

# Login.Mo.Gov

## The Workforce Portal

Powered by Okta

### CONTENTS

[Legal Notice](#) ..... 1

[RSA Secure ID](#).....2

[Logging In](#) .....2

[Desktop Single Sign-On \(DSSO\)](#) .....2

[Setting up MFA](#) .....2

[Reasons to setup MFA](#) .....2

[MFA Options](#) .....3

[Setup Your MFA Options](#) .....3

[Okta Verify](#) ..... 4

[Push Notices](#) .....5

[Google Authenticator](#) ..... 6

[Phone \(Text Message \(SMS\) or Voice Call\)](#) ..... 8

[On-Prem MFA \(RSA Token\)](#) ..... 9

ACRONYMS .....10

### 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.

# RSA SecureID

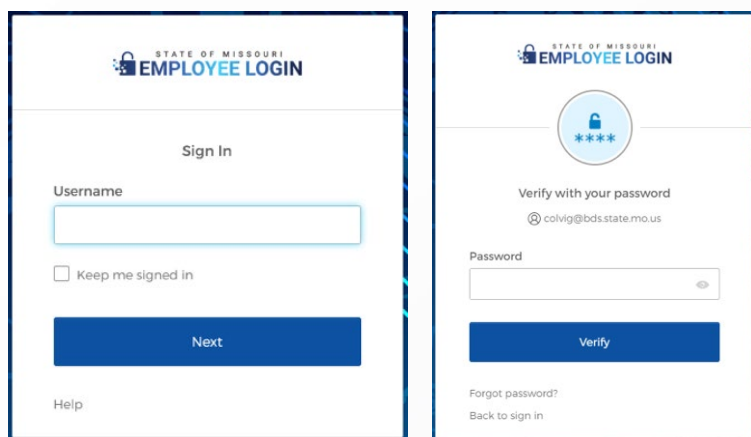
With the advent of Okta the use of RSA SecureID Soft Tokens will be discontinued. Users of RSA SecureID Soft Tokens will need to configure their Okta account with a new MFA option to maintain connectivity to state resources.

## Logging In

All users under OA can login to the Okta Portal at <https://login.mo.gov> using their Active Directory (AD) credentials, username@domain and password.

*Example: users1@bds.state.mo.us*

Employees can only login to the portal from a PC connected to the state network. Being connected to the state network can be physically while in a state building, wirelessly while in state building, if connected to mo.gov Wi-Fi, or remotely via VPN or VDI. Any attempts from off network will generate an unauthorized error or error code 403.



The image displays two side-by-side screenshots of the 'STATE OF MISSOURI EMPLOYEE LOGIN' portal. The left screenshot shows the 'Sign In' page with a 'Username' input field, a 'Keep me signed in' checkbox, and a blue 'Next' button. The right screenshot shows the 'Verify' page with a 'Password' input field and a blue 'Verify' button. Both pages include a 'Forgot password?' link and a 'Back to sign in' link.

## Desktop Single Sign-On (DSSO)

Once fully implemented DSSO will authenticate users to the Employee Portal without the user needing to input credentials. From the portal users will be able to access assigned applications and change settings to configure Multi-Factor Authentication (MFA) options.

## Setting up MFA

### Reasons to setup MFA

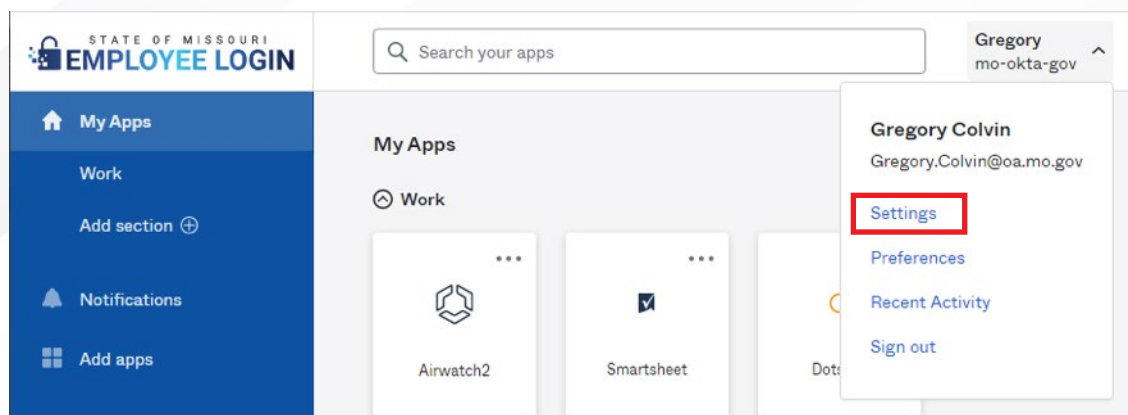
The initial use cases for Multi-Factor Authentication (MFA) will be for our remote users and OA-ITSD Administrators. If you are one of these users you can preemptively setup your MFA in preparation for the migration of services that will require MFA.

The remote use cases that will need MFA are VPN, VDI, and OWA. While all users with a valid state email address have access to Outlook on the web (OWA), also known as Webmail, not everyone uses it. If you do not use OWA then you do not need to setup MFA at this time. If at a future date you want to setup MFA you will need to do so from a PC connected to the state network.

## MFA Options

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>



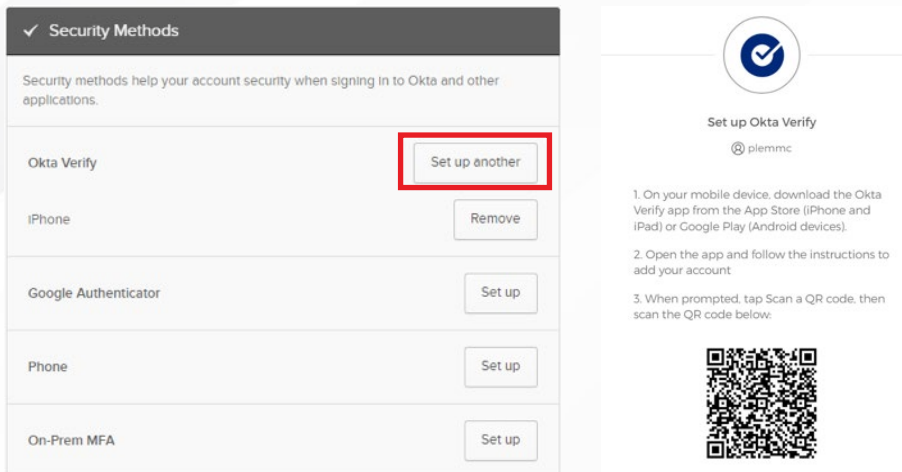
## Setup Your MFA Options

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

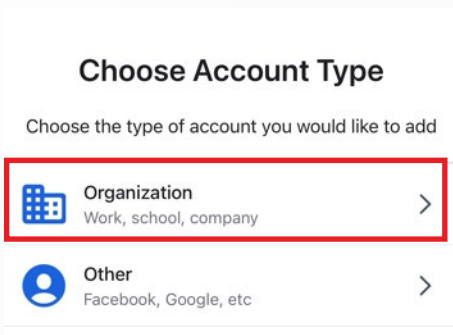
# OKTA Verify

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.

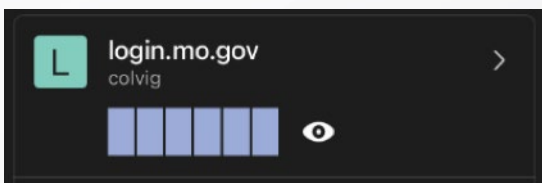
2. Under the Security Methods section select either "Set up" or "Set up another" for Okta Verify. A new screen will appear with instructions and a QR code.



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.

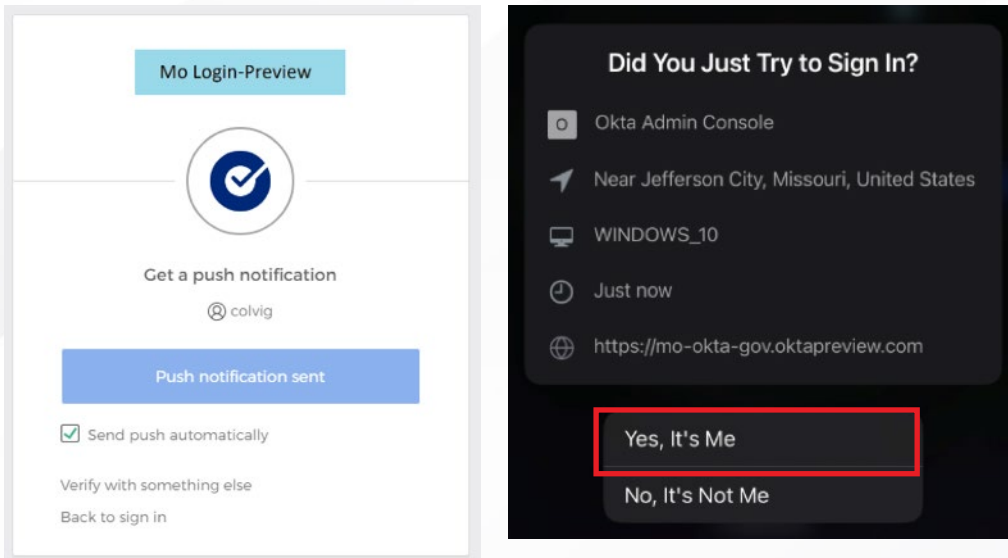


4. Your OTP for "login.mo.gov" will now display on the app dashboard. Clicking on the eye will reveal the OTP to use for authentication.



## 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.

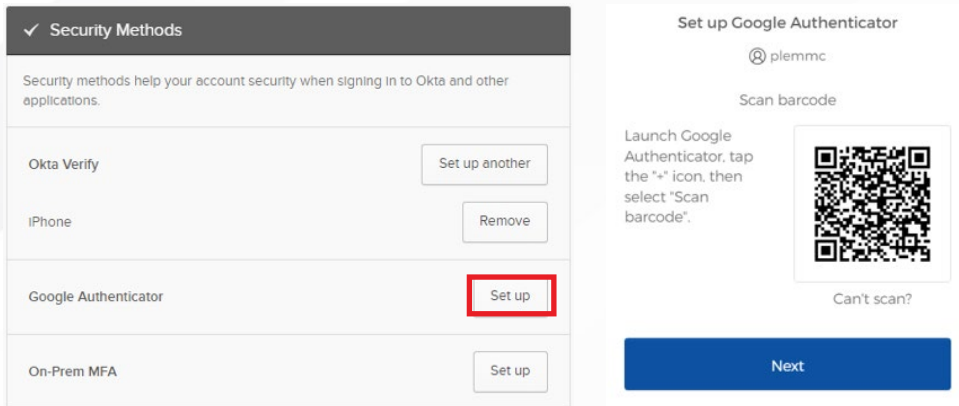


NOTE: Be aware of MFA Fatigue. If you did not access a service that requires MFA do not click “Yes, It’s Me.” Refer to NINJIO Cybersecurity Training [S7|E12 “Game Day Decision”](#) for more information.

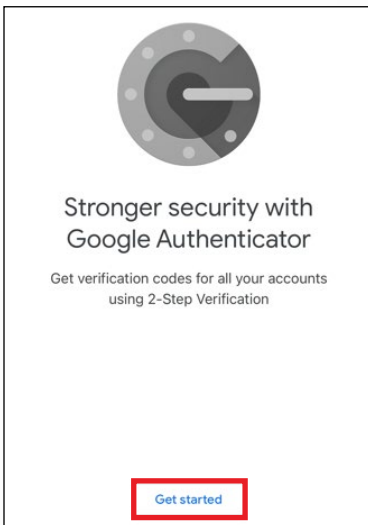
# Google Authenticator

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.

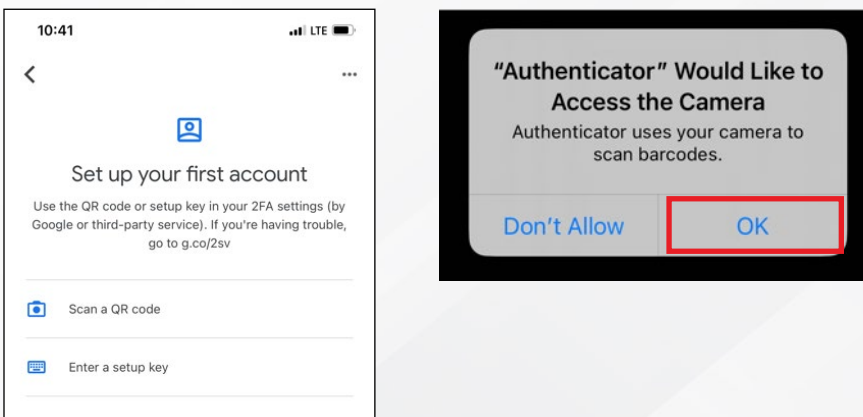
2. Under the Security Methods section within the Okta portal, select "Set up" for Google Authenticator. A new screen will appear with instructions and a QR code.



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.

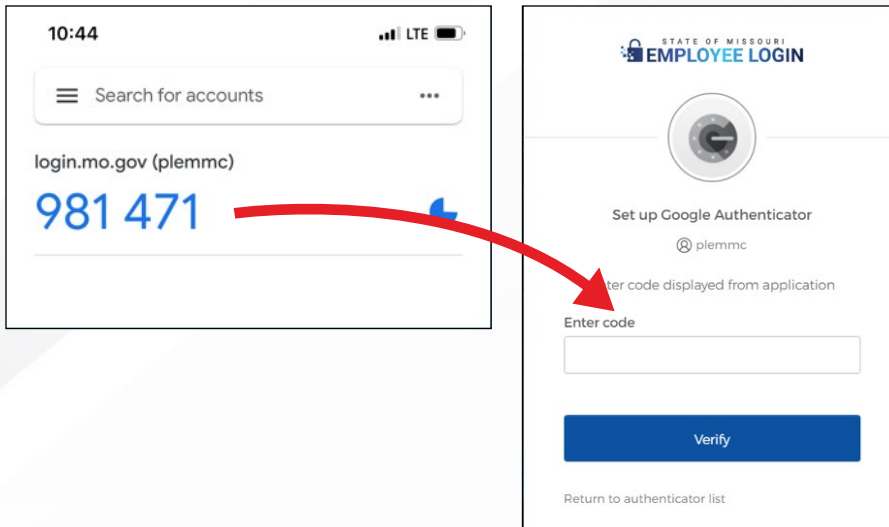


4. Open app and select the "Scan QR Code" option. Allow Authenticator to use the camera



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".

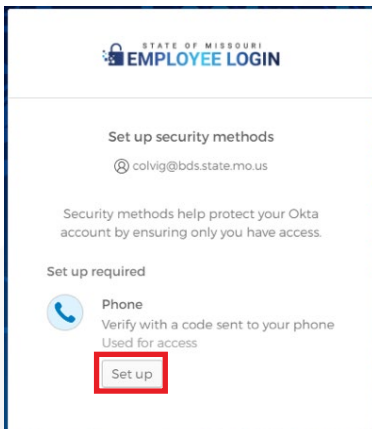


7. Your Google Authenticator is now associated with your Okta account and can be used for MFA requirements as needed.



# Phone (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

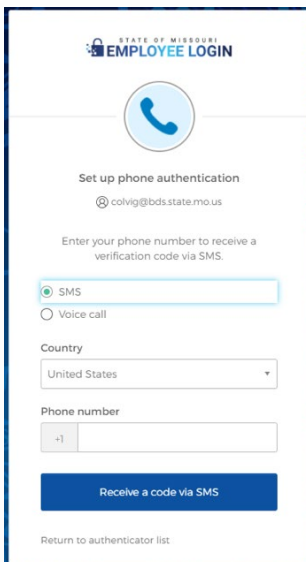
Security methods help protect your Okta account by ensuring only you have access.

Set up required

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

Set up

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.

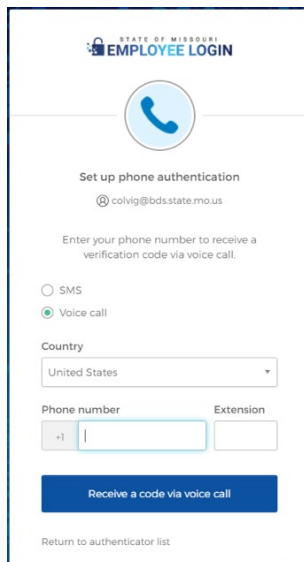
☒ SMS  
☐ Voice call

Country  
United States

Phone number  
+1

Receive a code via SMS

Return to authenticator list



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

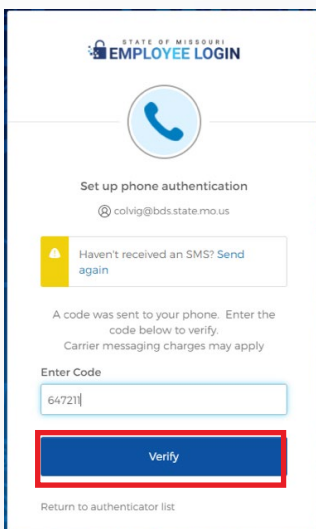
Phone number  
+1

Extension

Receive a code via voice call

Return to authenticator list

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  
64721

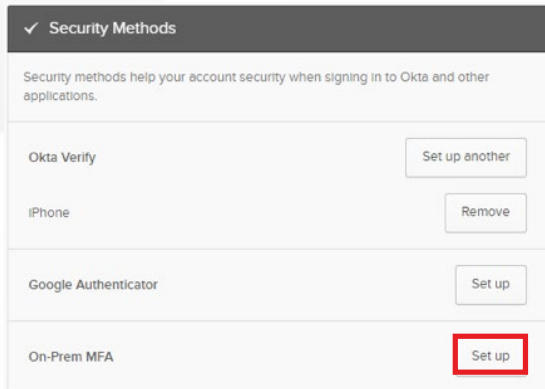
Verify

Return to authenticator list

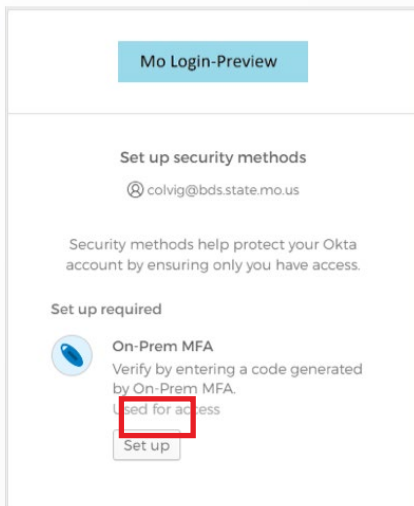


# On-Prem MFA (RSA Physical Token)

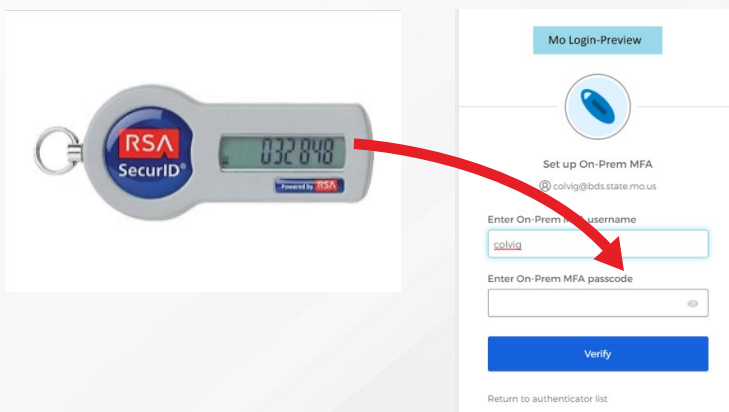
1. Request a hard token with an ITSD Service Portal ticket to  
"Service Catalog Requests OA / Computer Equipment / VDI / VDI RSA Token-Request"
2. Tokens will be delivered to your business office address and may take up to two weeks for processing and shipping. Once you have received the hard token, login to Okta and go to settings.
3. Click Setup for On-Prem MFA.



4. Click Setup



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



# ACRONYMS

- IAM – Identity and Access Management
- 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