



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


Rev20230913

# Contents

## 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.

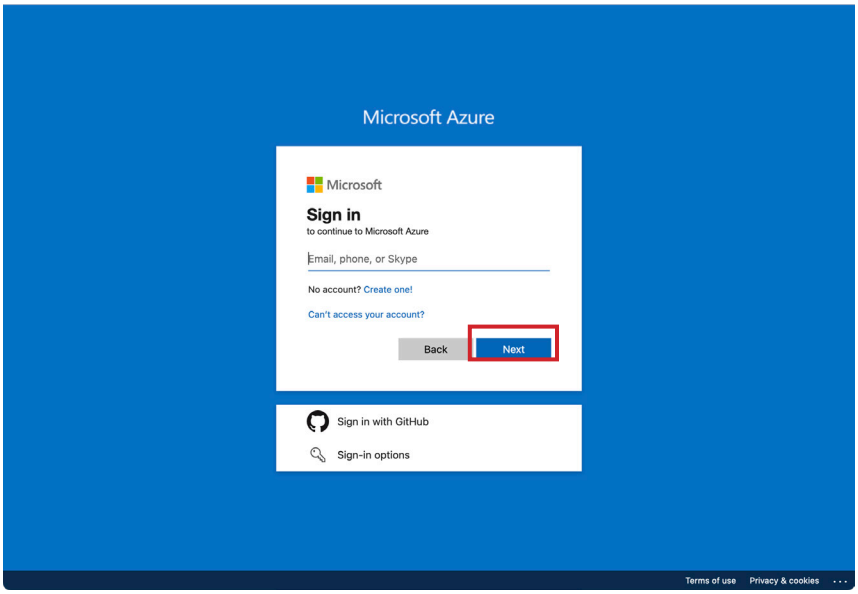
When you use app passwords, the following considerations apply:

- 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.

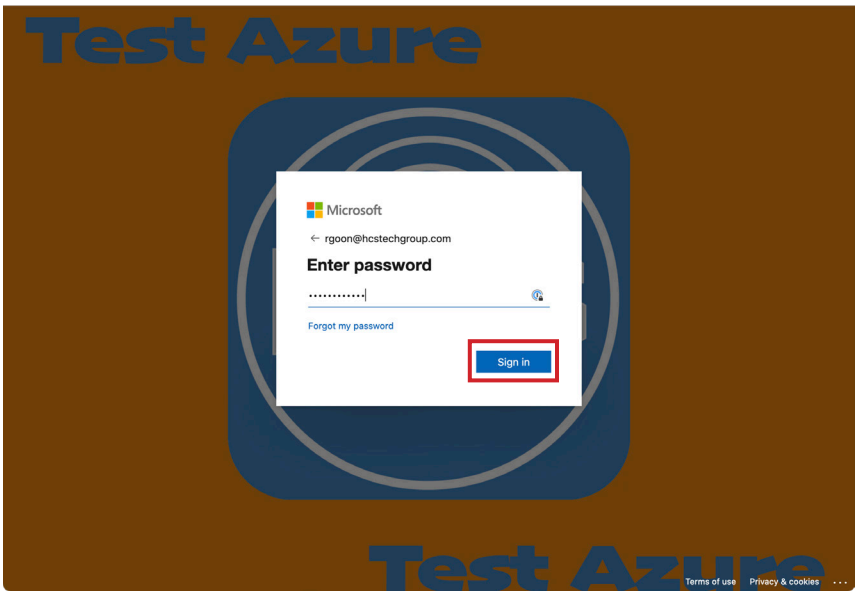
## Section 1: Enable App Password in Azure AD

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.

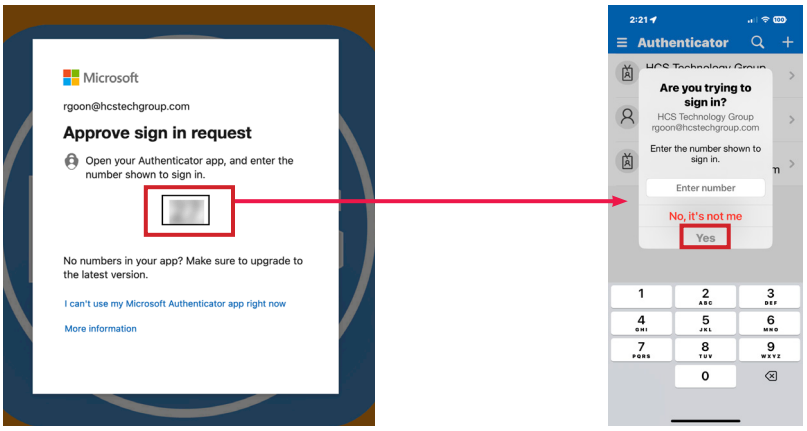
1. Sign in to the Azure portal. Enter the admin user name.
2. Click Next.



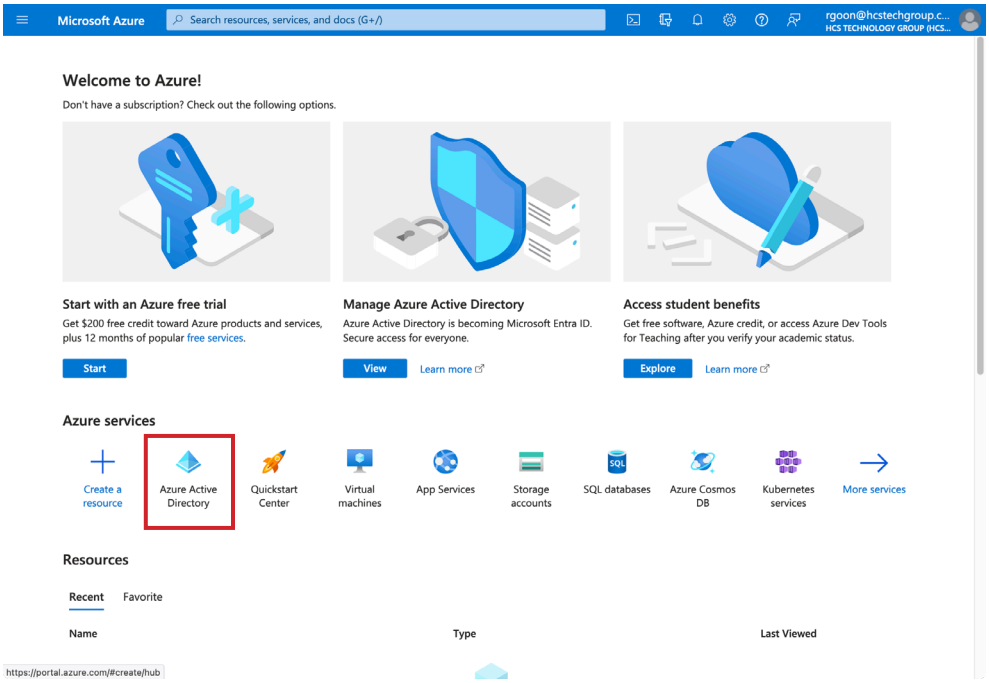

3. Enter the admin password.
4. Click Sign in.



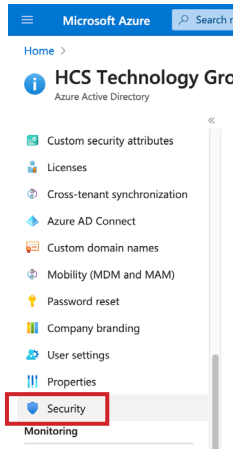
5. Open your Authenticator app on your device, i.e. iPhone or Android, and enter the number shown to sign in. Click Yes.



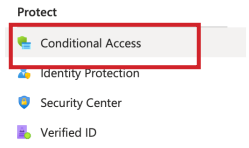

5. Click Azure Active Directory.



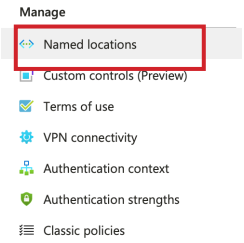
5. On the left-hand side bar, scroll down and click Security.



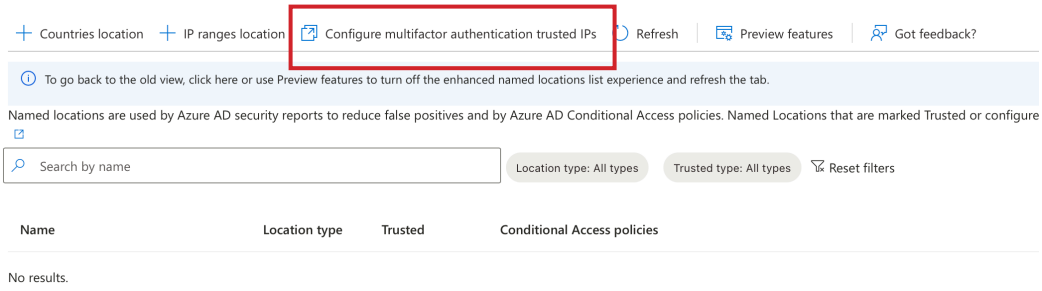

6. On the left-hand side bar, click Conditional Access.



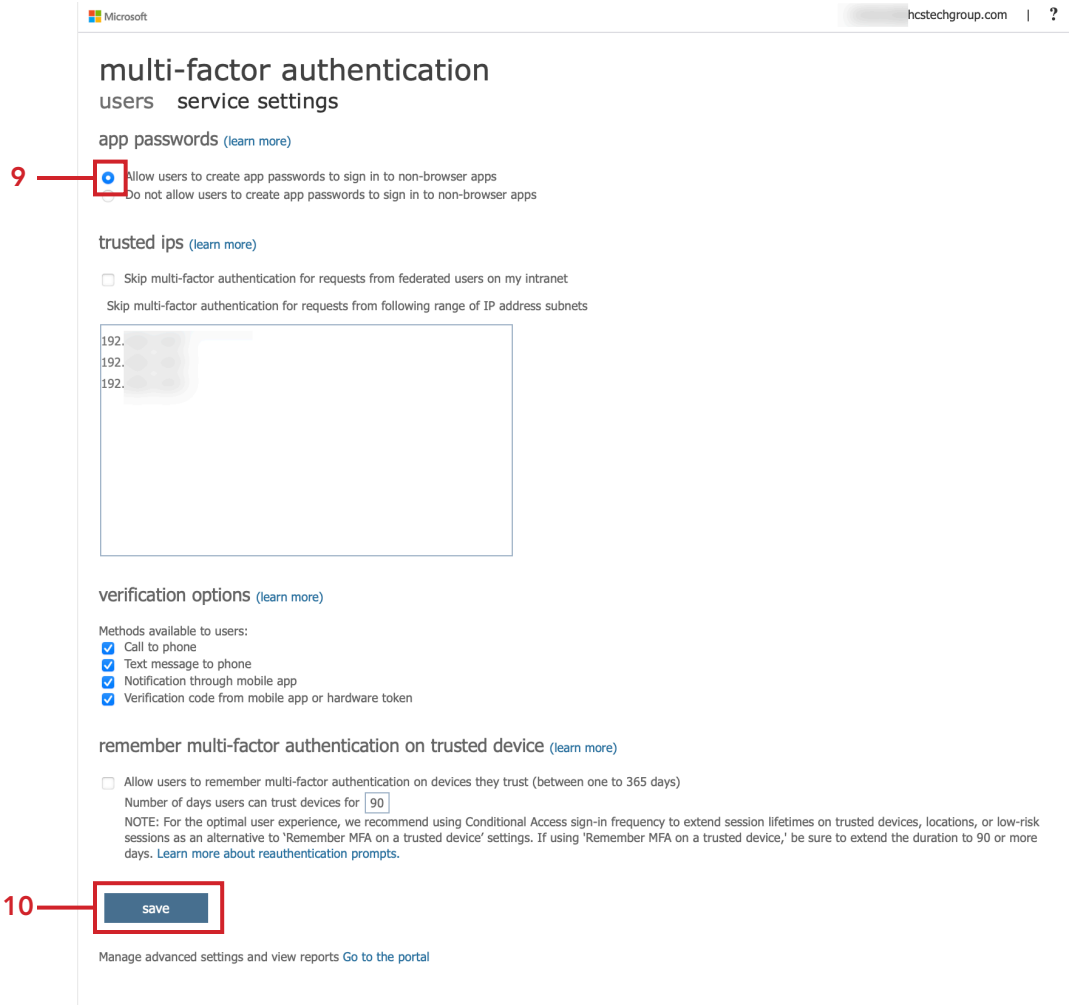

7. On the left-hand side bar, click Named location.




8. Click Configure multifactor authentication trusted IPs.



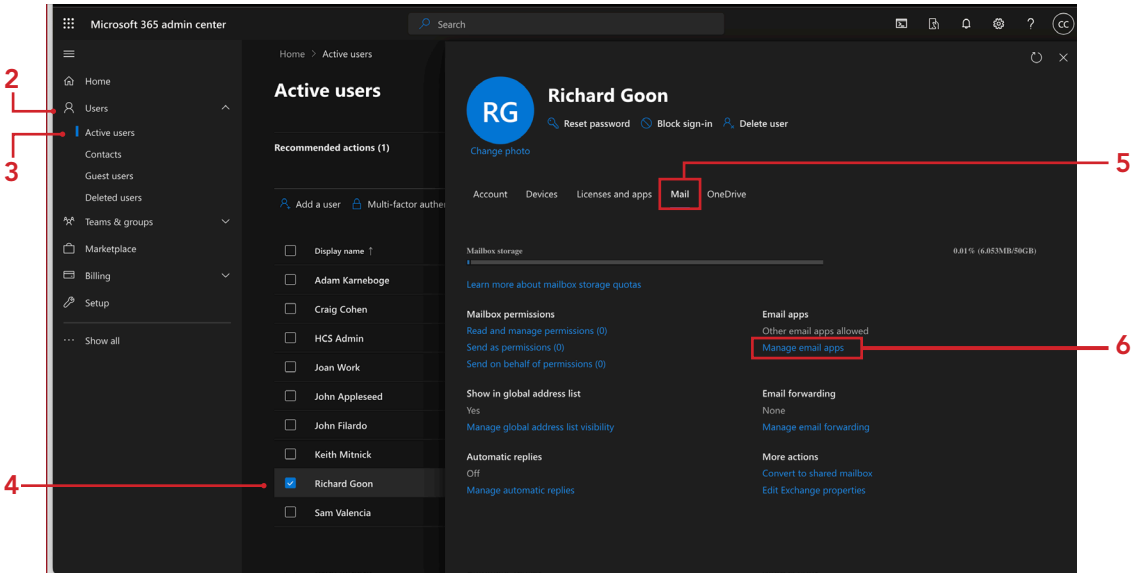
9. On the multi-factor authentication page, select the radio button for Allow users to create app passwords to sign in to non-browser apps option.
10. Click Save.



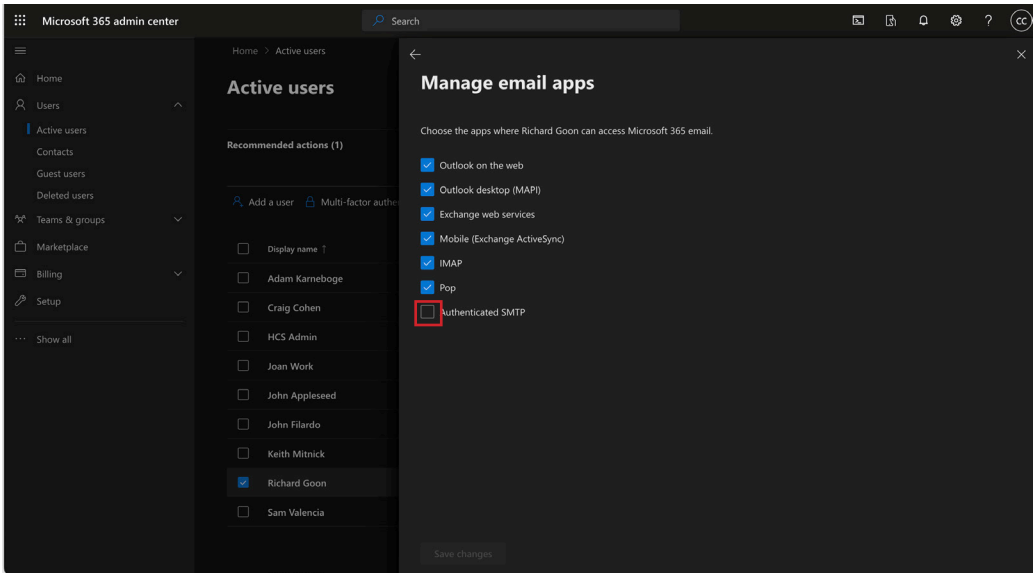
## Section 2: Enable SMTP Authentication (SMTP AUTH) on User Account

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.

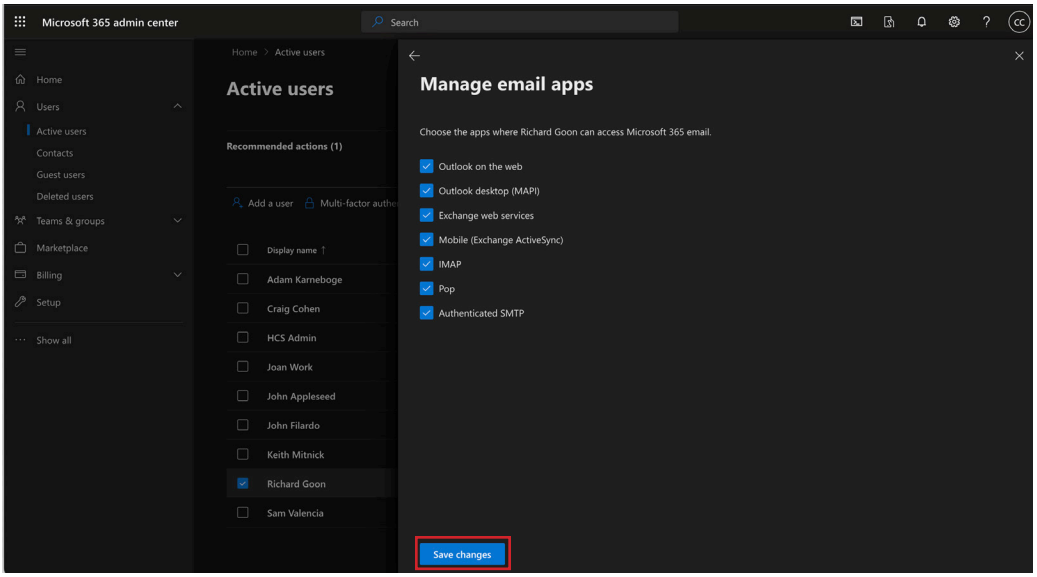
1. Open the Microsoft 365 admin center.
   https://admin.microsoft.com/Adminportal/Home#/homepage
2. Click Users.
3. Click Active users.
4. Select a user.
5. Click Mail.
6. Click Manage email apps.




7. Select the checkbox for Authenticated SMTP



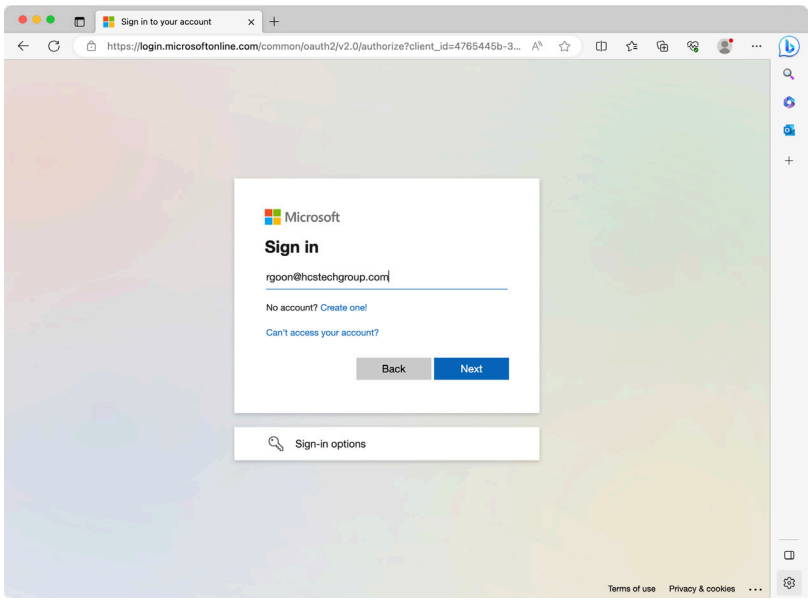
8. Click Save Changes.



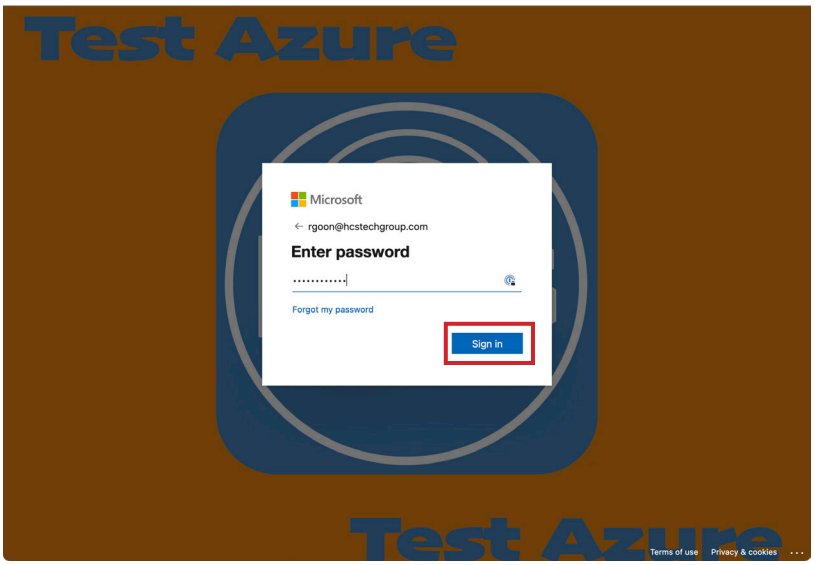
## Section 3: Create App Password for User Account

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

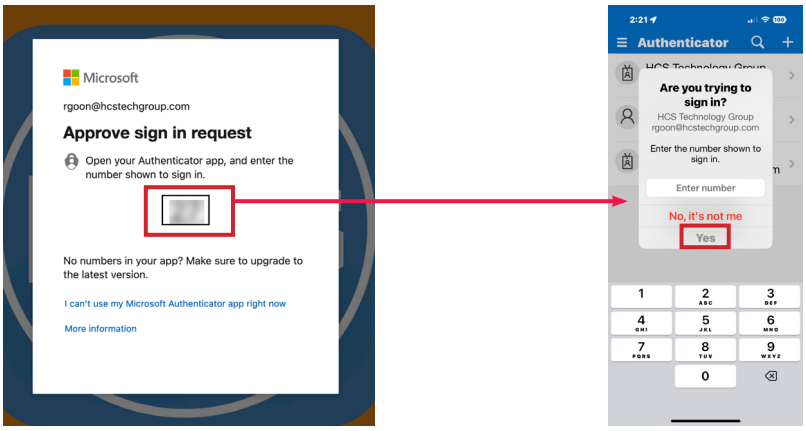
1. If necessary, sign into:
   https://microsoft365.com/login
2. Enter your user name.



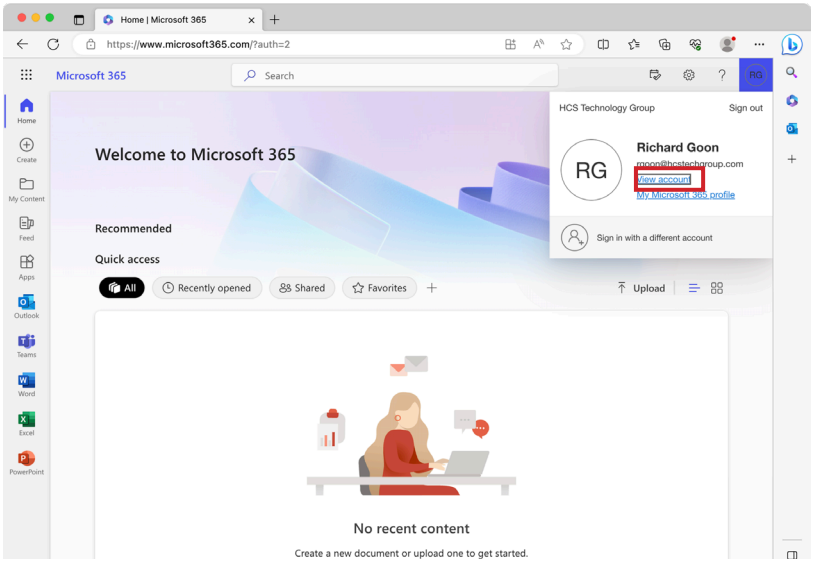

3. Enter your password.
4. Click Sign in.



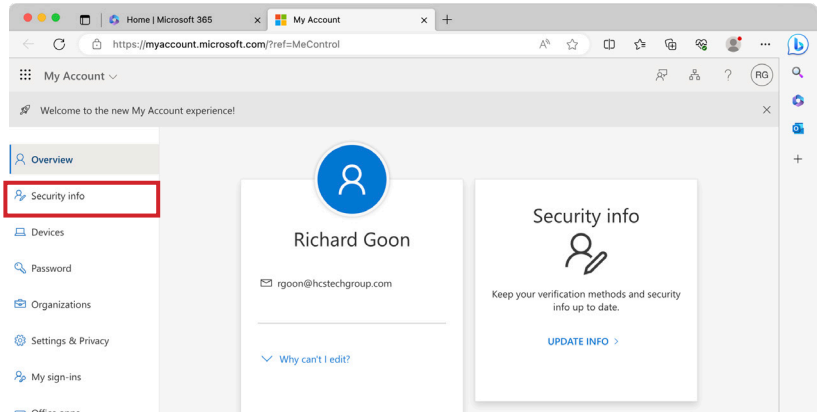
5. Open your Authenticator app on your device, i.e. iPhone or Android, and enter the number shown to sign in. Click Yes.



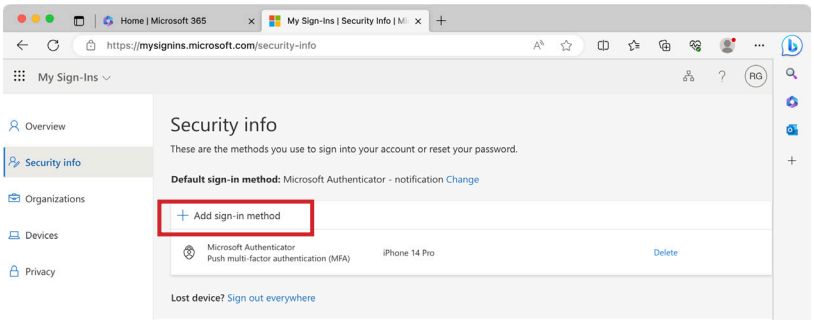

3. On the top right-hand, click on your account.
4. Click View account.



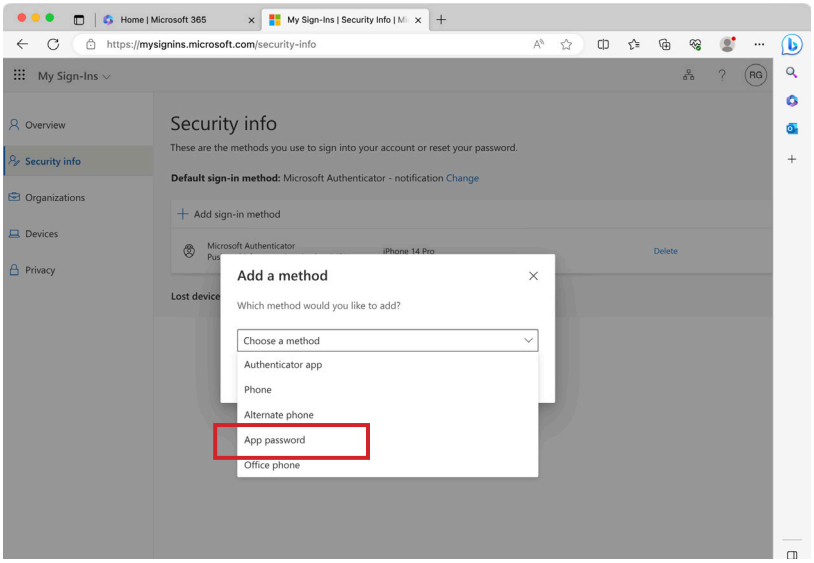
5. On the sidebar, click Security info.



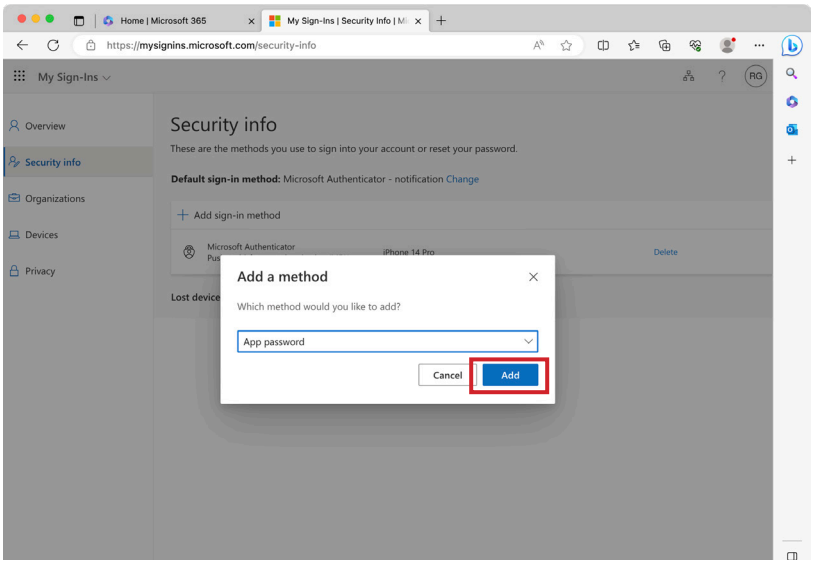

6. Click Add sign-in method.



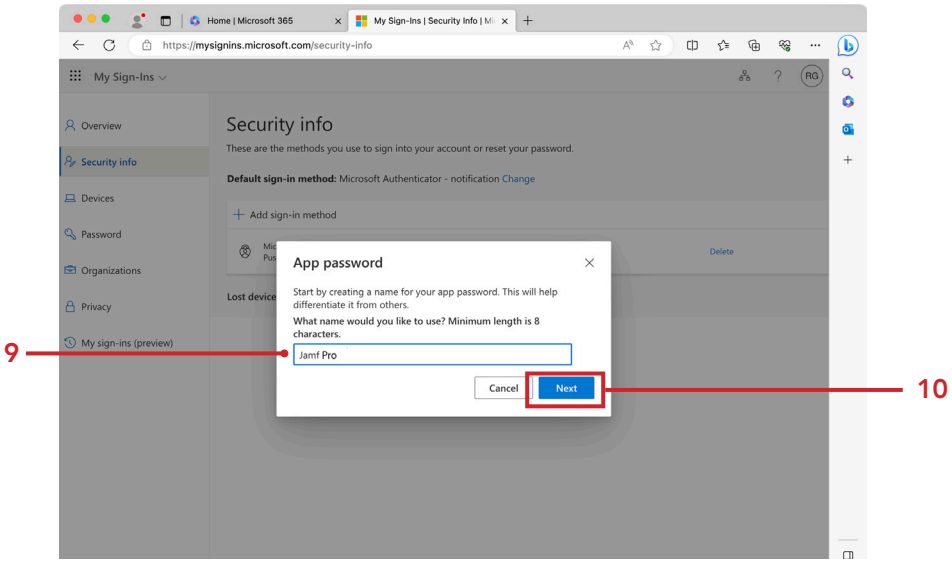

7. From the menu, select App password.



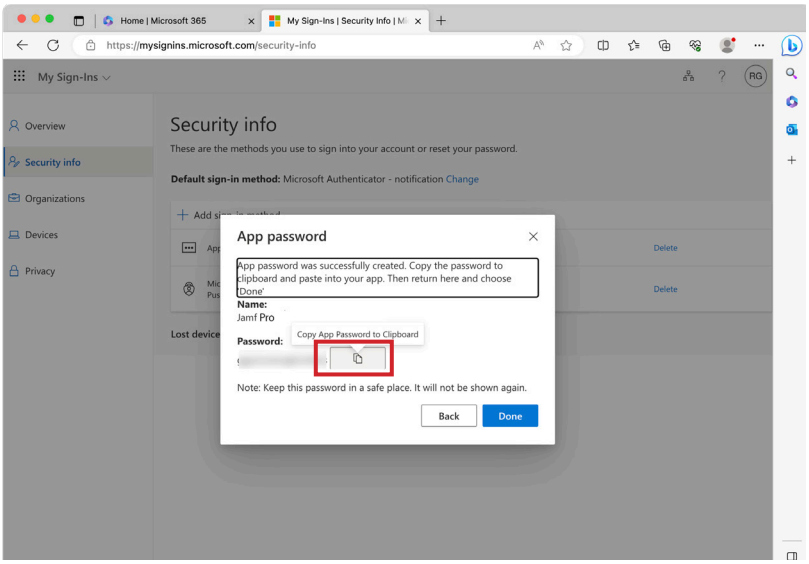
8. Click Add.




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.

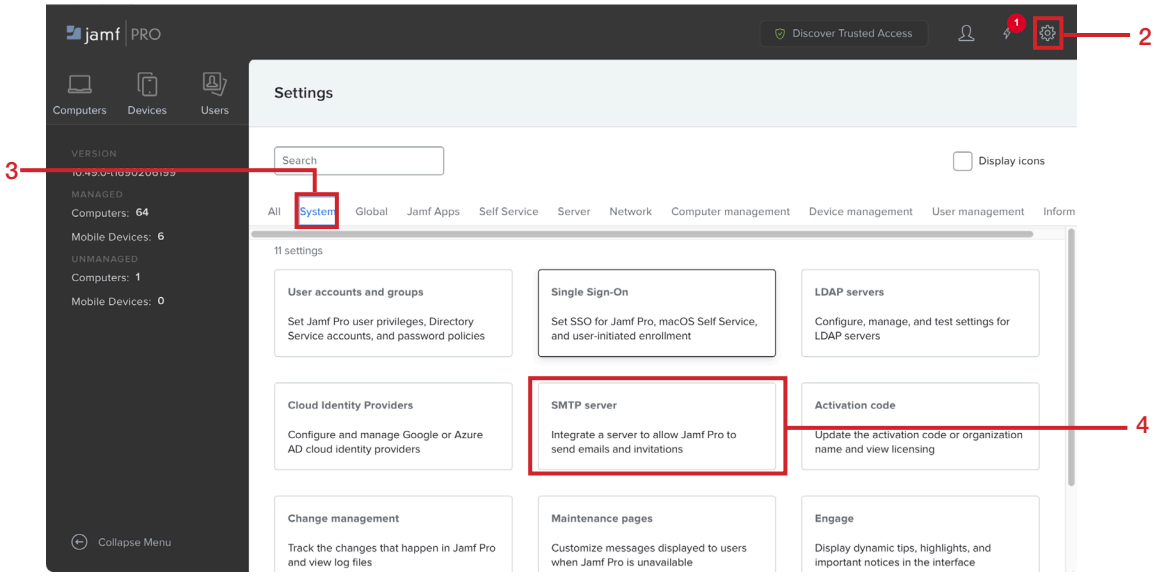


## Section 4: Configure the SMTP Server Settings

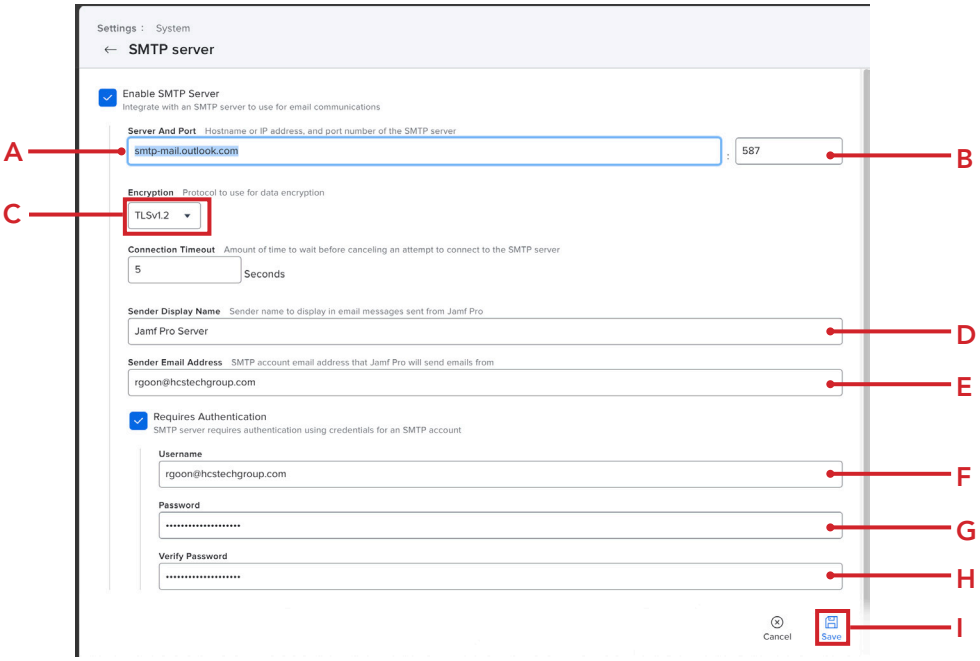
For this exercise, we will configure SMTP for Jamf Pro.

1. Log in to your Jamf Pro Server.

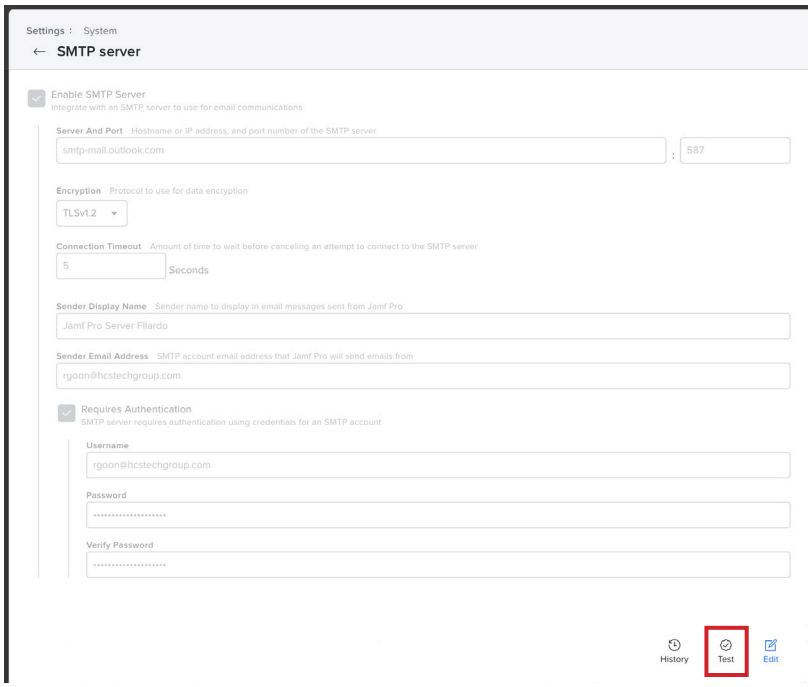

2. On the top-right corner, click Settings (⚙).
3. Click System.
4. Click SMTP Server.



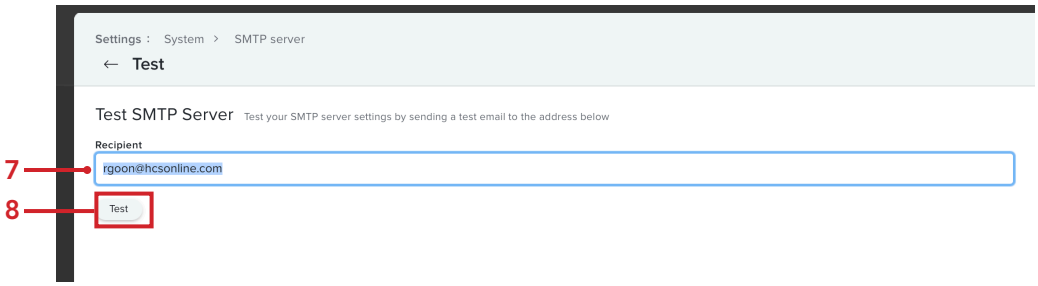
5. Enter the following:
   A. Server: **smtp-mail.outlook.com**
   B. Port: **587**
   C. Encryption: **TLSv1.2**
   D. Sender Display Name: **Jamf Pro Server**
   E. Sender Email Address: your Microsoft account, i.e. **rgoon@hcstechgroup.com**
   F. Username: your Microsoft account, i.e. **rgoon@hcstechgroup.com**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



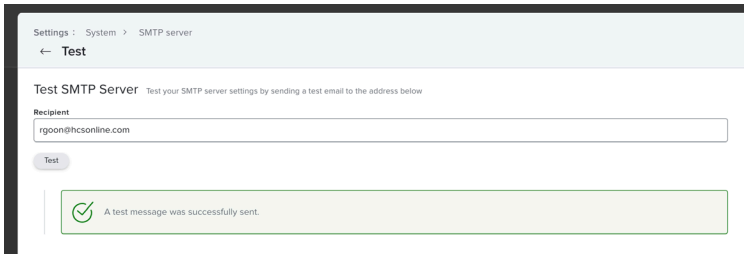

6. Click Test.



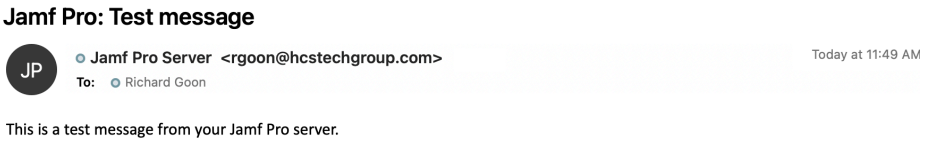
7. Enter your email address.
8. Click Test.




9. Confirm the message was sent out successfully.




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.

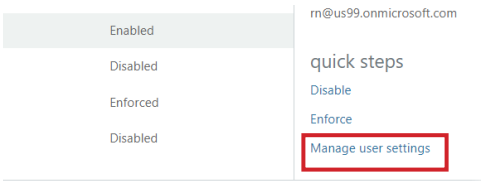


## Addendum

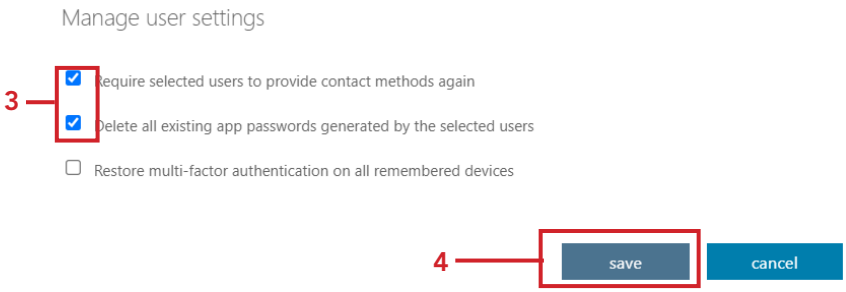
While producing this guide, we had an anomaly where App Password would not appear from the menu when we try to create an app password. Here are the steps to rectify the issue.

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.

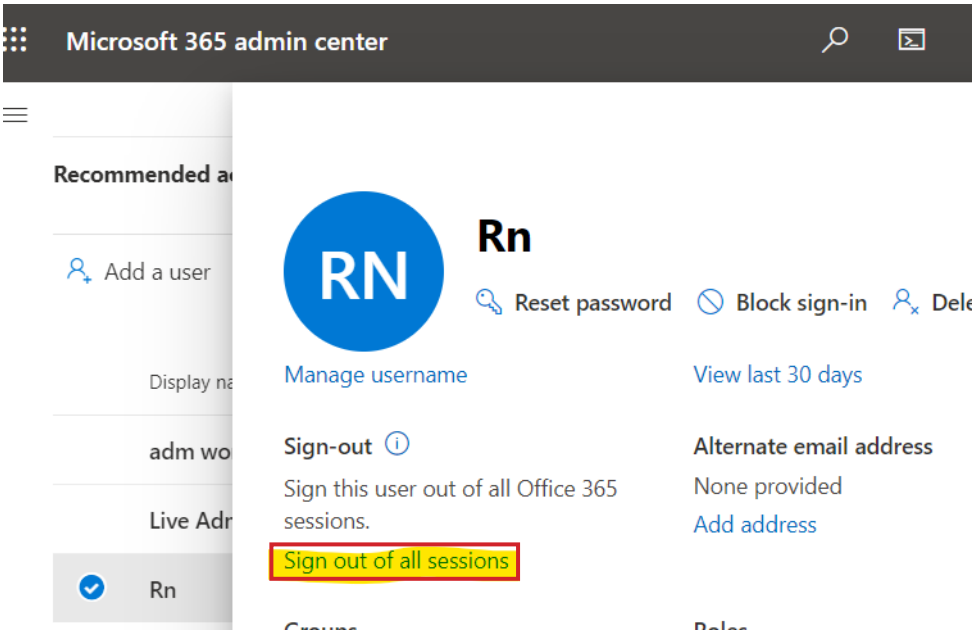
1. Go to the MFA Administration Page using your global administrator account
2. Select the user in question and click Manage User Settings.



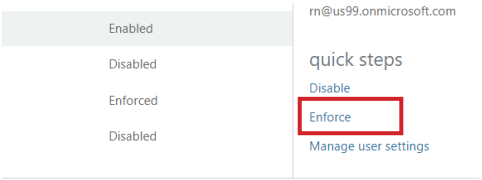

3. Select the following options:
   - Require selected users to provide contact methods again
   - Delete all existing app passwords generated by the selected users
4. Click Save




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



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




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