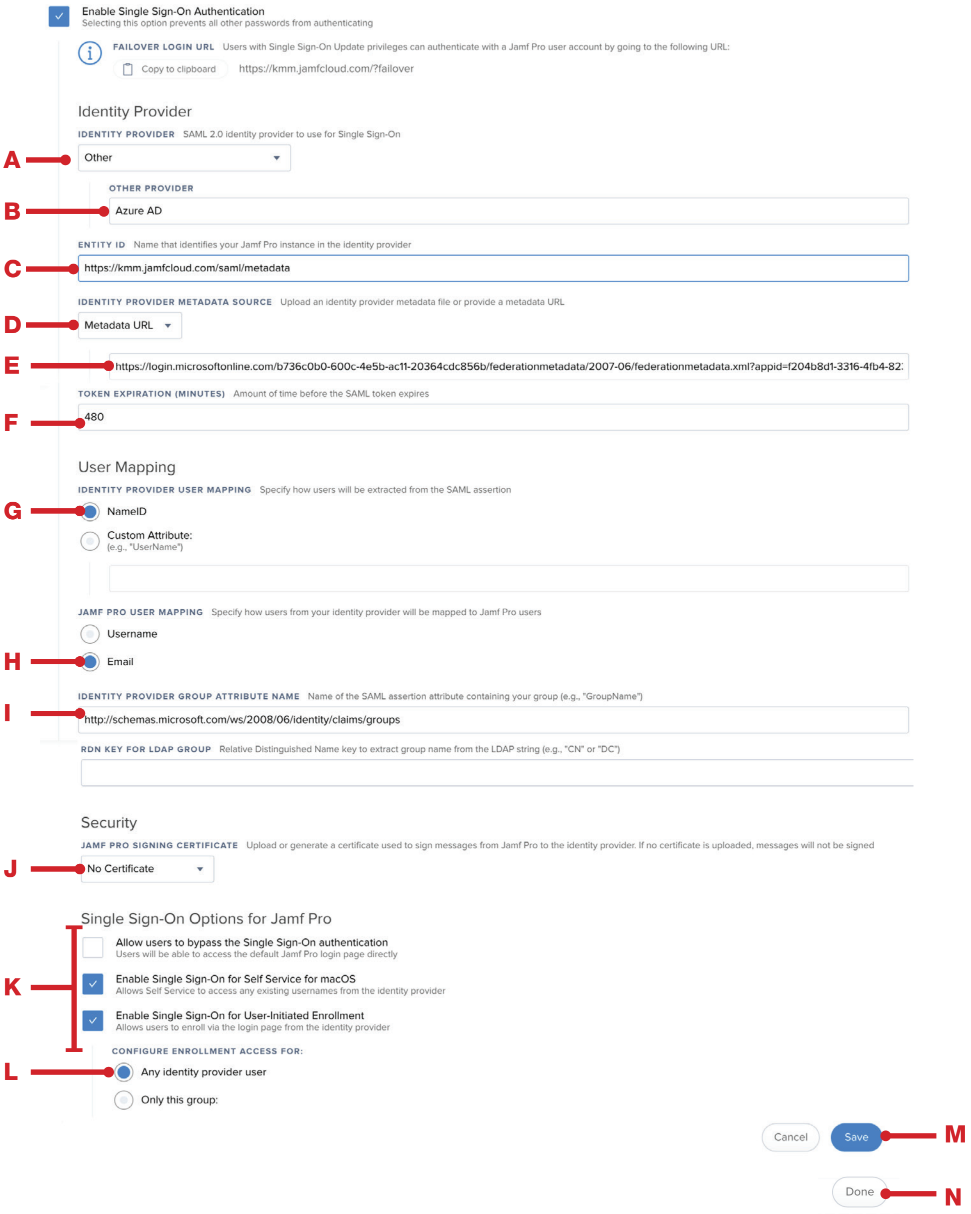


35. Click Edit.



35. Enter the following Information:

A. Identity Provider: Other
B. Other Provider: Azure AD
C. Entity ID: Enter your jamfcloud URL followed by /saml/metadata
D. Identity Provider Metadata Source: Set this to Metadata URL
E. Paste in the Metadata URL. You copied this in step 20.
F. Token Expiration: 480
G. Identity Provider User Mapping: NameID
H. Jamf Pro User Mapping: Email
I. Identity Provider Group Attribute Name:
http://schemas.microsoft.com/ws/2008/06/identity/claims/groups
J. Jamf Pro Signing Certificate: No Certificate
K: Single Sign -On Options for Jamf: Select what is needed in your environment. For this guide, I will select all of them.
L. Configure Enrollment access for: Any Identity Provider User.
M. Select Save
N. Select Done



☑ Enable Single Sign-On Authentication
Selecting this option prevents all other passwords from authenticating

FAILOVER LOGIN URL Users with Single Sign-On Update privileges can authenticate with a Jamf Pro user account by going to the following URL:
Copy to clipboard https://kmm.jamfcloud.com/?failover

Identity Provider

IDENTITY PROVIDER SAML 2.0 identity provider to use for Single Sign-On
Other

OTHER PROVIDER
Azure AD

ENTITY ID Name that identifies your Jamf Pro instance in the identity provider
https://kmm.jamfcloud.com/saml/metadata

IDENTITY PROVIDER METADATA SOURCE Upload an identity provider metadata file or provide a metadata URL
Metadata URL

https://login.microsoftonline.com/b736c0b0-600c-4e5b-ac11-20364cdc856b/federationmetadata/2007-06/federationmetadata.xml?appid=f204b8d1-3316-4fb4-82

TOKEN EXPIRATION (MINUTES) Amount of time before the SAML token expires
480

User Mapping

IDENTITY PROVIDER USER MAPPING Specify how users will be extracted from the SAML assertion
● NameID
○ Custom Attribute:
(e.g., "UserName")

JAMF PRO USER MAPPING Specify how users from your identity provider will be mapped to Jamf Pro users
○ Username
● Email

IDENTITY PROVIDER GROUP ATTRIBUTE NAME Name of the SAML assertion attribute containing your group (e.g., "GroupName")
http://schemas.microsoft.com/ws/2008/06/identity/claims/groups

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

Security

JAMF PRO SIGNING CERTIFICATE Upload or generate a certificate used to sign messages from Jamf Pro to the identity provider. If no certificate is uploaded, messages will not be signed
No Certificate

Single Sign-On Options for Jamf Pro

□ Allow users to bypass the Single Sign-On authentication
Users will be able to access the default Jamf Pro login page directly

☑ Enable Single Sign-On for Self Service for macOS
Allows Self Service to access any existing usernames from the identity provider

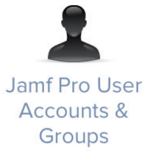
☑ Enable Single Sign-On for User-Initiated Enrollment
Allows users to enroll via the login page from the identity provider

CONFIGURE ENROLLMENT ACCESS FOR:
● Any identity provider user
○ Only this group:

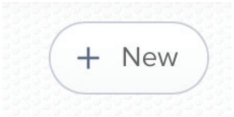
Cancel Save

Done

36. Select Jamf Pro User Accounts & Groups.

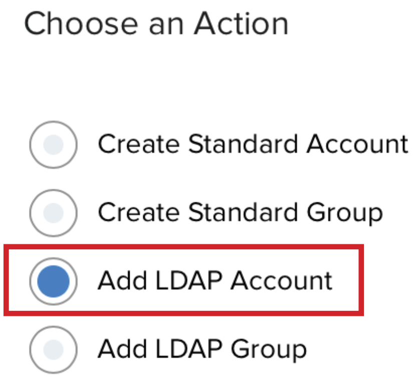


37. Select New.



38. Select Add LDAP Account.

NOTE: If you have groups setup in Azure Active Directory best practice is to add it here instead of adding a single user. I'm using a single user for simplicity of this guide.



Choose an Action

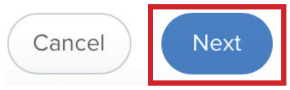
○ Create Standard Account

○ Create Standard Group

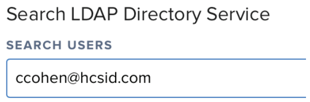
● Add LDAP Account

○ Add LDAP Group

39. Click Next.



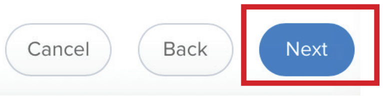
40. Search for a user account in your Azure Active Directory.



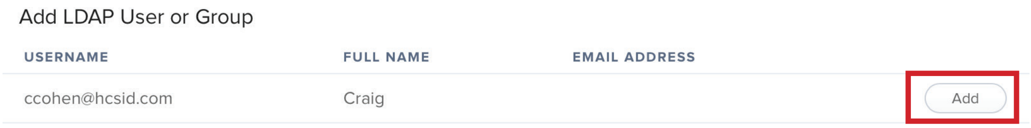
Search LDAP Directory Service

SEARCH USERS: ccohen@hcsid.com

41. Click Next.



42. Click Add.

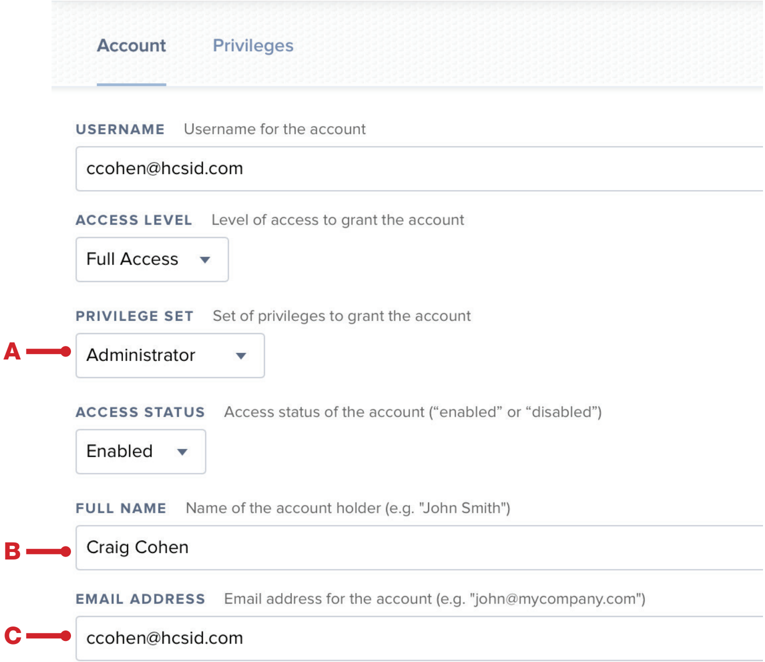


Add LDAP User or Group

USERNAME	FULL NAME	EMAIL ADDRESS	
ccohen@hcsid.com	Craig		Add

43. Enter the following:

A. Privilege Set, then select the appropriate privilege set for the user. I will select Administrator for this guide.
B. Full Name: Make sure the users full name is entered in the field.
C. Email Address: Enter the users email address.



USERNAME Username for the account
ccohen@hcsid.com

ACCESS LEVEL Level of access to grant the account
Full Access

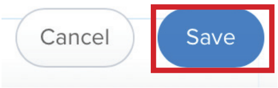
PRIVILEGE SET Set of privileges to grant the account
Administrator

ACCESS STATUS Access status of the account (“enabled” or “disabled”)
Enabled

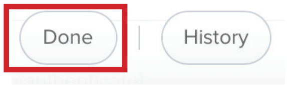
FULL NAME Name of the account holder (e.g. "John Smith")
Craig Cohen

EMAIL ADDRESS Email address for the account (e.g. "john@mycompany.com")
ccohen@hcsid.com

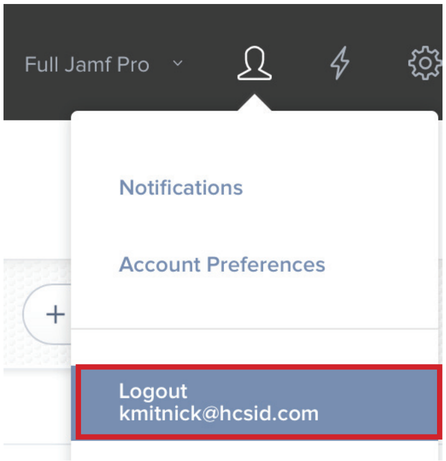
44. Click Save.



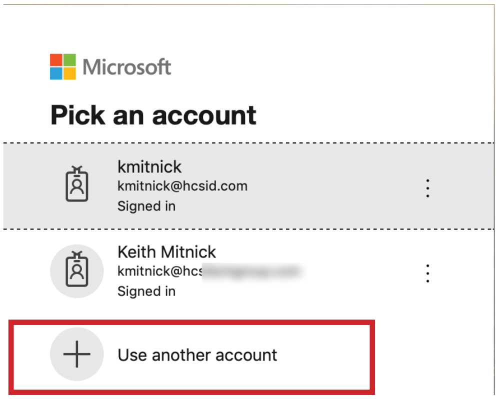
45. Click Done.



46. Click on the account menu, then select Logout for the user you’re currently logged in as.



47. Login to your Jamf Pro server. You will be re directed to a Microsoft login window. Select Use another account.

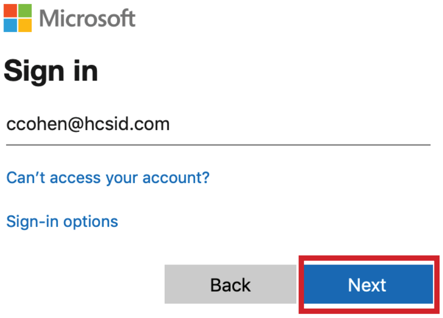


Pick an account

kmitnick
kmitnick@hcsid.com
Signed in

Keith Mitnick
kmitnick@hcs[redacted]
Signed in

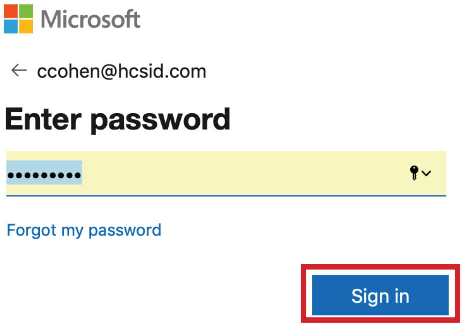
48. Enter the LDAP user account that we created in Jamf Pro in step 42. E.G. ccohen@hcsid.com. Select Next.



Sign in

ccohen@hcsid.com

49. Enter the users password then select Sign in.

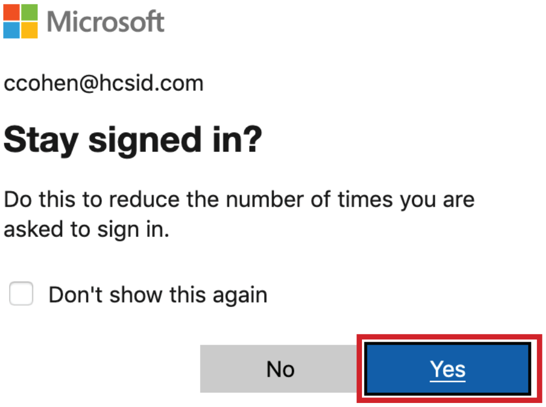


← ccohen@hcsid.com

Enter password

•••••••••

50. For the purposes of this guide, select yes at the screen below. In a production environment, you can decide for yourself what to do at this screen.



Microsoft

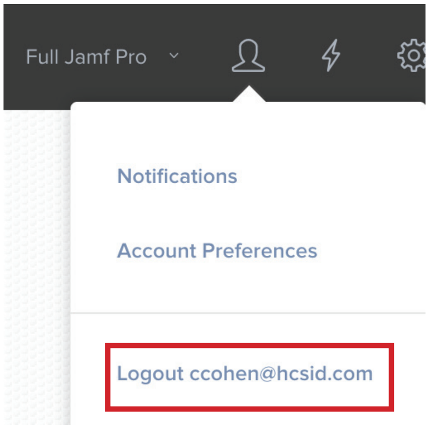
ccohen@hcsid.com

Stay signed in?

Do this to reduce the number of times you are asked to sign in.

□ Don't show this again

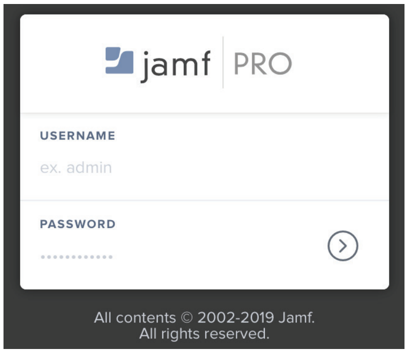
51. You are now signed into the Jamf Pro server via Single Sign On. (SSO). Click on the account menu, then select Logout for the user you're currently logged in as. This completes this section.



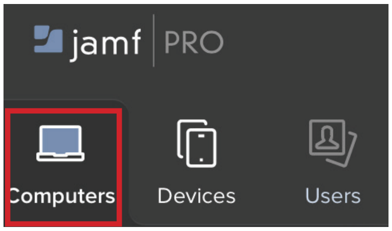
Section 6: Automated Device Enrollment with LDAPS

NOTE: This section assumes you have your Jamf Pro server tied into Apple business manager or Apple school manager. We don't cover configuring that in this guide.

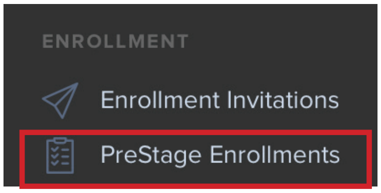
1. If necessary, Log into your Jamf Pro server.



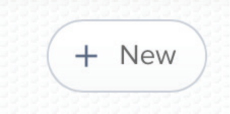
2. Select Computers.



3. Select PreStage Enrollments.

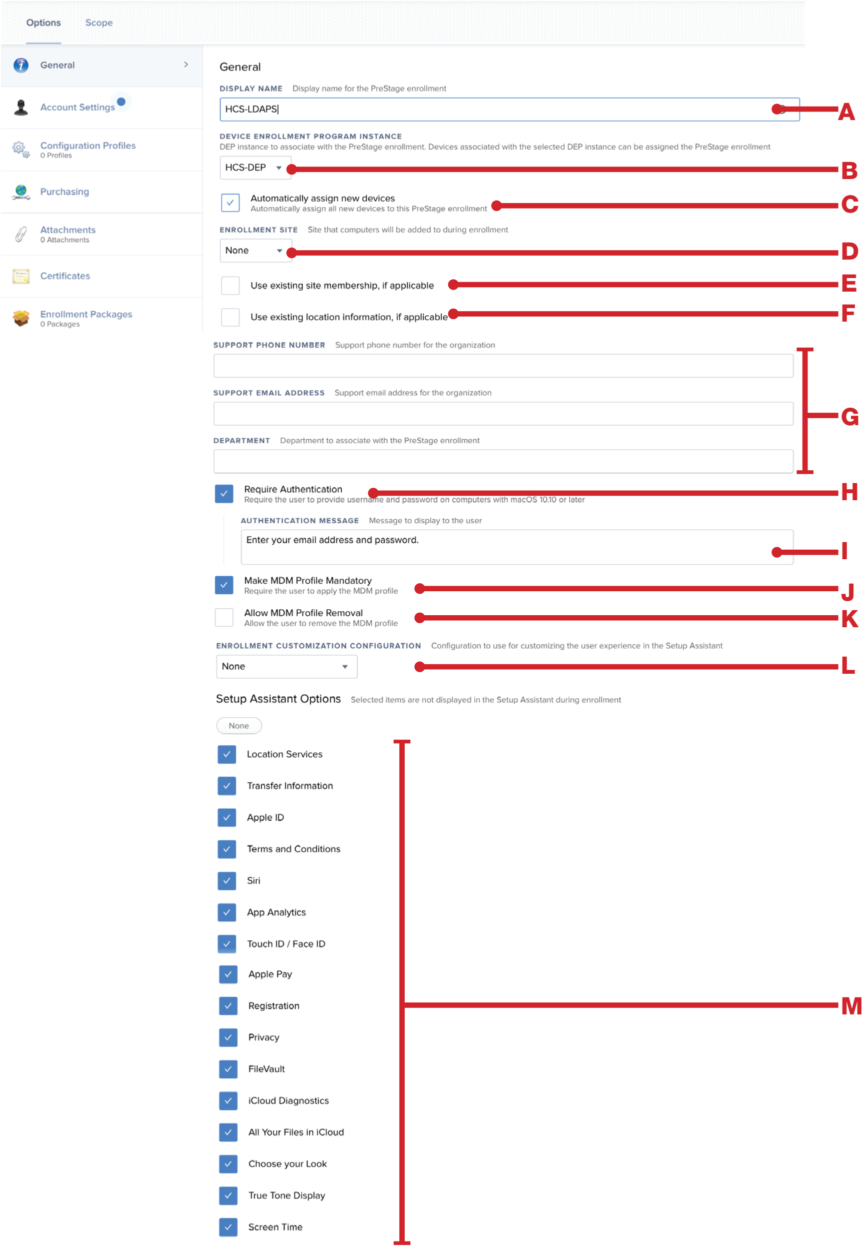


4. Select New.



5. Select General, then enter the following:

A. Display Name: Enter anything you want. I will enter HCS-LDAPS.
B. Device Enrollment Program Instance: Select your DEP instance.
C. Automatically assign new devices: I will enable this for simplicity. It's not necessary as you can have multiple PreStage Enrollments.
D. Enrollment Site: Leave this set to None. If you use sites, then select one.
E. Use existing site membership, if applicable: Disable this.
F. Use existing location information, if applicable: Disable this.
G. Support Phone, Support Email, and Department: Leave them blank.
H. Require Authentication: Enable this.
I. Authentication Message: Enter whatever you need here. For simplicity, I will ask the user for their email address and password.
J. Make MDM Profile Mandatory: Enable this.
K. All MDM Profile Removal: Disable this.
L. Enrollment Customization Configuration: None
M. Setup Assistance Options: For simplicity of this guide, Click the Select All button.



General

DISPLAY NAME Display name for the PreStage enrollment

HCS-LDAPS|

DEVICE ENROLLMENT PROGRAM INSTANCE
DEP instance to associate with the PreStage enrollment. Devices associated with the selected DEP instance can be assigned the PreStage enrollment

HCS-DEP

☑ Automatically assign new devices
Automatically assign all new devices to this PreStage enrollment

ENROLLMENT SITE Site that computers will be added to during enrollment

None

☐ Use existing site membership, if applicable

☐ Use existing location information, if applicable

SUPPORT PHONE NUMBER Support phone number for the organization

SUPPORT EMAIL ADDRESS Support email address for the organization

DEPARTMENT Department to associate with the PreStage enrollment

☑ Require Authentication
Require the user to provide username and password on computers with macOS 10.10 or later

AUTHENTICATION MESSAGE Message to display to the user

Enter your email address and password.

☑ Make MDM Profile Mandatory
Require the user to apply the MDM profile

☐ Allow MDM Profile Removal
Allow the user to remove the MDM profile

ENROLLMENT CUSTOMIZATION CONFIGURATION Configuration to use for customizing the user experience in the Setup Assistant

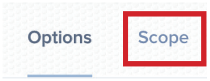
None

Setup Assistant Options Selected items are not displayed in the Setup Assistant during enrollment

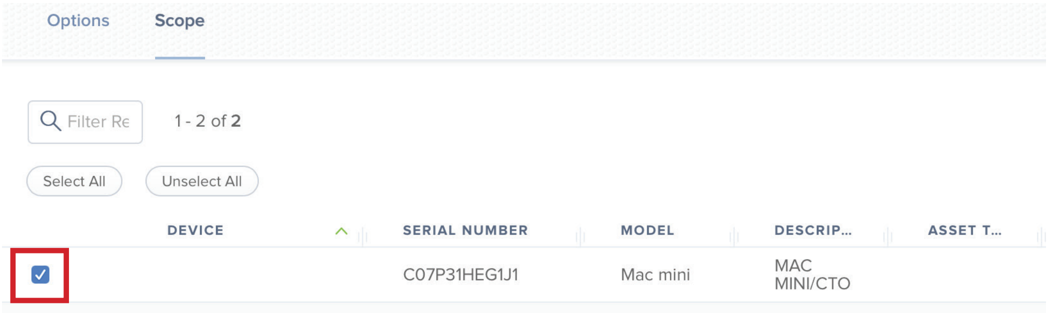
None

☑ Location Services
☑ Transfer Information
☑ Apple ID
☑ Terms and Conditions
☑ Siri
☑ App Analytics
☑ Touch ID / Face ID
☑ Apple Pay
☑ Registration
☑ Privacy
☑ FileVault
☑ iCloud Diagnostics
☑ All Your Files in iCloud
☑ Choose your Look
☑ True Tone Display
☑ Screen Time

6. Select Scope.

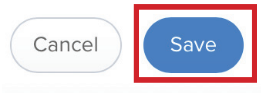


7. If necessary, select a Mac Computer from the list.

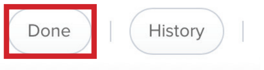


	DEVICE	SERIAL NUMBER	MODEL	DESCRIP...	ASSET T...
☑		C07P31HEG1J1	Mac mini	MAC MINI/CTO	

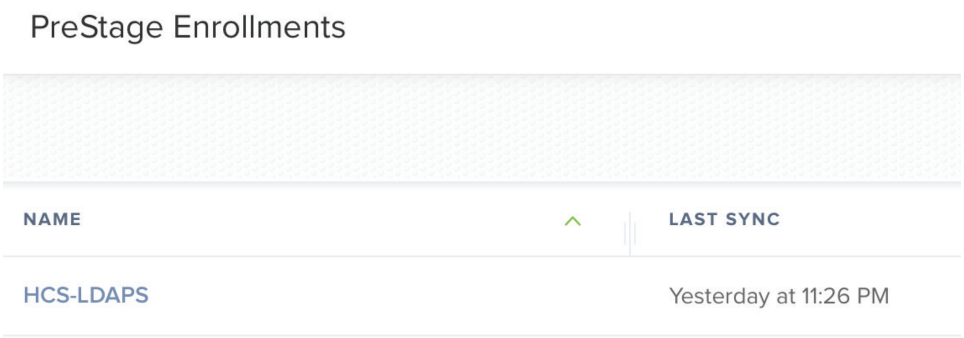
8. Select Save.



9. Select Done.



10. Your PreStage Enrollment will show up in the list. Stayed logged into your Jamf Pro server, we will need it in a later step.

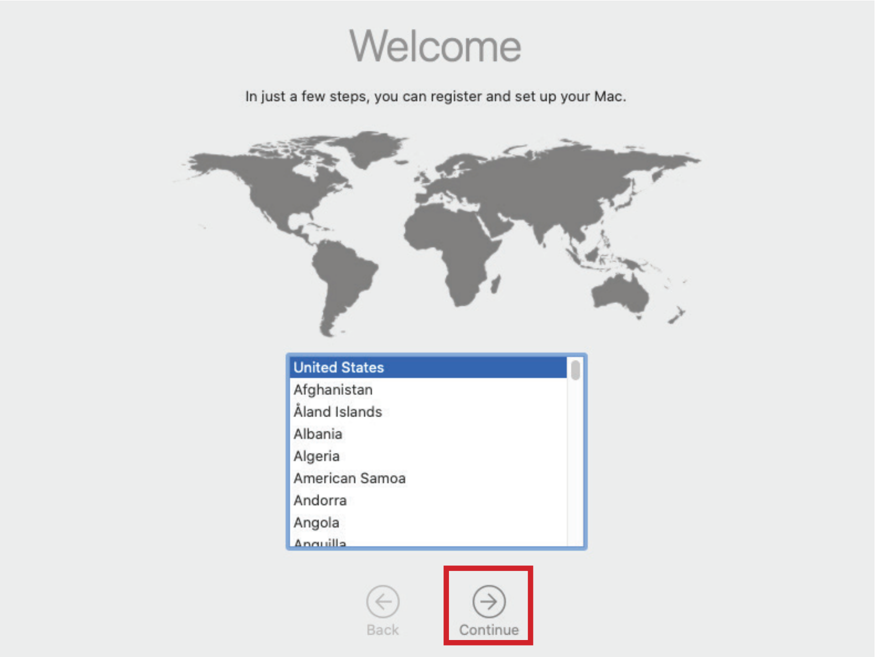


PreStage Enrollments

NAME	LAST SYNC
HCS-LDAPS	Yesterday at 11:26 PM

11. For this step, you need either a brand new Mac still in the box or a Mac with a clean install of macOS Catalina that has never been booted and is in the PreStage we just created.

    Power on the Mac Computer, then select your country.

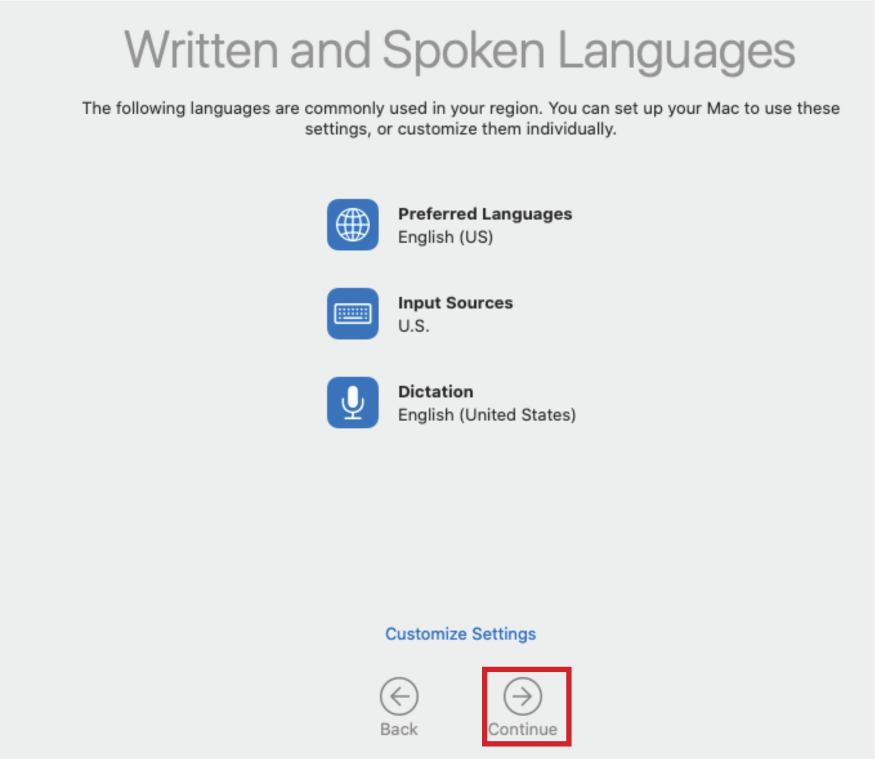


Welcome

In just a few steps, you can register and set up your Mac.

United States
Afghanistan
Åland Islands
Albania
Algeria
American Samoa
Andorra
Angola
Anguilla

12. Select Continue.



Written and Spoken Languages

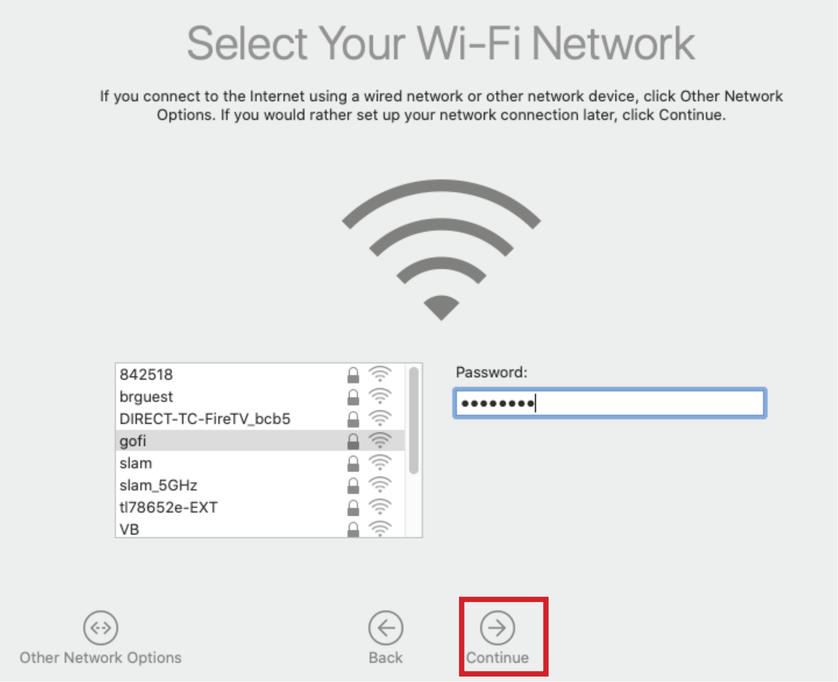
The following languages are commonly used in your region. You can set up your Mac to use these settings, or customize them individually.

Preferred Languages
English (US)

Input Sources
U.S.

Dictation
English (United States)

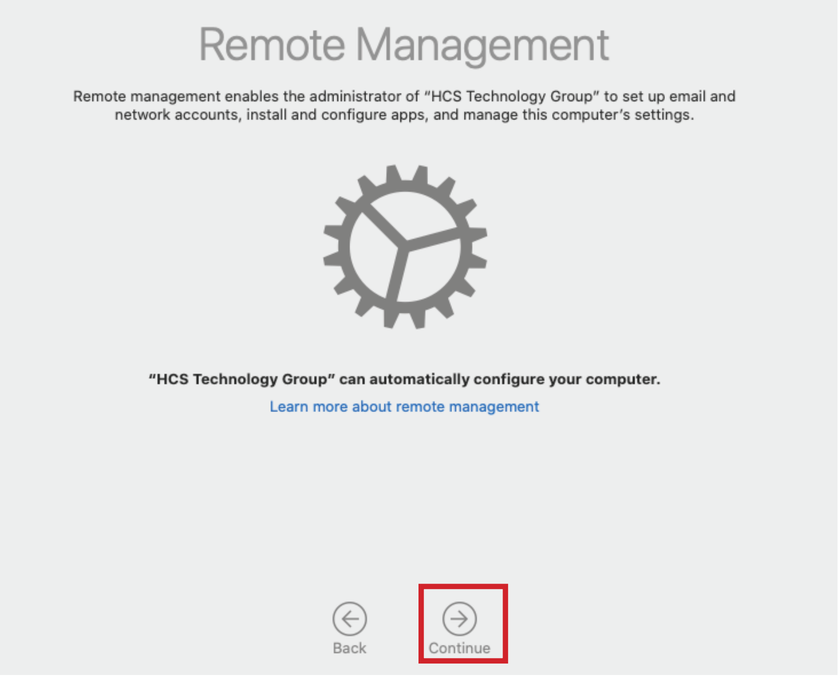
13. If necessary select your wifi. If you're Mac Computer is plugged into ethernet, you will not see this screen. Select Continue.



Select Your Wi-Fi Network

If you connect to the Internet using a wired network or other network device, click Other Network Options. If you would rather set up your network connection later, click Continue.

14. At the Remote Management screen, select Continue.



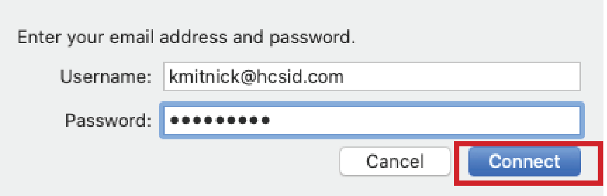
Remote Management

Remote management enables the administrator of "HCS Technology Group" to set up email and network accounts, install and configure apps, and manage this computer's settings.

"HCS Technology Group" can automatically configure your computer.

Learn more about remote management

15. Enter your LDAPS credentials. These credentials will come from Microsoft Azure LDAPS. Select Connect.



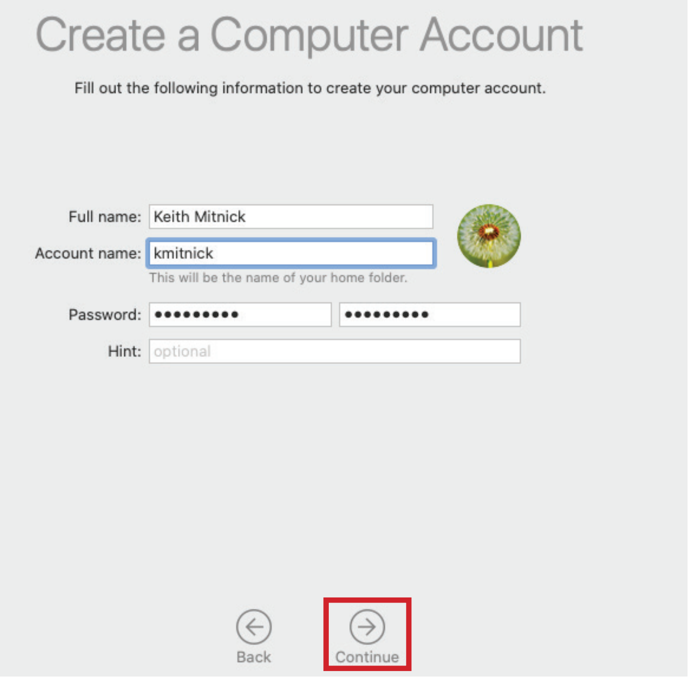
Enter your email address and password.

Username: kmitnick@hcsid.com

Password: ●●●●●●●●●

16. Create a computer account, then select Continue. You should not see any other screens after this as we chose to skip all setup screen for the simplicity of this guide.

Note: Your LDAPS credentials will show up here.



Create a Computer Account

Fill out the following information to create your computer account.

Full name: Keith Mitnick

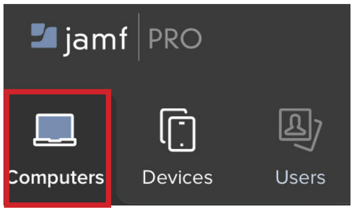
Account name: kmitnick

This will be the name of your home folder.

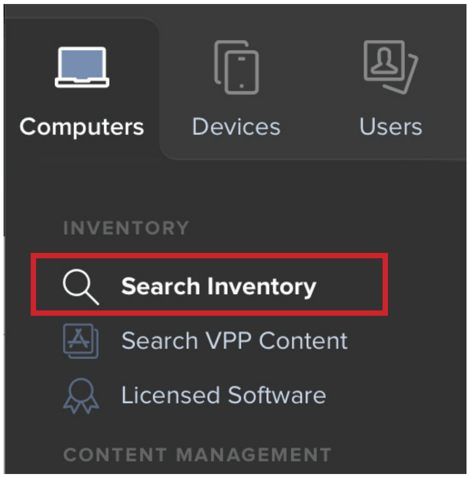
Password: ●●●●●●●●● ●●●●●●●●●

Hint: optional

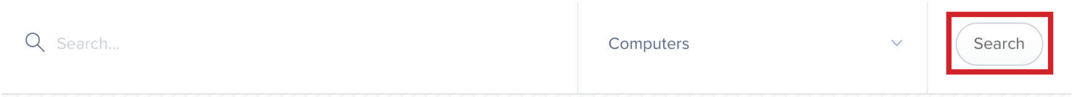
17. In your Jamf Pro server, Select Computers.



18. Select Search Inventory.

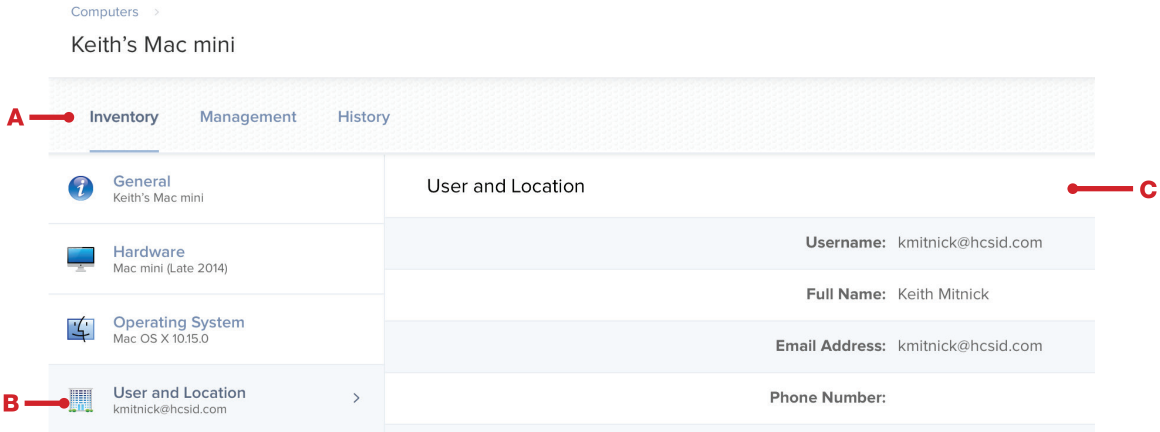


19. Search for the Mac computer we just enrolled. Enter the computer name in the search field, then select Search button.



20. Open the computer record, then select select the following:

A. Select the Inventory Tab.
B. Select User and Location.
C. Notice the information for the user was populated from LDAPS via Azure.



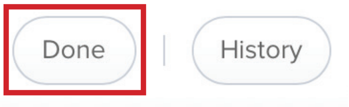
Username: kmitnick@hcsid.com

Full Name: Keith Mitnick

Email Address: kmitnick@hcsid.com

Phone Number:

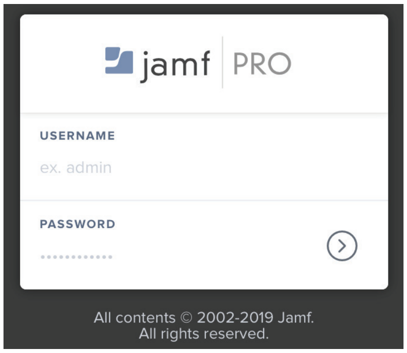
21. Select Done. This completes this lesson.



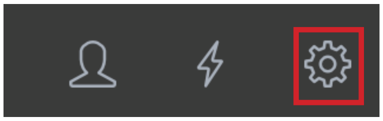
Section 7: Automated Device Enrollment with Single Sign On (SSO)

NOTE: This section assumes you have your Jamf Pro server tied into Apple business manager or Apple school manager. We don't cover configuring that in this guide.

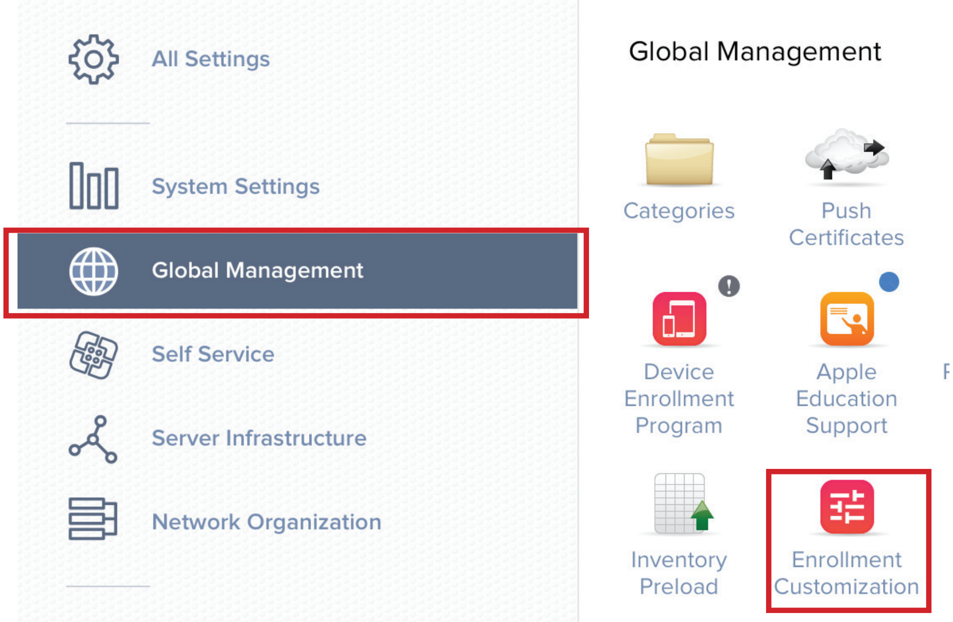
1. If necessary, Log into your Jamf Pro server.



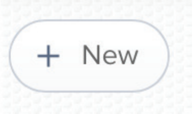
2. Click the Settings in the upper right corner.



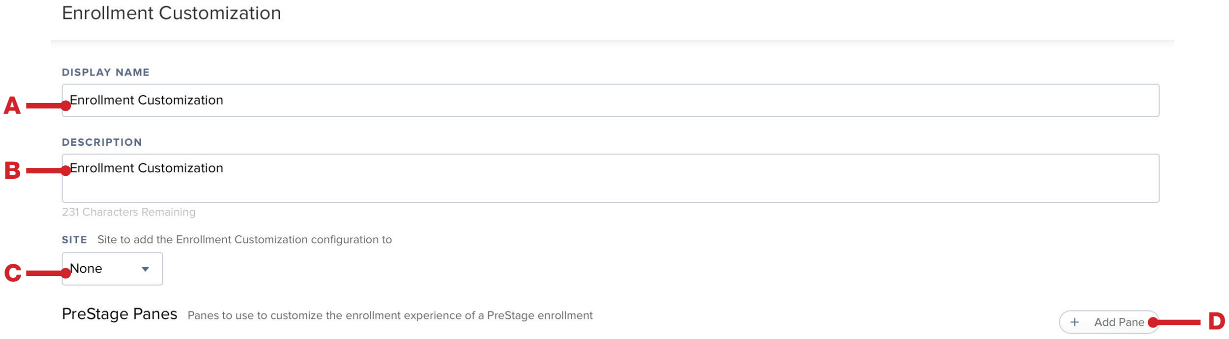
3. Select Global Management, then select Enrollment Customization.



4. Select New.



5. Enter a the following:
    A. Display Name: Enter a name of your choosing.
    B. Description: Enter a description of your choosing.
    C. Site: If you use sites, choose a site, Otherwise select None.
    D. Select the Add Pane button.



Enrollment Customization

DISPLAY NAME

Enrollment Customization

DESCRIPTION

Enrollment Customization

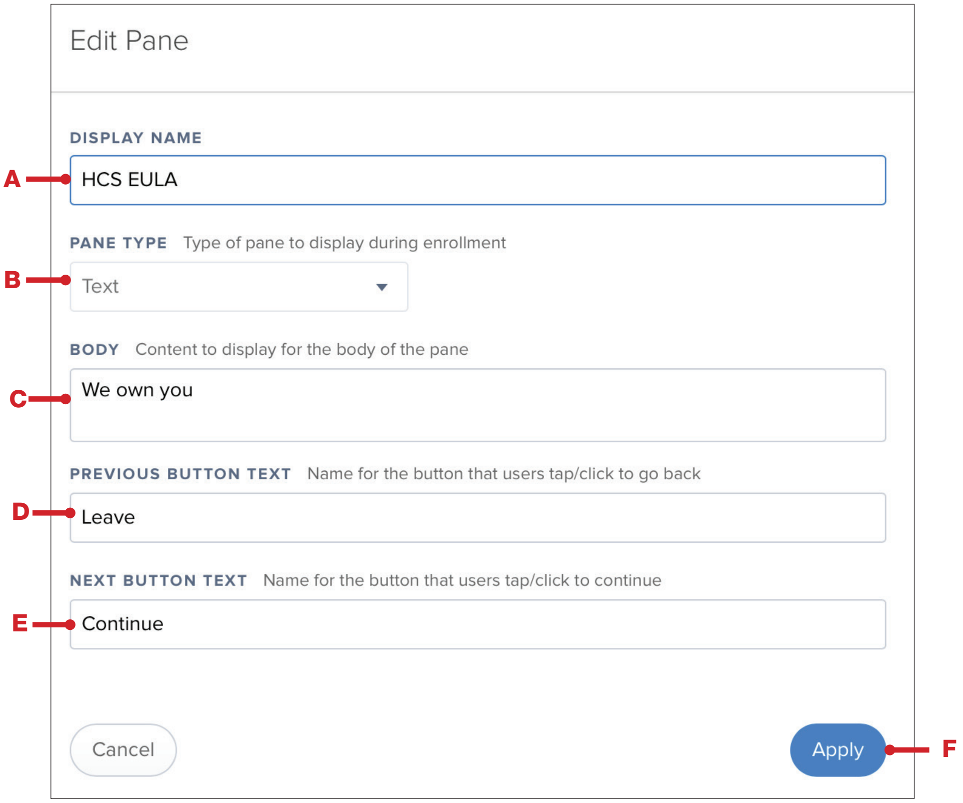
231 Characters Remaining

SITE Site to add the Enrollment Customization configuration to

None

PreStage Panes Panes to use to customize the enrollment experience of a PreStage enrollment

6. In this step we will configure a EULA page. Enter the following:
    A. Display Name: Enter a name of your choosing.
    B. Pane Type: Select Text
    C. Body: Enter a message.
    D. Previous Button Text: Enter a button name.
    E. Next Button Text: Enter a button name.
    F. Select Apply.



Edit Pane

DISPLAY NAME

HCS EULA

PANE TYPE Type of pane to display during enrollment

Text

BODY Content to display for the body of the pane

We own you

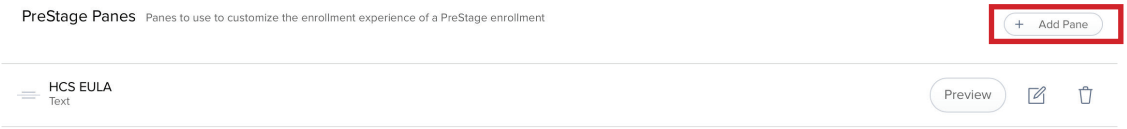
PREVIOUS BUTTON TEXT Name for the button that users tap/click to go back

Leave

NEXT BUTTON TEXT Name for the button that users tap/click to continue

Continue

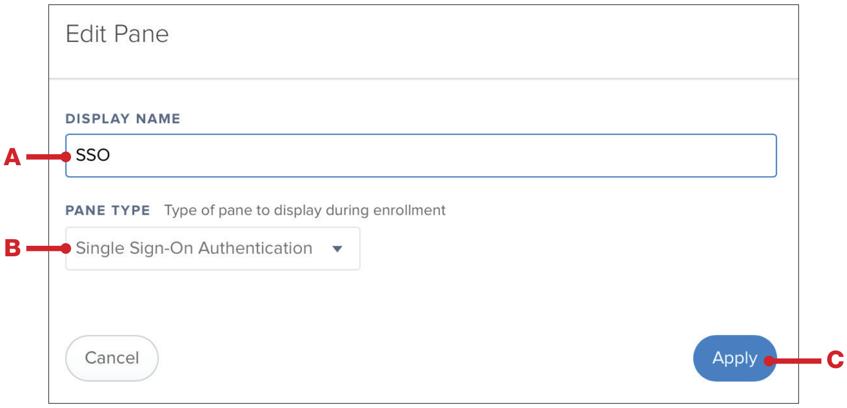
7. Your EULA will show up in the list. Select the Add Pane button.



PreStage Panes Panes to use to customize the enrollment experience of a PreStage enrollment

HCS EULA
Text

8. In this step we will configure an SSO sign in page.Enter the following:
    A. Display Name: Enter a display name.
    B. Pane Type: Select Single Sign-On Authentication
    C. Select Apply.

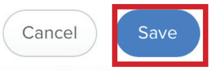


Edit Pane

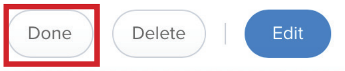
DISPLAY NAME
SSO

PANE TYPE Type of pane to display during enrollment
Single Sign-On Authentication

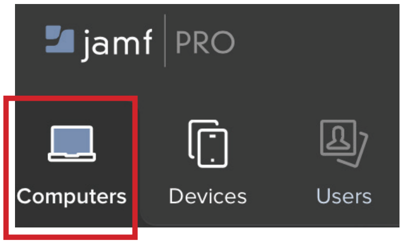
9. Select Save.



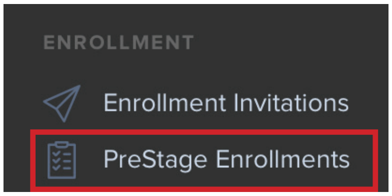
10. Select Done.



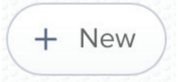
11. Select Computers.



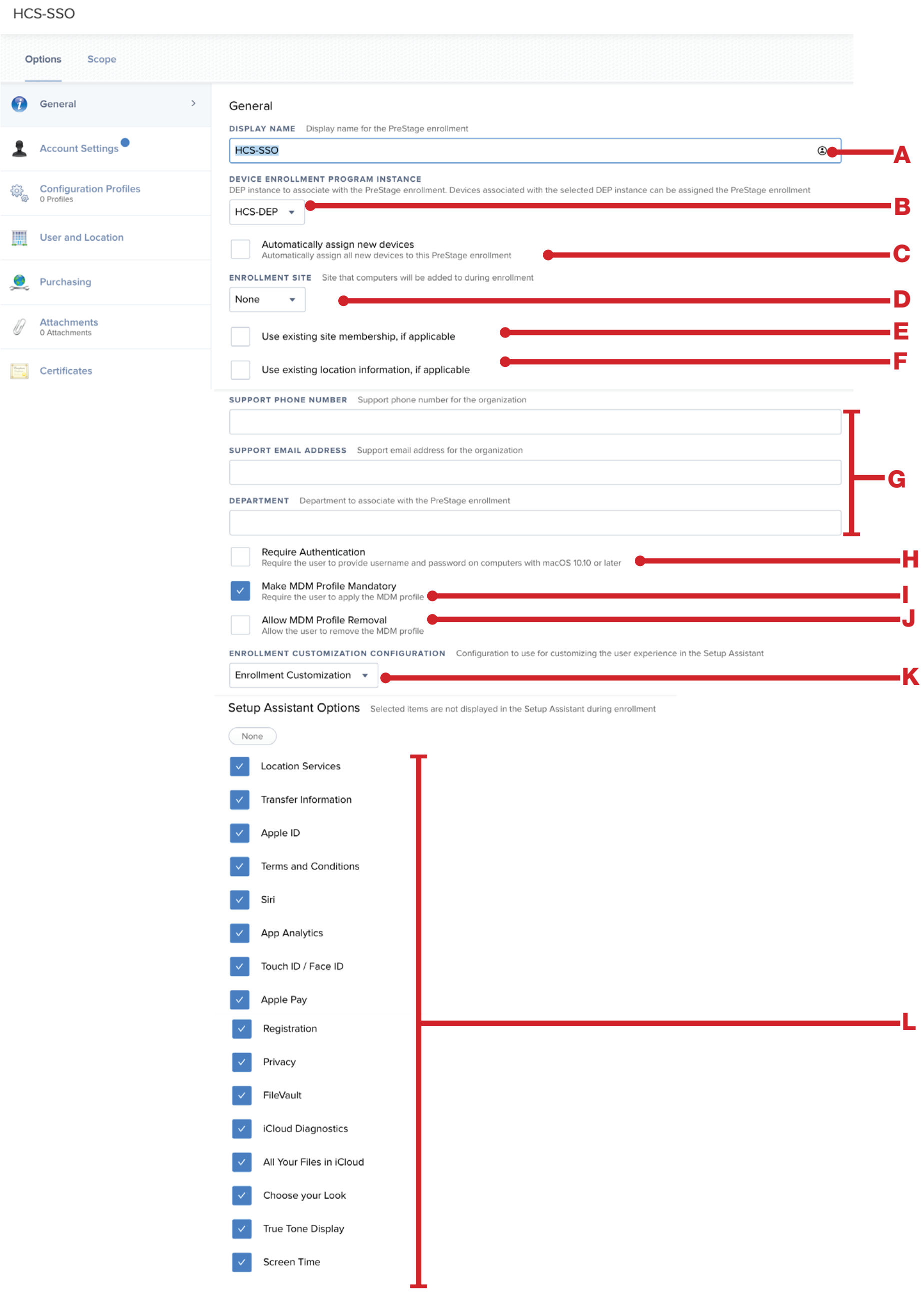
12. Select PreStage Enrollments.



13. Select New.



14. Select Options, then General. Enter the following info:
    A. Display Name: Enter anything you want. I will enter HCS-SSO.
    B. Device Enrollment Program Instance: Select your DEP instance.
    C. Automatically assign new devices: Disable this.
    D. Enrollment Site: Leave this set to None. If you use sites, then select one.
    E. Use existing site membership, if applicable: Disable this.
    F. Use existing location information, if applicable: Disable this.
    G. Support Phone, Support Email, and Department: Leave them blank.
    H. Require Authentication: You can disable this or keep it on if you want older versions of macOS to authenticate. If your using macOS Catalina, the Entollment Customization will be triggered instead.
    I.Make MDM Profile Mandatory: Enable this.
    J. All MDM Profile Removal: Disable this.
    K. Enrollment Customization Configuration: Select your Enrollment customization,
    L. Setup Assistance Options: For simplicity of this guide, Click the Select All button.



HCS-SSO

General

DISPLAY NAME Display name for the PreStage enrollment

HCS-SSO

DEVICE ENROLLMENT PROGRAM INSTANCE
DEP instance to associate with the PreStage enrollment. Devices associated with the selected DEP instance can be assigned the PreStage enrollment

HCS-DEP ▾

□ Automatically assign new devices
Automatically assign all new devices to this PreStage enrollment

ENROLLMENT SITE Site that computers will be added to during enrollment

None ▾

□ Use existing site membership, if applicable

□ Use existing location information, if applicable

SUPPORT PHONE NUMBER Support phone number for the organization

SUPPORT EMAIL ADDRESS Support email address for the organization

DEPARTMENT Department to associate with the PreStage enrollment

□ Require Authentication
Require the user to provide username and password on computers with macOS 10.10 or later

☑ Make MDM Profile Mandatory
Require the user to apply the MDM profile

□ Allow MDM Profile Removal
Allow the user to remove the MDM profile

ENROLLMENT CUSTOMIZATION CONFIGURATION Configuration to use for customizing the user experience in the Setup Assistant

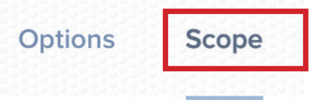
Enrollment Customization ▾

Setup Assistant Options Selected items are not displayed in the Setup Assistant during enrollment

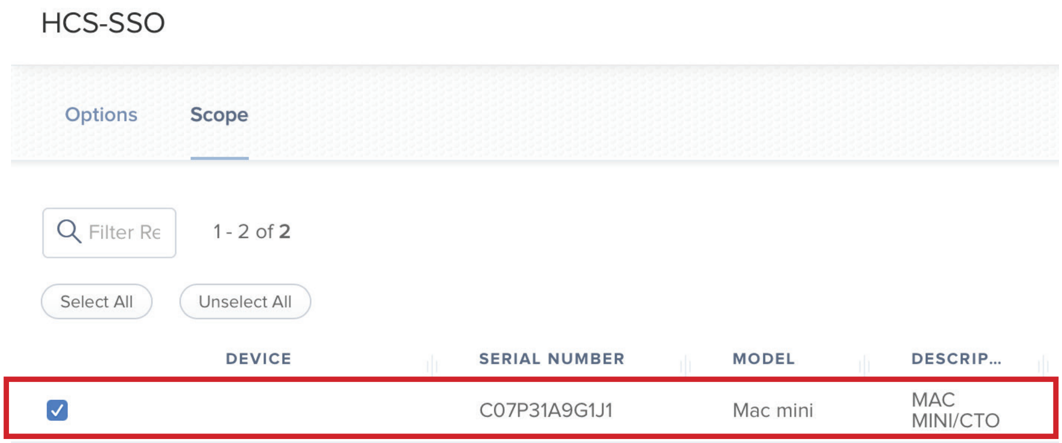
None

☑ Location Services
☑ Transfer Information
☑ Apple ID
☑ Terms and Conditions
☑ Siri
☑ App Analytics
☑ Touch ID / Face ID
☑ Apple Pay
☑ Registration
☑ Privacy
☑ FileVault
☑ iCloud Diagnostics
☑ All Your Files in iCloud
☑ Choose your Look
☑ True Tone Display
☑ Screen Time

15. Select Scope.



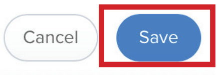
16. Select your Mac computers from the list.



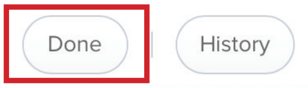
HCS-SSO

	DEVICE	SERIAL NUMBER	MODEL	DESCRIP...
☑		C07P31A9G1J1	Mac mini	MAC MINI/CTO

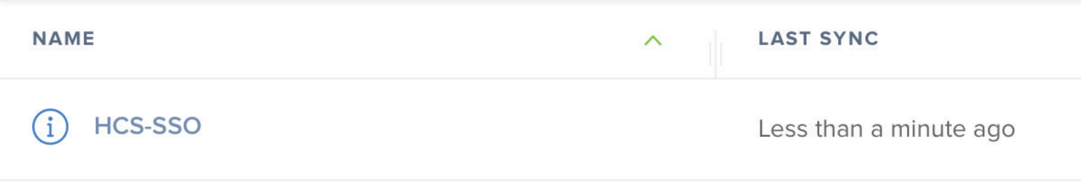
17. Click Save.



18. Click Done.



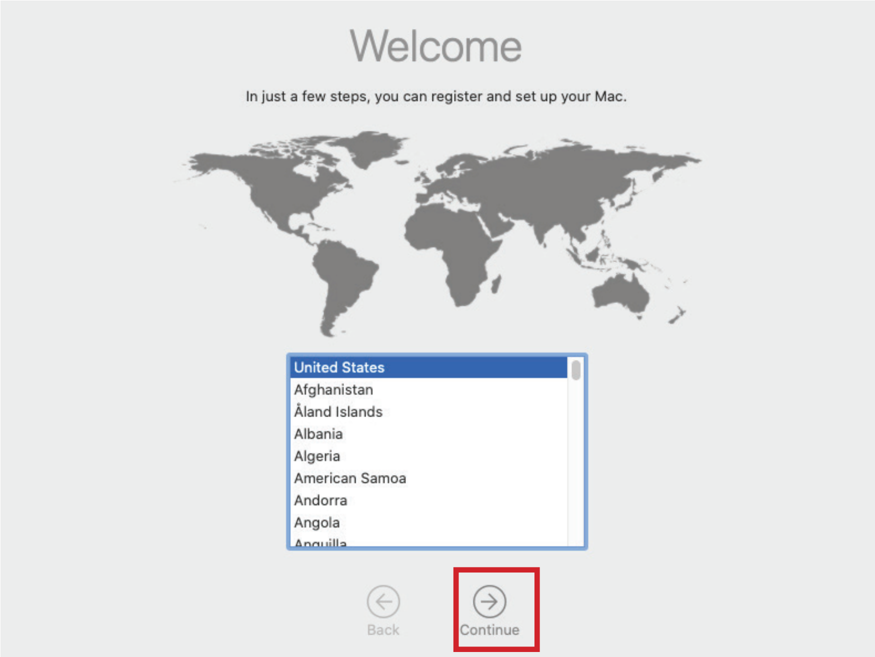
19. Your Prestage will show in the list. Notice the blue info icon, this means your PreStage is not yet in sync with apple business/school manager. It can take up to 5 minutes for the sync to compete. Once completed, the icon will go away. Stayed logged into your Jamf Pro server, we will need it in a later step.



NAME	LAST SYNC
ⓘ HCS-SSO	Less than a minute ago

20. For this step, you need either a brand new Mac still in the box or a Mac with a clean install of macOS Catalina that has never been booted and is in the PreStage we just created.

    Power on the Mac Computer, then select your country and click Continue.

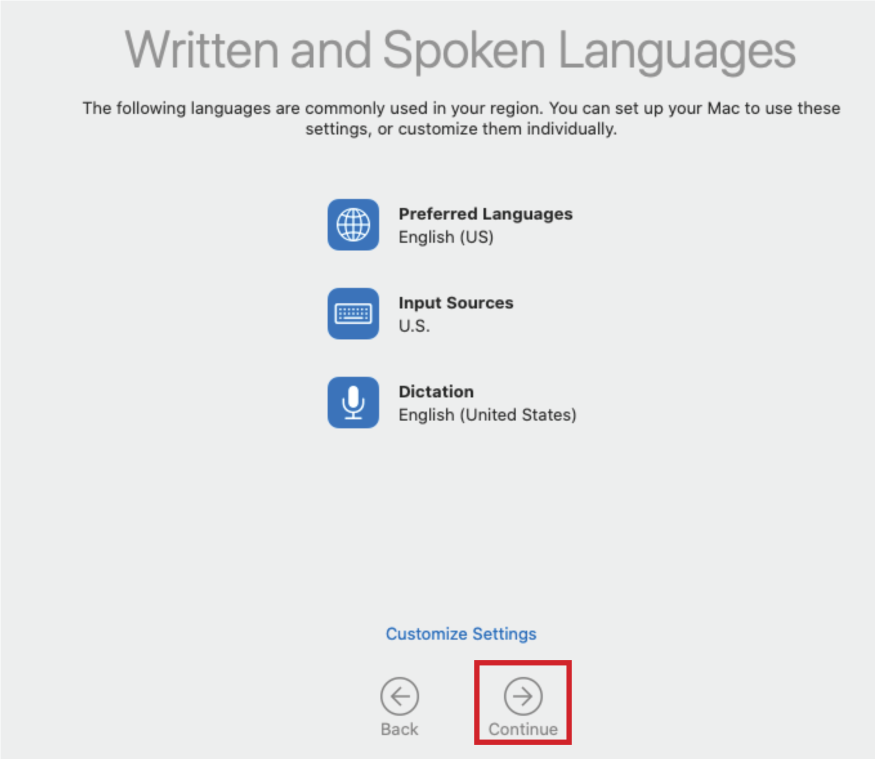


Welcome

In just a few steps, you can register and set up your Mac.

- United States
- Afghanistan
- Åland Islands
- Albania
- Algeria
- American Samoa
- Andorra
- Angola
- Anguilla

21. Click Continue.



Written and Spoken Languages

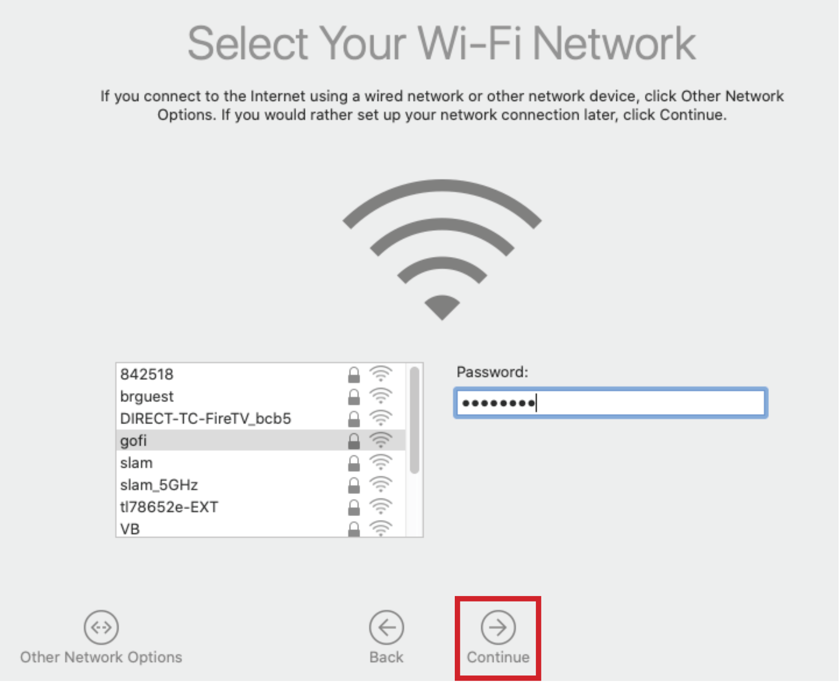
The following languages are commonly used in your region. You can set up your Mac to use these settings, or customize them individually.

Preferred Languages
English (US)

Input Sources
U.S.

Dictation
English (United States)

22. If necessary select your wifi. If you're Mac Computer is plugged into ethernet, you will not see this screen. Click Continue.

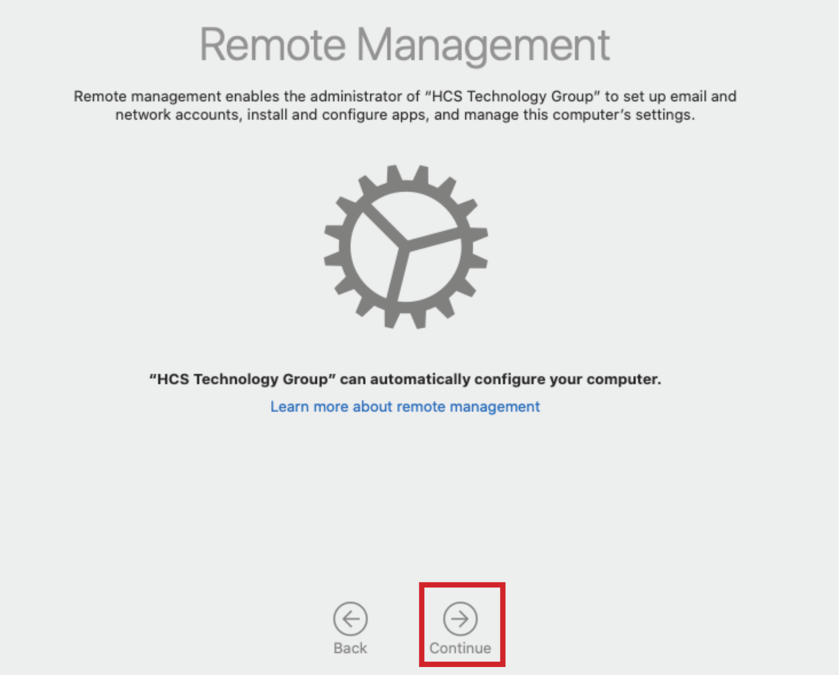


Select Your Wi-Fi Network

If you connect to the Internet using a wired network or other network device, click Other Network Options. If you would rather set up your network connection later, click Continue.

Password: ••••••••

23. At the Remote Management screen, click Continue.



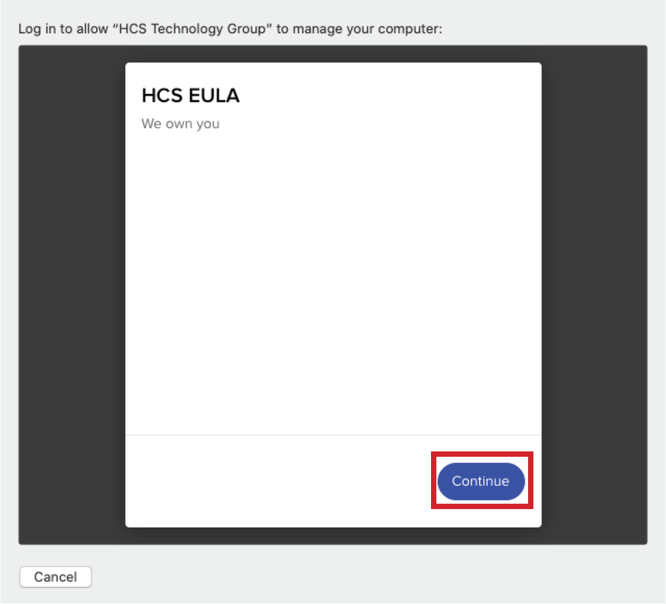
Remote Management

Remote management enables the administrator of "HCS Technology Group" to set up email and network accounts, install and configure apps, and manage this computer's settings.

"HCS Technology Group" can automatically configure your computer.

Learn more about remote management

24. At the EULA screen, click Continue.

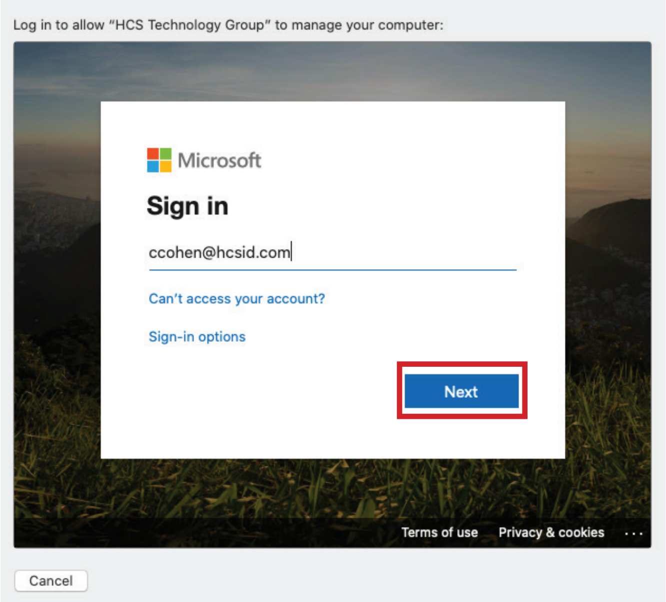


Log in to allow "HCS Technology Group" to manage your computer:

HCS EULA

We own you

25. At the Microsoft SSO Sign In screen, enter your Azure user name then click Next.



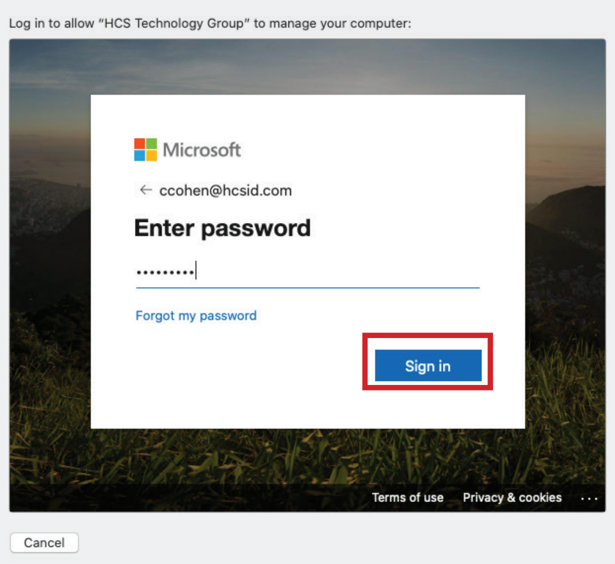
Log in to allow "HCS Technology Group" to manage your computer:

Microsoft

Sign in

ccohen@hcsid.com

26. Enter your password, then click Sign in.



Log in to allow "HCS Technology Group" to manage your computer:

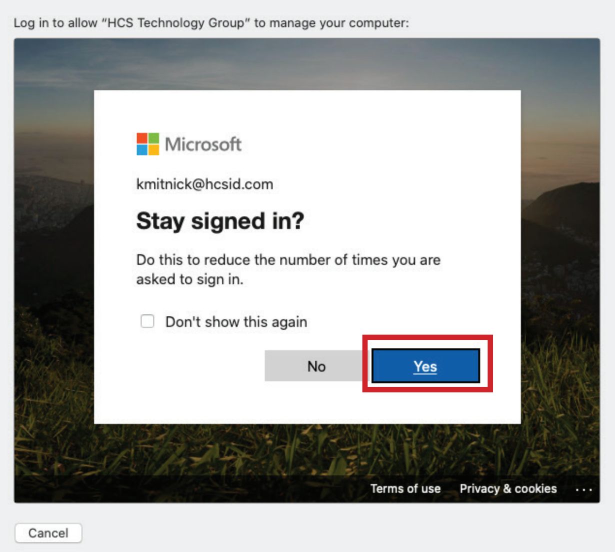
Microsoft

← ccohen@hcsid.com

Enter password

•••••••••

27. At the Stay signed in screen, make a choice. I will select Yes for this guide.



Log in to allow "HCS Technology Group" to manage your computer:

Microsoft

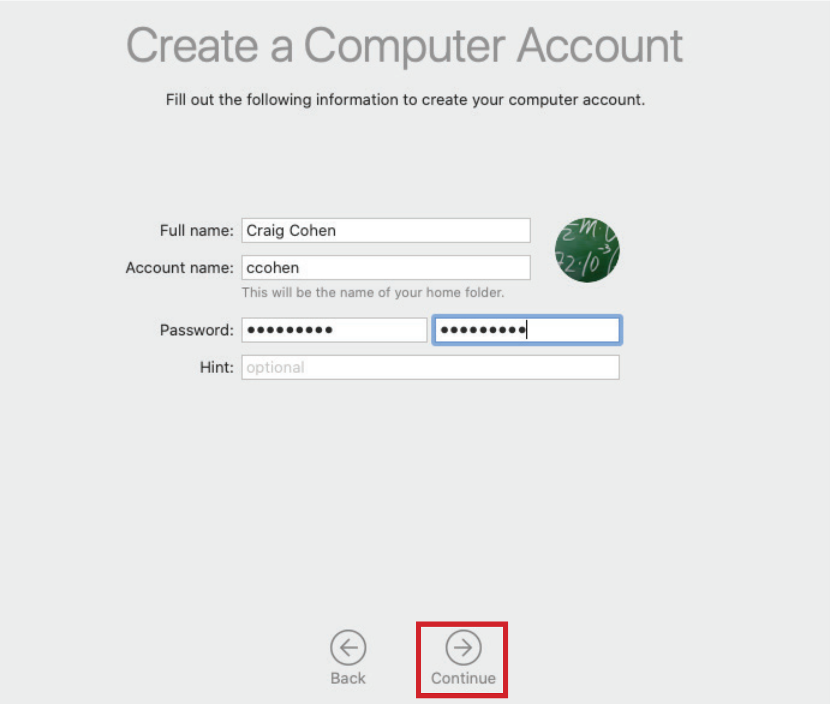
kmitnick@hcsid.com

Stay signed in?

Do this to reduce the number of times you are asked to sign in.

□ Don't show this again

28. Create a computer account, then click Continue. You should not see any other screens after this as we chose to skip all setup screen for the simplicity of this guide.



Create a Computer Account

Fill out the following information to create your computer account.

Full name: Craig Cohen

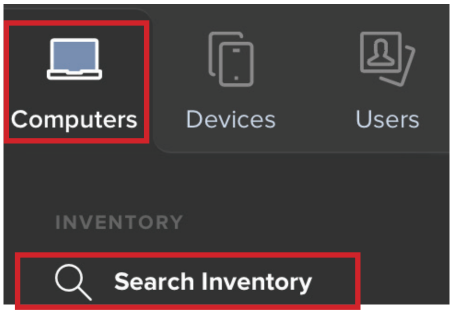
Account name: ccohen

This will be the name of your home folder.

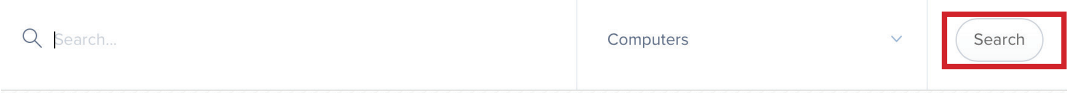
Password: •••••••••• ••••••••••

Hint: optional

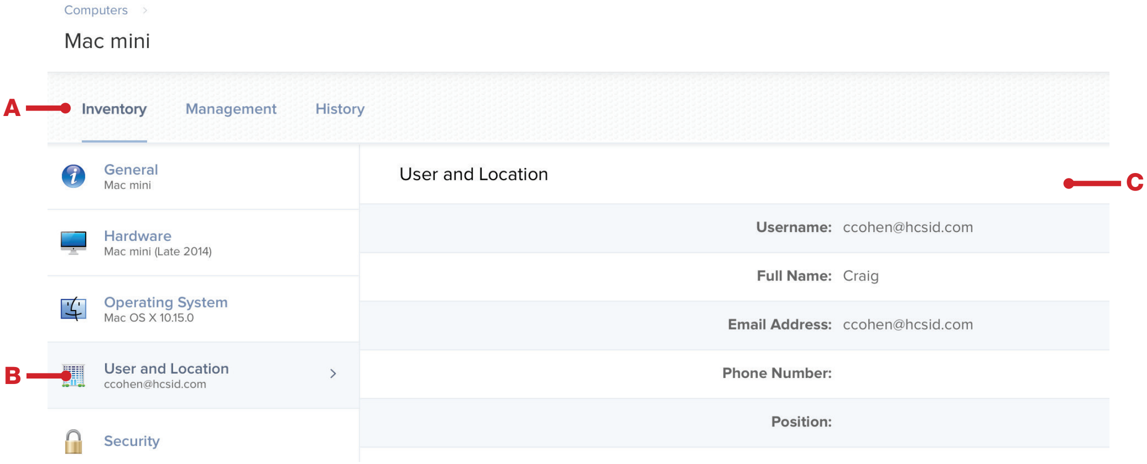
29. Switch back to your Jamf Pro server. Select Computers, then click Search Inventory.



30. Search for the Mac computer we just enrolled. Enter the computer name in the search field, then click Search.



31. Open the computer record, then select the following:
    - A. Select the Inventory Tab.
    - B. Select User and Location.
    - C. Notice the information for the user was populated from SSO via Azure.



Computers >

Mac mini

General
Mac mini

Hardware
Mac mini (Late 2014)

Operating System
Mac OS X 10.15.0

User and Location
ccohen@hcsid.com

Security

User and Location

Username: ccohen@hcsid.com

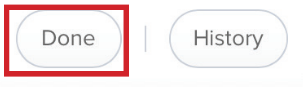
Full Name: Craig

Email Address: ccohen@hcsid.com

Phone Number:

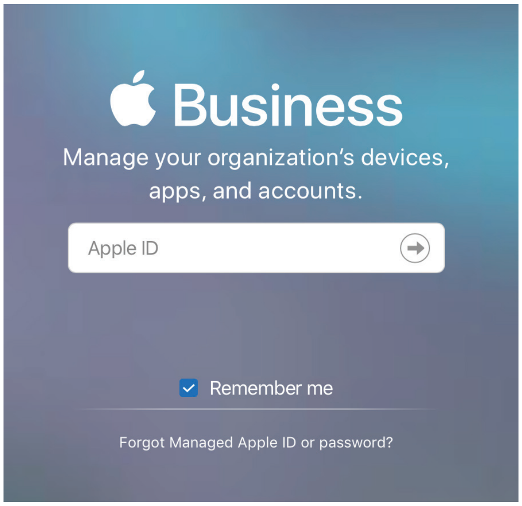
Position:

32. Click Done. This completes this lesson.

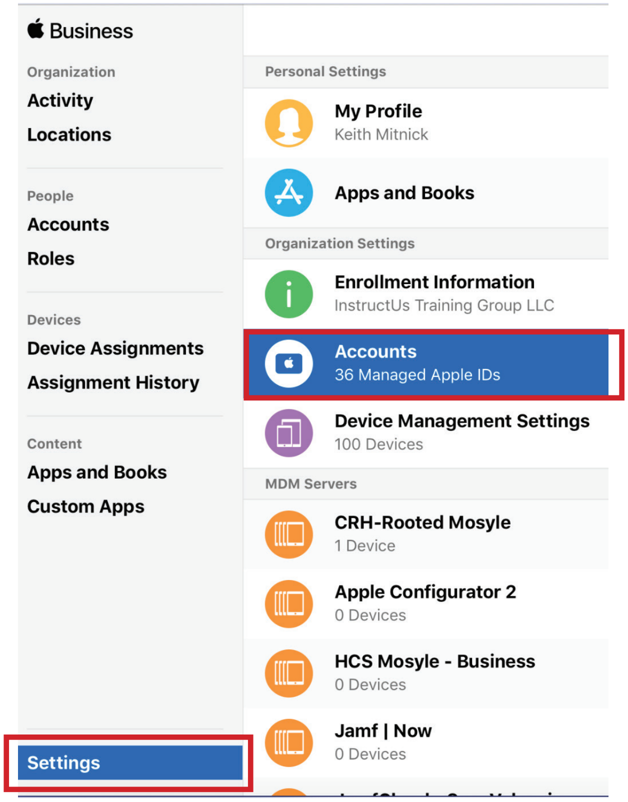


Section 8: Configure Apple Business Manager Federation with Azure Active Directory

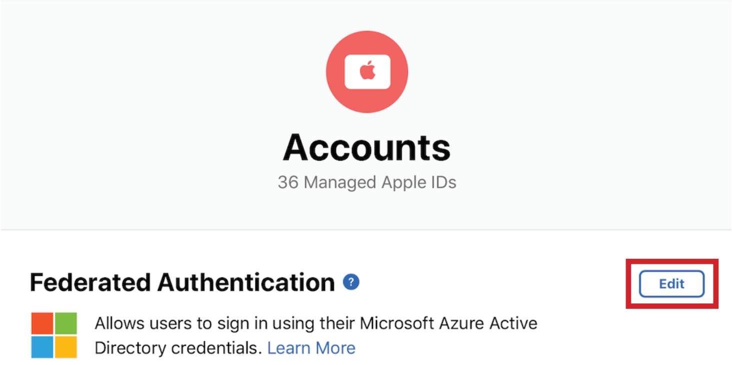
1. Log into Apple business manager at: https://business.apple.com


Business
Manage your organization's devices, apps, and accounts.
Apple ID
☑ Remember me
Forgot Managed Apple ID or password?

2. Select Settings, then select Accounts.



3. Select Federated Authentication then select Edit.



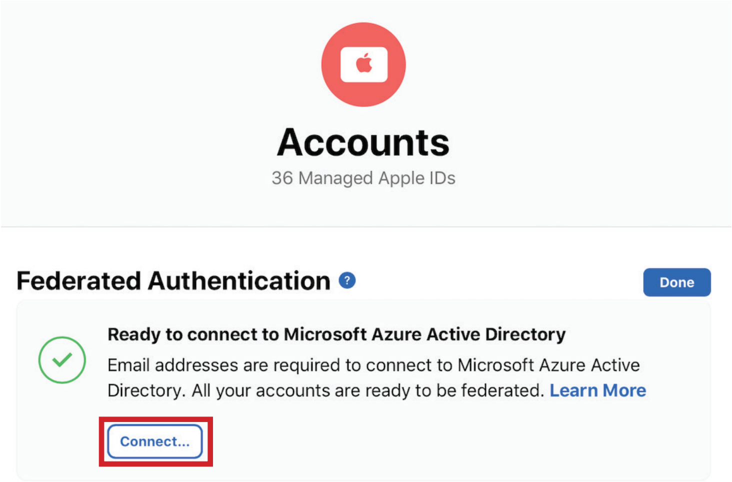
Accounts

36 Managed Apple IDs

Federated Authentication

Allows users to sign in using their Microsoft Azure Active Directory credentials. Learn More

4. Click Connect.



Accounts

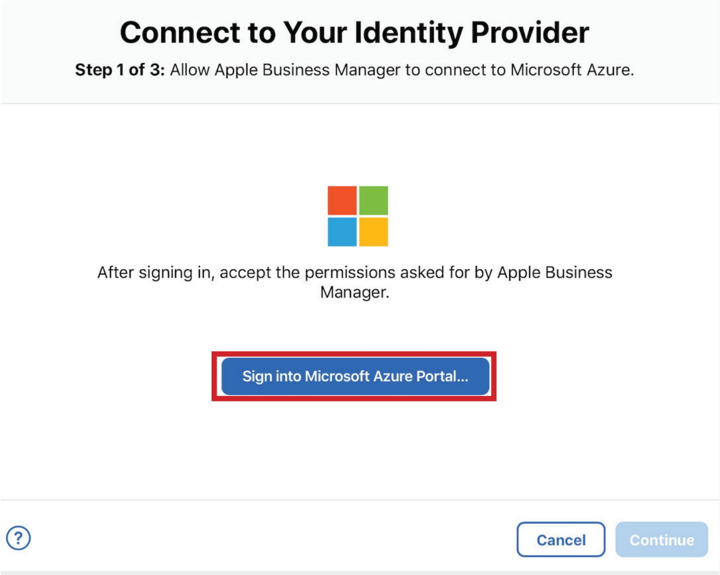
36 Managed Apple IDs

Federated Authentication

Ready to connect to Microsoft Azure Active Directory

Email addresses are required to connect to Microsoft Azure Active Directory. All your accounts are ready to be federated. **Learn More**

5. Click Sign into Microsoft Azure Portal.

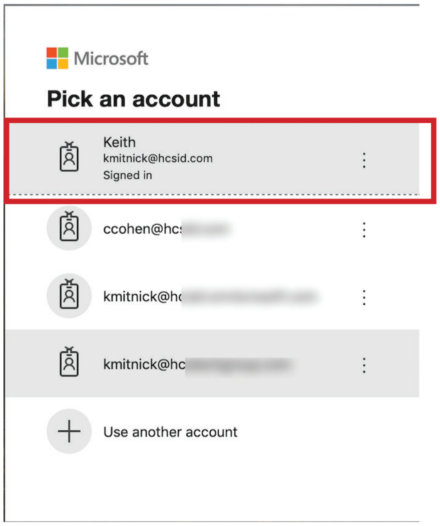


Connect to Your Identity Provider

Step 1 of 3: Allow Apple Business Manager to connect to Microsoft Azure.

After signing in, accept the permissions asked for by Apple Business Manager.

6. Select your account if shown in the list, otherwise select User another account.



Microsoft

Pick an account

Keith
kmitnick@hcsid.com
Signed in

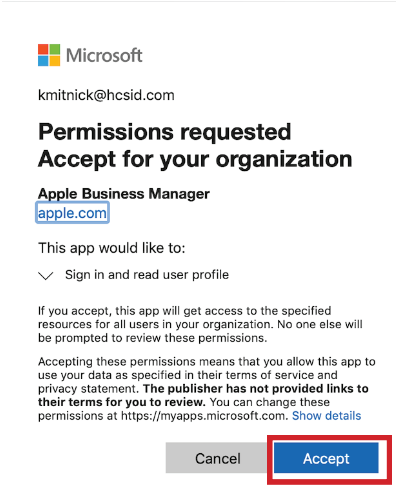
ccohen@hcs[redacted]

kmitnick@hc[redacted]

kmitnick@hc[redacted]

Use another account

7. Click Accept.



Microsoft

kmitnick@hcsid.com

Permissions requested
Accept for your organization

Apple Business Manager
apple.com

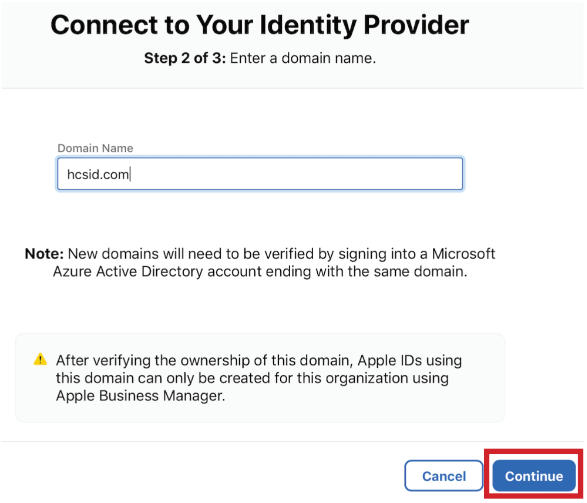
This app would like to:

Sign in and read user profile

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

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

8. Enter your domain name than click Continue.



Connect to Your Identity Provider

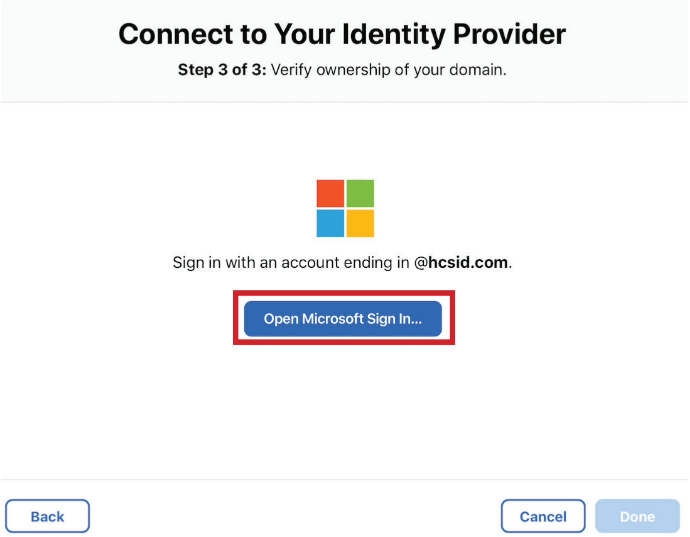
Step 2 of 3: Enter a domain name.

Domain Name: hcsid.com

Note: New domains will need to be verified by signing into a Microsoft Azure Active Directory account ending with the same domain.

After verifying the ownership of this domain, Apple IDs using this domain can only be created for this organization using Apple Business Manager.

9. Select Open Microsoft Sign In.

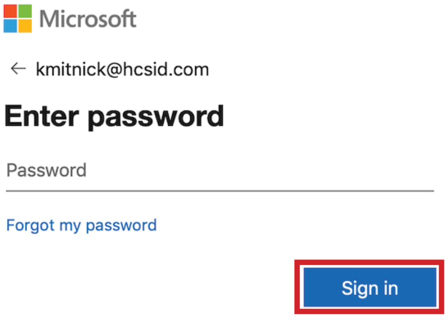


Connect to Your Identity Provider

Step 3 of 3: Verify ownership of your domain.

Sign in with an account ending in @**hcsid.com**.

10. Enter your credentials then select Sign in.

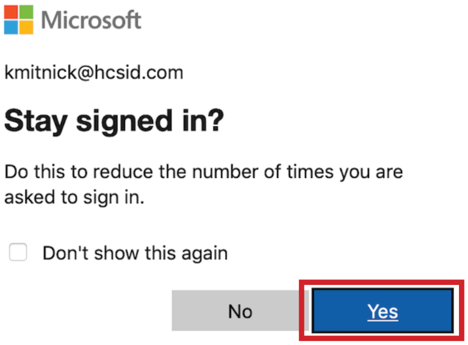


kmitnick@hcsid.com

Enter password

Password

11. Choose if you would like to stay singed in. For this guide, I will choose Yes.



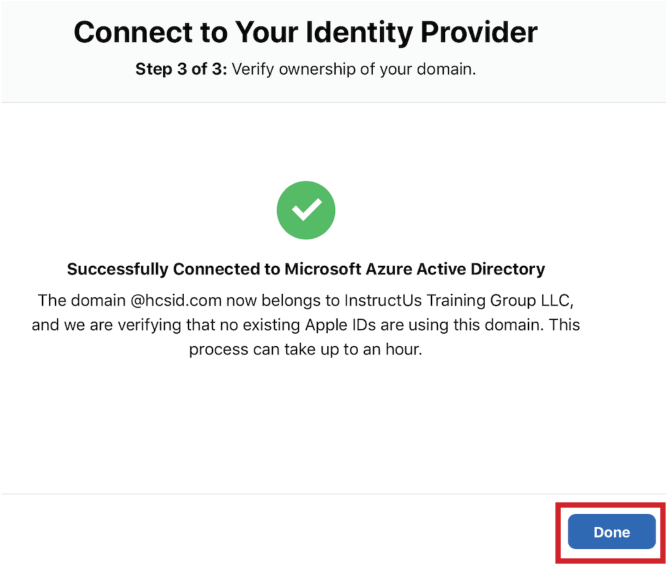
kmitnick@hcsid.com

Stay signed in?

Do this to reduce the number of times you are asked to sign in.

□ Don't show this again

12. Select Done.



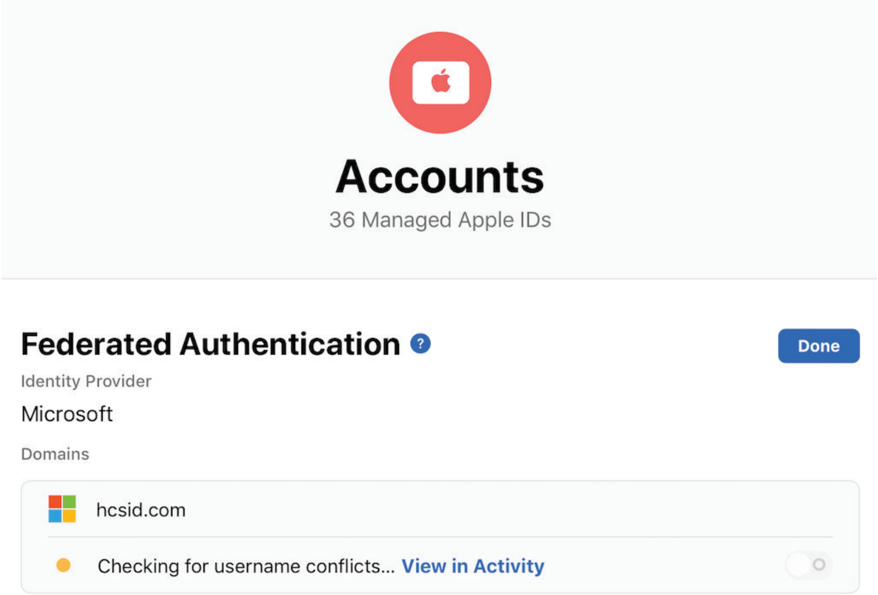
Connect to Your Identity Provider

Step 3 of 3: Verify ownership of your domain.

Successfully Connected to Microsoft Azure Active Directory

The domain @hcsid.com now belongs to InstructUs Training Group LLC, and we are verifying that no existing Apple IDs are using this domain. This process can take up to an hour.

13. Apple will check for any user name conflicts. During this time you will start to receive emails about the status of the federation.



Accounts

36 Managed Apple IDs

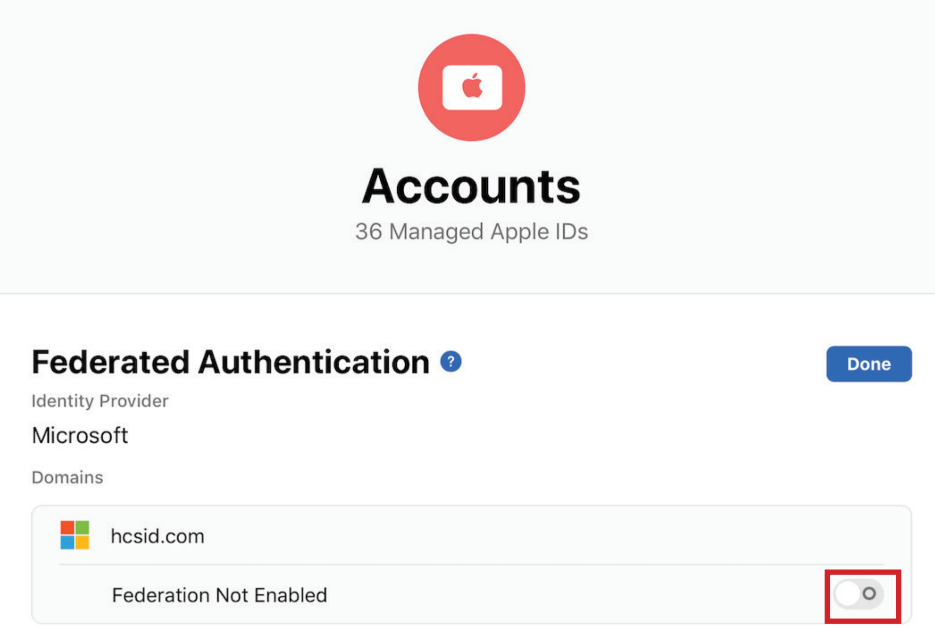
Federated Authentication

Identity Provider: Microsoft

Domains: hcsid.com

Checking for username conflicts... View in Activity

14. Select the switch icon to drag it to the right to enable the Federation.



Accounts

36 Managed Apple IDs

Federated Authentication

Identity Provider

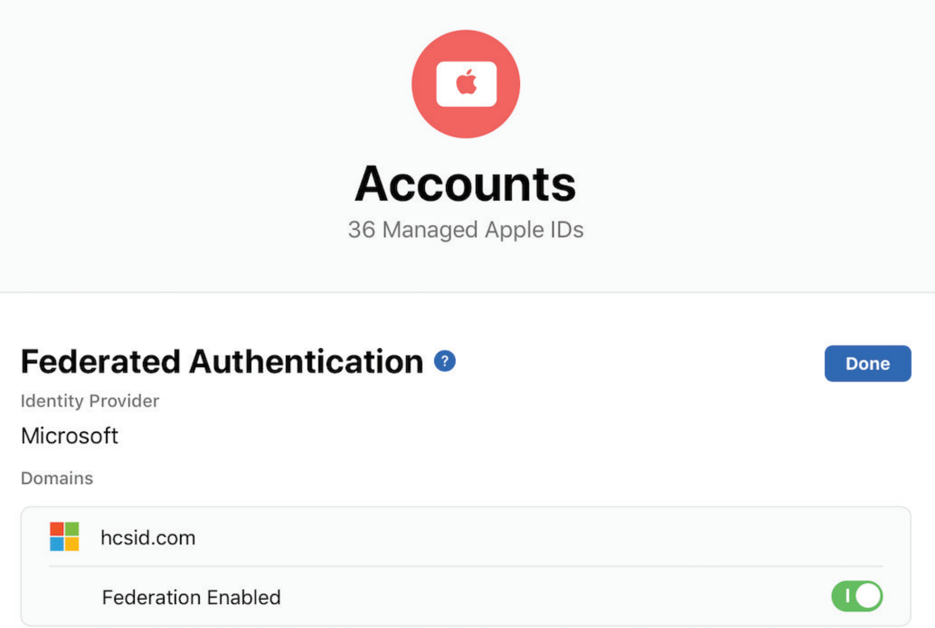
Microsoft

Domains

hcsid.com

Federation Not Enabled

15. The federation is now enabled. Let's test a connection to Apple Business Manager using a federated account. Log out of Apple Business Manager.



Accounts

36 Managed Apple IDs

Federated Authentication

Identity Provider

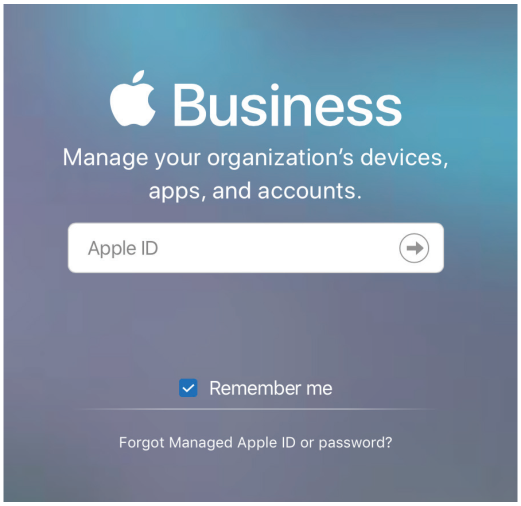
Microsoft

Domains

hcsid.com

Federation Enabled

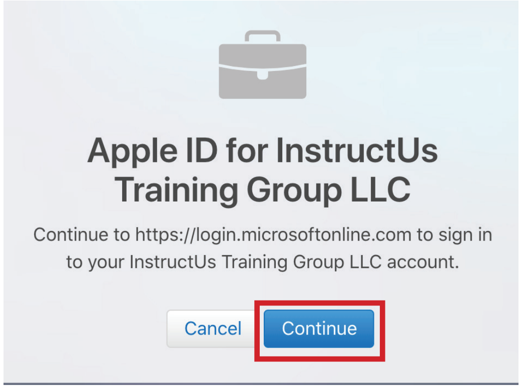
16. Log into Apple Business Manager with an account that is in your Azure Active Directory.
    E.G. kmitnick@hcsid.com



Business

Manage your organization’s devices, apps, and accounts.

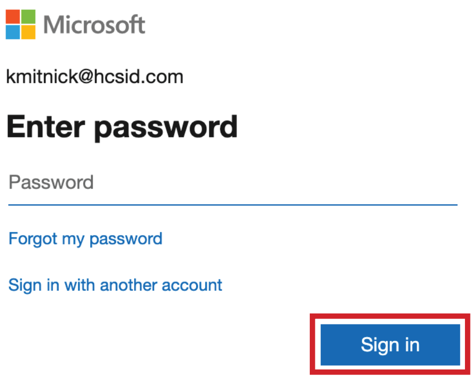
17. You will be redirected to login with Azure Active Directory. Select Continue.



Apple ID for InstructUs Training Group LLC

Continue to https://login.microsoftonline.com to sign in to your InstructUs Training Group LLC account.

18. Enter your credentials then select Sign in. This completes the guide.



Microsoft

kmitnick@hcsid.com

Enter password