Modèle d’enregistrement MFA : Enregistrement et connexion avec une application d’authentification tierce TOTP

Comment utiliser ce modèle :

* Ce modèle fournit des instructions d’enregistrement pour les utilisateurs qui souhaitent utiliser une application d’authentification tierce comme méthode de vérification MFA.
  + Les produits Salesforce prennent en charge l’utilisation d’applications d’authentification qui génèrent des codes temporaires reposant sur l’algorithme de mot de passe à usage unique basé sur le temps (TOTP) OATH ([RFC 6238](http://tools.ietf.org/html/rfc6238)). Il existe une variété d’applications d’authentification TOTP disponibles, y compris de nombreuses options gratuites. Les applications les plus utilisées sont notamment Google Authenticator, Microsoft Authenticator et Authy.
* Ce modèle suppose que vous activiez la MFA pour les connexions directes à l’organisation de votre client. Si vous utilisez plutôt un service de MFA de votre fournisseur d’identité SSO, modifiez le contenu et les captures d’écran selon les caractéristiques de cette implémentation (notamment les méthodes de vérification prises en charge par le fournisseur d’identité).
* Personnalisez ce modèle afin qu’il corresponde à l'implémentation de la MFA du client.
  + À partir de la version Summer ’23 de Salesforce, [l’expérience d'inscription à la MFA peut commencer avec une liste de toutes les méthodes de vérification prises en charge ou avec l’écran Connecter Salesforce Authenticator](https://help.salesforce.com/s/articleView?id=sf.security_optimize_verification_method_registration.htm). Choisissez la version du modèle appropriée pour l’organisation de votre client.
  + Consultez les commentaires pour obtenir des conseils.
  + Modifiez tous les espaces réservés, qui sont notés [entre crochets et en rouge], pour inclure les informations de votre client.
  + Incluez vos ressources de déploiement MFA et des instructions sur la façon dont les utilisateurs peuvent poser des questions ou obtenir de l’aide.
* Décidez comment vous souhaitez fournir aux utilisateurs les instructions d’enregistrement. Vous pouvez sauvegarder ce modèle sous forme de fichier PDF et l’envoyer par e-mail aux utilisateurs, l’héberger sur un site interne ou générer une page HTML pour un accès en ligne.

Supprimez ce texte avant de partager le document avec les utilisateurs.

Comment enregistrer et utiliser une application d’authentification tierce pour les connexions avec authentification multifacteur (MFA)

**Enregistrement d’une application d’authentification tierce**

Pour utiliser une application d’authentification tierce comme méthode de vérification des connexions par MFA, enregistrez l’application pour la lier à votre compte. Vous pouvez enregistrer une application à tout moment, même avant que la MFA ne soit activée.

Pour enregistrer une application d’authentification tierce la première fois que vous vous connectez après l’activation de la MFA, suivez les instructions à l’écran comme décrites ci-dessous.

|  |  |  |  |
| --- | --- | --- | --- |
| **1**  Graphical user interface, text  Description automatically generated  A picture containing graphical user interface  Description automatically generated | **2**  Graphical user interface, application  Description automatically generated | **3** | **4**  Qr code  Description automatically generated |
| Installez une application d’authentification tierce sur votre appareil mobile. Des applications sont disponibles sur l’App Store d’Apple ou sur Google Play. | Sur votre ordinateur, connectez-vous  à votre compte. Vous pouvez être invité(e) à confirmer votre identité avec un mot de passe à usage unique par  e-mail ou SMS. | Sélectionnez **Utiliser les codes de vérification d’une application d’authentification**. | L’écran Connecter une application Authenticator s’affiche. |

|  |  |  |  |
| --- | --- | --- | --- |
| **5**  Graphical user interface, application  Description automatically generated | **6**  Qr code  Description automatically generated | **7**  Graphical user interface, text, application, chat or text message  Description automatically generated | **8**  Qr code  Description automatically generated |
| Ouvrez votre application d’authentification sur votre appareil mobile et ajoutez un nouveau compte. | Utilisez l’application d’authentification pour scanner le code QR affiché sur votre ordinateur. | L’application d’authentification est liée à votre compte. L’application commence automatiquement à générer des codes d’accès à usage unique basés sur le temps. | Sur votre ordinateur, saisissez un code unique généré par l’application d’auth-entification dans le champ Code de vérification, puis cliquez sur **Connecter**. |

|  |  |  |  |
| --- | --- | --- | --- |
| **9**  A picture containing text, monitor, electronics, computer  Description automatically generated |  |  |  |
| C’est tout ! Vous avez lié avec succès votre application d’authentification tierce à votre compte. Il ne vous reste plus qu’à finir de vous connecter. |  |  |  |

Pour enregistrer une application d’authentification intégrée à partir des paramètres personnels dans votre compte :

1. Téléchargez et installez l’application d’authentification sur votre appareil mobile. Elle est disponible sur Apple Store ou Google Play.
2. Connectez-vous à votre compte, puis accédez à vos paramètres personnels.
3. Saisissez « Détails utilisateur avancés » dans la zone Recherche rapide, puis sélectionnez **Détails utilisateur avancés**.
4. Dans le champ Enregistrement d’application : authentificateur de mot de passe à usage unique, cliquez sur **Connecter**.
5. Pour des raisons de sécurité, vous pouvez être invité(e) à vous connecter à votre compte ou à vérifier votre identité à l’aide d’un code d’accès à usage unique envoyé par e-mail ou par SMS.
6. Suivez les étapes 4 à 9 du tableau ci-dessus.

**Connexion avec une application d’authentification tierce**

Pour utiliser une application d’authentification tierce afin de vérifier votre identité pour les connexions MFA :

|  |  |  |  |
| --- | --- | --- | --- |
| **1**  Graphical user interface, application  Description automatically generated | **2**  Graphical user interface, application, Teams  Description automatically generated | **3**  Graphical user interface, text, application, chat or text message  Description automatically generated | **4**  A picture containing text, monitor, electronics, computer  Description automatically generatedGraphical user interface, application, Teams  Description automatically generated |
| Sur l’écran de connexion, saisissez votre nom d’utilisateur et votre mot de passe, comme d’habitude. | Vous êtes invité(e) à saisir un  code à partir de votre application d’authentification pour vérifier votre identité. | Sur votre appareil mobile, ouvrez votre application d’authentification pour obtenir un code à usage unique basé sur le temps. | Sur votre ordinateur, saisissez  le code généré par l’application d’authentification, puis cliquez sur **Vérifier**. Vous êtes connecté(e) avec succès à votre compte. |

**Comment obtenir de l’aide**

* [Ajoutez des liens vers les ressources de déploiement MFA de votre entreprise.]
* [Ajoutez des informations de contact pour permettre aux utilisateurs de poser des questions et d’obtenir de l’aide.]

Comment enregistrer et utiliser une application d’authentification tierce pour les connexions avec authentification multifacteur (MFA)

**Enregistrement d’une application d’authentification tierce**

Pour utiliser une application d’authentification tierce comme méthode de vérification des connexions par MFA, enregistrez l’application pour la lier à votre compte. Vous pouvez enregistrer une application à tout moment, même avant que la MFA ne soit activée.

Pour enregistrer une application d’authentification tierce la première fois que vous vous connectez après l’activation de la MFA, suivez les instructions à l’écran comme décrites ci-dessous.

|  |  |  |  |
| --- | --- | --- | --- |
| **1**  Graphical user interface, text  Description automatically generated  A picture containing graphical user interface  Description automatically generated | **2**  Graphical user interface, application  Description automatically generated | **3**  Graphical user interface, text  Description automatically generated | **4** |
| Installez une application d’authentification tierce sur votre appareil mobile. Des applications sont disponibles sur l’App Store d’Apple ou sur Google Play. | Sur votre ordinateur, connectez-vous  à votre compte. Vous pouvez être invité(e) à confirmer votre identité avec un mot de passe à usage unique par  e-mail ou SMS. | L’écran Connecter Salesforce Authenticator s’affiche par défaut. Cliquez sur **Choisir une autre méthode de vérification**. | Sélectionnez **Utiliser les codes de vérification d’une application d’authentification**. |

|  |  |  |  |
| --- | --- | --- | --- |
| **5**  Qr code  Description automatically generated | **6**  Graphical user interface, application  Description automatically generated | **7**  Qr code  Description automatically generated | **8**  Graphical user interface, text, application, chat or text message  Description automatically generated |
| L’écran Connecter une application Authenticator s’affiche. | Ouvrez votre application d’authentification sur votre appareil mobile et ajoutez un nouveau compte. | Utilisez l’application d’authentification pour scanner le code QR affiché sur votre ordinateur. | L’application d’authentification est liée à votre compte. L’application commence automatiquement à générer des codes d’accès à usage unique basés sur le temps. |

|  |  |  |  |
| --- | --- | --- | --- |
| **9**  Qr code  Description automatically generated | **10**  A picture containing text, monitor, electronics, computer  Description automatically generated |  |  |
| Sur votre ordinateur, saisissez un code unique généré par l’application d’authentification dans le champ Code de vérification, puis cliquez sur **Connecter**. | C’est tout ! Vous avez lié avec succès votre application d’authentification tierce à votre compte. Il ne vous reste plus qu’à finir de vous connecter. |  |  |

Pour enregistrer une application d’authentification intégrée à partir des paramètres personnels dans votre compte :

1. Téléchargez et installez l’application d’authentification sur votre appareil mobile. Elle est disponible sur Apple Store ou Google Play.
2. Connectez-vous à votre compte, puis accédez à vos paramètres personnels.
3. Saisissez « Détails utilisateur avancés » dans la zone Recherche rapide, puis sélectionnez **Détails utilisateur avancés**.
4. Dans le champ Enregistrement d’application : authentificateur de mot de passe à usage unique, cliquez sur **Connecter**.
5. Pour des raisons de sécurité, vous pouvez être invité(e) à vous connecter à votre compte ou à vérifier votre identité à l’aide d’un code d’accès à usage unique envoyé par e-mail ou par SMS.
6. Suivez les étapes 5 à 10 du tableau ci-dessus.

**Connexion avec une application d’authentification tierce**

Pour utiliser une application d’authentification tierce afin de vérifier votre identité pour les connexions MFA :

|  |  |  |  |
| --- | --- | --- | --- |
| **1**  Graphical user interface, application  Description automatically generated | **2**  Graphical user interface, application, Teams  Description automatically generated | **3**  Graphical user interface, text, application, chat or text message  Description automatically generated | **4**  A picture containing text, monitor, electronics, computer  Description automatically generatedGraphical user interface, application, Teams  Description automatically generated |
| Sur l’écran de connexion, saisissez votre nom d’utilisateur et votre mot de passe, comme d’habitude. | Vous êtes invité(e) à saisir un code à partir de votre application d’authentification pour vérifier votre identité. | Sur votre appareil mobile, ouvrez votre application d’authentification pour obtenir un code à usage unique basé sur le temps. | Sur votre ordinateur, saisissez  le code généré par l’application d’authentification, puis cliquez sur **Vérifier**. Vous êtes connecté(e) avec succès à votre compte. |

**Comment obtenir de l’aide**

* [Ajoutez des liens vers les ressources de déploiement MFA de votre entreprise.]
* [Ajoutez des informations de contact pour permettre aux utilisateurs de poser des questions et d’obtenir de l’aide.]