WE ARE YOUR DOL

NEW YORK STATE OF OPPORTUNITY. Department of Labor

Instructions de configuration de l'authentification multifactorielle

L'État de New York a commencé à utiliser l'authentification multifactorielle (MFA) sur certaines de ses applications destinées au public.

La MFA est un moyen de garantir la sûreté et la sécurité de votre compte. Il faut un deuxième facteur pour prouver que vous êtes bien celui que vous prétendez être, au-delà du simple mot de passe. Si vous utilisez une application protégée par MFA, même si quelqu'un devine ou vole votre mot de passe, il ne pourra pas se connecter sans votre second facteur. Alors qu'un mot de passe est quelque chose que vous connaissez, le second facteur est quelque chose que vous êtes (généralement lu par un dispositif biométrique) ou quelque chose que vous avez.

Ce document est destiné à aider les clients à configurer leur authentification multifactorielle sur leur compte NY.gov.

INDEX

Google Authenticator

Okta Verify

SMS Verify (Vérification par SMS)

Authentification des appels vocaux

Configuration de l'authentification multifactorielle Google Authenticator

Si vous n'êtes pas encore inscrit à la MFA, vous serez invité à vous inscrire après vous être connecté aux services de travail en ligne et avoir cliqué sur le bouton de demande « Services de chômage ».

Sur l'écran de votre ordinateur, vous verrez un écran qui vous demande de configurer votre authentification multifactorielle.

- Sur votre téléphone intelligent, téléchargez l'application Google Authenticator. Vous trouverez ci-dessous les instructions pour télécharger l'application.
- Sur l'écran de votre ordinateur, cliquez sur **Setup** (**Configurer)** sous Google Authenticator pour lancer le processus de configuration.
- Choisissez l'iPhone ou l'Android en fonction de votre appareil.
    - Il vous sera demandé de télécharger l'application Google Authenticator depuis le Google Play Store (Android) ou l'App Store (iPhone). Si vous ne l'avez pas encore fait, vous devriez télécharger cette application dès maintenant. Vous trouverez ci-dessous les instructions pour télécharger l'application.

  CONSEIL : Si vous avez une tablette Apple, choisissez iPhone.
- Cliquez sur le bouton **Suivant** .
- **Suivez les instructions suivantes pour télécharger l'application Google Authenticator sur un appareil Android (Google Play) ou un appareil Apple (App Store).**
- Sur votre smartphone ou votre tablette, accédez à Google Play (Android) ou à l'App Store (appareil Apple). Assurez-vous que votre smartphone ou votre tablette exécute la dernière version du système d'exploitation (OS).
- Dans Google Play (Android) ou l'App Store (appareil Apple), recherchez l'application Google Authenticator.
- Sélectionnez l'application Google Authenticator.
- Téléchargez et installez l'application.
- Une fois que vous avez installé l'application Google Authenticator sur votre smartphone ou votre tablette, accédez à l'application sur votre appareil et ouvrez-la. *(REMARQUE : L'application peut apparaître légèrement différente selon la version du téléphone)*
- **Suivez les instructions suivantes pour utiliser l'application Google Authenticator sur votre smartphone ou votre tablette.**
- Après avoir choisi Apple Device ou Android sur l'écran de votre ordinateur, celui-ci affichera une boîte de dialogue contenant un code de réponse rapide (QR). Le

code QR apparaîtra sous la forme d'un carré rempli de points noirs.

  - Si vous ne parvenez pas à scanner le code QR sur votre smartphone ou votre tablette, cliquez sur l'onglet
    L'option **Can't Scan ?** se trouve sous le code QR sur l'écran de votre ordinateur.

- Si vous êtes en mesure de scanner le code QR sur votre smartphone ou votre tablette, accédez à votre application Google Authenticator et ouvrez-la, si elle n'est pas déjà ouverte.
- Cliquez sur **Get Started (Démarrer)**.
- Vous aurez la possibilité de **scanner un** code **QR** ou de **saisir une clé de configuration**. Choisissez-en un.

  CONSEIL : Si vous ne pouvez pas scanner le code, sélectionnez **Enter a setup key (Saisir une clé de configuration).** Voir ci-dessous pour les instructions concernant la saisie d'une clé de paramétrage.

- Si vous avez un téléphone Android, l'application vous demandera la permission d'utiliser votre appareil photo. Cliquez sur « Pendant l'utilisation de l'application ».
- Si vous avez un appareil Apple, vous verrez un message indiquant que « *Authenticator » souhaite accéder à la caméra*. Cliquez sur OK.
- Après avoir donné à votre téléphone la permission d'utiliser l'appareil photo, l'écran de votre smartphone affichera un écran vide avec un carré au centre.
- Dirigez l'appareil photo de votre smartphone ou de votre tablette vers le code QR qui se trouve sur l'écran de votre ordinateur, de sorte que le code QR de l'écran de l'ordinateur apparaisse dans la case verte de l'écran de votre smartphone. L'application scanne automatiquement le code sur votre téléphone ou votre tablette.
- **Suivez les instructions suivantes si vous avez sélectionné Saisir une clé de configuration dans l'application au lieu de Scanner un code QR.**
- Sur l'écran de votre ordinateur, vous verrez apparaître une clé secrète. Il s'agit du code que vous allez saisir dans l'application Google Authenticator. Un écran contenant les instructions pour saisir une clé de configuration s'affiche.
- Sur votre application Google Authenticator, vous verrez apparaître un écran vous permettant d'entrer les détails du compte. Sur cet écran, saisissez les informations suivantes :
  - Votre nom de compte NY.gov dans le champ « Account name » (Nome du compte).
  - Votre clé secrète dans le champ « Your Key » (Votre clé).
  - Sélectionnez « Time-Based » (Basé sur le temps) dans la liste déroulante Type de clé.
- Cliquez sur le bouton **Add (Ajouter).**
- **Suivez les instructions suivantes pour saisir le code de votre application Google Authenticator sur votre ordinateur.**

- Une fois que l'application a scanné avec succès le code QR ou que vous avez saisi avec succès la clé secrète dans l'application, l'application vous montrera un écran avec votre nom d'utilisateur et un code à six chiffres. Il s'agit du code que vous allez entrer dans l'ordinateur aux étapes suivantes. Ce code change toutes les 30 secondes.

- Saisissez le code à six chiffres de votre application dans le champ Enter Code (Entrer le code) sur l'écran de votre ordinateur et cliquez sur **Vérifier**.
- Vous serez redirigé vers l'écran d'inscription où vous pourrez configurer une autre méthode d'authentification multifactorielle. Remarquez que Google Authenticator figure désormais sous la rubrique des facteurs enregistrés.

  CONSEIL : Il est recommandé de configurer plus d'une méthode d'authentification multifactorielle.

- Lorsque vous avez configuré toutes les méthodes d'authentification multifactorielle que vous souhaitez, cliquez sur le bouton **Finish** (**Terminer)**.

  CONSEIL : Si vous devez configurer une méthode d'authentification multifactorielle qui utilise une application téléphonique, téléchargez les applications avant de cliquer sur le bouton **Setup (Configuration)** de la page du navigateur « Set up multifactor authentication » (Configurer l'authentification multifacteur). Les deux méthodes d'authentification multifactorielle qui utilisent des applications sont Okta Verify et Google Authenticator.

Messages d'erreur potentiels et comment les résoudre.

- Message d'erreur : La session a expiré.
- Remède : Le client doit s'identifier à nouveau.

- Message d'erreur : Le jeton ne correspond pas.
- Remède :
  - Le client doit vérifier l'exactitude.
  - Le client doit « Envoyer » le code à nouveau.

- Message d'erreur : Erreur trouvée.
- Remède : Le client doit saisir le code.

- Message d'erreur : Le code-barres ne se scanne pas.
- Remède :
  - Essayez les méthodes alternatives indiquées.
    - « Envoyer l'activation par SMS » – le client peut saisir un numéro de téléphone.

- « Configuration manuelle sans push » – Le client verra un code temporaire.
- « Envoyer un e-mail d'activation » – Le client recevra un e-mail sur le compte de messagerie utilisé pour la création de son compte.
- Assurez-vous que l'appareil du client a « autorisé » l'accès à la caméra.

Retour à la page principale

Configuration de l'authentification multifactorielle Okta Verify

Sur l'écran de votre ordinateur, vous verrez un écran qui vous demande de configurer votre authentification multifactorielle.

- Sur votre smartphone, téléchargez l'application Okta Verify. Vous trouverez ci-dessous les instructions pour télécharger l'application.
- Sur l'écran de votre ordinateur, cliquez sur **Setup (Configurer)** sous Okta Verify pour commencer le processus de configuration.
- Choisissez l'iPhone ou l'Android en fonction de votre appareil.
    - Il vous sera demandé de télécharger l'application Okta Verify depuis le Google Play Store (Android) ou l'App Store (iPhone). Si vous ne l'avez pas encore fait, vous devriez télécharger cette application dès maintenant. Vous trouverez ci-dessous les instructions pour télécharger l'application.

  CONSEIL : Si vous avez une tablette Apple, choisissez iPhone.
- Cliquez sur le bouton **Suivant** .
- **Suivez les instructions ci-dessous pour télécharger l'application Okta Verify sur un appareil Android (Google Play) ou Apple (App Store)**
- Sur votre smartphone ou votre tablette, accédez à Google Play (Android) ou à l'App Store (appareil Apple). Assurez-vous que votre smartphone ou votre tablette utilise la dernière version du système d'exploitation (OS).
- Dans Google Play ou App Store, recherchez l'application Okta Verify.
- Sélectionnez l'application mobile Okta Verify.
- Téléchargez et installez l'application.
- Une fois que vous avez installé l'application Okta Verify sur votre smartphone ou votre tablette, accédez à l'application sur votre appareil et ouvrez-la.
- **Utilisez les instructions suivantes pour configurer l'application Okta Verify sur votre smartphone ou votre tablette.**
- L'écran de votre ordinateur affiche maintenant une boîte de dialogue contenant un code de réponse rapide (QR). Le code QR apparaîtra sous la forme d'un carré rempli de points noirs.

  - Si vous ne parvenez pas à scanner le code QR, cliquez sur l'option **Can't Scan ? (Impossible de scanner)** sous le code QR sur l'écran de votre ordinateur. Voir ci-dessous les instructions pour configurer Okta Verify après avoir cliqué sur Can't Scan.

- Si vous êtes en mesure de scanner le code QR, naviguez vers l'application Okta Verify sur votre appareil et ouvrez l'application.
- Cliquez sur **Get Started (Démarrer)**.
- Cliquez sur **Next** (**Suivant)**.
- Cliquez sur **Add Account (Ajouter un compte)**.
- Cliquez sur **Other (Autre)**.
- Vous aurez la possibilité de **scanner un** code **QR** ou de **saisir la clé manuellement**. Choisissez-en un.
  - Si vous choisissez l'option **Enter Key Manually (Entrer la clé manuellement)**, vous devrez suivre les étapes ci-dessous pour Vérifier manuellement sans notification poussée dans la liste déroulante Can't Scan ci-dessous.
- **Suivez les instructions suivantes pour utiliser l'application Okta Verify afin de scanner un code QR.**
- Si vous disposez d'un appareil Android, l'application vous demandera la permission d'utiliser votre appareil photo. Cliquez sur OK.
- Si vous avez un appareil Apple, vous verrez un message indiquant que *"Okta Verify" souhaite accéder à la caméra*. Cliquez sur OK.
- Pointez l'appareil photo de votre smartphone ou de votre tablette sur le code QR qui s'affiche sur l'écran de votre ordinateur. L'application scanne automatiquement le code sur votre téléphone ou votre tablette.
- Sur votre écran d'ordinateur, vous verrez l'écran d'inscription avec une fenêtre contextuelle avec un code QR.
- Dans l'application Okta Verify, appuyez sur **Add Account (Ajouter un compte)**.
- Pointez l'appareil photo de votre smartphone ou de votre tablette sur le code QR affiché sur l'écran de votre ordinateur.
- Après avoir scanné le code QR, un nouvel écran apparaîtra sur votre application vous demandant d'autoriser les notifications poussées ? Choisissez soit **Autoriser** , soit **Ignorer**.
- Après avoir réussi à scanner le code QR sur votre smartphone, l'écran de votre ordinateur indiquera que vous avez réussi à scanner le code.
- **Utilisez les instructions suivantes pour configurer Okta Verify par e-mail ou SMS après avoir cliqué sur Can't Scan.**
- Après avoir cliqué sur **Can't Scan (Impossible de scanner)** sur l'écran de votre ordinateur, vous verrez un écran qui indique Setup Okta Verify. Sur cet écran, il y

a une liste déroulante qui offre les options suivantes : Envoyer le lien d'activation par e-mail, Envoyer le lien d'activation par SMS, et Configurer manuellement sans notification poussée.

CONSEIL : Vous trouverez ci-dessous les instructions pour la configuration manuelle sans notification poussée.

- Cliquez sur **Envoyer le lien d'activation par e-mail** ou **Envoyer le lien d'activation par SMS**. Vous recevrez un lien.

CONSEIL : Vous **devez** cliquer sur le lien depuis votre smartphone ou votre tablette.

- Sur votre smartphone ou votre tablette, naviguez dans votre application de messagerie ou de message texte pour accéder au lien. Ouvrez l'email ou le message texte qui vous a été envoyé. Cliquez sur le lien contenu dans le message.
- Vous serez dirigé vers le site Web de Okta Verify.
- Cliquez sur **Get Started (Commencer)**.
- Votre smartphone se connectera au site Web Okta Verify et vérifiera le lien. L'écran de votre ordinateur indiquera que vous avez scanné le code avec succès.
- **Utilisez les instructions suivantes pour configurer Okta Verify par e-mail ou manuellement sans notification poussée après avoir cliqué sur Can't Scan.**
- Après avoir cliqué sur **Can't Scan (Impossible de scanner)** sur l'écran de votre ordinateur, vous verrez un écran qui indique Setup Okta Verify. Sur cet écran, il y a une liste déroulante qui offre les options suivantes : Envoyer le lien d'activation par e-mail, Envoyer le lien d'activation par SMS, et Configurer manuellement sans notification poussée.
- Choisissez l'option : Vérifier manuellement sans notification poussée.
- Vous serez redirigé vers un écran qui contient une clé secrète.
- Ouvrez votre application Okta Verify.
- Cliquez sur **Get Started (Démarrer)**.
- Cliquez sur **Next** (**Suivant)**.
- Cliquez sur **Add Account (Ajouter un compte)**.
- Cliquez sur **Other (Autre)**.
- Sélectionnez Enter Key Manually (Saisir la clé manuellement).
- Entrez le code qui apparaît sur l'écran de votre ordinateur dans l'écran de votre smartphone. Sur votre smartphone, vous allez entrer un nom de compte (créé par vous) et la clé secrète qui s'affiche sur l'écran de votre ordinateur.
- Cliquez sur **Add Account (Ajouter un compte)**.
    - Une fois le code vérifié, l'écran de votre ordinateur indiquera que vous avez scanné le code avec succès.

- Cliquez sur **Done** (**Terminé)**.
- **Utilisez les instructions suivantes après avoir scanné avec succès un code QR ou vérifié manuellement le code avec votre application.**
- Une fois le code QR scanné, l'application affiche un écran contenant un code à six chiffres. Ce code change toutes les 30 secondes.

- Après avoir configuré avec succès votre application Okta Verify, l'écran de votre ordinateur affichera l'écran d'inscription où vous pourrez configurer une autre méthode d'authentification multifactorielle. L'écran montrera maintenant que Okta Verify est sous la rubrique des facteurs inscrits.
- Lorsque vous avez configuré toutes les méthodes d'authentification multifactorielle que vous souhaitez, cliquez sur le bouton Finish (Terminer) .

  CONSEIL : Si vous devez configurer une méthode d'authentification multifactorielle qui utilise une application téléphonique, téléchargez les applications avant de cliquer sur le bouton **Setup (Configuration)** de la page du navigateur « Set up multifactor authentication » (Configurer l'authentification multifacteur). Les deux méthodes d'authentification multifactorielle qui utilisent des applications sont Okta Verify et Google Authenticator.

Messages d'erreur potentiels et comment les résoudre.

- Message d'erreur : La session a expiré.
- Remède : Le client doit s'identifier à nouveau.

- Message d'erreur : Le jeton ne correspond pas.
- Remède :
  - Le client doit vérifier l'exactitude.
  - Le client doit « Envoyer » le code à nouveau.

- Message d'erreur : Erreur trouvée
- Remède : Le client doit saisir le code.

- Message d'erreur : Le code-barres ne se scanne pas.
- Remède
  - Essayez les méthodes alternatives indiquées.
    - « Envoyer l'activation par SMS » – le client peut saisir un numéro de téléphone.
    - « Configuration manuelle sans push » – Le client verra un code temporaire.

- « Envoyer un e-mail d'activation » – Le client recevra un e-mail sur le compte de messagerie utilisé pour la création de son compte.

- Assurez-vous que l'appareil du client a « autorisé » l'accès à la caméra.

Retour à la page principale

SMS Verify (Vérification par SMS)

Sur l'écran de votre ordinateur, vous devriez voir un écran qui vous demande de configurer votre authentification multifactorielle.

- Cliquez sur Setup (Configuration) sous SMS Authentication.
- Il vous sera demandé de saisir un numéro de téléphone.

  CONSEIL : Ce numéro de téléphone doit être capable de recevoir des messages texte.
- Après avoir saisi votre numéro de téléphone, cliquez sur **Envoyer le code**.
- Vous recevrez un message texte contenant un code. Saisissez ce code dans la case « Saisir le code ».
- Appuyez sur **Verify** (**Vérifier)**.
- Vous serez redirigé vers l'écran d'inscription à l'authentification multifactorielle. Remarquez que l'authentification par SMS est maintenant sous la rubrique des facteurs inscrits.
- Il est recommandé de configurer plus d'une méthode d'authentification multifactorielle.
- Lorsque vous avez configuré toutes les méthodes d'authentification multifactorielle que vous souhaitez, cliquez sur le bouton **Finish** (**Terminer)**.

Retour à la page principale

Authentification des appels vocaux

Sur l'écran de votre ordinateur, vous devriez voir un écran qui vous demande de configurer votre authentification multifactorielle.

- Cliquez sur Setup (Configuration) sous Authentification des appels vocaux.
- Il vous sera demandé de saisir un numéro de téléphone.
- Après avoir saisi votre numéro de téléphone, cliquez sur **Call** (**Appeler)**.
- Vous recevrez un appel téléphonique. Lorsque vous répondez à l'appel, une voix enregistrée vous lit un numéro à cinq chiffres.

  CONSEIL : Le numéro ne sera répété qu'une seule fois. Assurez-vous d'avoir un stylo et du papier à portée de main pour noter le nombre.
- Saisissez ce code dans la case « Saisir le code ».

- Appuyez sur **Verify** (**Vérifier)**.
- Vous serez redirigé vers l'écran d'inscription à l'authentification multifactorielle. Remarquez que l'authentification des appels vocaux est maintenant sous la rubrique des facteurs inscrits.
- Il est recommandé de configurer plus d'une méthode d'authentification multifactorielle.
- Lorsque vous avez configuré toutes les méthodes d'authentification multifactorielle que vous souhaitez, cliquez sur le bouton Finish (Terminer).

Retour à la page principale