Salesforce Admin Security

Guide d'installation MFA résistant au phishing

Date d'entrée en vigueur : Environnements de production à partir du 1er juillet 2026 | Sandbox à partir du 22 juin 2026. À lire également : **Préparation MFA résistant au phishing (administrateurs) :** help.salesforce.com/s/articleView?id=005321563.

1. Qu'est-ce qui est requis ?

À partir du 1er juillet 2026, tous les utilisateurs Salesforce disposant de privilèges devront se connecter avec une méthode MFA résistante au phishing. Les utilisateurs privilégiés sont les utilisateurs ayant :

- le profil System Administrator ou System Administrator Mysolution
- la Permission système Modify All Data, View All Data, Customize Application ou Author Apex

Les applications d'authentification standard (telles que Google Authenticator, Microsoft Authenticator ou Authy) qui génèrent des codes TOTP à 6 chiffres ne satisfont pas à la nouvelle exigence. Les utilisateurs n'ayant pas enregistré une méthode appropriée seront bloqués à l'écran de connexion.

Les méthodes qualifiées sont :

- Authentificateurs intégrés : Touch ID, Face ID (Mac/iPhone), Windows Hello (Windows 10/11)
- Clés de sécurité physiques : YubiKey, Google Titan Key, ou une autre clé WebAuthn/FIDO2/U2F
- Clés d'accès (passkeys) synchronisées stockées dans un gestionnaire de mots de passe (Apple iCloud Keychain, 1Password, Bitwarden, etc.)

> ℹ Salesforce recommande d'enregistrer au moins deux méthodes qualifiées par administrateur comme solution de secours, en cas de perte ou d'indisponibilité d'un appareil.

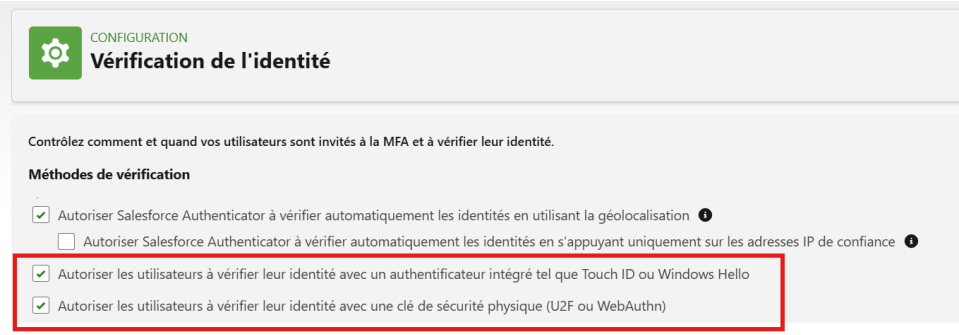
2. Vue d'ensemble des scénarios

Le tableau ci-dessous résume les configurations les plus courantes et l'expérience de connexion après configuration.

Platform	Method	Expérience de connexion après configuration	Qualifié ?
Windows	Clé de sécurité physique (YubiKey, etc.)	Insertion/pression de la clé + bouton tactile	☑ Qualifié
Windows	Windows Hello (Code PIN / Visage / Empreinte)	Fenêtre Windows Hello – pratiquement transparent	☑ Qualifié
Windows	Clé d'accès externe (1Password, Bitwarden)	Pop-up d'extension, confirmation dans l'application	☑ Qualifié
Mac	Apple Passkey (iCloud Keychain)	Transparent – Touch ID ou écran de connexion Mac	☑ Qualifié
Mac	Clé d'accès externe (1Password, Bitwarden)	Pop-up d'extension, confirmation dans l'application	☑ Qualifié
Mac	Clé de sécurité physique (YubiKey, etc.)	Insertion/pression de la clé + bouton tactile	☑ Qualifié
All	Application TOTP (Google/Microsoft Authenticator)	Bloqué – NE SATISFAIT PAS à l'exigence	✗ Non qualifié

3. Activation de la clé de sécurité

Comme indiqué, cette méthode deviendra obligatoire dans Salesforce à partir du 1er juillet 2026. Avant cette date, vous pouvez l'activer pour les utilisateurs ayant un profil d'administrateur système. Pour ce faire, accédez à Configuration, Vérification d'identité et activez les options correspondantes, conformément à la politique de votre organisation :



Enregistrez votre clé d'accès (passkey) pour votre compte dans l'environnement de production et répétez ces étapes pour tous les comptes utilisateurs Sandbox. Choisissez l'une des méthodes d'installation sous Windows ou Mac.

> ⚠ Enregistrez toujours une clé de secours. Si vous perdez l'unique clé, vous serez verrouillé et devrez contacter le Support Salesforce pour rétablir l'accès.

4. Instructions d'installation

Scénario A : Windows Hello (Windows)

Recommandé pour : les utilisateurs Windows 10/11 disposant d'un appareil prenant en charge le code PIN, la reconnaissance faciale ou le déverrouillage par empreinte digitale.

1. Vérifiez que Windows Hello est configuré sur votre appareil (Paramètres, Comptes, Options de connexion).
2. Connectez-vous à Salesforce et cliquez sur votre avatar en haut à droite. Choisissez Paramètres, Données utilisateur avancées.
3. Dans la section Enregistrement de l'application : Clés de sécurité et authentificateurs intégrés, cliquez sur Enregistrer.
4. Le navigateur affiche une fenêtre de sécurité Windows. Authentifiez-vous avec votre méthode Windows Hello (code PIN, visage ou empreinte digitale).
5. L'enregistrement est terminé. La clé est stockée dans le module de plateforme sécurisée (TPM) de l'appareil.

> ℹ Les clés Windows Hello sont liées à l'appareil : elles ne sont pas synchronisées avec d'autres appareils. Enregistrez Windows Hello séparément sur chaque appareil Windows sur lequel vous utilisez Salesforce.

Scénario B : Passkey sur iPhone, iPad ou téléphone Android (Windows)

Recommandé pour : les utilisateurs Windows 10/11 disposant d'un téléphone prenant en charge la connexion biométrique.

1. Connectez-vous à Salesforce et cliquez sur votre avatar en haut à droite. Choisissez Paramètres, Données utilisateur avancées.
2. Dans la section Enregistrement de l'application : Clés de sécurité et authentificateurs intégrés, cliquez sur Enregistrer.
3. Une vérification du compte par e-mail suit. Saisissez le code de vérification que vous recevrez par e-mail.

4. Sur l’écran suivant, choisissez d’enregistrer la clé de sécurité.
5. Le navigateur affiche une fenêtre de sécurité Windows pour stocker la clé d’accès. Choisissez l’option ‘Modifier’ à l’écran pour enregistrer la clé sur un appareil autre qu’une clé USB/clé de sécurité.
6. Sur l’écran suivant, choisissez l’option iPhone, iPad ou appareil Android.
7. Scannez le code QR et finalisez l’enregistrement de la clé d’accès dans le gestionnaire de mots de passe de votre téléphone.
8. Donnez à la clé d’accès (Passkey) un nom permettant de l’identifier dans votre environnement.

Scénario C : Apple Passkey (iCloud Keychain sur Mac)

Recommandé pour : les utilisateurs Mac à l’aise avec iCloud et souhaitant une expérience des plus fluides.

1. Connectez-vous à Salesforce et cliquez sur votre avatar en haut à droite. Choisissez Paramètres, Données utilisateur avancées.
2. Dans la section Enregistrement de l’application : Clés de sécurité et authentificateurs intégrés, cliquez sur Enregistrer.
3. Scannez le code QR avec votre iPhone et confirmez la création sur votre téléphone.
4. La clé d’accès est stockée dans iCloud Keychain et synchronisée avec les autres appareils Apple connectés au même identifiant Apple.

Scénario D : Clé de sécurité physique de type YubiKey ou Google Titan (Windows et Mac)

Recommandé pour : les organisations appliquant des politiques de sécurité strictes, les postes de travail partagés, ou les utilisateurs préférant une approche purement matérielle.

Même procédure que le Scénario A. Les étapes sont identiques : insérez la clé, suivez les instructions du navigateur. Vous stockez désormais la clé d’accès dans une clé USB spéciale, par exemple une YubiKey.

Scénario E : Gestionnaire de mots de passe externe (Windows et Mac)

Recommandé pour : les utilisateurs souhaitant une solution multiplateforme ou utilisant déjà 1Password, Bitwarden, etc.

1. Vérifiez que l’extension de navigateur de votre gestionnaire de mots de passe est installée et active dans Chrome ou Edge.
2. Connectez-vous à Salesforce et cliquez sur votre avatar en haut à droite. Choisissez Paramètres, Données utilisateur avancées.
3. Dans la section Enregistrement de l’application : Clés de sécurité et authentificateurs intégrés, cliquez sur Enregistrer.
4. Lorsque la boîte de dialogue de la clé d’accès s’affiche, sélectionnez le gestionnaire de mots de passe parmi les options.
5. Dans l’extension du gestionnaire de mots de passe, confirmez avec votre mot de passe maître ou par biométrie.
6. La clé d’accès est stockée dans votre coffre-fort et disponible sur tout appareil où le gestionnaire de mots de passe est installé.

5. Utilisateurs SSO

Si votre organisation utilise l’authentification unique (SSO) (ex. : Azure AD, Okta, Ping), l’exigence MFA résistante au phishing doit être satisfaite au niveau du fournisseur d’identité (IdP), et non directement dans Salesforce.

- Votre IdP doit transmettre des signaux ACR/AMR (RFC 8176) confirmant qu’une méthode résistante au phishing a été utilisée.
- Si ces signaux sont absents, Salesforce invite l’utilisateur à enregistrer directement une méthode qualifiée.