Modèles d'e-mail pour les communications sur la MFA

Ces modèles d'e-mails sont conçus pour aider les partenaires Salesforce à communiquer avec leurs clients sur l’exigence de la MFA de Salesforce, les plans d’activation automatique et d’application de Salesforce, et la façon de se préparer à la MFA.

* [**Modèle 1**](#mfa_email_template_1) : Utilisez cette notification pour communiquer aux administrateurs clients et aux parties prenantes la date d’activation de la MFA pour leur organisation ⎯ informez-les à l’avance de l’activation automatique de Salesforce ou activez de façon proactive la MFA pour eux.
* [**Modèle 2**](#mfa_email_template_2) : Utilisez cet exemple de campagne drip par e-mail pour préparer les utilisateurs du client à se connecter avec la MFA.

Modèle 1 : Notification de la date de lancement de la MFA aux administrateurs et aux parties prenantes

Comment utiliser ce modèle :

Cet e-mail est basé sur la notification d’activation automatique de la MFA que Salesforce envoie aux clients, en général 30 à 60 jours avant l’activation de la MFA pour les connexions directes à l’organisation du client.

* Si vos clients sont eux-mêmes responsables de l’activation de la MFA, utilisez ce modèle pour vous assurer qu'ils sont informés de l’exigence de la MFA, des plans d’activation automatique et d’application de Salesforce, et de la manière d’activer eux-mêmes la MFA.
* Si vous administrez les organisations de vos clients et que vous prévoyez d’activer proactivement la MFA pour eux, modifiez ce modèle pour communiquer vos plans de déploiement et votre calendrier.

Cet e-mail inclut des espaces réservés où vous pouvez ajuster le message et les détails. Les espaces réservés sont signalés [entre crochets et en rouge].

**Conseils** :

* Personnalisez ces e-mails pour indiquer aux clients où ils peuvent obtenir davantage d’informations et d’aide, comme les sessions sur l’activation que vous organiserez ou les ressources sur l’activation et l’intégration de la MFA que votre équipe a créées. Le modèle contient des liens vers des ressources créées par Salesforce que vous pouvez garder ou supprimer.
* Pour une meilleure visibilité, envoyez les e-mails les mardis, mercredis et jeudis.

**E-mail : Annonce de la date d'activation de la MFA et conseils sur la façon de s'y préparer**

*Ligne d’objet :*

L’authentification multifacteur (MFA) sera bientôt disponible pour votre organisation [nom du produit] à partir de [nom de version ou date]

*Corps :*

Bonjour [Nom],

Comme vous le savez peut-être, [nom du produit] est élaboré sur les technologies Salesforce. Salesforce exige l’utilisation de l’authentification multifacteur (MFA) et est en train de l’activer pour les clients. Nous vous contactons pour vous informer que la MFA sera automatiquement activée pour votre organisation [nom du produit] à partir de [nom de version ou date]. Les clients sont contractuellement tenus d’utiliser la MFA lorsqu'ils accèdent à [nom du produit]. Pour en savoir plus sur cette exigence, consultez la [FAQ sur l'authentification multifacteur Salesforce](https://help.salesforce.com/s/articleView?id=000388806&type=1).

**Qu'est-ce que la MFA et pourquoi Salesforce l’exige-t-elle ?**

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. La MFA est l'une des méthodes les plus simples et les plus efficaces pour renforcer la sécurité des connexions et protéger votre entreprise et vos données contre les menaces de sécurité.

La MFA est une méthode d'authentification sécurisée qui demande aux utilisateurs de confirmer leur identité en fournissant deux preuves (ou facteurs) ou plus lorsqu'ils se connectent. L'un des facteurs est une information que l'utilisateur connaît, par exemple son nom d'utilisateur et son mot de passe. Les autres facteurs sont des méthodes de vérification d’identité que l'utilisateur possède, par exemple une application Salesforce Authenticator ou une clé de sécurité. En associant l'accès des utilisateurs à plusieurs types de facteur, la MFA est très efficace pour prévenir les menaces courantes telles que les attaques par hameçonnage et les piratages de compte. Pour voir le fonctionnement de la MFA, regardez cette [courte vidéo](https://salesforce.vidyard.com/watch/Zs9r7CyxF6Wu9rfNmMnmFf).

**Soyez prêt pour l’activation automatique de la MFA**

Votre organisation est incluse dans la phase d’activation automatique qui aura lieu lors du déploiement de la version [nom de la version majeure de Salesforce]. Cette mesure active la MFA pour tous les utilisateurs qui se connectent directement avec leur nom d'utilisateur et leur mot de passe.

Pour en savoir plus sur l’activation automatique de la MFA, consultez cet [article](http://click.mail.salesforce.com/?qs=3e6803cb6be010dd859b550a900cd02189719ed0de4b23246bd7c2aeedb842c4d79ca1ec7de5511af4a03c8041be45a07428ae5a7cf49794). Voici un résumé de ce qui vous attend :

* La MFA est activée automatiquement par le [mécanisme de Mise à jour de version](https://help.salesforce.com/s/articleView?id=sf.release_updates.htm). La mise à jour de version d’activation automatique de la MFA pour votre organisation est désormais visible dans le nœud Mise à jour de version dans Configuration et elle entrera en vigueur avec [nom de la version majeure de Salesforce].
* Lorsque cette mise à jour de version entrera en vigueur, elle activera le paramètre **Demander l'authentification multifacteur (MFA) pour toutes les connexions directes de l'interface utilisateur à votre organisation Salesforce**.
* Une fois votre organisation activée automatiquement, les utilisateurs sont invités à fournir une méthode de vérification MFA à chaque connexion. S’ils ne l’ont pas encore fait, ils sont guidés à travers les étapes pour enregistrer une méthode.
* Une période de grâce de 30 jours permet aux utilisateurs d’ignorer l'inscription et de se connecter sans authentification. La période de grâce commence le jour de l'activation automatique dans votre organisation et la même période de 30 jours s'applique à tous les utilisateurs de l’organisation.
* Les administrateurs Salesforce peuvent désactiver temporairement la MFA (jusqu’à ce que Salesforce active la MFA à une date ultérieure).

Pour s’assurer que la MFA est activée pour toutes les connexions directes, Salesforce applique la Mise à jour de version de la MFA à toutes les organisations de production, donc même les organisations qui respectent déjà l’exigence de la MFA et celles qui utilisent l’authentification unique (SSO) pour accéder à Salesforce. Notez que la mise à jour de version n’affecte pas les connexions via SSO.

**Une étape importante avant l’activation automatique**

Certains types d’utilisateurs exemptés de l’exigence de MFA doivent être exclus manuellement par un administrateur Salesforce afin de s'assurer qu’ils ne sont pas affectés par la Mise à jour de version de la MFA. Avant le déploiement de [nom de la version majeure de Salesforce] pour votre organisation, vérifiez si vous avez l'un de ces types d’utilisateurs exemptés et abandonnez la MFA pour leurs comptes. Pour en savoir plus, consultez [Exclusion des utilisateurs exempts de la MFA](http://click.mail.salesforce.com/?qs=3e6803cb6be010ddeb61e48d43a9fa791dd23cc44985ca7647cffa9c42cc4f22cef9f07997c78300d6021600f687fe7503249b002f47daf7) dans l’aide de Salesforce.

**N’attendez pas, activez tout de suite la MFA !**

Pour protéger vos données et éviter des perturbations potentielles pour vos utilisateurs lors de l’activation automatique, [activez vous-même la MFA dès que possible](http://click.mail.salesforce.com/?qs=3e6803cb6be010dd7f22920c4b004d7a57f1e887c2788c4b346c608cab017610a8fe9d48ecaf3d5eca914b7071f8a1ad6563c48a9067686c). L’activation de la MFA ne prend que quelques minutes. Le [Pack de déploiement de la MFA](http://click.mail.salesforce.com/?qs=3e6803cb6be010ddf736dfeb169ae352ebab07e11c615ee511b7b71445154797d516ca079c2aa95c17403ccdfa1b046396d6c1d4f1f5fab1) vous donne tout ce dont vous avez besoin pour préparer vos utilisateurs.

**Obtenir plus d'informations**

Nous avons créé des ressources pour vous aider dans votre parcours MFA.

* Pour plus d’informations sur l’exigence de la MFA, ajoutez ce lien à vos favoris : [FAQ sur l'authentification multifacteur Salesforce](http://click.mail.salesforce.com/?qs=3e6803cb6be010dd15a016a544cebeec605fa238f5fe4e273a3562843c564046a78f13dc6a78567cee4548742ab2008007693e71963face1). Cette ressource est mise à jour régulièrement avec les dernières informations.
* Pour assurer le suivi des jalons d’activation automatique et d’application pour tous les produits Salesforce, vérifiez la [Feuille de route de l’application automatique de la MFA](http://click.mail.salesforce.com/?qs=3e6803cb6be010dd8571ccda7476d28a586d26aff760e887fc940b030abe9813b6ea7a6735b70bca5de7e8df247cc81e268254e263cbccf0).
* Pour vérifier que votre implémentation planifiée satisfait aux conditions de l’exigence de la MFA, utilisez le [MFA Requirement Checker](http://click.mail.salesforce.com/?qs=3e6803cb6be010ddc3071b48a443147ead35f30f9eb2789fc1d7df4c850e2c6ac91e6b1e6f84e7cab8bdaf0a4a30199fd711e3bbe4675c8c).
* Pour poser des questions et obtenir des conseils des experts en sécurité Salesforce, rejoignez-nous sur le parcours du groupe [MFA - Getting Started de la Trailblazer Community](http://click.mail.salesforce.com/?qs=3e6803cb6be010dd95a70238744760edb320306d0a40cf5ef5f8adf19156f6c99fa87774698bad57dbba882e49488c1f76507d4796043495).

Nous vous remercions de votre collaboration pour garantir la confidentialité, la sécurité et la disponibilité des données et des services essentiels de votre entreprise.

Cordialement,

[nom de la société]

Modèle 2 : Campagne drip par e-mail pour préparer les utilisateurs à la MFA

Ceci est un exemple de campagne drip par e-mail que vous pouvez utiliser pour informer les utilisateurs de vos clients sur la MFA et les sensibiliser sur le lancement de la MFA ou l’activation automatique de la MFA par Salesforce. Ce modèle suppose qu'un client utilisera le service MFA de Salesforce, mais il est adaptable si vous passez par le service de MFA d’un fournisseur d’identité SSO.

Ces e-mails incluent des espaces réservés que vous pouvez remplacer par des détails concernant votre déploiement. Les espaces réservés sont signalés [entre crochets et en rouge].

Décidez de la cadence de la campagne par e-mail sur la MFA. Vous pouvez exécuter la campagne drip sur une semaine ou espacer les e-mails sur plusieurs semaines. Voici un exemple de programme pour une campagne d’un mois.

|  |  |  |  |
| --- | --- | --- | --- |
| **4 semaines avant le lancement** | **3 semaines avant le lancement** | **2 semaines avant le lancement** | **1 semaine avant le lancement** |
| *E-mail 1* | *E-mail 2* | *E-mail 3* | *E-mail 4* |

**Conseils** :

* Personnalisez ces e-mails pour rappeler aux utilisateurs les sessions de formation et l’emplacement des ressources d’aide. Les modèles incluent des liens vers des ressources Salesforce, que vous pouvez utiliser telles quelles ou remplacer par vos propres documents. Ils recommandent également des ressources d’intégration incluses dans   
  le pack de déploiement de la MFA.
* Pour une meilleure visibilité auprès des utilisateurs, envoyez les e-mails les mardis, mercredis et jeudis.

**E-mail 1 : annonce de l’arrivée de la MFA et présentation**

*Ligne d’objet :*

Bientôt disponible : une meilleure sécurité de connexion avec l’authentification multifacteur

*Corps :*

Bonjour [Nom],

Chez [nopm de l’entreprise], nous prenons très au sérieux la protection de vos données commerciales et des données de vos clients. En raison des menaces de cybersécurité croissantes en nombre et en sophistication, il est plus important que jamais de mettre en   
œuvre des mesures de sécurité fiables, notamment pour les connexions. C’est pourquoi nous déployons l’authentification multifacteur (ou MFA) pour votre compte [nom du produit] à partir du [date].

**Pourquoi la MFA ?**

Les attaques d’hameçonnage et de piratage de compte sont en augmentation et représentent un risque réel pour votre vie privée et la sécurité de votre entreprise. À eux seuls, les noms d’utilisateur et les mots de passe n’offrent pas toujours une protection suffisante contre ces types de menaces. La MFA limite ces dernières en ajoutant au mot de passe une méthode de vérification d’identité qui confirme l’identité de la personne qui tente de se connecter. Pour savoir ce qu’est la MFA et comment elle fonctionne, regardez cette [courte vidéo](https://salesforce.vidyard.com/watch/Zs9r7CyxF6Wu9rfNmMnmFf).

**Les avantages de la MFA (et son intérêt pour vous)**

* Ajout d’une couche de sécurité supplémentaire à votre compte [nom du produit] qui permet d’empêcher les personnes malintentionnées d’y accéder.
* Protection de l’accès aux données sensibles et aux systèmes critiques.
* Réduction de la probabilité que vous soyez la prochaine victime d’une attaque.
* [Ajoutez des avantages spécifiques à l’entreprise de votre client]

**À quoi s’attendre**

Dans les [période] à venir, nous vous en dirons plus sur la MFA et les changements auxquels vous pouvez vous attendre. Si vous avez des questions ou souhaitez plus d’informations, consultez [partagez une FAQ ou un forum client que vous créez pour fournir des détails sur votre déploiement].

Merci

[nom de la société]

**E-mail 2 : compte à rebours jusqu’au lancement de la MFA et définition des attentes des utilisateurs**

*Ligne d’objet :*

La MFA arrive dans [##] jours : voici à quoi s’attendre

*Corps :*

Bonjour [Nom],

Le [date], nous déploierons l’authentification multifacteur (MFA) pour tous les utilisateurs de [nom du produit] afin d’ajouter une couche supplémentaire de sécurité de connexion. Voici ce à quoi vous pourrez vous attendre lorsque la MFA sera activée.

**Comment fonctionne la MFA**

La MFA exige au moins deux méthodes (ou facteurs) de vérification d’identité pour prouver que vous êtes bien la personne que vous prétendez être avant de pouvoir vous connecter. En exigeant plusieurs types de preuves pour confirmer votre identité, il est beaucoup plus difficile pour une personne malintentionnée d’accéder à votre compte. Même si votre mot de passe est compromis, une personne malveillante a toujours besoin d’un autre facteur pour se connecter.

La MFA nécessite les deux méthodes de vérification suivantes pour accéder à votre compte :

* Une chose que vous savez, à savoir votre nom d’utilisateur et votre mot de passe [nom du produit].
* Une chose que vous possédez comme une application d’authentification sur votre appareil mobile ou une clé de sécurité USB.

À titre d’exemple d’application de la MFA qui peut vous être familière, prenons les deux méthodes que vous utilisez pour retirer de l’argent au guichet automatique. Votre carte est ce que vous possédez, et votre code PIN est ce que vous savez.

**La connexion à [nom du produit] sera un peu différente**

La MFA ajoute une petite étape de connexion supplémentaire qui ne prend que quelques secondes. Vous vous connectez toujours à votre compte [nom du produit]comme vous le faites aujourd’hui, en saisissant votre nom d’utilisateur et votre mot de passe sur l’écran de connexion.

Graphical user interface, application, Teams

Description automatically generated

Ensuite, vous êtes invité(e) à fournir une méthode de vérification supplémentaire. Nous parlerons des méthodes de vérification disponibles dans le prochain message. Mais en un mot, c’est aussi simple que ça !

**Prochaines étapes**

Vous n’avez rien à faire pour le moment. Si vous ne l’avez pas déjà fait, regardez cette [courte vidéo](https://salesforce.vidyard.com/watch/Zs9r7CyxF6Wu9rfNmMnmFf) pour en savoir plus sur le fonctionnement de la MFA. Si vous avez des questions ou souhaitez plus d’informations, consultez [partagez une FAQ ou un forum client que vous créez pour fournir des détails sur votre déploiement].

Merci

[nom de la société]

**E-mail 3 : compte à rebours jusqu’au lancement de la MFA et présentation des différentes méthodes de vérification**

*Ligne d’objet :*

La MFA arrive dans [##] jours : voici comment vous y préparer

*Corps :*

Bonjour [Nom],

Le [date], nous déploierons l’authentification multifacteur (MFA) pour tous les utilisateurs de [nom du produit] afin d’ajouter une couche supplémentaire de sécurité de connexion. Voici ce que vous pouvez faire dès maintenant pour vous assurer d’être prêt(e).

**Décider comment vous voulez confirmer votre identité**

Lorsque la MFA sera activée, vous vous connecterez votre compte [nom du produit]en fournissant une méthode de vérification d’identité ainsi que votre nom d’utilisateur et votre mot de passe. Il est temps de commencer à réfléchir à la ou aux méthode(s) de vérification que vous souhaitez utiliser. Nous vous recommandons de configurer plusieurs méthodes, afin d’avoir toujours une solution de secours en cas de perte ou d’oubli de votre méthode principale. Vous pouvez choisir parmi les options suivantes.

|  |  |
| --- | --- |
| Application mobile Salesforce Authenticator | Facile à installer et à utiliser. L’application envoie une notification à votre téléphone, où vous pouvez rapidement approuver la demande de connexion en une seule touche. Si vous travaillez à partir d’un emplacement approuvé, Salesforce Authenticator peut même automatiser l’étape d'authentification supplémentaire pour vous. Pour en savoir plus, [regardez cette vidéo](https://salesforce.vidyard.com/watch/JyZ_mibupf6sOzMwvhtA3g). |
| Applications mobiles d’authentification tierces, telles que Google Authenticator, Microsoft Authenticator ou Authy | Utilisez n’importe quelle application d’authentification qui génère des codes de mot de passe à usage unique basé sur le temps (TOTP). Avec cette option, vous saisissez le code fourni par l’application lors du processus de connexion. |
| Clé de sécurité [marque] | Les clés de sécurité sont de petits appareils physiques que vous connectez à un port de votre ordinateur ou de votre téléphone portable. Lorsque le processus de connexion vous y invite, vous connectez simplement la clé et elle confirme votre identité.  Si vous souhaitez utiliser une clé de sécurité, contactez [informations de contact]. |
| Applications d’authentification intégrées, telles que Windows Hello, Touch ID ou Face ID | Vérifiez votre identité à l’aide d’un lecteur biométrique,  tel qu’un scanner d’empreinte digitale, d’iris ou de reconnaissance faciale, intégré à votre ordinateur ou à votre appareil mobile. Dans certains cas, les applications d’authentification intégrées confirment l’identité via un code PIN ou un mot de passe configuré dans votre système d’exploitation. Cette option simplifie la MFA car elle repose sur des mécanismes intégrés plutôt que sur une application d’authentification ou une clé de sécurité physique distincte.  Les applications d’authentification intégrées sont liées à des appareils spécifiques. Si vous vous connectez à partir de plusieurs ordinateurs, 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. |

**Comment configurer des méthodes de vérification pour les connexions MFA**

Vous devez enregistrer au moins une méthode de vérification pour la MFA. Le processus d’enregistrement relie la méthode à votre compte [nom du produit] afin que vous puissiez l’utiliser pour prouver votre identité lorsque vous vous connectez.

La première fois que vous vous connecterez après l’activation de la MFA le [date], vous serez automatiquement invité(e) à enregistrer une méthode. Des invites faciles à suivre vous guideront tout au long du processus.

**Que faire dès maintenant ?**

* Décidez du type de méthode de vérification que vous souhaitez utiliser pour les connexions MFA.
* Prenez connaissance des étapes pour son enregistrement. Les étapes d’enregistrement varient un peu pour chaque méthode. Consultez [lien vers les ressources d’enregistrement de méthode de vérification].

Si vous avez des questions ou souhaitez plus d’informations, consultez [partagez une FAQ ou un forum client que vous créez pour fournir des détails sur votre déploiement].

Merci

[nom de la société]

**E-mail 4 : avis final et instructions pour l’enregistrement**

*Ligne d’objet :*

Les connexions MFA commencent dans [##] jours : assurez-vous d’être prêt(e)

*Corps :*

Bonjour [Nom],

Le [date] à [heure], nous activerons l’authentification multifacteur (MFA) pour tous les utilisateurs de [nom du produit] afin d’améliorer la sécurité de vos données commerciales   
et de celles de vos clients. Après cette date, vous devrez fournir une méthode de vérification d’identité en plus de votre nom d’utilisateur et de votre mot de passe lorsque vous vous connecterez à votre compte [nom du produit]. Pour savoir ce qu’est la MFA et comment elle fonctionne, regardez cette [courte vidéo](https://salesforce.vidyard.com/watch/Zs9r7CyxF6Wu9rfNmMnmFf).

**Que faire dès maintenant ?**

Voici comment vous assurer d’être prêt(e) pour la connexion MFA.

* Décidez du type de méthode de vérification que vous souhaitez utiliser pour les connexions MFA. Si vous souhaitez utiliser une clé de sécurité, contactez [informations de contact].
* Pour éviter les retards de connexion à partir du [date], enregistrez dès maintenant une méthode de vérification. Cela ne prend que quelques minutes.
* Les étapes d’enregistrement varient un peu pour chaque méthode. Pour savoir comment enregistrer une méthode, que ce soit maintenant ou lors de votre première connexion après l’activation de la MFA, consultez [lien vers les ressources d’enregistrement de méthode de vérification].

**Conseil** : [téléchargez ces instructions][enregistrez ces instructions comme favori] dès maintenant pour les avoir sous la main quand l’authentification MFA sera activée.

**Comment obtenir de l’aide**

Si vous avez des questions ou souhaitez plus d’informations, consultez [partagez une FAQ ou un forum client que vous créez pour fournir des détails sur votre déploiement].

Merci

[nom de la société]