**Logo, circle

Description automatically generated**

**Impact de l’exigence de la MFA et des jalons d’activation automatique et d’application de la MFA sur vos clients**

Objectif de ce document : Aider les partenaires Salesforce à comprendre le fonctionnement de l’activation automatique et l’application de la MFA, ainsi que la manière dont ces mesures sont planifiées. Utilisez ces informations pour planifier la MFA et vous assurer que vos clients y sont préparés.

Les cybermenaces au niveau mondial sont en constante évolution, et les types d’attaques susceptibles de paralyser une entreprise et d’exploiter les consommateurs sont en augmentation. Pour lutter contre cette réalité, un élément clé d'une stratégie de sécurité solide consiste à protéger l’accès aux comptes utilisateurs de vos clients. Les noms d'utilisateur et les mots de passe à eux seuls ne constituent plus une protection suffisante contre les cyberattaques. **Voilà pourquoi Salesforce a instauré pour tous les clients une exigence contractuelle qui exige l’utilisation de l’authentification multifacteur (MFA) lors de l’accès aux organisations Salesforce (y compris les solutions partenaires) via des connexions directes avec un nom d'utilisateur et un mot de passe et l’authentification unique (SSO).** Pour connaître les détails et les politiques de l’exigence de la MFA, consultez la [FAQ sur l'authentification multifacteur de Salesforce](https://help.salesforce.com/s/articleView?id=000388806&type=1) et la [Salesforce Partner MFA FAQ](https://salesforce.quip.com/6iJTAyb07itL).

L’exigence contractuelle est entrée en vigueur le 1er février 2022, et la plupart des clients doivent maintenant utiliser la MFA pour leurs organisations Salesforce.

**Remarque** : Salesforce a accordé des prolongations de l’exigence de la MFA à tous les clients des Partenaires OEM Salesforce, ainsi qu’aux fournisseurs de services ou aux clients des fournisseurs de services qui ont demandé à Salesforce de les aider à trouver une solution pour le cas d’utilisation de connexion partagée d’administrateur partenaire. Salesforce a annoncé la solution à ce cas d’utilisation le 13 octobre 2022 et toutes les prolongations partenaires expireront le 15 novembre 2023. Pour en savoir plus, consultez [Comment satisfaire à l'exigence de MFA pour le Cas d'utilisation de connexion partagée d'administrateur partenaire](https://help.salesforce.com/s/articleView?id=000388982&type=1).

**Contenu :**

* [Préparation de vos clients :L’activation automatique de la MFA est en cours et son application est imminente](#mfa_prep_customers)
  + [Savoir qui est concerné par les jalons d’activation automatique et d’application](#mfa_who_is_affected)
  + [Comment Salesforce active automatiquement la MFA et comment les clients peuvent savoir quand ils seront affectés](#mfa_how_it_works)
  + [À quoi s’attendre lorsque Salesforce active automatiquement la MFA pour les organisations de vos clients](#mfa_autoenable_effects)
  + [À quoi s’attendre lorsque Salesforce applique la MFA pour les organisations de vos clients](#mfa_enforcement_effects)
  + [Comment abandonner la MFA pour les cas d'utilisation qui ne l’exigent pas](#mfa_waive_for_exempt_use_cases)
* [Comment satisfaire à l'exigence de MFA pour le cas d'utilisation de connexion partagée d'administrateur partenaire](#mfa_partner_admin_use_case_solution)
* [Ressources MFA de Salesforce](#mfa_resources)

**Préparation de vos clients : L’activation automatique de la MFA est en cours et son application est imminente**

**Partenaires OEM Salesforce** : Étant donné que Salesforce ne communique pas avec vos clients, pensez à les informer à l’avance de l’exigence de la MFA, ainsi que des actions de Salesforce concernant son activation automatique et son application. Donnez-leur également des conseils sur la façon de respecter l’exigence contractuelle d’utilisation de la MFA lors de l’accès aux organisations Salesforce. Pour les modèles d’e-mails de notification, consultez « MFA Comms Email Templates-Partners.docx » dans le Pack de déploiement de la MFA pour les partenaires.

Afin d’aider les clients à satisfaire à l’exigence de la MFA, Salesforce active automatiquement l’authentification multifacteur pour les connexions directes aux organisations de production Salesforce. La première phase d’activation automatique de la MFA a eu lieu lors de la version Spring ’23. Des phases supplémentaires sont prévues pour les prochaines versions majeures, jusqu’à la version Spring ’24. L’application de la MFA, où la MFA devient partie intégrante du processus de connexion, devrait débuter avec la version Summer '24.

**Remarques :**

* Il est actuellement prévu que les organisations appartenant aux clients OEM de Salesforce soient automatiquement activées lors de la version Spring ’24.
* Les clients qui on reçu une [prolongation du cas d'utilisation de connexion partagée d’administrateur partenaire](#mfa_partner_admin_use_case_solution) sont programmés pour être activés automatiquement lors de la version Spring ’24.
* Le calendrier d’activation automatique et d’application est susceptible d’être modifié. Pour assurer le suivi des dates actuelles de ces jalons, vérifiez la [Feuille de route de l’application automatique de la MFA](https://help.salesforce.com/s/articleView?id=000389313&type=1).

Afin d’éviter des perturbations potentielles pour vos clients lorsque ces jalons se produiront, nous vous recommandons, à vous ou à vos clients, d’activer la MFA dès que possible au lieu d’attendre que Salesforce le fasse. Vous pouvez ainsi déployer la MFA selon un calendrier qui vous convient et vous assurer que les utilisateurs de vos clients bénéficient d’une formation préalable et de supports de présentation. Consultez [Activation de la MFA pour les connexions directes des utilisateurs](https://help.salesforce.com/s/articleView?id=sf.security_mfa_overview.htm) et [Gestion des changements pour un déploiement de la MFA réussi](https://security.salesforce.com/mfa-change-management) afin d’obtenir des conseils. De plus, consultez [Comment abandonner la MFA pour les cas d'utilisation qui ne l’exigent pas](#mfa_waive_for_exempt_use_cases) plus bas dans ce document.

**Savoir qui est concerné par les jalons d’activation automatique et d’application**

Salesforce active automatiquement et, à terme, appliquera la MFA à toutes les organisations de production Salesforce (y compris les solutions partenaires), même celles qui respectent déjà l’exigence de la MFA et celles qui utilisent l’authentification unique comme méthode d’accès.

Pourquoi ? Le paramètre au niveau de l'organisation qui est activé pendant l’activation automatique veille à ce que toutes les connexions directes à l’organisation exigent la MFA. Et cela simplifie la maintenance quotidienne. Vous n’avez pas à vous rappeler d’activer la MFA lorsque de nouveaux utilisateurs sont ajoutés à l’organisation d'un client. Si certains utilisateurs d’un client contournent occasionnellement l’authentification unique et se connectent directement, ils seront automatiquement couverts.

**Important**: L’activation automatique de la MFA n’active pas la MFA pour les implémentations SSO et les utilisateurs qui accèdent à leur organisation via SSO ne sont pas affectés. Cependant, n'oubliez pas que l’exigence contractuelle de la MFA s’applique également aux connexions SSO.

Étant donné que toutes les organisations de production seront activées automatiquement, nous vous recommandons de communiquer à l’avance cette mesure à vos clients. Les modèles de communication/d’e-mail sont inclus dans le Pack de déploiement de la MFA pour les partenaires. Consultez le fichier .docx intitulé « MFA Comms Email Templates ».

**Comment Salesforce active automatiquement la MFA et comment les clients peuvent savoir quand ils seront affectés**

Salesforce active automatiquement la MFA pour les connexions directes aux organisations de production en plusieurs phases via le [mécanisme de Mise à jour de version](https://help.salesforce.com/s/articleView?id=sf.release_updates.htm). Pour une notification préalable, la **Mise à jour de version d’activation automatique de la MFA** s’affiche dans le nœud Mises à jour de version dans l’organisation d’un client une version avant son entrée en vigueur. Par exemple, les clients qui sont programmés pour être activés automatiquement lors de la version Summer ’23 commencent à voir la Mise à jour de version de la MFA après la fin du déploiement de Spring ’23.

Nous vous recommandons, à vous ou à vos clients, de vérifier le nœud Mises à jour de version dans leurs organisations après chaque version majeure. Si la Mise à jour de version de la MFA s’affiche, il est prévu qu’elles soient activées automatiquement lors de la prochaine version. Si la mise à jour de version ne s’affiche pas encore, elles seront activées automatiquement lors d’une prochaine version. Continuez à vérifier le nœud après chaque version majeure jusqu’à ce que vous voyiez la mise à jour de version. (Dans de rares cas, plusieurs semaines peuvent être nécessaires après une version majeure pour que les nouvelles mises à jour s’affichent dans le nœud Mises à jour de version.)

**Remarques :**

* Si un client est programmé pour être activé automatiquement dans la phase suivante, mais qu'il reçoit ensuite une prolongation pour satisfaire à l’exigence de la MFA, il continuera à voir la Mise à jour de version de la MFA dans Configuration. Cependant, il ne sera pas activé automatiquement lorsque la Mise à jour de version sera activée.
* Si un client reçoit une prolongation peu de temps avant l’activation automatique, il peut être techniquement impossible d’empêcher l’activation automatique de la MFA dans l’organisation du client. Dans ce cas, un administrateur Salesforce peut rapidement désactiver la MFA à partir de la page Vérification de l'identité dans Configuration, en décochant simplement la case **Demander l'authentification multifacteur (MFA) pour toutes les connexions directes de l'interface utilisateur à votre organisation Salesforce.** Pour plus de d'informations, consultez [cet article](https://help.salesforce.com/s/articleView?id=000394046&type=1).

**À quoi s’attendre lorsque Salesforce active automatiquement la MFA pour les organisations de vos clients**

Lorsque la Mise à jour de version d’activation automatique de la MFA entre en vigueur, elle active le paramètre **Demander l'authentification multifacteur (MFA) pour toutes les connexions directes de l'interface utilisateur à votre organisation Salesforce au niveau de l'organisation.**



Voici ce à quoi s’attendre après l’activation automatique de la MFA par Salesforce :

* Les utilisateurs qui disposent de l’autorisation utilisateur Authentification multifacteur pour les connexions à l'interface utilisateur et qui sont déjà connectés avec la MFA ne connaîtront aucun changement.
* Les utilisateurs qui auparavant n’utilisaient pas la MFA constateront un changement. La prochaine fois qu'ils se connecteront directement avec leur nom d'utilisateur et leur mot de passe, ils seront guidés tout au long de la procédure d’inscription à la MFA. Après cela, ils recevront des défis MFA lors de chaque connexion.
* Après l’activation de la MFA par Salesforce, une période de grâce de 30 jours permet aux utilisateurs d’ignorer l'inscription et de se connecter sans MFA. La période de grâce commence le jour de l'activation automatique dans une organisation et la même période de 30 jours s'applique à tous les utilisateurs de l’organisation.
* Si un client n’est pas prêt pour la MFA lorsque l’activation automatique entre en vigueur et que la période de grâce de 30 jours n’est pas suffisante, vous (ou l'un des administrateurs Salesforce de votre client) pouvez temporairement le désactiver pour tous les utilisateurs jusqu’à ce que Salesforce applique la MFA à une date ultérieure.

Pour plus d'informations et de conseils, consultez cette [rubrique d’aide](https://help.salesforce.com/s/articleView?id=sf.mfa_registration_grace_period.htm).

**À quoi s’attendre lorsque Salesforce applique la MFA pour les organisations de vos clients**

À l’avenir, Salesforce fera de la MFA une partie permanente du processus de connexion directe. Voici ce à quoi s’attendre lorsque Salesforce appliquera la MFA :

* Le paramètre **Demander l'authentification multifacteur (MFA) pour toutes les connexions directes de l'interface utilisateur à votre organisation Salesforce** sera réactivé s’il était désactivé auparavant. Vous et vos clients ne serez plus en mesure de désactiver ce paramètre.
* Les utilisateurs recevront un défi MFA lors de chaque connexion directe avec leur nom d'utilisateur et leur mot de passe.
* Les utilisateurs qui n’utilisaient pas encore la MFA seront invités à s’y inscrire lorsqu’ils se connecteront et ne pourront pas accéder à leur compte tant qu’ils ne l’auront pas fait.
* Les utilisateurs qui disposent de l’autorisation utilisateur Authentification multifacteur pour les connexions à l'interface utilisateur et qui sont déjà connectés avec la MFA ne connaîtront aucun changement.

**Comment abandonner la MFA pour les cas d'utilisation qui ne l’exigent pas**

Il existe certains cas d’utilisation où la MFA n’est pas requise, tels que les types de connexion d’intégration de système via l’API, les connexions d’utilisateur externe aux sites Experience Cloud, les tests automatisés et les comptes RPA, Developer Edition et les organisations test, etc. La plupart de ces cas sont automatiquement exclus lorsque Salesforce active automatiquement la MFA et l’applique. Toutefois, certains cas d’utilisation exemptés doivent être exclus manuellement par vous ou par les administrateurs Salesforce de vos clients afin de s’assurer qu’ils ne sont pas affectés lorsque la MFA est activée.

Vérifiez si vos clients ont l’un de ces cas d’utilisation exemptés et prenez les mesures nécessaires afin d’abandonner la MFA pour leurs comptes. La liste des cas d’utilisation exemptés et les étapes pour abandonner la MFA sont documentées dans [Exclusion des utilisateurs exempts de la MFA](https://help.salesforce.com/s/articleView?id=sf.security_mfa_exclude_exempt_users.htm) dans l’aide de Salesforce.

**Comment satisfaire à l'exigence de MFA pour le cas d'utilisation de connexion partagée d'administrateur partenaire**

L’exigence de la MFA a créé des difficultés pour les fournisseurs de services Salesforce qui partagent des licences fournies par le client au sein de leur organisation afin d’effectuer des services administratifs dans les organisations clientes. Ce scénario est appelé cas d'utilisation de connexion partagée d’administrateur partenaire (ou cas d’utilisation d’administrateur partenaire en abrégé).

Le cas d’utilisation d’administrateur partenaire a empêché certains fournisseurs de services et leurs clients d’adopter la MFA car celle-ci exige que chaque utilisateur fournisse une méthode de vérification avant de se connecter. Si plusieurs personnes partagent une licence, seule une de ces personnes peut se connecter une fois la MFA activée. Par conséquent, Salesforce a accordé une prolongation afin de satisfaire à l’exigence de la MFA à tous les clients des Partenaires OEM Salesforce, ainsi qu’aux fournisseurs de services ou aux clients de fournisseurs de services qui ont demandé à Salesforce de les aider à trouver une solution pour le cas d’utilisation d’administrateur partenaire.

Le 13 octobre 2022, Salesforce a annoncé une solution pour le cas d’utilisation d’administrateur partenaire. Toutes les prolongations des cas d’utilisation d’administrateur partenaire ( y compris toute prolongation accordée après la date d’annonce de la solution) expireront le 15 novembre 2023. Pour les clients qui bénéficient de cette prolongation, l’exigence de la MFA entrera en vigueur à la date d’expiration de la prolongation. Il est actuellement prévu que les clients qui ont obtenu cette prolongation soient automatiquement activés lors de la version Spring ’24.

**Remarque** : À moins que le client d’un partenaire ne l’ait directement contacté, Salesforce n’a pas communiqué avec vos clients à ce sujet.

Si ce cas d'utilisation s’applique à vous et à vos clients, consultez [Comment satisfaire à l'exigence de MFA pour le Cas d'utilisation de connexion partagée d'administrateur partenaire](https://help.salesforce.com/s/articleView?id=000388982&type=1) pour obtenir plus de détails sur la solution et des réponses aux questions courantes. Voici un aperçu :

* Vos clients sont encouragés à fournir à votre entreprise assez de licences uniques afin de couvrir chaque employé qui se connecte à son organisation pour effectuer des services administratifs.
* Si cela n’est pas envisageable, vous pouvez déployer un outil de gestion de compte privilégié ou un outil de gestion de mot de passe d’entreprise pour fonctionner comme une méthode de vérification MFA pour les informations d’identification partagées. Pour satisfaire à l’exigence de la MFA de cette manière, votre implémentation doit respecter les critères suivants :
  + L’outil de gestion de compte privilégié ou de gestion de mot de passe d’entreprise doit prendre en charge l’utilisation de la MFA, et la MFA doit être activée pour l'outil.
  + L’outil doit donner la possibilité de restreindre les autorisations d’accès aux utilisateurs autorisés uniquement, via des techniques telles que le contrôle d'accès en fonction des rôles et l’accès le moins privilégié.
  + Tous les utilisateurs de l’outil doivent être des membres du personnel de votre entreprise. Vos employés doivent utiliser une licence partagée fournie par le client uniquement aux fins de fourniture de support ou d’autres services administratifs à votre client.

**Ressources MFA de Salesforce**

* Pour en savoir plus sur la Mise à jour de version d’activation automatique de la MFA, consultez cette [note de publication](https://help.salesforce.com/s/articleView?id=release-notes.rn_security_mfa_auto_enablement_phase3.htm&release=244&type=5).
* Pour assurer le suivi du calendrier des jalons d’activation automatique et d’application, vérifiez la [Feuille de route de l’application automatique de la MFA](https://help.salesforce.com/s/articleView?id=000389313&type=1).
* Pour préparer les utilisateurs de votre client à la MFA, consultez le [site Gestion des changements pour un déploiement de la MFA réussi](https://security.salesforce.com/mfa-change-management). De plus, utilisez les ressources et les modèles fournis dans cette version partenaire du Pack de déploiement de la MFA. (Si vos clients ont un rôle à jouer dans la préparation de leurs utilisateurs finaux à la MFA, conseillez-leur de télécharger le [Pack de déploiement de la MFA pour les administrateurs](https://security.salesforce.com/mfa-rollout-pack).
* Pour activer de façon proactive la MFA pour vos clients, consultez [Activation de la MFA pour les connexions directes des utilisateurs](https://help.salesforce.com/s/articleView?id=sf.security_mfa_overview.htm) dans l’aide de Salesforce.
* Pour connaître tous les détails sur l’exigence de la MFA, consultez la [FAQ sur l'authentification multifacteur de Salesforce](https://help.salesforce.com/s/articleView?id=000388806&type=1) et la [Salesforce Partner MFA FAQ](https://salesforce.quip.com/6iJTAyb07itL).