MFA Options

Multi-Factor Authentication (MFA) is a security measure that enhances the protection of your university accounts by requiring multiple forms of verification before granting access. This additional layer of security ensures that even if your password is compromised, unauthorized users will not be able to access your account without the second form of verification.

At WSU, MFA is an essential part of safeguarding sensitive information and maintaining the integrity of our digital resources.

There are two primary types of MFA solutions: software and hardware.

- **Software solutions** typically involve applications like Okta Verify and Google Authenticator. These apps generate time-sensitive codes or push notifications to your smartphone, which you must approve to complete the login process. Software solutions are convenient and flexible, allowing users to authenticate from virtually anywhere with their mobile device.

- **Hardware solutions** involve physical devices such as USB security keys (e.g., YubiKey). These devices must be inserted into your computer to verify your identity. Hardware solutions offer a high level of security as they are less susceptible to phishing attacks and malware compared to software solutions. However, they require the user to carry the physical device, which can be a limitation for some.

Both software and hardware MFA solutions are available at the university, providing students, faculty and staff with options that best fit their needs and preferences.

---

**SMS and Voice Call MFA Warning**

SMS (text message to your cell phone) and Voice Call MFA Options will no longer be available in the coming months - Please move now to Okta Verify, Google Authenticator/Software TOTP, or a USB Security Key for Multi-Factor Authentication. For additional information on how to set these up, please see the links below.

---

**Software Solutions and Related Articles**

- Okta Verify
- Google Authenticator / Software TOTP
- Email MFA
- Security Question

**Hardware Solutions and Related Articles**

- c200 TOTP Hardware Token
- webauthn / FIDO2 / biometrics
- Lost or Stolen MFA Device