Multi-Factor Authentication

Frequently Asked Questions

May 2025

1. What is Multi-Factor Authentication (MFA)?

   It is a security measure that requires users to provide two or more verification factors to gain access to an account or system. It is a way to verify a user's identity by requiring at least two distinct forms of proof.

2. Why should I implement MFA?

   Implementing Multi-Factor Authentication (MFA) is a critical step in safeguarding sensitive data. It adds an extra layer of security by requiring users to verify their identity through more than one method when accessing Single Sign-On (SSO).

   MFA not only **protects students and district information** but also helps maintain the integrity of your user account.

   As user credentials attacks become more common, using a second authentication factor adds a layer of security to Single Sign On to protect district's sensitive data and reduce risks of unauthorized access.

3. Is there a Guidance Document to set up MFA?

   Yes, guidance documents are available in the Single Sign On - Links And Docs section.

4. Do I have to buy an Application (App) to use MFA?

   No. You do not have to purchase an application. You may download an MFA application of your choice for FREE. We strongly recommend you avoid purchasing an app for this purpose and be suspicious of any app that requires payment for authentication services. Guidance documents are available for Google Authenticator, Microsoft Authenticator and Passwords (Apple users) under the Links and Documents menu on the SSO home page.

5. What are some commonly used MFA applications?

   Commonly used MFA applications are Microsoft Authenticator, Google Authenticator, Passwords (for Apple users) and Samsung Pass. Be sure not to use a scam app. Check the app reviews prior to downloading it to give you a sense of customer satisfaction and comments.

6. What if I do not have any of the Multi-Factor Authentication Apps mentioned in the Guidance?

   It is not a problem. SSO will work with any MFA application already on your smart phone, mobile device or you may download an MFA application.

7. How can I download the App to my phone?

   Visit the **App Store** or **Play store** on the phone or mobile device and search for a Multi-Factor Authentication Application. Download the app of your choice. Remember these apps are FREE. If it involves a cost, reject and do not download.

8. Why use a Mobile Authenticator Application?

   Authenticator apps such as Google Authenticator and Microsoft Authenticator can generate a time-based one-time password (TOTP) that changes every 30 seconds. The TOTP is used as the second factor in the authentication process, providing an additional layer of security.

9. How can I implement MFA at my district?

   MFA will be enabled for SSO users in phases beginning July 1st, 2025. Share the guidance documents to help educate and onboard users. A video link is also available.

10. Can my MFA be reset?

    Yes. The district's SSO Administrator is able to reset your MFA. If you do not know who this person is in your district, follow the organizational structure starting with your immediate supervisor.
    In addition, delete the previous SSO set up from your MFA application to avoid confusion with multiple SSO accounts linked to the MFA application.

11. Is MFA difficult for users to adopt?

    Most users adapt quickly, especially with user-friendly methods like authenticator apps. Providing clear instructions, guidance documents, video and support can ease the transition.

12. What should I do if I lose access to my MFA App?

    Contact your district's SSO Administrator to have your SSO account reset for MFA. SSO Administrator will verify your identity following the district's access management policy or protocols.

13. Will passwords changes continue to be required for SSO?

    Yes. The Department of Education is adding a layer of security with MFA implementation and password changes will continue to be required every 90 days.

14. Does MFA impact my @affiliates account?

    No. It does not impact your affiliates account. You may continue to use your affiliates account to access the Data document library.

15. What if I do not have an SSO account?

    In this case, MFA implementation will not impact you. MFA applies to all SSO account users.

16. Are there any MFA guidance documents for commonly used apps?

    Yes, MFA guidance documents can be found on the SSO home page. On the left-hand menu, select **Links And Docs**. Guidance documents are included in the Documents list. Single Sign On - Links And Docs

17. Will districts have to enable MFA for district users?

    No, MFA will be enabled by the Office of Management and Enterprise Systems (OMES) for all district SSO users.

18. Can I have more than one QR code assigned to my SSO account?

    No, the MFA is introduced for security purposes to authenticate that it is you accessing your account. Therefore, only one QR code can be assigned to set up MFA with your SSO account.

19. Will the MFA app send a prompt to my mobile device every time I want to log into SSO?

    No. The MFA app will not send you a prompt or push notification with the 6-digit code. To get the 6-digit code, you need to open the authenticator app on your mobile device and find the code under the SDE Single Sign On account.

20. Why are my 6 digits/verification code not working?

    Did you enter the numbers and these timed out? We recommend testing the 6 digits a couple of times to ensure it is not a timed-out issue. If this does not work, an option may be to reset your MFA, which may requested from the district's SSO administrator.

21. How do I find the 6 digits/verification code on my phone again?

    Find your MFA app on your phone or mobile device, select it and scroll to find your **SDE SSO account**. Under the SDE SSO account you will find the 6 digit/validation code. Remember, the numbers time out every 30 seconds.

22. I am an educator not associated with a district. Who can I reach out for support with MFA?

    For MFA guidance, go to the Single Sign On Home page and on the left hand side menu on the screen, select Links And Docs. Under the documents section, there is a generic SSO Login Guidance along with specific MFA guidance for Google Authenticator and Microsoft Authenticator. You may also reach the Oklahoma Office of Management and Enterprise Services (OMES) service desk at (405) 521-2444.

23. How can I delete the SSO account from my MFA app?

    Depending on the app, the steps are slightly different. For Google Authenticator, select the SSO account and swipe to the left. For Microsoft Authenticator, select the Single Sign On account, once in the account, on the top right corner, select the gear icon and then remove the account.

24. What if my Multi-Factor Authentication app requires an URL?

    If your application asks for an URL, you may enter https://sdeweb01.sde.ok.gov/SSO2/Signin.aspx along with any other information it requires. Account name: SDE SSO Login. Code or Secret key is the lengthy Manual Setup Code or simply select QR code.

25. Is there another MFA method available?

    We understand there may be cases in which users may need an alternative to using a personal device for authentication. In such cases, the use of a district device is preferred. If a district device is not available, please contact the district's SSO administrator for support. A single-use PIN may be provided.

26. How do I go about adding the Manual Setup Code rather than the QR Code?

    If you select the Manual Setup Code option,

    In Microsoft MFA App: For Account Name = **SDE SSO Login** and enter the Secret Key = lengthy **Manual Setup Code** provided on the SSO screen. Lastly, select finish to set up.

    In Google MFA App: For Code name = **SDE SSO Login** and enter Your key = lengthy **Manual Setup Code** provided on the SSO screen. Lastly, select Add to set up.

27. What is TOTP?

    Time-based One-Time Password or TOTP is a type of MFA where a new 6-digit code is generated every 30 seconds by an authenticator app.

28. How does TOTP work?

    TOTP uses a **shared secret key** between the authenticator app and the SSO system. Both use the current time to independently generate the same one-time password. The user enters the 6-digits from the MFA app during login and the server checks if the code is correct based on time and secret.

29. Why use TOTP MFA app over text message password?

Time-based One-Time Password (TOTP) is not vulnerable to SIM swapping, text or SMS phishing. Authenticator apps can generate a code without internet or cellular service. For Privacy reasons, phone numbers are not needed, protecting user identity.