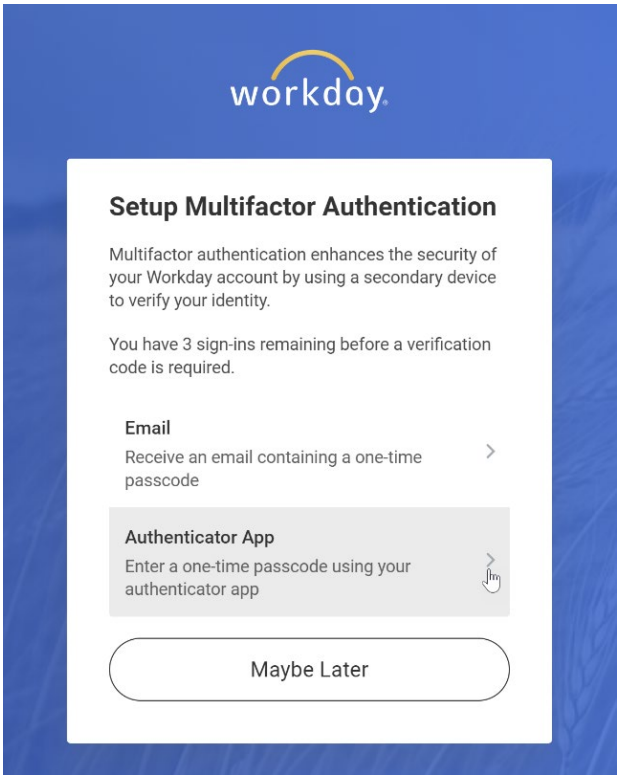
THIS GUIDE IS FOR: Service Desk, Security Provisioning, terminated, retired or external employees

Multifactor authentication for terminated employees

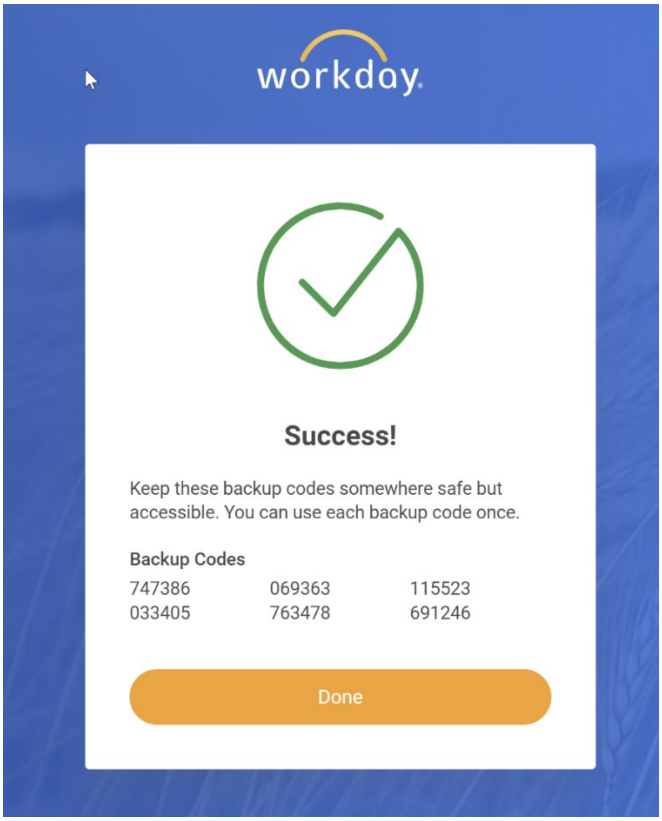
When an employee is terminated or retires, agency HR will be prompted to update the employee's personal email address. When the termination is complete, the employee will receive a username and password to use with the Non-Active Employee Sign-In.

1. User selects Non-Active Employee Sign-In.
2. User enters the username and password given in the email.
    a. NOTE: If the user does not receive the email with credentials, they can contact the OMES Service Desk for a password reset.
3. If the user is chosen for multifactor authentication, they will be given two options:



    a. The email option will go to the employee's work email address and they will likely be unable to access this. **DO NOT USE THIS OPTION.**
    b. The Authenticator App will require that the user download a third-party app such as Google Authenticator or 2FAS. These options are free.
4. The system will provide a QR code. The user will use the third-party app to scan the QR code.

5. The employee will enter the six-digit code generated by the app, then select **Next**.
6. The employee should save the backup codes they see on the screen. This will get them back into Workday in case they lose their device.



7. Select **Done**.