Set-Up Mobile Devices for Email After (Multi-Factor Authentication) MFA Enrollment User Guide

Version: 1.0
Release Date: 8/14/2018
Table of Contents

Purpose of this User Guide ......................................................... 3
Tools and Terms ........................................................................ 3
  Multi-Factor Authentication (MFA) ........................................... 3
  App Passwords ...................................................................... 3
Managing App Passwords .......................................................... 4
  Things to Know about App Passwords .................................... 4
  Where to Manage App Passwords .......................................... 4
  Creating a New App Password ................................................ 5
Configuring an App Password in Outlook ............................... 6
Configuring an App Password on a Phone or Tablet .................. 7
Tips and Frequently Asked Questions ......................................... 8
  See the Video on Multi-Factor Authentication (MFA) ............. 8
  Official Microsoft Trouble Shooting Tips for MFA ............... 8
  Questions about this Document ............................................. 8
Purpose of this User Guide
The Dallas County Community College District (DCCCD) implementation of MFA (Multi-Factor Authentication) is implemented for non-student accounts only.

This guide is intended to aid and serve as a “how to” for all users to configure mobile devices to read DCCCD email after they enroll in MFA. To access email from a phone or computing device outside of the DCCCD Administrative network, other than via a web browser, you will need to configure an App Password.

Tools and Terms
Multi-Factor Authentication (MFA)
Multi-Factor Authentication (MFA), also known as 2-Step Authentication, is a Microsoft delivered feature which allows an enrolled user to better protect their account by requiring additional steps when signing in. By setting up multi-factor authentication, you add an extra layer of security to your Office 365 account. The first step is to sign in with your password and a code is automatically sent to your phone.

When you sign in from outside the DCCCD Administrative network or Secure Wireless Network, you will be prompted for a code or an authorization from the Microsoft Authenticator App.

It is strongly recommended to set up more than one verification method. For example, if you travel a lot, consider setting up the Microsoft Authenticator for your verification method. It is an easy to use verification method that does not result in any text or call related charges.

App Passwords
App Password is a special password that can be used for mobile devices instead of Multi-Factor Authentication. With some older applications and devices, this may be the only workable configuration.
Managing App Passwords

Things to Know about App Passwords

- You should create a separate App Password for each device that uses one.
- The same App Password can be used for multiple applications on the same device.
- Once an App Password is created, there is no way to go back and get the value. You must create a new App Password and delete the old one.
- If an account becomes compromised, it is a standard operating procedure to clear all App Passwords.
- Never install an App Password on a device you do not have complete control over.
- If exposed, App Passwords are dangerous as they bypass the account password and MFA. Keep them in a safe place until you have them safely configured on the device.

Where to Manage App Passwords

App passwords can be managed on the additional security verification screen by selecting the app password link at the top.

Creating a New App Password

1. Choose the **Create** button.
2. Give the App Password a name that references the device for which it will be used.
3. Choose the **next** button.
4. Copy the App Password to the clipboard for use when configuring your device.
5. Close the window.

**Note:** Once you close this window, you cannot return and get the App Password value. Please make sure you have the App Password value secured in a safe place.
Configuring an App Password in Outlook

To access Outlook from a phone or computing device outside of the DCCCD Administrative network, you will need to perform these additional steps.

**Do not set-up an App Password on a shared computing device.**

1. Open Outlook, such as Outlook 2010, 2013, or 2016.
2. Whenever you're prompted for your password, paste the app password in the box. For example, if you've already added your account to Outlook, paste the app password on the login screen:

![Microsoft Outlook login screen](image)

3. Or, if you're adding your Office 365 account to Outlook, enter your app password Auto Account Setup screen:

![Auto Account Setup screen](image)

4. Restart Outlook.
Configuring an App Password on a Phone or Tablet

Do not set-up an App Password on a shared computing device.

Due to the many deferent devices on the market, we will reference Microsoft documentation on how to configure your device.

Except when prompted for a password, follow the directions as presented and use the App Password instead of your normal password. For information on creating App Passwords, see the Creating a New App Password section above.

Choose from the following supported device options:

- Android mobile setup
- iPhone or iPad setup
- Windows Phone setup

Notes:

- Use the “Exchange” or “ActiveSync” option. Other protocols such as POP and IMAP, are not support by the DCCCD for security reasons.
- Configuring a new password, in the Android native email and calendar accounts, may require removing the account and resetting it up.
Tips and Frequently Asked Questions

See the Video on Multi-Factor Authentication (MFA)
https://channel9.msdn.com/posts/Multi-Factor-Account-Setup

Official Microsoft Trouble Shooting Tips for MFA

Questions about this Document
If you have any questions regarding this user guide, please contact IT Operations and Support Services, via email, at DocumentCenter@dcccd.edu.