WE ARE YOUR DOL

NEW YORK STATE OF OPPORTUNITY. Department of Labor

Instrucciones de configuración de la autenticación multifactorial

El Estado de Nueva York ha empezado a utilizar autenticación multifactorial (MFA, por sus siglas en inglés) en algunas de sus aplicaciones de acceso público.

La MFA es una manera de ayudar a garantizar la seguridad y protección de su cuenta. Requiere un segundo factor para demostrar que usted es quien dice ser, además de una simple contraseña. Si está usando una aplicación protegida con MFA, incluso si alguien lograra adivinar o robar su contraseña aún no podría iniciar sesión sin su segundo factor. Mientras que una contraseña es algo que usted sabe, el segundo factor es algo que usted es (generalmente medido con un dispositivo biométrico) o algo que usted tiene.

Este documento tiene la intención de indicarle cómo ayudar a los clientes a configurar su autenticación multifactorial en sus cuentas de NY.gov.

ÍNDICE

Configuración de la autenticación multifactorial con Google Authenticator

Si aún no está inscrito en MFA, se le pedirá que se inscriba después de iniciar sesión en los servicios en línea de trabajo y hacer clic en la aplicación "Unemployment Services".

En la pantalla de su computadora verá una ventana que le pedirá configurar su autenticación multifactorial.

- Descargue la aplicación Google Authenticator en su teléfono inteligente. Vea más adelante las instrucciones para descargar la aplicación.
- En la pantalla de su computadora, haga clic en **Setup (Configurar)** en Google Authenticator para iniciar el proceso de configuración.
- Seleccione iPhone o Android, dependiendo de su dispositivo.
    - Se le indicará que descargue la aplicación móvil Google Authenticator de la tienda Google Play Store (Android) o App Store (iPhone). Si aún no lo ha hecho, debe descargar esta aplicación ahora. Vea a continuación las instrucciones para descargar la aplicación.

  CONSEJO: si tiene una tableta de Apple, seleccione iPhone.
- Oprima el botón **Next (Siguente).**
- **Siga estas instrucciones para descargar la aplicación móvil Google Authenticator en un dispositivo Android (Google Play) o en un dispositivo Apple (App Store).**
- En su teléfono inteligente o tableta, diríjase a Google Play (Android) o a la App Store (dispositivo Apple). Asegúrese de que su teléfono inteligente o tableta cuenta con la versión más reciente del sistema operativo (OS).
- En Google Play (Android) o en la App Store (Apple), busque la aplicación móvil Google Authenticator.
- Seleccione la aplicación móvil Google Authenticator.
- Descargue e instale la aplicación móvil.
- Una vez que instale la aplicación móvil Google Authenticator en su teléfono inteligente o tableta, diríjase a la aplicación en su dispositivo y ábrala. *(NOTA: la aplicación puede tener un aspecto ligeramente distinto, dependiendo de la versión del teléfono)*
- **Siga estas instrucciones para usar la aplicación móvil Google Authenticator en su teléfono inteligente o tableta.**
- Después de elegir si su dispositivo es Apple o Android en la pantalla de su computadora, aparecerá un cuadro de diálogo con un código de respuesta rápida (QR, por sus siglas en inglés). El código QR tiene el aspecto de un cuadrado relleno de puntos negros.

  - Si no puede escanear el código QR en su teléfono inteligente o tableta, haga clic en la opción **Can't Scan? (¿No puede escanear?)** debajo del código QR en la pantalla de su computadora.
- Si puede escanear el código QR en su teléfono inteligente o tableta, diríjase a su aplicación móvil Google Authenticator y ábrala, si aún no está abierta.
- Haga clic en **Get Started (Comenzar)**.
- Recibirá las siguientes opciones: **Scan a QR code (Escanear un código QR)** o **Enter a setup key (Escribir una clave de configuración).** Elija una.

  CONSEJO: si no puede escanear el código, seleccione **Enter a setup key (Escribir una clave de configuración).** Vea a continuación las instrucciones para escribir una clave de configuración.
- Si tiene un teléfono Android, la aplicación le pedirá permiso para usar su cámara. Oprima "While Using the App" (Mientras se usa la aplicación).
- Si tiene un dispositivo Apple, verá un mensaje que dice: *"Authenticator" Would Like to Access the Camera (Authenticator quiere usar la cámara)*. Haga clic en OK.
- Después de darle permiso a su teléfono para usar la cámara, la pantalla de su teléfono inteligente mostrará una pantalla negra con un cuadrado en el centro.
- Apunte la cámara de su teléfono o tableta al código QR que está en la pantalla de su computadora, de modo que el código QR de la pantalla de su computadora aparezca en el cuadro verde de la pantalla de su teléfono. La aplicación escaneará automáticamente el código a su teléfono o tableta.
- **Siga estas instrucciones si seleccionó Enter a setup key (Escribir una clave de configuración) en la aplicación, en vez de escanear el código QR.**
- En la pantalla de su computadora aparecerá una clave secreta. Ese es el código que debe escribir en la aplicación Google Authenticator. Se le mostrará una pantalla que contiene instrucciones para escribir una clave de configuración.
- En su aplicación Google Authenticator verá una pantalla para escribir los detalles de la cuenta. En esa pantalla capture la siguiente información:
  - El nombre de su cuenta de NY.gov en el campo 'Account name' (Nombre de la cuenta).
  - Su clave secreta en el campo 'Your Key' (Su clave.
  - Seleccione 'Time-Base' (Por tiempo) en el menú desplegable Type of Key (Tipo de clave).
- Oprima el botón **Add (Añadir).**
- **Siga estas instrucciones para capturar el código de su aplicación Google Authenticator en su computadora.**

- Una vez que la aplicación escanee con éxito el código QR o que usted haya capturado con éxito la clave secreta en la aplicación móvil, la aplicación le mostrará una pantalla con su nombre de usuario y un código de seis dígitos. Ese es el código que deberá escribir en la computadora en los siguientes pasos. Este código cambiará cada 30 segundos.

- Escriba el código de seis dígitos de su aplicación en el campo Enter Code (Escribir código) en la pantalla de su computadora, y haga clic en **Verify (Verificar).**
- Se le dirigirá de nuevo a la pantalla de inscripción, en donde puede configurar otro método de autenticación multifactorial. Observe que Google Authenticator ya aparece debajo del encabezado "Enrolled factors" (Factores inscritos).

  CONSEJO: es recomendable que configure más de un método de autenticación multifactorial.

- Cuando haya configurado todos los métodos de autenticación multifactorial que desee, oprima el botón **Finish (Terminar).**

  CONSEJO: si va a configurar un método de autenticación multifactorial que usa una aplicación telefónica, descargue las aplicaciones antes de oprimir el botón **Setup (Configurar)** en la página "Set up multifactor authentication" (Configurar autenticación multifactorial) en su navegador. Los dos métodos de autenticación multifactorial que usan aplicaciones son Okta Verify y Google Authenticator.

Mensajes de error potenciales y cómo resolverlos.

- Mensaje de error: La sesión ha expirado.
- Remedio: El cliente debe volver a iniciar sesión.

- Mensaje de error: El token no coincide.
- Remedio:
  - El cliente debe revisar que sea correcto.
  - El cliente debe "enviar" el código de nuevo.

- Mensaje de error: Se encontró un error.
- Remedio: El cliente debe capturar el código.

- Mensaje de error: El código de barras no se escanea.
- Remedio:
  - Probar los métodos alternativos descritos.
    - "Enviar activación por mensaje de texto" – El cliente puede escribir

un número de teléfono.

- "Configurar manualmente sin enviar mensaje" – El cliente verá un código temporal.
- "Enviar correo electrónico de activación" – Se le enviará un correo electrónico al cliente a la cuenta que usó para crear su cuenta.
- Asegúrese de que el dispositivo del cliente permitió el acceso a la cámara

Regresar a la página principal

Configuración de la autenticación multifactorial con Okta Verify

En la pantalla de su computadora verá una ventana que le pedirá configurar su autenticación multifactorial.

- Descargue la aplicación Okta Verify en su teléfono inteligente. Vea más adelante las instrucciones para descargar la aplicación.
- En la pantalla de su computadora, haga clic en **Setup (Configurar)** en Okta Verify para iniciar el proceso de configuración.
- Seleccione iPhone o Android, dependiendo de su dispositivo.
    - Se le indicará que descargue la aplicación móvil Okta Verify de la tienda Google Play Store (Android) o App Store (iPhone). Si aún no lo ha hecho, debe descargar esta aplicación ahora. Vea a continuación las instrucciones para descargar la aplicación.

  CONSEJO: si tiene una tableta de Apple, seleccione iPhone.
- Oprima el botón **Next (Siguente).**
- **Siga estas instrucciones para descargar la aplicación móvil Okta Verify en un dispositivo Android (Google Play) o en un dispositivo Apple (App Store).**
- En su teléfono inteligente o tableta, diríjase a Google Play (Android) o a la App Store (dispositivo Apple). Asegúrese de que su teléfono inteligente o tableta cuenta con la versión más reciente del sistema operativo (OS).
- En Google Play (Android) o en la App Store (Apple), busque la aplicación móvil Okta Verify.
- Seleccione la aplicación móvil Okta Verify.
- Descargue e instale la aplicación móvil.
- Una vez que instale la aplicación móvil Okta Verify en su teléfono inteligente o tableta, diríjase a la aplicación en su dispositivo y ábrala.
- **Siga estas instrucciones para configurar la aplicación móvil Okta Verify en su teléfono inteligente o tableta.**

- La pantalla de su computadora mostrará un cuadro de diálogo con un código de respuesta rápida (QR, por sus siglas en inglés). El código QR tiene el aspecto de un cuadrado relleno de puntos negros.
    - Si no puede escanear el código QR, haga clic en la opción **Can't Scan? (¿No puede escanear?)** debajo del código QR en la pantalla de su computadora. Vea más adelante las instrucciones para configurar Okta Verify después de hacer clic en "Cant' Scan" (No puede escanear).
- Si puede escanear el código, diríjase a la aplicación móvil Okta Verify en su dispositivo y ábrala.
- Haga clic en **Get Started (Comenzar)**.
- Haga clic en **Next (Siguiente).**
- Haga clic en **Add Account (Añadir cuenta)**
- Haga clic en **Other (Otro)**.
- Recibirá las siguientes opciones: **Scan a QR code (Escanear un código QR)** o **Enter Key Manually (Escribir la clave).** Elija una.
    - Si elige **Enter Key Manually (Escribir la clave)**, deberá seguir los pasos que se muestran más adelante para "Verificar manualmente sin notificación *push*" de la lista desplegable de "Can't Scan" (No puede escanear).
- **Siga estas instrucciones para usar la aplicación móvil Okta Verify para escanear un código QR.**
- Si tiene un dispositivo Android, la aplicación le pedirá permiso para usar su cámara. Haga clic en OK.
- Si tiene un dispositivo Apple, verá un mensaje que dice: *"Okta Verify" Would Like to Access the Camera (Okta Verify quiere usar la cámara)*. Haga clic en OK.
- Apunte la cámara de su teléfono o tableta al código QR que está en la pantalla de su computadora. La aplicación escaneará automáticamente el código a su teléfono o tableta.
- En el monitor de su computadora verá la pantalla de inscripción con un mensaje emergente que contiene un código QR.
- En la aplicación Okta Verify, toque **Add Account (Añadir cuenta).**
- Apunte la cámara de su teléfono o tableta al código QR que está en la pantalla de su computadora.
- Después de escanear el código QR, aparecerá una nueva pantalla en su aplicación que le preguntará si desea permitir notificaciones *push.* Seleccione **Allow (Permitir)** o **Skip (Omitir)**.
- Después de escanear con éxito el código QR en su teléfono inteligente, la pantalla de su computadora indicará que ha escaneado el código con éxito.
- **Siga estas instrucciones para configurar Okta Verify por correo electrónico o mensaje de texto después de hacer clic en "Can't Scan"**

(No puede escanear).

- Después de hacer clic en **"Can't Scan" (No puede escanear)** en la pantalla de su computadora, verá una ventana que dice Setup Okta Verify (Configurar Okta Verify). En esta pantalla hay una lista desplegable que contiene las siguientes opciones: Send activation link via email (Enviar enlace de activación por correo electrónico), Send activation link via SMS (Enviar enlace de activación por mensaje de texto) y Setup Manually Without Push Notification (Configurar manualmente sin notificación *push*).

  CONSEJO: las instrucciones para configurar manualmente sin notificación *push* se encuentran más adelante.

- Haga clic en **Send activation link via email (Enviar enlace de activación por correo electrónico)** o **Send activation link via SMS (Enviar enlace de activación por mensaje de texto).** Se le enviará un enlace.
  CONSEJO: **debe** oprimir el enlace desde su teléfono inteligente o tableta.
- En su teléfono inteligente o tableta, vaya a su aplicación de correo electrónico o mensajes de texto para ver el enlace. Abra el correo electrónico o mensaje de texto que se le envió. Oprima el enlace que está en el mensaje.
- Lo llevará al sitio de internet de Okta Verify.
- Haga clic en **Get Started (Comenzar)**.
- Su teléfono inteligente se conectará al sitio de internet de Okta Verify y verificará el enlace. La pantalla de su computadora indicará que escaneó con éxito el código.
- **Use las siguientes instrucciones para configurar Okta Verify siguiendo el proceso "Verificar manualmente sin notificación *push*" de la lista desplegable de "Can't Scan" (No puede escanear).**
- Después de hacer clic en **"Can't Scan" (No puede escanear)** en la pantalla de su computadora, verá una ventana que dice Setup Okta Verify (Configurar Okta Verify). En esta pantalla hay una lista desplegable que contiene las siguientes opciones: Send activation link via email (Enviar enlace de activación por correo electrónico), Send activation link via SMS (Enviar enlace de activación por mensaje de texto) y Setup Manually Without Push Notification (Configurar manualmente sin notificación *push*).
- Seleccione la opción: Verify manually without push notification (Verificar manualmente sin notificación *push).*
- Aparecerá una pantalla que contiene una clave secreta.
- Abra su aplicación móvil Okta Verify.
- Haga clic en **Get Started (Comenzar)**.
- Haga clic en **Next (Siguiente).**
- Haga clic en **Add Account (Añadir cuenta)**
- Haga clic en **Other (Otro)**.

- Seleccione Enter Key Manually (Capturar clave manualmente).
- Escriba el código de la pantalla de su computadora en la pantalla de su teléfono inteligente. En su teléfono inteligente escribirá un nombre de cuenta (elegido por usted) y la clave secreta que aparece en la pantalla de su computadora.
- Haga clic en **Add Account (Añadir cuenta)**
    - Después de verificar el código, la pantalla de su computadora indicará que escaneó con éxito el código.
- Haga clic en **Done (Terminar)**.
- **Siga estas instrucciones después de escanear con éxito un código QR o de verificar manualmente el código con su aplicación.**
- Después de escanear el código QR, la aplicación mostrará una pantalla con un código de seis dígitos. Este código cambiará cada 30 segundos.
- Después de configurar con éxito su aplicación Okta Verify, el monitor de su computadora le mostrará la pantalla de inscripción, en donde puede configurar otro método de autenticación multifactorial. En esta pantalla verá que Okta Verify ya está debajo del encabezado Enrolled Factors (Factores inscritos)
- Cuando haya configurado todos los métodos de autenticación multifactorial que desee, oprima el botón Finish (Terminar).

    CONSEJO: si va a configurar un método de autenticación multifactorial que usa una aplicación telefónica, descargue las aplicaciones antes de oprimir el botón **Setup (Configurar)** en la página "Set up multifactor authentication" (Configurar autenticación multifactorial) en su navegador. Los dos métodos de autenticación multifactorial que usan aplicaciones son Okta Verify y Google Authenticator.

Mensajes de error potenciales y cómo resolverlos.

- Mensaje de error: La sesión ha expirado.
- Remedio: El cliente debe volver a iniciar sesión.
- Mensaje de error: El token no coincide.
- Remedio:
    - El cliente debe revisar que sea correcto.
    - El cliente debe "enviar" el código de nuevo.
- Mensaje de error: Se encontró un error.
- Remedio: El cliente debe capturar el código.

- Mensaje de error: El código de barras no se escanea.
- Remedio:
    - Probar los métodos alternativos descritos.
        - "Enviar activación por mensaje de texto" – El cliente puede escribir un número de teléfono.
        - "Configurar manualmente sin enviar mensaje" – El cliente verá un código temporal.
        - "Enviar correo electrónico de activación" – Se le enviará un correo electrónico al cliente a la cuenta que usó para crear su cuenta.
    - Asegúrese de que el dispositivo del cliente permitió el acceso a la cámara.

Regresar a la página principal

Verificación por mensaje de texto

En la pantalla de su computadora verá una ventana que le pedirá configurar su autenticación multifactorial.

- Haga clic en Setup under SMS Authentication (Configurar con autenticación por mensaje de texto).
- Se le pedirá que escriba un número de teléfono.

  CONSEJO: debe ser el número de un teléfono capaz de recibir mensajes de texto.
- Después de escribir su número de teléfono, oprima **Send code (Enviar código).**
- Recibirá un mensaje de texto que contiene un código. Escriba el código en el cuadro Enter Code (Escribir código).
- Oprima **Verify (Verificar)**.
- Se le dirigirá de nuevo a la pantalla de inscripción de autenticación multifactorial. Observe que SMS Authentication (Autenticación por mensaje de texto) ya aparece debajo del encabezado "Enrolled factors" (Factores inscritos).
- Es recomendable que configure más de un método de autenticación multifactorial.
- Cuando haya configurado todos los métodos de autenticación multifactorial que desee, oprima el botón **Finish (Terminar).**

Regresar a la página principal

Autenticación por llamada de voz

En la pantalla de su computadora verá una ventana que le pedirá configurar su autenticación multifactorial.

- Haga clic en Setup under Voice Call Authentication (Configurar con autenticación por llamada de voz).
- Se le pedirá que escriba un número de teléfono.
- Después de escribir su número de teléfono, oprima **Call (Llamar).**
- Recibirá una llamada telefónica. Cuando conteste la llamada, una voz grabada le leerá un número de cinco dígitos.

  CONSEJO: solamente escuchará el número una vez. Tenga listo lápiz y papel para anotar el número.
- Escriba el código en el cuadro Enter Code (Escribir código).
- Oprima **Verify (Verificar)**.
- Se le dirigirá de nuevo a la pantalla de inscripción de autenticación

multifactorial. Observe que Voice Call Authentication (Autenticación por llamada de voz) ya aparece debajo del encabezado "Enrolled factors" (Factores inscritos).

- Es recomendable que configure más de un método de autenticación multifactorial.

- Cuando haya configurado todos los métodos de autenticación multifactorial que desee, oprima el botón Finish (Terminar).

Regresar a la página principal