Multi-Factor Authentication User Setup Guide

This document is designed to provide assistance and guidance to someone setting up Multi-Factor Authentication in Office 365. Multi-factor, or 2 factor, authentication (MFA or 2FA) follows the concept of "Something You Know" (a password) and "Something You Have" (a 6-digit code from an app or a text message, etc). In practical terms, this means that if someone has, or guesses, your password, that alone is not enough to allow them to access your email.

Before any of the steps in this document can be undertaken, the IT department will have enabled MFA for your account. If you did not receive this document from RadioOneSystemManager or someone in the IT department, you can stop here and contact the helpdesk for assistance. (Helpdesk@urban1.com or 301-429-4611)

Setting up MFA is not complicated and it adds an important layer of security to email on top of the standard username and password. Once setup, Outlook Web Access (https://outlook.office.com/owa) will prompt for the second factor (e.g. SMS Text message, App Notification, or even a phone call) and can be relied upon as a way to access email even if other applications have not yet been configured for MFA.

Many modern applications understand MFA and will seamlessly take advantage of the second factor. Some older applications do *not* understand MFA – a good example of this is Outlook 2010 – These applications require an "App Password" – More information on that can be found in the instructions below.

It is important to note that using MFA in Office365 only effects applications that are based in the Office 365 cloud – for us that includes examples like Email, The UNN Portal, Microsoft Teams etc. On the other hand, many applications we use every day are not impacted in any way – logging on to your computer, using Lawson, Wide Orbit, Broadway, etc. Those application will not be impacted by this change at all.

At the end of this guide, once the initial configuration is complete and you have confirmed that you are able to access Outlook Web Access (https://outlook.office.com/owa) using MFA, you will find some tips and additional information about some specific applications and how to make sure they are working now that MFA has been activated.

The first thing we're going to do is to look for older copies of your username and password that might be saved on your computer. Clearing these out *first*, before starting the setup for Multi-Factor Authentication (MFA) can save us some confusion later in the process. **TIP:** This is extremely important if you are using Outlook 2010 on your computer!

1) Let's look in Windows Credential Manager – If you click on the Start Button and begin typing 'Credential Manager" in the "*Search Programs and Files"* box, you will see it appear in the list. Click on it once and it will open in a new window.

2) What you see in Credential Manager is specific to the computer you are working on. You may see one or two lines, or many. What we want to do is look for all the entries that say:
"Microsoft Office" or "Outlook" or "Autodiscover"
Click on them to expand them and see the details and then click on "REMOVE FROM VAULT" This should only take a few seconds for each entry. Once they are gone, we are ready to move on and begin the enrollment process.

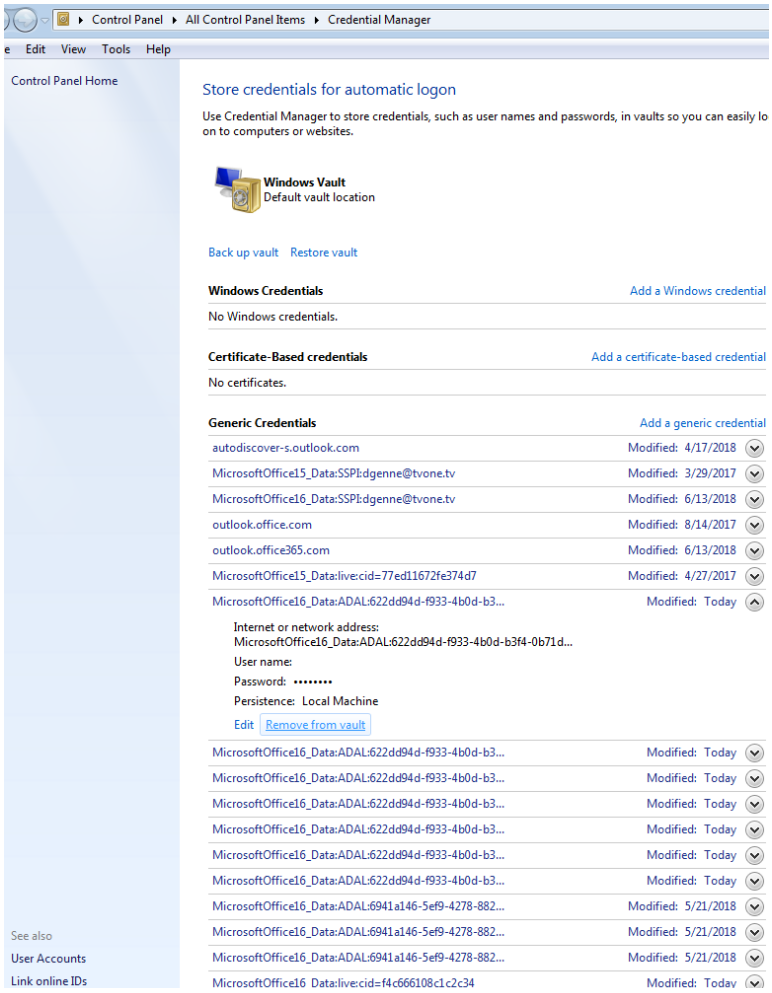


Figure 1 Remove Credentials from Vault

Figure 2 Find Credential Manager

3) Once you have are ready to set up Multi-Factor Authentication (MFA) for your account go to this link: https://aka.ms/MFASetup - If you are not already logged into Office 365 in your browser, you will see some variation of a window prompting you to enter your username and password. (Figure 1)

   Choose your account from the list, or enter your login name.

   TIP: Your current email address will probably work, but if it doesn't, try your previous one, or ask for help.

   E.g. If JDoe@urban1.com doesn't work, try JDoe@Radio-one.com

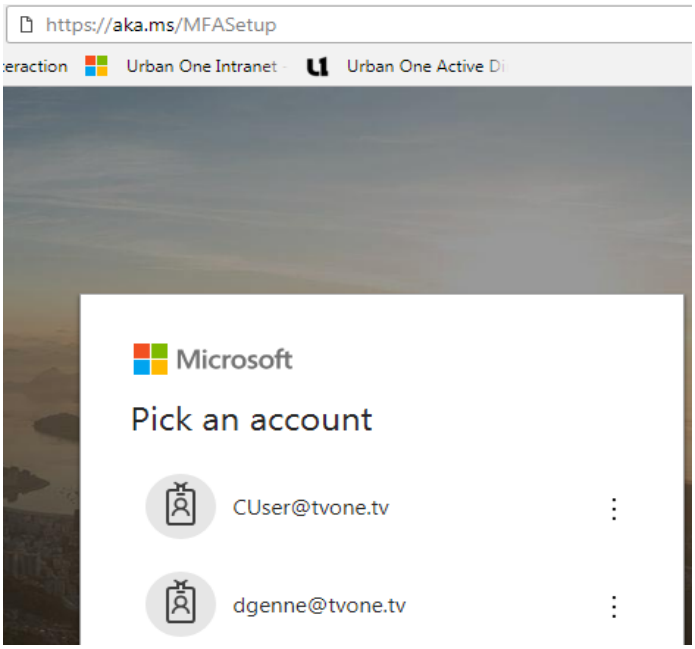


Figure 3: https://aka.ms/MFASetup

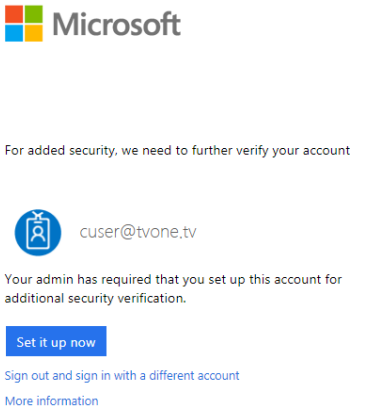


Figure 4: Confirm

4) Once you have logged in, you should see a message asking you to verify your account and confirm that you want to begin setting up MFA – Please Click on the "Set it up now button. (Figure2)

5) STEP 1: The next screen we see lets us complete the basics – enter a cell phone and get a Text Message delivered to it. (Figure 3)

   TIP: Country Code is required – the United States is at the top of the list (+1)

   Click Next

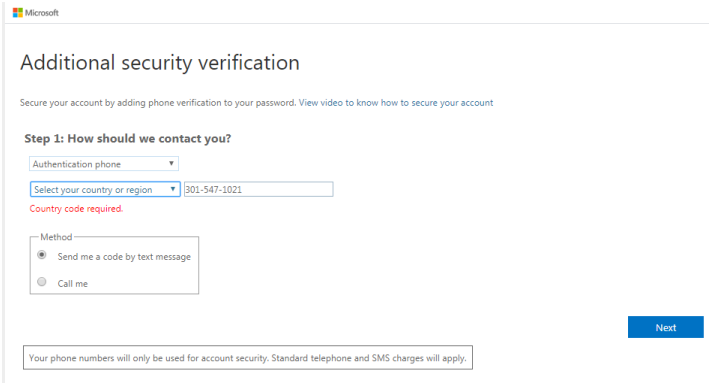


Figure 5: Enter Mobile Phone Number

6) STEP 2: And Verify Code by the code from the Text Message you received in the box provided. Click VERIFY button (Figure 4)

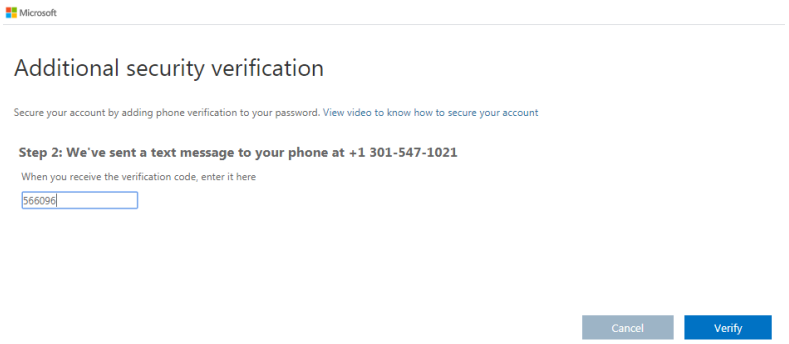


Figure 6: Verify Code

7) STEP 3: Keep Using your existing applications (App Password)

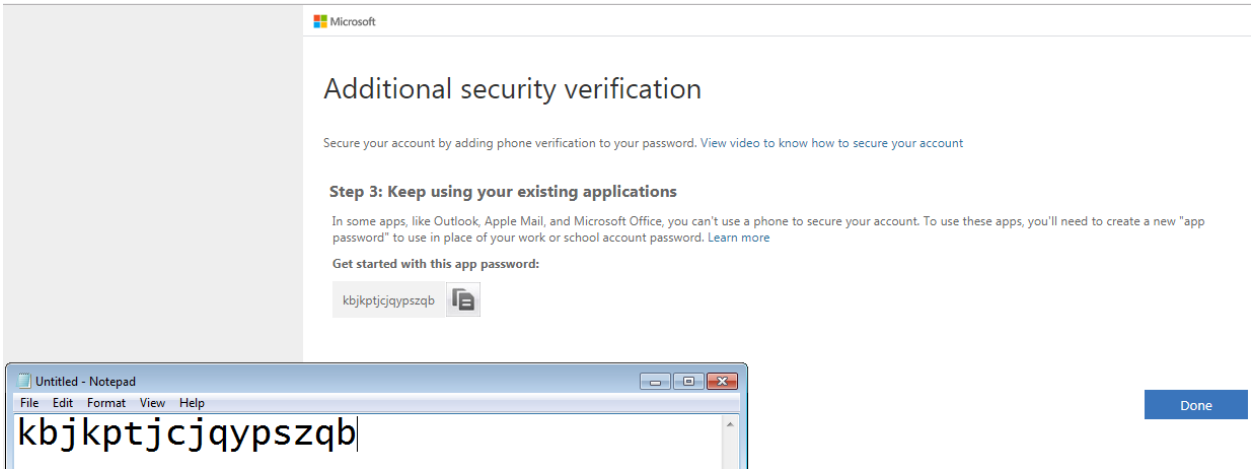


Figure 7: Initial App Password

This is an App Password as mention in the 5th paragraph of the introduction. When an application does not understand MFA, it will not allow you to log in with your username and password. Instead you will need to provide this App Password.

TIP: Copy this App Password now, and paste it into a Notepad window or other place for temporary safe keeping. You can create additional App Passwords at any time, but each one is only displayed *once*.

Click Done when you are ready to move on.

8) More Options: On this next screen you have some options.

We strongly recommended that you set up at least 2 ways of getting a notification. For example: Using the Microsoft Authenticator and getting a text message. App (See below for more information on the Authenticator App)

TIP: Configure the Authenticator app here, and make your default verification option "Notify Me Through App"

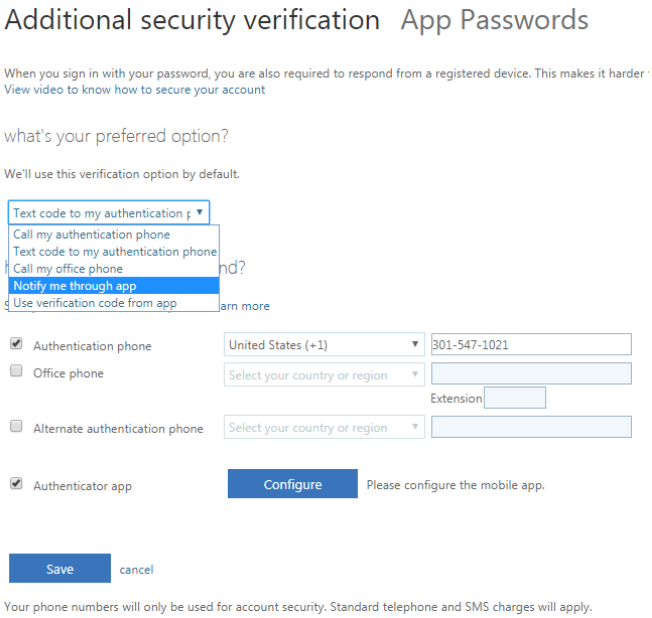


Figure 8: Default Option

9) (Optional – RECOMMENDED)
Configure Authenticator App – Check the Box Next to Authenticator All and then click Configure.

-A new box will pop up showing a QR code.

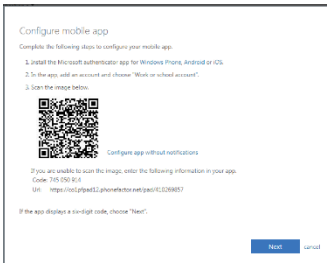


Figure 9: QR Code

- Go to the App Store or Google Play Store and download the Microsoft Authenticator app – it is a free app and fairly small so it downloads and installs quickly.

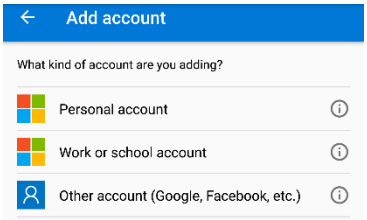


Figure 10: Work Account

Once it is installed – choose Add Account – Work or School Account – then center the QR Code in the box on the phone screen. It automatically capture the QR code and configures itself. Once you see a 6-digit number and a 30-second countdown timer, it's all set.

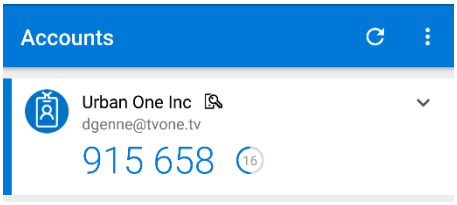
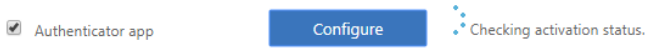


Figure 11: Successfully Configured

Now Click Next at the bottom of the QR Code box. The system takes a second to verify that the App Configured correctly. While that is happening, you should see this:

Figure 12: Checking Activation Status



And then this:

Figure 13: Mobile App Configured

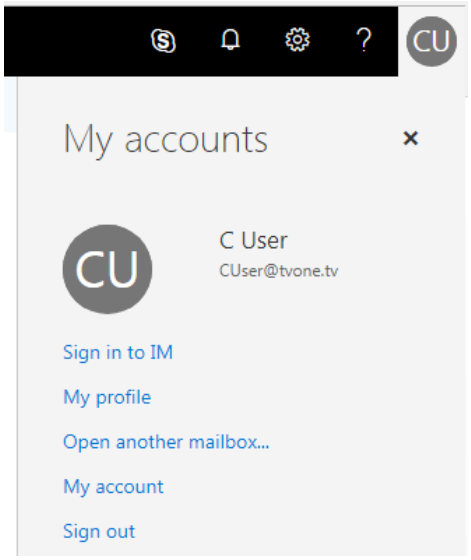
10) We're just about finished – Now double check your settings – You can use any of the available options shown, but our default recommendations are:
    a. Set Default Option to "Notify Me Through App"
    b. Check Authentication Phone and/or Alternate Authentication Phone to receive text messages.
11) Click Save to exit out of the Multi-Factor Authentication Setup!

Additional Information and Tips and Tricks:

You can make changes to your Multi-Factor options and settings at any time.

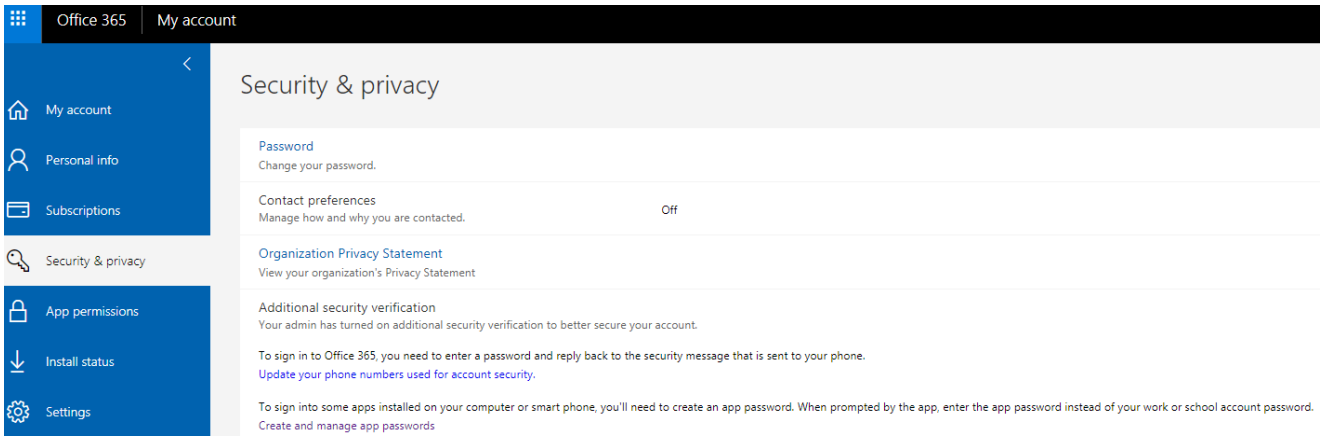
To get started, simply Log in to Outlook Web Access: https://outlook.office.com/OWA

Click on your Initials (or Profile Picture) in the Upper Right-hand Corner and then Click on My Account

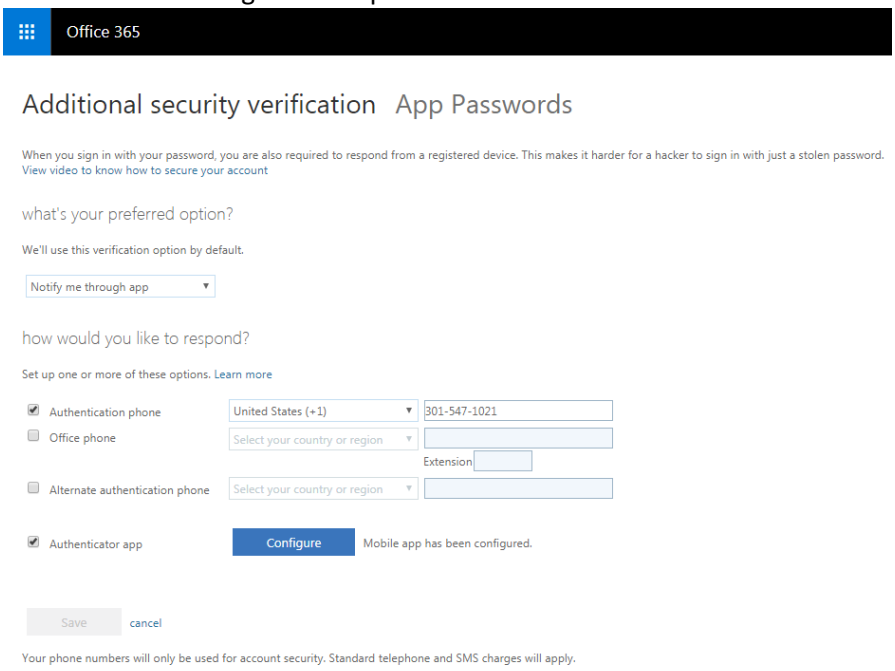


Click on My Account will take you to a new page where you will see several options. The ones related to MFA can be found under the Security & Privacy tab on the left.

Click on Security & Privacy and then click on "Additional Security Verification" to see the options available.



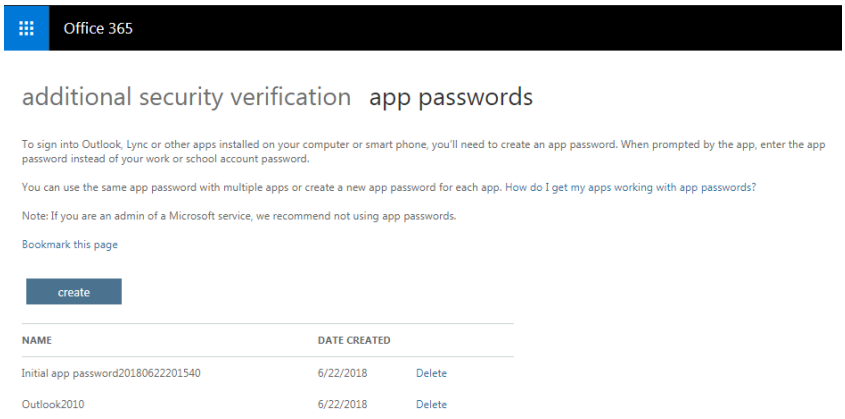
The first is: “Update your Phone Numbers used for Account Security” – Click on this to change the cell phone number



The second choice “Create and Manage App Passwords” is useful for legacy applications that do not support MFA – like Outlook 2010, and Native Mail applications on Phones.

To Create a new AppPassword, Click the Create button, assign it a Name and Copy the password when it appears on screen.

Each App Password only appears once, at the time it is created. You can create up to 40 App Password if you want.



Once strategy is to create an App Password for each Device that needs it. For Example – An App Password for your desktop computer, A second App Password for your Android Phone, and a third App Password for your iPad.