Business

How to Setup a Federated Connection to Apple Business Manager

TECHNOLOGY GROUP

Rev20230414

Contents

What is Federated Authentication?

Federated authentication is a method of linking a user's identity across multiple separate identity management systems. For businesses embracing a work-from-anywhere policy, federated authentication offers a secure, flexible way to reduce IT overhead. With federated authentication, a single digital identity unlocks an employee's access to different services and authenticates them without additional passwords. Federated authentication further reduces the risk of Bring-Your-Own Device (BYOD) in the workplace. In addition, IT admins can set policies and controls over what, where, and when users can access data. They can grant or revoke employee access at a moment's notice when employees join the team or leave for another job.

Can I link Google Workspace or Microsoft Azure Active Directory to Apple Business Manager using Federated Authentication?

Yes, you can! In Apple Business Manager, you will need to use federated authentication to link Google Workspace or Microsoft Azure Active Directory (Azure AD) with Apple Business Manager. When Apple Business Manager and Google Workspace or Azure AD are linked, users who sign-in to Apple Business Manager using their Google Workspace or Azure AD user name and password have those same credentials become their Managed Apple ID automatically. If a user is removed from Google Workspace or Azure AD, that user can be removed from Apple Business Manager.

NOTE: You can link to only Google Workspace or Azure AD, but not at the same time.

What are the requirements?

You will need the following to connect a cloud identity to Apple Business Manager:

- You will need to verify the domain your are using. This will let Apple know you own the Domain and areable to make changes to DNS records.
- An account with Google Workspace or Microsoft Azure Active Directory configured.

The minimum requirements for devices:

- Google Workspace: iOS 15.5, iPadOS 15.5, MacOS 12.4
- Microsoft Azure Active Directory: iOS 11.3, iPadOS 13.1, MacOS 10.13.4

Links

Azure AD sync requirements with Apple Business Manager
https://support.apple.com/guide/apple-business-manager/azure-ad-sync-requirements-axmd88331cd6/web

Sync users from Azure AD into Apple Business Manager
https://support.apple.com/guide/apple-business-manager/sync-users-from-azure-ad-axm3ec7b95ad/1/web/1

What was used in this guide:

- Apple Business Manager
- Microsoft Azure Active Directory (Azure AD)

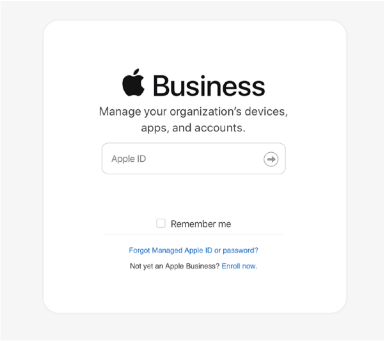
In this guide, we will show:

- How to verify your domain in Apple Business Manager
- Use federated authentication to link to Azure Active Directory (Azure AD)to Apple Business Manager
- Use Directory Sync to Import users

Section 1: Verify the Domain

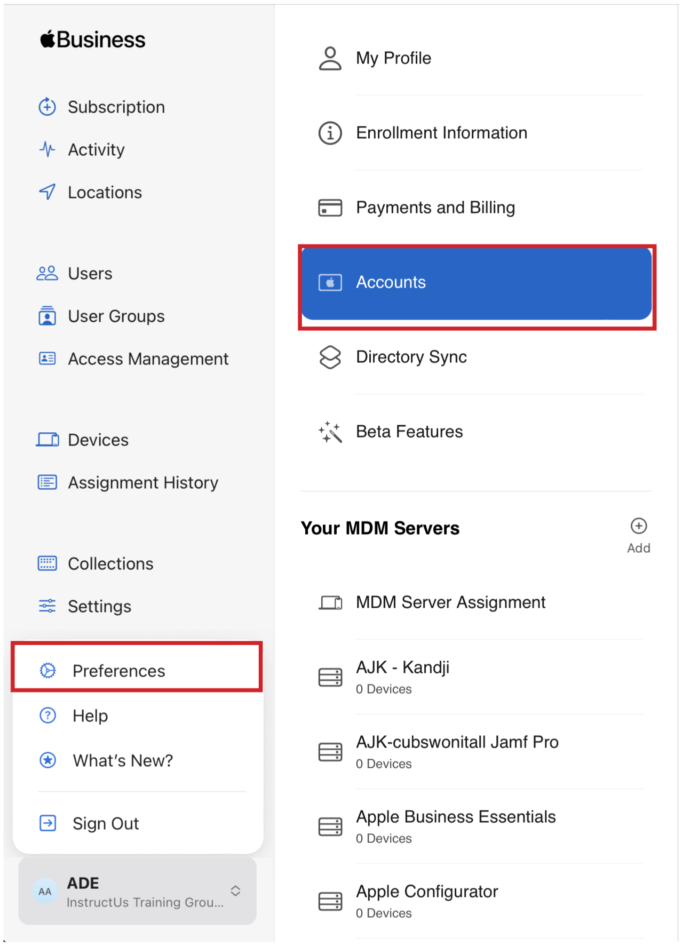
Before you begin, you must verify the domain you are about to federate. This ensures that your organization is the one that has authority to modify the domain name service (DNS) records for your domain.

1. Log in to Your Apple Business Manager, with Administrator credentials.

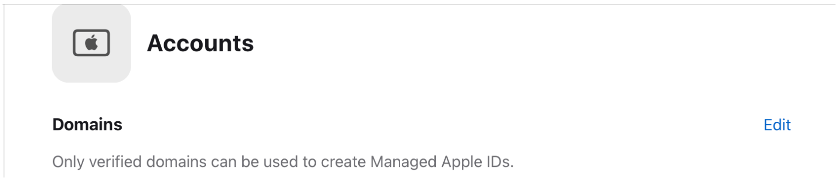

Business
Apple ID
Remember me
Forgot Managed Apple ID or password?
Not yet an Apple Business? Enroll now.

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

2. Click your name at the bottom of the sidebar, click Preferences.
3. Click Accounts.



4. Click Edit in the Domains section.



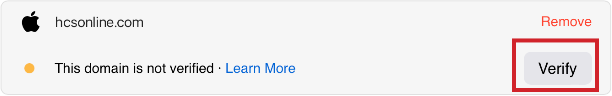
Accounts

Domains

Edit

Only verified domains can be used to create Managed Apple IDs.

5. Click Verify next to the domain.



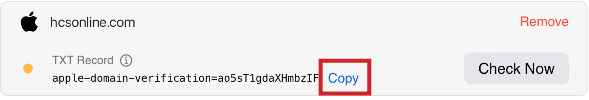
hcsonline.com

Remove

This domain is not verified · Learn More

Verify

6. In the TXT record field, click Copy.



hcsonline.com

Remove

TXT Record ⓘ

apple-domain-verification=ao5sT1gdaXHmbzIF Copy

Check Now

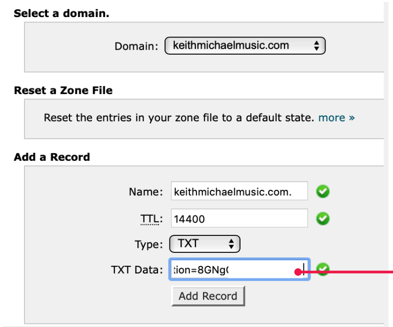
7. Open TextEdit, open a new blank document if necessary, and paste in the copied TXT record. You'll need this for a later step.
8. Create a DNS TXT record at your domain registrar. This procedure will vary depending on your domain registrar. If you are using one of the following services, see their documentation for creating a TXT record in a zone file, or contact your DNS administrator:
    - Google: Verify your domain with a TXT record
    - GoDaddy: Add a TXT record
    - Microsoft Azure: Add a TXT record for verification
    - Network Solutions: Managing Advanced DNS Records
    - NameCheap: How do I add TXT record for my domain?

    If you have a different domain registrar, contact them for information on how to add a TXT record to your DNS zone file.

    As an example, this guide uses Site Ground.
9. After you log in to Site Ground, go to the cPanel for DNS settings.
10. Select Advanced DNS Zone Editor.

10. Create a TXT record. Paste in the value that you copied in step 6.

11. Log out of your domain registrar.



Select a domain.

Domain: keithmichaelmusic.com

Reset a Zone File

Reset the entries in your zone file to a default state. more »

Add a Record

Name: keithmichaelmusic.com.

TTL: 14400

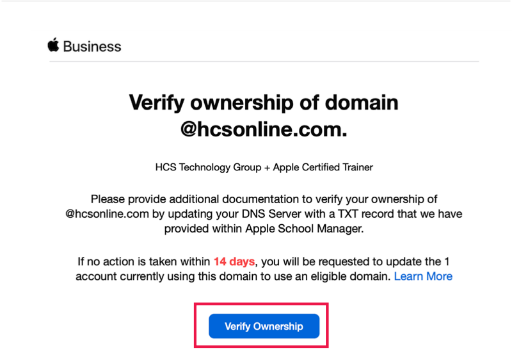
Type: TXT

TXT Data: :ion=8GNg(

Add Record

Paste in the value that you copied in step 5

12. Check the email account that is tied to the Apple Business Manager account that you signed in with. In the verification email message, click Verify Ownership.



Verify ownership of domain @hcsonline.com.

HCS Technology Group + Apple Certified Trainer

Please provide additional documentation to verify your ownership of @hcsonline.com by updating your DNS Server with a TXT record that we have provided within Apple School Manager.

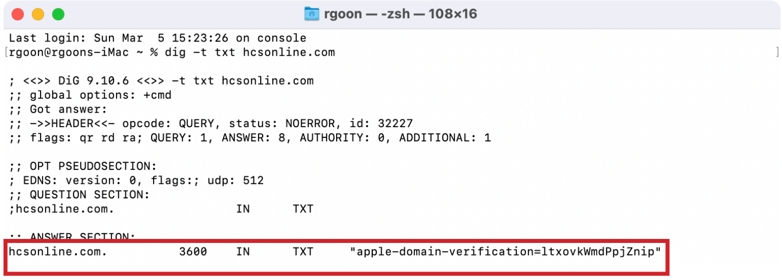
If no action is taken within 14 days, you will be requested to update the 1 account currently using this domain to use an eligible domain. Learn More

13. To test your DNS TXT record, Open Terminal then enter the following command:

```
dig -t txt yourdomaingoeshere.com
```

The results will return the TXT record you created at your domain registrar.

NOTE: It can take up to 24 hours for the new DNS record to propagate across the internet.

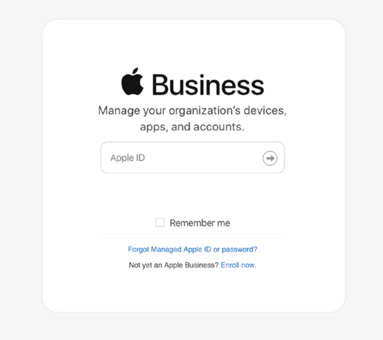


```
Last login: Sun Mar  5 15:23:26 on console
rgoon@rgoons-iMac ~ % dig -t txt hcsonline.com

; <<>> DiG 9.10.6 <<>> -t txt hcsonline.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32227
;; flags: qr rd ra; QUERY: 1, ANSWER: 8, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;hcsonline.com.                 IN      TXT

;; ANSWER SECTION:
hcsonline.com.          3600    IN      TXT     "apple-domain-verification=ltxovkWmdPpjZnip"
```

Section 1: Integrate Microsoft Azure Active Directory into Apple Business Manager

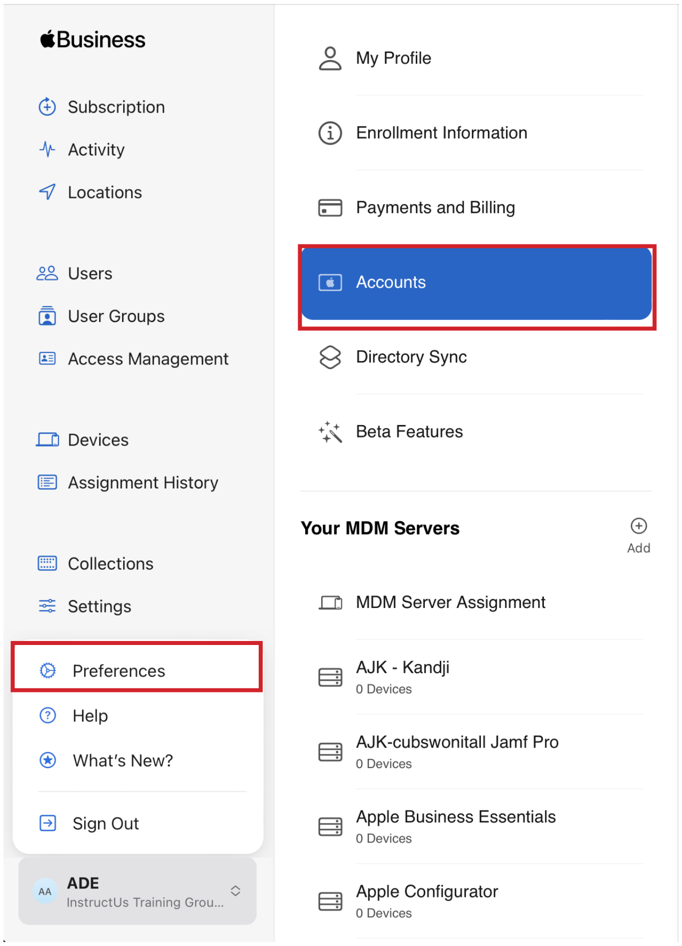
After the Domain has been verified, you may proceed to start integrating Microsoft Azure Directory into Apple Business Manager. You will need administration credentials for your Microsoft account.

1. Log in to Your Apple Business Manager, with Administrator credentials.

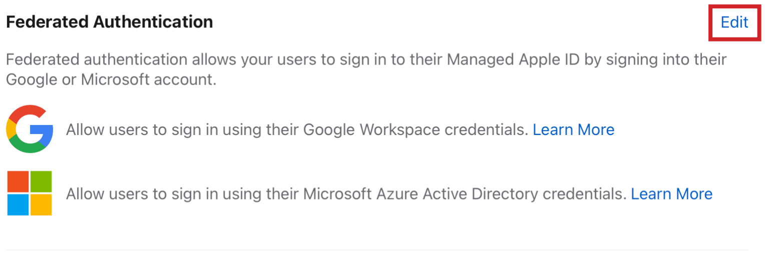


Business
Manage your organization's devices, apps, and accounts.
Apple ID
Remember me
Forgot Managed Apple ID or password?
Not yet an Apple Business? Enroll now.

2. Click your name at the bottom of the sidebar, click Preferences,
3. Click Accounts .



4. Click Edit in the Federated Authentication section.



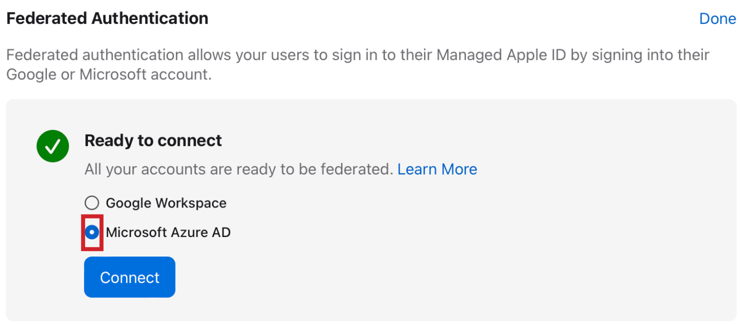
Federated Authentication Edit

Federated authentication allows your users to sign in to their Managed Apple ID by signing into their Google or Microsoft account.

Allow users to sign in using their Google Workspace credentials. Learn More

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

5. Select Microsoft Azure AD.
6. Click Connect.



Federated Authentication Done

Federated authentication allows your users to sign in to their Managed Apple ID by signing into their Google or Microsoft account.

Ready to connect

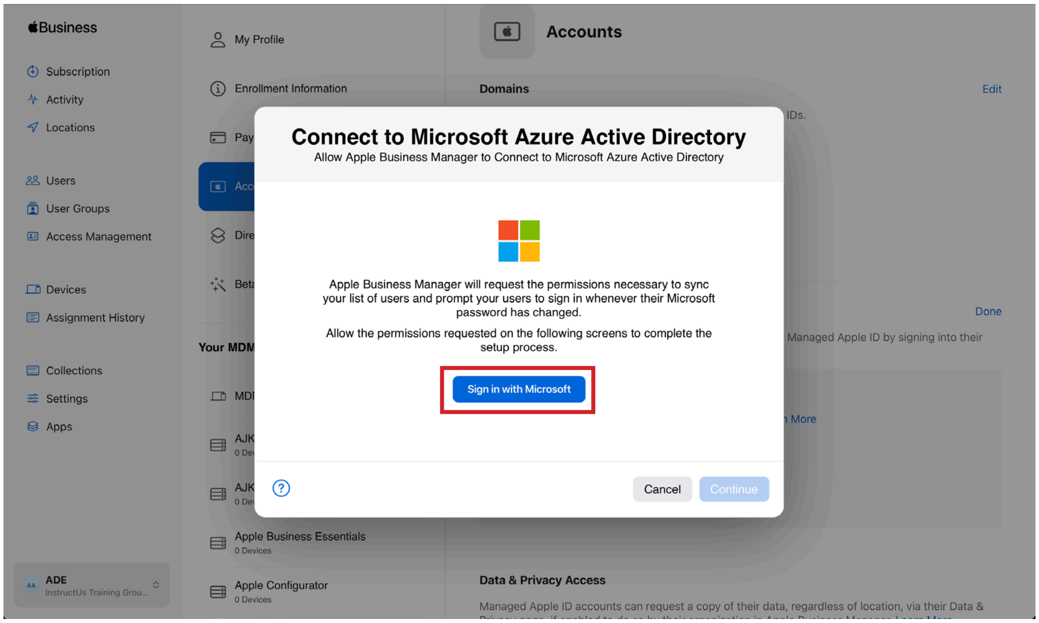
All your accounts are ready to be federated. Learn More

○ Google Workspace

● Microsoft Azure AD

Connect

7. Click Sign in with Microsoft



Connect to Microsoft Azure Active Directory

Allow Apple Business Manager to Connect to Microsoft Azure Active Directory

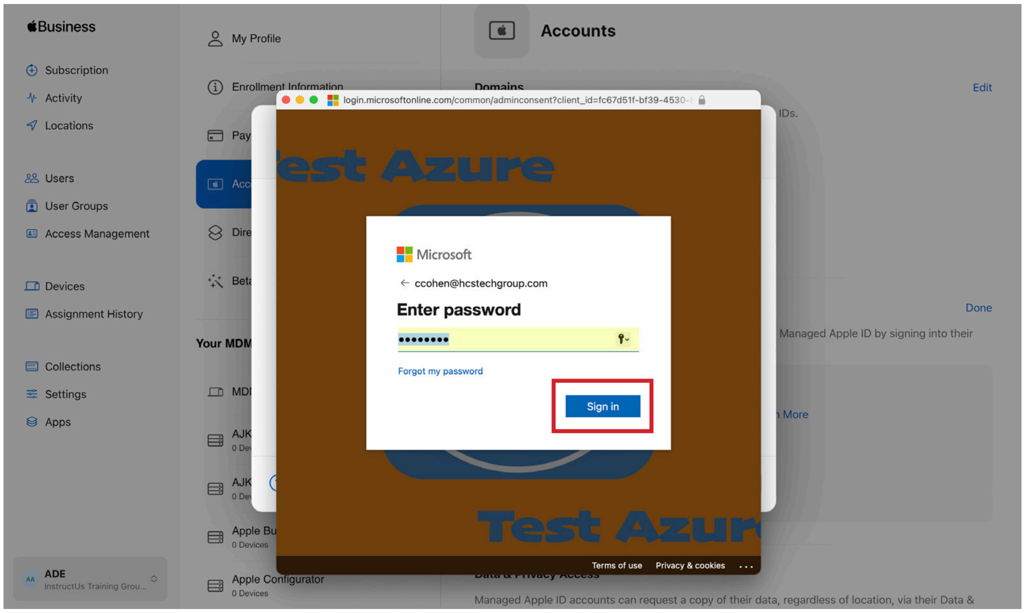
Apple Business Manager will request the permissions necessary to sync your list of users and prompt your users to sign in whenever their Microsoft password has changed.

Allow the permissions requested on the following screens to complete the setup process.

Sign in with Microsoft

Cancel Continue

8. Enter the administrator credentials for your Microsoft account. Click Sign in.



login.microsoftonline.com/common/adminconsent?client_id=fc67d51f-bf39-4530-

Microsoft

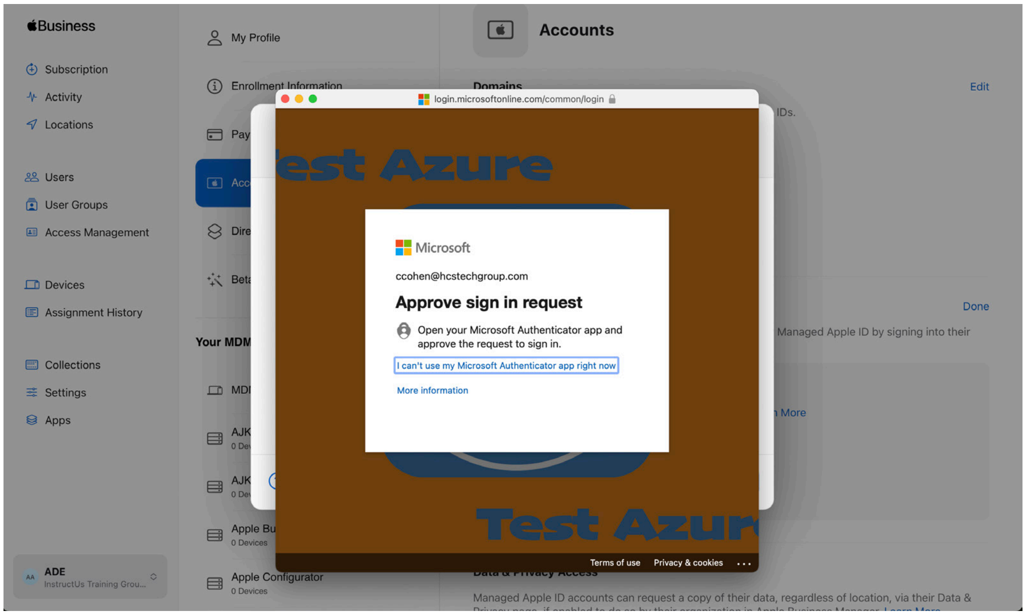
ccohen@hcstechgroup.com

Enter password

Managed Apple ID by signing into their

Managed Apple ID accounts can request a copy of their data, regardless of location, via their Data &

9. If multi-factor authentication is turned on, use the multi-factor app to allow access.



login.microsoftonline.com/common/login

Microsoft

ccohen@hcstechgroup.com

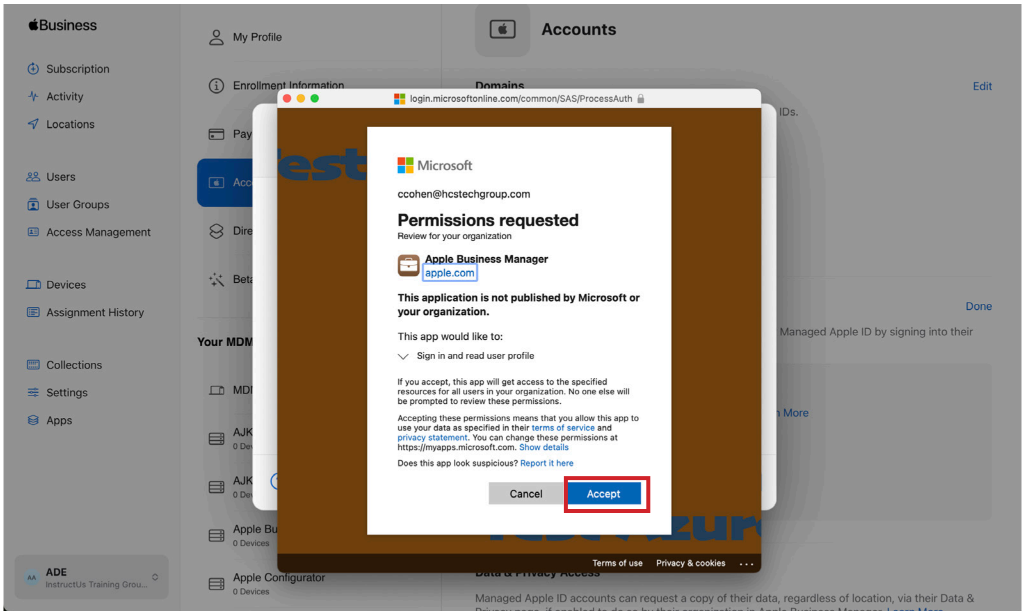
Approve sign in request

Open your Microsoft Authenticator app and approve the request to sign in.

Managed Apple ID by signing into their

Managed Apple ID accounts can request a copy of their data, regardless of location, via their Data &

10. Click Accept.



Microsoft

ccohen@hcstechgroup.com

Permissions requested

Review for your organization

Apple Business Manager
apple.com

This application is not published by Microsoft or your organization.

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.

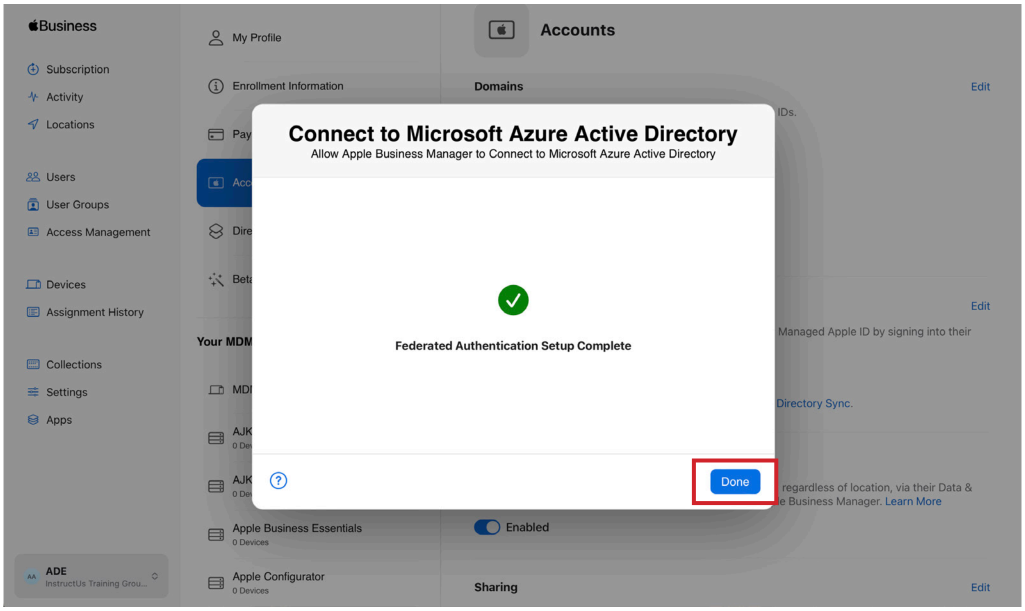
Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

Cancel | Accept

Managed Apple ID accounts can request a copy of their data, regardless of location, via their Data &

11. Click Done.



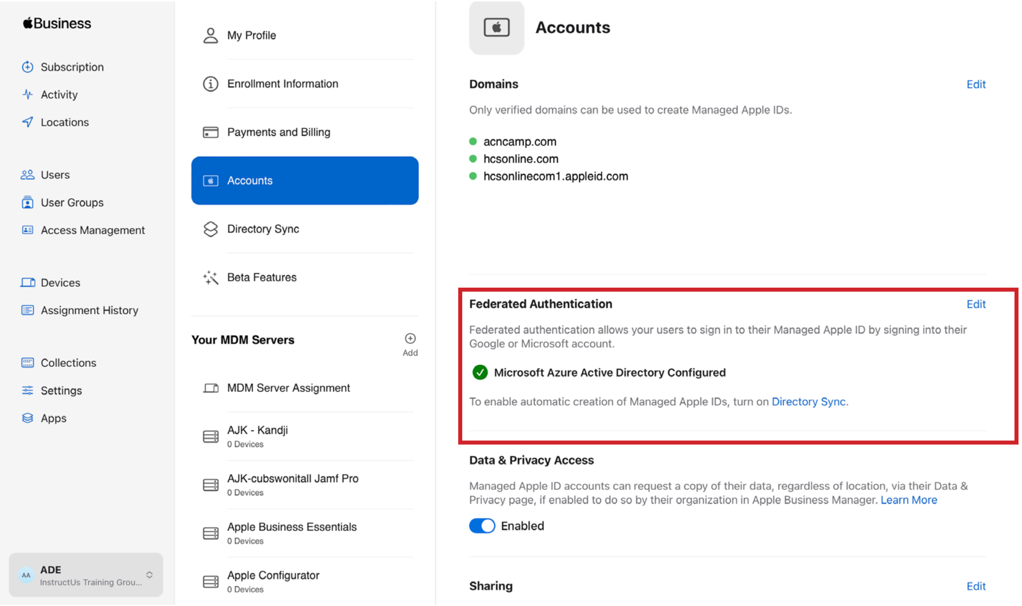
Connect to Microsoft Azure Active Directory

Allow Apple Business Manager to Connect to Microsoft Azure Active Directory

Federated Authentication Setup Complete

Done

12. Confirm Microsoft Azure Active Directory has been configured.



Accounts

Domains Edit

Only verified domains can be used to create Managed Apple IDs.

- acncamp.com
- hcsonline.com
- hcsonlinecom1.appleid.com

Federated Authentication Edit

Federated authentication allows your users to sign in to their Managed Apple ID by signing into their Google or Microsoft account.

✓ **Microsoft Azure Active Directory Configured**

To enable automatic creation of Managed Apple IDs, turn on Directory Sync.

Data & Privacy Access

Managed Apple ID accounts can request a copy of their data, regardless of location, via their Data & Privacy page, if enabled to do so by their organization in Apple Business Manager. Learn More

Enabled

Sharing Edit

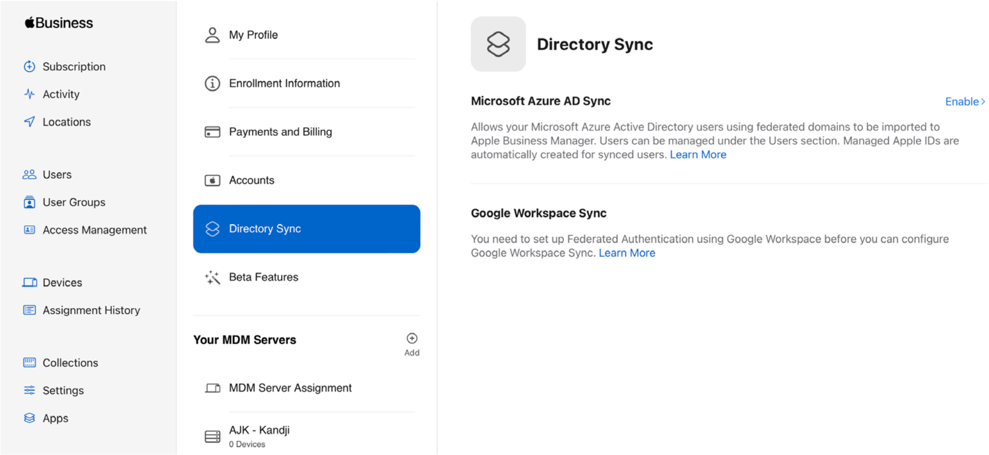
Section 3: Directory Sync

You can use the System for Cross-domain Identity Management (SCIM) to import users into Apple Business Manager. Using this system, you merge Apple Business Manager properties (such as roles) with user account data imported from Microsoft Azure Active Directory (Azure AD). When a user is copied from Azure AD using SCIM to Apple Business Manager, the default role is Staff. After the sync is complete, only the Roles user attribute can be edited.

NOTE: You have only 4 calendar days to complete the token transfer to Azure AD and successfully establish a connection, or you must begin the process again.

Please review the article on Azure AD sync requirements with Apple Business Manager:
https://support.apple.com/guide/apple-business-manager/azure-ad-sync-requirements-axmd88331cd6/web

1. Click Directory Sync.
2. Click Enable.



Directory Sync

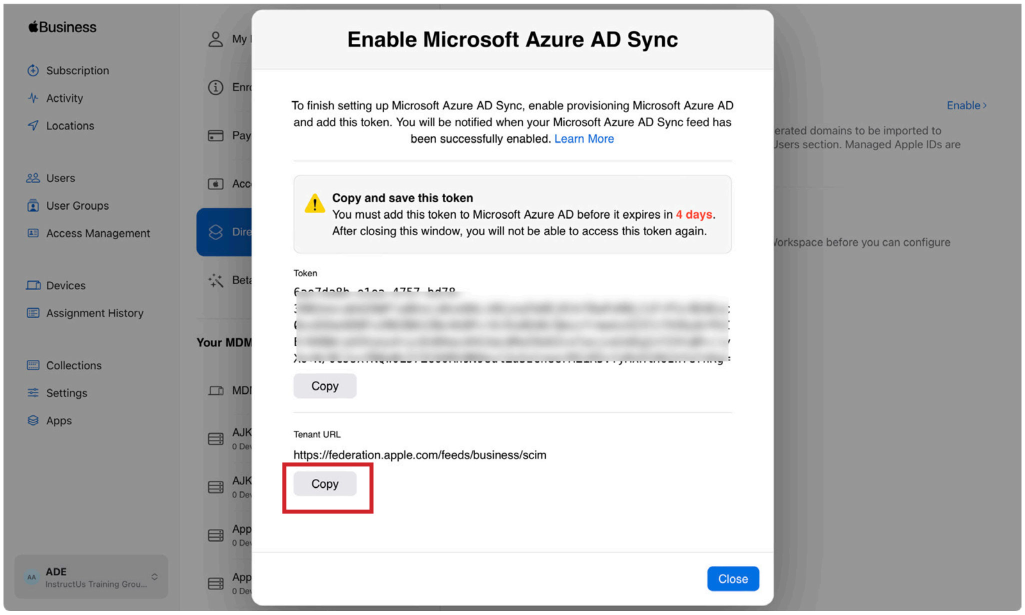
Microsoft Azure AD Sync Enable >

Allows your Microsoft Azure Active Directory users using federated domains to be imported to Apple Business Manager. Users can be managed under the Users section. Managed Apple IDs are automatically created for synced users. Learn More

Google Workspace Sync

You need to set up Federated Authentication using Google Workspace before you can configure Google Workspace Sync. Learn More

3. Click Copy for Tenant URL: https://federation.apple.com/feeds/business/scim
   NOTE: Keep this window open.



Enable Microsoft Azure AD Sync

To finish setting up Microsoft Azure AD Sync, enable provisioning Microsoft Azure AD and add this token. You will be notified when your Microsoft Azure AD Sync feed has been successfully enabled. Learn More

Copy and save this token
You must add this token to Microsoft Azure AD before it expires in 4 days.
After closing this window, you will not be able to access this token again.

Token
[redacted]

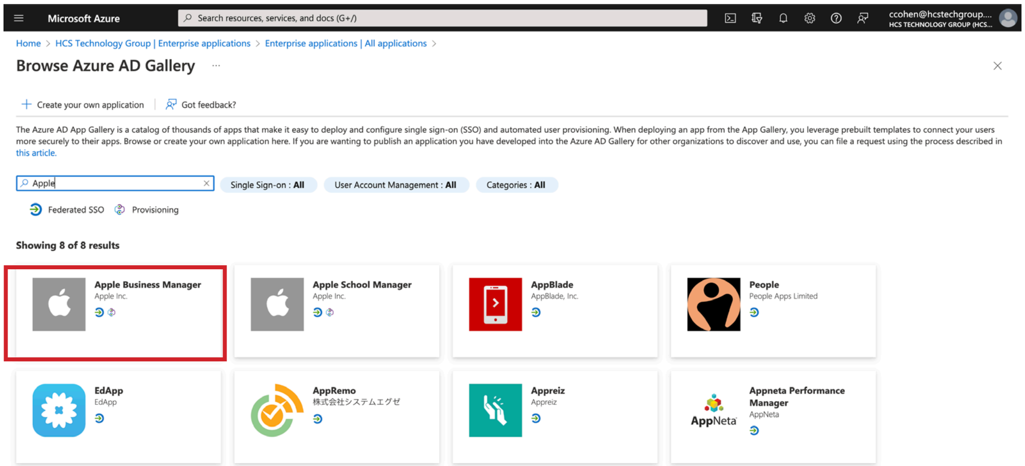
Copy

Tenant URL
https://federation.apple.com/feeds/business/scim

Copy

Close

4. In a new browser window, log in to your Azure web portal: (https://portal.azure.com).
5. Click Enterprise applications.
6. Search for Apple Business Manager.
7. After the search is complete, click Apple Business Manager.


Microsoft Azure
Search resources, services, and docs (G+/)
ccohen@hcstechgroup....
HCS TECHNOLOGY GROUP (HCS...

Home > HCS Technology Group | Enterprise applications > Enterprise applications | All applications >

Browse Azure AD Gallery

+ Create your own application
Got feedback?

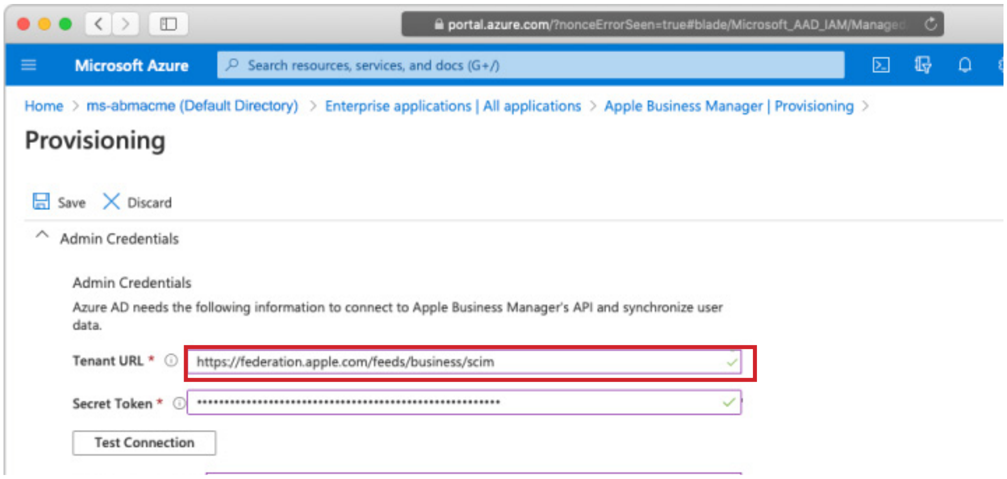
The Azure AD App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO) and automated user provisioning. When deploying an app from the App Gallery, you leverage prebuilt templates to connect your users more securely to their apps. Browse or create your own application here. If you are wanting to publish an application you have developed into the Azure AD Gallery for other organizations to discover and use, you can file a request using the process described in this article.

Apple

Single Sign-on : **All** User Account Management : **All** Categories : **All**

Showing 8 of 8 results

8. In the Apple Business Manager Azure AD app, delete any content in the Tenant URL field, then paste in the tenant URL from Apple Business Manager.


portal.azure.com/?nonceErrorSeen=true#blade/Microsoft_AAD_IAM/Managed
Microsoft Azure
Search resources, services, and docs (G+/)

Home > ms-abmacme (Default Directory) > Enterprise applications | All applications > Apple Business Manager | Provisioning >

Provisioning

Admin Credentials

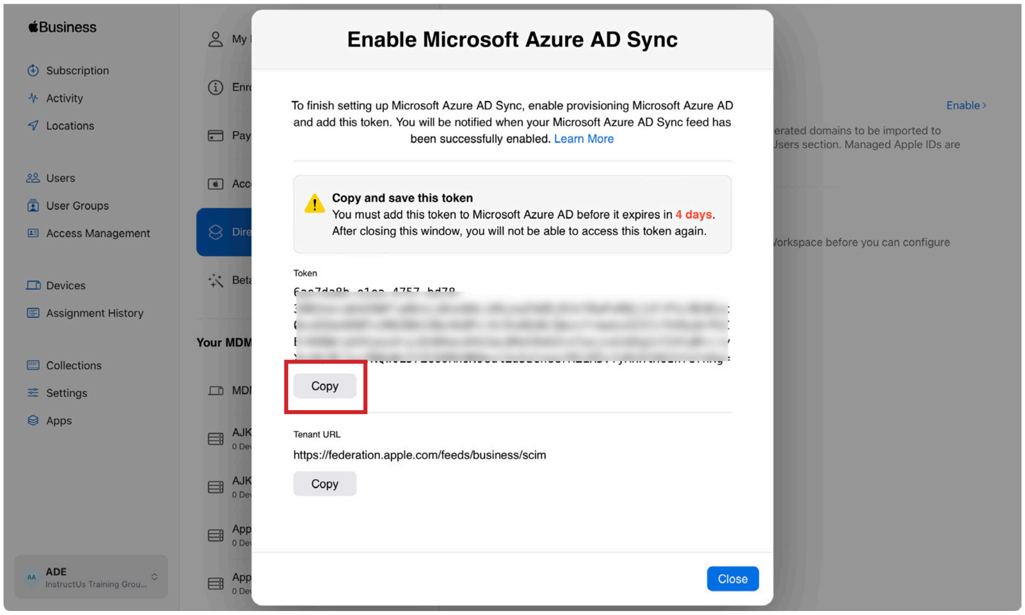
Admin Credentials

Azure AD needs the following information to connect to Apple Business Manager's API and synchronize user data.

Tenant URL * https://federation.apple.com/feeds/business/scim

Secret Token * ••

9. Click Copy for Token.



Enable Microsoft Azure AD Sync

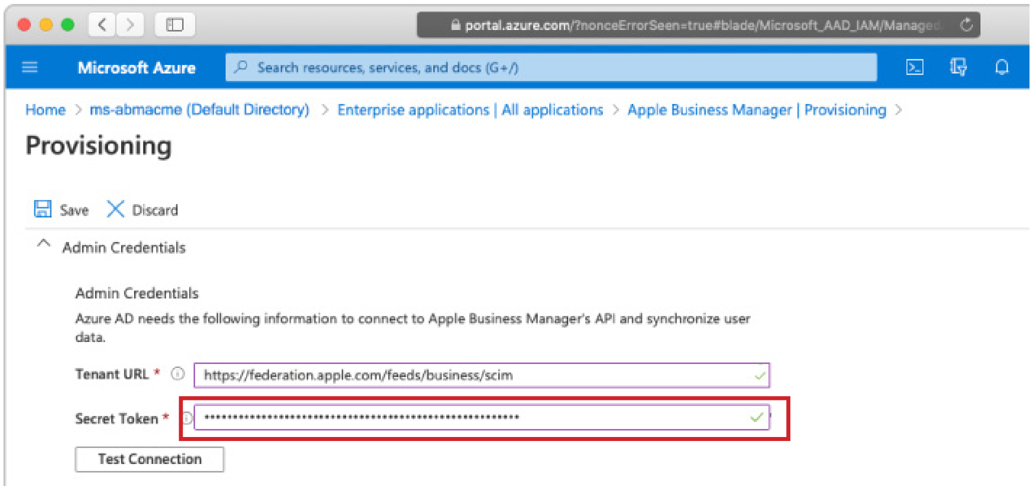
To finish setting up Microsoft Azure AD Sync, enable provisioning Microsoft Azure AD and add this token. You will be notified when your Microsoft Azure AD Sync feed has been successfully enabled. Learn More

Copy and save this token
You must add this token to Microsoft Azure AD before it expires in 4 days. After closing this window, you will not be able to access this token again.

Token
[redacted]

Tenant URL
https://federation.apple.com/feeds/business/scim

10. In the Apple Business Manager Azure AD app, paste the copied token from Apple Business Manager into the Secret Token field.


portal.azure.com/?nonceErrorSeen=true#blade/Microsoft_AAD_IAM/Managed
Microsoft Azure
Search resources, services, and docs (G+/)
Save
Discard
Test Connection

Home > ms-abmacme (Default Directory) > Enterprise applications | All applications > Apple Business Manager | Provisioning >

Provisioning

Admin Credentials

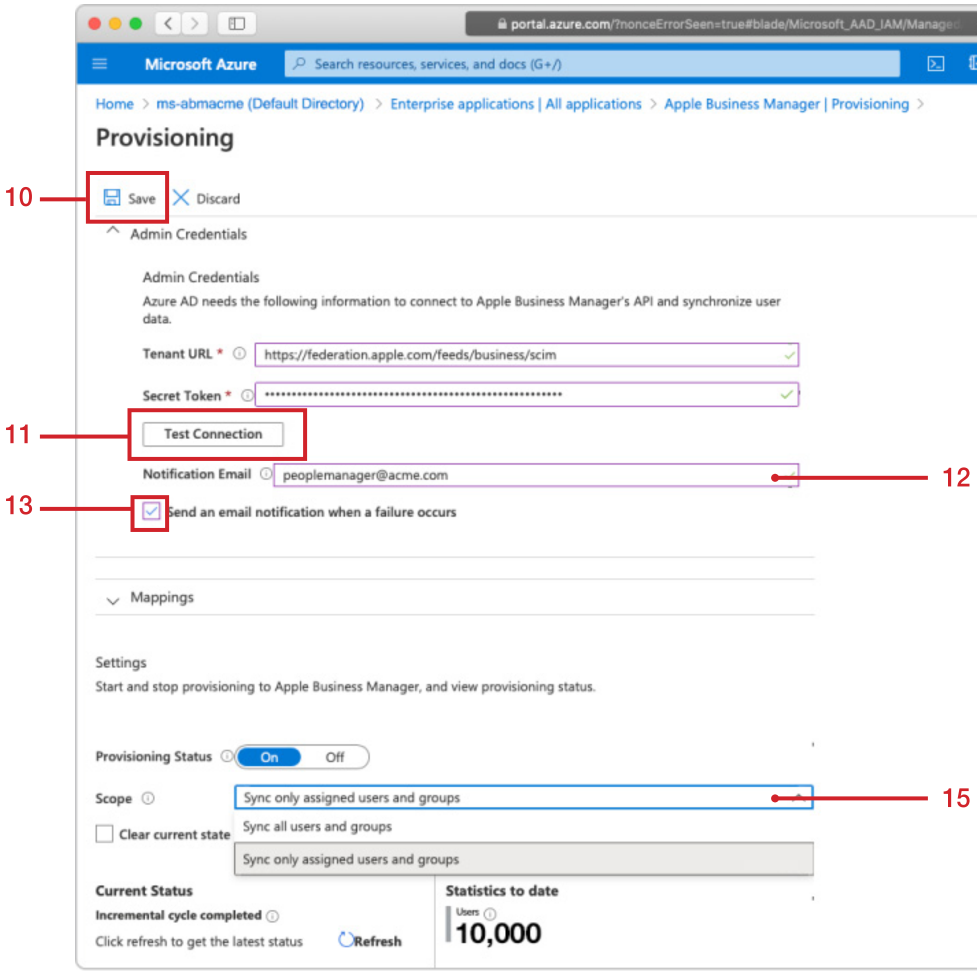
Admin Credentials
Azure AD needs the following information to connect to Apple Business Manager's API and synchronize user data.

Tenant URL * https://federation.apple.com/feeds/business/scim

Secret Token * ••

10. Click Save
11. Click Test Connection. If the connection is successful, Apple Business Manager shows the SCIM connection as active. It can take up to 60 seconds to reflect the latest connection status.
12. In the Settings section, enter the email address of an Apple Business Manager Administrator or People Manager,
13. Select the "Send an email notification when a failure occurs" checkbox so they receive any provisioning error notifications.
14. Add additional mappings if required. By default: First Name, Last Name, UPN, Object ID, Department and Employee ID is created. Only use attributes listed by Apple otherwise it may break the SCIM connection. Also do not add user attributes during provisioning.
    NOTE: Please see Addendum on how the attributes are mapped and what is required.
15. Select the scope of users you want to sync:

Sync only assigned users and groups	This option syncs only the accounts that appear in the Apple Business Manager Azure AD app to Apple Business Manager. When using this method to sync, Azure AD accounts must have the role of user to sync to Apple Business Manager.
Sync all users and groups	This option syncs all accounts (syncing groups isn't supported) that appear in the Azure AD User tab to Apple Business Manager and creates Managed Apple IDs for all federated Azure AD accounts, even if you intend to use only a specific number of accounts.


portal.azure.com/?nonceErrorSeen=true#blade/Microsoft_AAD_IAM/Managed
Microsoft Azure
Search resources, services, and docs (G+/)
Home > ms-abmacme (Default Directory) > Enterprise applications | All applications > Apple Business Manager | Provisioning >
10
Save
Discard
11
Test Connection
12
13
Mappings
15
On
Off
Refresh

Provisioning

Admin Credentials

Admin Credentials

Azure AD needs the following information to connect to Apple Business Manager's API and synchronize user data.

Tenant URL * https://federation.apple.com/feeds/business/scim

Secret Token * ••

Notification Email peoplemanager@acme.com

☑ Send an email notification when a failure occurs

Settings

Start and stop provisioning to Apple Business Manager, and view provisioning status.

Provisioning Status: On

Scope: Sync only assigned users and groups

- Sync all users and groups
- Sync only assigned users and groups

□ Clear current state

Current Status

Incremental cycle completed

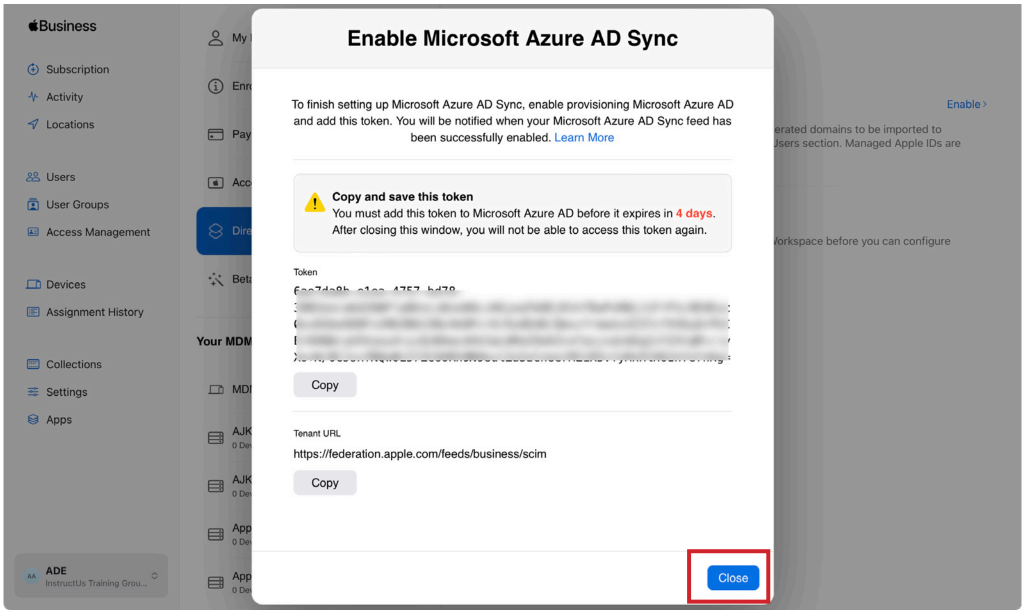
Click refresh to get the latest status

Statistics to date

Users

10,000

16. Go back to Apple Business Manager. Click Close.



Enable Microsoft Azure AD Sync

To finish setting up Microsoft Azure AD Sync, enable provisioning Microsoft Azure AD and add this token. You will be notified when your Microsoft Azure AD Sync feed has been successfully enabled. Learn More

Copy and save this token
You must add this token to Microsoft Azure AD before it expires in 4 days. After closing this window, you will not be able to access this token again.

Token
[redacted]

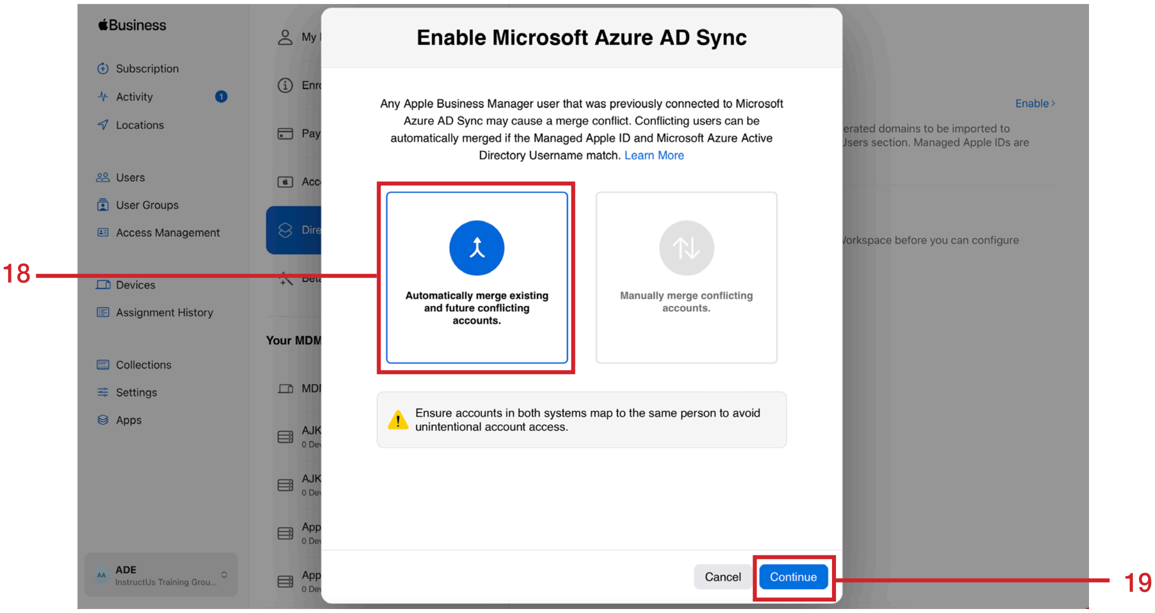
Copy

Tenant URL
https://federation.apple.com/feeds/business/scim

Copy

Close

17. Turn on federated authentication, if it isn't turned on already.
18. If automatic merge is turned on, new accounts are merged with existing accounts in Apple Business Manager. When you have automatic merge turned off, all user account conflicts will need to be resolved manually. This guide will use automatic merge.
For more info, please see:
https://support.apple.com/guide/apple-business-manager/resolve-scim-user-account-conflicts-axm313013d12/1/web/1
19. Click Continue.



Enable Microsoft Azure AD Sync

Any Apple Business Manager user that was previously connected to Microsoft Azure AD Sync may cause a merge conflict. Conflicting users can be automatically merged if the Managed Apple ID and Microsoft Azure Active Directory Username match. Learn More

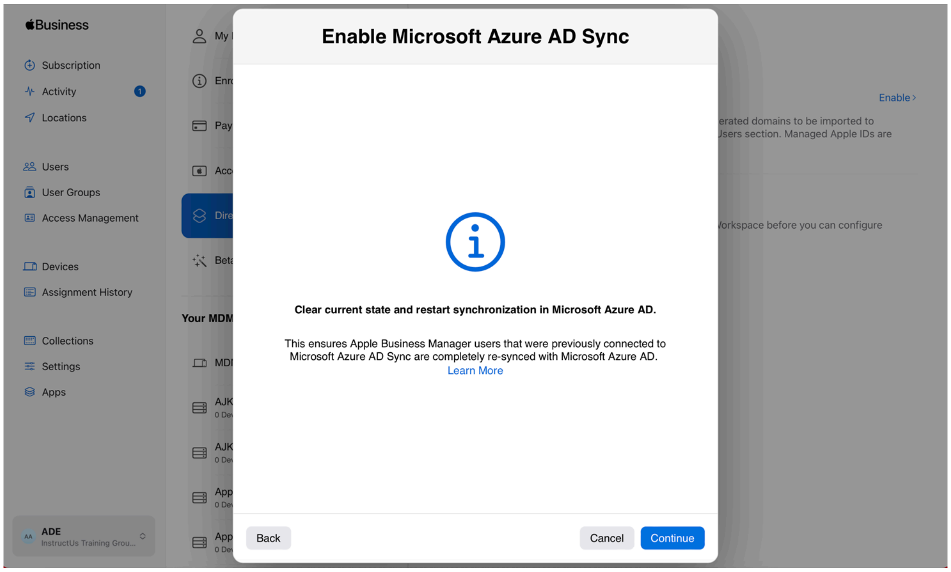
Automatically merge existing and future conflicting accounts.

Manually merge conflicting accounts.

Ensure accounts in both systems map to the same person to avoid unintentional account access.

Cancel Continue

20. Click Continue.

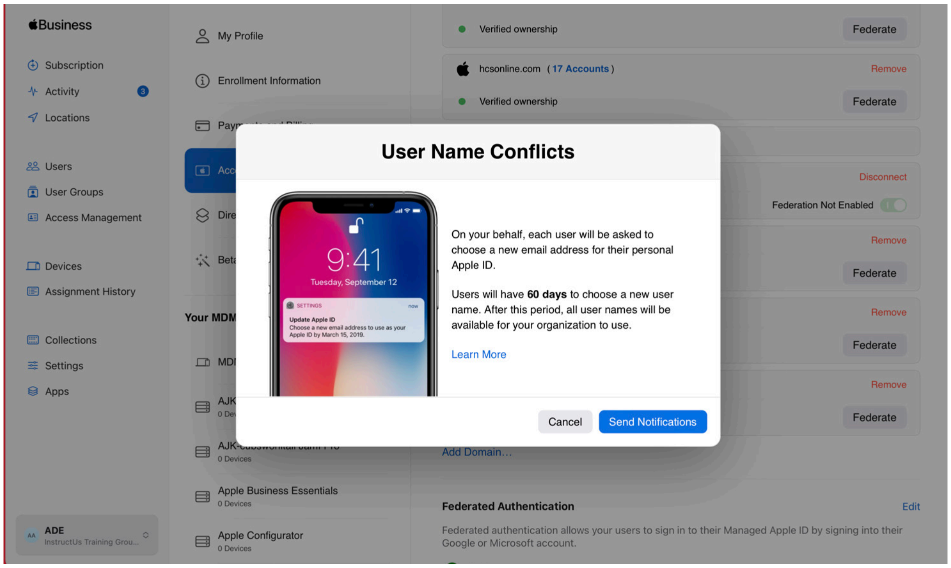


Enable Microsoft Azure AD Sync

Clear current state and restart synchronization in Microsoft Azure AD.

This ensures Apple Business Manager users that were previously connected to Microsoft Azure AD Sync are completely re-synced with Microsoft Azure AD.
Learn More

21. Confirm a message appears about User Name Conflicts. Click Send Notifications.



Federated authentication allows your users to sign in to their Managed Apple ID by signing into their Google or Microsoft account.

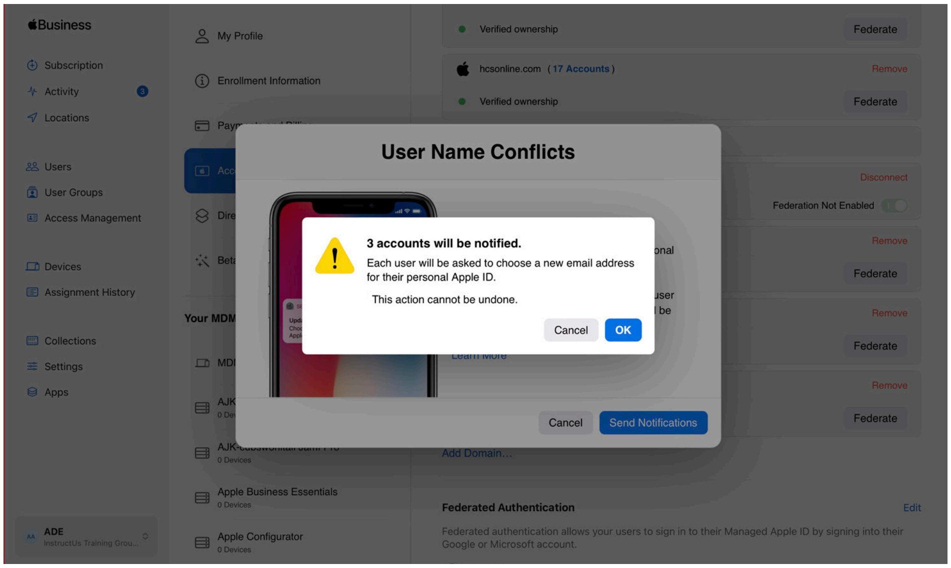
User Name Conflicts

On your behalf, each user will be asked to choose a new email address for their personal Apple ID.

Users will have **60 days** to choose a new user name. After this period, all user names will be available for your organization to use.

Learn More

22. If there are any conflicts, you will receive a message on the number of conflicts. Click OK.



User Name Conflicts

3 accounts will be notified.

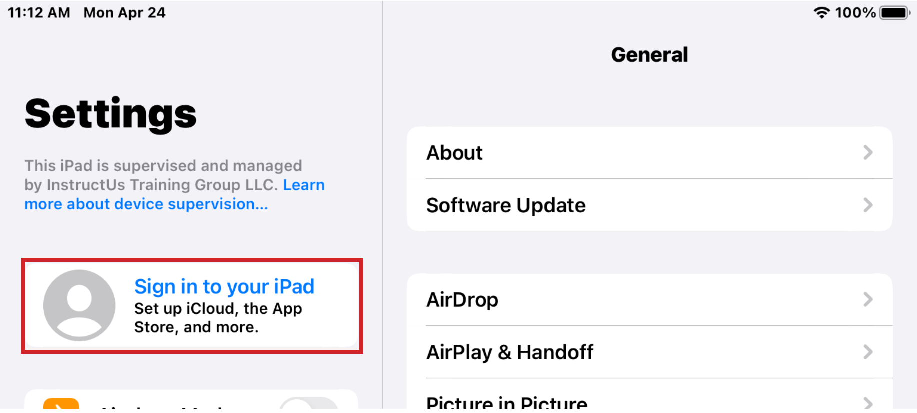
Each user will be asked to choose a new email address for their personal Apple ID.

This action cannot be undone.

Section 4: Test a federated account

1. On a device, go to Settings.

2. Tap Sign in to your iPad.



11:12 AM Mon Apr 24

100%

Settings

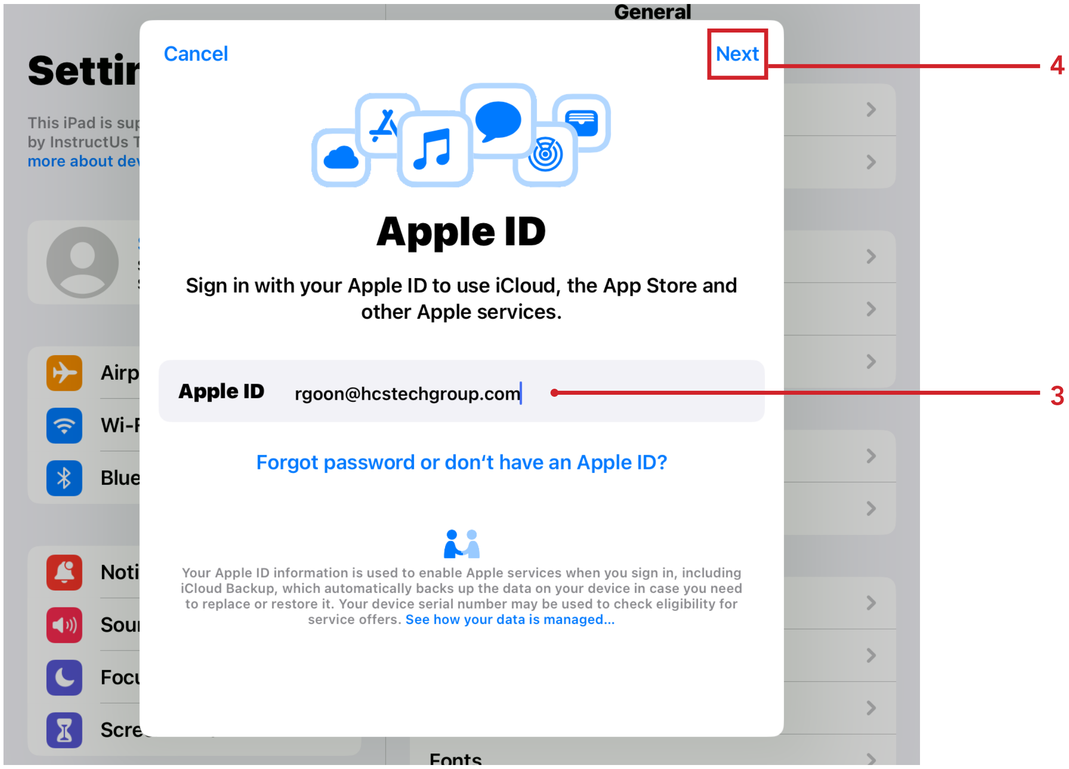
This iPad is supervised and managed by InstructUs Training Group LLC. Learn more about device supervision...

Sign in to your iPad
Set up iCloud, the App Store, and more.

General

- About
- Software Update
- AirDrop
- AirPlay & Handoff
- Picture in Picture

3. Enter the federated account name.
4. Tap Next.



Apple ID

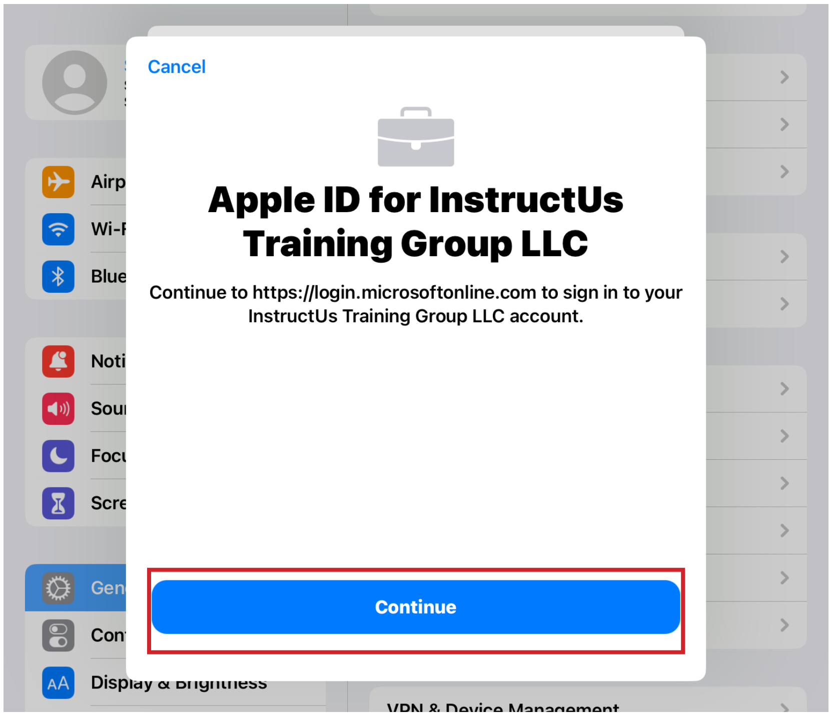
Sign in with your Apple ID to use iCloud, the App Store and other Apple services.

Apple ID rgoon@hcstechgroup.com

Forgot password or don't have an Apple ID?

Your Apple ID information is used to enable Apple services when you sign in, including iCloud Backup, which automatically backs up the data on your device in case you need to replace or restore it. Your device serial number may be used to check eligibility for service offers. See how your data is managed...

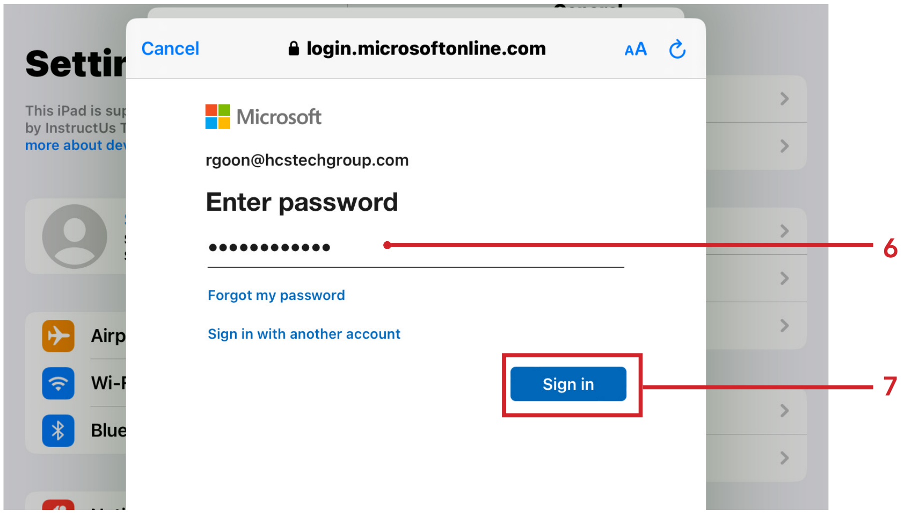
5. Tap Continue.



Apple ID for InstructUs Training Group LLC

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

6. Enter the password for the federated account.
7. Tap Sign in.

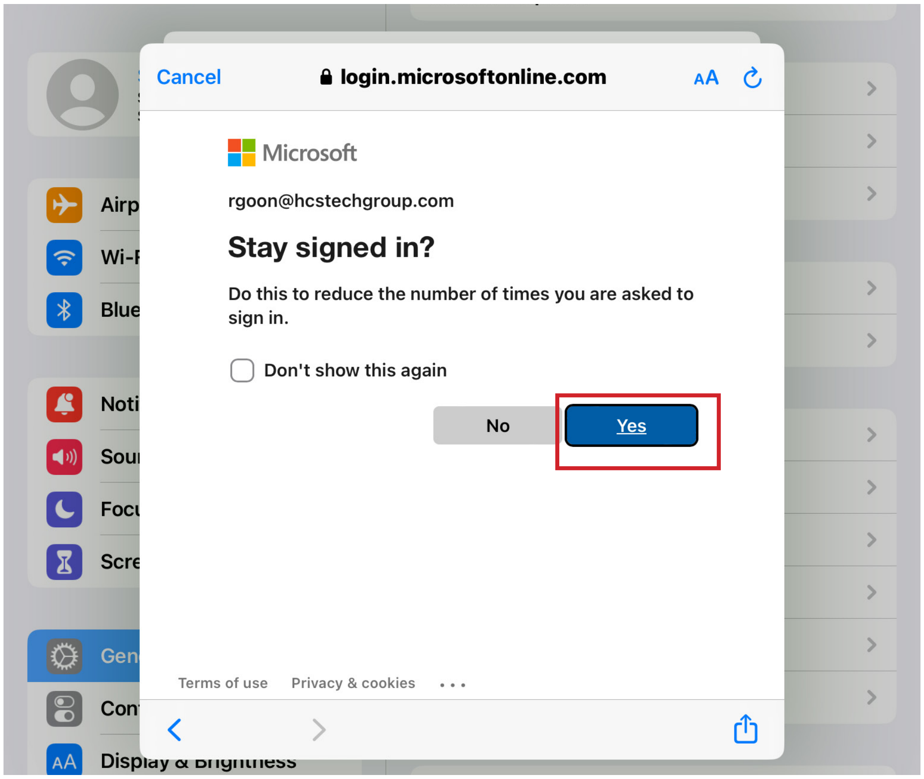


rgoon@hcstechgroup.com

Enter password

••••••••••••

8. Tap Yes.



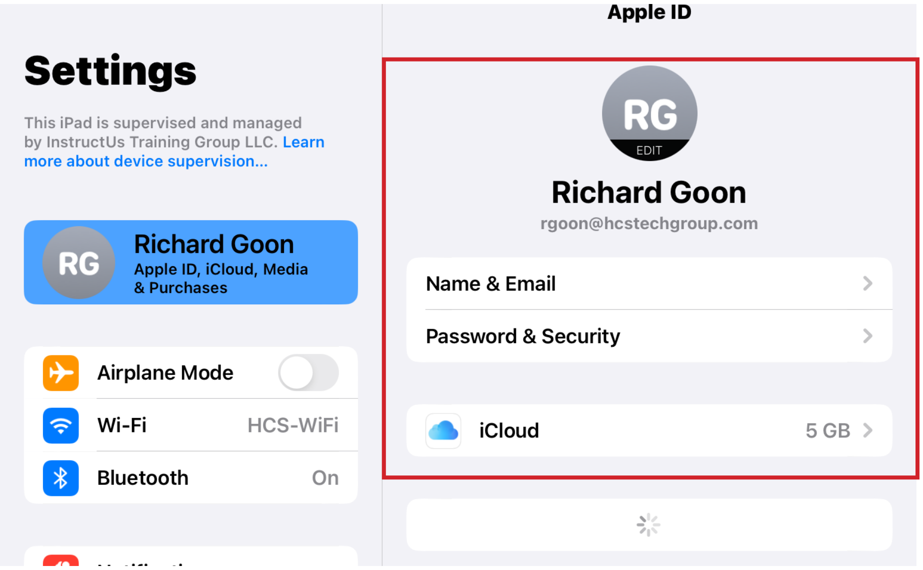
rgoon@hcstechgroup.com

Stay signed in?

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

☐ Don't show this again

3. Confirm you are signed in with your federated - managed Apple ID.



This iPad is supervised and managed by InstructUs Training Group LLC. Learn more about device supervision...

Richard Goon

rgoon@hcstechgroup.com

Addendum: SCIM user attribute mapping

When an account is copied from Azure AD using SCIM to Apple Business Essentials, the following user attributes are stored as read-only.

NOTE: Adding attributes not listed in the table breaks the SCIM connection.

Azure AD	Apple Business Essentials	Required
First Name	First Name	✓
Last Name	Last Name	✓
User Principal Name	Managed Apple ID and email address	✓
Object ID	(Not shown in Apple Business Essentials. This attribute is used to identify conflicting accounts.)	✓
Department	Department	✗
Employee ID	Person Number	✗
Custom attribute (must be created in the Apple Business Manager Azure AD app)	Cost Center	✗
Custom attribute (must be created in the Apple Business Manager Azure AD app)	Division	✗