

Setting up Multi-Factor Authentication (MFA) for your Office 365 Account

Multi-factor authentication (MFA) is a 2-step verification process that the Iowa DOT is using to increase security. MFA authentication will be required when logging into a cloud application if you are not using a DOT registered device.

By setting up MFA, you add an extra layer of security to your Office 365 account. The first layer of authentication is signing in with your email address and network password. For the second layer of authentication, you can choose from these options (**Option 3 is the Recommended Method for users with DOT issued smart phones or those who wish to use the application on a personal smart phone**):

1. Setup a phone number(s) to receive phone call – you will need to answer the phone and select to Approve or Deny the authentication request (Go to Step A for this setup option)
2. Setup a phone number(s) to receive a text message with a code that you will enter into the system (Go to Step A for this setup option)
3. Setup the Microsoft Authenticator app on your DOT Mobile device or a personal mobile device to send a notification to Approve/Deny or enter the verification code from the app (Go to Step B on page 3 for this setup option) – **RECOMMENDED METHOD for users with a DOT Smart phone**

We strongly recommend setting up more than one verification method. The Microsoft Authenticator app (Option 3) is the quickest way to authenticate, but you will also want a phone number setup. If you are only setting up phone numbers, we strongly suggest setting up more than one number. The second number could be a close family member or colleague's number that you would only use if the primary phone is lost/stolen/damaged.

A. Setting up a phone number(s) to receive a phone call or text message

1. Go to the MFA setup for Office 365 using this link - <https://aka.ms/mfasetup> and sign in using your work email address and your network password. After you sign in, you'll see this page:



anya.denning@iowadot.us

More information required

Your organization needs more information to keep your account secure

[Use a different account](#)

[Learn more](#)

[Next](#)

2. Click on **Next**.
3. Select **Authentication phone** from the drop down and then enter the Country code and phone number as shown here:

Additional security verification

Secure your account by adding phone verification to your password. [View video to know how to secure your account](#)

Step 1: How should we contact you?


Authentication phone ▼

United States (+1) ▼ 5152901234

Method

☐ Send me a code by text message

☒ Call me



Next

Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.

You can select to receive a text message with a verification code or a phone call with a prompt to Approve/Not Approve. Click on **Next**.

- Next, you will need to verify this authentication method. Type in the code that is text to your authentication phone, or approve the request in the phone call.

Additional security verification

Secure your account by adding phone verification to your password. [View video to know how to secure your account](#)

Step 2: We've sent a text message to your phone at +1 5152902967

When you receive the verification code, enter it here

962249

Cancel

Verify

- After verifying, select **Done**.
- Select **Yes** to stay logged on and it will take you back in to select additional options.
- From here you can setup an **Alternate authentication phone** (this would only be used as a backup if your primary phone is lost/stolen/broken). We strongly recommend having at least one alternate method of authentication setup. Note - We cannot use the **Office Phone** option at this time, but you will not need to use multi-factor authentication when you are in the office on a DOT device.

From here you can also choose to setup the Microsoft Authenticator app as an additional verification method. Use the instructions in step B-1 to install the Microsoft Authenticator app using the Company Portal, then select the check box for Authenticator App and click on **Configure** to bring up the **Configure Mobile App** screen shown on page 5. Follow the instructions from there to continue setting up the Microsoft Authenticator app.



Anya.denning@iowadot.us |

Additional security verification

When you sign in with your password, you are also required to respond from a registered device. This makes it harder for a hacker to sign in with just a stolen password.
[View video to know how to secure your account](#)

what's your preferred option?

We'll use this verification option by default.

☒ Call my authentication phone
☐ Text code to my authentication phone
☐ Call my office phone
☐ Notify me through app
☐ Use verification code from app

Set up one or more of these options. [Learn more](#)

☒ Authentication phone

United States (+1)

5159991234

☐ Office phone

Select your country or region

(515) 233-7793

Extension

☒ Alternate authentication phone

United States (+1)

5159999999

☐ Authenticator app

Configure

Mobile app has been configured.

Save

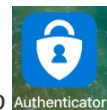
cancel

Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.

8. After you verify your alternate contact method, choose **Save**. When you see the **Updates Successful** screen, select **Close**.


B. Setting up the Microsoft Authenticator app

The Microsoft Authenticator app is a quicker way to authenticate. It works best if you have the Microsoft Authenticator app ready before starting to register for MFA.



1. If you have a DOT mobile device, please check it for the **Microsoft Authenticator** app , if



you do not have this app, please go to the **Company Portal**  (use the Company Portal to install that app and not the App Store for a DOT device). Search for 'Microsoft Authenticator' and Install the app. (You may need your iTunes password)

- a. NOTE – if you want to install Microsoft Authenticator on a personal device, go to the app store for that device and search for 'Microsoft Authenticator' and install.
2. On your computer, go to the MFA setup for Office 365 using this link - <https://aka.ms/mfasetup> and sign in using your work email address and your network password. After you sign in, you'll see this page:



anya.denning@iowadot.us

More information required

Your organization needs more information to keep your account secure

[Use a different account](#)

[Learn more](#)

Next

3. Click on **Next**.



Additional security verification

Secure your account by adding phone verification to your password. [View video to know how to secure your account](#)

Step 1: How should we contact you?

Mobile app



How do you want to use the mobile app?

☒ Receive notifications for verification

☐ Use verification code

To use these verification methods, you must set up the Microsoft Authenticator app.

Set up

Next

4. Select **Mobile app** and **Receive notifications for verification** then click on **Set up**. You should now see the below pop up window in your browser.

Configure mobile app

Complete the following steps to configure your mobile app.

1. Install the Microsoft authenticator app for [Windows Phone](#), [Android](#) or [iOS](#).
2. In the app, add an account and choose "Work or school account".
3. Scan the image below.



Please scan the QR code in your browser window, not this QR code.

If you are unable to scan the image, enter the following information in your app.

Code: 604 350 522

Url: <https://cys01pfpad11.phonefactor.net/pad/358441951>

If the app displays a six-digit code, choose "Next".

Next

cancel

5. Open the Microsoft Authenticator app on your mobile device. Add an account by going to the **accounts** screen, select **+**, and then specify that you want to add a **work or school account**. If you get a message about a backup, select **Continue**. This is resetting any backup you may have for the Microsoft Authenticator app only.
6. This will open a camera screen on your mobile device, you should now scan the QR code that popped up in your browser window.
7. When the app on your phone shows your account name with a six-digit code underneath, it is setup.
8. Click **Next** on your computer, you should now see a message "Mobile app has been configured for notifications and verification codes".
9. Click on **Next**, then approve the notification on your phone in the Microsoft Authenticator app.
 - a. If setting up the Microsoft Authenticator app after setting up phone numbers click on **Save**. When you see the **Updates successful** screen, select **Close**. Then you are done.
10. Now you need to setup at least one phone number to use. You can use the same device that has the Microsoft Authenticator app. We recommend setting up one additional phone number in the next screen as well, just in case your primary device is lost/stolen/broken.

11. After entering your phone number, select **Done**.

Please select one additional **Alternate authentication phone** here and click on **Save**. When you see the **Updates successful** screen, select **Close**.

Note - We cannot use the **Office Phone** option at this time, but you will not need to use multi-factor authentication when you are in the office on a DOT device. The second number could be a close family member or colleague's number that you would only use if the primary phone is lost/stolen/damaged. It will not send them a notification when you select **Save**.

If you have any questions or problems, please contact the Service Desk at 515-239-1075 or DOT.Helpdesk@iowadot.us.