

Login.mo.gov the Workforce Portal, powered by Okta

Contents

Legal Notice.....	1
Accessing the Okta Portal	2
Okta Username	2
Setting up MFA/2FA.....	2
Reasons to setup MFA/2FA.....	2
MFA Options	2
Setup Your MFA Options.....	3
Okta Verify - In app setup instructions.	4
Okta Verify – though portal setup instructions	8
Push Notices.....	9
Google Authenticator.....	11
Phone (Text Message (SMS) or Voice Call) - DEPRECATED.....	13
On-Prem MFA (RSA Token).....	14
Authentication Process	15
Acronyms	15

Legal Notice

Two-factor authentication is required to remotely access State of Missouri computer systems. Such access is intended only for authorized users and State of Missouri business purposes. If you use your personal device as a two-factor authentication token to access State of Missouri computer systems, the token content would not be produced in response to a Sunshine Law request. If you use your personal device to communicate regarding public business, such communications may be subject to the Missouri Sunshine Law.

Accessing the Okta Portal

All state employees and contractors with state provided accounts can login to the Okta Portal at <https://login.mo.gov>.

Okta Username

Okta is connected to Active Directory (AD) for account information. We are setup to support two username formats. Users can use either their AD username or email for username.

- lastf@bds.state.mo.us
- First.last@oa.mo.gov

The image displays two sequential steps of the Okta Employee Login process. The first screenshot shows the 'Sign In' page with a 'Username' input field, a 'Keep me signed in' checkbox, and a 'Next' button. The second screenshot shows the 'Verify with your password' page with a password input field, a 'Verify' button, and links for 'Forgot password?' and 'Back to sign in'.

Setting up MFA/2FA

Reasons to setup MFA/2FA

Multi-Factor Authentication (MFA) also known as Two-Factor Authentication (2FA) will be used to securely connect to publicly accessible state resource. A publicly accessible state resource is one that can be reached from outside the state network. Examples include, but are not limited to, Virtual Private Network (VPN), Virtual Desktop Infrastructure (VDI) and Office.com.

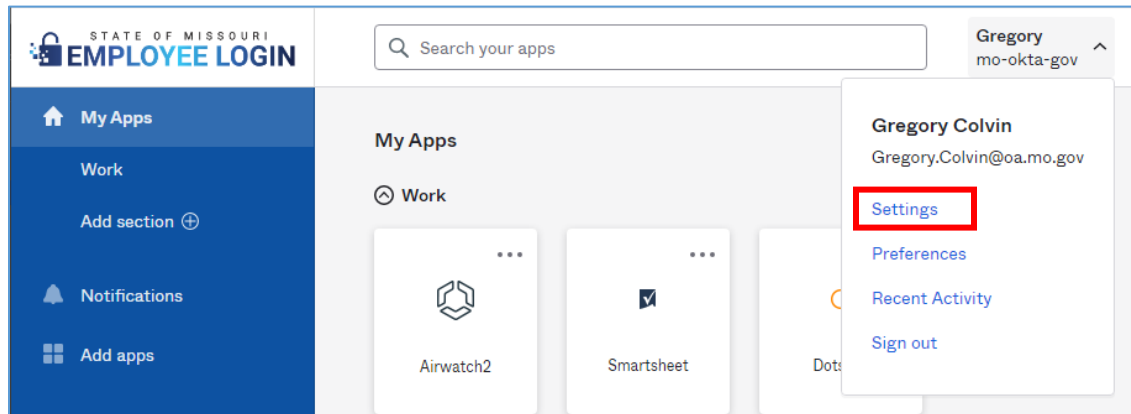
MFA Options

There are a few MFA options available. The recommended MFA setup for best security and ease of use is to setup Okta Verify. For users with unique circumstances, ITSD also has Google Authenticator and RSA Hard Token available for MFA.

To add an MFA option to your account you will need to go to the settings page of the Portal on your PC and select the desired MFA option from the Security Methods section.

Below are the setup instructions for each method currently available:

Login to your Okta Portal at <https://login.mo.gov>



Setup Your MFA Options

- A. [Okta Verify](#)
- B. [Google Authenticator](#)
- C. [On-Prem MFA \(RSA Physical Token\)](#)

Okta Verify

Okta Verify Setup Instructions

Okta Verify is the preferred, highly secure, and phishing resistant method for Multi-Factor Authentication (MFA). You can download Okta Verify to your phone from your device's app store. It is available on both Apple and Android devices.

Okta Verify - In app setup instructions.

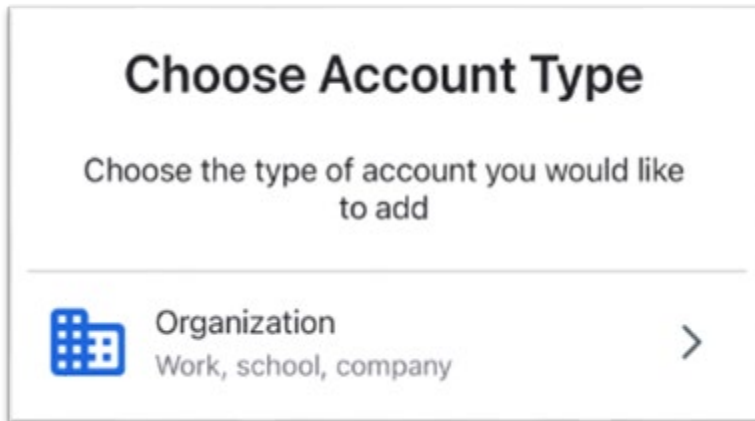
1. Open Okta Verify App on your phone.



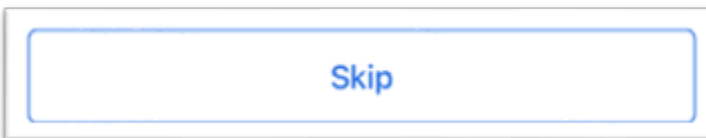
2. Click the "+" in the top bar



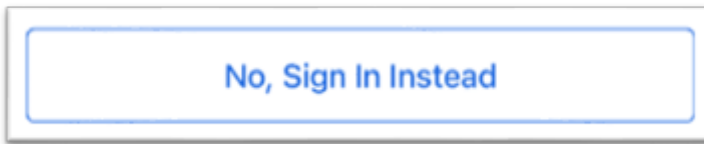
3. Click "Organization"



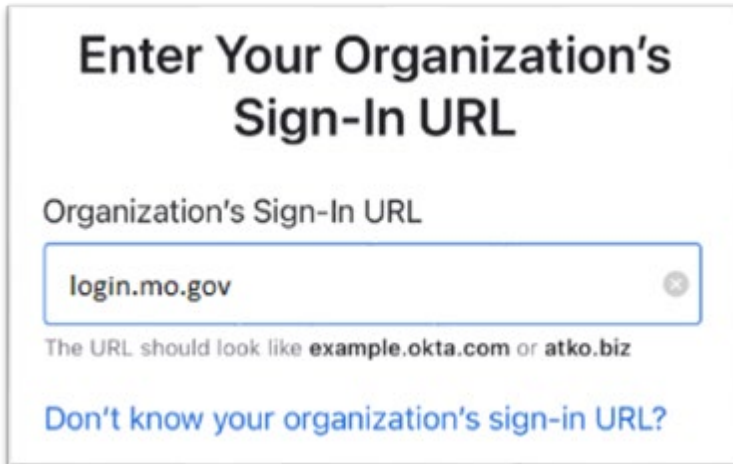
4. Click "Skip" on the "Add Account from Another Device?" Page



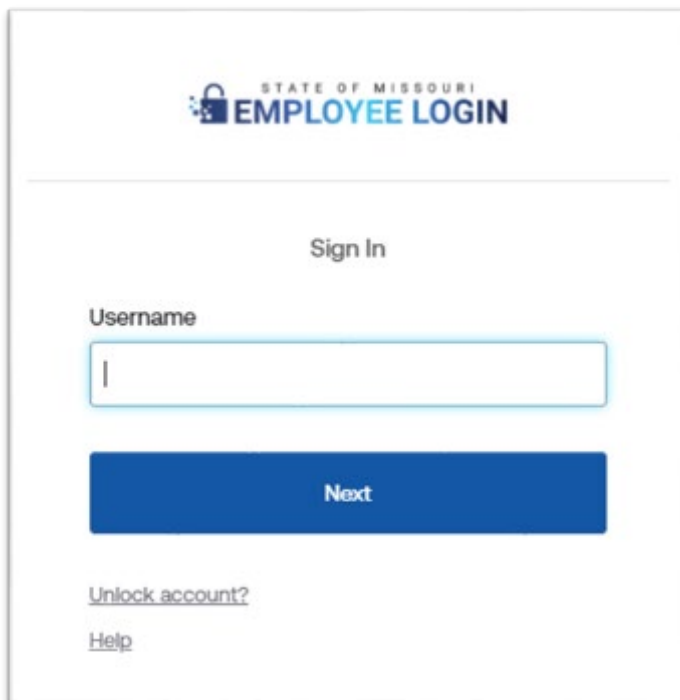
5. Click “No, Sign in Instead” at the bottom of the screen



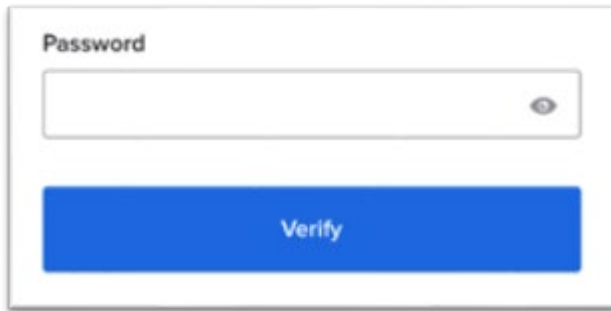
6. Enter “login.mo.gov” for the Organization’s Sign-In URL

A screenshot of a web form titled "Enter Your Organization's Sign-In URL". The form has a white background and a thin grey border. At the top, the title is in a large, bold, black font. Below the title, the label "Organization's Sign-In URL" is in a smaller black font. A text input field contains the text "login.mo.gov" and has a small grey 'x' icon on the right side. Below the input field, there is a line of text: "The URL should look like example.okta.com or atko.biz". At the bottom of the form, there is a blue link that says "Don't know your organization's sign-in URL?".

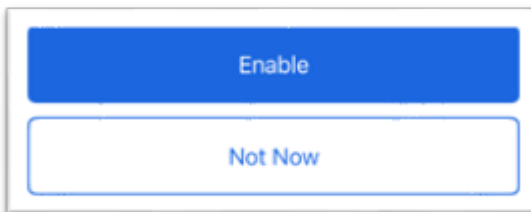
7. Enter your computer user ID or work email in the username field.

A screenshot of a web form titled "Sign In". The form has a white background and a thin grey border. At the top, there is a logo for "STATE OF MISSOURI EMPLOYEE LOGIN" with a blue padlock icon. Below the logo, the text "Sign In" is centered. Underneath, the label "Username" is in a bold black font. A text input field contains a single vertical bar "|". Below the input field is a large blue button with the text "Next" in white. At the bottom of the form, there are two links: "Unlock account?" and "Help", both in a smaller, blue font.

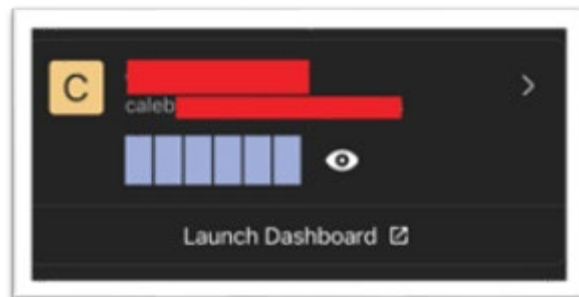
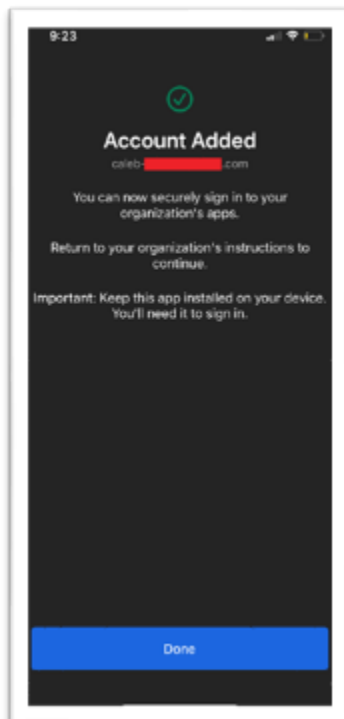
8. Enter your computer password



9. Choose either “Enable” or “Not Now” to Enable Face ID or Passcode Confirmation.

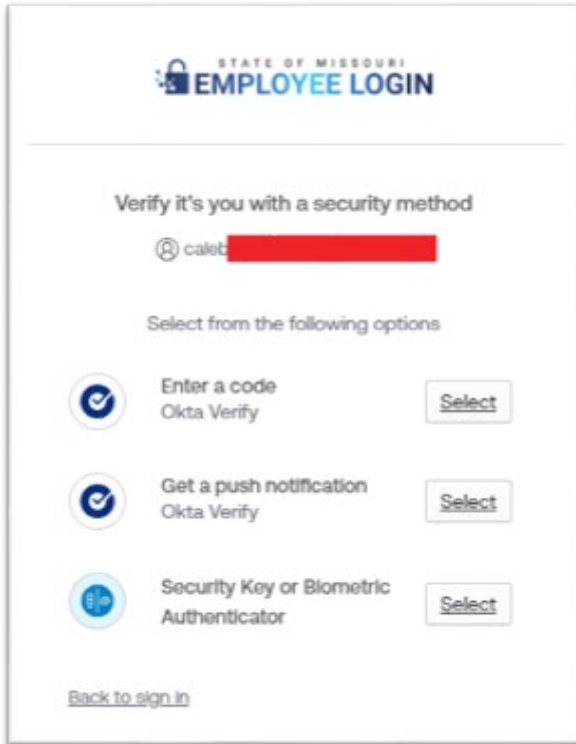


10. You will then see the “Account Added” screen. After selecting “Done” you will be taken to the app’s dashboard, and then you will see your Okta Verify account.



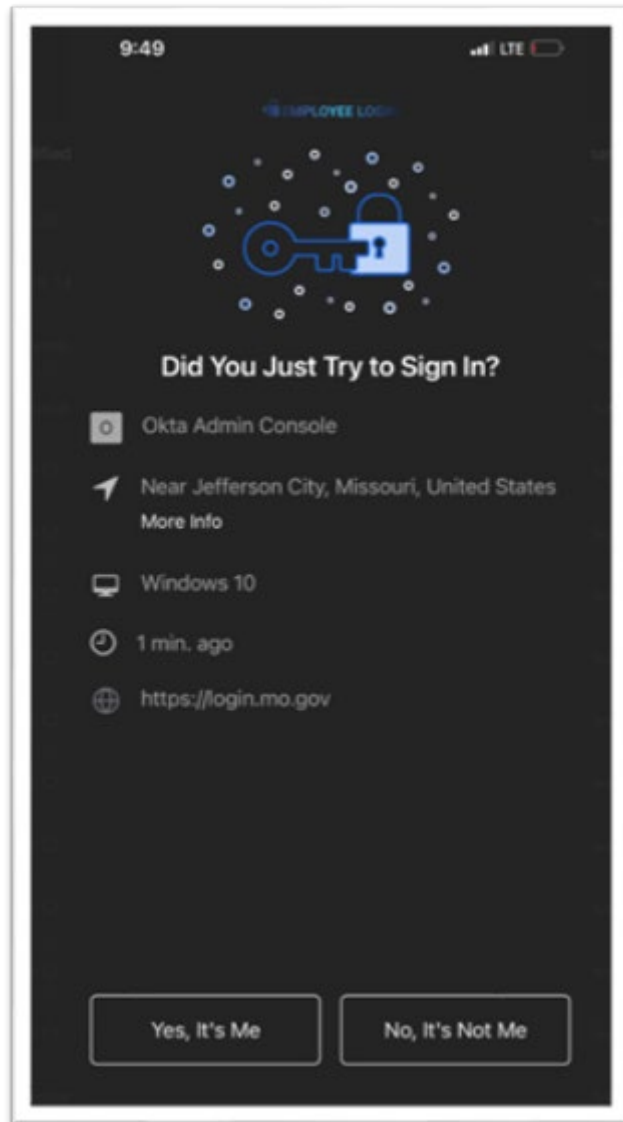
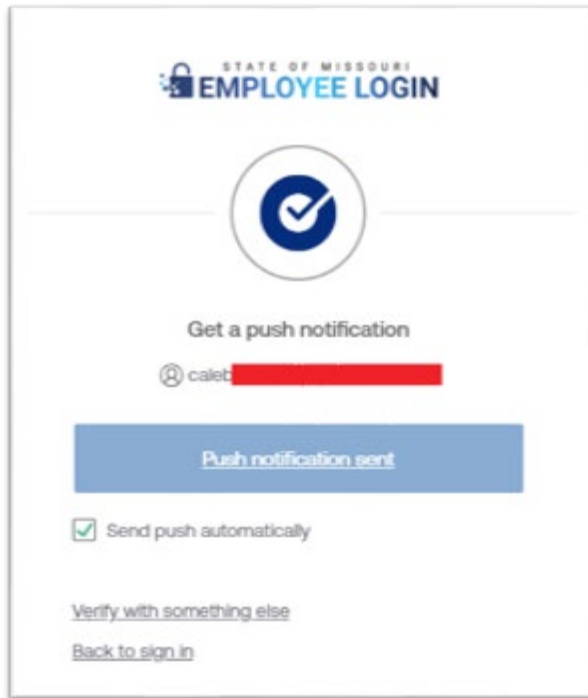
11. You have successfully enrolled Okta Verify as your MFA. Now that your Okta verify is set up, when you are prompted for MFA when signing in you will see “Enter a Code” and “Get a Push

Notification” for Okta Verify. Selecting the Code means you will have to open the Okta Verify App on your device and select the eyeball in order to receive your 6-digit code.



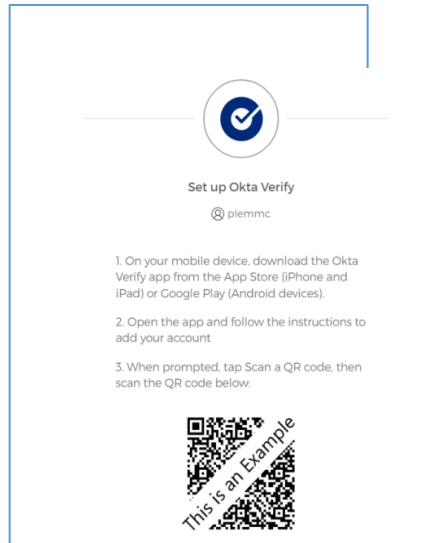
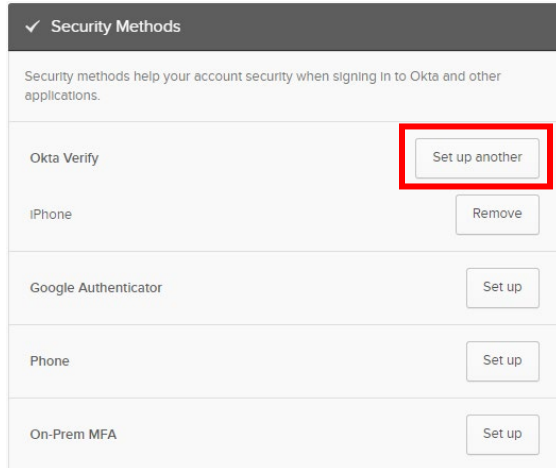
12. If you select “Get a Push Notification” you will receive a notice on your phone asking, “Did you Just Try to Sign In?” If you did click “Yes, It’s Me” to authenticate.

If you did not just sign in, be sure to select the “No, It’s Not Me” option to make sure that if someone else is trying to get into your account they do not get access to it.

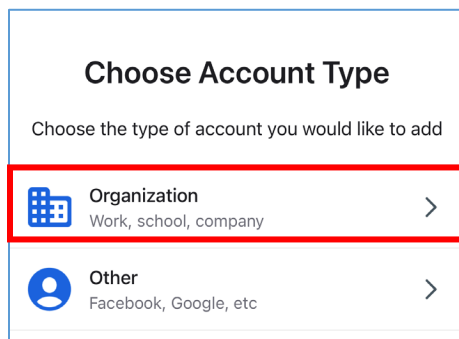


Okta Verify – though portal setup instructions

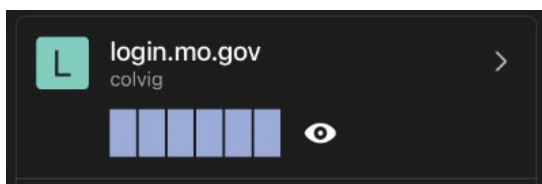
1. To start you can use either your state issued iPhone or download Okta Verify to your personal phone from your device’s app store.
2. Login to Okta Portal (login.mo.gov) Under the Security Methods section select either “Set up” or “Set up another” for Okta Verify. A new screen will appear with instructions and a QR code.



3. Open the app on the phone and choose “Organization” and approve the use of the device camera to scan to QR code. Once approved scan the QR code to complete the setup for Okta Verify.

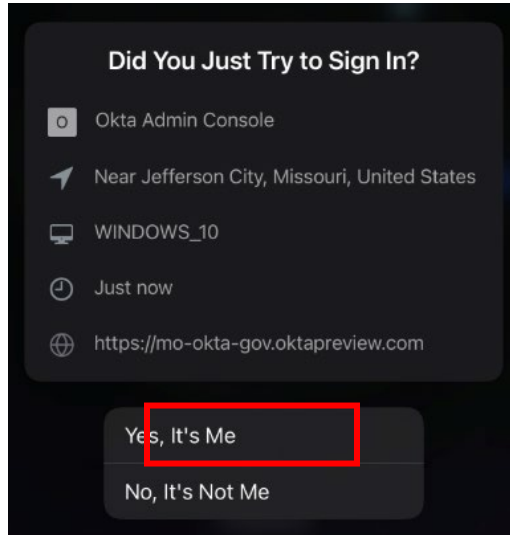
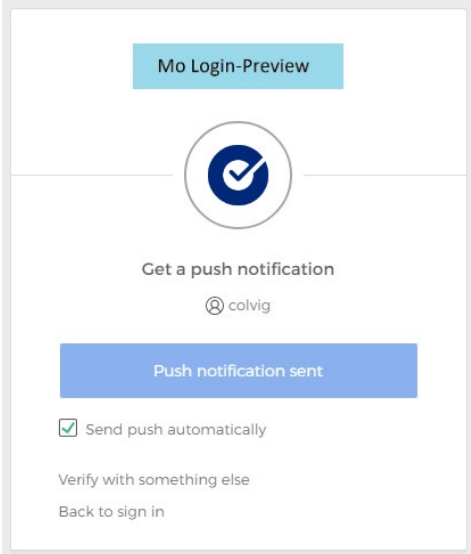


4. Your OTP for “login.mo.gov” will now display on the app dashboard. Clicking on the eye will reveal the OTP to use for authentication.



Push Notices

Okta Verify has an additional option once setup to use Push Notices. When attempting to access a service that requires MFA you will receive a notice on your phone asking, “Did you Just Try to Sign In?” and, only if you did, click “Yes, It’s Me” to authenticate.

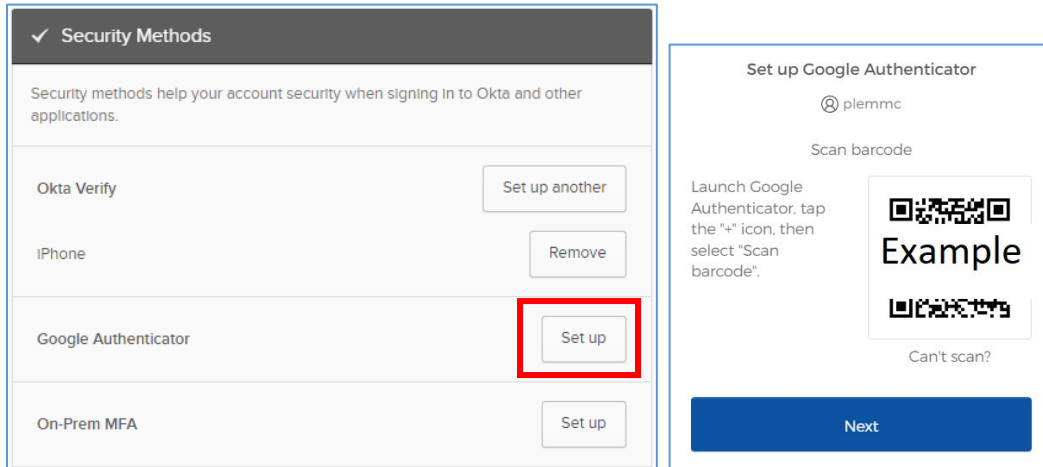


NOTE: Be aware of MFA Fatigue. If you did not access a service that requires MFA do not click "Yes, It's Me."

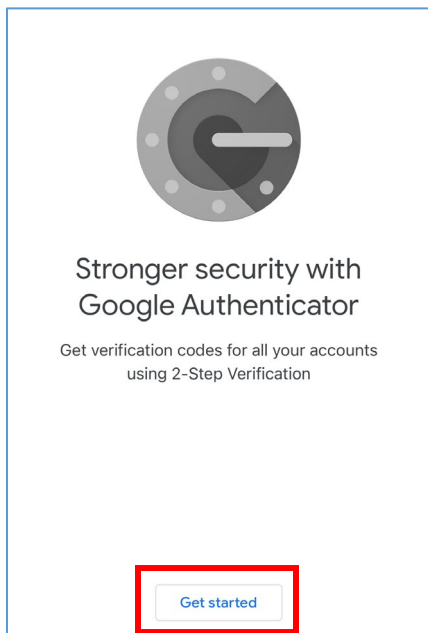
Google Authenticator

Google Authenticator

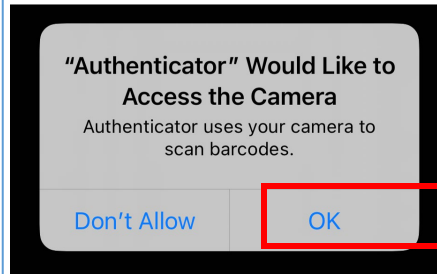
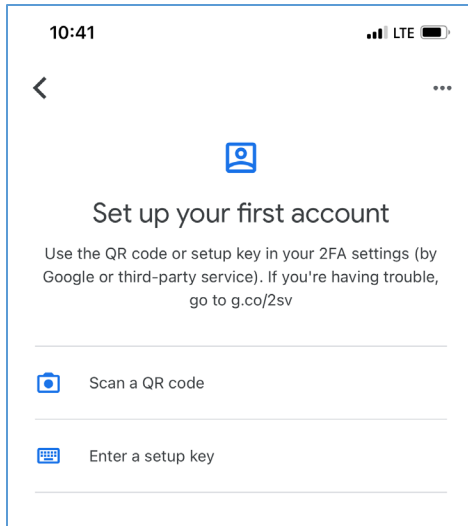
1. To setup Google Authenticator start with installing the app on your device from your device's app store. Google Authenticator is available for personal devices. All state managed devices should use Okta Verify.
2. Under the Security Methods section select "Set up" for Google Authenticator. A new screen will appear with instructions and a QR code.



3. Open the app on your device and select either "Get started" if this is your first time using Google Authenticator or the "+" in the lower right corner to add a new authenticator.

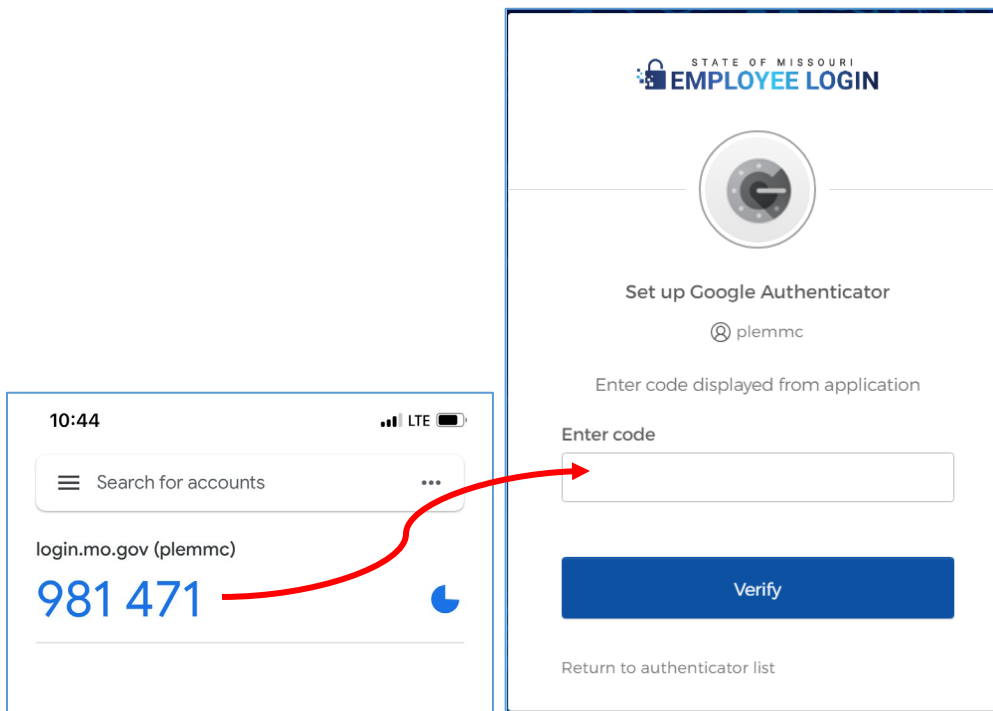


4. Open app and select the "Scan QR Code" option. Allow Authenticator to use the camera



5. Scan the code provided and select "Next"

6. Enter in the 6 digit code provided in the app in the "Enter Code" section of your web browser and select "Verify".



7. Your Google Authenticator is now associated with your Okta account and can be used for MFA requirements as needed.

Phone (SMS or CALL) - DEPRECATED

Phone (Text Message (SMS) or Voice Call) - DEPRECATED

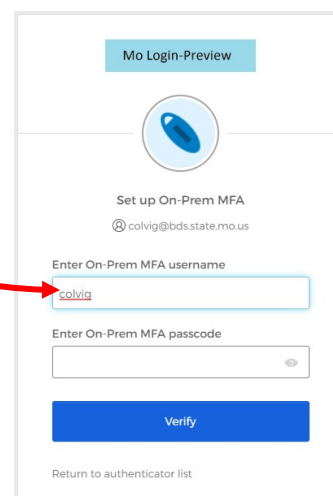
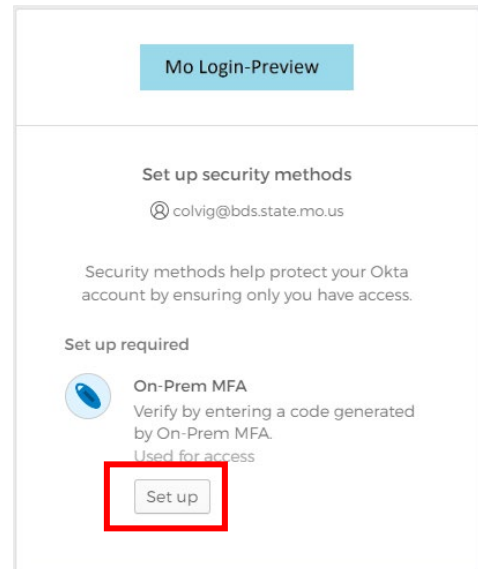
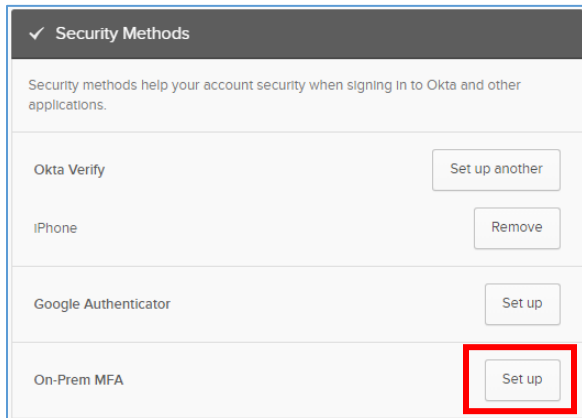
New enrollments for SMS stopped 9/13/2024

SMS support stops 12/31/2024

On-Prem MFA (RSA Physical Token)

On-Prem MFA (RSA Token)

1. Request a hard token with an ITSD Service Portal ticket to “Service Catalog Requests OA / Computer Equipment / VDI / VDI RSA Token-Request”
2. Once you received the hard token login to Okta and go to settings.
3. Click Setup for On-Prem MFA.
4. Click Setup
4. Enter the code on the hard token in the indicated field.



Authentication Process

Most Okta integrated connections are intuitive and straight forward with username, password, and MFA. A few services have unique steps to follow. For these services, please follow the appropriate connection instructions. <https://distributedteams.mo.gov/connectivity-2/>

- VPN Connection
- VDI Connection

Acronyms

- 2FA – Two-Factor Authentication
- MFA – Multi-Factor Authentication
- OTP – One Time Password
- SSO – Single Sign-On
- DSSO – Desktop Single Sign-On
- OWA – Outlook Web App
- VPN – Virtual Private Network
- VDI – Virtual Desktop Infrastructure
- QR – Quick Response
- RSA – Rivest-Shamir-Adleman