jamf | PRO

How to Configure Jamf Pro SMTP to
Use the Microsoft Graph API

Contents

Preface

Configuring Jamf Pro to use the Microsoft Graph API for SMTP enhances security, ensures compliance, and simplifies management, all while aligning with Microsoft's modern authentication framework. It also future-proofs your organization's Jamf Pro setup and improves the reliability of email notifications. This is particularly beneficial for organizations heavily invested in the Microsoft 365 ecosystem.

This guide is designed to complement Jamf's documentation on configuring the Microsoft Graph API for SMTP by offering a more visual, step-by-step approach. Please note that Microsoft occasionally updates the names and locations of certain items, so your experience may differ slightly. For the most up-to-date information, refer to Jamf's official documentation at:

Configuring Jamf Pro to Use Microsoft Graph API with SMTP

Requirements for This Guide:
Ensure you have administrative privileges for the following systems and tools:

- Jamf Pro Server: Version 11.4 or later.
- Microsoft Entra ID: Access to manage settings and configurations.
- Exchange Admin Center: Administrative access for email configuration.
- PowerShell for Mac: Version 7.4 or later installed.
- PowerShell Exchange Module: Installed and configured.
- An email account managed by your organization, such as jamfalerts@yourdomain.com.

NOTE: An Exchange administrator with at least Organization Management permissions is required to configure permissions in Exchange admin center.

Download Link:
PowerShell for Mac: Installing PowerShell on macOS (Version 7.4)

https://learn.microsoft.com/en-us/powershell/scripting/install/installing-powershell-on-macos?view=powershell-7.4

This guide is designed for Mac administrators and demonstrates all configurations using a Mac computer. It includes instructions for installing PowerShell for Mac and the Exchange Module. If you already have these tools installed, you can skip the corresponding steps. For those following this guide on a Windows computer, some steps may differ, and your results may vary.

Section 1: Creating an app registration in Microsoft Entra for Jamf Pro

What You'll Need:
Learn what hardware, software, and information you'll need to complete the tutorials in this section.
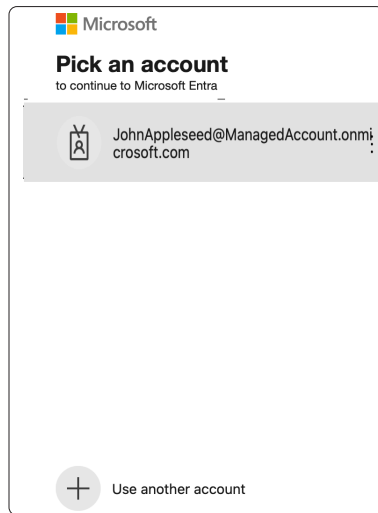
Hardware and Software:
Requirements for following along with this section:
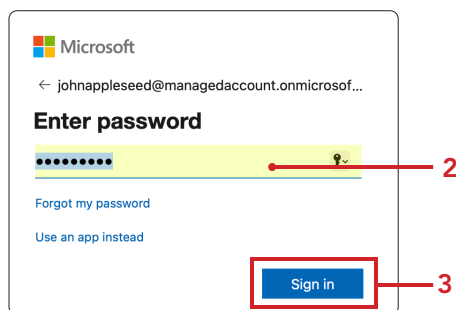- Access to Microsoft Entra with administrative privileges

In this section we will configure an app registration in Microsoft Entra to be used in Jamf Pro for SMTP.

1. Log in to the Microsoft Entra admin center at: https://entra.microsoft.com/.
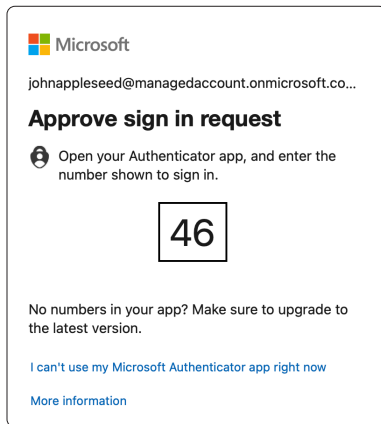

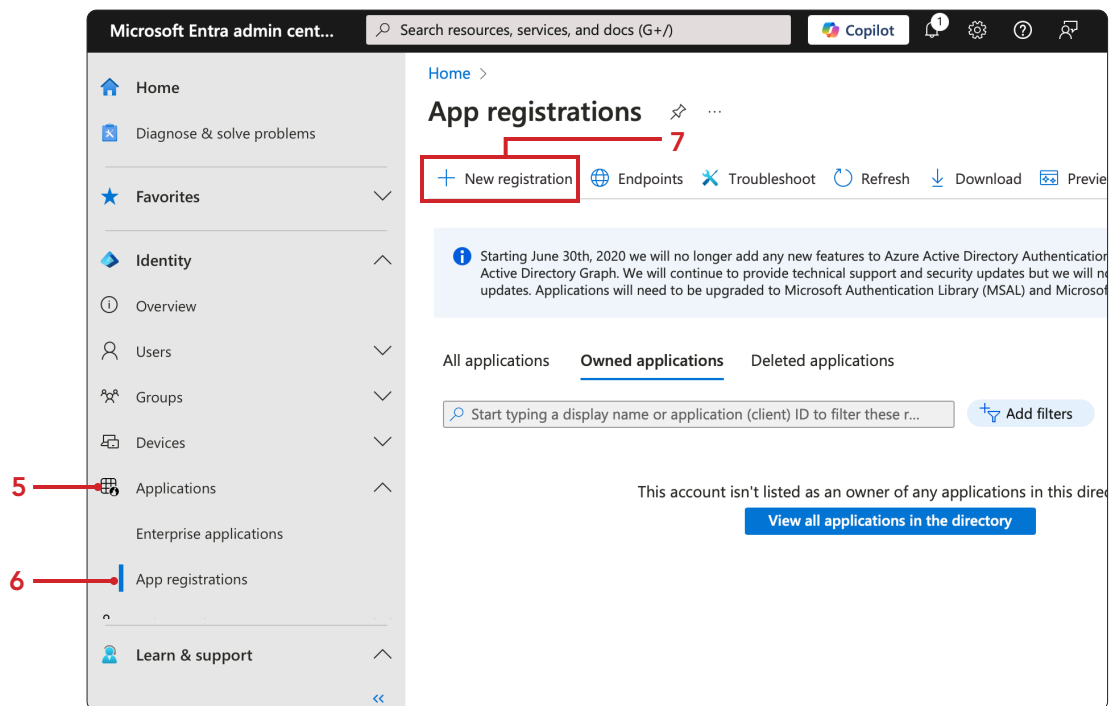2. Enter your password.

3. Click Sign in.

4. If you're using Multi Factor Authentication , approve your sign in request.
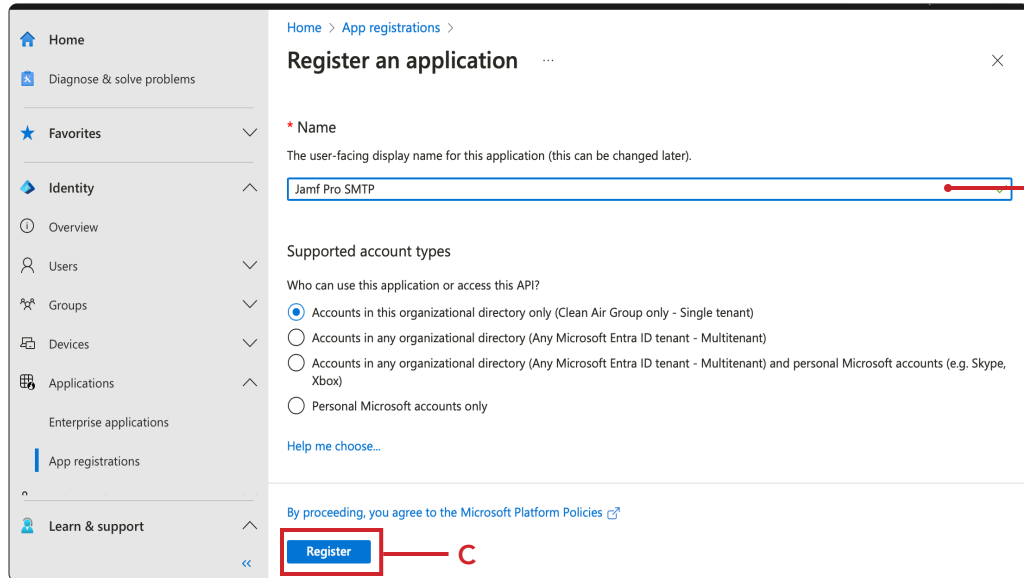

5. Click Applications.

6. Click App registrations.

7. Click New Registration (+).

8. Configure the following:
    A. Name: Jamf Pro SMTP
    B. Leave all other items at their default settings
    C. Click Register


9. Open TextEdit located in the Applications folder.

TextEdit

10. Create a new document and enter the following:
    A. Client ID:
    B. Tenant ID:
    C. Object ID:
    D. Service Principal ID:
   E. Client Secret Value ID:
    F. Email Group ID:

11. Save the file to your Desktop and name it: Entra_Registration_Info

12. Keep the document open. We will fill in the information in this document throughout the guide.
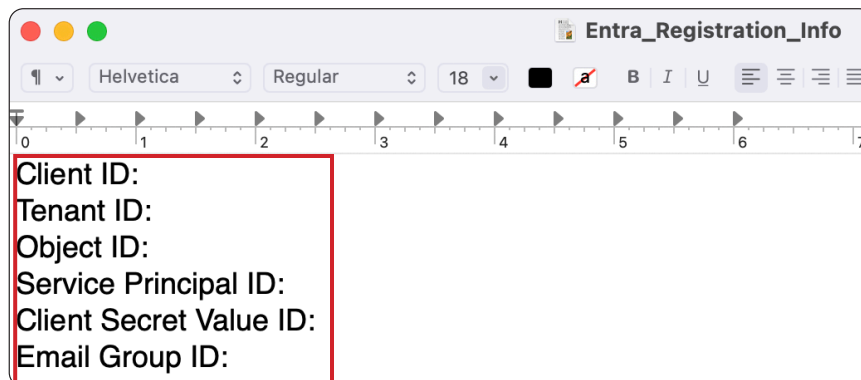
13. Switch back to Microsoft Entra and copy and paste the following information into the Entra_Registration_Info document on your Desktop:
   A. Application (client) ID
   B. Object ID
   C. Directory (tenant) ID
   D. In the "Managed application in local directory section", Click Jamf Pro SMTP
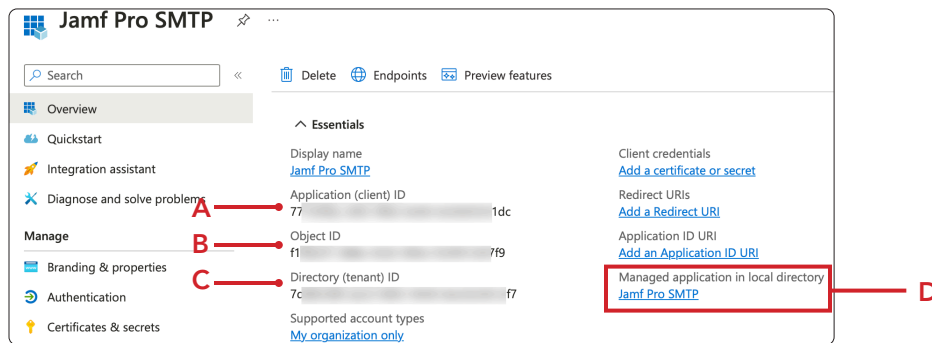
14. Copy the Object ID and paste it into the Service Principal ID section of the Entra_Registration_Info document.
   NOTE: The Object ID is also known as the Service Principal ID. This is different from the Object ID in the previous step.

Copy this Object Id and paste it into your Entra_Registration_Info for Service Principal ID
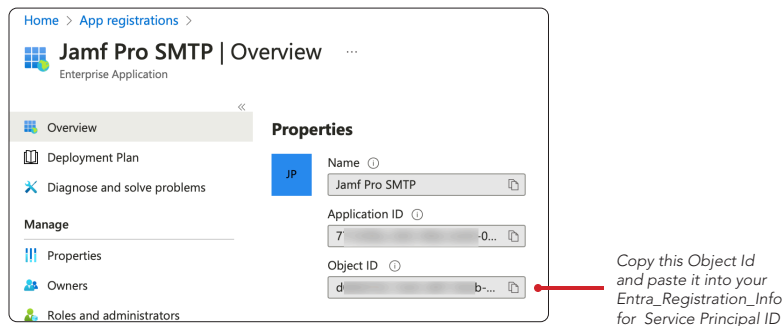
15. Confirm the information in the Entra_Registration_Info document looks similar to the picture below. Save the document but keep it open. We will need to add more info in a later step.
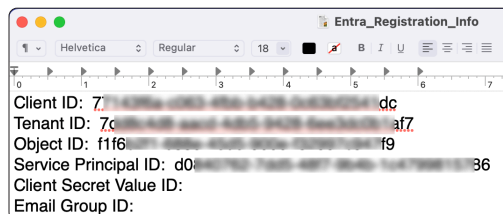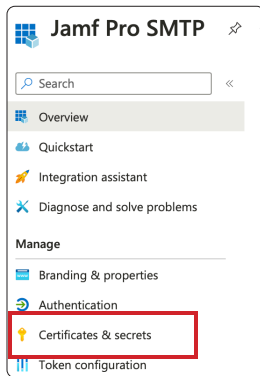

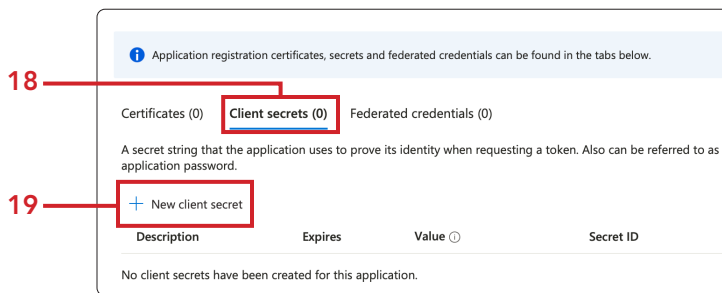16. Click the back button in your browser.
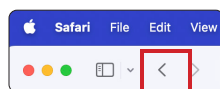
17. Click Certificates & secrets.

18. Click Client Secrets.

19. Click New client secret (+).

20. Configure the following:
    A. Description: Jamf Pro SMTP
    B. Expires: Select a time of your choosing. This guide will select Recommended: 180 days (6months)
    C. Click Add

21. Copy the Value.

22. Switch back to the Entra_Registration_Info document and paste in the Value to the Client Secret Value ID: section of the document. Save the document but keep it open. We will need to add more info in a later step.

This completes this section. In the next section, we will create a mail enabled security group to be used for sending Email from the Jamf Pro server.

Section 2: Configuring a Mail-enabled security group in Exchange admin center

What You'll Need:
Learn what hardware, software, and information you'll need to complete the tutorials in this section.

Hardware and Software:
Requirements for following along with this section:
- • Exchange Admin Center access with administrative privileges

An Exchange administrator with at least Organization Management permissions is required to configure permissions in Exchange admin center. In this section we will configure a Mail-enabled security group and add members to the group that need to receive mail from the Jamf Pro server.

1. Log in to the Exchange Admin Center: https://admin.exchange.microsoft.com/#/adminRoles
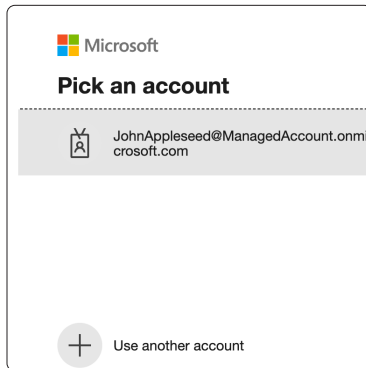
2. Enter your password.

3. Click Sign in.
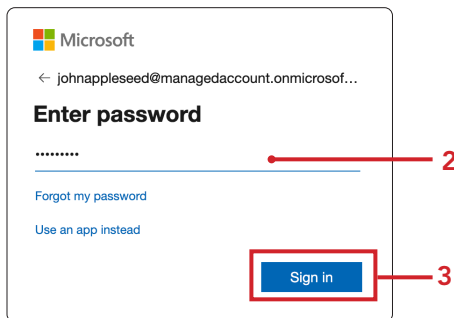
4. If you're using Multi Factor Authentication, approve your sign in request.
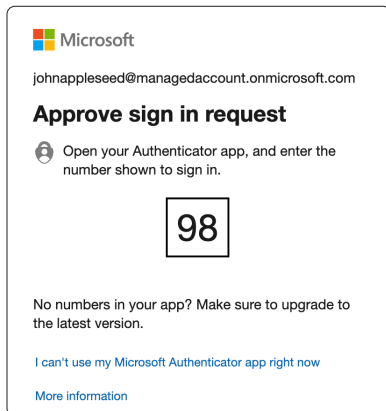
5. Click Recipients.

6. Click Groups.

7. Click Mail-enabled security.

8. Click Add a group.
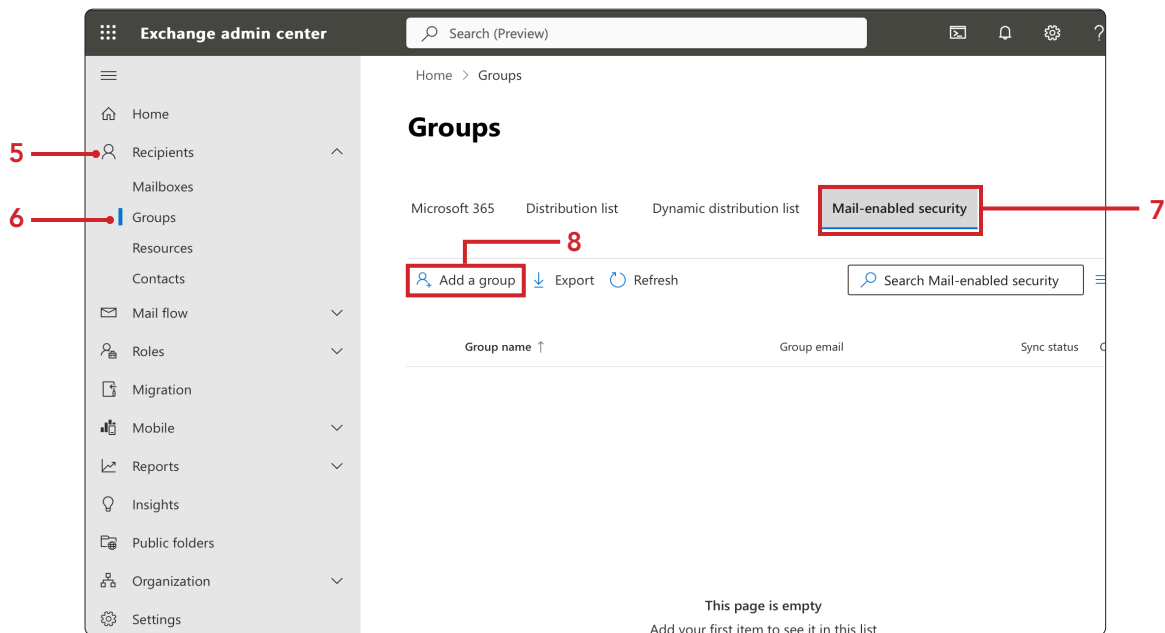
9. Select the radio-button for Mail-enabled security

10. Click Next.
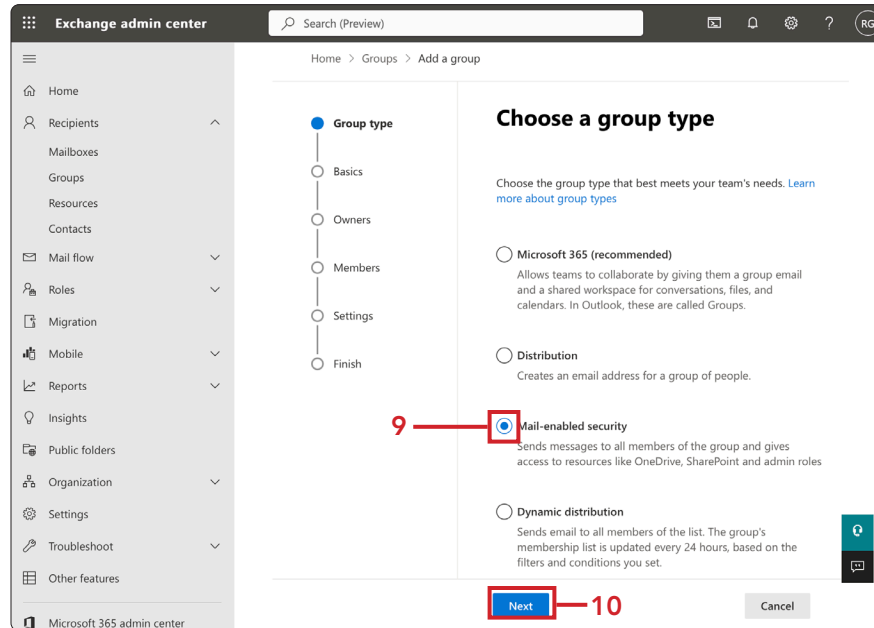
11. Configure the following:
    A. Name: JamfProSMTP
    B. Description: Optional - This guide will use: Used for Jamf Pro SMTP
    C. Click Next
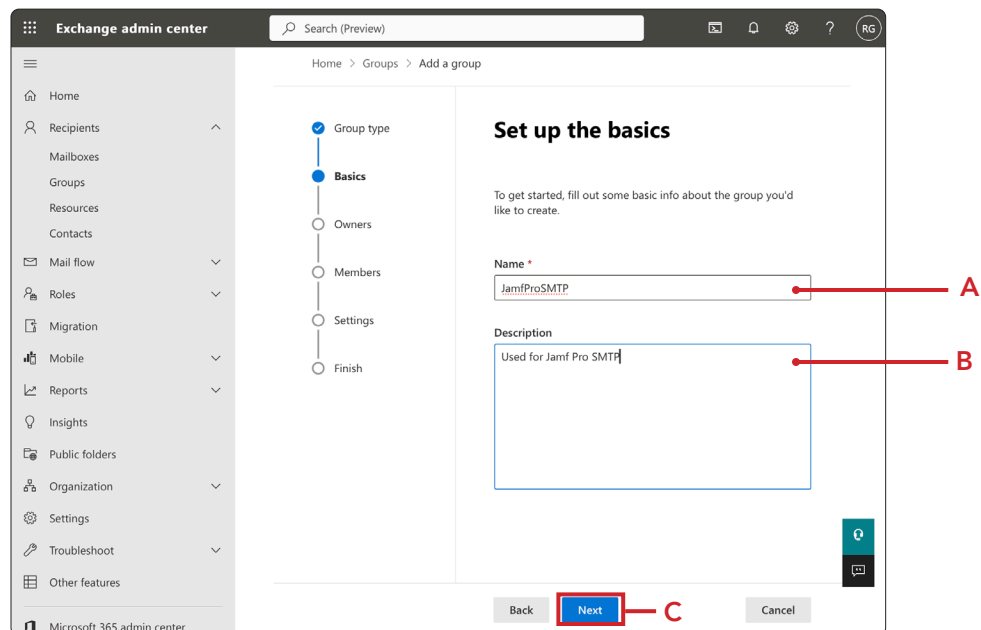
12. Click Assign owners.

Assign owners

Group owners have unique permissions to manage the group. They can add and remove members, change group settings, rename the group, update its description, and more.

� You have to have at least one owner. We recommend adding two, so one can help out in the other's absence.

\+ Assign owners

13. Select the Exchange administrator accounts that should have permissions to manage the group.

14. Click Add.

Assign owners

Select up to 20 people to join this group as owners. You can add more later from Active teams & groups.

🔍 Search for a name or email address

⚪ **Display name**

⚪ JA Jamf Alerts
        jamfalerts@managedaccount.org

13 ── ✔ KM Keith Mitnick
             kmitnick@managedaccount.org

14 ── Add (1)   Cancel

15. Click Next.

Assign owners

Group owners have unique permissions to manage the group. They can add and remove members, change group settings, rename the group, update its description, and more.

ⓘ You have to have at least one owner. We recommend adding two, so one can help out in the other's absence.

+ Assign owners

○   Display name

○ KM Keith Mitnick
        kmitnick@managedaccount.org

Back   Next   Cancel

16. Click Add members.

Add members

Group members have access to everything the group can access, and will receive email messages sent to the group email address. By default, they can invite guests to join your group, but they can't edit group settings.

+ Add members

Add your first group member
New members will receive an email when you add them

17. Choose an account to use for sending email from the Jamf Pro server. We recommend selecting an email account managed by your organization, such as jamfalerts@yourdomain.com.
NOTE: We recommend documenting the member email address that you're using in this step as you will need it when setting up SMTP on the Jamf Pro server in the last section of this guide.

18. Click Add.

Add members

Select up to 20 people to join this group as members. You can add more later from Active teams & groups.

🔍 Search for a name or email address

◯ **Display name**

17─── ☑ JA Jamf Alerts
jamfalerts@managedaccount.org

18─── Add (1)   Cancel

19. Click Next.

Add members

Group members have access to everything the group can access, and will receive email messages sent to the group email address. By default, they can invite guests to join your group, but they can't edit group settings.

+ Add members

◯ Display name

◯ JA Jamf Alerts
jamfalerts@managedaccount.org

Back   Next   Cancel

20. Configure the following:
 A. Group email address: create an address of your choosing. This guide will use jamfsmtp
 B. Domains: Select your domain.
 C. Approval: Select the checkbox for "require owner approval to join the group"
 D. Click Next

Edit settings

Mail-enabled security group

Has all the functionality of a distribution list and additionally can be used to control access to OneDrive and SharePoint.

Group email address *   Domains

A ———— jamfsmtp @ managedaccount.org ———— B

Communication
☐ Allow people outside of my organization to send email to this Mail-enabled security group

Approval
C ———— ☑ Require owner approval to join the group

Back **Next** ———— D   Cancel

21. Click Create group.

Review and finish adding group

You're almost there - make sure everything looks right before adding your new group.

Group type
Mail-enabled security
Edit

Basics
Name: JamfProSMTP
Description: Used for Jamf Pro SMTP
Edit

Owners
Keith Mitnick
Edit

Members
Jamf Alerts
Edit

Settings
Email: jamfsmtp@managedaccount.org
Communication: Disabled
Require owner approval to join the group: Yes

Back **Create group**   Cancel

22.Click Close.

23.Confirm the group is shown in the list.

24.Open the Entra_Registration_Info and enter the name of your Group Email address as shown in the previous step. This guide will use jamfsmtp@managedaccount.org. Save the document but keep it open. We will need this info later on in the guide.

This completes this section. In the next section, we will install PowerShell for Mac and create a service principal to provide application specific identity.

Section 3: Creating a service principal using PowerShell

What You'll Need:
Learn what hardware, software, and information you'll need to complete the tutorials in this section.

Hardware and Software:
Requirements for following along with this section:
- PowerShell for Mac: Version 7.4 or later installed.
- PowerShell Exchange Module: Installed and configured.

Download Link:
PowerShell for Mac: Installing PowerShell on macOS (Version 7.4)

https://learn.microsoft.com/en-us/powershell/scripting/install/installing-powershell-on-macos?view=powershell-7.4

In this section we will create a service principal using PowerShell. This a security identity used by applications, automated tools, or services to access resources within an Microsoft Entra tenant. It functions like a user identity, but it is specifically designed for enabling secure access to resources with specific permissions.

1. Install PowerShell for Mac and follow all the default prompts.

powershell-7.4.6-
osx-arm64.pkg

2. If you're presented with this screen, following the instructions in the link below to install PowerShell for Mac.

   https://support.apple.com/guide/mac-help/apple-cant-check-app-for-malicious-software-mchleab3a043/mac
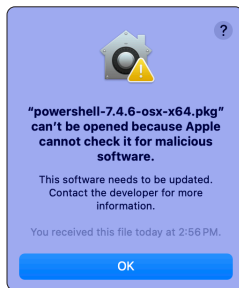
3. If you're presented with this screen, click Install and follow the default prompts to install PowerShell for Mac.

4. Open PowerShell for Mac located in the Applications folder.

PowerShell

5. To install the PowerShell Exchange Module, Run the command below and enter Y when prompted to install the module.

```
Install-Module -Name ExchangeOnlineManagement
```



```
Last login: Mon Jan  6 15:31:37 on ttys000
/usr/local/microsoft/powershell/7/pwsh ; exit;
keith@HCS ~ % /usr/local/microsoft/powershell/7/pwsh ; exit;
PowerShell 7.4.6
PS /Users/keith> Install-Module -Name ExchangeOnlineManagement

Untrusted repository
You are installing the modules from an untrusted repository. If you trust this
repository, change its InstallationPolicy value by running the Set-PSRepository
 cmdlet. Are you sure you want to install the modules from 'PSGallery'?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help
(default is "N"):Y
PS /Users/keith>
```
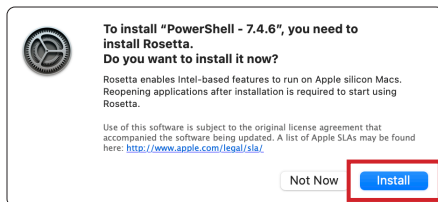
6. Run the command below:

```
Import-module ExchangeOnlineManagement
```

```
PS /Users/keith> Import-module ExchangeOnlineManagement
PS /Users/keith>
```

7. We need to create the variables for PowerShell. Open the Entra_Registration_Info document located on your Desktop and paste in the corresponding values between the single quotes in the sample code below. It should look similar to the picture below. Copy the filled in Sample code when done.

```
$Tenant='7dd8c                           f7';
$ClientId='7714                          41dc';
$ServicePrincipal='d084076               815786';
$EmailGroupId='jamfsmtp@managedaccount.org';
```

Sample Code:
```
$Tenant=' ';
$ClientId=' ';
$ServicePrincipal=' ';
$EmailGroupId=' ';
```

8. Paste the code into PowerShell to set the variables.
   NOTE: You can copy the entire block of the code from the previous step and paste it into PowerShell to set all the variables at once.

```
              $Tenant='7d                    f7';
PS /Users/work> $ClientId='771               ldc';
PS /Users/work> $ServicePrincipal='d084      786';
PS /Users/work> $EmailGroupId='jamfsmtp@managedaccount.org';
PS /Users/work>
```

9. Run the command below:

```
Connect-ExchangeOnline -Organization $Tenant
```

```
[PS /Users/keith> Connect-ExchangeOnline -Organization $Tenant
----------------------------------------------------------------------
This V3 EXO PowerShell module contains new REST API backed Exchange Online cmdlets which doesn't require WinRM for Client-Server communication
. You can now run these cmdlets after turning off WinRM Basic Auth in your client machine thus making it more secure.

Unlike the EXO* prefixed cmdlets, the cmdlets in this module support full functional parity with the RPS (V1) cmdlets.

V3 cmdlets in the downloaded module are resilient to transient failures, handling retries and throttling errors inherently.

REST backed EOP and SCC cmdlets are also available in the V3 module. Similar to EXO, the cmdlets can be run without WinRM basic auth enabled.

For more information check https://aka.ms/exov3-module

Starting with EXO V3.7, use the LoadCmdletHelp parameter alongside Connect-ExchangeOnline to access the Get-Help cmdlet, as it will not loaded
 by default.
----------------------------------------------------------------------
PS /Users/keith>
```
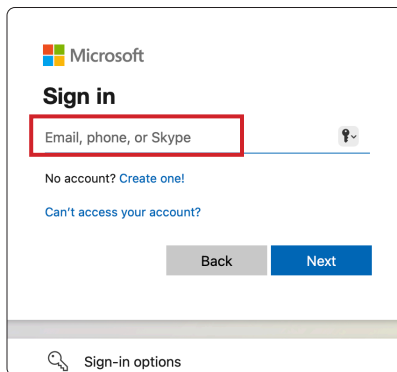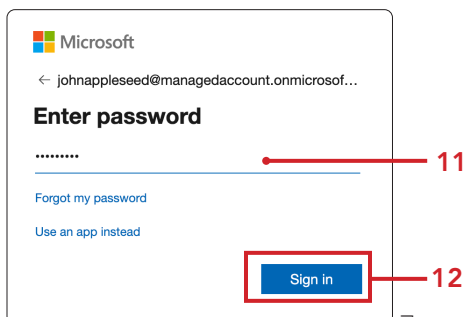
10. When prompted, enter the credentials of an Exchange account with administrative privileges.

Microsoft
Sign in

Email, phone, or Skype

No account? Create one!

Can't access your account?

Back   Next

Sign-in options

11. Enter your password.

12. Click Sign in.

Microsoft

← johnappleseed@managedaccount.onmicrosof…
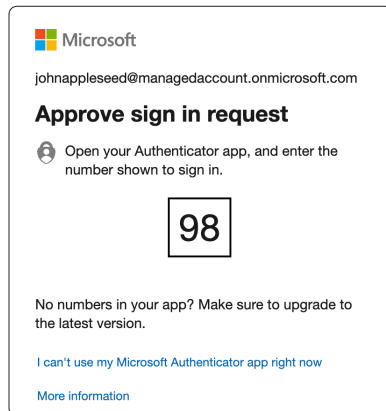
Enter password

••••••••• — 11

Forgot my password
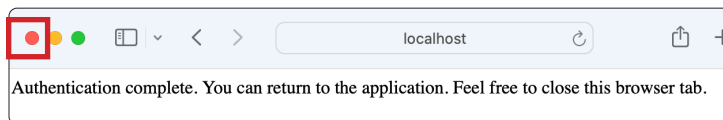
Use an app instead

Sign in — 12

13. If you're using Multi Factor Authentication , approve your sign in request.

14. Close your web browser when you see the message below.

15. In PowerShell, run the command below to make sure Enable-OrganizationCustomization setting is enabled in the Microsoft Entra tenant.

Get-OrganizationConfig | fl Identity, IsDehydrated

NOTE: A response of False means it's configured correctly. If you get a response of True, then it's disabled. Run this command to enable it.

Enable-OrganizationCustomization

```
PS /Users/keith> Get-OrganizationConfig | fl Identity, IsDehydrated

Identity      : ManagedAccount.onmicrosoft.com
IsDehydrated : False

PS /Users/keith>
```

16. Run the command below to create a new service principal.

New-ServicePrincipal -AppId $ClientId -ObjectId $ServicePrincipal -DisplayName "Service Principal"

```
                                        keith — pwsh — 179×38
PS /Users/keith>  New-ServicePrincipal -AppId $ClientId -ObjectId $ServicePrincipal -DisplayName "Service Principal"

DisplayName                         ObjectId                              AppId
-----------                         --------                              -----
Service Principal                   d08              786                  771            41dc

PS /Users/keith>
```

17. Run the command below to create a role to send mail for mail-enabled security groups.

New-ManagementRoleAssignment -App $ClientId -Role "Application Mail.Send" -RecipientGroupScope $EmailGroupId

```
                                        keith — pwsh — 179×38
PS /Users/keith> New-ManagementRoleAssignment -App $ClientId -Role "Application Mail.Send" -RecipientGroupScope $EmailGroupId

Name                            Role                    RoleAssigneeName        RoleAssigneeType        AssignmentMethod        EffectiveUserName
----                            ----                    ---------------         ----------------        ----------------        -----------------
Application Mail.Send-d084076…   Application Mail.Send    d084           47…     ServicePrincipal        Direct

PS /Users/keith>
```

This completes this section. In the next section, we will configure the SMTP settings on the Jamf Pro server.

Section 4: Configuring SMTP server settings in Jamf Pro

What You'll Need:
Learn what hardware, software, and information you'll need to complete the tutorials in this section.

Hardware and Software:
Requirements for following along with this section:
- A Jamf Pro server with administrative privileges

*Access to an email account

In this section we will configure the Jamf Pro server to use Microsoft Graph API for SMTP.

1. Log into your Jamf pro server with administrative privileges.

2. Click Settings.

3. Enter smtp in the search field.

4. Click on SMTP server.

5. Click Edit.

6. Open the Entra_Registration_Info document located on your Desktop.
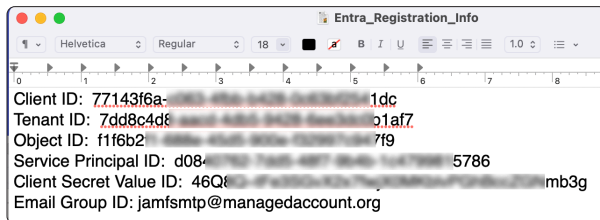
7. Switch back to the Jamf Pro server and configure the following:
    A. Enable SMTP
    B. Authentication Method: Microsoft Graph API
    C. Tenant ID: Enter the Tenant ID from the Entra_Registration_Info document
    D. Client ID: Enter the Client ID from the Entra_Registration_Info document
    E. Client Secret: Enter the Client Secret Value ID from the Entra_Registration_Info document.
    F. Sender email address: Enter the email address that you added as a member of the Mail-enabled security group in section two of this guide.
    G. Click Save.

8. On the bottom right, click Test.

9. Enter an email address that you have access to.

10. Click Test.

11. Confirm the email was sent successfully.

12. Confirm the email was delivered.

This completes the guide.