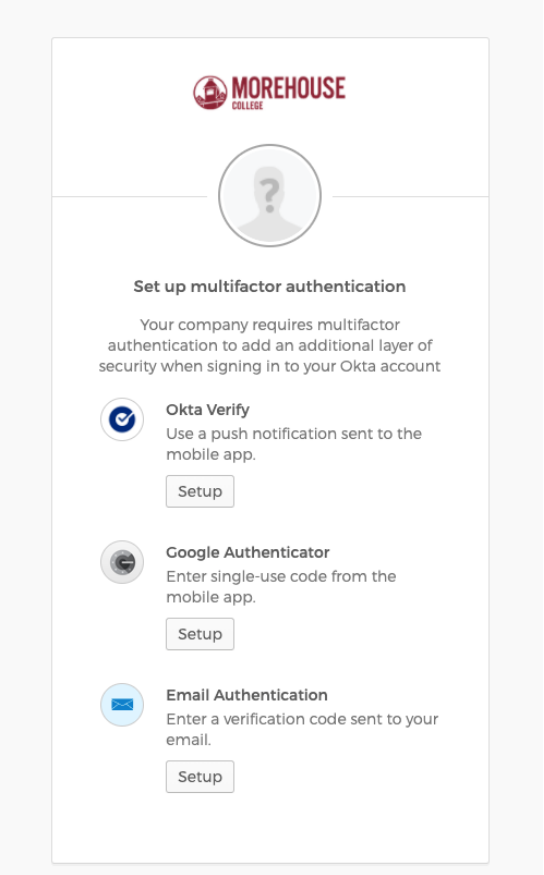
Setting Up and Authenticating with Multi-factor Authentication (MFA)

In addition to your username and password, Okta MFA prompts you for a second factor before logging you in. The product supports a variety of factor options.



OKTA VERIFY (RECOMMENDED)

Okta Verify is a mobile app that verifies your identity in one of two ways. Okta can send you a push notification that you approve using Okta Verify. Alternatively, Okta Verify can generate a six-digit code that you enter into your Okta login screen to access your required app.

Install Okta Verify

1. Download the Okta Verify app from the Apple App Store or Google Play onto your primary mobile device.
2. Using your computer's browser, navigate to your organization's Okta page, e.g. [company.okta.com].
3. Fill in your company-issued credentials and click **Sign In.**
4. When prompted to enroll in Okta Verify, open the Okta Verify app on your phone and scan the barcode that appears in your computer's browser.
5. The next time you log into Okta, it should offer to send you a push notification or ask you for a numeric code. If you choose the push notification, then approve it when it arrives on your phone. If you choose to use the code, then access the code in Okta Verify and enter it into your browser.

Note: You can only register Okta Verify on one device at a time. Authenticating on a second device cancels authorization for the first one.

Prefer a video walkthrough?

- View Video Overview: Set up Okta Verify with Push for MFA
- View Video Overview: Set up Okta Verify, OTP for MFA

GOOGLE AUTHENTICATOR

This is a third-party app that generates a six-digit code for you to type into your Okta login screen. You have 30 seconds to input the code before it generates another. If you miss the window, use the next code to log in. After five unsuccessful attempts, Okta will lock your account for protection and you must contact an administrator for help.

Set up Google Authenticator

1. Using your browser, navigate to your organization's Okta page, e.g. [company.okta.com].
2. Fill in your company-issued credentials and click **Sign In.**
3. You will see a prompt on your device that "Extra verification is required for your account"
4. Click **Setup** or **Configure Factor.**
5. On the **Set Up Google Authenticator** screen, click the device type icon. Click **Next.** A barcode will appear on your screen.

Install the Google Authenticator app on your device

1. On your mobile device, open the Apple App Store or Google Play and install Google Authenticator.
2. Open the Google Authenticator app.
3. Tap **Scan a Barcode**. (You might need to install a barcode scanner app; follow the prompts and then re-tap **Scan a Barcode**.)
4. Hold your device up to the computer screen and scan the barcode.
5. Click **Next**.
6. Type the Google Authenticator code that appears on your mobile device into the **Setup Google Authenticator** screen on your computer and click **Verify**.

Prefer a video walkthrough?

- View Video Overview: Set up Google Authenticator for MFA

EMAIL AUTHENTICATION

Although we do offer email as a factor for convenience and to help our customers migrate from legacy identity platforms, we do not consider it to be a secure, modern method for secondary authentication. We strongly recommend against turning on email authentication. This experience is an insecure method of additional verification because:

- Third parties can compromise email addresses.
- Email often travels in plain text using insecure protocols.
- People often use email for primary credential recovery.

Set up email authentication

1. Using your browser, navigate to your organization's Okta page, e.g. [company.okta.com].
2. Fill in your company-issued credentials and click **Sign In**.
3. You will see a prompt on your device that "Extra verification is required for your account"
4. Click **Setup** or **Configure Factor.**
5. Choose **Email**. Type in your email and click **Verify**.

Having trouble?

If you're having trouble setting up any of these factors, we recommend contacting servicedesk@morehouse.edu or the IT admin directly.