



How to Auto Configure
Microsoft 365 Mail Account with Jamf Pro



Contents

Section 1: Confirming Your Jamf Pro Server Settings..... 4

Section 2: Creating Configuration Profiles 11

Section 3: Deploying a Device with Automated Mail Settings 16



The purpose of this guide is to automatically configure a Mac Computer and iOS device with Office 365 mail settings. This will allow a user to provide only their password when configuring their mail application and will also provide managed and secure email.

To follow along with this guide you will need the following:

- Jamf Pro Server with administrative access. This guide will use Jamf Pro cloud hosted version 10.38.1
- Jamf Pro Server integrated with Microsoft Azure as the Cloud Identity Provider.
- A Mac Computer enrolled and assigned to a user. This guide will use macOS Monterey 12.4.
- An iOS device enrolled and assigned to a user. This guide will use iPadOS version 15.5
- Microsoft Authenticator App - This is optional for Multi-factor Authentication.
- This guide will use a PreStage Enrollment that requires an Enrollment Customization that uses Single Sign-On during enrollment.
- This guide will use the Apple Mail app.



Section 1: Confirming Your Jamf Pro Server Settings

In this section, we will confirm the Jamf Pro server is configured with the following items:

- Microsoft Azure for Single Sign-On
- Microsoft Azure as a Cloud Identity Provider
- An Enrollment Customization configured for Single Sign-On
- A PreStage Enrollment that will use an Enrollment Customization for Single Sign-On
- Confirm Inventory Collection for LDAP is set for Computers and iOS Devices

NOTE: This guide does NOT cover configuring the items above.

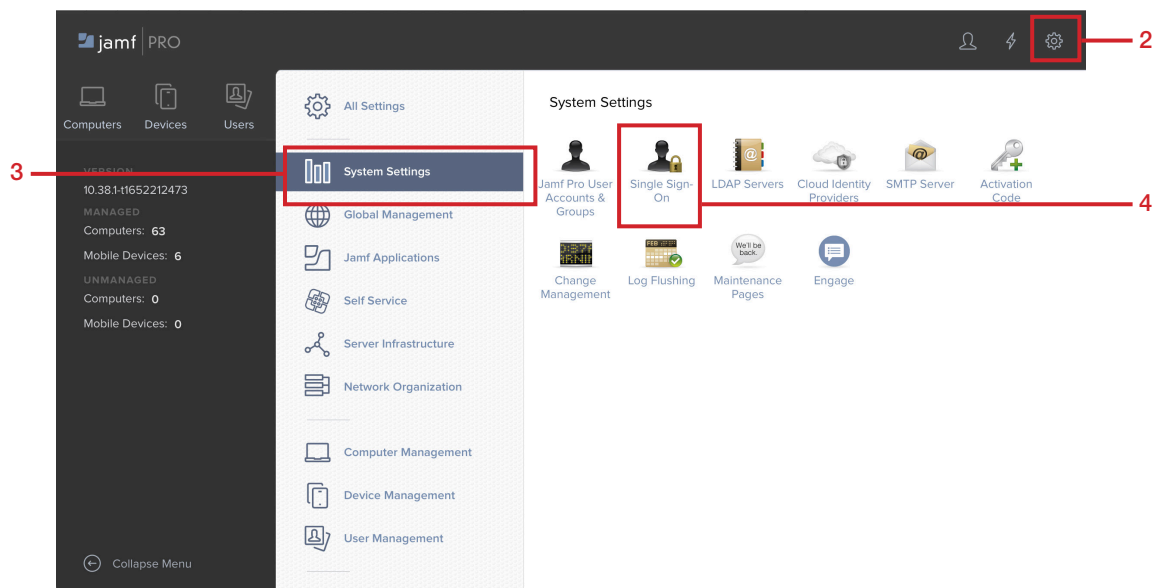
1. Log into your Jamf Pro server with administrative credentials.



2. In the upper-right, click Settings (looks Like a gear).

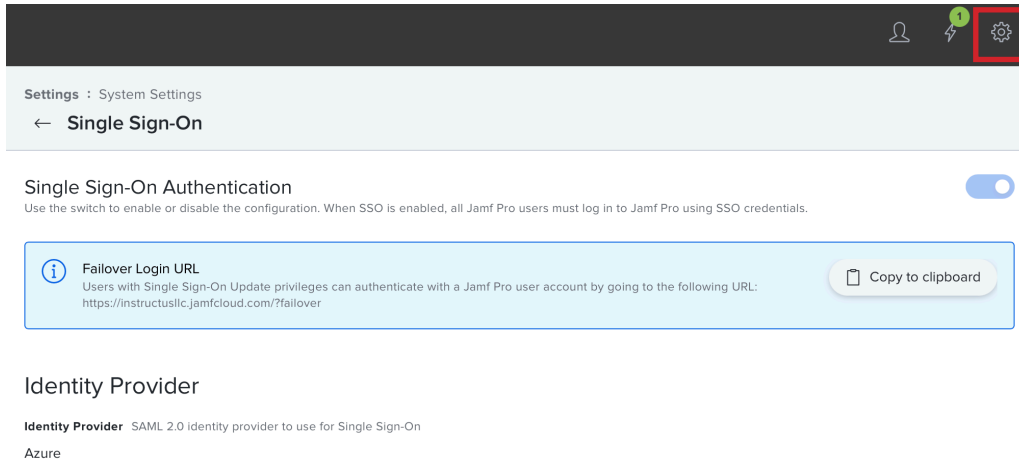
3. Click System Settings.

4. Click Single Sign-On.

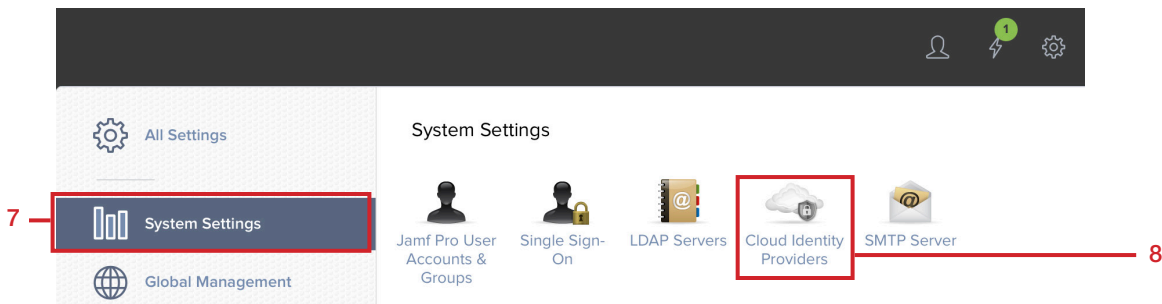




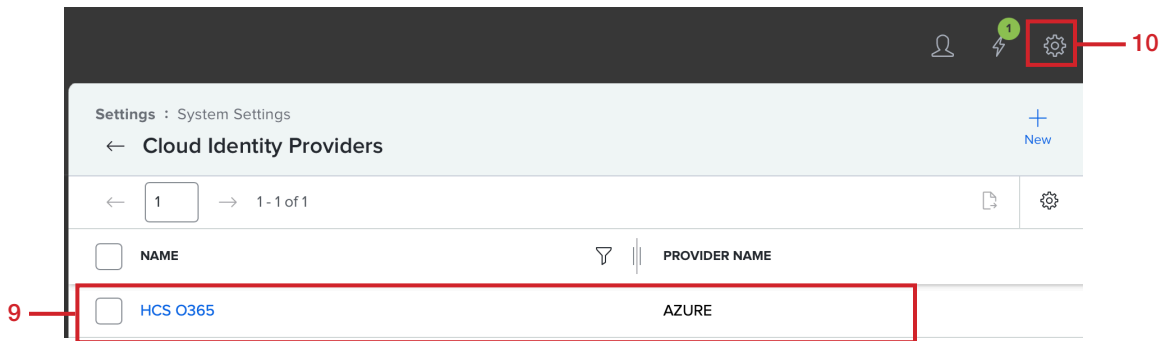
- 5. Confirm your Microsoft Azure is integrated into Jamf Pro for Single Sign-On.
- 6. Click Settings (looks like a gear).



- 7. Click System Settings.
- 8. Click Cloud Identity Providers.



- 9. Confirm your Microsoft Azure is integrated into Jamf Pro.
- 10. Click Settings (looks like a gear).

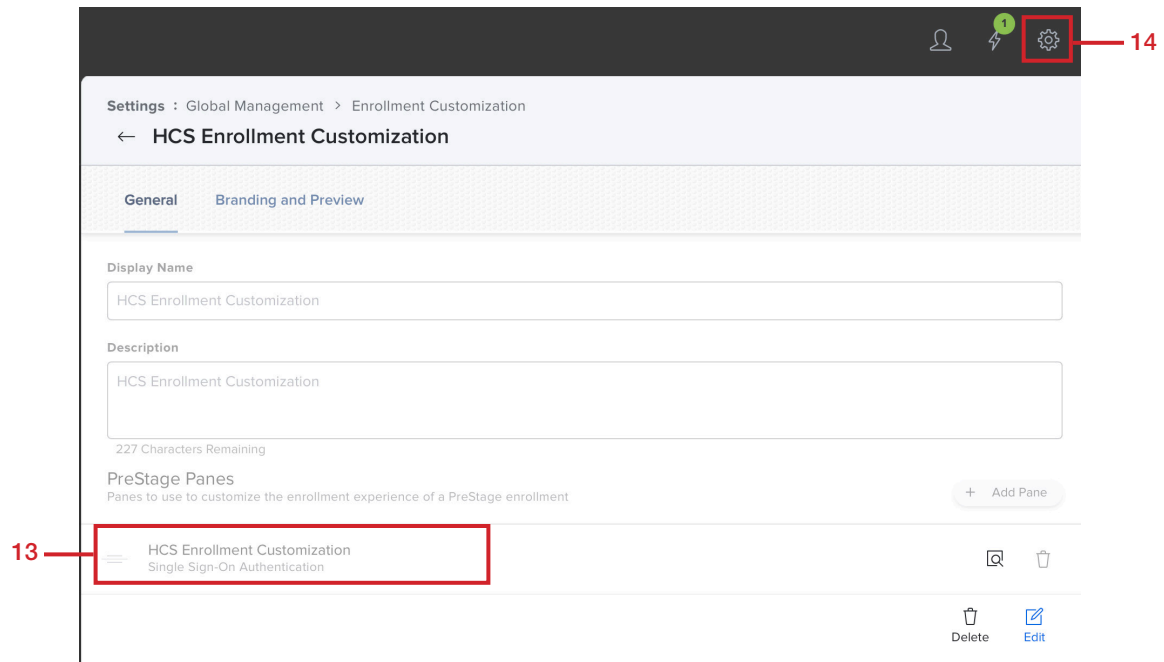




- 11. Click Global Management
- 12. Click Enrollment Customization.



- 13. Confirm your Enrollment Customization is configured to use Single Sign-On.
- 14. Click Settings (looks like a gear).

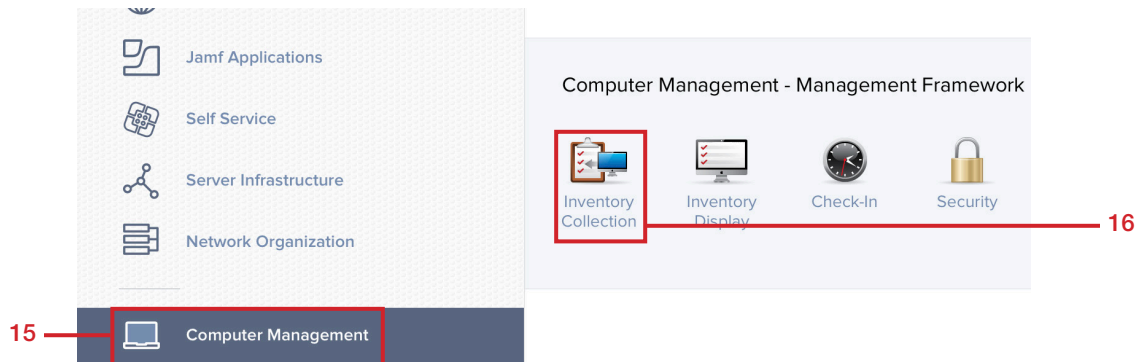




Confirmation of collecting user and location information from LDAP is very important and provides the mapping information from LDAP to Jamf Pro. If this is not configured for Computers and iOS Devices, the automation of email settings will not work.

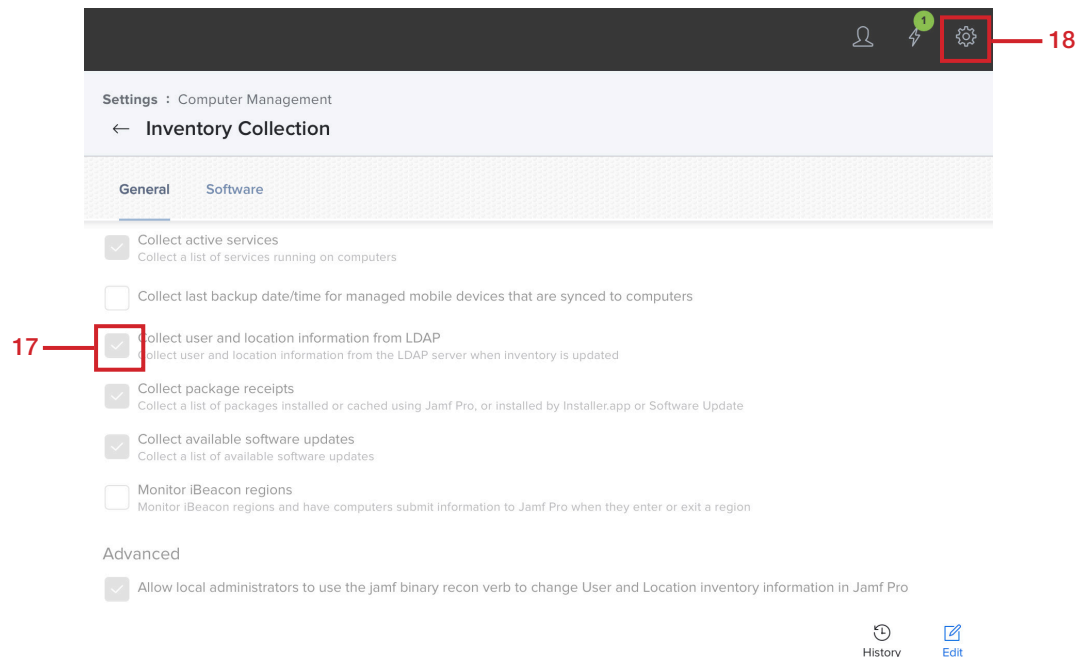
15. Click Computer Management.

16. Click Inventory Collection.



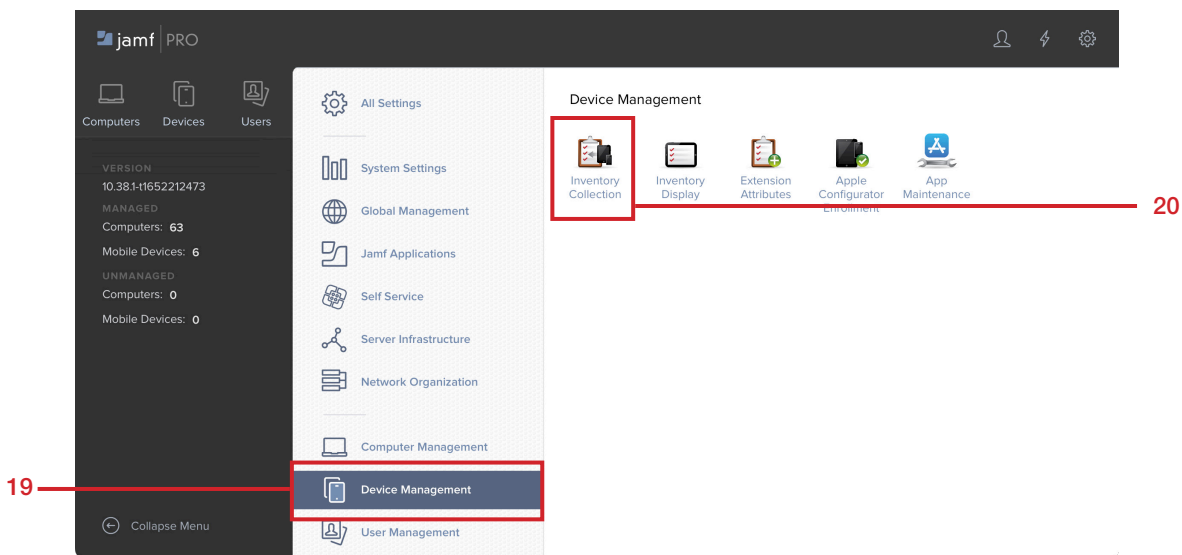
17. Confirm the checkbox for Collect user and location information from LDAP is selected.

18. Click Settings (looks like a gear).

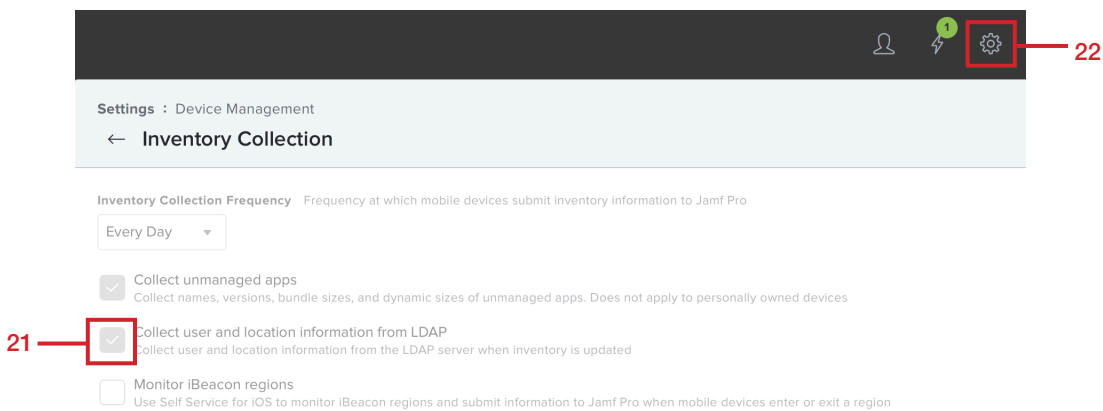




- 19. Click Device Management.
- 20. Click Inventory Collection.



- 21. Confirm the checkbox for Collect user and location information from LDAP is selected.
- 22. Click Settings (looks like a gear).

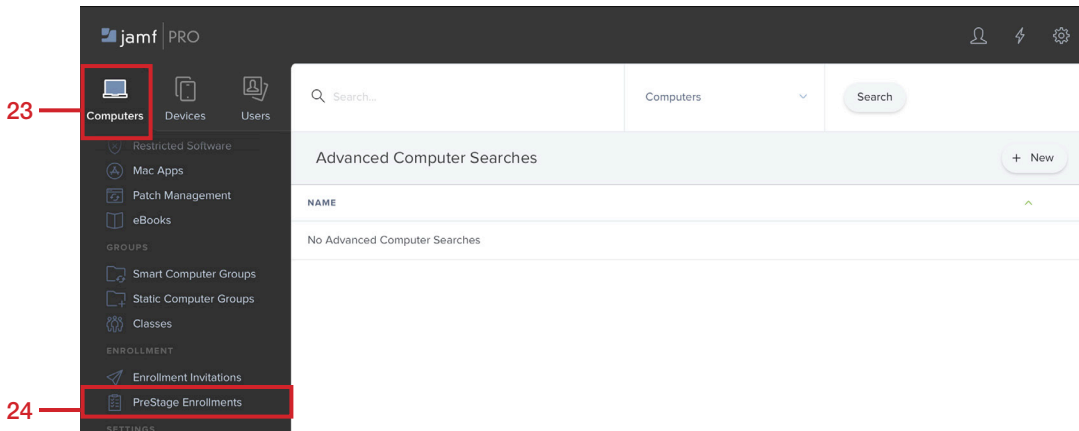




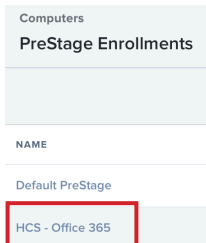
If you don't have a PreStage Enrollment configured, you can skip these steps and manually enroll your device into your Jamf Pro server. User Initiated Enrollment is NOT covered in this guide. You will need a PreStage setup for iOS devices that use an Enrollment Customization . This guide will only cover confirming it for computers. If you want to confirm it for iOS, Select the Devices tab, then select PreStage Enrollments.

23. Click Computers.

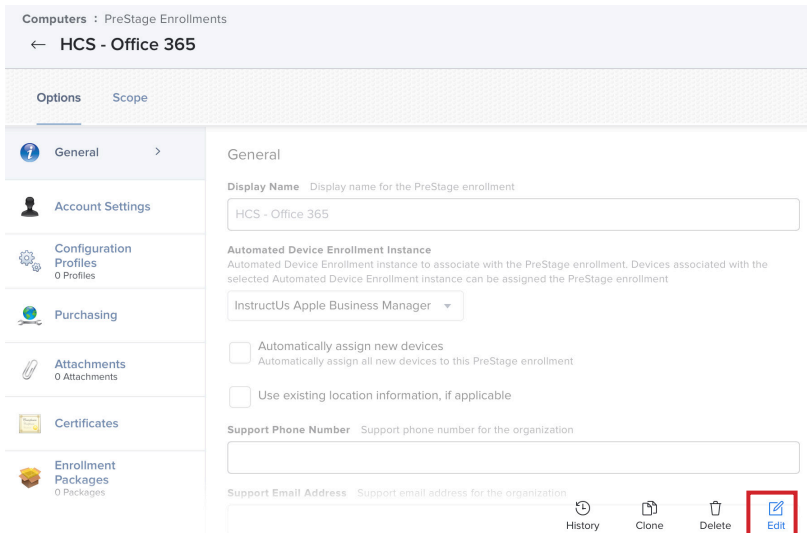
24. Click PreStage Enrollments.



25. Select your PreStage.



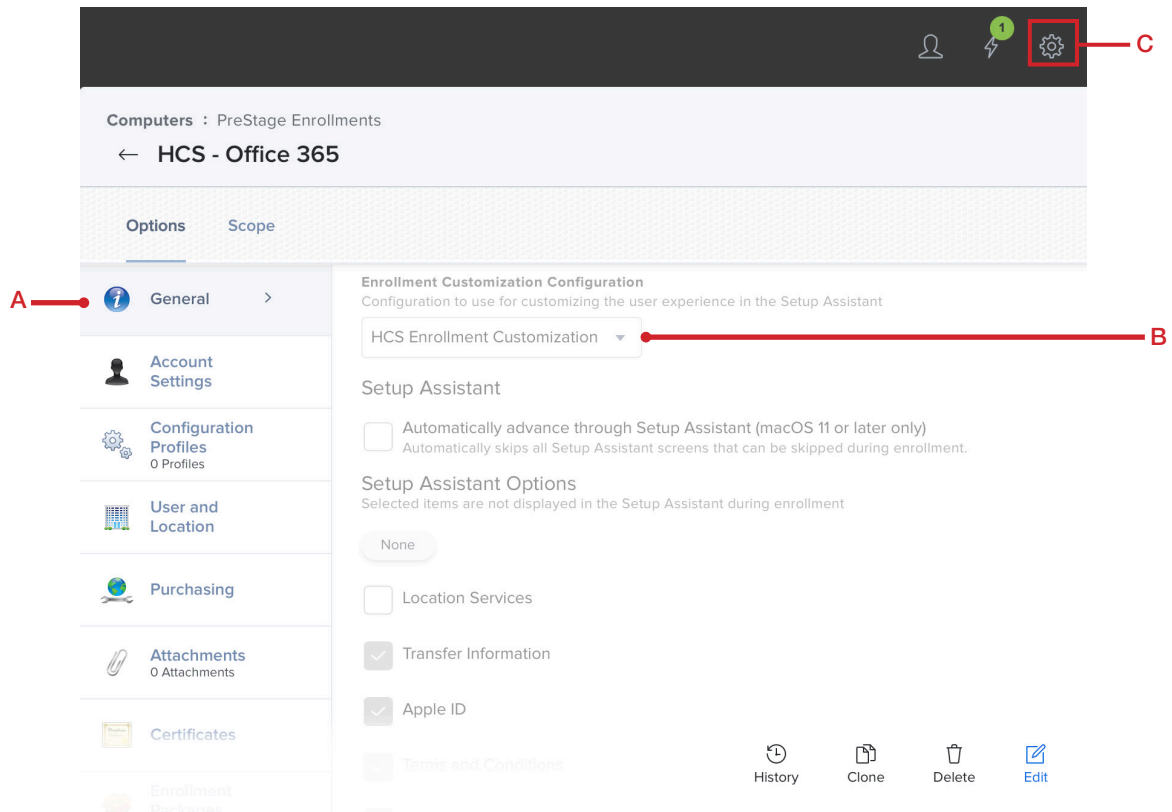
26. Click Edit.





27. Confirm the following:

- A. Click General.
- B. Enrollment Customization Configuration: Make sure your Enrollment Customization that is using Single Sign-On is selected.
- C. Click Settings (looks like a gear).



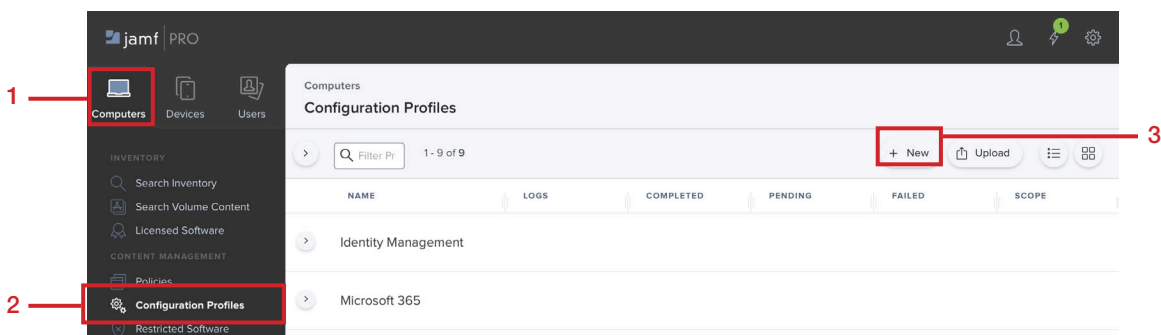
This completes this section. In the next section, we will create configuration profiles to automate the mail settings for a Mac computer and iOS device.



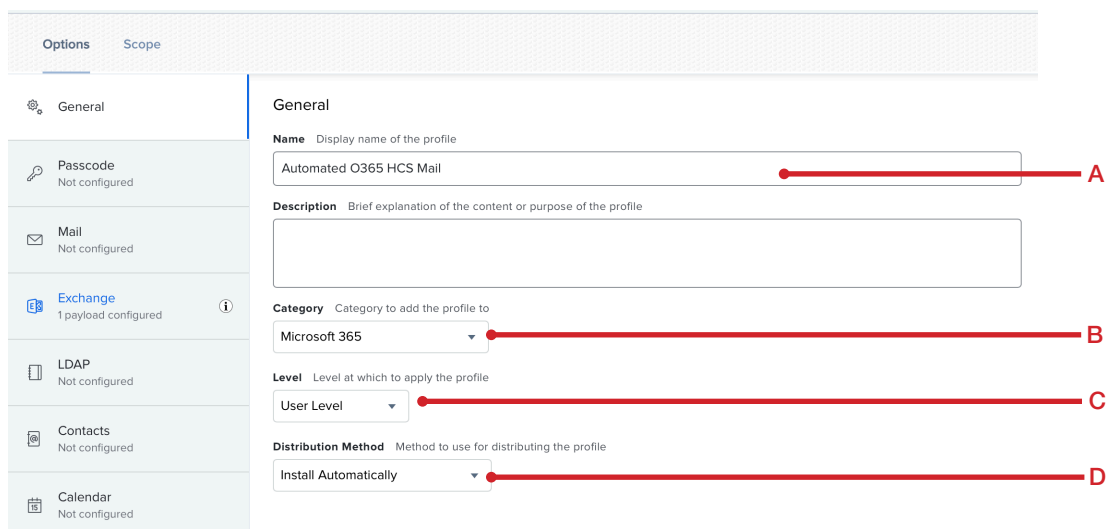
Section 2: Creating Configuration Profiles

In this section, we will create configuration profiles to automate the mail settings for a Mac computer and iOS device. You will need administrative access to your Microsoft Azure so you can get the Tenant ID which is required for the iOS configuration profile.

1. Click Computers.
2. Click Configuration Profiles.
3. Click New.



4. Select the General payload, then enter the following:
 - A. Name: A name of your choosing - This guide will use Automated O365 HCS Mail
 - B. Category: Select a category of your choosing
 - C. Level - Select User Level
 - D. Distribution Method: install Automatically





In this step, we will use variables that come from Microsoft Azure to pre fill the users name and email address. A list of common Microsoft Azure variables can be found here:

https://docs.jamf.com/10.38.0/jamf-pro/documentation/Mobile_Device_Configuration_Profiles.html?hl=mobile%2Cdevice%2Cconfiguration%2Cprofiles%2Cjamf%2Cpro%2Cdocumentation%2Cjamf

5. Select the Exchange Payload, then configure the following:

- A. Account Name - A name of your choosing - This guide will use HCS O365 Mail
- B. User: We will use the variable \$EMAIL that will populate the user account info which is the same as their email address. NOTE: This may be different in your environment.
- C. Email Address: We will use the variable \$EMAIL that will populate the user Email address
- D. Use OAuth for authentication (macOS 10.14 or later) - Make sure this is checked.
- E. Optional - If you want to restrict what can be done with mail, feel free to select the options under then OAuth setting.
- F. Internal Exchange Host: <https://outlook.office365.com/EWS/Exchange.asmx> (Port 443)
- G. Use SSL for Internal Exchange Host - Make sure this is checked
- H. External Exchange Host: <https://outlook.office365.com/EWS/Exchange.asmx> (Port 443)
- I. Use SSL for External Exchange Host - Make sure this is checked

The screenshot shows the 'Exchange' configuration page in Jamf Pro. On the left is a sidebar with navigation options: General, Passcode, Mail, Exchange (1 payload configured), LDAP, Contacts, Calendar, Network, and VPN. The main area is titled 'Exchange' and contains the following fields and options:

- Account Name:** HCS O365 Mail (labeled A)
- Domain:** (empty field)
- User:** \$EMAIL (labeled B)
- Email Address:** \$EMAIL (labeled C)
- Use OAuth for authentication (macOS 10.14 or later):** (labeled D)
- Allow messages to be moved:** (labeled E)
- Allow recent addresses to be synced:** (labeled E)
- Allow Mail Drop:** (labeled E)
- Use Only in Mail:** (labeled E)
- Internal Exchange Host:** <https://outlook.office365.com/EWS/Exchange.asmx> : 443 (labeled F)
- Internal Server Path:** (empty field)
- Use SSL for Internal Exchange Host:** (labeled G)
- External Exchange Host:** <https://outlook.office365.com/EWS/Exchange.asmx> : 443 (labeled G)
- External Server Path:** (empty field)
- Use SSL for External Exchange Host:** (labeled H)



6. Select Scope and scope to your needs. Click Save.

7. Click Devices.

8. Configuration Profiles.

9. Click New

10. Select the General Payload, then configure the following:

- A. Name: A name of your choosing - This guide will use: Automated O365 HCS Mail
- B. Category: Select a category of your choosing
- C. Level - Select Device Level
- D. Distribution Method: install Automatically



11. In this step you will need the Tenant ID from your Microsoft Azure. Click the Exchange ActiveSync payload. Click Configure and enter the following:
- A. Account Name: com.apple.eas.account
 - B. Exchange ActiveSync Host: outlook.office365.com
 - C. Use SSL - Make sure the checkbox is selected
 - D. User: We will use the variable \$EMAIL that will populate the user account info which is the same as their email address. NOTE: This may be different in your environment.
 - E. Email Address: We will use the variable \$EMAIL that will populate the user Email address
 - F. Use OAuth for authentication (iOS 12 or later)
 - G. OAuth Sign in URL: <https://login.microsoftonline.com/YOURTENENTIDHERE/oauth2/v2.0/authorize>
 - H. OAuth Token Request URL: <https://login.microsoftonline.com/YOURTENENTIDHERE/oauth2/v2.0/token>
 - I. Set all other options to your needs.
 - J. Click Save when done.

The screenshot shows the 'Exchange ActiveSync' configuration screen. On the left is a sidebar with various account types, and on the right is the configuration form. Red lines and letters A through J point to the following elements:

- A:** Account Name field, containing 'com.apple.eas.account'
- B:** Exchange ActiveSync Host field, containing 'outlook.office365.com'
- C:** 'Use SSL' checkbox, which is checked
- D:** User field, containing '\$EMAIL'
- E:** Email Address field, containing '\$EMAIL'
- F:** 'Use OAuth for authentication (iOS 12 or later)' checkbox, which is checked
- G:** OAuth Sign in URL field, containing 'https://login.microsoftonline.com/1.../oauth2/v2.0/authorize'
- H:** OAuth Token Request URL field, containing 'https://login.microsoftonline.com/.../oauth2/v2.0/authorize'
- I:** A vertical line on the right side of the 'Enabled Services' section, which includes 'Calendars', 'Contacts', 'Mail', 'Notes', and 'Reminders' (all checked)
- J:** The 'Save' button at the bottom right of the screen



12. Select Scope then scope to your needs and click Save.

Mobile Devices : Configuration Profiles

← Automated O365 HCS Email

Options Scope

Targets Limitations Exclusions

Target Mobile Devices
Mobile devices to assign the profile to. Does not apply to personally owned devices

Specific Mobile Devices

Target Users
Users to distribute the profile to

Specific Users

Selected Deployment Targets + Add

TARGET	TYPE
No Targets	

Cancel Save

This completes this section. In the next section, we will enroll a Mac computer and iOS device into the Jamf Pro server.



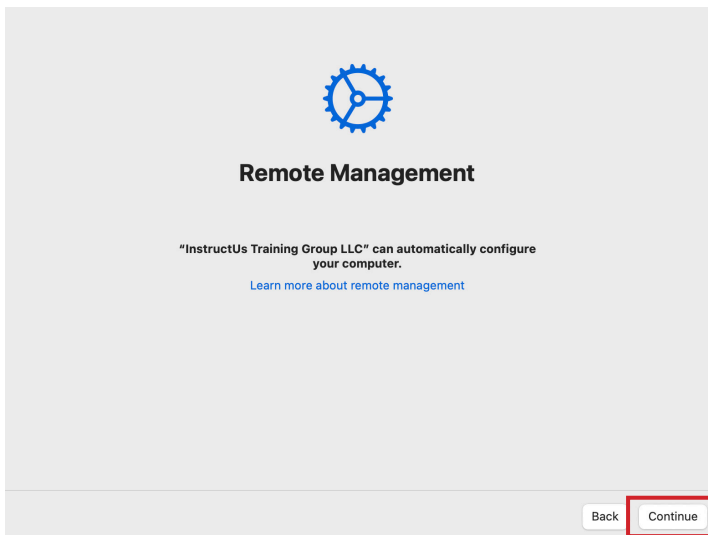
Section 3: Deploying a Device with Automated Mail Settings

In this section, we use automated device enrollment to enroll a Mac computer and iOS device into the Jamf Pro server. You will need your Microsoft Azure user name and password during the enrollment process. This will add your information to the device record in Jamf Pro and that information is passed to the variables we set in the configuration profiles in section 2 of this guide. (\$EMAIL was the variable we used in section 2)

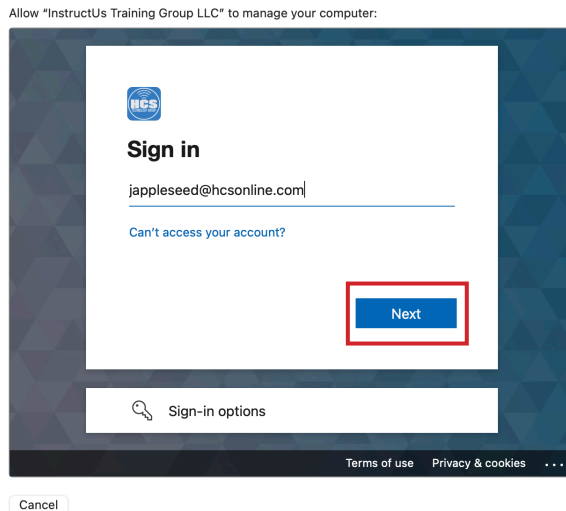
In order to keep this guide concise, we are only showing a few of the Automated Device Enrollment screens to demonstrate the Single Sign-On message during enrollment. This guide will use a Mac computer that we erased and is ready for Automated Device Enrollment.

macOS

1. Power on your Mac computer and follow the onscreen instructions. When you get to the Remote Management screen, Click Continue.



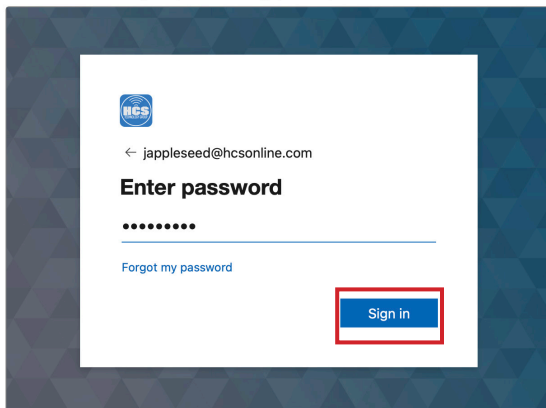
2. Enter your Microsoft Azure Single Sign-On name. This is usually your email address. Click Next.





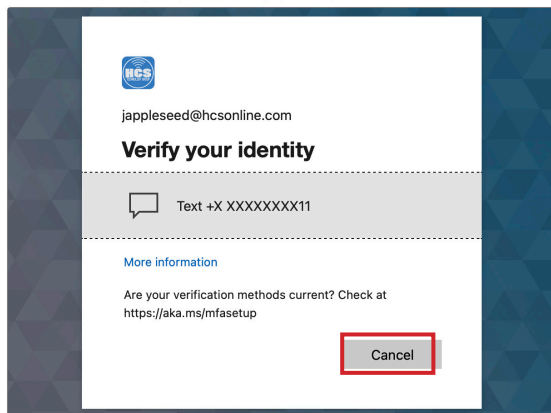
3. Enter your password then click Sign in.

Allow "InstructUs Training Group LLC" to manage your computer:



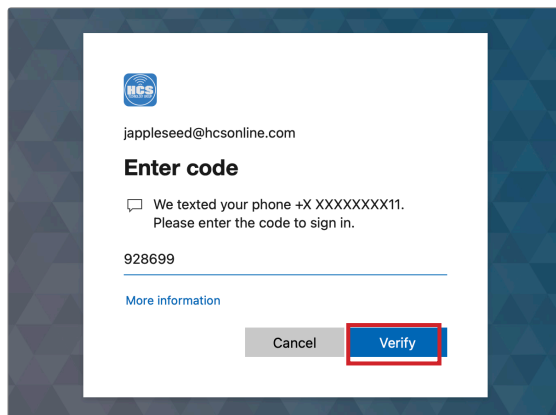
4. If you are using Multi Factor Authentication, select a verification method. This guide will use Text.

Allow "InstructUs Training Group LLC" to manage your computer:



5. Enter the code that was sent to your phone then click Verify.

Allow "InstructUs Training Group LLC" to manage your computer:



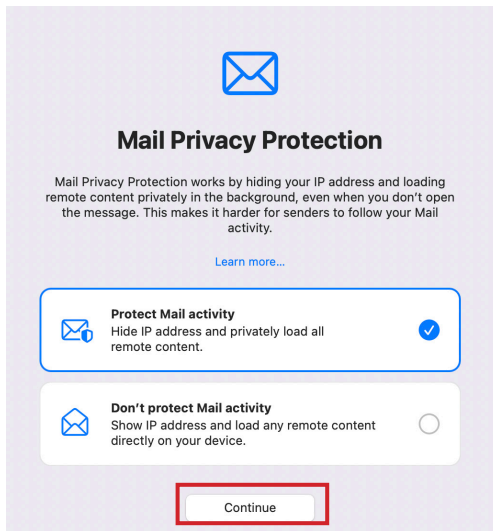
NOTE: In order to keep this guide concise, we are only showing the Single Sign-On messages during enrollment. Follow the additional on screen instructions to complete the setup and log into your Mac.




6. Open the Mail application located in the Dock.



7. Choose an option below, then click Continue.




8. Select your account then click  (Reconnect) to the right of your account. This guide will use HCS O365 Mail as our account.





9. Enter your password then click Sign in.

Enter the password for the account "HCS O365 Mail".



Microsoft

← jappleseed@hconline.com

Enter password

.....

[Forgot my password](#)

[Sign in with another account](#)


Sign in

[Terms of use](#) [Privacy & cookies](#) ...

Cancel

10. If you are using Multi Factor Authentication, select a verification method. This guide will use Text.

Enter the password for the account "HCS O365 Mail".



jappleseed@hconline.com

Verify your identity

Text +X XXXXXXXX11

Are your verification methods current? Check at <https://aka.ms/mfasetup>


Cancel

[Terms of use](#) [Privacy & cookies](#) ...

Cancel

11. Enter the code that was sent to your phone then click Verify.

Enter the password for the account "HCS O365 Mail".



jappleseed@hconline.com

Enter code

We texted your phone +X XXXXXXXX11. Please enter the code to sign in.

690395

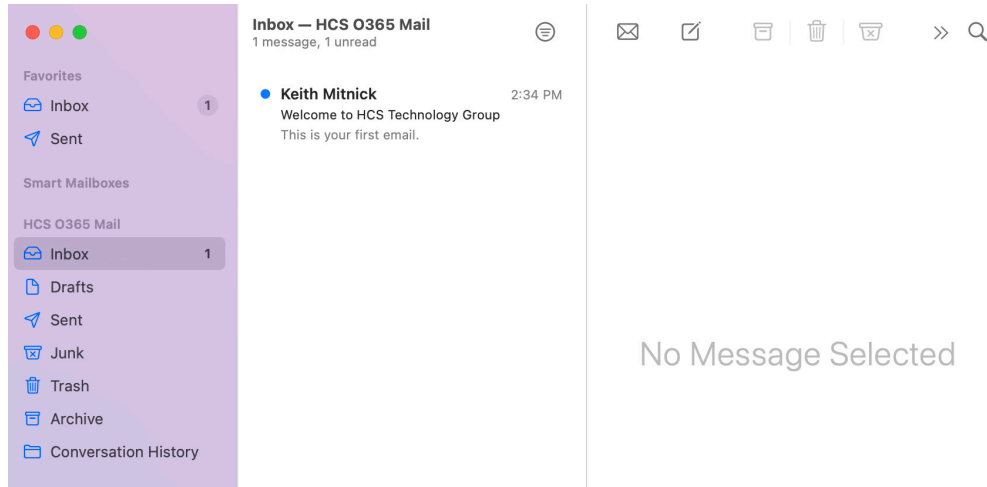
Cancel **Verify**

[Terms of use](#) [Privacy & cookies](#) ...

Cancel



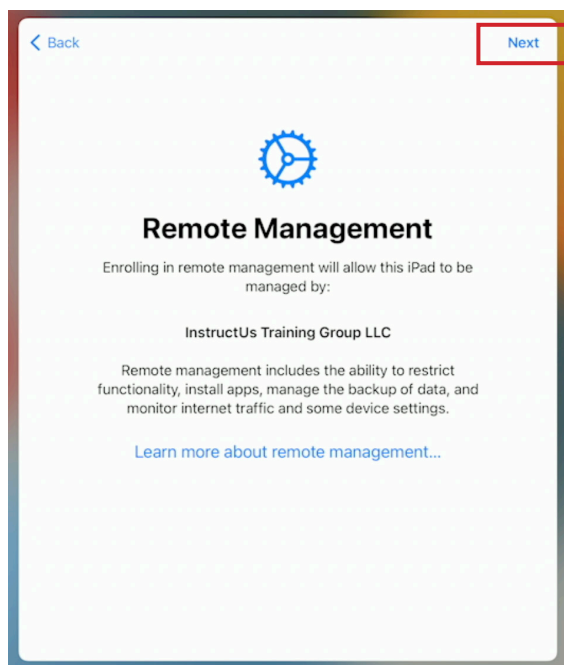
12. If all went well, Email will start to load into your account and all we had to do was enter our password. The configuration profile handled everything else needed to configure Apple Mail.



iOS/iPadOS

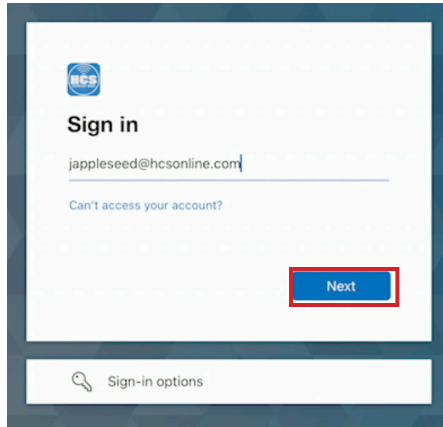
In order to keep this guide concise, we are only showing a few of the Automated Device Enrollment screens to demonstrate the Single Sign-On message during enrollment. This guide will use an iPad that we erased and is ready for Automated Device Enrollment.

13. Power on your iPad and follow the on screen instructions. When you get to the Remote Management screen, Click Next.

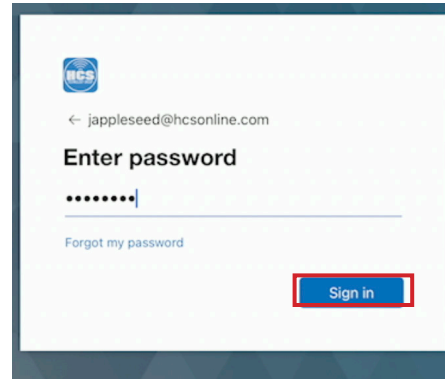




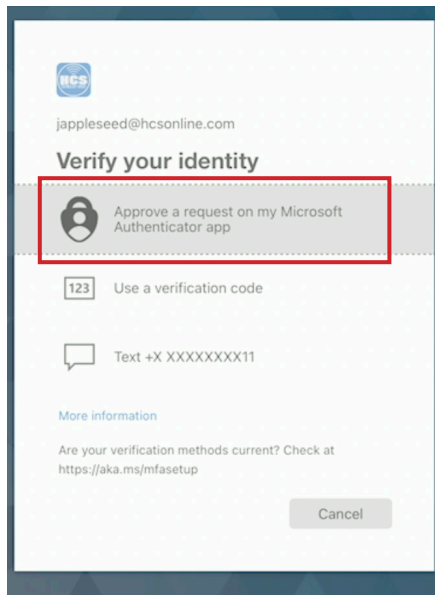
14. Enter your Microsoft Azure Single Sign-On name. This is usually your email address. Click Next.



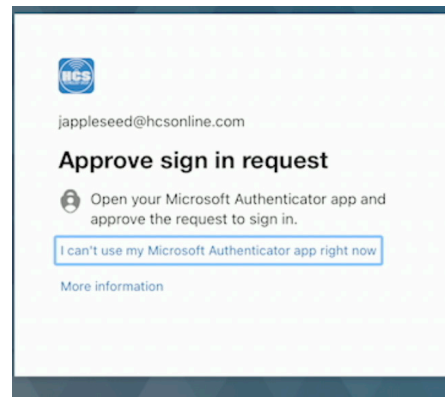
15. Enter your password then click Sign in.



16. Select your method for verifying your identity. This guide will use the Microsoft Authenticator App.

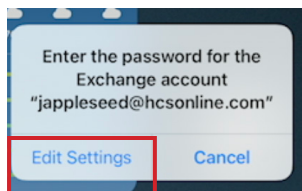


17. Approve the sign in request on your phone.



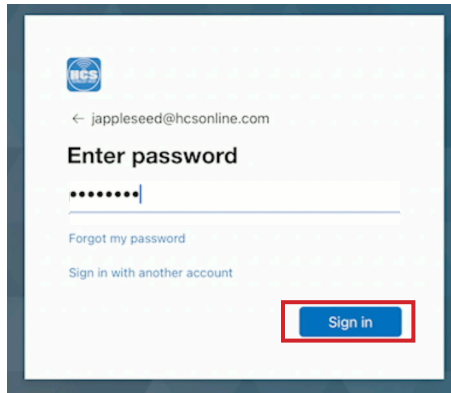
NOTE: We used text as a way of verification in the previous lessons. We wanted to show there are other ways to verify by using the Microsoft Authenticator app.

18. Click Edit Settings at the message below. Notice the users email address is populated in the message.

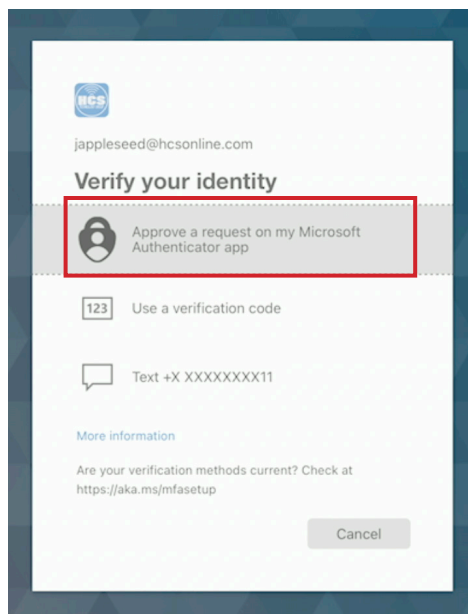




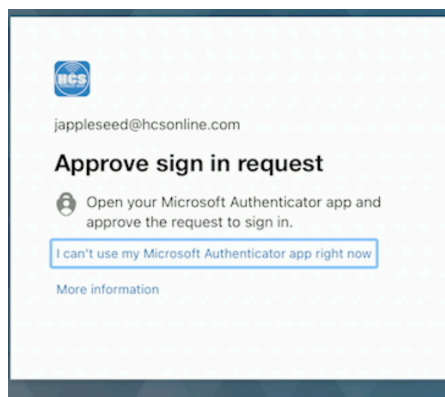
19. Enter your password then click Sign in.



20. Select your method for verifying your identity. This guide will use the Microsoft Authenticator App.

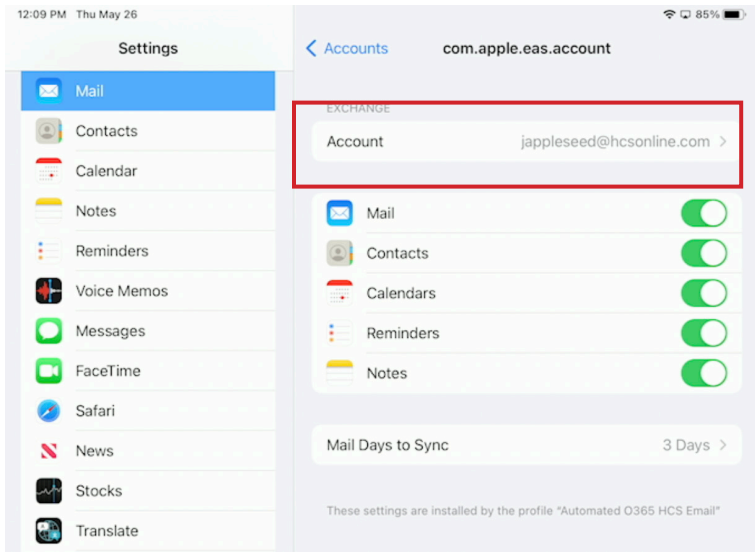


21. Approve the sign in request on your phone.





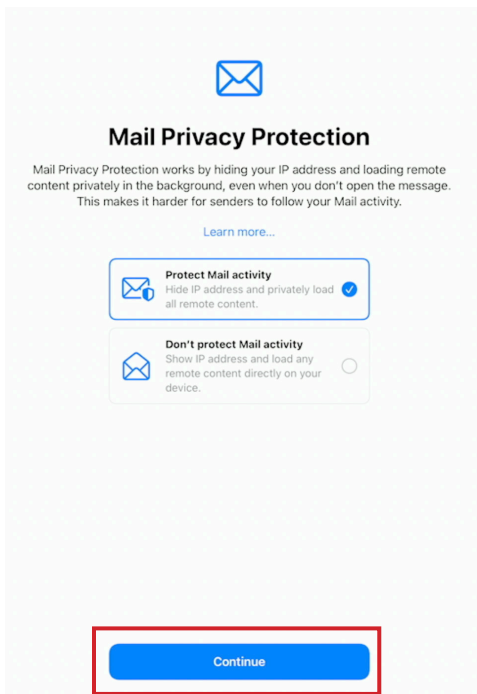
22. The email account is now configured.



23. Open the Mail app on your device. This guide will open it from the Dock.

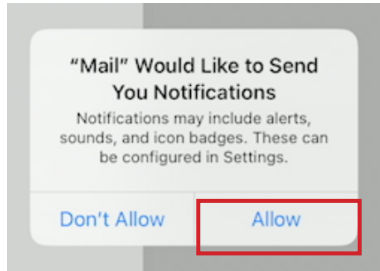


24. Select a Mail Privacy Protection setting. This guide will use Protect Mail activity. Tap Continue.

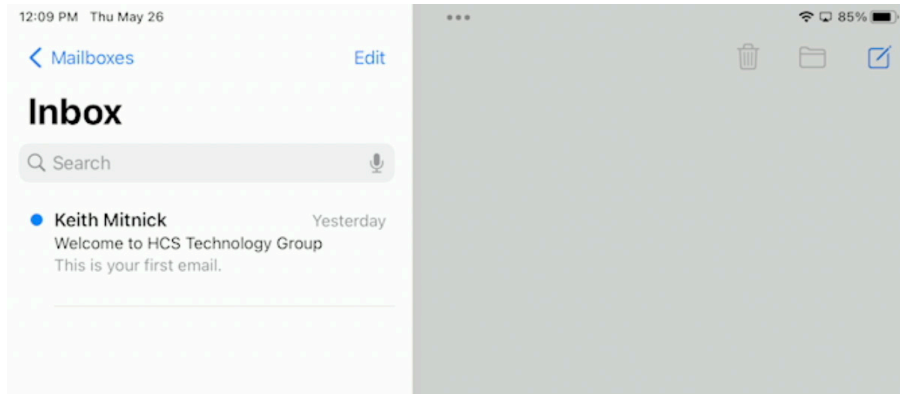




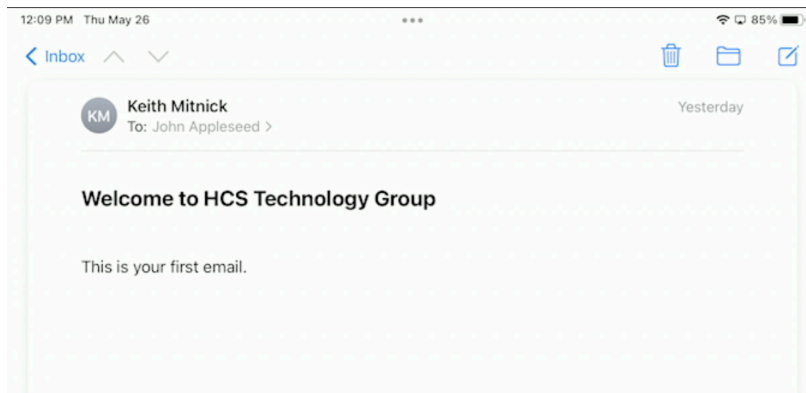
25. At the message below, make a selection. This guide will tap Allow.



26. Confirm the Mail app opens with your mail account already configured and ready to use. .



27. Tap on an email to see it display. All settings were configured for us and all we had to provide was our password.



This completes the guide.