jamf PRO



Jamf Pro: Configure SMTP Server Integration with Microsoft 365 Per App Password



Contents

Preface	3
Section 1: Enable App Password in Azure AD	4
Section 2: Enable SMTP Authentication (SMTP AUTH) on User Account	8
Section 3: Create App Password for User Account	10
Section 4: Configure the SMTP Server Settings	15
Addendum	18

Preface

What is an App Password and what does it do?

An app password is a long, randomly generated password that you provide only once instead of your regular password when signing in to an app or device that doesn't support two-step verification. You only need to create an app password if you have two-step verification turned on and are using an app that doesn't support it.

For example, some older, non-browser apps like Office 2010 or earlier and Apple Mail before iOS 11 don't understand pauses or breaks in the authentication process. An Azure Active Directory Multi-Factor Authentication (Azure AD MFA) user who attempts to sign in to one of these older, non-browser apps, can't successfully authenticate. To use these applications in a secure way with Azure AD Multi-Factor Authentication enforced for user accounts, can use app passwords.

How do I know if I need an App Password?

After you turn on two-step verification or set up the Authenticator app, you may run into issues if you use apps or older devices that don't support two-step verification. If you have two-step verification turned on and an app isn't prompting you to enter a security code when you sign in, you may be able to sign in with an app password instead.

Is it on automatically?

App Password needs to be configured and enabled in Azure AD.

When you use app passwords, the following considerations apply:

- There's a limit of 40 app passwords per user.
- If you suspect that a user account is compromised and revoke / reset the account password, app passwords should also be updated. App passwords aren't automatically revoked when a user account password is revoked / reset. The user should delete existing app passwords and create new ones.
- Applications that cache passwords and use them in on-premises scenarios can fail because the app password isn't known outside the work or school account.
- After Azure AD Multi-Factor Authentication is enforced on a user's account, app passwords can be used with most non-browser clients. However, administrative actions can't be performed by using app passwords through non-browser applications. The actions can't be performed even when the user has an administrative account.
- To run PowerShell scripts, create a service account with a strong password and don't enforced the account for two-step verification.



Section 1: Enable App Password in Azure AD

Users can't create app passwords. To give users the ability to create app passwords, an admin needs to enable the app password feature. NOTE: The admin account has to have Global administrator or Privileged Authentication

administrator role assigned.

- 1. Sign in to the Azure portal. Enter the admin user name.
- 2. Click Next.

Microsoft Azure	
Microsoft Sign in to continue to Microsoft Azure Email, phone, or Skype No account? Create one! Can't access your account? Back Next	
Sign in with GitHub	

- 3. Enter the admin password.
- 4. Click Sign in.

Test Azure
Microsoft (- rgoon@hestechgroup.com Enter password



5. Open your Authenticator app on your device, i.e. iPhone or Android, and enter the number shown to sign in. Click Yes.



5. Click Azure Active Directory.





5. On the left-hand side bar, scroll down and click Security.



6. On the left-hand side bar, click Conditional Access.

Protect	
💺 Conditional Access	
Identity Protection	
Security Center	
ᡖ Verified ID	

7. On the left-hand side bar, click Named location.



8. Click Configure multifactor authentication trusted IPs.

+ Countries location +	IP ranges location Of Configu	re multifactor authe	ed named locations list experience	resh	atures 🛛 🖗 Got feedb	oack?
Named locations are used by A	Azure AD security reports to redu	ce false positives an	d by Azure AD Conditional Acc	ess policies. Named Loca	tions that are marked Trus	ted or configure
Search by name			Location type: All types	Trusted type: All types	₩ Reset filters	
Name No results.	Location type	Trusted	Conditional Access policies	5		



9. On the multi-factor authentication page, select the radio button for Allow users to create app passwords to sign in to non-browser apps option.

10. Click Save.

	Microsoft hcstechgroup.com	?
	multi-factor authentication users service settings	
	app passwords (learn more)	
9 —	Allow users to create app passwords to sign in to non-browser apps to not allow users to create app passwords to sign in to non-browser apps	
	trusted ips (learn more)	
	Skip multi-factor authentication for requests from federated users on my intranet	
	Skip multi-factor authentication for requests from following range of IP address subnets	
	192. 192. 192.	
	verification options (learn more)	
	Methods available to users: Image: Call to phone Image: Text message to phone Notification through mobile app Image: Verification code from mobile app or hardware token	
	remember multi-factor authentication on trusted device (learn more)	
	 Allow users to remember multi-factor authentication on devices they trust (between one to 365 days) Number of days users can trust devices for 90 NOTE: For the optimal user experience, we recommend using Conditional Access sign-in frequency to extend session lifetimes on trusted devices, locations, or low-risk sessions as an alternative to 'Remember MFA on a trusted device', be sure to extend the duration to 90 or more days. Learn more about reauthentication prompts. 	
10—	save	
	Manage advanced settings and view reports Go to the portal	



Section 2: Enable SMTP Authentication (SMTP AUTH) on User Account

SMTP AUTH is set as per-mailbox for security. To enable this on a Mailbox, you have to have access to Microsoft 365 admin center.

- 1. Open the Microsoft 365 admin center. https://admin.microsoft.com/Adminportal/Home#/homepage
- 2. Click Users.
- 3. Click Active users.
- 4. Select a user.
- 5. Click Mail.
- 6. Click Manage email apps.

	III Microsoft 365 admin center		rch	E.	1 B O	۲	? 📿	
	=	Home > Active users					О×	
2 	 G Home A Users ▲ Artice surger 	Active users	Richard Goon	e user				
3	Contacts Guest users Deleted users	Recommended actions (1)	Change photo Account Devices Licenses and apps Mail OneDrive					— 5
	124 Teams & groups ✓	Display name †	Mailbox storage			6.053MB/5		
	少 Setup	Craig Cohen	Learn more about mailbox storage quotas Mailbox permissions E Read and manage comprisions C	imail apps				
	··· Show all	HCS Admin Joan Work	Send as permissions (0) Send on behalf of permissions (0)	Manage email apps				<u> </u>
		John Appleseed John Filardo	Show in global address list E Yes N Manage global address list visibility N	mail forwarding None Manage email forwarding				
4—		 Keith Mitnick Richard Goon 	Automatic replies N Off C Manage automatic replies E	More actions Convert to shared mailbox Edit Exchange properties				
		Sam Valencia						

7. Select the checkbox for Authenticated SMTP

::: Microsoft 365 admin center	P s	earch	ß	φ	۲	? (()
≡						×
යි Home	Active users	Manage email apps				
A Users ^						
Active users	Decomposed of entire (1)	Choose the apps where Richard Goon can access Microsoft 365 email.				
Contacts	Recommended actions (1)	✓ Outlook on the web				
Deleted users		🗹 Outlook desktop (MAPI)				
⁴ x ^A Teams & groups ✓	🐥 Add a user 🛛 💾 Multi-factor authe	Z Exchange web services				
🗂 Marketplace	Display name 1	Mobile (Exchange ActiveSync)				
🗖 Billing 🗸 🗸		имар				
A Setup		Pop				
be beap	Craig Cohen	Luthenticated SMTP				
··· Show all						
	John Appleseed					



8. Click Save Changes.





Section 3: Create App Password for User Account

After app password and SMTP AUTH has been enabled for the users, each user may create an app password in their account.

- 1. If necessary, sign into: https://microsoft365.com/login
- 2. Enter your user name.

••• • 🗖 📑 Sign in to your account	x +	
← C	com/common/oauth2/v2.0/authorize?client_id=4765445b-3 A 않 û 다 않 🔞 😵 💽 …	b
		Q
		0
		•
		+
	Microsoft	
	Sign in	
	rgoon@hcstechgroup.com	
	No account? Create one!	
	Can't access your account?	
	Back Next	
	Q. Sim-in ontions	
	2 alar mahaana	
		-
	Terms of use Privacy & cookies	252

- 3. Enter your password.
- 4. Click Sign in.





5. Open your Authenticator app on your device, i.e. iPhone or Android, and enter the number shown to sign in. Click Yes.



- 3. On the top right-hand, click on your account.
- 4. Click View account.





5. On the sidebar, click Security info.



6. Click Add sign-in method.

🗧 🔍 🗖 📋 🖏 Home M	vlicrosoft 365 x 📑 My Sign-Ins Security Info Mi x +								
← C 🗘 https://my	signins.microsoft.com/security-info	٨	CD	₹⁄≡	¢	~~			b
\cdots My Sign-Ins \vee						8	?	RG	Q,
									0
A Overview	Security info								0
$\mathcal{P}_{\! I\!\! I}$ Security info	These are the methods you use to sign into your account or reset your password.								+
Crganizations	+ Add sign-in method								
💻 Devices	Microsoft Authenticator Buch multi-factor authentication (AEA) iPhone 14 Pro				Delete				
A Privacy	Lost device? Sign out everywhere								

7. From the menu, select App password.





8. Click Add.



9. Enter a name for the app password. In this example, we named it Jamf Pro.
 10. Click Next.





- 11. Confirm a password has been generated. Copy the password. NOTE: Password will be shown once only. If You lose the password, there is no resetting it. You must delete it from your account and create a new app password.
- 12. Click Done.





Section 4: Configure the SMTP Server Settings

For this exercise, we will configure SMTP for Jamf Pro.

1. Log in to your Jamf Pro Server.



- 2. On the top-right corner, click Settings (🐯).
- 3. Click System.
- 4. Click SMTP Server.

	ଅ jamf PRO		Ø	Discover Trusted Access 🗕 🖉 🙋	2
	Computers Devices Users	Settings			
3—	VERSION 1043-0410902200199 MANAGED Computers: 64 Mobile Devices: 6	Search All System Global Jamf Apps Self Servic	e Server Network Computer management	Display icons	rm
	UNMANAGED Computers: 1 Mobile Devices: 0	User accounts and groups Set Jamf Pro user privileges, Directory Service accounts, and password policies	Single Sign-On Set SSO for Jamf Pro, macOS Self Service, and user-initiated enrollment	LDAP servers Configure, manage, and test settings for LDAP servers	
		Cloud Identity Providers Configure and manage Google or Azure AD cloud identity providers	SMTP server Integrate a server to allow Jamf Pro to send emails and invitations	Activation code Update the activation code or organization name and view licensing	4
	Collapse Menu	Change management Track the changes that happen in Jamf Pro and view log files	Maintenance pages Customize messages displayed to users when Jamf Pro is unavailable	Engage Display dynamic tips, highlights, and important notices in the interface	



5. Enter the following:

- A. Server: smtp-mail.outlook.com
- B. Port: 587
- C. Encryption: **TLSv1.2** D. Sender Display Name: **Jamf Pro Server**
- ${\sf E. Sender Email Address: your Microsoft account, i.e.} \ rgoon@hcstechgroup.com$
- F. Username: your Microsoft account, i.e. **rgoon@hcstechgroup.com**
- G. Password: Copied from previous section, paste in to field.
- H. Verify : Copied from previous section, paste in to field.

I. Click Save.

In	legrate with an SMTP server to use for email communications
5	erver And Port Hostname or IP address, and port number of the SMTP server
-[smtp-mail.outlook.com
	Personal and the test for data assessments
9	connection Timeout Amount of time to wait before canceling an attempt to connect to the SMTP server
	5 Seconds
	ender Display Name Sender name to display in email messages sent from Jamf Pro
	Jami Pro Server
5	iender Email Address SMTP account email address that Jamf Pro will send emails from
	rgoon@hcstechgroup.com
	Requires Authentication SMTP server requires authentication using credentials for an SMTP account.
	Username
	rgoon@hcstechgroup.com
	Password
	Letter Browned
	Verity Password

6. Click Test.

Settings : System					
← SMTP server					
Enable SMTP Server Integrate with an SMTP server to use for email communications					
Server And Port Hostname or IP address, and port number of the SMTP server					
smtp-mail.outlook.com	. 587				
Encryption Protocol to use for data encryption					
TLSVI.2 💌					
Connection Timeout Amount of time to wait before canceling an attempt to connect to the SMTP server					
5 Seconds					
Sender Display Name Sender name to display in email messages sent from Jamf Pro					
Jamf Pro Server Filardo					
Sender Email Address SMTP account email address that Jamf Pro will send emails from					
Requires Authentication					
SMTP server requires authentication using credentials for an SMTP account					
Username					
Password					
Verify Password					
	(1) History	⊘ Test	Edit		
	,	1000			



- 7. Enter your email address.
 8. Click Test.

		Settings : System > SMTP server ← Test
		Test SMTP Server Test your SMTP server settings by sending a test email to the address below Recipient
7—	-	irgoon@hcsonline.com
8 —		Test

9. Confirm the message was sent out successfully.

← Test	rstem → SMTP ser	ver							
Test SMTP	Server Test your	SMTP server se	tings by sending	a test email to	the address	below			
rgoon@hcson	line.com								
Test									
Ch	A test message wa	as successfully	sent.						

10. Go to your email and confirm you received the test message from your Jamf Pro server. NOTE: Make sure to check your Junk folder.

Jamf Pro: Test message



Today at 11:49 AM o Jamf Pro Server <rgoon@hcstechgroup.com> To: O Richard Goon

This is a test message from your Jamf Pro server.



Addendum

While producing this guide, we had an anomaly where App Password would not appear from the menu when we try to create an app password. Here are the steps to rectify the issue.

NOTE: It is important that the user sign out from their account from all sources. It also may take up to three to five minutes before App Password shows up in the menu.

- 1. Go to the MFA Administration Page using your global administrator account
- 2. Select the user in question and click Manage User Settings.



- 3. Select the following options:
 - Require selected users to provide contact methods again
 - Delete all existing app passwords generated by the selected users
- 4. Click Save

Manage user settings



4

5. In the Microsoft 365 Admin Portal, Select the user and sign out the user from all sessions.

cancel

	Microsoft 365 ad	dmin center	۷ 🗵	
=				
	Recommended a			
	Add a user	RN Rn	S Block sign-in ♀	Del€
	Display na	Manage username	View last 30 days	
	adm wo	Sign-out ()	Alternate email address	
	Live Adr	Sign this user out of all Office 365 sessions.	None provided Add address	
	🗢 Rn	Sign out of all sessions	2	
		CHOLUDA	La la a	



6. Ask the user to sign in again. If this does not work, go to MFA Administration Page, select the user and click Enforce.

Enabled	rn@us99.onmicrosoft.com		
Disabled	quick steps		
Enforced	Disable Enforce		
Disabled	Manage user settings		

7. Have the user sign out and sign in again.