



Using Multi-Factor Authentication

Modified Date: October 6, 2022

Zane State College has enabled Multi-Factor Authentication (MFA) for student and employee user accounts. MFA provides increased user security by requiring a second-factor authenticator to login (in addition to a password). The second-factor authenticator may include a phone call, text message, email, or the Authenticator app.

The College will utilize Microsoft's MFA solution to provide seamless integration with our single-sign-on environment. For ease of use, contact information will be pre-populated for use as second-factor authenticators (phone call or text). The Microsoft Authenticator app is also available for Apple and Android smart devices as an authentication option.

MFA is enabled on My ZSC, Blackboard, Microsoft Office 365 and Zoom. MFA is initially setup by the College; however, you may review and change your information by navigating an Internet browser to <https://aka.ms/mfasetup>. Please see below for additional instructions.

1. Using a desktop or laptop computer open an Internet browser to <https://aka.ms/mfasetup>.
2. Review your current phone number and determine if changes need to be made?

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

how would you like to respond?

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

<input checked="" type="checkbox"/>	Authentication phone	* United States (+1)	7405885000
<input type="checkbox"/>	Office phone (do not use a Lync phone)	Select your country or region	
<input type="checkbox"/>	Alternate authentication phone	Select your country or region	Extension
<input type="checkbox"/>	Authenticator app or Token	Set up Authenticator app	

Save cancel

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


3. Review your preferred verification options. This is done by clicking on the drop-down box and selecting one of the three options.
 - a. Call my authentication phone
 - b. Text code to my authentication phone
 - c. Notify me through app (Only used with Microsoft's Authenticator app)

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 

- Call my authentication phone
- Text code to my authentication phone
- Call my office phone
- Notify me through app

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

Authentication phone *

Office phone (do not use a Lync phone)

Alternate authentication phone

Authenticator app or Token

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

4. If you would like to use the Microsoft Authenticator app, click the Set up Authenticator app button.

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


how would you like to respond?

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

Authentication phone *

Office phone (do not use a Lync phone)

Alternate authentication phone

Authenticator app or Token 

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

5. Using your mobile smart phone or tablet, download the Microsoft Authenticator app from the Apple App Store or Google Play Store.
6. Open the app and add an account, choosing "Work or school account".

7. Scan the QR code that is showing on your computer screen with your authenticator app.

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.



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

Code: 450 279 768

Url: <https://mobileappcommunicator.auth.microsoft.com/activate/112914365/WUS>

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

Next

cancel

8. Click the Next button on your desktop or laptop computer. Microsoft will verify the connection works with your smart device and you are finished.

If you have questions or would like additional help, please contact the Technology Solutions Center at techhelp@zanestate.edu or call us at 740.588.1327.