Configure app passwords for Microsoft Entra multifactor authentication - Microsoft Entra ID

By Justinha

Archived: 2026-04-06 02:11:35 UTC

Enforce Microsoft Entra multifactor authentication with legacy applications using app passwords

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. A Microsoft Entra multifactor authentication (Microsoft Entra multifactor authentication) 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 Microsoft Entra multifactor authentication enforced for user accounts, you can use app passwords. These app passwords replaced your traditional password to allow an app to bypass multifactor authentication and work correctly.

Modern authentication is supported for the Microsoft Office 2013 clients and later. Office 2013 clients, including Outlook, support modern authentication protocols and can work with two-step verification. After Microsoft Entra multifactor authentication is enforced, app passwords aren't required for the client.

This article shows you how to use app passwords for legacy applications that don't support multifactor authentication prompts.

Note

App passwords don't work for accounts that are required to use modern authentication.

When a user account is enforced for Microsoft Entra multifactor authentication, the regular sign-in prompt is interrupted by a request for additional verification. Some older applications don't understand this break in the sign-in process, so authentication fails. To maintain user account security and leave Microsoft Entra multifactor authentication enforced, app passwords can be used instead of the user's regular username and password. When an app password is used during sign-in, there's no additional verification prompt, so authentication is successful.

App passwords are automatically generated, not specified by the user. This automatically generated password makes it harder for an attacker to guess, so is more secure. Users don't have to keep track of the passwords or enter them every time as app passwords are only entered once per application.

When you use app passwords, the following considerations apply:

- There's a limit of 40 app passwords per user.
- 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. An example of this scenario is Exchange emails

that are on-premises, but the archived mail is in the cloud. In this scenario, the same password doesn't work.

- After Microsoft Entra multifactor authentication is enforced on a user's account, app passwords can be used with most non-browser clients like Outlook and Microsoft Skype for Business. However, administrative actions can't be performed by using app passwords through non-browser applications, such as Windows PowerShell. 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.
- 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.
    - For more information, see Create and delete app passwords from the Additional security verification page.

Warning

App passwords don't work in hybrid environments where clients communicate with both on-premises and cloud auto-discover endpoints. Domain passwords are required to authenticate on-premises. App passwords are required to authenticate with the cloud.

App password names should reflect the device on which they're used. If you have a laptop that has non-browser applications like Outlook, Word, and Excel, create one app password named **Laptop** for these apps. Create another app password named **Desktop** for the same applications that run on your desktop computer.

It's recommended to create one app password per device, rather than one app password per application.

Microsoft Entra ID supports federation, or single sign-on (SSO), with on-premises Active Directory Domain Services (AD DS). If your organization is federated with Microsoft Entra ID and you're using Microsoft Entra multifactor authentication, the following app password considerations apply:

Note

The following points apply only to federated (SSO) customers.

- App passwords are verified by Microsoft Entra ID, and therefore, bypass federation. Federation is actively used only when setting up app passwords.
- The Identity Provider (IdP) is not contacted for federated (SSO) users, unlike the passive flow. The app passwords are stored in the work or school account. If a user leaves the company, the user's information flows to the work or school account by using **DirSync** in real time. The disable / deletion of the account can take up to three hours to synchronize, which can delay the disable / deletion of the app password in Microsoft Entra ID.
- On-premises client Access Control settings aren't honored by the app passwords feature.
- No on-premises authentication logging or auditing capability is available with the app passwords feature.

Some advanced architectures require a combination of credentials for multifactor authentication with clients. These credentials can include a work or school account username and passwords, and app passwords. The

requirements depend on how the authentication is performed. For clients that authenticate against an on-premises infrastructure, a work or school account username and password a required. For clients that authenticate against Microsoft Entra ID, an app password is required.

For example, suppose you have the following architecture:

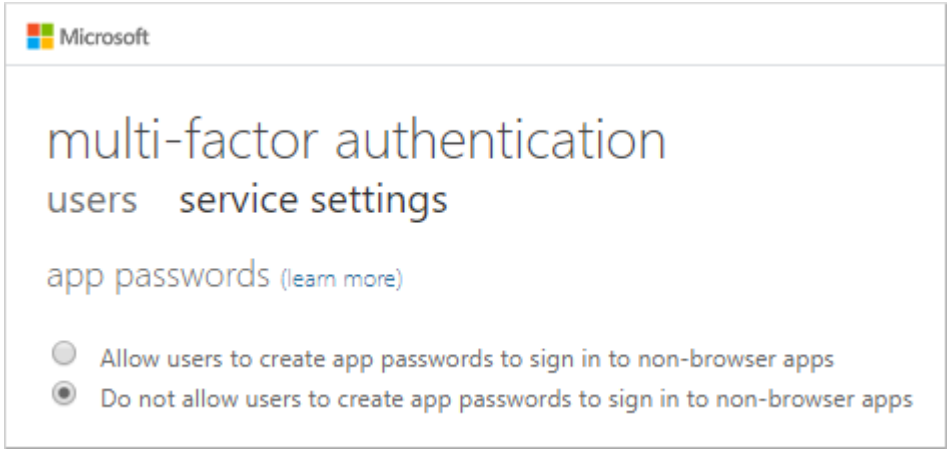
- Your on-premises instance of Active Directory is federated with Microsoft Entra ID.
- You use Exchange online.
- You use Skype for Business on-premises.
- You use Microsoft Entra multifactor authentication.

In this scenario, you use the following credentials:

- To sign in to Skype for Business, use your work or school account username and password.
- To access the address book from an Outlook client that connects to Exchange online, use an app password.

By default, users can't create app passwords. The app passwords feature must be enabled before users can use them. To give users the ability to create app passwords, **admin needs** to complete the following steps:

1. Sign in to the Microsoft Entra admin center as at least an Authentication Policy Administrator.
2. Browse to **Conditional Access** > **Named locations**.
3. Select **"Configure MFA trusted IPs"** in the bar across the top of the *Conditional Access | Named Locations* window.
4. On the **Multifactor authentication** page, select the **Allow users to create app passwords to sign in to non-browser apps** option.



Note

If App passwords are enabled, users will be required to create an app password as part of Microsoft Entra multifactor authentication registration.

When you disable the ability for users to create app passwords, existing app passwords continue to work. However, users can't manage or delete those existing app passwords once you disable this ability.

When you disable the ability to create app passwords, it's also recommended to create a Conditional Access policy to disable the use of legacy authentication. This approach prevents existing app passwords from working, and forces the use of modern authentication methods.

When users complete their initial registration for Microsoft Entra multifactor authentication, users will be asked to create an app password at the end of the registration process.

Users can also create app passwords after registration. For more information and detailed steps for your users, see the following resource:

- Create app passwords from the Security info page

- For more information on how to allow users to quickly register for Microsoft Entra multifactor authentication, see Combined security information registration overview.
- For more information about enabled and enforced user states for Microsoft Entra multifactor authentication, see Enable per-user Microsoft Entra multifactor authentication to secure sign-in events

---