DoDEA Information Technology ▶

Empowering DoDEA's global community through innovative, industry-leading technology services and solutions.

Microsoft 365: Second Factor Authentication

Pros & Cons

For Microsoft 365 access, DoD requires that you prove your identity in multiple ways – called factors. Every factor has pros and cons. The first factor DoDEA uses is password. However, passwords can be stolen, guessed or hacked. The second factor strengthens security to keep your access information and government data safe. The following can help you determine the best second factor for you. Some key considerations are mobility (the ability to sign in from anywhere), availability and if you need a silent option.

Data Connected Mobile Phone

OTP Voice Callback

SMS Text Message

- Easy to setup and use.
- High mobility with cell service.
- One-time password (OTP) security.

- May incur cost for calls &/or SMS text.
- Cannot be used if there is no cellular coverage or if the phone is off, lost or stolen.
- Callback may be loud or disruptive.

Android or Apple (iOS) Device with Authenticator App

Push

Mobile OTP

- Quiet & quick.
- High mobility.
- Does NOT use data plan.
- Does NOT require cell signal nor network connection.

- Must have device physically available for sign in and ensure device is protected otherwise.

Direct Dial Work Phone

Voice Callback

- Easy to setup.
- Does NOT require data nor cell signal.

- Low mobility unless IP Communicator is available on work laptop or phone is coupled with mobile phone forwarding.
- May be loud or disruptive.
- Only available for phone numbers that can receive direct calls from off base.

Hardware Token or Key

FIDO

Hardware Token

- High mobility.
- Quiet & quick.
- Does NOT use data plan.
- Does NOT require cell signal nor network connection.

- Must have token or key physically protected and available at all times.
- Not yet widely available – may delay access.
- You must track the expiration date of the token in order to request a replacement.
- Codes expire quickly - may cause lock out.
- May not work on some Android, iPhone, or newer MacBook without an adapter.

Your personal device can be used for the mobile phone and the authenticator app. For more information on multi-factor authentication (MFA) or to setup your Microsoft 365 MFA, visit the resources:

- About Non-CAC secure Access with MFA & Frequently Asked Questions (FAQ)
- M365 Account Setup using Authentication Phone
- If you do not have a phone that can receive calls directly nor a mobile device available, contact the Global Service Desk using the desktop icon on your government computer or enter an IT Service Request (ITSR) on the website.