Configure Multi Factor Authentication (MFA) for Office 365

Last Modified on 23/01/2020 2:10 pm GMT

With Cloud Services such as Office 365 becoming more critical to the operation of many organisations, it is important to protect these services and the data held within them. Multi-Factor Authentication provides an additional layer of security protection when signing into your Office 365 accounts, requiring not just the password for the account, but also a second 'factor', commonly a code by text or a call to a trusted phone number.

Prerequisites

Licence Requirements

If you have Office 365 licences, you already have Multi-Factor Authentication (MFA) available for your Office 365 users.

Additional options for MFA are available through the Azure Active Directory Premium Plan 1 licence, including the ability to whitelist based on factors such as locations and the application being accessed.

Software Requirements

In order to honour Multi-Factor Authentication requests, you must ensure an application that utilises Microsoft's Modern Authentication platform. The supported applications include:

- Web Portal Applications
- Outlook 2013 and later*
- Outlook 2016 for Mac and later
- Mail for Mac OSX 10.14 (Mojave) and later
- Mail for iOS11 and later
- Outlook for Mobile
- Microsoft Teams
- Office 2016 and later
- OneDrive

- Office for Mobile

*Modern Authentication must be enabled in your Office 365 tenant. Outlook 2013 requires a registry key to be applied.

The full list of supported applications can be found on the Microsoft Docs portal.

If the application you are using is not a supported application, you will likely need to use an App Password to connect. The details and steps for these can be found later in the guide.

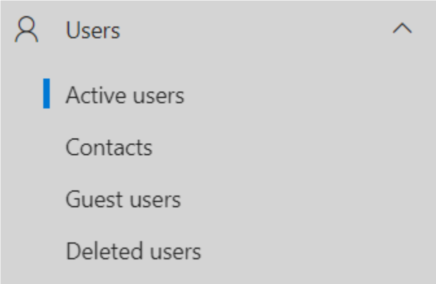
Enable MFA for Users

The accounts you use with Office 365 are managed through the Azure Active Directory service, which is where Multi-Factor Authentication must be applied. You can access this through the Microsoft 365 Admin Center.

You can apply MFA on a per-user basis with the standard licensing, which the below steps cover. With the Premium licences, you can apply this based on other criteria, such as location or device policies, which is not covered below, but can be found on the Microsoft Docs portal.

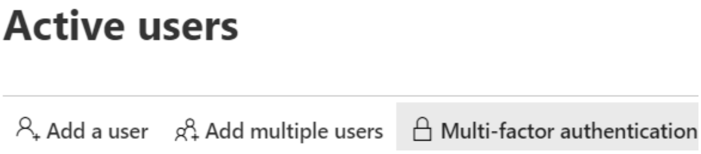
You must use an admin account with the **Global Administrator** role to change these settings.

1. Log into the Microsoft 365 Admin Center using global admin credentials for the tenant: https://admin.microsoft.com



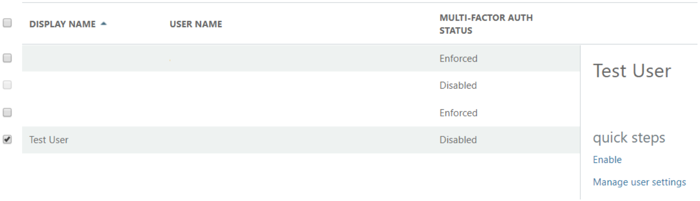
2. From the Left-Hand menu, select '**Users > Active Users**'

3. Select **Multi-factor authentication**



Active users

4. Select the User you want to Enable MFA for



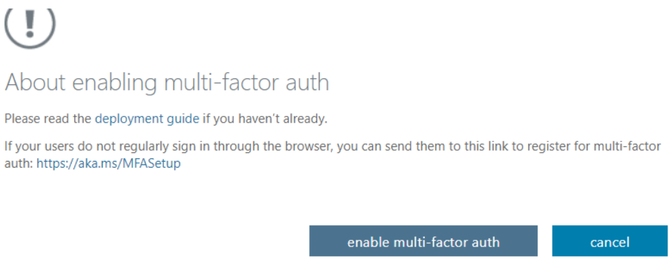
	DISPLAY NAME	USER NAME	MULTI-FACTOR AUTH STATUS
□			Enforced
□			Disabled
□			Enforced
☑	Test User		Disabled

Test User

quick steps

5. Select **Enable** on the right-hand panel

6. Confirm to **Enable Multi-Factor Auth**



About enabling multi-factor auth

Please read the deployment guide if you haven't already.

If your users do not regularly sign in through the browser, you can send them to this link to register for multi-factor auth: https://aka.ms/MFASetup

When the user next logs into the Office 365 portal, they will be prompted to set up their Multi-Factor Authentication options. Once set, the MFA status will change to enforced and apply for future logins. Users who do not commonly access through a web browser can be sent the following link to configure their settings: https://aka.ms/MFASetup.

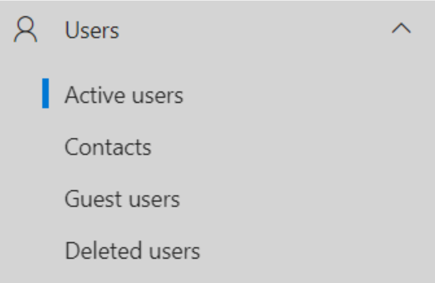
Change MFA Settings

At times, you may wish to prevent users from being able to use certain options for their additional factors or prevent users from using unsupported applications. In these cases, you will need to edit the Service Settings for Multi-Factor authentication.

If there is no requirement to allow unsupported (legacy) applications to connect to Office 365, it is recommended to disable App Passwords.

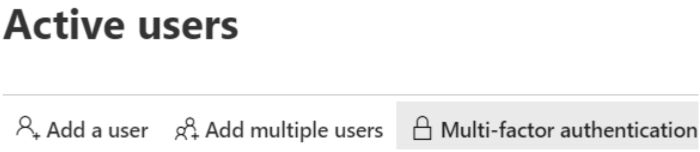
1. Log into the Microsoft 365

Admin Center using global admin credentials for the tenant: https://admin.microsoft.com

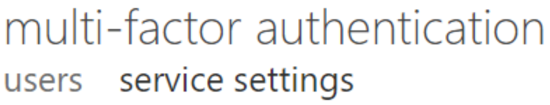


2. From the Left-Hand menu, select '**Users > Active Users**'

3. Select **Multi-factor authentication**

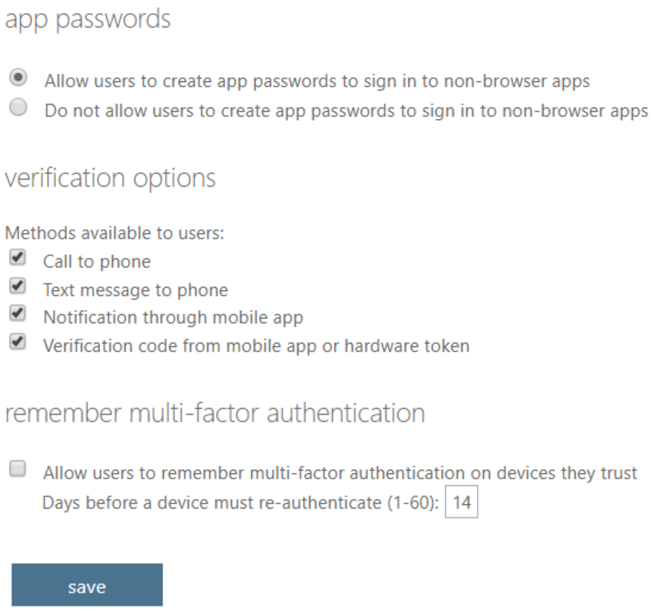


4. Select the **Service Settings** heading



5. Change the required settings

6. Press **Save**



app passwords

● Allow users to create app passwords to sign in to non-browser apps
○ Do not allow users to create app passwords to sign in to non-browser apps

verification options

Methods available to users:
☑ Call to phone
☑ Text message to phone
☑ Notification through mobile app
☑ Verification code from mobile app or hardware token

remember multi-factor authentication

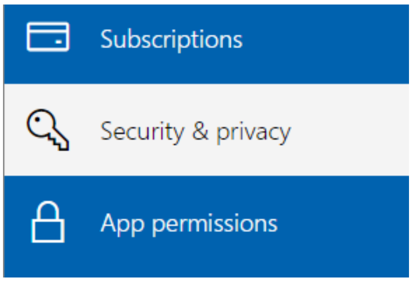
□ Allow users to remember multi-factor authentication on devices they trust
Days before a device must re-authenticate (1-60): 14

Legacy Applications

⚠ From October 13th 2020, Microsoft will be deprecating Basic Authentication for Exchange Online, which App Passwords rely on. This will prevent App Passwords from being accepted. This affects all connections to email services other than SMTP.

If your users use an application to access emails that does not support Microsoft's Modern Authentication platform, they will not be able to log in with their normal password, as it will not be able to handle the prompt for the additional factor. These applications are referred to as Legacy Applications. In order to access services using these applications, they will need to use an App Password in place of their normal password. App Passwords ignore the Multi-Factor Authentication requirement when signing in, but will only work for the Legacy Applications. The steps for the user are below;

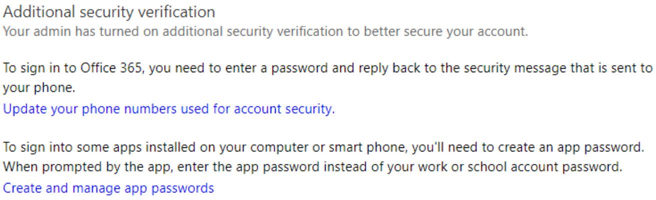
1. Sign in your Office 365 account at https://portal.office.com/account/



2. Select **Security & Privacy** from the left-hand menu

3. Select Additional Security Verification

4. Select Create and **Manage App Passwords**



Additional security verification
Your admin has turned on additional security verification to better secure your account.

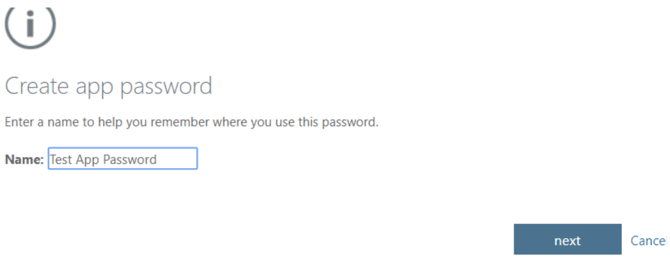
To sign in to Office 365, you need to enter a password and reply back to the security message that is sent to your phone.
Update your phone numbers used for account security.

To sign into some apps installed on your computer or smart phone, you'll need to create an app password. When prompted by the app, enter the app password instead of your work or school account password.
Create and manage app passwords

Note: This option will not appear if App Passwords have been disabled in the Service Settings

5. Select Create

6. Give the App Password a **Name**



Create app password

Enter a name to help you remember where you use this password.

Name: Test App Password

7. Copy the password shown into the Application you need to sign into

Once your App Password is generated, you will only be shown it once to copy out. Once the display has been closed, you will no longer be able to see that App Password and must create a new one if it was not recorded.

You should delete App Passwords that are no longer required.