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

Comment utiliser ce modèle :

* Ce modèle fournit des instructions d’enregistrement pour les utilisateurs qui souhaitent utiliser une application d’authentification intégrée, telle que Windows Hello, Touch ID ou Face ID, comme méthode de vérification MFA.
* 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 intégrée pour les connexions avec authentification multifacteur (MFA)

|  |  |
| --- | --- |
| **Vérification des critères d’utilisation d’une application d’authentification intégrée** | * Votre ordinateur/appareil mobile, votre système d’exploitation et votre navigateur prennent en charge la norme appropriée en matière d’authentification Web ([FIDO2 WebAuthn](https://fidoalliance.org/fido2/fido2-web-authentication-webauthn/)). |
| * Votre service d’authentification intégré, tel que Windows Hello, Touch ID ou Face ID, est activé et configuré pour vérifier votre identité de manière biométrique, à l’aide d’un scan d’empreinte digitale ou de reconnaissance faciale, ou d’un code PIN, par exemple. |

**Enregistrement d’une application d’authentification intégrée**

Pour utiliser une application d’authentification intégrée comme méthode de vérification des connexions par MFA, suivez le processus d’enregistrement pour la lier à votre compte.

**Conseil** : une application d’authentification intégrée est liée à votre appareil. Si vous vous connectez à partir de plusieurs ordinateurs (par exemple, un ordinateur de bureau et un ordinateur portable), vous devez soit enregistrer une application d’authentification intégrée sur chacun d’eux, soit enregistrer un deuxième type de méthode de vérification que vous pouvez utiliser sur les appareils ne disposant pas d’une telle application.

Lorsque vous vous connectez pour la première fois après l’activation de la MFA, suivez les instructions à l’écran.

|  |  |  |  |
| --- | --- | --- | --- |
| **1**  Graphical user interface, application  Description automatically generated | **2** | **3**  Graphical user interface, text, application, chat or text message, website  Description automatically generated | **4**  Graphical user interface, application, Teams  Description automatically generated |
| Dans un navigateur compatible, 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 une application d’authentification intégrée sur votre appareil** dans la liste des méthodes de vérification. | Cliquez sur **Inscription**. | Lorsque votre navigateur vous y invite, fournissez l’identificateur que vous avez précédemment configuré avec votre application d’authentification intégrée, tel qu’un scan d’empreinte digitale ou de visage, votre code PIN ou votre mot de passe. |

|  |  |  |  |
| --- | --- | --- | --- |
| **5**  Graphical user interface, application, Teams  Description automatically generated | **6**  A picture containing text, monitor, electronics, computer  Description automatically generated |  |  |
| Attribuez un nom à votre application d’authentification intégrée pour qu’elle soit facile à reconnaître, puis cliquez sur **Terminé**. | C’est tout ! Vous avez lié avec succès votre application d’authentification intégrée 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. Dans un navigateur pris en charge, connectez-vous à votre compte, puis accédez à vos paramètres personnels.
2. Saisissez « Détails utilisateur avancés » dans la zone Recherche rapide, puis sélectionnez **Détails utilisateur avancés**.
3. Dans la section Applications d’authentification intégrées, cliquez sur **Ajouter**.
4. 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.
5. Suivez les étapes 3 à 6 du tableau ci-dessus.

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

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

|  |  |  |  |
| --- | --- | --- | --- |
| **1**  Graphical user interface, application  Description automatically generated | **2**  Graphical user interface, text, application  Description automatically generated | **3**  Graphical user interface, text, application  Description automatically generated | **4**  A picture containing text, monitor, electronics, computer  Description automatically generated |
| Dans un navigateur pris en charge, sur l’écran de connexion, saisissez votre nom d’utilisateur et votre mot de passe, comme d’habitude. | Lorsque vous voyez l’écran Vérifier votre identité, cliquez sur **Vérifier**. | Lorsque votre navigateur vous y invite, fournissez l’identificateur que vous avez précédemment configuré avec votre application d’authentification intégrée, tel qu’un scan d’empreinte digitale ou de visage, votre code PIN ou votre mot de passe. | 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 intégrée pour les connexions avec authentification multifacteur (MFA)

|  |  |
| --- | --- |
| **Vérification des critères d’utilisation d’une application d’authentification intégrée** | * Votre ordinateur/appareil mobile, votre système d’exploitation et votre navigateur prennent en charge la norme appropriée en matière d’authentification Web ([FIDO2 WebAuthn](https://fidoalliance.org/fido2/fido2-web-authentication-webauthn/)). |
| * Votre service d’authentification intégré, tel que Windows Hello, Touch ID ou Face ID, est activé et configuré pour vérifier votre identité de manière biométrique, à l’aide d’un scan d’empreinte digitale ou de reconnaissance faciale, ou d’un code PIN, par exemple. |

**Enregistrement d’une application d’authentification intégrée**

Pour utiliser une application d’authentification intégrée comme méthode de vérification des connexions par MFA, suivez le processus d’enregistrement pour la lier à votre compte.

**Conseil** : une application d’authentification intégrée est liée à votre appareil. Si vous vous connectez à partir de plusieurs ordinateurs (par exemple, un ordinateur de bureau et un ordinateur portable), vous devez soit enregistrer une application d’authentification intégrée sur chacun d’eux, soit enregistrer un deuxième type de méthode de vérification que vous pouvez utiliser sur les appareils ne disposant pas d’une telle application.

Lorsque vous vous connectez pour la première fois après l’activation de la MFA, suivez les instructions à l’écran.

|  |  |  |  |
| --- | --- | --- | --- |
| **1**  Graphical user interface, application  Description automatically generated | **2**  Graphical user interface, text  Description automatically generated | **3** | **4**  Graphical user interface, text, application, chat or text message, website  Description automatically generated |
| Dans un navigateur compatible, 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 une application d’authentification intégrée sur votre appareil** dans la liste des méthodes de vérification. | Cliquez sur **Inscription**. |

|  |  |  |  |
| --- | --- | --- | --- |
| **5**  Graphical user interface, application, Teams  Description automatically generated | **6**  Graphical user interface, application, Teams  Description automatically generated | **7**  A picture containing text, monitor, electronics, computer  Description automatically generated |  |
| Lorsque votre navigateur vous y invite, fournissez l’identificateur que vous avez précédemment configuré avec votre application d’authentification intégrée, tel qu’un scan d’empreinte digitale ou de visage, votre code PIN ou votre mot de passe. | Attribuez un nom à votre application d’authentification intégrée pour qu’elle soit facile à reconnaître, puis cliquez sur **Terminé**. | C’est tout ! Vous avez lié avec succès votre application d’authentification intégrée 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. Dans un navigateur pris en charge, connectez-vous à votre compte, puis accédez à vos paramètres personnels.
2. Saisissez « Détails utilisateur avancés » dans la zone Recherche rapide, puis sélectionnez **Détails utilisateur avancés**.
3. Dans la section Applications d’authentification intégrées, cliquez sur **Ajouter**.
4. 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.
5. Suivez les étapes 4 à 7 du tableau ci-dessus.

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

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

|  |  |  |  |
| --- | --- | --- | --- |
| **1**  Graphical user interface, application  Description automatically generated | **2**  Graphical user interface, text, application  Description automatically generated | **3**  Graphical user interface, text, application  Description automatically generated | **4**  A picture containing text, monitor, electronics, computer  Description automatically generated |
| Dans un navigateur pris en charge, sur l’écran de connexion, saisissez votre nom d’utilisateur et votre mot de passe, comme d’habitude. | Lorsque vous voyez l’écran Vérifier votre identité, cliquez sur **Vérifier**. | Lorsque votre navigateur vous y invite, fournissez l’identificateur que vous avez précédemment configuré avec votre application d’authentification intégrée, tel qu’un scan d’empreinte digitale ou de visage, votre code PIN ou votre mot de passe. | 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.]