STATE OF MISSOURI

OTKA USER GUIDE

CONTENTS

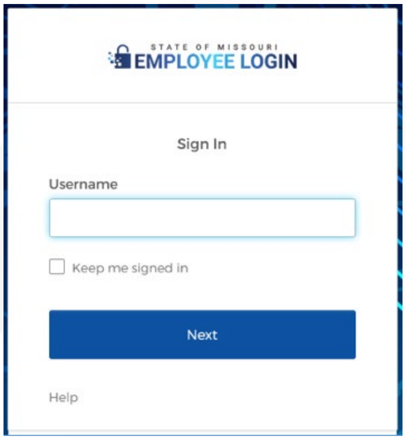
Legal Notice

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 only 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. However, 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 can login to their Okta Portal at https://login.mo.gov using their Active Directory (AD) credentials, username and password.

NOTE: Approximately 1% of users will have to use full username@domain.
Examples: **user1@ads.state.mo.us, user2@bds.state.mo.us, user3@cds.state.mo.us**



STATE OF MISSOURI EMPLOYEE LOGIN

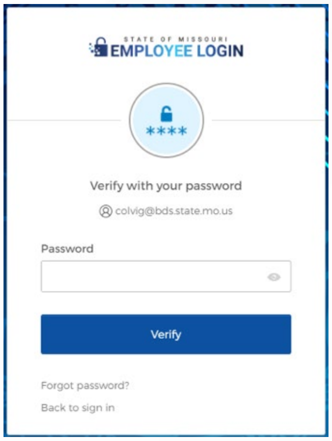
Sign In

Username

□ Keep me signed in

Next

Help



STATE OF MISSOURI EMPLOYEE LOGIN

Verify with your password

colvig@bds.state.mo.us

Password

Verify

Forgot password?

Back to sign in

Setting up MFA/2FA

Reasons to setup MFA/2FA

Multi-Factor Authentication (MFA) also known as Two-Factor Authentication (2FA) is 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 Outlook Web App (OWA) – also known as WebMail.

MFA Options

There are five MFA options available. It is recommended to setup two, and only two for your account.

Top Recommendations

1. Okta Verify and Phone (SMS)
2. Google Authenticator and Phone (SMS)

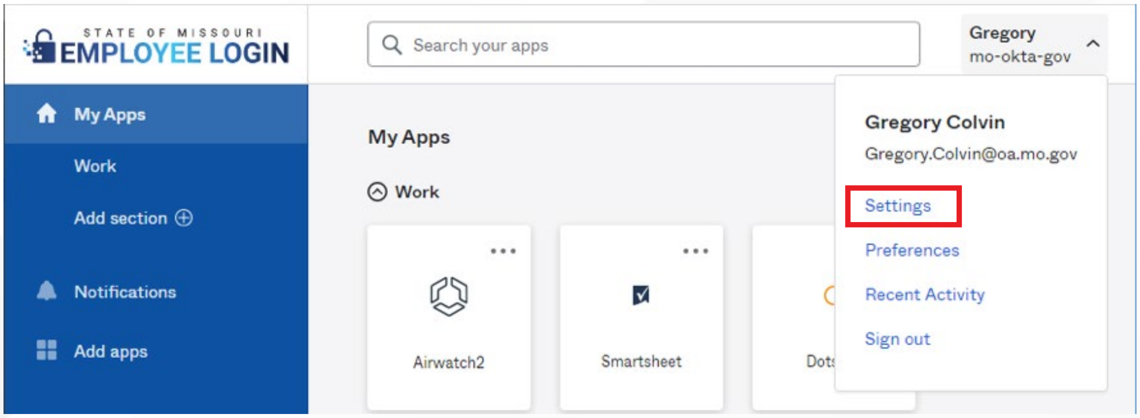
NOTE: Okta Verify is the most user friendly and SMS provides a backup

For users with unique circumstances we also have Voice Calling, 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



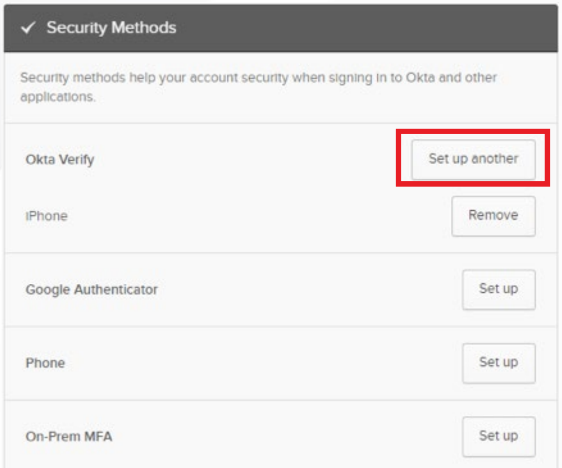
Setup Your MFA Options

A. Okta Verify
B. Google Authenticator
C. Phone (Text Message (SMS) or Voice Call)
D. On-Prem MFA (RSA Physical Token)

OKTA Verify

1. Okta Verify is the preferred and most secure method of MFA, and the required MFA option for state managed devices. To start you can use either your state issued iPhone or download Okta Verify to your personal phone from your device's app store.

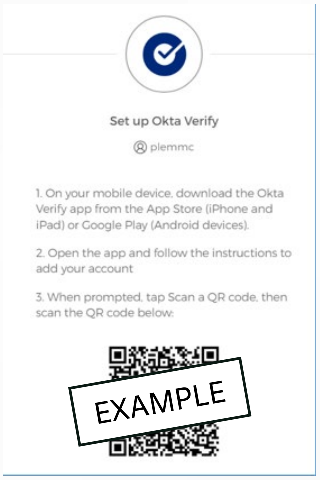
2. Under the Security Methods section select either "Set up" or "Set up another" for Okta Verify. After you authenticate with your password and other existing MFA (only if you have one setup already), a new screen will appear with instructions and a QR code.



✓ Security Methods

Security methods help your account security when signing in to Okta and other applications.

Okta Verify	Set up another
iPhone	Remove
Google Authenticator	Set up
Phone	Set up
On-Prem MFA	Set up



Set up Okta Verify

plemmc

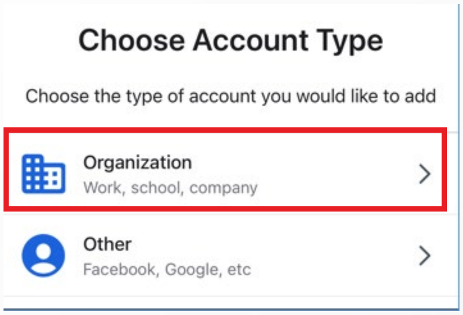
1. On your mobile device, download the Okta Verify app from the App Store (iPhone and iPad) or Google Play (Android devices).

2. Open the app and follow the instructions to add your account

3. When prompted, tap Scan a QR code, then scan the QR code below:

EXAMPLE

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.



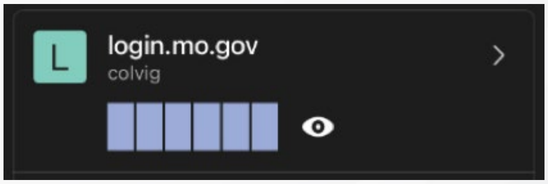
Choose Account Type

Choose the type of account you would like to add

Organization
Work, school, company

Other
Facebook, Google, etc

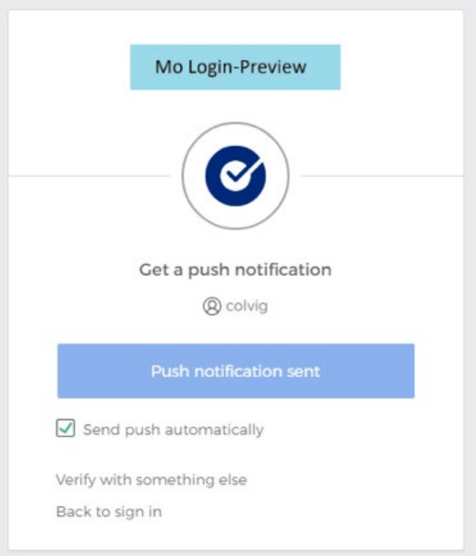
4. Your OTP for "login.mo.gov" will now display on the app dashboard. Clicking on the eye will reveal the OTP to use for authentication.



login.mo.gov
colvig

Push Notices

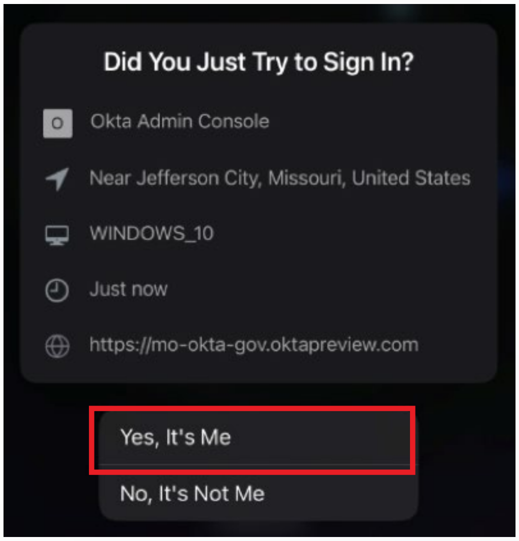
Okta Verify has an additional option once setup to use Push Notices. When attempting to access a service that requires MFA you will receive a notice on your phone asking "Did you Just Try to Sign In?" and only if you did click "Yes, It's Me" to authenticate.



Mo Login-Preview

Get a push notification

colvig



Did You Just Try to Sign In?

Okta Admin Console

Near Jefferson City, Missouri, United States

WINDOWS_10

Just now

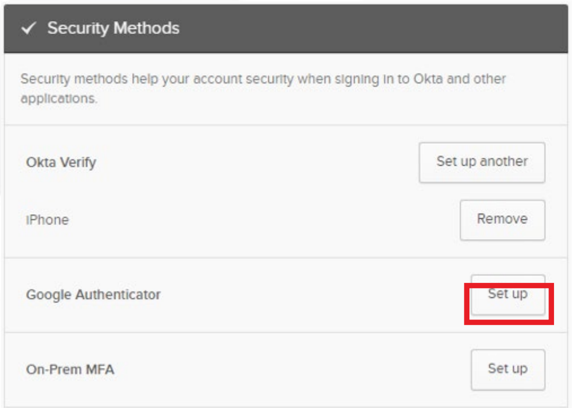
https://mo-okta-gov.oktapreview.com

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

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.

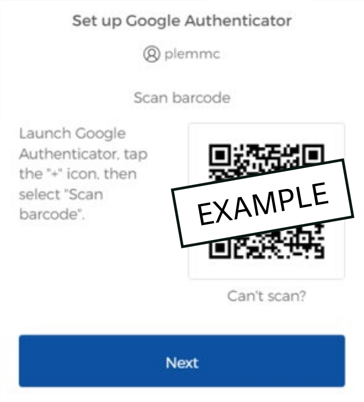
2. Under the Security Methods section select "Set up" for Google Authenticator. After you authenticate with your password and other existing MFA (only if you have one setup already), a new screen will appear with instructions and a QR code.



✓ Security Methods

Security methods help your account security when signing in to Okta and other applications.

Okta Verify	Set up another
iPhone	Remove
Google Authenticator	Set up
On-Prem MFA	Set up



Set up Google Authenticator

plemmc

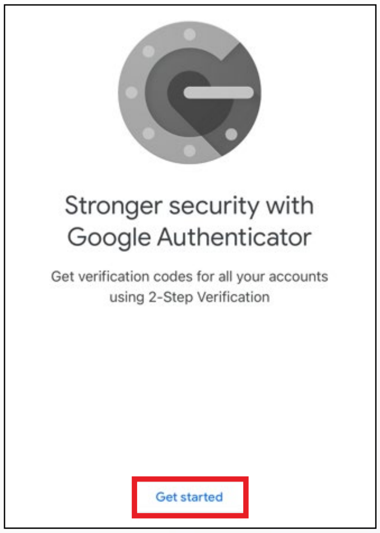
Scan barcode

Launch Google Authenticator, tap the "+" icon, then select "Scan barcode".

Can't scan?

Next

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.

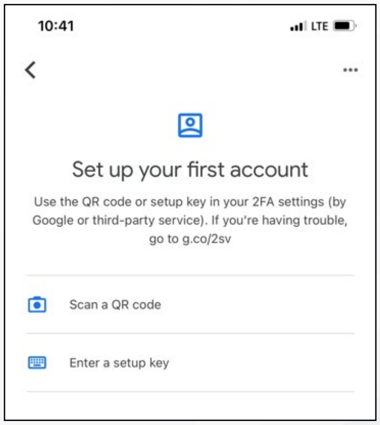


Stronger security with Google Authenticator

Get verification codes for all your accounts using 2-Step Verification

Get started

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



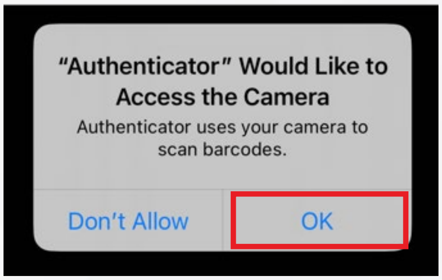
10:41 LTE

Set up your first account

Use the QR code or setup key in your 2FA settings (by Google or third-party service). If you're having trouble, go to g.co/2sv

Scan a QR code

Enter a setup key



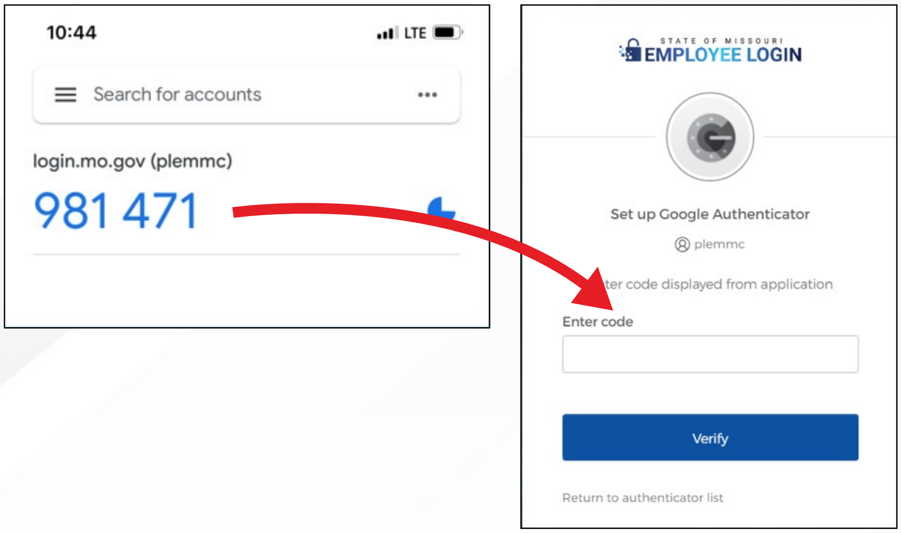
"Authenticator" Would Like to Access the Camera

Authenticator uses your camera to scan barcodes.

Don't Allow | OK

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”.



10:44

login.mo.gov (plemmc)

981 471

STATE OF MISSOURI EMPLOYEE LOGIN

Set up Google Authenticator

plemmc

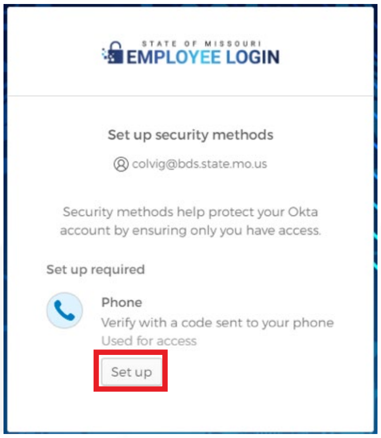
ter code displayed from application

Enter code

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

Phone (Text Message (SMS) or Voice Call)

1. To setup a phone select the Phone option from the settings menu then select Set Up.



STATE OF MISSOURI EMPLOYEE LOGIN

Set up security methods

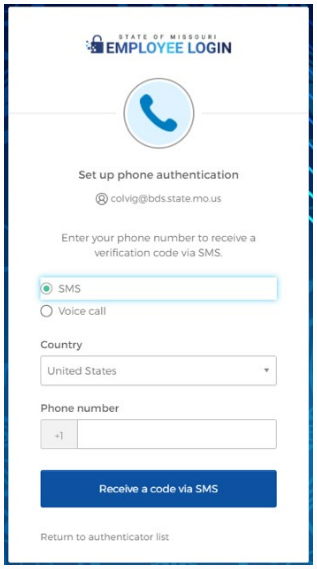
colvig@bds.state.mo.us

Security methods help protect your Okta account by ensuring only you have access.

Set up required

Phone
Verify with a code sent to your phone
Used for access

2. Select either SMS (text message) or Voice Call for your method of receiving the code. You can only select one. Then put in the phone number to receive the text or call and click to receive a code.



STATE OF MISSOURI EMPLOYEE LOGIN

Set up phone authentication

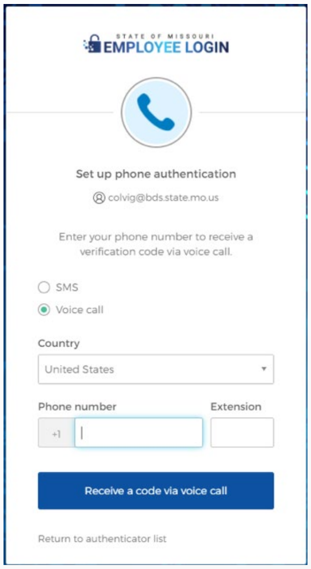
colvig@bds.state.mo.us

Enter your phone number to receive a verification code via SMS.

● SMS
○ Voice call

Country: United States

Phone number: +1



STATE OF MISSOURI EMPLOYEE LOGIN

Set up phone authentication

colvig@bds.state.mo.us

Enter your phone number to receive a verification code via voice call.

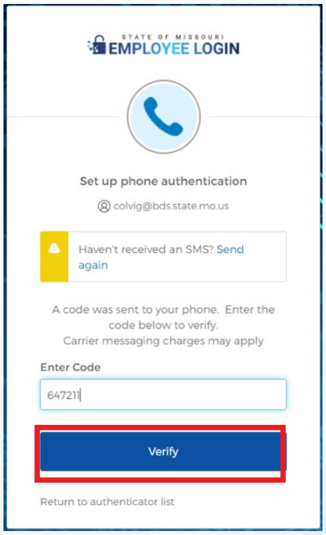
○ SMS
● Voice call

Country: United States

Phone number: +1

Extension

3. You will receive either a text or voice call depending on your selection. Put the provided code into the Enter Code box and click Verify. Your device is now synced to your Okta account and this method of MFA can be used to access services that will require MFA.



STATE OF MISSOURI EMPLOYEE LOGIN

Set up phone authentication

colvig@bds.state.mo.us

Haven't received an SMS? Send again

A code was sent to your phone. Enter the code below to verify.
Carrier messaging charges may apply

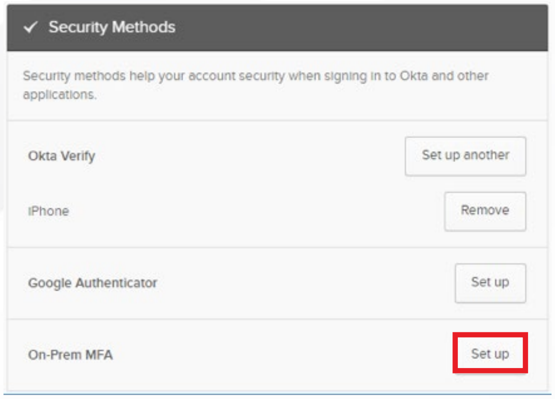
Enter Code: 647211

On-Prem MFA (RSA Physical 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.



✓ Security Methods

Security methods help your account security when signing in to Okta and other applications.

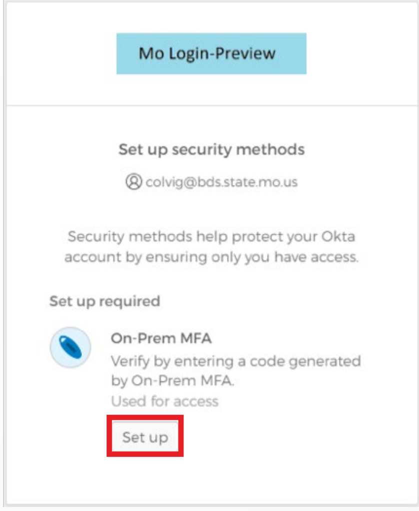
Okta Verify — Set up another

iPhone — Remove

Google Authenticator — Set up

On-Prem MFA — Set up

4. Click Setup



Mo Login-Preview

Set up security methods

colvig@bds.state.mo.us

Security methods help protect your Okta account by ensuring only you have access.

Set up required

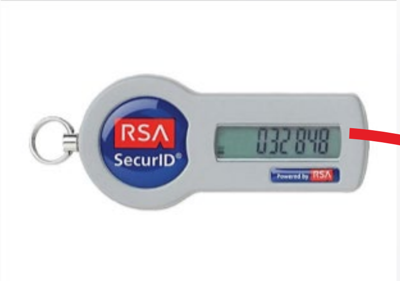
On-Prem MFA

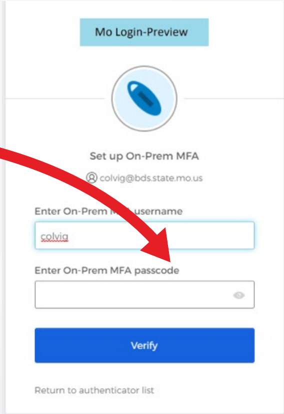
Verify by entering a code generated by On-Prem MFA.

Used for access

Set up

5. Enter the code on the hard token in the indicated field.





Mo Login-Preview

Set up On-Prem MFA

colvig@bds.state.mo.us

Enter On-Prem MFA username: colvig

Enter On-Prem MFA passcode

Verify

Return to authenticator list

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.

- Okta VPN Guide
- Okta VDI Guide

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