# BlackBerry UEM

## Gestion des caractéristiques des terminaux

Administration

12.16

# Table des matières

# Gestion des fonctions et du comportement des terminaux

Vous disposez de plusieurs options pour contrôler le comportement du terminal. Vous pouvez utiliser des profils et des stratégies informatiques pour activer ou limiter l'utilisation de nombreuses fonctionnalités. Vous pouvez également envoyer des commandes aux terminaux pour lancer diverses actions.

Vous pouvez spécifier les paramètres de différents types de terminaux dans la même stratégie informatique ou le même profil, puis attribuer la stratégie informatique ou le profil à des comptes d'utilisateur, groupes d'utilisateurs ou groupes de terminaux.

# Gestion de terminaux à l'aide de stratégies informatiques

Vous pouvez utiliser des stratégies informatiques pour gérer la sécurité et le comportement des terminaux de votre organisation. Une stratégie informatique est un ensemble de règles qui contrôlent des fonctions et fonctionnalités sur des terminaux. Vous pouvez configurer des règles pour tous les types de terminaux dans la même stratégie informatique. Le système d'exploitation du terminal dresse la liste des fonctions qui peuvent être contrôlées à l'aide de stratégies informatiques, et le type d'activation du terminal détermine les règles de stratégie informatique qui s'appliquent à un terminal spécifique. Les terminaux ignorent les règles de stratégie informatique qui ne les concernent pas.

BlackBerry UEM inclut une stratégie informatique par défaut dotée de règles préconfigurées pour chaque type de terminal. Si aucune stratégie informatique n'est attribuée à un compte d'utilisateur, un groupe d'utilisateurs auquel appartient un utilisateur ou un groupe de terminaux auquel appartiennent les terminaux d'un utilisateur, BlackBerry UEM envoie la stratégie informatique par défaut aux terminaux de l'utilisateur. BlackBerry UEM envoie automatiquement une stratégie informatique à un terminal lorsqu'un utilisateur l'active, lorsque vous mettez à jour une stratégie informatique attribuée ou lorsqu'une stratégie informatique différente est attribuée à un compte d'utilisateur ou à un terminal.

BlackBerry UEM sur site se synchronise quotidiennement avec BlackBerry Infrastructure via le port 3101 pour déterminer si des informations de stratégie informatique mises à jour sont disponibles. Si des informations de stratégie informatique mises à jour sont disponibles, BlackBerry UEM les récupère et, par défaut, stocke les mises à jour dans la base de données BlackBerry UEM. Les administrateurs disposant des autorisations Afficher les stratégies informatiques et Créer et modifier les stratégies informatiques sont informés de la mise à jour lorsqu'ils se connectent. Si la stratégie de sécurité de votre organisation n'autorise pas les mises à jour automatiques, vous pouvez désactiver les mises à jour automatiques et les importer manuellement dans BlackBerry UEM. Pour plus d'informations, reportez-vous à Importation des mises à jour des stratégies informatiques et des métadonnées de terminal.

Les mises à jour des informations de stratégie informatique sont automatiquement appliquées dans les instances de UEM Cloud.

Pour plus d'informations sur les règles de stratégie informatique pour chaque type de terminal, téléchargez la Fiche de référence des stratégies.

## Limiter ou autoriser les fonctionnalités du terminal

Lorsque vous configurez des règles de stratégie informatique, vous pouvez limiter ou autoriser les fonctionnalités du terminal. Les règles de stratégie informatique disponibles pour chaque type de terminal dépendent du système d'exploitation et de la version du terminal, ainsi que du type d'activation du terminal. Par exemple, selon le type de terminal et d'activation, vous pouvez utiliser des règles de stratégie informatique pour :

- Appliquer des exigences en matière de mot de passe au terminal ou à l'espace Travail d'un terminal
- Empêcher les utilisateurs d'utiliser les fonctionnalités du terminal, telles que l'appareil photo
- Contrôler les connexions utilisant la technologie sans fil Bluetooth
- Contrôler la disponibilité de certaines applications
- Exiger le cryptage et d'autres fonctionnalités de sécurité

Selon le type d'activation du terminal, vous pouvez utiliser des règles de stratégie informatique pour contrôler l'ensemble du terminal et/ou uniquement l'espace Travail d'un terminal.

Pour les terminaux Android 8.0 et version ultérieure, vous pouvez créer un message de support du terminal qui s'affiche sur le terminal pour certaines fonctions lorsqu'elles sont désactivées par des règles de stratégie informatique.

Pour plus d'informations sur les règles de stratégie informatique pour chaque type de terminal, téléchargez la Fiche de référence des stratégies.

# Configuration des exigences de mot de passe du terminal

Vous pouvez utiliser des règles de stratégie informatique pour définir les exigences de mot de passe pour les terminaux. Vous pouvez définir des exigences de longueur et de complexité du mot de passe, l'expiration du mot de passe et le résultat de tentatives de saisie de mots de passe incorrects. Les rubriques suivantes expliquent les règles de mot de passe qui s'appliquent aux différents terminaux et les types d'activation.

Pour plus d'informations sur les règles de stratégie informatique, téléchargez la Fiche de référence des stratégies.

## Configuration des exigences relatives à iOS et aux mots de passe

Vous pouvez choisir si les terminaux iOS et iPadOS doivent avoir un mot de passe. Si vous nécessitez un mot de passe, vous pouvez définir les exigences de ce mot de passe.

**Remarque :** Les terminaux iOS et iPadOS, et certaines des règles de mot de passe du terminal utilisent le terme « code secret ». Les termes « mot de passe » et « code secret » ont la même signification.

| Règle | Description |
|---|---|
| Mot de passe requis pour le terminal | Spécifiez si l'utilisateur doit définir un mot de passe pour le terminal. |
| Accepter les valeurs simples | Spécifiez si le mot de passe peut contenir des caractères séquentiels ou répétés, tels que DEFG ou 3333. |
| Exiger des valeurs alphanumériques | Spécifiez si le mot de passe doit contenir à la fois des lettres et des chiffres. |
| Longueur minimum du mot de passe | Précisez la longueur minimale du mot de passe. Si vous entrez une valeur inférieure à la valeur minimale requise par le terminal, la valeur minimale du terminal est utilisée. |
| Nombre minimal de caractères complexes | Spécifiez le nombre minimum de caractères non-alphanumériques que doit contenir le mot de passe. |
| Durée maximum du code (1-730 jours, ou aucun) | Spécifiez le nombre maximum de jours pendant lesquels le mot de passe peut être utilisé. |
| Verrouillage automatique maximum | Spécifiez la valeur maximum à définir par l'utilisateur pour le verrouillage automatique, qui correspond au nombre de minutes d'inactivité à l'issue desquelles le terminal doit se verrouiller. Si vous définissez cette règle sur Aucun, toutes les valeurs prises en charge sont disponibles sur le terminal. Si la valeur sélectionnée se trouve en dehors de la plage prise en charge par le terminal, celui-ci utilisera la valeur la plus proche qu'il prend en charge. |
| Historique de code (1-50 codes, ou aucun) | Spécifiez le nombre de mots de passe précédents que le terminal vérifie pour empêcher un utilisateur de réutiliser un mot de passe récent. |

| Règle | Description |
|---|---|
| Délai de grâce maximum pour le verrouillage du terminal | Spécifiez la valeur maximum que l'utilisateur peut définir pour le délai de grâce relatif au verrouillage du terminal. Il s'agit du délai pendant lequel le terminal peut rester verrouillé avant qu'un mot de passe soit requis pour le déverrouiller. Si vous définissez cette règle sur "Aucun", toutes les valeurs sont disponibles sur le terminal. Si vous définissez cette règle sur "Immédiatement", le mot de passe est requis immédiatement après le verrouillage du terminal. |
| Nombre maximum d'échecs de tentatives de saisie du mot de passe | Spécifiez le nombre de tentatives de saisie du mot de passe possibles avant la réinitialisation du terminal. |
| Autoriser les modifications de mot de passe (sous supervision uniquement) | Spécifiez si l'utilisateur peut ajouter, modifier ou supprimer le mot de passe. |

Pour plus d'informations sur les règles relatives aux mots de passe de stratégie informatique, téléchargez la Fiche de référence des stratégies.

### Configuration des exigences de mot de passe pour macOS

Vous pouvez choisir si les règles relatives au mot de passe pour les terminaux macOS s'appliquent au terminal ou à l'utilisateur, et si un mot de passe est requis. Si vous nécessitez un mot de passe, vous pouvez définir les exigences de ce mot de passe.

| Règle | Description |
|---|---|
| Cibles de règles de stratégie informatique | Cette règle indique si les règles de stratégie informatique pour le mot de passe s'appliquent uniquement au compte de l'utilisateur attribué ou à l'ensemble du terminal. |
| Mot de passe requis pour le terminal | Spécifiez si l'utilisateur doit définir un mot de passe pour le terminal. |
| Autoriser les mots de passe simples | Spécifiez si le mot de passe peut contenir des caractères séquentiels ou répétés, tels que DEFG ou 3333. |
| Exiger des valeurs alphanumériques | Spécifiez si le mot de passe doit contenir à la fois des lettres et des chiffres. |
| Longueur minimale du mot de passe | Précisez la longueur minimale du mot de passe. |
| Nombre minimal de caractères complexes | Spécifiez le nombre minimum de caractères non-alphanumériques que doit contenir le mot de passe. |
| Délai d'expiration du mot de passe | Spécifiez le nombre maximal de jours pendant lesquels le mot de passe peut être utilisé avant d'expirer et avant que l'utilisateur soit obligé de définir un nouveau mot de passe. |

| Règle | Description |
| --- | --- |
| Verrouillage automatique maximum | Spécifiez la durée maximale d'inactivité de l'utilisateur (en minutes) à l'issue de laquelle le terminal doit se verrouiller. Si vous définissez cette période sur « Aucun », l'utilisateur peut sélectionner n'importe quelle valeur. |
| Historique de mot de passe | Spécifiez le nombre maximal d'anciens mots de passe que le terminal vérifie pour empêcher un utilisateur de réutiliser un mot de passe. |
| Délai de grâce maximum pour le verrouillage du terminal | Spécifiez la valeur maximum que l'utilisateur peut définir pour le délai de grâce relatif au verrouillage du terminal. Il s'agit du délai pendant lequel le terminal peut rester verrouillé avant qu'un mot de passe soit requis pour le déverrouiller. |
| Nombre maximum d'échecs de tentatives de saisie du mot de passe | Spécifiez le nombre d'échecs de tentatives de saisie du mot de passe à l'issue desquels le terminal doit être nettoyé. |

Pour plus d'informations sur les règles relatives aux mots de passe de stratégie informatique, téléchargez la Fiche de référence des stratégies.

### Configuration des exigences de mot de passe pour Android

Il existe quatre groupes de règles de stratégie informatique pour les mots de passe Android. Le groupe de règles que vous utilisez dépend du type d'activation du terminal et si vous configurez des exigences pour le mot de passe du terminal ou pour le mot de passe de l'espace Travail.

Après avoir défini des règles de mot de passe dans la stratégie informatique, utilisez un profil de conformité pour appliquer les exigences de mot de passe.

| Type d'activation | Règles de mot de passe prises en charge |
| --- | --- |
| Travail et Personnel - Confidentialité des données de l'utilisateur (Android Enterprise) et Travail et Personnel - Contrôle total (Android Enterprise) | Utilisez les règles de mot de passe global pour configurer les exigences de mot de passe du terminal.<br>Utilisez les règles de mot de passe du profil professionnel pour définir les exigences en matière de mot de passe pour le profil professionnel.<br>Les règles de mot de passe de Knox sont ignorées par le terminal. |
| Espace Travail uniquement (Android Enterprise) | Utilisez les règles de mot de passe global pour définir les exigences relatives au mot de passe du terminal. Dans la mesure où le terminal dispose uniquement d'un espace Travail, le mot de passe est aussi celui de l'espace Travail.<br>Toutes les autres règles de mot de passe sont ignorées par le terminal. |
| Contrôles MDM | Utilisez les règles de mot de passe global pour configurer les exigences de mot de passe du terminal.<br>Toutes les autres règles de mot de passe sont ignorées par le terminal.<br>**Remarque :** Le type d'activation Contrôles MDM est déconseillé pour les terminaux avec Android 10. Pour plus d'informations, rendez-vous sur le site Web https://support.blackberry.com/community pour consulter l'article 48386. |

| Type d'activation | Règles de mot de passe prises en charge |
|---|---|
| Contrôles MDM (Samsung Knox) | Utilisez les règles de mot de passe Knox MDM pour configurer les exigences de mot de passe du terminal.<br>Toutes les autres règles de mot de passe sont ignorées par le terminal. |
| Travail et Personnel - Confidentialité des données de l'utilisateur (Samsung Knox) | Vous n'avez aucun contrôle sur le mot de passe du terminal.<br>Utilisez les règles de mot de passe de Knox Premium - Espace Travail pour définir les exigences de mot de passe pour l'espace Travail.<br>Toutes les autres règles de mot de passe sont ignorées par le terminal.<br>**Remarque :** Les types d'activation Samsung Knox seront obsolètes dans une future version. Les terminaux qui prennent en charge Knox Platform for Enterprise peuvent être activés à l'aide des types d'activation Android Enterprise. Pour plus d'informations, rendez-vous sur le site Web https://support.blackberry.com/community pour consulter l'article 54614. |
| Travail et Personnel - Contrôle total (Samsung Knox) | Utilisez les règles de mot de passe Knox MDM pour configurer les exigences de mot de passe du terminal.<br>Utilisez les règles de mot de passe de Knox Premium - Espace Travail pour définir les exigences de mot de passe pour l'espace Travail.<br>Toutes les autres règles de mot de passe sont ignorées par le terminal. |
| Espace Travail uniquement (Samsung Knox) | Utilisez les règles de mot de passe de Knox Premium - Espace Travail pour définir les exigences de mot de passe pour l'espace Travail.<br>Toutes les autres règles de mot de passe sont ignorées par le terminal. |

#### Android : règles de mot de passe global

Les règles de mot de passe global définissent les exigences de mot de passe du terminal pour les terminaux dotés des types d'activation suivants :

- Travail et Personnel - Confidentialité des données de l'utilisateur (Android Enterprise)
- Travail et Personnel - Contrôle total (Android Enterprise)
- Espace Travail uniquement (Android Enterprise)
- Contrôles MDM (sans Samsung Knox)

**Remarque :** Le type d'activation Contrôles MDM est déconseillé pour les terminaux avec Android 10. Pour plus d'informations, rendez-vous sur https://support.blackberry.com/community pour lire l'article 48386.

| Règle | Description |
| --- | --- |
| Exigences en matière de mot de passe | Précisez les exigences minimum pour le mot de passe. Vous pouvez choisir l'une des options suivantes :<br>• Non spécifié : aucun mot de passe requis<br>• Quelque chose : l'utilisateur doit définir un mot de passe, mais il n'existe aucune exigence de longueur ni de qualité<br>• Numérique : le mot de passe doit inclure au moins un chiffre<br>• Alphabétique : le mot de passe doit inclure au moins une lettre<br>• Alphanumérique : le mot de passe doit inclure au moins une lettre et un chiffre<br>• Complexe : vous pouvez définir des exigences spécifiques pour différents types de caractères |
| Nombre maximum d'échecs de tentatives de saisie du mot de passe | Spécifiez le nombre d'échecs de tentatives de saisie du mot de passe à l'issue desquels le terminal doit être nettoyé ou désactivé.<br>Les terminaux activés en mode Commandes MDM sont nettoyés.<br>Les terminaux dotés des types d'activation « Travail et Personnel - confidentialité de l'utilisateur » et « Travail et Personnel - confidentialité de l'utilisateur (Premium) » sont désactivés et le profil professionnel est supprimé. |
| Délai d'inactivité maximal avant verrouillage | Spécifiez le nombre maximum de minutes d'inactivité de l'utilisateur à l'issue de laquelle le terminal ou l'espace Travail se verrouille. Sur les terminaux Android dotés d'un profil professionnel, l'espace Travail se verrouille également. Les utilisateurs peuvent définir une période plus courte sur le terminal. Cette règle est ignorée si aucun mot de passe n'est requis. |
| Délai d'expiration du mot de passe | Spécifiez le délai maximum pendant lequel le mot de passe peut être utilisé. Passé ce délai, l'utilisateur doit définir un nouveau mot de passe. S'il est défini sur 0, le mot de passe n'expire pas. |
| Restriction d'historique du mot de passe | Spécifiez le nombre maximum de mots de passe précédents que le terminal vérifie pour empêcher un utilisateur de réutiliser un mot de passe numérique, alphabétique, alphanumérique ou complexe récent. S'il est défini sur 0, le terminal ne vérifie pas les mots de passe précédents. |
| Longueur minimale du mot de passe | Spécifiez le nombre minimal de caractères pour un mot de passe numérique, alphabétique, alphanumérique ou complexe. |
| Nombre minimum de lettres majuscules requises dans le mot de passe | Spécifiez le nombre minimum de lettres majuscules que doit contenir un mot de passe complexe. |
| Nombre minimum de lettres minuscules requises dans le mot de passe | Spécifiez le nombre minimum de lettres minuscules que doit contenir un mot de passe complexe. |

| Règle | Description |
| --- | --- |
| Nombre minimum de lettres requises dans le mot de passe | Spécifiez le nombre minimum de lettres que doit contenir un mot de passe complexe. |
| Nombre minimum de caractères non alphabétiques requis dans le mot de passe | Spécifiez le nombre minimum de caractères non alphabétiques (nombres ou symboles) que doit contenir un mot de passe complexe. |
| Nombre minimum de chiffres requis dans le mot de passe | Spécifiez le nombre minimum de chiffres que doit contenir un mot de passe complexe. |
| Nombre minimum de symboles requis dans le mot de passe | Spécifiez le nombre minimum de caractères non-alphanumériques que doit contenir un mot de passe complexe. |

Pour plus d'informations sur les règles relatives aux mots de passe de stratégie informatique, téléchargez la Fiche de référence des stratégies.

**Android : règles de mot de passe des profils professionnels**

Les règles de mot de passe des profils professionnels définissent les exigences de mot de passe de l'espace Travail des terminaux dotés des types d'activation suivants :

- Travail et Personnel - Confidentialité des données de l'utilisateur (Android Enterprise)
- Travail et Personnel - Contrôle total (Android Enterprise)

| Règle | Description |
| --- | --- |
| Exigences en matière de mot de passe | Spécifiez les exigences minimales à appliquer au mot de passe de l'espace Travail. Vous pouvez choisir l'une des options suivantes :<br>• Quelque chose : l'utilisateur doit définir un mot de passe, mais il n'existe aucune exigence de longueur ni de qualité<br>• Numérique : le mot de passe doit inclure au moins un chiffre<br>• Alphabétique : le mot de passe doit inclure au moins une lettre<br>• Alphanumérique : le mot de passe doit inclure au moins une lettre et un chiffre<br>• Complexe : vous pouvez définir des exigences spécifiques pour différents types de caractères<br>• Numérique complexe : le mot de passe doit contenir des caractères numériques, sans répétition (4444) ni séquence ordonnée (1234, 4321, 2468).<br>• Biométrique (faible) : le mot de passe est compatible avec la technologie de reconnaissance biométrique à sécurité faible.<br>Pour les terminaux BlackBerry optimisés par Android, vous pouvez forcer l'utilisateur à définir des mots de passe différents pour l'espace Travail et le terminal en utilisant la règle des terminaux BlackBerry « Forcer la différence entre le mot de passe de l'espace Travail et celui du terminal ». |

| Règle | Description |
| --- | --- |
| Nombre maximum d'échecs de tentatives de saisie du mot de passe | Spécifiez le nombre de tentatives de saisie possibles pour le mot de passe de l'espace Travail avant la désactivation du terminal et la suppression du profil professionnel. |
| Délai d'inactivité maximal avant verrouillage | Spécifiez le nombre maximum de minutes d'inactivité de l'utilisateur à l'issue desquelles le terminal et l'espace Travail se verrouilleront. Si vous définissez cette règle et la règle Android globale « Délai d'inactivité maximal avant verrouillage » du système d'exploitation natif, le terminal et l'espace Travail se verrouilleront une fois le délai écoulé. Les utilisateurs peuvent définir une période plus courte sur le terminal. |
| Délai d'expiration du mot de passe | Spécifiez la durée de validité maximale du mot de passe de l'espace Travail. Passé ce délai, l'utilisateur devra définir un nouveau mot de passe. S'il est défini sur 0, le mot de passe n'expire pas. |
| Restriction d'historique du mot de passe | Spécifiez le nombre maximum de mots de passe d'espace Travail précédents que le terminal doit vérifier pour empêcher un utilisateur de réutiliser un mot de passe numérique, alphabétique, alphanumérique ou complexe récent. S'il est défini sur 0, le terminal ne vérifie pas les mots de passe précédents. |
| Longueur minimale du mot de passe | Spécifiez le nombre minimal de caractères pour un mot de passe d'espace Travail numérique, alphabétique, alphanumérique ou complexe. |
| Nombre minimum de lettres majuscules requises dans le mot de passe | Spécifiez le nombre minimum de lettres majuscules que doit contenir un mot de passe d'espace Travail complexe. |
| Nombre minimum de lettres minuscules requises dans le mot de passe | Spécifiez le nombre minimum de lettres minuscules que doit contenir un mot de passe d'espace Travail complexe. |
| Nombre minimum de lettres requises dans le mot de passe | Spécifiez le nombre minimum de lettres que doit contenir un mot de passe d'espace Travail complexe. |
| Nombre minimum de caractères non alphabétiques requis dans le mot de passe | Spécifiez le nombre minimum de caractères non alphabétiques (chiffres ou symboles) que doit contenir un mot de passe d'espace Travail complexe. |
| Nombre minimum de chiffres requis dans le mot de passe | Spécifiez le nombre minimum de chiffres que doit contenir un mot de passe d'espace Travail complexe. |
| Nombre minimum de symboles requis dans le mot de passe | Spécifiez le nombre minimum de caractères non alphanumériques que doit contenir un mot de passe d'espace Travail complexe. |

| Règle | Description |
| --- | --- |
| Forcer la différence entre le mot de passe du profil professionnel et celui du terminal | Indiquez si les utilisateurs doivent définir des mots de passe différents pour le terminal et le profil professionnel. Lorsque les mots de passe sont identiques, le déverrouillage du terminal déverrouille le profil professionnel. |

Pour plus d'informations sur les règles relatives aux mots de passe de stratégie informatique, téléchargez la Fiche de référence des stratégies.

#### Android : règles de mot de passe de Knox MDM

Les règles de mot de passe de Knox MDM définissent les exigences de mot de passe du terminal pour les terminaux dotés des types d'activation suivants :

- Travail et Personnel - Contrôle total (Samsung Knox)
- Contrôles MDM (Knox MDM)

Les terminaux dotés de ces types d'activation doivent avoir un mot de passe de terminal.

Si vous activez des terminaux avec des types d'activation Android Enterprise pour utiliser Knox Platform for Enterprise, utilisez les règles de mot de passe global Android. Les types d'activation Samsung Knox et les règles de stratégie informatique Knox MDM seront obsolètes dans une prochaine version. Pour plus d'informations, rendez-vous sur le site Web https://support.blackberry.com/community pour lire l'article 54614.

**Remarque :** Le type d'activation Contrôles MDM est déconseillé pour les terminaux avec Android 10. Pour plus d'informations, rendez-vous sur https://support.blackberry.com/community pour lire l'article 48386.

| Règle | Description |
| --- | --- |
| Exigences en matière de mot de passe | Précisez les exigences minimum pour le mot de passe. Vous pouvez choisir l'une des options suivantes :<br>• Numérique : le mot de passe doit inclure au moins un chiffre<br>• Alphabétique : le mot de passe doit inclure au moins une lettre<br>• Alphanumérique : le mot de passe doit inclure au moins une lettre et un chiffre<br>• Complexe : vous pouvez définir des exigences spécifiques pour différents types de caractères |
| Longueur minimale du mot de passe | Précisez la longueur minimale du mot de passe. Le mot de passe doit contenir au moins 4 caractères. |
| Nombre minimum de lettres minuscules requises dans le mot de passe | Spécifiez le nombre minimum de lettres minuscules que doit contenir un mot de passe complexe. |
| Nombre minimum de lettres majuscules requises dans le mot de passe | Spécifiez le nombre minimum de lettres majuscules que doit contenir un mot de passe complexe. |

| Règle | Description |
|---|---|
| Nombre minimum de caractères complexes requis dans le mot de passe | Spécifiez le nombre minimum de caractères complexes (par exemple, nombres ou symboles) que doit contenir un mot de passe complexe. Si vous définissez cette valeur sur 1, au moins un chiffre est requis. Si vous spécifiez une valeur supérieure à 1, au moins un chiffre et un symbole sont requis. |
| Longueur maximale de la séquence de caractères | Spécifiez la longueur maximale d'une séquence alphabétique autorisée dans un mot de passe alphabétique, alphanumérique ou complexe. Par exemple, si la longueur est définie sur 5, la séquence alphabétique "abcde" est autorisée, mais pas la séquence "abcdef". Si elle est définie sur 0, il n'y a aucune restriction de séquence alphabétique. |
| Délai d'inactivité maximal avant verrouillage | Spécifiez le délai d'inactivité maximal à l'issue duquel le terminal doit se verrouiller (verrou Keyguard). Si le terminal est géré par plusieurs solutions EMM, la valeur la plus faible est utilisée comme délai d'inactivité. Si le terminal utilise un mot de passe, l'utilisateur doit saisir celui-ci pour le déverrouiller. Si ce délai est défini sur 0, le terminal ne dispose d'aucun délai d'inactivité. |
| Nombre maximum d'échecs de tentatives de saisie du mot de passe | Spécifiez le nombre d'échecs de tentatives de saisie du mot de passe à l'issue desquels le terminal doit être nettoyé. |
| Restriction d'historique du mot de passe | Spécifiez le nombre maximum de mots de passe précédents que le terminal vérifie pour empêcher un utilisateur de réutiliser un mot de passe récent. S'il est défini sur 0, le terminal ne vérifie pas les mots de passe précédents. |
| Délai d'expiration du mot de passe | Spécifiez le délai maximum pendant lequel le mot de passe du terminal peut être utilisé. Passé ce délai, le mot de passe expire et l'utilisateur doit en définir un nouveau. S'il est défini sur 0, le mot de passe n'expire pas. |
| Autoriser la visibilité du mot de passe | Spécifiez si le mot de passe du terminal est visible lorsque l'utilisateur le saisit. Si cette règle n'est pas sélectionnée, les utilisateurs et les applications tierces ne peuvent pas modifier la configuration de la visibilité. |
| Autoriser l'authentification par empreinte digitale | Spécifiez si l'utilisateur peut utiliser l'authentification par empreintes digitales pour le terminal. |

Pour plus d'informations sur les règles relatives aux mots de passe de stratégie informatique, téléchargez la Fiche de référence des stratégies.

#### Android : Knox Premium - règles de mot de passe de l'espace Travail

Les règles de mot de passe Knox Premium - Espace Travail définissent les exigences de mot de passe de l'espace Travail des terminaux dotés des types d'activation suivants :

- Travail et Personnel - Confidentialité des données de l'utilisateur (Samsung Knox)
- Travail et Personnel - Contrôle total (Samsung Knox)
- Espace Travail uniquement (Samsung Knox)

Les terminaux dotés de ces types d'activation doivent avoir un mot de passe pour l'espace Travail.

Si vous activez des terminaux avec des types d'activation Android Enterprise pour utiliser Knox Platform for Enterprise, utilisez les règles de mot de passe des profils professionnels de Android. Les types d'activation Samsung Knox et les règles de stratégie informatique Premium Knox sont obsolètes dans une prochaine version. Pour plus d'informations, rendez-vous sur le site Web https://support.blackberry.com/community pour lire l'article 54614.

| Règle | Description |
|---|---|
| Exigences en matière de mot de passe | Précisez les exigences minimum pour le mot de passe. Vous pouvez choisir l'une des options suivantes :<br>• Numérique : le mot de passe doit inclure au moins un chiffre<br>• Numérique complexe : le mot de passe doit inclure au moins un chiffre, sans séquences répétées (4444) ni dans l'ordre (1234, 4321, 2468)<br>• Alphabétique : le mot de passe doit inclure au moins une lettre<br>• Alphanumérique : le mot de passe doit inclure au moins une lettre et un chiffre<br>• Complexe : vous pouvez définir des exigences spécifiques pour différents types de caractères |
| Nombre minimum de lettres minuscules requises dans le mot de passe | Spécifiez le nombre minimum de lettres minuscules que doit contenir un mot de passe complexe. |
| Nombre minimum de lettres majuscules requises dans le mot de passe | Spécifiez le nombre minimum de lettres majuscules que doit contenir un mot de passe complexe. |
| Nombre minimum de caractères complexes requis dans le mot de passe | Spécifiez le nombre minimum de caractères complexes (par exemple, nombres ou symboles) que doit contenir un mot de passe complexe. Au moins trois caractères complexes sont requis, y compris au moins un nombre et un symbole. |
| Longueur maximale de la séquence de caractères | Spécifiez la longueur maximale d'une séquence alphabétique autorisée dans un mot de passe alphabétique, alphanumérique ou complexe. Par exemple, si la longueur est définie sur 5, la séquence alphabétique "abcde" est autorisée, mais pas la séquence "abcdef". Si elle est définie sur 0, il n'y a aucune restriction de séquence alphabétique. |
| Longueur minimale du mot de passe | Précisez la longueur minimale du mot de passe. Si vous saisissez une valeur inférieure au minimum requis par Knox Workspace, la valeur minimum de Knox Workspace est utilisée. |
| Délai d'inactivité maximal avant verrouillage | Spécifiez le délai d'inactivité maximal de l'utilisateur dans l'espace Travail avant le verrouillage de l'espace Travail. Si elle est définie sur 0, l'espace Travail ne dispose d'aucune période d'inactivité. |
| Nombre maximum d'échecs de tentatives de saisie du mot de passe | Spécifiez le nombre de tentatives de saisie du mot de passe possibles avant la réinitialisation de l'espace Travail. S'il est défini sur 0, il n'existe aucune restriction du nombre de tentatives de saisie du mot de passe pour un utilisateur. |

| Règle | Description |
|---|---|
| Restriction d'historique du mot de passe | Spécifiez le nombre maximum de mots de passe précédents que le terminal vérifie pour empêcher un utilisateur de réutiliser un mot de passe récent. S'il est défini sur 0, le terminal ne vérifie pas les mots de passe précédents. |
| Délai d'expiration du mot de passe | Spécifiez le nombre maximum de jours pendant lesquels le mot de passe peut être utilisé. Passé ce délai, le mot de passe expire et l'utilisateur doit en définir un nouveau. S'il est défini sur 0, le mot de passe n'expire pas. |
| Nombre minimum de caractères modifiés pour les nouveaux mots de passe | Spécifiez le nombre minimum de caractères modifiés que doit contenir un nouveau mot de passe par rapport au précédent. Si vous définissez cette règle sur 0, aucune restriction ne s'applique. |
| Autoriser les verrouillages personnalisés | Spécifiez si le terminal est autorisé à utiliser des verrouillages personnalisés, comme des agents d'approbation. Si cette règle n'est pas sélectionnée, les verrouillages personnalisés sont désactivés. |
| Autoriser les agents d'approbation de verrouillage | Spécifiez si l'utilisateur peut maintenir l'espace Travail déverrouillé pendant 2 heures à l'issue du délai d'inactivité maximum de l'espace Travail. Si vous ne définissez aucune valeur de délai d'inactivité, l'utilisateur peut effectuer cette action par défaut. |
| Autoriser la visibilité du mot de passe | Spécifiez si le mot de passe du terminal est visible lorsque l'utilisateur le saisit. Si cette règle n'est pas sélectionnée, les utilisateurs et les applications tierces ne peuvent pas modifier la configuration de la visibilité. |
| Appliquer l'authentification à deux facteurs | Spécifiez si l'utilisateur doit utiliser l'authentification à deux facteurs pour accéder à l'espace Travail. Par exemple, vous pouvez utiliser cette règle si vous souhaitez que l'utilisateur s'authentifie à l'aide d'une empreinte et d'un mot de passe. |
| Autoriser l'authentification par empreinte digitale | Spécifiez si l'utilisateur peut utiliser l'authentification par empreintes digitales pour accéder à l'espace Travail. |

Pour plus d'informations sur les règles relatives aux mots de passe de stratégie informatique, téléchargez la Fiche de référence des stratégies.

### Configuration des exigences de mot de passe pour Windows 10

Vous pouvez choisir si les terminaux Windows 10 doivent avoir un mot de passe. Si vous nécessitez un mot de passe, vous pouvez définir les exigences de ce mot de passe.

| Règle | Description |
|---|---|
| Mot de passe requis pour le terminal | Spécifiez si l'utilisateur doit définir un mot de passe pour le terminal. |
| Autoriser les mots de passe simples | Spécifiez si le mot de passe peut contenir des caractères séquentiels ou répétés, tels que DEFG ou 3333. |

| Règle | Description |
|---|---|
| Longueur minimale du mot de passe | Précisez la longueur minimale du mot de passe. Le mot de passe doit contenir au moins 4 caractères. |
| Complexité du mot de passe | Spécifiez la complexité du mot de passe. Vous pouvez choisir les options suivantes :<br>• Alphanumérique : le mot de passe doit contenir des lettres et des chiffres<br>• Numérique : le mot de passe doit contenir uniquement des chiffres |
| Nombre minimum de types de caractères | Spécifiez le nombre minimum de types de caractères que doit contenir un mot de passe alphanumérique. Vous avez le choix entre les options suivantes :<br>**1.** Chiffres requis<br>**2.** Chiffres et lettres minuscules requis<br>**3.** Chiffres, lettres minuscules et lettres majuscules requis<br>**4.** Chiffres, lettres minuscules, lettres majuscules et caractères spéciaux requis<br>Les exigences relatives aux caractères du mot de passe pour les tablettes et ordinateurs Windows 10 dépendent du type de compte d'utilisateur, et non de ce paramètre. |
| Expiration du mot de passe | Spécifiez le nombre maximum de jours pendant lesquels le mot de passe peut être utilisé. S'il est défini sur 0, le mot de passe n'expire pas. |
| Historique de mot de passe | Spécifiez le nombre de mots de passe précédents que le terminal vérifie pour empêcher un utilisateur de réutiliser un mot de passe récent. S'il est défini sur 0, le terminal ne vérifie pas les mots de passe précédents. |
| Nombre maximum d'échecs de tentatives de saisie du mot de passe | Spécifiez le nombre de tentatives de saisie du mot de passe possibles avant la réinitialisation du terminal. S'il est défini sur 0, le terminal n'est pas réinitialisé, quel que soit le nombre de fois où l'utilisateur saisit un mot de passe incorrect.<br>Cette règle ne s'applique pas aux terminaux qui autorisent plusieurs comptes d'utilisateur, y compris les tablettes et ordinateurs Windows 10. |
| Délai d'inactivité maximal avant verrouillage | Spécifiez la période d'inactivité de l'utilisateur à l'issue de laquelle le terminal se verrouille. S'il est défini sur 0, le terminal ne se verrouille pas automatiquement. |
| Autoriser l'accès sans mot de passe | Spécifiez si l'utilisateur doit saisir le mot de passe à l'issue de la période de grâce associée au délai d'inactivité. Si cette règle est sélectionnée, l'utilisateur peut définir la période de grâce du mot de passe sur le terminal. Cette règle ne s'applique pas aux ordinateurs et tablettes Windows 10. |

Pour plus d'informations sur les règles relatives aux mots de passe de stratégie informatique, téléchargez la Fiche de référence des stratégies.

# Création et gestion des stratégies informatiques

Vous pouvez utiliser la stratégie informatique par défaut ou créer des stratégies informatiques personnalisées (pour spécifier les règles de stratégie informatique pour différents groupes d'utilisateurs de votre organisation, par exemple). Si vous prévoyez d'utiliser la stratégie informatique par défaut, il vous est conseillé de l'examiner

et, si nécessaire, de la mettre à jour pour veiller à ce que les règles respectent les normes de sécurité de votre organisation.

### Créer une stratégie informatique

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Stratégie > Stratégies informatiques**.
3. Cliquez sur +.
4. Saisissez le nom et la description de la stratégie informatique.
5. Cliquez sur l'onglet correspondant à chaque type de terminal de votre organisation et configurez les valeurs appropriées pour les règles de stratégie informatique.

   Maintenez la souris sur le nom d'une règle pour afficher des conseils d'aide.
6. Cliquez sur **Ajouter**.

**À la fin :** Classer les stratégies informatiques

### Copier une stratégie informatique

Vous pouvez copier les stratégies informatiques existantes pour créer rapidement des stratégies informatiques personnalisées destinées aux différents groupes de votre entreprise.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Stratégie > Stratégies informatiques**.
3. Cliquez sur le nom de la stratégie informatique que vous souhaitez copier.
4. Cliquez sur  .
5. Saisissez le nom et la description de la nouvelle stratégie informatique.
6. Apportez les modifications dans l'onglet correspondant à chaque type de terminal.
7. Cliquez sur **Ajouter**.

**À la fin :** Classer les stratégies informatiques

### Classer les stratégies informatiques

Le classement est utilisé pour déterminer la stratégie informatique envoyée par BlackBerry UEM à un terminal dans les scénarios suivants :

- Un utilisateur est membre de plusieurs groupes d'utilisateurs présentant des stratégies informatiques différentes.
- Un terminal est membre de plusieurs groupes de terminaux présentant des stratégies informatiques différentes.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Stratégie > Stratégies informatiques**.
3. Cliquez sur ↓↑.
4. Utilisez les flèches pour déplacer les stratégies informatiques vers le haut ou le bas du classement.
5. Cliquez sur **Enregistrer**.

### Afficher une stratégie informatique

Vous pouvez afficher les informations suivantes sur une stratégie informatique :

- Règles de stratégie informatique spécifiques à chaque type de terminal

- Liste et nombre de comptes d'utilisateur auxquels est attribuée la stratégie informatique (directement et indirectement)
- Liste et nombre de groupes d'utilisateurs auxquels est attribuée la stratégie informatique (directement)

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Stratégie > Stratégies informatiques**.
3. Cliquez sur le nom de la stratégie informatique que vous souhaitez afficher.

## Modifier une stratégie informatique

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Stratégie > Stratégies informatiques**.
3. Cliquez sur le nom de la stratégie informatique que vous souhaitez modifier.
4. Cliquez sur  .
5. Apportez les modifications dans l'onglet correspondant à chaque type de terminal.
6. Cliquez sur **Enregistrer**.

**À la fin :** si nécessaire, modifiez le classement de la stratégie informatique.

## Supprimer une stratégie informatique de comptes d'utilisateur ou groupes d'utilisateurs

Si une stratégie informatique est directement attribuée à des comptes d'utilisateur ou à des groupes d'utilisateurs, vous pouvez la supprimer des utilisateurs ou des groupes. Si une stratégie informatique est indirectement attribuée par un groupe d'utilisateurs, vous pouvez supprimer la stratégie informatique du groupe ou supprimer les comptes d'utilisateur du groupe. Lorsque vous supprimez une stratégie informatique de groupes d'utilisateurs, la stratégie informatique est supprimée de chaque utilisateur appartenant aux groupes sélectionnés.

**Remarque :** la stratégie informatique par défaut peut uniquement être supprimée d'un compte d'utilisateur si vous l'avez directement attribuée à l'utilisateur.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Stratégie > Stratégies informatiques**.
3. Cliquez sur le nom de la stratégie informatique que vous souhaitez supprimer des comptes d'utilisateur ou des groupes d'utilisateurs.
4. Effectuez l'une des tâches suivantes :

| Tâche | Étapes |
|---|---|
| Supprimer une stratégie informatique de comptes d'utilisateur | **a.** Cliquez sur l'onglet **Attribué aux utilisateurs**.<br>**b.** Si nécessaire, recherchez les comptes d'utilisateur.<br>**c.** Sélectionnez les comptes d'utilisateur desquels vous souhaitez supprimer la stratégie informatique.<br>**d.** Cliquez sur  . |
| Supprimer une stratégie informatique de groupes d'utilisateurs | **a.** Cliquez sur l'onglet **Attribué aux groupes**.<br>**b.** Si nécessaire, recherchez les groupes d'utilisateurs.<br>**c.** Sélectionnez les groupes d'utilisateurs desquels vous souhaitez supprimer la stratégie informatique.<br>**d.** Cliquez sur  . |

### Supprimer une stratégie informatique

Vous ne pouvez pas supprimer la stratégie informatique par défaut. Lorsque vous supprimez une stratégie informatique personnalisée, BlackBerry UEM supprime la stratégie informatique des utilisateurs et des terminaux auxquels elle a été attribuée.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Stratégie > Stratégies informatiques**.
3. Sélectionnez les cases à cocher des stratégies informatiques que vous souhaitez supprimer.
4. Cliquez sur .
5. Cliquez sur **Supprimer**.

### Exporter des stratégies informatiques

Vous pouvez exporter des stratégies informatiques vers un fichier .xml à des fins d'audit.

**Remarque :**

Les profils qui sont associés à des stratégies informatiques ne sont pas exportés.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Stratégie > Stratégies informatiques**.
3. Sélectionnez les cases à cocher des stratégies informatiques que vous souhaitez exporter.
4. Cliquez sur .
5. Cliquez sur **Suivant**.
6. Cliquez sur **Exporter**.

## Comment BlackBerry UEM choisit la stratégie informatique à attribuer

BlackBerry UEM envoie une seule stratégie informatique à un terminal et utilise des règles prédéfinies pour déterminer la stratégie informatique à attribuer à un utilisateur et les terminaux que l'utilisateur active.

| Attribué à | Règles |
| --- | --- |
| Compte d'utilisateur<br>(afficher l'onglet Synthèse) | 1. Une stratégie informatique directement attribuée à un compte d'utilisateur est prioritaire sur une stratégie informatique attribuée indirectement par groupe d'utilisateurs.<br>2. Si un utilisateur est membre de plusieurs groupes d'utilisateurs dotés de stratégies informatiques différentes, BlackBerry UEM attribue la stratégie informatique avec le rang le plus élevé.<br>3. La stratégie informatique par défaut est attribuée si aucune stratégie informatique n'est attribuée à un compte d'utilisateur directement ou par appartenance aux groupes d'utilisateurs. |

| Attribué à | Règles |
| --- | --- |
| Terminal<br>(afficher l'onglet Terminal) | Par défaut, un terminal hérite de la stratégie informatique attribuée par BlackBerry UEM à l'utilisateur qui active le terminal. Si un terminal appartient à un groupe de terminaux, les règles suivantes s'appliquent :<br>**1.** Une stratégie informatique attribuée à un groupe de terminaux est prioritaire sur la stratégie informatique attribuée par BlackBerry UEM à un compte d'utilisateur.<br>**2.** Si un terminal est membre de plusieurs groupes de terminaux dotés de stratégies informatiques différentes, BlackBerry UEM attribue la stratégie informatique avec le rang le plus élevé. |

BlackBerry UEM peut devoir résoudre des stratégies informatiques en conflit lorsque vous effectuez l'une des opérations suivantes :

- Attribuer une stratégie informatique à un compte d'utilisateur, groupe d'utilisateurs ou groupe de terminaux
- Supprimer une stratégie informatique d'un compte d'utilisateur, groupe d'utilisateurs ou groupe de terminaux
- Modifier le classement d'une stratégie informatique
- Supprimer une stratégie informatique
- Modifier l'appartenance à un groupe d'utilisateurs (comptes d'utilisateur et groupes imbriqués)
- Modifier les attributs des terminaux
- Modifier l'appartenance à un groupe de terminaux
- Supprimer un groupe d'utilisateurs ou un groupe de terminaux

# Importation des mises à jour des stratégies informatiques et des métadonnées de terminal

BlackBerry envoie régulièrement des mises à jour des stratégies informatiques et des métadonnées de terminal aux installations BlackBerry UEM pour fournir des informations sur les mises à jour des fournisseurs de terminaux et de systèmes d'exploitation.

Par exemple, après la sortie d'un nouveau modèle de terminal, BlackBerry peut envoyer des métadonnées de terminal mises à jour aux installations BlackBerry UEM afin que les profils d'activation et de conformité incluent le nouveau modèle de terminal et puissent être autorisés ou limités par le profil. Après les mises à jour d'Apple, de Google ou de Microsoft, un nouveau pack de stratégies informatiques peut être envoyé aux installations BlackBerry UEM UEM pour vous permettre de contrôler les nouvelles fonctions intégrées à la mise à jour du système d'exploitation.

Par défaut, BlackBerry UEM installe ces mises à jour automatiquement. Si la stratégie de sécurité de votre organisation n'autorise pas les mises à jour automatiques, vous pouvez désactiver les mises à jour automatiques et les importer manuellement dans BlackBerry UEM.

Vous pouvez également configurer des notifications d'évènement pour informer les administrateurs de l'installation des mises à jour des stratégies informatiques et des métadonnées de terminal.

## Importer manuellement des mises à jour des stratégies informatiques et des métadonnées de terminal

BlackBerry envoie des notifications lorsque de nouvelles mises à jour sont disponibles. Les fichiers de mise à jour sont cumulatifs. Si vous manquez une mise à jour, la mise à jour suivante installe toutes les règles de stratégie informatique ou les métadonnées de terminal mises à jour précédemment.

**Avant de commencer :** Téléchargez les métadonnées ou le pack de stratégies informatiques en suivant les instructions contenues dans l'e-mail de notification de mise à jour.

1. Sur la barre de menus, cliquez sur **Paramètres**.
2. Cliquez sur **Infrastructure > Importer les données de configuration**.
3. Effectuez l'une des actions suivantes ou les deux :
   - Pour désactiver les mises à jour automatiques des packs de stratégies informatiques, décochez la case **Mettre à jour automatiquement les données des packs de stratégies informatiques**.
   - Pour désactiver les mises à jour automatiques des métadonnées de terminal, décochez la case **Mettre à jour automatiquement les métadonnées de terminal**.
4. Cliquez sur le bouton **Parcourir** approprié pour trouver le fichier de données que vous voulez importer, et après avoir localisé le fichier, cliquez sur **Ouvrir**.

# Création de messages de support de terminal

Pour les terminaux Android, vous pouvez créer un message de support qui s'affiche sur le terminal lorsqu'une fonction est désactivée par une stratégie informatique. Le message s'affiche sur l'écran des paramètres pour la fonction qui est désactivée. Si vous ne créez pas de message de support, le terminal affiche le message par défaut pour le système d'exploitation.

Vous pouvez également spécifier un message de support administrateur qui s'affiche sur l'écran des paramètres des administrateurs de terminaux. Par exemple, vous pouvez afficher un avertissement indiquant que votre entreprise peut surveiller et gérer des applications et des données dans le profil professionnel.

Si des utilisateurs de votre entreprise travaillent dans plusieurs langues, vous pouvez ajouter des messages de support dans d'autres langues et spécifier la langue par défaut qui s'affiche sur les terminaux qui n'utilisent pas l'une des langues disponibles.

## Créer des messages de support de terminal

Les messages de support de terminal sont pris en charge par les terminaux Android 8.0 et version ultérieure.

1. Dans la barre de menus, cliquez sur **Paramètres > Paramètres généraux**.
2. Cliquez sur **Messages de support de terminal personnalisés**.
3. Sur l'onglet **Messages de support de terminal personnalisés**, cliquez sur **Ajouter**.
4. Sélectionnez la langue dans laquelle vous voulez que la notification s'affiche.
5. Dans le champ **Note de fonctionnalité désactivée**, saisissez la note que vous voulez afficher sur le terminal lorsqu'une fonction est désactivée. Le message peut contenir jusqu'à 200 caractères.
6. Si vous le souhaitez, dans le champ **Message de support administrateur**, saisissez une note qui s'affiche sur l'écran des paramètres des administrateurs de terminaux.
7. Si vous voulez créer un message dans plusieurs langues, cliquez sur **Ajouter une langue supplémentaire** et répétez les étapes 4 à 6 pour chaque langue.
8. Si vous avez ajouté des messages dans plusieurs langues, sélectionnez **Langue par défaut** en regard de la langue que vous souhaitez voir s'afficher sur les terminaux qui n'utilisent pas l'une des langues disponibles. Par exemple, si l'anglais et le français sont les langues disponibles, et que l'anglais est la langue par défaut, le message anglais s'affichera sur les terminaux qui utilisent l'allemand.
9. Cliquez sur **Enregistrer**.

# Application des règles de conformité aux terminaux

Vous pouvez utiliser des profils de conformité pour encourager les utilisateurs à suivre les normes de votre entreprise en matière d'utilisation de terminaux. Un profil de conformité définit les conditions des terminaux non acceptables dans votre organisation. Par exemple, vous pouvez choisir d'interdire les terminaux « crackés » ou « flashés » ou de déclencher une alerte d'intégrité en cas d'accès non autorisé au système d'exploitation.

Un profil de conformité spécifie les informations suivantes :

- Conditions affectant la conformité d'un terminal
- E-mails et notifications que reçoivent les utilisateurs s'ils ne respectent pas les conditions de conformité
- Actions prises si les utilisateurs ne corrigent pas le problème, notamment : restriction d'accès de l'utilisateur aux ressources de l'entreprise, suppression des données professionnelles du terminal ou suppression de toutes les données du terminal

Pour les terminaux Samsung Knox, vous pouvez ajouter une liste d'applications limitées à un profil de conformité. Toutefois, BlackBerry UEM ne fait pas appliquer les règles de conformité. Au lieu de cela, la liste des applications limitées est envoyée aux terminaux et le terminal applique la conformité. Les applications limitées ne peuvent pas être installées ou si elles sont déjà installées, elles sont désactivées. Lorsque vous supprimez une application de la liste limitée, l'application est réactivée si elle est déjà installée.

BlackBerry UEM inclut un profil de conformité par défaut. Le profil de conformité par défaut n'applique aucune condition de conformité. Pour appliquer les règles de conformité, vous pouvez modifier les paramètres du profil de conformité par défaut ou créer et attribuer des profils de conformité personnalisés. Les comptes d'utilisateur ne présentant pas de profil de conformité personnalisé se voient attribuer le profil de conformité par défaut.

## Créer un profil de conformité

**Avant de commencer :**

- Si vous définissez des règles pour autoriser ou interdire certaines applications, ajoutez ces applications à la liste des applications limitées. Pour plus d'informations, reportez-vous à la section Ajouter une application à la liste des applications limitées. Notez que cela ne s'applique pas aux applications intégrées pour les terminaux iOS sous supervision. Pour restreindre les applications intégrées, vous devez créer un profil de conformité et ajouter les applications à la liste d'applications limitées dans le profil. Pour plus d'informations, reportez-vous à iOS : Paramètres des profils de conformité.
- Si vous souhaitez envoyer une notification par e-mail aux utilisateurs lorsque leurs terminaux ne sont pas conformes, modifiez l'e-mail de conformité par défaut ou créez un nouveau modèle d'e-mail. Pour plus d'informations, reportez-vous à la section Créer un modèle pour les notifications d'e-mail de conformité.

**Remarque :** Si vous définissez des règles pour un système d'exploitation cracké ou débridé, des versions limitées du système d'exploitation ou des modèles de terminaux restreints, les utilisateurs ne pourront pas effectuer de nouvelles activations pour les terminaux non conformes, quelle que soit l'action d'application que vous avez définie.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Conformité > Conformité**.
3. Cliquez sur +.
4. Saisissez le nom et la description du profil de conformité.
5. Si vous souhaitez envoyer un message de notification aux utilisateurs lorsque leurs terminaux ne sont plus conformes, effectuez l'une des opérations suivantes :

- Dans la liste déroulante **E-mail envoyé lorsqu'une violation est détectée**, sélectionnez un modèle d'e-mail. Pour afficher l'e-mail de conformité par défaut, cliquez sur Paramètres > Paramètres généraux > Modèles d'e-mail.
- Dans la liste déroulante des **Intervalle d'application**, sélectionnez l'intervalle des vérifications de conformité à effectuer par BlackBerry UEM.
- Développez la section **Envoi d'une notification de terminal lorsqu'une violation est détectée**. Modifiez l'e-mail, si nécessaire.

Vous pouvez utiliser des variables pour renseigner les informations sur l'utilisateur, le terminal et la conformité dans les notifications. Pour plus d'informations, reportez-vous à la section Variables.

6. Cliquez sur l'onglet correspondant à chaque type de terminal de votre organisation et configurez les valeurs appropriées pour chaque paramètre de profil. Pour plus de détails sur chaque paramètre de profil, reportez-vous à la section Paramètres des profils de conformité.
7. Cliquez sur **Ajouter**.

**À la fin :** Si nécessaire, classez les profils.

# Paramètres des profils de conformité

Les profils de conformité sont pris en charge sur les types de terminaux suivants :

- iOS
- macOS
- Android
- Windows

## Communs : paramètres de profil de conformité

#### Terminaux iOS, iPadOS et Android

Pour chaque règle de conformité que vous sélectionnez dans les onglets du terminal, choisissez l'action que BlackBerry UEM doit effectuer si le terminal d'un utilisateur n'est pas conforme.

| Communs : paramètre de profil de conformité | Description |
|---|---|
| Comportement de l'invite | Ce paramètre indique si BlackBerry UEM invite l'utilisateur à corriger un problème de conformité et donne à l'utilisateur le temps de le résoudre avant de prendre des mesures, ou si BlackBerry UEM prend des mesures immédiates.<br>Valeurs possibles :<br>• Invite à la conformité<br>• Action d'application immédiate |

| Communs : paramètre de profil de conformité | Description |
| --- | --- |
| Méthode d'invite | Ce paramètre indique la manière dont BlackBerry UEM invite l'utilisateur à corriger un problème de conformité.<br>Valeurs possibles<br>• Notification de terminal<br>• Notification par e-mail et sur les terminaux<br>Les applications BlackBerry Dynamics n'envoient pas de notifications par e-mail aux utilisateurs. Les applications BlackBerry Dynamics envoient uniquement des notifications sur les terminaux, quelle que soit la valeur de ce paramètre.<br>Pour les règles de conformité qui s'appliquent au terminal, la valeur par défaut est Notification par e-mail et sur les terminaux. Pour les règles de conformité qui s'appliquent uniquement aux applications BlackBerry Dynamics, la valeur par défaut est Notification sur le terminal.<br>Ce paramètre est uniquement valide si le paramètre Comportement de l'invite est défini sur Invite à la conformité. |
| Nombre d'invites | Ce paramètre spécifie le nombre de fois où l'utilisateur est invité à corriger un problème de conformité.<br>La valeur par défaut est 3.<br>Ce paramètre est uniquement valide si le paramètre Comportement de l'invite est défini sur Invite à la conformité. |
| Intervalle entre les invites | Ce paramètre spécifie le délai entre les invites, en minutes, heures ou jours.<br>Le paramètre par défaut est 4 jours.<br>Ce paramètre est uniquement valide si le paramètre Comportement de l'invite est défini sur Invite à la conformité. |

| Communs : paramètre de profil de conformité | Description |
|---|---|
| Action d'application pour les terminaux | Ce paramètre spécifie l'action prise par BlackBerry UEM sur les terminaux non conformes.<br><br>Valeurs possibles :<br><br>• Surveiller et consigner : BlackBerry UEM identifie la violation de conformité mais n'exécute aucune action d'application sur le terminal.<br>• Ne pas faire confiance : sur les terminaux iOS, iPadOS, macOS, Android et Windows, cette option empêche l'utilisateur d'accéder aux ressources et applications professionnelles du terminal. Les données et les applications ne sont pas supprimées du terminal.<br><br>**Remarque :** sur les terminaux iOS et iPadOS, le compte de messagerie professionnel est supprimé de l'application de messagerie d'origine. Les utilisateurs doivent restaurer les paramètres du compte de messagerie de l'application, une fois le terminal redevenu conforme.<br>• Supprimer uniquement les données professionnelles<br>• Supprimer toutes les données<br>• Supprimer du serveur : sur les terminaux iOS, iPadOS, Android et Windows, un terminal peut être désactivé de BlackBerry UEM s'il enfreint la règle « Non joignable ».<br><br>La valeur par défaut est Surveiller et consigner.<br><br>Ce paramètre ne s'applique pas aux terminaux activés en mode Confidentialité de l'utilisateur.<br><br>Sur les terminaux activés via « Travail et Personnel - Confidentialité des données de l'utilisateur », il vous est impossible de supprimer toutes les données d'un terminal d'utilisateur. Si vous sélectionnez « Supprimer toutes les données », BlackBerry UEM exécute la même action qu'avec « Supprimer uniquement les données professionnelles ».<br><br>Pour les terminaux Samsung Knox Workspace qui n'ont qu'un espace Travail, si vous sélectionnez Supprimer uniquement des données professionnelles, Supprimer toutes les données ou Supprimer du serveur, toutes les données seront supprimées du terminal.<br><br>Les actions d'application de la règle Une application interdite est installée ne concernent pas les terminaux iOS et iPadOS supervisés. L'installation d'applications interdites est impossible. |
| Action d'application pour les applications BlackBerry Dynamics | Ce paramètre définit comment traiter les applications BlackBerry Dynamics lorsqu'un terminal n'est pas conforme.<br><br>Valeurs possibles :<br><br>• Ne pas autoriser l'exécution d'applications BlackBerry Dynamics<br>• Supprimer les données d'applications BlackBerry Dynamics<br>• Surveiller et consigner : BlackBerry UEM identifie la violation de conformité mais n'exécute aucune action d'application<br><br>La valeur par défaut est Surveiller et consigner. |

**Terminaux Windows 10 et macOS**

Pour chaque règle de conformité que vous sélectionnez dans les onglets du terminal, choisissez l'action que BlackBerry UEM doit effectuer si le terminal d'un utilisateur n'est pas conforme.

| Communs : paramètre de profil de conformité | Description |
|---|---|
| Action d'application | Ce paramètre spécifie l'action prise par BlackBerry UEM sur les terminaux non conformes.<br>Valeurs possibles :<br>• Invite à la conformité<br>• Ne pas faire confiance : sur les terminaux Windows, cette option empêche l'utilisateur d'accéder aux ressources et applications professionnelles du terminal. Les données et les applications ne sont pas supprimées du terminal.<br>**Remarque :** Untrust n'est pas pris en charge pour les applications BlackBerry Dynamics.<br>• Supprimer uniquement les données professionnelles<br>• Supprimer toutes les données<br>• Supprimer du serveur : sur les terminaux Windows, un terminal peut être désactivé de BlackBerry UEM s'il enfreint la règle Non joignable.<br>• Aucun : identifie une violation de conformité mais n'exécute aucune action.<br>Le paramètre par défaut est « Invite à la conformité ». |
| Méthode d'invite | Les valeurs possibles sont :<br>• Notification par e-mail<br>• Notification de terminal<br>• Les deux<br>Le paramètre par défaut est « Les deux ».<br>Ce paramètre est uniquement valide si le paramètre « Action d'application » est défini sur « Invite à la conformité ».<br>Les notifications du terminal ne sont pas prises en charge sur les terminaux Windows 10. |
| Nombre d'invites | Ce paramètre spécifie le nombre de fois où l'utilisateur est invité à se remettre en conformité.<br>La valeur par défaut est 3.<br>Ce paramètre est uniquement valide si le paramètre « Action d'application » est défini sur « Invite à la conformité ». |
| Intervalle entre les invites | Ce paramètre spécifie le délai entre les invites, en minutes, heures ou jours.<br>Le paramètre par défaut est 4 jours.<br>Ce paramètre est uniquement valide si le paramètre « Action d'application » est défini sur « Invite à la conformité ». |

| Communs : paramètre de profil de conformité | Description |
|---|---|
| Action à l'expiration de l'intervalle entre les invites | Ce paramètre détermine l'action à prendre lorsque l'utilisateur a reçu le nombre total d'invites défini dans Nombre d'invites, et que le terminal n'est toujours pas conforme.<br>Valeurs possibles :<br>• Aucun<br>• Ne pas faire confiance : sur les terminaux Windows, cette option empêche l'utilisateur d'accéder aux ressources et applications professionnelles du terminal. Les données et les applications ne sont pas supprimées du terminal.<br>**Remarque :** Untrust n'est pas pris en charge pour les applications BlackBerry Dynamics. Utilisez une autre action d'application.<br>• Supprimer uniquement les données professionnelles<br>• Supprimer toutes les données<br>Le paramètre par défaut est « Ne pas faire confiance ».<br>Ce paramètre est uniquement valide si le paramètre « Action d'application » est défini sur « Invite à la conformité ». |
| Action d'application pour les applications BlackBerry Dynamics | Ce paramètre définit comment traiter les applications BlackBerry Dynamics lorsqu'un terminal n'est pas conforme.<br>Valeurs possibles :<br>• Supprimer les données d'applications BlackBerry Dynamics<br>• Ne pas autoriser l'exécution d'applications BlackBerry Dynamics<br>La valeur par défaut est Supprimer les données d'applications BlackBerry Dynamics. |

## iOS : Paramètres des profils de conformité

Reportez-vous à la section Communs : paramètres de profil de conformité pour une description des actions possibles si vous sélectionnez une règle de conformité.

Ces paramètres s'appliquent également aux terminaux iPadOS.

| iOS : paramètre Profil de conformité | Description |
|---|---|
| Système d'exploitation cracké | Ce paramètre crée une règle de conformité qui garantit qu'il ne sera pas possible de cracker les terminaux. Un terminal est cracké lorsqu'un utilisateur ou un utilisateur malveillant contourne différentes restrictions pour modifier le système d'exploitation d'un terminal.<br>Si vous sélectionnez ce paramètre, les utilisateurs ne pourront pas non plus effectuer de nouvelles activations pour les terminaux crackés, quelle que soit l'action d'application que vous avez définie. |

| iOS : paramètre Profil de conformité | Description |
| --- | --- |
| L'application non attribuée est installée | Ce paramètre crée une règle de conformité pour empêcher l'installation d'applications non attribuées sur les terminaux des utilisateurs.<br>Lorsque vous sélectionnez ce paramètre et qu'une application non attribuée est installée sur un terminal, un message d'avertissement et un lien sont affichés sur l'onglet Terminaux gérés. Lorsque vous cliquez sur le lien, la liste des applications qui mettent le terminal hors conformité est affichée.<br>Ce paramètre ne s'applique pas aux terminaux activés avec le type d'activation Confidentialité de l'utilisateur. |
| Une application requise n'est pas installée | Ce paramètre crée une règle de conformité pour veiller à ce que les applications requises soient installées sur les terminaux.<br>Lorsque vous sélectionnez ce paramètre et qu'une application requise n'est pas installée sur un terminal, un message d'avertissement et un lien sont affichés sur l'onglet Terminaux gérés. Lorsque vous cliquez sur le lien, la liste des applications qui mettent le terminal hors conformité est affichée. |
| Une version limitée du SE est installée | Ce paramètre crée une règle de conformité pour vérifier qu'aucune version limitée du système d'exploitation n'est installée sur les terminaux.<br>Vous pouvez sélectionner les versions limitées du système d'exploitation.<br>Si vous sélectionnez ce paramètre, les utilisateurs ne pourront pas effectuer de nouvelles activations pour les terminaux qui ne sont pas conformes, quelle que soit l'action d'application que vous avez définie. |
| Modèle de terminal interdit détecté | Ce paramètre crée une règle de conformité permettant d'interdire certains modèles de terminaux.<br>Vous pouvez choisir l'une des options suivantes :<br>• Autoriser les modèles de terminaux sélectionnés<br>• Ne pas autoriser les modèles de terminaux sélectionnés<br>Vous pouvez sélectionner les modèles de terminaux autorisés ou interdits.<br>Si vous sélectionnez ce paramètre, les utilisateurs ne pourront pas effectuer de nouvelles activations pour les terminaux qui ne sont pas conformes, quelle que soit l'action d'application que vous avez définie. |
| Terminal non joignable | Ce paramètre crée une règle de conformité pour veiller à ce que les terminaux ne restent pas déconnectés de BlackBerry UEM au-delà du laps de temps spécifié. |
| Heure du dernier contact | Ce paramètre spécifie la durée (en nombre de jours) pendant laquelle un terminal peut rester déconnecté de BlackBerry UEM.<br>Ce paramètre s'applique uniquement si le paramètre Terminal non joignable est sélectionné. |
| Vérification de la version de la bibliothèque BlackBerry Dynamics | Ce paramètre crée une règle de conformité qui vous permet de sélectionner les versions de la bibliothèque BlackBerry Dynamics ne pouvant pas être activées.<br>Vous pouvez sélectionner les versions bloquées de la bibliothèque. |

| iOS : paramètre Profil de conformité | Description |
| --- | --- |
| Vérification de la connectivité BlackBerry Dynamics | Ce paramètre crée une règle de conformité pour veiller à ce que les applications BlackBerry Dynamics ne restent pas déconnectées de BlackBerry UEM au-delà du laps de temps spécifié. L'action de mise en œuvre concerne les applications BlackBerry Dynamics.<br><br>Le paramètre Baser l'intervalle de connectivité sur des applications de délégation de l'authentification indique que la vérification de la connectivité est basée sur le moment où une application de délégation de l'authentification se connecte à BlackBerry UEM. Ce paramètre s'applique uniquement si une délégation d'authentification est spécifiée dans un profil BlackBerry Dynamics.<br><br>Le paramètre Heure du dernier contact spécifie le nombre de jours pendant lesquels un terminal peut rester déconnecté de BlackBerry UEM avant de ne plus être conforme.<br><br>Les applications BlackBerry Dynamics n'invitent pas les utilisateurs à respecter cette règle. Si vous définissez le paramètre Comportement d'invite sur Invite à la conformité, l'utilisateur n'est pas invité à le faire. Si le terminal est en mesure de contacter UEM, il revient en conformité lorsque l'utilisateur ouvre l'application BlackBerry Dynamics. |
| Capture d'écran de l'application BlackBerry Dyr détectée | Ce paramètre crée une règle de conformité qui réagit aux captures d'écran des applications BlackBerry Dynamics sur les terminaux.<br><br>Le paramètre Nombre maximal de captures d'écran au cours de la période spécifie le nombre de captures d'écran autorisées dans le délai spécifié dans le champ Durée de la période.<br><br>Le paramètre Action d'application pour les applications BlackBerry Dynamics spécifie l'action qui se produit si l'utilisateur dépasse le nombre autorisé de captures d'écran. |

| iOS : paramètre Profil de conformité | Description |
|---|---|
| Une application interdite est installée | Ce paramètre crée une règle de conformité pour empêcher les utilisateurs d'installer certaines applications.<br><br>Pour interdire des applications, effectuez l'une des tâches suivantes :<br><br>• Sélectionnez une application dans la liste des applications interdites. Pour plus d'informations, reportez-vous à la section Ajouter une application à la liste des applications limitées.<br><br>Effectuez l'une des opérations suivantes :<br><br>• Pour sélectionner des applications à l'aide de leur nom, cliquez sur l'option Sélectionner les applications depuis la liste des applications.<br>• Pour sélectionner des applications en utilisant l'ID du package d'applications, cliquez sur l'option Spécifier l'ID du package d'applications. Vous ne devez pas utiliser l'ID du package pour ajouter des applications publiques. Ajoutez les applications publiques à la liste d'applications restreintes, puis utilisez l'option Sélectionner des applications dans la liste des applications pour sélectionner ces applications.<br>• Sélectionnez une application intégrée (terminaux supervisés uniquement).<br><br>Pour supprimer une application de la liste, cliquez sur ✕.<br><br>Lorsque vous sélectionnez ce paramètre et qu'une application interdite est installée sur un terminal, un message d'avertissement et un lien sont affichés sur l'onglet Terminaux gérés. Lorsque vous cliquez sur le lien, la liste des applications qui mettent le terminal hors conformité est affichée.<br><br>Les actions d'application de cette règle ne concernent pas les terminaux supervisés. L'installation d'applications interdites est impossible. Si des applications limitées (intégrées ou installées par l'utilisateur) sont déjà installées, ces applications sont automatiquement supprimées du terminal. |
| Afficher les applications autorisées sur le terminal uniquement | Ce paramètre crée une règle de conformité répertoriant les applications qui peuvent être installées sur les terminaux des utilisateurs. Toutes les autres applications sont interdites.<br><br>Pour autoriser des applications spécifiques, effectuez l'une des tâches suivantes :<br><br>• Sélectionnez une application dans la liste des applications interdites. Pour plus d'informations, reportez-vous à la section Ajouter une application à la liste des applications limitées.<br>• Sélectionnez une application intégrée.<br><br>Par défaut, certaines applications sont incluses dans la liste autorisée. Pour supprimer une application de la liste, cliquez sur ✕.<br><br>Ce paramètre est valide uniquement pour les terminaux supervisés. |

## macOS : paramètres de profil de conformité

Reportez-vous à la section Communs : paramètres de profil de conformité pour une description des actions possibles si vous sélectionnez une règle de conformité.

| macOS : paramètre de profil de conformité | Description |
|---|---|
| Une version limitée du SE est installée | Ce paramètre crée une règle de conformité pour vérifier qu'aucune version limitée du système d'exploitation n'est installée sur les terminaux.<br>Vous pouvez sélectionner les versions limitées du système d'exploitation.<br>Si vous sélectionnez ce paramètre, les utilisateurs ne pourront pas effectuer de nouvelles activations pour les terminaux qui ne sont pas conformes, quelle que soit l'action d'application que vous avez définie. |
| Modèle de terminal interdit détecté | Ce paramètre crée une règle de conformité permettant d'interdire certains modèles de terminaux.<br>Vous pouvez choisir l'une des options suivantes :<br>• Autoriser les modèles de terminaux sélectionnés<br>• Ne pas autoriser les modèles de terminaux sélectionnés<br>Vous pouvez sélectionner les modèles de terminaux autorisés ou interdits.<br>Si vous sélectionnez ce paramètre, les utilisateurs ne pourront pas effectuer de nouvelles activations pour les terminaux qui ne sont pas conformes, quelle que soit l'action d'application que vous avez définie. |
| Vérification de la version de la bibliothèque BlackBerry Dynamics | Ce paramètre crée une règle de conformité qui vous permet de sélectionner les versions de la bibliothèque BlackBerry Dynamics ne pouvant pas être activées.<br>Vous pouvez sélectionner les versions bloquées de la bibliothèque. |
| Vérification de la connectivité BlackBerry Dynamics | Ce paramètre crée une règle de conformité pour veiller à ce que les applications BlackBerry Dynamics ne restent pas déconnectées de BlackBerry UEM au-delà du laps de temps spécifié. L'action d'application concerne les applications BlackBerry Dynamics.<br>Le paramètre Baser l'intervalle de connectivité sur des applications de délégation de l'authentification indique que la vérification de la connectivité est basée sur le moment où une application de délégation de l'authentification se connecte à BlackBerry UEM. Ce paramètre s'applique uniquement si une délégation d'authentification est spécifiée dans un profil BlackBerry Dynamics.<br>Le paramètre Heure du dernier contact spécifie le nombre de jours pendant lesquels un terminal peut rester déconnecté de BlackBerry UEM avant de ne plus être conforme. |

### Android : Paramètres des profils de conformité

Reportez-vous à la section Communs : paramètres de profil de conformité pour une description des actions possibles si vous sélectionnez une règle de conformité.

| Android : paramètre de conformité | Description |
| --- | --- |
| SE « débridé » ou échec de l'attestation Knox | Ce paramètre crée une règle de conformité qui spécifie les actions qui se produisent si un utilisateur ou un utilisateur malveillant accède au niveau racine d'un terminal Android. Un terminal est flashé lorsqu'un utilisateur ou un utilisateur malveillant accède au niveau racine du système d'exploitation Android. Cette règle s'applique à l'état « débridé » du terminal qui est détecté par UEM Client, l'attestation BlackBerry Dynamics SDK ou Knox.<br><br>Si vous sélectionnez ce paramètre, les utilisateurs ne pourront pas effectuer de nouvelles activations pour les terminaux routés, quelle que soit l'action d'application que vous avez définie.<br><br>Si vous définissez une règle de conformité pour SE « débridé » ou échec de l'attestation Knox, la sélection de l'option Autoriser l'anti-débogage pour les applications BlackBerry Dynamics arrête les applications BlackBerry Dynamics si BlackBerry Dynamics Runtime détecte un outil de débogage actif. |
| Échec d'attestation SafetyNet | Ce paramètre crée une règle de conformité qui spécifie les actions qui se produisent si les terminaux ne passent pas l'attestation SafetyNet.<br><br>Lorsque vous utilisez l'attestation SafetyNet, BlackBerry UEM vérifie l'authenticité et l'intégrité des terminaux et des applications Android dans l'environnement de votre organisation.<br><br>Pour que ces paramètres prennent effet, vous devez activer la fonction d'attestation SafetyNet dans la console de gestion sous Paramètres > Attestation > Fréquence d'attestation SafetyNet.<br><br>Pour plus d'informations sur la configuration d'attestation SafetyNet, reportez-vous à la section Configuration de l'attestation des terminaux Android et des applications BlackBerry Dynamics à l'aide de SafetyNet. |
| L'application non attribuée est installée | Ce paramètre crée une règle de conformité pour empêcher l'installation d'applications non attribuées sur les terminaux des utilisateurs.<br><br>Lorsque vous sélectionnez ce paramètre et qu'une application non attribuée est installée sur un terminal Android, un message d'avertissement et un lien sont affichés sur l'onglet Terminaux gérés. Lorsque vous cliquez sur le lien, la liste des applications qui mettent le terminal hors conformité est affichée.<br><br>Pour les terminaux Android Enterprise et Samsung Knox, les utilisateurs ne peuvent pas installer d'applications non attribuées dans l'espace Travail. Les mesures d'application ne s'appliquent pas.<br><br>Ce paramètre ne s'applique pas aux terminaux activés en mode Confidentialité de l'utilisateur. |

| Android : paramètre de conformité | Description |
| --- | --- |
| Une application requise n'est pas installée | Ce paramètre crée une règle de conformité pour veiller à ce que les applications requises soient installées sur les terminaux.<br><br>Lorsque vous sélectionnez ce paramètre et qu'une application requise n'est pas installée sur un terminal Android, un message d'avertissement et un lien sont affichés sur l'onglet Terminaux gérés. Lorsque vous cliquez sur le lien, la liste des applications qui mettent le terminal hors conformité est affichée.<br><br>Pour les terminaux Android Enterprise, les actions d'application ne s'appliquent pas.<br><br>Pour les terminaux Samsung Knox, les applications internes requises sont automatiquement installées. Les mesures d'application s'appliquent uniquement aux applications publiques requises. |
| Une version limitée du SE est installée | Ce paramètre crée une règle de conformité pour vérifier qu'aucune version limitée du système d'exploitation n'est installée sur les terminaux.<br><br>Vous pouvez sélectionner les versions limitées du système d'exploitation.<br><br>Si vous sélectionnez ce paramètre, les utilisateurs ne pourront pas effectuer de nouvelles activations pour les terminaux qui ne sont pas conformes, quelle que soit l'action d'application que vous avez définie. |
| Modèle de terminal interdit détecté | Ce paramètre crée une règle de conformité permettant d'interdire certains modèles de terminaux.<br><br>Vous pouvez choisir l'une des options suivantes :<br><br>• Autoriser les modèles de terminaux sélectionnés<br>• Ne pas autoriser les modèles de terminaux sélectionnés<br><br>Vous pouvez spécifier les modèles de terminaux autorisés ou interdits.<br><br>Si vous sélectionnez ce paramètre, les utilisateurs ne pourront pas effectuer de nouvelles activations pour les terminaux qui ne sont pas conformes, quelle que soit l'action d'application que vous avez définie. |
| Terminal non joignable | Ce paramètre crée une règle de conformité pour veiller à ce que les terminaux ne restent pas déconnectés de BlackBerry UEM au-delà d'un laps de temps spécifié.<br><br>Le paramètre Heure du dernier contact spécifie le nombre de jours pendant lesquels un terminal peut rester déconnecté de BlackBerry UEM avant de ne plus être conforme. |

| Android : paramètre de conformité | Description |
| --- | --- |
| Niveau requis du correctif de sécurité manquant | Ce paramètre crée une règle de conformité pour veiller à ce que les correctifs de sécurité requis soient installés sur les terminaux.<br>Vous pouvez spécifier les modèles de terminal sur lesquels les correctifs de sécurité doivent être installés, ainsi qu'une date pour ces correctifs. Les terminaux exécutant un correctif de sécurité de date équivalente ou ultérieure aux dates de correctif de sécurité spécifiées sont considérés comme conformes.<br>Après une mise à niveau, si vous avez déjà créé un profil de conformité avec le paramètre Niveau requis du correctif de sécurité manquant activé, l'action d'application est définie sur Surveiller et consigner.<br>Ce paramètre est valide pour les terminaux et pour les applications BlackBerry Dynamics développées avec BlackBerry Dynamics SDK 6.0 et versions ultérieures. |
| Vérification de la version de la bibliothèque BlackBerry Dynamics | Ce paramètre crée une règle de conformité qui vous permet de sélectionner les versions de la bibliothèque BlackBerry Dynamics ne pouvant pas être activées.<br>Vous pouvez sélectionner les versions bloquées de la bibliothèque. |
| Vérification de la connectivité BlackBerry Dynamics | Ce paramètre crée une règle de conformité pour veiller à ce que les applications BlackBerry Dynamics ne restent pas déconnectées de BlackBerry UEM au-delà du laps de temps spécifié. L'action de mise en œuvre concerne les applications BlackBerry Dynamics.<br>Le paramètre Baser l'intervalle de connectivité sur des applications de délégation de l'authentification indique que la vérification de la connectivité est basée sur le moment où une application de délégation de l'authentification se connecte à BlackBerry UEM. Ce paramètre s'applique uniquement si une délégation d'authentification est spécifiée dans un profil BlackBerry Dynamics.<br>Le paramètre Heure du dernier contact spécifie le nombre de jours pendant lesquels un terminal peut rester déconnecté de BlackBerry UEM avant de ne plus être conforme.<br>Les applications BlackBerry Dynamics n'invitent pas les utilisateurs à respecter cette règle. Si vous définissez le paramètre Comportement d'invite sur Invite à la conformité, l'utilisateur n'est pas invité à le faire. Si le terminal est en mesure de contacter UEM, il revient en conformité lorsque l'utilisateur ouvre l'application BlackBerry Dynamics. |

| Android : paramètre de conformité | Description |
|---|---|
| Une application interdite est installée | Ce paramètre crée une règle de conformité pour vérifier qu'aucune application interdite n'est installée sur les terminaux. Pour limiter les applications, reportez-vous à la section Ajouter une application à la liste des applications limitées.<br><br>Pour les terminaux Android Enterprise, les utilisateurs ne peuvent pas installer d'applications interdites dans l'espace Travail. Les mesures d'application ne s'appliquent pas.<br><br>Pour les terminaux Samsung Knox, les applications interdites dans l'espace Travail sont automatiquement désactivées. Les mesures d'application ne s'appliquent pas.<br><br>Pour les terminaux Android Enterprise et Samsung Knox avec des activations Travail et Personnel - Contrôle total, sélectionnez Appliquer les mesures de conformité dans l'espace personnel pour appliquer la règle aux applications du profil professionnel et du profil personnel. Cette option est uniquement prise en charge sur les terminaux Android 10 et versions antérieures.<br><br>Ce paramètre ne s'applique pas aux terminaux activés en mode Confidentialité de l'utilisateur.<br><br>Lorsque vous sélectionnez ce paramètre et qu'une application interdite est installée sur un terminal Android, un message d'avertissement et un lien sont affichés sur l'onglet Terminaux gérés. Lorsque vous cliquez sur le lien, la liste des applications qui mettent le terminal hors conformité s'affiche.<br><br>**Remarque :** Si vous avez activé un terminal à l'aide du type d'activation Android Enterprise - Contrôle total et que vous utilisez cette option pour désactiver les applications côté personnel du terminal, lorsque le terminal est mis à niveau d'Android 10 vers Android 11, ces applications sont désactivées de manière permanente, sauf si vous réactivez le terminal. Pour en savoir plus, rendez-vous sur le site Web support.blackberry.com/community pour consulter l'article 76852. |
| Le mot de passe ne répond pas aux critères de complexité | Ce paramètre crée une règle de conformité pour faire en sorte que l'utilisateur définisse des mots de passe pour le terminal ou l'espace de travail répondant aux exigences de complexité définies dans la stratégie informatique qui leur a été attribuée. |

### Windows : Paramètres des profils de conformité

Reportez-vous à la section Communs : paramètres de profil de conformité pour une description des actions possibles si vous sélectionnez une règle de conformité.

| Windows : paramètre Profil de conformité | Description |
|---|---|
| Une application requise n'est pas installée | Ce paramètre crée une règle de conformité pour veiller à ce que les applications requises soient installées sur les terminaux.<br><br>Les dispositions des applications internes ne peuvent pas être surveillées. |

| Windows : paramètre Profil de conformité | Description |
|---|---|
| Une version limitée du SE est installée | Ce paramètre crée une règle de conformité pour veiller à ce qu'une version limitée du système d'exploitation ne soit pas installée sur les terminaux, comme spécifié dans ce paramètre.<br>Vous pouvez sélectionner les versions limitées du système d'exploitation. |
| Modèle de terminal interdit détecté | Ce paramètre crée une règle de conformité pour interdire les modèles de terminaux spécifiés.<br>Valeurs possibles :<br>• Autoriser les modèles de terminaux sélectionnés<br>• Ne pas autoriser les modèles de terminaux sélectionnés<br>Vous pouvez sélectionner les modèles de terminaux autorisés ou interdits. |
| Terminal non joignable | Ce paramètre crée une règle de conformité pour veiller à ce que les terminaux ne restent pas déconnectés de BlackBerry UEM au-delà du laps de temps spécifié. |
| Vérification de la version de la bibliothèque BlackBerry Dynamics | Ce paramètre crée une règle de conformité qui vous permet de sélectionner les versions de la bibliothèque BlackBerry Dynamics ne pouvant pas être activées.<br>Vous pouvez sélectionner les versions bloquées de la bibliothèque. |
| Vérification de la connectivité BlackBerry Dynamics | Ce paramètre crée une règle de conformité pour veiller à ce que les applications BlackBerry Dynamics ne restent pas déconnectés de BlackBerry UEM au-delà du laps de temps spécifié. L'action de mise en œuvre concerne les applications BlackBerry Dynamics. |
| Signature antivirus | Ce paramètre crée une règle de conformité pour veiller à ce qu'une signature antivirus soit activée sur les terminaux. |
| État de l'antivirus | Ce paramètre crée une règle de conformité pour veiller à ce qu'un logiciel antivirus soit activé sur les terminaux.<br>Vous pouvez sélectionner les fournisseurs autorisés. |
| État du pare-feu | Ce paramètre crée une règle de conformité pour veiller à ce qu'un pare-feu soit activé sur les terminaux. |
| État de cryptage | Ce paramètre crée une règle de conformité pour veiller à ce que le cryptage soit activé sur les terminaux. |
| État des mises à jour Windows | Ce paramètre crée une règle de conformité pour veiller à ce que les terminaux autorisent BlackBerry UEM à installer les mises à jour de Windows OS ou avertissent les utilisateurs lorsque des mises à jour obligatoires sont disponibles. |
| Une application interdite est installée | Ce paramètre crée une règle de conformité pour vérifier qu'aucune application interdite n'est installée sur les terminaux. Pour limiter les applications, reportez-vous à la section Ajouter une application à la liste des applications limitées. |

| Windows : paramètre Profil de conformité | Description |
|---|---|
| Le délai de grâce a expiré | Ce paramètre crée une règle de conformité pour spécifier les actions qui se produisent si l'attestation du délai de grâce a expiré. |
| La clé d'attestation d'identité n'est pas présente | Ce paramètre crée une règle de conformité pour indiquer les actions qui se produisent si la clé d'attestation d'identité n'est pas présente sur le terminal. |
| La politique de prévention de l'exécution des données est désactivée | Ce paramètre crée une règle de conformité pour spécifier les actions qui se produisent si la politique de prévention de l'exécution des données est désactivée sur le terminal. |
| BitLocker est désactivé | Ce paramètre crée une règle de conformité pour préciser les actions qui se produisent si BitLocker est désactivé sur le terminal. |
| Le démarrage sécurisé est désactivé | Ce paramètre crée une règle de conformité pour spécifier les actions qui se produisent si le démarrage sécurisé est désactivé sur le terminal. |
| L'intégrité du code est désactivée | Ce paramètre crée une règle de conformité pour exposer les actions qui se produisent si la fonction intégrité du code est désactivée sur le terminal. |
| Le terminal est en mode sécurisé | Ce paramètre crée une règle de conformité pour spécifier les actions qui se produisent si le terminal est en mode sécurisé. |
| Le terminal est dans l'environnement de pré-installation Windows | Ce paramètre crée une règle de conformité pour définir les actions qui se produisent si le terminal est dans l'environnement de pré-installation Windows. |
| Le lancement rapide du pilote contre les programmes malveillants ne s'est pas chargé | Ce paramètre crée une règle de conformité pour spécifier les actions qui se produisent si le lancement rapide du pilote contre les programmes malveillants n'est pas chargé. |
| Le mode sécurisé virtuel est désactivé | Ce paramètre crée une règle de conformité pour déterminer les actions qui se produisent si le mode sécurisé virtuel est désactivé. |
| Le débogage au démarrage est activé | Ce paramètre crée une règle de conformité pour spécifier les actions qui se produisent si le débogage au démarrage est activé. |
| Le débogage du noyau sur le système d'exploitation OS est activé | Ce paramètre crée une règle de conformité pour indiquer les actions qui se produisent si le débogage du noyau sur le système d'exploitation OS est activé. |
| La signature test est activée | Ce paramètre crée une règle de conformité pour préciser les actions qui se produisent si la signature test est activée. |

| Windows : paramètre Profil de conformité | Description |
|---|---|
| La liste de révision du gestionnaire de démarrage n'est pas la version attendue | Ce paramètre crée une règle de conformité pour définir les actions qui se produisent si la liste de révision du gestionnaire de démarrage n'est pas la version attendue. |
| La liste de révision de l'intégrité du code n'est pas la version attendue | Ce paramètre crée une règle de conformité pour exposer les actions qui se produisent si la liste de révision de l'intégrité du code n'est pas la version attendue. |
| Le hachage de la stratégie d'intégrité du code est présent et sa valeur n'est pas autorisée | Ce paramètre crée une règle de conformité pour spécifier les actions qui se produisent si le hachage de la stratégie d'intégrité du code est présent et que sa valeur n'est pas autorisée. |
| Le hachage de la stratégie de configuration du démarrage sécurisé personnalisé est présent et sa valeur n'est pas autorisée | Ce paramètre crée une règle de conformité pour indiquer les actions qui se produisent si le hachage de la stratégie de configuration du démarrage sécurisé personnalisé est présent et que sa valeur n'est pas autorisée. |
| La valeur PCR n'est pas une valeur autorisée | Ce paramètre crée une règle de conformité pour préciser les actions qui se produisent si la valeur PCR n'est pas une valeur autorisée. |

# Gérer les profils de conformité BlackBerry Dynamics

Des profils de conformité BlackBerry Dynamics sont importés de Good Control lorsque vous synchronisez Good Control avec BlackBerry UEM. Vous ne pouvez pas modifier les profils de conformité BlackBerry Dynamics, mais ceux-ci peuvent être utilisés comme référence lors de la création de nouveaux profils de conformité dans BlackBerry UEM. Les utilisateurs auxquels un profil de conformité a été attribué dans Good Control conservent le même profil à l'issue de la synchronisation avec BlackBerry UEM. Lorsqu'un profil de conformité BlackBerry Dynamics est attribué à un utilisateur, ce profil de conformité BlackBerry Dynamics est prioritaire sur les règles BlackBerry Dynamics des autres profils de conformité BlackBerry UEM attribués à l'utilisateur, le cas échéant.

| Paramètre | Description |
|---|---|
| Système d'exploitation cracké | Ce paramètre spécifie les actions prises si un utilisateur ou un utilisateur malveillant contourne diverses restrictions sur un terminal pour modifier le système d'exploitation, installer des applications non approuvées ou obtenir des autorisations élevées, ainsi que les actions prises pour les applications BlackBerry Dynamics si un système d'exploitation cracké est utilisé. |

| Paramètre | Description |
| --- | --- |
| Vérification du système d'exploitation | Ce paramètre spécifie les versions autorisées et interdites du système d'exploitation ainsi que les actions prises pour les applications BlackBerry Dynamics si un système d'exploitation interdit est installé sur un terminal. |
| Vérification du modèle de matériel | Ce paramètre spécifie les modèles de matériel autorisés et interdits ainsi que les actions prises pour les applications BlackBerry Dynamics si un modèle de matériel interdit est utilisé. |
| Vérification de la version de la bibliothèque BlackBerry Dynamics | Ce paramètre spécifie les bibliothèques BlackBerry Dynamics qui peuvent être utilisées ainsi que les actions prises pour les applications BlackBerry Dynamics si un terminal utilise une version non autorisée de la bibliothèque. |
| Vérification de la connectivité | Ce paramètre spécifie si un terminal doit se connecter à BlackBerry UEM sous un certain nombre de jours ainsi que les actions prises pour les applications BlackBerry Dynamics si un terminal ne se connecte pas à BlackBerry UEM.<br><br>Le sous-paramètre Baser l'intervalle de connectivité sur des applications de délégation de l'authentification détermine si l'application définie comme délégué d'authentification gère l'intervalle de connectivité.<br>Si vous utilisez le délégué d'authentification pour gérer l'intervalle de connectivité, les applications les moins utilisées ne seront ni bloquées ni nettoyées si elles ne se connectent pas à BlackBerry UEM. |

# Envoi de commandes aux utilisateurs et aux terminaux

Vous pouvez envoyer diverses commandes pour gérer les comptes utilisateur et les terminaux. La liste des commandes disponibles dépend du type de terminal et d'activation. Vous pouvez envoyer des commandes à un utilisateur ou un terminal en particulier ou à plusieurs utilisateurs et terminaux à l'aide de commandes groupées.

Par exemple, vous pouvez utiliser les commandes dans les situations suivantes :

- Si un terminal a été égaré, vous pouvez envoyer une commande pour le verrouiller ou supprimer les données professionnelles qu'il contient.
- Si vous souhaitez redistribuer un terminal à un autre utilisateur de votre entreprise, ou si un terminal a été perdu ou volé, vous pouvez envoyer une commande pour supprimer toutes les données qu'il contient.
- Lorsqu'un employé quitte votre organisation, vous pouvez envoyer une commande au terminal personnel de l'utilisateur afin de supprimer uniquement les données professionnelles.
- Si un utilisateur a oublié le mot de passe de son espace Travail, vous pouvez envoyer une commande pour réinitialiser ce mot de passe.
- Pour les utilisateurs disposant de terminaux DEP supervisés, vous pouvez envoyer une commande de mise à jour du système d'exploitation.

## Envoyer une commande à un terminal

**Avant de commencer :**

Si vous souhaitez définir une période d'expiration pour les commandes de BlackBerry UEM qui suppriment des données sur les terminaux, reportez-vous à la section Définir une heure d'expiration pour les commandes.

1. Sur la barre de menus, cliquez sur **Utilisateurs > Terminaux gérés**.
2. Recherchez un compte d'utilisateur.
3. Dans les résultats de la recherche, cliquez sur le nom du compte d'utilisateur.
4. Cliquez sur l'onglet du terminal.
5. Dans la fenêtre **Gérer le terminal**, sélectionnez la commande que vous souhaitez envoyer au terminal.

## Envoyer une commande groupée

Vous pouvez envoyer une commande à plusieurs comptes d'utilisateurs ou terminaux à la fois en sélectionnant les utilisateurs ou les terminaux dans la liste des utilisateurs et en envoyant une commande groupée.

**Avant de commencer :** Si vous souhaitez définir une période d'expiration pour les commandes qui suppriment des données sur les terminaux, reportez-vous à Définir une heure d'expiration pour les commandes.

1. Sur la barre de menus, cliquez sur **Utilisateurs > Terminaux gérés**.
2. Si nécessaire, filtrez la liste des utilisateurs.
3. Effectuez l'une des opérations suivantes :
   - Cochez la case en haut de la liste d'utilisateurs pour sélectionner tous les utilisateurs et les terminaux de la liste.
   - Cochez la case pour chaque utilisateur et terminal que vous souhaitez inclure. Vous pouvez appuyer sur Maj+Clic pour sélectionner plusieurs utilisateurs.
4. Dans le menu, cliquez sur l'une des icônes suivantes :

| Icône | Description |
|---|---|
|  | Localiser les terminaux<br>Vous pouvez sélectionner jusqu'à 100 terminaux simultanément.<br>Pour plus d'informations, reportez-vous à Localiser un terminal. |
|  | Envoyer un e-mail<br>Pour plus d'informations, reportez-vous à la section Envoyer un e-mail aux utilisateurs. |
|  | Envoyer un e-mail d'activation<br>Pour plus d'informations, reportez-vous à la section Envoyer un e-mail d'activation à plusieurs utilisateurs. |
|  | Ajouter à des groupes d'utilisateurs<br>Vous pouvez sélectionner jusqu'à 200 terminaux simultanément.<br>Pour plus d'informations, reportez-vous à la section Ajouter des utilisateurs à des groupes d'utilisateurs. |
|  | Exporter<br>Pour plus d'informations, reportez-vous à la section Exporter une liste d'utilisateurs vers un fichier .csv. |
|  | Supprimer les terminaux<br>Seuls les administrateurs de sécurité peuvent utiliser cette commande groupée. Vous pouvez sélectionner jusqu'à 200 terminaux simultanément.<br>Pour plus d'informations, reportez-vous à Référence des commandes. |
|  | Mettre à jour les informations sur le terminal<br>Pour plus d'informations, reportez-vous à Référence des commandes. |
|  | Supprimer toutes les données du terminal<br>Seuls les administrateurs de sécurité peuvent utiliser cette commande. Vous pouvez sélectionner jusqu'à 200 terminaux simultanément. Cette commande groupée n'est pas prise en charge pour les terminaux macOS.<br>Pour plus d'informations, reportez-vous à Référence des commandes. |
|  | Supprimer uniquement les données professionnelles<br>Seuls les administrateurs de sécurité peuvent utiliser cette commande. Vous pouvez sélectionner jusqu'à 200 terminaux simultanément.<br>Pour plus d'informations, reportez-vous à Référence des commandes. |

| Icône | Description |
|---|---|
| | Modifier la propriété du terminal<br>Vous pouvez sélectionner jusqu'à 100 terminaux simultanément.<br>Pour plus d'informations, reportez-vous à la section Modifier l'étiquette de propriété du terminal. |
| | Mettre à jour le système d'exploitation<br>Vous pouvez forcer les terminaux supervisés iOS à installer une mise à jour de système d'exploitation disponible. Seuls les administrateurs de sécurité peuvent utiliser cette commande. Vous pouvez sélectionner jusqu'à 200 terminaux simultanément.<br>Pour plus d'informations, reportez-vous à Mettre à jour le système d'exploitation sur les terminaux iOS supervisés. |
| | Modifier les mots de passe de console<br>Vous pouvez envoyer un mot de passe BlackBerry UEM Self-Service à plusieurs utilisateurs à la fois.<br>Pour plus d'informations, reportez-vous à la section Envoyer un mot de passe BlackBerry UEM Self-Service à plusieurs utilisateurs. |

# Définir une heure d'expiration pour les commandes

Lorsque vous envoyez la commande « Supprimer toutes les données du terminal » ou « Supprimer uniquement des données professionnelles » à un terminal, ce dernier doit être connecté à BlackBerry UEM pour que la commande se termine. Si le terminal ne parvient pas à se connecter à BlackBerry UEM, la commande reste en attente et le terminal n'est pas supprimé de BlackBerry UEM sauf si vous le supprimez manuellement. Sinon, vous pouvez configurer BlackBerry UEM pour supprimer automatiquement les terminaux lorsque les commandes ne se terminent pas après le délai spécifié.

1. Dans la barre de menus, cliquez sur **Paramètres > Paramètres généraux > Expiration de la commande de suppression**.
2. Pour l'une ou les deux commandes **Supprimer toutes les données du terminal** et **Supprimer uniquement les données professionnelles**, sélectionnez **Supprimer automatiquement le terminal si la commande expire**.
3. Dans le champ **Expiration de la commande**, saisissez le nombre de jours après lequel la commande expire et le terminal est automatiquement retiré de BlackBerry UEM.
4. Cliquez sur **Enregistrer**.

# Référence des commandes

Les commandes que vous pouvez envoyer aux terminaux dépendent du type de terminal et d'activation. Vous pouvez envoyer certaines commandes à plusieurs terminaux en même temps.

## Commandes pour terminaux iOS

Ces commandes s'appliquent également aux terminaux iPadOS.

| Commande | Description | Types d'activation |
|---|---|---|
| Afficher le rapport de terminal | Cette commande affiche des informations détaillées sur un terminal. Vous pouvez exporter et enregistrer le rapport de terminal sur votre ordinateur. Pour plus d'informations, reportez-vous à la section Afficher et enregistrer un rapport de terminal. | Contrôles MDM<br>Confidentialité de l'utilisateur |
| Afficher les actions du terminal | Cette commande affiche les actions en cours sur un terminal. Pour plus d'informations, reportez-vous à la section Affichage des actions du terminal. | Contrôles MDM<br>Confidentialité de l'utilisateur |
| Supprimer toutes les données du terminal | Cette commande supprime toutes les informations utilisateur et données d'application stockées sur le terminal et rétablit les paramètres d'usine par défaut.<br>Si le terminal ne parvient pas à se connecter à BlackBerry UEM lorsque vous envoyez cette commande, vous pouvez annuler la commande ou supprimer le terminal de la console. Si le terminal se connecte à BlackBerry UEM à l'issue de sa suppression, seules les données professionnelles sont supprimées du terminal.<br>Pour envoyer cette commande à plusieurs terminaux, reportez-vous à la section Envoyer une commande groupée. | Contrôles MDM |
| Supprimer uniquement les données professionnelles | Cette commande supprime les données professionnelles, y compris les stratégies informatiques, profils, applications et certificats présents sur le terminal.<br>Si le terminal ne parvient pas à se connecter à BlackBerry UEM lorsque vous envoyez cette commande, vous pouvez annuler la commande ou supprimer le terminal de la console. Si le terminal se connecte à BlackBerry UEM à l'issue de sa suppression, les données professionnelles sont supprimées du terminal.<br>Pour envoyer cette commande à plusieurs terminaux, reportez-vous à la section Envoyer une commande groupée. | Contrôles MDM<br>Confidentialité de l'utilisateur |
| Verrouiller le terminal | Cette commande verrouille un terminal. L'utilisateur doit saisir le mot de passe du terminal existant pour déverrouiller le terminal. Si un terminal est temporairement perdu, vous pouvez utiliser cette commande.<br>Lorsque vous envoyez cette commande, le terminal se verrouille uniquement s'il existe un mot de passe de terminal. Sinon, aucune action n'est prise sur le terminal.<br>Cette commande n'est pas prise en charge par les terminaux Apple TV. | Contrôles MDM |

| Commande | Description | Types d'activation |
|---|---|---|
| Déverrouiller le terminal et effacer le mot de passe | Cette commande déverrouille le terminal et supprime le mot de passe existant. L'utilisateur est invité à créer un mot de passe. Vous pouvez utiliser cette commande si l'utilisateur oublie le mot de passe de son terminal.<br>Cette commande n'est pas prise en charge par les terminaux Apple TV. | Contrôles MDM |
| Activer le mode Perdu | Cette commande verrouille le terminal et vous permet de définir le numéro de téléphone et le message à afficher sur l'écran. Par exemple, vous pouvez afficher le numéro à appeler par la personne qui trouvera le terminal.<br>Après avoir envoyé cette commande, vous verrez l'emplacement du terminal sur BlackBerry UEM.<br>Cette commande est prise en charge sur les terminaux supervisés uniquement.<br>Cette commande n'est pas prise en charge par les terminaux Apple TV. | Contrôles MDM |
| Désactiver BlackBerry 2FA | Cette commande désactive les terminaux qui sont activés avec le type d'activation BlackBerry 2FA. Le terminal est supprimé de BlackBerry UEM et l'utilisateur ne peut pas utiliser la fonction BlackBerry 2FA.<br>Cette commande n'est pas prise en charge par les terminaux Apple TV. | Contrôles MDM |
| Mettre à jour le système d'exploitation | Cette commande force les terminaux à installer une mise à jour de système d'exploitation disponible.<br>Pour plus d'informations, reportez-vous à la section Mettre à jour le système d'exploitation sur les terminaux iOS sous supervision.<br>Pour envoyer cette commande à plusieurs terminaux, reportez-vous à la section Envoyer une commande groupée.<br>Cette commande est prise en charge sur les terminaux supervisés uniquement.<br>Cette commande n'est pas prise en charge par les terminaux Apple TV. | Contrôles MDM |
| Redémarrer le terminal | Cette commande force les terminaux à redémarrer.<br>Cette commande est prise en charge sur les terminaux supervisés uniquement.<br>Cette commande n'est pas prise en charge par les terminaux Apple TV. | Contrôles MDM |

| Commande | Description | Types d'activation |
|---|---|---|
| Désactiver le terminal | Cette commande force les terminaux à se désactiver.<br>Cette commande est prise en charge sur les terminaux supervisés uniquement.<br>Cette commande n'est pas prise en charge par les terminaux Apple TV. | Contrôles MDM |
| Nettoyage des applications | Cette commande nettoie les données de toutes les applications gérées par Microsoft Intune sur le terminal. Les applications ne sont pas supprimées du terminal.<br>Pour plus d'informations, reportez-vous à la section Nettoyage des applications gérées par Microsoft Intune. | Contrôles MDM |
| Mettre à jour les informations du terminal | Cette commande envoie et reçoit des informations mises à jour sur le terminal. Par exemple, vous pouvez envoyer des règles de stratégie informatique ou des profils mis à jour à un terminal et recevoir des informations mises à jour sur un terminal comme la version du système d'exploitation ou le niveau de la batterie.<br>Pour envoyer cette commande à plusieurs terminaux, reportez-vous à la section Envoyer une commande groupée. | Contrôles MDM<br>Confidentialité de l'utilisateur |
| Mettre à jour le fuseau horaire | Cette commande définit l'heure du terminal en fonction de la région que vous sélectionnez. | Contrôles MDM |
| Supprimer le terminal | Cette commande supprime le terminal de BlackBerry UEM mais ne supprime pas les données de celui-ci. Le terminal peut continuer à recevoir des e-mails et d'autres données professionnelles.<br>Cette commande est destinée aux terminaux qui ont été irrémédiablement perdus ou endommagés et qui ne sont pas censés contacter à nouveau le serveur. Si un terminal supprimé tente de contacter BlackBerry UEM, l'utilisateur reçoit une notification et le terminal ne pourra pas communiquer avec BlackBerry UEM s'il n'est pas réactivé.<br>Pour envoyer cette commande à plusieurs terminaux, reportez-vous à la section Envoyer une commande groupée. | Contrôles MDM<br>Confidentialité de l'utilisateur |
| Actualiser les plans cellulaires eSIM | Pour les terminaux disposant d'un forfait cellulaire basé sur une carte eSIM, cette commande interroge les détails du forfait mis à jour pour le terminal à partir de l'URL de l'opérateur du terminal. | Contrôles MDM |

### Commandes pour terminaux macOS

| Commande | Description |
|---|---|
| Afficher le rapport de terminal | Cette commande affiche des informations détaillées sur un terminal. Vous pouvez exporter et enregistrer le rapport de terminal sur votre ordinateur. Pour plus d'informations, reportez-vous à la section Afficher et enregistrer un rapport de terminal. |
| Afficher les actions du terminal | Cette commande affiche les actions en cours sur un terminal. Pour plus d'informations, reportez-vous à la section Affichage des actions du terminal. |
| Verrouiller le bureau | Cette commande permet de définir un code PIN et de verrouiller le terminal. |
| Supprimer uniquement les données professionnelles | Cette commande supprime les données professionnelles, y compris les stratégies informatiques, profils, applications et certificats présents sur le terminal et supprime éventuellement le terminal de BlackBerry UEM.<br>Pour envoyer cette commande a plusieurs appareils, voir Envoyer une commande groupée. |
| Supprimer toutes les données du terminal | Cette commande permet de supprimer les informations utilisateur et les données des applications stockées du terminal. Il rétablit les réglages d'usine par défaut du terminal, verrouille le terminal avec un code PIN que vous définissez et supprime éventuellement le terminal du BlackBerry UEM. |
| Mettre à jour les données du bureau | Cette commande envoie et reçoit des informations mises à jour sur le terminal. Par exemple, vous pouvez envoyer des règles de stratégie informatique ou des profils mis à jour à un terminal et recevoir des informations mises à jour sur un terminal comme la version du système d'exploitation ou le niveau de la batterie.<br>Pour envoyer cette commande a plusieurs appareils, voir Envoyer une commande groupée. |
| Supprimer le terminal | Cette commande supprime le terminal de BlackBerry UEM. Le terminal peut continuer à recevoir des e-mails et d'autres données professionnelles.<br>Pour envoyer cette commande a plusieurs appareils, voir Envoyer une commande groupée. |

### Commandes pour terminaux Android

| Commande | Description | Types d'activation |
|---|---|---|
| Afficher le rapport de terminal | Cette commande affiche des informations détaillées sur un terminal. Vous pouvez exporter et enregistrer le rapport de terminal sur votre ordinateur. Pour plus d'informations, reportez-vous à la section Afficher et enregistrer un rapport de terminal. | Tous (sauf BlackBerry 2FA) |
| Afficher les actions du terminal | Cette commande affiche les actions en cours sur un terminal. Pour plus d'informations, reportez-vous à la section Affichage des actions du terminal. | Tous (sauf BlackBerry 2FA) |

| Commande | Description | Types d'activation |
| --- | --- | --- |
| Verrouiller le terminal | Cette commande verrouille le terminal. L'utilisateur doit saisir le mot de passe du terminal existant pour déverrouiller le terminal. Si un terminal est temporairement perdu, vous pouvez utiliser cette commande.<br><br>Lorsque vous envoyez cette commande, le terminal se verrouille uniquement s'il existe un mot de passe de terminal. Sinon, aucune action n'est prise sur le terminal. | Contrôles MDM<br><br>Travail et Personnel - Contrôle total (Android Enterprise)<br><br>Travail et Personnel - Confidentialité des données de l'utilisateur (Android Enterprise)<br><br>Espace Travail uniquement (Android Enterprise) |
| Supprimer toutes les données du terminal | Cette commande supprime toutes les informations utilisateur et données d'application stockées sur le terminal, y compris les informations de l'espace Travail, et rétablit les paramètres d'usine par défaut du terminal.<br><br>Si le terminal ne parvient pas à se connecter à BlackBerry UEM lorsque vous envoyez cette commande, vous pouvez annuler la commande ou supprimer le terminal de la console. Si le terminal se connecte à BlackBerry UEM après que vous l'avez supprimé, seules les données professionnelles sont supprimées du terminal, y compris de l'espace Travail, le cas échéant.<br><br>Pour envoyer cette commande à plusieurs terminaux, reportez-vous à la section Envoyer une commande groupée. | Contrôles MDM<br><br>Travail et Personnel - Contrôle total (Android Enterprise)<br><br>Travail et Personnel - Contrôle total (Samsung Knox)<br><br>Espace Travail uniquement - (Samsung Knox) |

| Commande | Description | Types d'activation |
| --- | --- | --- |
| Supprimer uniquement les données professionnelles | Cette commande supprime les données professionnelles, y compris la stratégie informatique, les profils, les applications et les certificats qui sont sur le terminal, et désactive le terminal. Si le terminal dispose d'un espace Travail, les informations relatives à l'espace Travail et l'espace Travail lui-même sont supprimés du terminal, mais toutes les applications et données personnelles restent sur le terminal. Pour plus d'informations, consultez la section Désactivation des terminaux.<br><br>Lorsque vous utilisez cette commande sur les terminaux Android Enterprise, vous pouvez saisir une raison qui apparaîtra dans la notification sur le terminal de l'utilisateur pour expliquer pourquoi le profil professionnel a été supprimé.<br><br>Pour les activations Travail et Personnel - Contrôle total (Android Enterprise), cette commande est prise en charge uniquement par les terminaux exécutant Android 11 et versions ultérieures.<br><br>Si le terminal ne parvient pas à se connecter à BlackBerry UEM lorsque vous envoyez cette commande, vous pouvez annuler la commande ou supprimer le terminal de la console. Si le terminal se connecte à BlackBerry UEM après que vous l'avez supprimé, les données professionnelles sont supprimées du terminal, y compris de l'espace Travail, le cas échéant.<br><br>Pour envoyer cette commande à plusieurs terminaux, reportez-vous à la section Envoyer une commande groupée. | Contrôles MDM<br><br>Travail et Personnel - Confidentialité des données de l'utilisateur (Android Enterprise)<br><br>Travail et Personnel - Contrôle total (Android Enterprise)<br><br>Travail et Personnel - Confidentialité des données de l'utilisateur (Samsung Knox)<br><br>Travail et Personnel - Contrôle total (Samsung Knox)<br><br>Espace Travail uniquement - (Samsung Knox) |
| Déverrouiller le terminal et effacer le mot de passe | Cette commande déverrouille le terminal et invite l'utilisateur à créer un nouveau mot de passe pour le terminal. Si l'utilisateur ignore le message l'invitant à créer un mot de passe pour le terminal, le mot de passe existant est conservé. Vous pouvez utiliser cette commande si un utilisateur oublie le mot de passe de son terminal.<br><br>**Remarque :** Cette commande n'est pas prise en charge par les terminaux dotés de Samsung Knox SDK 3.2.1 ou version ultérieure. | Contrôles MDM (terminaux Samsung uniquement)<br><br>Travail et Personnel - Contrôle total (Samsung Knox)<br><br>Travail et Personnel - Confidentialité des données de l'utilisateur (Samsung Knox) |

| Commande | Description | Types d'activation |
| --- | --- | --- |
| Spécifier le mot de passe du terminal et verrouiller le terminal | Cette commande vous permet de créer un mot de passe, puis de verrouiller le terminal. Vous devez créer un mot de passe conforme aux règles de mots de passe existantes. Pour déverrouiller le terminal, l'utilisateur doit saisir le nouveau mot de passe.<br>**Remarque :** Pour les types d'activation Travail et Personnel - Confidentialité des données de l'utilisateur, seuls les terminaux BlackBerry optimisés par Android version 8.x et ultérieure prennent en charge cette commande.<br>**Remarque :** Pour le type d'activation Travail et Personnel - Contrôle total (Android Enterprise), seuls les terminaux qui utilisent une version du système d'exploitation Android antérieure à Android 11 prennent en charge cette commande. | Travail et Personnel - Contrôle total (Samsung Knox)<br>Espace Travail uniquement (Android Enterprise)<br>Travail et Personnel - Contrôle total (Android Enterprise)<br>Travail et Personnel - Confidentialité des données de l'utilisateur (Android Enterprise) |
| Réinitialiser le mot de passe de l'espace Travail | Cette commande supprime le mot de passe actuel de l'espace Travail du terminal. Lorsque l'utilisateur ouvre l'espace Travail, le terminal l'invite à définir un nouveau mot de passe de l'espace Travail. | Travail et Personnel - Contrôle total (Samsung Knox)<br>Travail et Personnel - Confidentialité des données de l'utilisateur - (Samsung Knox)<br>Espace Travail uniquement - (Samsung Knox) |
| Spécifier le mot de passe de l'espace Travail et verrouiller | Vous pouvez définir un mot de passe de profil professionnel et verrouiller le terminal. Lorsque l'utilisateur ouvre une application professionnelle, il doit saisir le mot de passe que vous avez défini. | Travail et Personnel - Confidentialité des données de l'utilisateur (Android Enterprise)<br>Travail et Personnel - Contrôle total (Android Enterprise) |
| Désactiver/ Activer l'espace Travail | Cette commande désactive ou active l'accès aux applications de l'espace Travail sur le terminal. | Travail et Personnel - Contrôle total (Samsung Knox)<br>Travail et Personnel - Confidentialité des données de l'utilisateur - (Samsung Knox)<br>Espace Travail uniquement - (Samsung Knox) |
| Désactiver BlackBerry 2FA | Cette commande désactive les terminaux qui sont activés avec le type d'activation BlackBerry 2FA. Le terminal est supprimé de BlackBerry UEM et l'utilisateur ne peut pas utiliser la fonction BlackBerry 2FA. | BlackBerry 2FA |

| Commande | Description | Types d'activation |
|---|---|---|
| Nettoyage des applications | Cette commande nettoie les données de toutes les applications gérées par Microsoft Intune sur le terminal. Les applications ne sont pas supprimées du terminal.<br>Pour plus d'informations, reportez-vous à la section Nettoyage des applications gérées par Microsoft Intune | Tout (sauf BlackBerry 2FA) |
| Mettre à jour les informations du terminal | Cette commande envoie et reçoit des informations mises à jour sur le terminal. Par exemple, vous pouvez envoyer des règles de stratégie informatique ou des profils mis à jour à un terminal et recevoir des informations mises à jour sur un terminal comme la version du système d'exploitation ou le niveau de la batterie.<br>Pour envoyer cette commande à plusieurs terminaux, reportez-vous à la section Envoyer une commande groupée. | Tous (sauf BlackBerry 2FA) |
| Demander un rapport de bogues | Cette commande envoie une requête au terminal pour les journaux du client. L'utilisateur du terminal doit accepter ou refuser la requête. | Espace Travail uniquement (Android Enterprise)<br>Travail et Personnel - Contrôle total (Android Enterprise) |
| Redémarrer le terminal | Cette commande envoie une requête de redémarrage au terminal. Un message s'affiche pour indiquer à l'utilisateur que le terminal va redémarrer dans une minute. L'utilisateur du terminal peut reporter le redémarrage pour 10 minutes. | Espace Travail uniquement (Android Enterprise) |
| Supprimer le terminal | Cette commande supprime le terminal de BlackBerry UEM mais ne supprime pas les données de celui-ci. Le terminal peut continuer à recevoir des e-mails et d'autres données professionnelles.<br>Cette commande est destinée aux terminaux qui ont été irrémédiablement perdus ou endommagés et qui ne sont pas censés contacter à nouveau le serveur. Si un terminal supprimé tente de contacter BlackBerry UEM, l'utilisateur reçoit une notification et le terminal ne pourra pas communiquer avec BlackBerry UEM s'il n'est pas réactivé.<br>Pour envoyer cette commande à plusieurs terminaux, reportez-vous à la section Envoyer une commande groupée. | Tous (sauf BlackBerry 2FA) |

### Commandes pour terminaux Windows

| Commande | Description |
|---|---|
| Afficher le rapport de terminal | Cette commande affiche des informations détaillées sur un terminal. Vous pouvez exporter et enregistrer le rapport de terminal sur votre ordinateur. Pour plus d'informations, reportez-vous à la section Afficher et enregistrer un rapport de terminal. |
| Afficher les actions du terminal | Cette commande affiche les actions en cours sur un terminal. Pour plus d'informations, reportez-vous à la section Affichage des actions du terminal. |
| Verrouiller le terminal | Cette commande verrouille un terminal. L'utilisateur doit saisir le mot de passe du terminal existant pour déverrouiller le terminal. Si un terminal est temporairement perdu, vous pouvez utiliser cette commande.<br>Lorsque vous envoyez cette commande, le terminal se verrouille uniquement s'il existe un mot de passe de terminal. Sinon, aucune action n'est prise sur le terminal.<br>Cette commande est uniquement prise en charge sur les terminaux exécutant Windows 10 Mobile. |
| Générer le mot de passe et verrouiller le terminal | Cette commande génère un mot de passe et verrouille le terminal. Le mot de passe généré est envoyé par e-mail à l'utilisateur. Vous pouvez utiliser l'adresse électronique présélectionnée ou spécifier une adresse électronique. Le mot de passe généré est conforme aux règles de mots de passe existantes.<br>Cette commande est uniquement prise en charge sur les terminaux exécutant Windows 10 Mobile. |
| Supprimer uniquement les données professionnelles | Cette commande supprime les données professionnelles, y compris les stratégies informatiques, profils, applications et certificats présents sur le terminal et supprime éventuellement le terminal de BlackBerry UEM.<br>Le compte d'utilisateur n'est pas supprimé lorsque vous envoyez cette commande.<br>Après avoir envoyé cette commande, vous avez la possibilité de supprimer le terminal de BlackBerry UEM. Si le terminal ne parvient pas à se connecter à BlackBerry UEM, vous pouvez le supprimer de BlackBerry UEM. Si le terminal se connecte à BlackBerry UEM alors que vous l'avez supprimé, seules les données professionnelles sont supprimées du terminal, y compris de l'espace Travail, le cas échéant.<br>Pour envoyer cette commande a plusieurs appareils, voir Envoyer une commande groupée. |

| Commande | Description |
| --- | --- |
| Supprimer toutes les données du terminal | Cette commande permet de supprimer les informations utilisateur et les données des applications stockées sur le terminal. Elle rétablit les paramètres d'usine par défaut sur le terminal et supprime éventuellement le terminal de BlackBerry UEM.<br><br>Après avoir envoyé cette commande, vous avez la possibilité de supprimer le terminal de BlackBerry UEM. Si le terminal ne parvient pas à se connecter à BlackBerry UEM, vous pouvez le supprimer de BlackBerry UEM. Si le terminal se connecte à BlackBerry UEM alors que vous l'avez supprimé, seules les données professionnelles sont supprimées du terminal, y compris de l'espace Travail, le cas échéant.<br><br>Pour envoyer cette commande a plusieurs appareils, voir Envoyer une commande groupée. |
| Redémarrer le bureau/ terminal | Cette commande force les terminaux à redémarrer. |
| Mettre à jour les informations du terminal | Cette commande envoie et reçoit des informations mises à jour sur le terminal. Par exemple, vous pouvez envoyer des règles de stratégie informatique ou des profils mis à jour à un terminal et recevoir des informations mises à jour sur un terminal comme la version du système d'exploitation ou le niveau de la batterie.<br><br>La commande envoie une requête au terminal pour créer une demande de validation de certificat d'intégrité. Le terminal envoie la requête au service d'attestation d'intégrité Microsoft pour en vérifier la conformité. Cette fonctionnalité est uniquement prise en charge dans un environnement sur site.<br><br>Pour envoyer cette commande a plusieurs appareils, voir Envoyer une commande groupée. |
| Supprimer le terminal | Cette commande supprime le terminal de BlackBerry UEM. Le terminal peut continuer à recevoir des e-mails et d'autres données professionnelles.<br><br>Pour envoyer cette commande a plusieurs appareils, voir Envoyer une commande groupée. |

# Désactivation des terminaux

Lorsque vous ou un utilisateur désactivez un terminal, la connexion entre le terminal et le compte d'utilisateur dans BlackBerry UEM est supprimée. Vous ne pouvez pas gérer le terminal, et ce dernier ne s'affiche plus dans la console de gestion. L'utilisateur ne peut pas accéder aux données professionnelles du terminal.

Vous pouvez désactiver un terminal à l'aide de la commande Supprimer uniquement les données professionnelles ou Supprimer toutes les données du terminal. BlackBerry UEM peut également désactiver un terminal si celui-ci enfreint le profil de conformité et que l'action d'application spécifiée consiste à désactiver le terminal. Les utilisateurs peuvent désactiver leurs terminaux à l'aide des méthodes suivantes :

- Pour les terminauxiOS et Android, les utilisateurs peuvent sélectionner Désactiver mon terminal sur l'écran « À propos de » de l'application BlackBerry UEM Client.
- Pour les terminaux Windows 10, les utilisateurs peuvent sélectionner Paramètres > Comptes > Accès professionnel > Supprimer.

Pour les terminaux qui utilisent Knox MDM, lorsque le terminal est désactivé, les applications internes sont désinstallées, et l'option Désinstaller devient disponible pour toutes les applications publiques installées depuis la liste d'applications selon les besoins.

Pour les terminaux Android Enterprise dotés d'un profil professionnel uniquement, si vous désactivez un terminal, vous pouvez supprimer toutes les données de la carte SD, ainsi que la protection contre la réinitialisation définie en usine.

Pour les terminaux Android Enterprise dotés d'activations Travail et Personnel - Confidentialité des données de l'utilisateur et Travail et Personnel - Contrôle total, si vous utilisez la commande Supprimer uniquement les données professionnelles, vous pouvez saisir une raison qui apparaît dans la notification sur le terminal de l'utilisateur pour expliquer pourquoi le profil professionnel a été supprimé. Si le terminal est désactivé pour violation des règles de conformité, la notification spécifie la raison pour laquelle le terminal n'est pas conforme.

Pour les terminaux Android Enterprise dotés d'activations Travail et Personnel - Contrôle total, seule la commande Supprimer toutes les données du terminal est prise en charge par les terminaux exécutant Android version 10 et antérieure. La commande Supprimer uniquement les données professionnelles est prise en charge par les terminaux exécutant Android version 11 et ultérieure. La commande Supprimer uniquement les données professionnelles supprime toutes les données et applications professionnelles, mais permet à l'utilisateur de conserver les données personnelles et les applications et de continuer à utiliser le terminal non géré.

Pour les terminaux Samsung Knox Workspace qui ont été activés à l'aide des types d'activation Travail et Personnel - Contrôle total ou Espace Travail uniquement, désactiver le terminal supprime toutes les données de celui-ci ou de l'espace Travail uniquement. Vous pouvez spécifier les données qui seront effacées à l'aide de la règle de stratégie informatique Effacement des données à la désactivation.

# Contrôle des mises à jour du logiciel qui sont installées sur les terminaux

Vous pouvez contrôler les versions logicielles des terminaux qui sont installées sur les terminaux Android Enterprise et Samsung Knox. Pour les terminaux Android Enterprise, vous pouvez également définir une période de mise à jour pour les applications qui s'exécutent en premier plan.

Pour les terminaux Android Enterprise avec des activations Espace Travail uniquement et Travail et Personnel - Contrôle total, vous pouvez spécifier si l'utilisateur peut choisir le moment où les mises à jour logicielles disponibles seront installées ou si elles sont automatiquement installées. Vous pouvez spécifier différentes règles en fonction du modèle du terminal et de la version du SE actuellement installée. Pour tous les terminaux Android Enterprise, vous pouvez également définir une période de mise à jour pour les applications qui s'exécutent en premier plan. Par défaut, lorsqu'une application est en premier plan, Google Play ne peut pas la mettre à jour. Vous pouvez également contrôler la façon dont Google Play applique les modifications au terminal, par exemple en spécifiant si l'utilisateur peut autoriser le changement ou si le changement ne se produit que lorsque le terminal est connecté à un réseau Wi-Fi.

Pour les terminaux Android Enterprise avec des activations Espace Travail uniquement et Travail et Personnel - Contrôle total, pour tous les terminaux pour lesquels vous avez spécifié une règle de mise à jour du système d'exploitation autre que la règle par défaut, vous pouvez également suspendre les mises à jour pendant les dates où les mises à jour ne doivent pas avoir lieu. Par exemple, vous pouvez suspendre les mises à jour pendant les périodes de congés. Si vous souhaitez suspendre les mises à jour pour tous les terminaux, vous devez d'abord créer une règle de mise à jour du système d'exploitation pour tous les terminaux. Par exemple, vous pouvez créer une règle de mise à jour du système d'exploitation pour tous les terminaux exécutant Android 7.0 et versions ultérieures afin d'appliquer automatiquement les mises à jour à certaines heures.

Sur les terminaux Samsung Knox, vous pouvez utiliser E-FOTA (Enterprise Firmware Over the Air) pour contrôler le moment où les mises à jour du micrologiciel de Samsung sont installées.

Les terminaux Samsung Knox activés en tant que Espace Travail uniquement (Samsung Knox), Travail et Personnel - Contrôle total (Samsung Knox), Espace Travail uniquement (terminal Android Enterprise entièrement géré) et Travail et Personnel - Contrôle total (terminal Android Enterprise entièrement géré avec profil professionnel) prennent en charge les restrictions logicielles via E-FOTA.

E-FOTA n'est pas pris en charge pour les types d'activation Travail et Personnel - Confidentialité des données de l'utilisateur (Samsung Knox) ou Travail et Personnel - Confidentialité des données de l'utilisateur (Android Enterprise avec profil professionnel).

Le contrôle des versions du micrologiciel garantit que les terminaux des utilisateurs utilisent des versions du micrologiciel prises en charge par leurs applications et conformes aux stratégies de votre entreprise. Vous pouvez utiliser un profil d'exigences SR pour créer des règles de micrologiciel pour les terminaux Samsung Knox qui sont activés sur UEM. Vous pouvez planifier l'installation des mises à jour du micrologiciel et indiquer le moment où des mises à jour forcées doivent être installées. Pour plus d'informations sur la fonction E-FOTA, consultez le site https://seap.samsung.com/sdk/enterprise-fota.

**Remarque :** En fonction du fournisseur de services sans fil utilisé par un terminal, les mises à jour E-FOTA peuvent ne pas être disponibles. Certains fournisseurs de services sans fil (par exemple, AT&T et Verizon) utilisent leurs propres systèmes pour gérer les mises à jour sans fil.

Sur les terminaux utilisant des activations Contrôles MDM, vous ne pouvez pas contrôler quand et comment les utilisateurs mettent à jour le système d'exploitation de leur terminal, mais vous pouvez utiliser des profils de conformité pour limiter la version du système d'exploitation d'un terminal. Pour les terminaux, si vous souhaitez appliquer une action particulière en cas d'installation d'une version restreinte du logiciel sur un terminal, vous devez créer un profil de conformité et l'attribuer aux utilisateurs, groupes d'utilisateurs ou groupes de terminaux. Le profil de conformité spécifie les actions qui seront prises si l'utilisateur ne supprime pas la version restreinte du logiciel du terminal.

Vous ne pouvez pas contrôler les versions logicielles installées sur les terminaux iOS, mais vous pouvez forcer les terminaux iOS sous supervision à installer une mise à jour disponible. Pour plus d'informations, reportez-vous à Mettre à jour le système d'exploitation sur les terminaux iOS supervisés.

# Créer un profil de configuration logicielle minimale requise du terminal pour les terminaux Android Enterprise

Les règles de mise à jour du système d'exploitation ne s'appliquent qu'aux terminaux Espace Travail uniquement et Travail et Personnel - Contrôle total. Les règles de mise à jour de l'application s'appliquent à tous les terminaux Android Enterprise. Pour plus d'informations sur la définition de règles pour les terminaux Samsung Knox qui utilisent E-FOTA, reportez-vous à la section Créer un profil de configuration logicielle minimale requise du terminal pour les terminaux Samsung Knox.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Conformité > Configuration logicielle minimale requise du terminal**.
3. Cliquez sur +.
4. Saisissez le nom et la description du profil.
5. Cliquez sur l'onglet **Android**.
6. Pour Espace Travail uniquement et les terminaux Travail et Personnel - Contrôle total, suivez les étapes suivantes pour définir les règles de mise à jour du système d'exploitation :
   a) Dans le tableau **Règle de mise à jour du système d'exploitation**, cliquez sur +.
   b) Dans la liste déroulante **Modèle du terminal**, sélectionnez un modèle de terminal.
   c) Dans la liste déroulante **Version du système d'exploitation**, sélectionnez la version du système d'exploitation installée.
   d) Dans la liste déroulante **Mettre à jour la règle**, sélectionnez l'une des options suivantes :
      - Sélectionnez **Par défaut** pour permettre à l'utilisateur de choisir le moment où les mises à jour seront installées.
      - Sélectionnez **Mettre automatiquement à jour** pour installer les mises à jour sans demander à l'utilisateur.
      - Sélectionnez **Mettre automatiquement à jour entre** pour installer les mises à jour entre les heures que vous avez définies, sans demander à l'utilisateur. L'utilisateur peut choisir d'installer les mises à jour en dehors de cette fenêtre.
      - Sélectionnez **Reporter jusqu'à 30 jours** pour bloquer l'installation des mises à jour pendant 30 jours. Après 30 jours, l'utilisateur peut choisir le moment d'installer une mise à jour. Selon le fabricant du terminal et le fournisseur de services sans fil, il est possible que les mises à jour de sécurité ne puissent pas être reportées.
   e) Une fois terminé, cliquez sur **Ajouter**.
   f) Répétez l'étape 6 pour chacune des règles que vous souhaitez ajouter.

   Les règles définies pour les terminaux Samsung Knox qui utilisent E-FOTA ont priorité sur ces règles.
7. Pour les terminaux Espace Travail uniquement et Travail et Personnel - Contrôle total, si vous souhaitez spécifier des périodes où les mises à jour du système d'exploitation ne doivent pas se produire, effectuez les opérations suivantes :
   a) Dans le tableau **Suspendre les mises à jour du SE**, cliquez sur +.
   b) Dans la liste déroulante **Mois de début**, sélectionnez le mois du début de la période de suspension.
   c) Dans la liste déroulante **Jour de début**, sélectionnez le jour du début de la période de suspension.
   d) Dans la liste déroulante **Durée**, sélectionnez la durée de la suspension.

La suspension ne peut pas dépasser 90 jours. Si vous spécifiez plusieurs périodes de suspension, il doit y avoir au moins 60 jours entre les périodes.

Ces paramètres ne s'appliquent pas aux terminaux Samsung Knox utilisant E-FOTA.

8. Pour spécifier une période de mise à jour pour les applications qui s'exécutent en premier plan, sélectionnez **Activer la période de mise à jour pour les applications qui s'exécutent au premier plan**, puis définissez les options suivante :
   - **Heure de début (heure locale du terminal)** : indique l'heure à laquelle les applications commencent à se mettre à jour.
   - **Durée** : indique le nombre d'heures pendant lesquelles vous autoriserez la mise à jour des applications.
9. Pour spécifier comment Google Play applique les modifications aux applications exécutées au premier plan, sélectionnez Politique de mise à jour automatique de l'application. Sélectionnez l'une des options suivantes :
   - **L'utilisateur peut autoriser** : l'utilisateur est invité à autoriser les applications à se mettre à jour sur l'appareil. Notez qu'il s'agit du paramètre par défaut si vous ne sélectionnez pas l'option Politique de mise à jour automatique de l'application.
   - **Toujours** : les applications sont toujours mises à jour. Notez que pour une application toujours en cours d'exécution, telle que BlackBerry UEM Client, BlackBerry Work ou BlackBerry Connectivity, si vous ne sélectionnez pas l'option **Activer la période de mise à jour pour les applications qui s'exécutent au premier plan**, l'application n'est mise à jour que lorsque l'utilisateur met à jour manuellement l'application sur le terminal.
   - **Wi-Fi uniquement** : les applications se mettent à jour uniquement lorsque le terminal est connecté à un réseau Wi-Fi. Notez que pour une application toujours en cours d'exécution, telle que BlackBerry UEM Client, BlackBerry Work ou BlackBerry Connectivity, si vous ne sélectionnez pas l'option **Activer la période de mise à jour pour les applications qui s'exécutent au premier plan**, l'application n'est mise à jour que lorsque l'utilisateur met à jour manuellement l'application sur son terminal.
   - **Désactiver** : les applications ne sont jamais mises à jour.

     **Remarque :**

     Ce profil affecte le paramètre Mise à jour automatique des applis dans Google Play. Si vous sélectionnez **Toujours**, **Wi-Fi uniquement** ou **Désactiver**, l'utilisateur ne peut pas sélectionner une autre option sur le terminal. Par exemple, si vous sélectionnez **Désactiver** dans le profil, l'utilisateur ne peut pas activer la mise à jour d'une application sur le terminal. Cependant, les utilisateurs peuvent toujours mettre à jour manuellement les applications dans Google Play.
10. Cliquez sur **Ajouter**.

**À la fin :** Si nécessaire, classez les profils.

# Créer un profil de configuration logicielle minimale requise du terminal pour les terminaux Samsung Knox

**Remarque :** En fonction du fournisseur de services sans fil utilisé par un terminal, les mises à jour E-FOTA peuvent ne pas être disponibles. Certains fournisseurs de services sans fil (par exemple, T&T et Verizon) utilisent leurs propres systèmes pour gérer les mises à jour sans fil.

**Avant de commencer :** Vérifiez qu'une licence E-FOTA a été ajoutée à BlackBerry UEM. Pour utiliser E-FOTA, vous devez sélectionner la règle globale Android Autoriser les mises à jour par liaison radio dans la stratégie informatique associée dans la console de gestion BlackBerry UEM.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Conformité > Configuration logicielle minimale requise du terminal**.

3. Cliquez sur +.
4. Saisissez le nom et la description du profil.
5. Dans le tableau **Règles relatives aux micrologiciels des terminaux Samsung**, cliquez sur +.
6. Sélectionnez **Appliquer la restriction à tous les terminaux Android** pour autoriser l'application des mises à jour Android OS aux terminaux Samsung.
7. Dans le champ **Modèle du terminal**, saisissez le modèle de terminal ou sélectionnez-le dans la liste déroulante.
8. Dans la liste déroulante **Langue**, sélectionnez une langue.
9. Dans le champ **Code de l'opérateur**, saisissez le code CSC du fournisseur de services sans fil pour le terminal.
10. Cliquez sur **Obtenir la version du micrologiciel**.
11. Répétez les étapes 5 à 8 pour chaque règle de micrologiciel que vous souhaitez ajouter.
12. Une fois terminé, cliquez sur **Ajouter**.
13. Dans le tableau **Règles relatives aux micrologiciels des terminaux Samsung**, cliquez sur **Planifier** en regard de la version du micrologiciel que vous avez ajoutée.
14. Dans la boîte de dialogue **Planifier une mise à jour forcée**, procédez comme suit (**Remarque** : si vous sélectionnez l'option Planifier une mise à jour forcée, le terminal KNOX n'est plus limité à la version du micrologiciel et vous pouvez le mettre à jour manuellement si une version ultérieure est disponible.) :
    a) Dans les champs **Planifier une mise à jour forcée entre**, sélectionnez une plage de dates au cours de laquelle la mise à jour doit être installée. La plage de dates doit être comprise entre 3 à 7 jours. La valeur par défaut est de 7 jours.
    b) Dans les listes déroulantes **Planifier une mise à jour forcée pendant les heures de**, précisez le moment où la mise à jour forcée doit être installée et le fuseau horaire de l'utilisateur. La durée doit être comprise entre 1 et 12 heures.
15. Cliquez sur **Enregistrer**.

**À la fin :** Si nécessaire, classez les profils.

### Ajouter une licence E-FOTA

Vous pouvez utiliser E-FOTA (Enterprise Firmware Over the Air) pour contrôler quand les mises à jour du micrologiciel de Samsung sont installées sur les terminaux Samsung Knox. Le contrôle des versions du micrologiciel garantit que les terminaux des utilisateurs utilisent des versions du micrologiciel prises en charge par leurs applications et conformes aux stratégies de votre entreprise.

Avant de créer un profil d'exigences de demande de service pour terminaux afin de contrôler les versions du micrologiciel, vous devez ajouter une licence E-FOTA dans UEM.

1. Sur la barre de menus, cliquez sur **Gestion des licences** > **Résumé des licences**.
2. Dans la section **E-FOTA**, cliquez sur **Ajouter une licence**.
3. Dans la boite de dialogue **Ajouter une licence E-FOTA**, entrez le nom, l'ID client, le secret du client, l'ID de client et la clé de licence.
4. Cliquez sur **Enregistrer**.

## Afficher les utilisateurs exécutant une version annulée du logiciel

Vous pouvez afficher la liste des utilisateurs qui exécutent une version annulée du logiciel. Une version annulée du logiciel correspond à une version du logiciel qui n'est plus acceptée par un fournisseur de services, mais peut toujours être installée sur le terminal de l'utilisateur.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.

2. Cliquez sur **Conformité > Configuration logicielle minimale requise du terminal**.
3. Cliquez sur le nom du profil que vous souhaitez afficher.
4. Cliquez sur l'onglet **x utilisateurs exécutant une SR annulée** pour afficher la liste des utilisateurs qui exécutent une version annulée du logiciel.

# Gestion des mises à jour du système d'exploitation sur les terminaux avec des activations Contrôles MDM

Vous ne pouvez pas contrôler le moment où des versions logicielles sont installées sur des terminaux avec des activations Contrôles MDM ; cependant, vous pouvez utiliser des profils de conformité pour aider à gérer les terminaux que les utilisateurs ont mis à jour vers une version de système d'exploitation que votre organisation n'autorise pas. Par exemple, les terminaux Android 10 et versions ultérieures ne prennent pas en charge les activations Contrôles MDM. Si les utilisateurs de terminaux Android 9.x effectuent une mise à niveau vers Android 10, certaines fonctions de gestion du terminal ne fonctionneront plus, laissant ce dernier dans un état compromis. Vous pouvez utiliser des groupes de terminaux et des profils de conformité pour détecter les terminaux Android avec le type d'activation Contrôles MDM et définir des règles de conformité pour prendre les mesures appropriées, telles que la notification à l'utilisateur, l'annulation de l'approbation du terminal ou l'annulation de la gestion du terminal.

Procédez comme suit pour gérer les mises à jour du système d'exploitation sur les terminaux avec des activations Contrôles MDM.

| Étape | Action |
|---|---|
| 1 | Créez un groupe de terminaux qui inclut des terminaux conformes aux paramètres suivants :<br>• Type d'activation Contrôles MDM<br>• Version du système d'exploitation du terminal que vous souhaitez restreindre<br>Si un utilisateur met à niveau un terminal vers le système d'exploitation spécifié, il intègre automatiquement le groupe de terminaux en question. |
| 2 | Créez un profil de conformité et spécifiez la version du système d'exploitation du terminal en tant que version limitée du système d'exploitation. |
| 3 | Dans le profil de conformité, spécifiez l'action d'application appropriée pour votre organisation. Par exemple, vous pouvez informer l'utilisateur que son type d'activation n'est pas pris en charge par le système d'exploitation du terminal et lui recommander de réactiver celui-ci avec un autre type d'activation, ou vous pouvez désactiver le terminal. |
| 4 | Attribuez le profil de conformité au groupe de terminaux. |
| 5 | Vous pouvez également créer une notification d'évènement pour informer les administrateurs lorsqu'un terminal n'est pas conforme au profil de conformité. |

# Affichage des mises à jour disponibles pour les terminaux iOS

Vous pouvez voir si une mise à jour logicielle est disponible pour les terminaux iOS de vos utilisateurs pour les prévenir qu'ils peuvent mettre à niveau le logiciel vers la dernière version.

1. Sur la barre de menus, cliquez sur **Utilisateurs > Terminaux gérés**.
2. Recherchez un compte d'utilisateur.
3. Dans les résultats de la recherche, cliquez sur le nom du compte d'utilisateur.
4. Sélectionnez l'onglet Terminal.
5. Dans la section Terminal activé, vérifiez si une mise à jour est disponible.

# Mettre à jour le système d'exploitation sur les terminaux iOS supervisés

Vous pouvez forcer les terminaux iOS à installer une mise à jour de système d'exploitation disponible. Pour mettre à jour le système d'exploitation sur plusieurs terminaux, reportez-vous à la section Envoyer une commande groupée.

Vous pouvez également contrôler le calendrier des mises à jour du logiciel iOS à l'aide des règles de stratégie informatique Retarder les mises à jour logicielles et Délai d'application des mises à jour logicielles. Pour plus d'informations, téléchargez la Fiche de référence des stratégies.

1. Sur la barre de menus, cliquez sur **Utilisateurs > Terminaux gérés**.
2. Recherchez un compte d'utilisateur.
3. Dans les résultats de la recherche, cliquez sur le nom du compte d'utilisateur.
4. Cliquez sur l'onglet du terminal.
5. Si une mise à jour du logiciel est disponible dans le volet de gauche, cliquez sur **Mettre à jour maintenant**.
6. Dans la liste déroulante, sélectionnez l'une des options suivantes :
   - **Télécharger et installer** : la mise à jour est automatiquement téléchargée et installée sur le terminal.
   - **Télécharger uniquement** : la mise à jour est automatiquement téléchargée sur le terminal et l'utilisateur est invité à l'installer.
   - **Installer les mises à jour téléchargées** : si la mise à jour est déjà téléchargée sur le terminal, elle est automatiquement installée.
7. Dans la liste **Version du SE**, sélectionnez la version du système d'exploitation vers laquelle vous souhaitez mettre à jour le terminal
8. Cliquez sur **Mettre à jour**.

# Configuration de la communication entre les terminaux et BlackBerry UEM

Le profil Enterprise Management Agent fait en sorte que les terminaux contactent BlackBerry UEM régulièrement pour vérifier si des mises à jour de la configuration ou des applications sont disponibles. Lorsque des mises à jour sont disponibles pour un terminal, BlackBerry UEM invite celui-ci à contacter BlackBerry UEM pour les recevoir. Si, pour une raison quelconque, le terminal ne reçoit pas l'invite, le profil Enterprise Management Agent est utilisé pour veiller à ce que le terminal contacte BlackBerry UEM aux intervalles spécifiés.

Dans des environnements sur site, vous pouvez également utiliser le profil Enterprise Management Agent pour permettre à BlackBerry UEM d'établir une liste des applications personnelles sur les terminaux des utilisateurs. Pour désactiver la liste des applications personnelles, vous devez désélectionner l'option Autoriser la liste d'applications personnelles. Pour plus d'informations, consultez Désactiver la liste d'applications personnelles.

Vous pouvez attribuer un profil Enterprise Management Agent à des utilisateurs, des groupes d'utilisateurs et des groupes de terminaux.

## Créer un profil Enterprise Management Agent

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Stratégie > Enterprise Management Agent**.
3. Cliquez sur +.
4. Saisissez le nom et la description du profil.
5. Définissez les valeurs de chaque type de terminal tel que requis par votre entreprise.
6. Cliquez sur **Ajouter**.

**À la fin :** Si nécessaire, classez les profils.

### iOS : paramètres de profil Enterprise Management Agent

| Paramètre | Description |
|---|---|
| Fréquence d'interrogation de Enterprise Management Agent | Indiquez la fréquence (en secondes) à laquelle le terminal interroge les commandes du serveur de Enterprise Management Agent. Le terminal interroge uniquement lorsque le client UEM Client est ouvert sur le terminal.<br>Valeurs possibles :<br>• 900 à 86 400<br>La valeur par défaut est 3600. |
| Autoriser la collection d'applications personnelles | Ce paramètre spécifie si BlackBerry UEM doit recevoir une liste des applications personnelles installées sur les terminaux de l'utilisateur.<br>Ce paramètre n'est pas pris en charge sur les terminaux ayant des activations Confidentialité de l'utilisateur. |

### Android : paramètres de profil Enterprise Management Agent

| Paramètre | Description |
|---|---|
| Modifications de l'application | Indiquez la fréquence, en secondes, à laquelle le terminal vérifie les changements dans les applications installées.<br>Valeurs possibles :<br>• De 3600 à 86400 secondes<br>La valeur par défaut est 3600. |
| Seuil de niveau de batterie | Indiquez le pourcentage de changement du niveau de la batterie (de 5 à 100) requis que le terminal ne renvoie les informations à BlackBerry UEM.<br>Valeurs possibles :<br>• 5 à 100 %<br>La valeur par défaut est 20. |
| Seuil d'espace libre RAM | Indiquez le changement nécessaire de la quantité de mémoire libre en mégaoctets avant que le terminal ne renvoie des informations à BlackBerry UEM.<br>Par défaut, le terminal n'envoie pas ces informations à BlackBerry UEM. |
| Seuil de stockage interne | Indiquez le changement nécessaire de la quantité d'espace de stockage libre interne en mégaoctets avant que le terminal ne renvoie des informations à BlackBerry UEM.<br>La valeur par défaut est 250. |
| Seuil de la carte mémoire | Indiquez le changement nécessaire de la quantité d'espace libre externe en mégaoctets avant que le terminal ne renvoie des informations à BlackBerry UEM.<br>La valeur par défaut est 500. |
| Fréquence d'interrogation de Enterprise Management Agent | Indiquez la fréquence (en secondes) à laquelle le terminal interroge les commandes du serveur de Enterprise Management Agent.<br>Valeurs possibles :<br>• Minimum : 900<br>La valeur par défaut est 900. |
| Autoriser la collection d'applications personnelles | Ce paramètre spécifie si BlackBerry UEM doit recevoir une liste des applications personnelles installées sur les terminaux de l'utilisateur.<br>Ce paramètre n'est pas pris en charge sur les terminaux ayant des activations Confidentialité de l'utilisateur. |

### Windows : paramètres de profil Enterprise Management Agent

| Paramètre | Description |
|---|---|
| Intervalle d'interrogation des mises à jour de configuration de terminal | Indiquez la fréquence, en minutes, à laquelle le terminal recherche des mises à jour de configuration lorsque la notification Push n'est pas disponible. |
| Intervalle d'interrogation pour la première série de nouvelles tentatives | Indiquez le temps d'attente, en minutes, entre deux tentatives lors de la première série de tentatives, si l'interrogation des mises à jour de la configuration du terminal échoue. |
| Nombre de premières nouvelles tentatives | Indiquez le nombre de tentatives de la première série de tentatives. |
| Intervalle d'interrogation pour la deuxième série de nouvelles tentatives | Indiquez le temps d'attente, en minutes, entre deux tentatives lors de la deuxième série de tentatives, si l'interrogation des mises à jour de la configuration du terminal échoue. |
| Nombre de secondes nouvelles tentatives | Indiquez le nombre de tentatives de la deuxième série de tentatives. |
| Intervalle d'interrogation pour les nouvelles tentatives planifiées restantes | Indiquez le temps d'attente, en minutes, entre les tentatives suivantes après la deuxième série de tentatives, si l'interrogation des mises à jour de la configuration du terminal échoue. |
| Nombre de nouvelles tentatives planifiées restantes | Indiquez le nombre de tentatives suivantes après la deuxième série de tentatives, si l'interrogation des mises à jour de la configuration du terminal échoue. Si ce nombre est défini sur « 0 », le terminal continue d'interroger jusqu'à ce qu'une connexion réussisse ou que le terminal soit désactivé. |
| Interroger lors de la connexion de l'utilisateur | Indiquez si le terminal doit lancer une session de gestion lors de la connexion d'un utilisateur quelconque. |
| Interrogation de tous les utilisateurs lors de la première connexion | Indiquez si le terminal doit lancer une session de gestion lors de la première connexion de tous les utilisateurs. |
| Autoriser la collection d'applications personnelles | Ce paramètre spécifie si BlackBerry UEM doit recevoir une liste des applications personnelles installées sur les terminaux de l'utilisateur. |

# Affichage des informations d'entreprise sur les terminaux

Vous pouvez configurer BlackBerry UEM de manière à afficher des informations sur l'entreprise ou des avis d'entreprise personnalisés sur les terminaux.

Pour les terminaux iOS, macOS, Android et Windows 10, vous pouvez créer des avis d'entreprise personnalisés et les afficher lors de l'activation. Par exemple, un avis peut inclure les conditions qu'un utilisateur doit suivre pour se conformer aux exigences de sécurité de l'entreprise. L'utilisateur doit accepter l'avis pour continuer le processus d'activation. Vous pouvez créer plusieurs avis pour couvrir différents besoins et créer des versions distinctes de chaque avis pour prendre en charge différentes langues.

Vous pouvez créer des profils de terminaux pour afficher des informations relatives à votre entreprise sur les terminaux. Pour les terminaux iOS et Android, les informations sur l'entreprise s'affichent dans le BlackBerry UEM Client sur le terminal. Sous Windows 10, le numéro de téléphone et l'adresse e-mail sont indiqués dans les informations d'assistance technique du terminal. Pour les terminaux Samsung Knox, vous pouvez utiliser le profil du terminal pour afficher l'avis d'entreprise personnalisé lorsque l'utilisateur redémarre le terminal.

Pour les terminaux Samsung Knox et iOS supervisés, vous pouvez également utiliser le profil du terminal pour ajouter un fond d'écran personnalisé afin d'afficher des informations destinées aux utilisateurs. Par exemple, vous pouvez créer une image affichant vos informations de contact, informations de site Web interne ou le logo de votre entreprise. Sur les terminaux Samsung Knox, le fond d'écran s'affiche dans l'espace Travail.

**Remarque :** Les profils de terminaux ne sont pas pris en charge pour les terminaux iOS activés avec un type d'activation de confidentialité utilisateur.

| Emplacement des informations sur l'entreprise | Configuration des informations sur l'entreprise |
|---|---|
| Afficher un avis d'entreprise lors de l'activation des terminaux iOS, macOS, Android et Windows 10 | Créez un avis d'entreprise et attribuez-le à un profil d'activation. |
| Afficher un avis d'entreprise lors du redémarrage des terminaux Samsung Knox | Créez un avis d'entreprise et attribuez-le dans l'onglet Android du profil de terminal. Pour modifier l'avis qui s'affiche au redémarrage du terminal, vous devez mettre à jour le profil du terminal. |
| Affichez les informations d'organisation dans leBlackBerry UEM Client sur les terminaux iOS et Android, ou dans les informations d'assistance sur les terminaux Windows 10 | Saisissez les informations que vous voulez afficher dans l'onglet approprié du profil de terminal. |
| Dans une image en fond d'écran sur les terminaux Samsung Knox ou iOS supervisés | Sélectionnez un fichier image dans l'onglet approprié du profil de terminal. |

# Créer des avis d'entreprise

Vous pouvez créer des avis d'entreprise personnalisés à afficher lors de l'activation de terminaux iOS, macOS, Android et Windows 10.

Les terminaux Samsung Knox peuvent également afficher les avis d'entreprise lorsqu'un utilisateur redémarre le terminal.

1. Sur la barre de menus, cliquez sur **Paramètres**.
2. Dans le volet de gauche, développez **Paramètres généraux.**
3. Cliquez sur **Avis d'entreprise**.
4. Cliquez sur + située à droite de l'écran.
5. Dans le champ **Nom**, saisissez le nom de l'avis d'entreprise.
6. Vous pouvez également réutiliser le texte d'un avis d'entreprise existant en le sélectionnant dans la liste déroulante **Texte copié à partir d'un avis d'entreprise**.
7. Dans la liste déroulante **Langue du terminal**, sélectionnez la langue à utiliser par défaut pour l'avis d'entreprise.
8. Dans le champ **Avis d'entreprise**, saisissez le texte de l'avis d'entreprise.
9. Vous pouvez également cliquer plusieurs fois sur **Ajouter une langue supplémentaire** pour publier l'avis d'entreprise dans plusieurs langues.
10. Si vous publiez l'avis d'entreprise dans plusieurs langues, sélectionnez l'option **Langue par défaut** sous l'un des messages pour définir sa langue comme langue par défaut.
11. Cliquez sur **Enregistrer**.

**À la fin :**

- Pour afficher l'avis d'organisation pendant l'activation, attribuez l'avis d'organisation à un profil d'activation.
- Pour afficher l'avis d'entreprise lors du redémarrage d'un terminal Samsung Knox, associez l'avis d'entreprise à un profil de terminal.

# Créer un profil de terminal

**Avant de commencer :** Pour les terminaux Samsung Knox, créez des avis d'entreprise.

**Remarque :** Les profils de terminaux ne sont pas pris en charge pour les terminaux iOS activés avec un type d'activation de confidentialité utilisateur.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Personnaliser > Terminal**.
3. Cliquez sur +.
4. Saisissez le nom et la description du profil. Chaque profil de terminal doit avoir un nom unique.
5. Effectuez l'une des tâches suivantes :

| Tâche | Étapes |
|---|---|
| Attribuer un avis d'entreprise à afficher sur les terminaux Samsung Knox au redémarrage du terminal | a. Cliquez sur **BlackBerry** ou **Android**.<br>b. Dans la liste déroulante **Attribuer un avis d'entreprise**, sélectionnez l'avis d'entreprise que vous souhaitez afficher sur les terminaux. |

| Tâche | Étapes |
| --- | --- |
| Pour les terminaux iOS et Android, définissez les informations d'entreprise à afficher dans l'application BlackBerry UEM Client.<br>Pour Windows 10, définissez le numéro de téléphone et l'adresse e-mail à afficher dans les informations d'assistance sur les terminaux. | **a.** Cliquez sur **iOS**, **Android** ou **Windows**.<br>**b.** Saisissez le nom, l'adresse, le numéro de téléphone et l'adresse électronique de votre organisation. |

6. Si nécessaire, effectuez les opérations suivantes :

| Tâche | Étapes |
| --- | --- |
| Ajoutez une image de fond d'écran à l'espace Travail sur les terminaux Samsung Knox | **a.** Cliquez sur **BlackBerry** ou **Android**.<br>**b.** Dans la section **Fond d'écran de l'espace Travail**, cliquez sur **Parcourir.**<br>**c.** Sélectionnez l'image que vous souhaitez utiliser comme fond d'écran.<br>**d.** Cliquez sur **Ouvrir**. |
| Ajouter un fond d'écran aux terminaux iOS supervisés | **a.** Cliquez sur **iOS**.<br>**b.** Dans la zone **Fond d'écran du terminal**, sélectionnez si le fond d'écran s'affiche sur l'**écran d'accueil**, l'**écran de verrouillage** ou **les deux**.<br>**c.** Cliquez sur **Parcourir** et sélectionnez l'image que vous souhaitez utiliser comme fond d'écran.<br>**d.** Cliquez sur **Ouvrir**.<br>**e.** Dans le champ **Définir le fond d'écran pour**, sélectionnez l'endroit où vous voulez que le fond d'écran s'affiche. |

7. Cliquez sur **Ajouter**.

**À la fin :**

- Si nécessaire, classez les profils.

# Utilisation des services de localisation sur les terminaux

Un profil de service de localisation vous permet de demander l'emplacement de terminaux et d'afficher leur emplacement approximatif sur une carte. Vous pouvez également permettre aux utilisateurs de localiser leurs terminaux à l'aide de BlackBerry UEM Self-Service. Si vous activez l'historique de localisation des terminaux iOS et Android, les terminaux doivent donner périodiquement des informations sur leur emplacement et les administrateurs peuvent afficher l'historique de localisation.

Les profils de service de localisation utilisent les services de localisation sur les terminaux iOS, Android et Windows 10 Mobile. Selon le terminal et les services disponibles, les services de localisation peuvent utiliser les informations des réseaux GPS, cellulaires et Wi-Fi pour déterminer l'emplacement du terminal.

## Configurer les paramètres du service de localisation

Vous pouvez configurer les paramètres des profils de service de localisation, tels que l'unité de vitesse qui s'affiche pour un terminal lorsque vous affichez son emplacement sur une carte. Si vous activez l'historique de localisation pour les terminaux iOS et Android, BlackBerry UEM conserve l'historique pendant 1 mois par défaut.

1. Dans la barre de menus, cliquez sur **Paramètres > Paramètres généraux > Service de localisation**.
2. Si vous disposez d'un environnement sur site, dans le champ **Durée de stockage de l'historique de localisation**, indiquez le nombre de jours, de semaines ou de mois pendant lequel BlackBerry UEM stocke l'historique de localisation des terminaux.
3. Dans la liste déroulante **Unité de vitesse affichée**, cliquez sur **km/h** ou **mph**.
4. Cliquez sur **Enregistrer**.

## Créer un profil de service de localisation

Vous pouvez attribuer un profil de service de localisation aux comptes d'utilisateur, groupes d'utilisateurs ou groupes de terminaux. Les utilisateurs doivent accepter le profil pour que la console de gestion ou BlackBerry UEM Self-Service puisse afficher l'emplacement de terminaux iOS et Android sur une carte. Les terminaux Windows 10 Mobile acceptent automatiquement le profil.

**Avant de commencer :** Configurer les paramètres du service de localisation

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Protection > Service de localisation**.
3. Cliquez sur +.
4. Saisissez le nom et la description du profil de service de localisation.
5. Vous pouvez également décocher la case correspondant aux types de terminaux pour lesquels vous ne souhaitez pas configurer le profil.
6. Effectuez l'une des tâches suivantes :

| Tâche | Étapes |
| --- | --- |
| Activer l'historique de localisation des terminaux iOS | **a.** Dans l'onglet **iOS**, vérifiez que la case **Consigner l'historique de localisation du terminal** est cochée.<br>**Remarque :** BlackBerry UEM enregistre l'emplacement du terminal toutes les heures et signale dans la mesure du possible les changements significatifs d'emplacement du terminal (un déplacement de 500 mètres ou plus, par exemple). |
| Activer l'historique de localisation des terminaux Android | **a.** Dans l'onglet **Android**, vérifiez que la case **Consigner l'historique de localisation du terminal** est cochée.<br>**b.** Dans le champ **Distance de vérification de la localisation d'un terminal**, indiquez la distance minimale du déplacement d'un terminal avant que son emplacement soit mis à jour.<br>**c.** Dans le champ **Fréquence de mise à jour de la localisation**, indiquez la fréquence à laquelle l'emplacement du terminal est mis à jour.<br>**Remarque :** Les conditions de distance et de fréquence doivent être remplies avant que l'emplacement du terminal soit mis à jour. |

7. Cliquez sur **Ajouter**.

**À la fin :** Si nécessaire, classez les profils.

# Localiser un terminal

Vous pouvez localiser des terminaux iOS, Android et Windows 10 Mobile (par exemple, en cas de perte ou de vol d'un terminal). Les utilisateurs doivent accepter le profil de service de localisation pour que la console de gestion puisse afficher l'emplacement des terminaux iOS et Android sur une carte. Les terminaux Windows 10 Mobile acceptent automatiquement le profil. L'historique de localisation est disponible pour les terminaux iOS et Android si vous l'avez activé dans le profil.

**Avant de commencer :** Créez et attribuez un profil de service de localisation.

1. Sur la barre de menus, cliquez sur **Utilisateurs > Terminaux gérés**.
2. Cochez la case de chaque terminal que vous souhaitez localiser.
3. Cliquez sur .
4. Trouvez les terminaux sur la carte à l'aide des icônes suivantes. Si un terminal iOS ou Android ne répond pas avec les dernières informations d'emplacement et que l'historique de localisation est activé dans le profil, la carte affiche le dernier emplacement connu du terminal.

   - Emplacement actuel : 
   - Dernier emplacement connu : 

   Vous pouvez cliquer ou passer la souris sur une icône pour afficher les informations d'emplacement, telles que la latitude et la longitude et l'heure à laquelle l'emplacement a été enregistré (il y a 1 minute ou il y a 2 heures, par exemple).
5. Pour afficher l'historique de localisation d'un terminal iOS ou Android, procédez comme suit :
   a) Cliquez sur **Afficher l'historique de localisation**.
   b) Sélectionnez une plage de date et d'heure.

c) Cliquez sur **Envoyer**.

# Utiliser le mode Perdu sur les terminaux iOS supervisés

Vous pouvez activer et gérer le mode Perdu sur les terminaux iOS supervisés. En cas de perte d'un terminal, l'activation du mode Perdu vous permet de :

- verrouiller le terminal et définir le message à afficher (par exemple, vous pouvez afficher le numéro à appeler par la personne qui trouvera le terminal) ;
- afficher l'emplacement actuel du terminal sans avoir recours à un profil de service de localisation ;
- assurer le suivi de tous les terminaux en mode Perdu à partir de la console de gestion.

## Activer le mode Perdu

Le mode Perdu est pris en charge sur les terminaux surveillés iOS.

1. Sur la barre de menus, cliquez sur **Utilisateurs > Terminaux gérés**.
2. Cliquez sur le terminal dont vous souhaitez activer le mode Perdu.
3. Dans l'onglet Terminal, cliquez sur **Activer le mode Perdu**.
4. Dans les champs **Numéro de téléphone de contact** et **Message**, entrez les informations qui conviennent.
5. Vous pouvez également sélectionner **Remplacer le texte « glisser pour déverrouiller »** et saisir le texte à afficher.
6. Cliquez sur **Activer**.

## Localiser un terminal en mode Perdu

**Avant de commencer :** Activer le mode Perdu

1. Sur la barre de menus, cliquez sur **Utilisateurs > Terminaux gérés**.
2. Cliquez sur un terminal sur lequel le mode Perdu est activé.
3. Dans l'onglet Terminal, cliquez sur **Obtenir l'emplacement du terminal**.

## Désactiver le mode Perdu

**Avant de commencer :** Activer le mode Perdu

1. Sur la barre de menus, cliquez sur **Utilisateurs > Terminaux gérés**.
2. Cliquez sur un terminal sur lequel le mode Perdu est activé.
3. Dans l'onglet Terminal, cliquez sur **Désactiver le mode Perdu**.

# Utilisation du verrouillage d'activation sur les terminaux iOS

La fonctionnalité de verrouillage d'activation sur les terminaux iOS permet aux utilisateurs de protéger leurs terminaux lorsqu'ils sont perdus ou volés. Lorsque la fonctionnalité est activée, l'utilisateur doit confirmer son ID et son mot de passe Apple pour désactiver la fonction Localiser mon iPhone, effacer le terminal ou réactiver et utiliser le terminal.

Pour gérer la fonctionnalité de verrouillage d'activation dans BlackBerry UEM :

- L'appareil doit être supervisé.
- Le terminal doit disposer d'un compte iCloud configuré.
- La fonction Localiser mon iPhone ou Trouver mon iPad doit être activée sur le terminal.

Lorsqu'un terminal est activé sur BlackBerry UEM, le verrouillage d'activation est désactivé par défaut. Vous pouvez l'activer pour chaque terminal individuellement, ou vous pouvez l'appliquer à l'aide de la stratégie informatique. Lorsque vous activez le verrouillage d'activation, BlackBerry UEM stocke un code de contournement que vous pouvez utiliser pour désactiver le verrouillage, afin que le terminal puisse être effacé et réactivé sans l'identifiant et le mot de passe Apple de l'utilisateur.

## Activation du verrouillage d'activation

Procédez comme suit pour activer le verrouillage d'activation pour chaque terminal individuellement. Si le verrouillage d'activation est appliqué à l'aide d'une règle de stratégie informatique, il est déjà activé.

**Remarque :** Lors de l'activation de la fonctionnalité de verrouillage d'activation, un léger retard peut survenir entre BlackBerry UEM et Apple.

**Avant de commencer :**

- L'appareil doit être supervisé.
- Le terminal doit disposer d'un compte iCloud configuré.
- La fonction Localiser mon iPhone ou Trouver mon iPad doit être activée sur le terminal.

1. Sur la barre de menus, cliquez sur **Utilisateurs**.
2. Recherchez un compte d'utilisateur.
3. Dans les résultats de la recherche, cliquez sur le nom du compte d'utilisateur.
4. Cliquez sur l'onglet du terminal.
5. Dans la fenêtre **Gestion du terminal**, cliquez sur **Activer le verrouillage d'activation**.

**À la fin :** Pour afficher la liste des codes de contournement pour les terminaux, consultez Affichage du code de contournement du verrouillage d'activation

## Désactiver le verrouillage d'activation

Procédez comme suit pour désactiver le verrouillage d'activation pour chaque terminal individuellement. Si le verrouillage d'activation est appliqué à l'aide d'une règle de stratégie informatique, il ne peut pas être désactivé.

**Remarque :** Lors de l'activation de la fonctionnalité de verrouillage d'activation, un léger délai peut s'écouler entre BlackBerry UEM et Apple.

1. Sur la barre de menus, cliquez sur **Utilisateurs**.

2. Recherchez un compte d'utilisateur.
3. Dans les résultats de la recherche, cliquez sur le nom du compte d'utilisateur.
4. Cliquez sur l'onglet du terminal.
5. Dans la fenêtre **Gestion du terminal**, sélectionnez **Désactiver le verrouillage d'activation**.

# Affichage du code de contournement du verrouillage d'activation

Vous pouvez afficher le code de contournement du verrouillage d'activation et la date à laquelle ce code de contournement a été généré.

1. Sur la barre de menus, cliquez sur **Utilisateurs > Verrouillage d'activation Apple**.
2. Recherchez un terminal.
3. Dans les résultats de la recherche, cliquez sur le terminal.
4. Si nécessaire, faites défiler vers la droite jusqu'à l'écran principal pour afficher le code de contournement.

# Gestion des fonctionnalités iOS à l'aide des profils de charge utile personnalisée

Vous pouvez utiliser des profils de charge utile personnalisée pour contrôler les fonctions sur les terminaux iOS qui ne sont pas contrôlés par les règles ou profils BlackBerry UEM existants.

**Remarque :** Si une fonction est commandée par une stratégie ou un profil BlackBerry UEM existant, un profil de charge utile personnalisée peut ne pas fonctionner comme prévu. Vous devez utiliser les stratégies ou profils existants chaque fois que cela est possible.

Vous pouvez créer des profils de configuration Apple à l'aide d'Apple Configurator et les ajouter aux profils de charge utile personnalisée BlackBerry UEM. Vous pouvez affecter les profils de charge utile personnalisée aux utilisateurs, aux groupes d'utilisateurs et aux groupes de terminaux.

- Contrôlez une fonctionnalité iOS existante qui n'est pas comprise dans les politiques et les profils BlackBerry UEM. Par exemple, avec BES10, l'assistant du PDG a pu accéder à la fois à son propre compte de messagerie et au compte du PDG sur un iPhone. Dans BlackBerry UEM, vous pouvez attribuer un seul profil de messagerie à un terminal, de sorte que l'assistant peut uniquement accéder à son propre compte de messagerie. Pour résoudre ce problème, vous pouvez attribuer un profil de messagerie pour permettre à l'iPhone de l'assistant d'accéder au compte de messagerie de l'assistant et un profil personnalisé pour permettre à l'iPhone de l'assistant d'accéder au compte de messagerie du PDG.
- Contrôlez une nouvelle fonctionnalité iOS, lancée après la dernière version du logiciel BlackBerry UEM. Par exemple, vous voulez contrôler une nouvelle fonctionnalité qui est disponible pour les terminaux lors d'une mise à niveau récente de iOS, mais BlackBerry UEM ne dispose pas de règles de stratégie informatique pour cette nouvelle fonctionnalité avant la prochaine version du logiciel BlackBerry UEM. Pour résoudre ce problème, vous pouvez créer un profil de charge utile personnalisée qui contrôle cette fonction jusqu'à la prochaine version du logiciel BlackBerry UEM.

## Création d'un profil de charge utile personnalisée

**Avant de commencer :** Téléchargez et installez la dernière version d'Apple Configurator d'Apple.

1. Dans Apple Configurator, créez un profil de configuration Apple.
2. Dans la console de gestion BlackBerry UEM, cliquez sur **Règles et profils**.
3. Cliquez sur **Personnaliser > Charge utile personnalisée**.
4. Cliquez sur +.
5. Saisissez le nom et la description du profil.
6. Dans Apple Configurator, copiez le code XML pour le profil de configuration Apple. Lorsque vous copiez le texte, copiez uniquement les éléments en caractères gras, comme illustré dans l'exemple de code suivant.

```
<?xml version="1.0" encoding="UTF-8"?>
    <!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
    "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
    <plist version="1.0">
    <dict>
         <key>PayloadContent</key>
         <array>
               <dict>
                    <key>CalDAVAccountDescription</key>
                    <string>CalDAV Account Description</string>
                    <key>CalDAVHostName</key>
                    <string>caldav.server.example</string>
```

```
                    <key>CalDAVPort</key>
                    <integer>8443</integer>
                    <key>CalDAVPrincipalURL</key>
                    <string>Principal URL for the CalDAV account</string>
                    <key>CalDAVUseSSL</key>
                    </true>
                    <key>CalDAVUsername</key>
                    <string>Username</string>
                    <key>PayloadDescription</key>
                    <string>Configures CalDAV account.</string>
                    <key>PayloadDisplayName</key>
                    <string>CalDAV (CalDAV Account Description)</string>
                    <key>PayloadIdentifier</key>
                    <string>.caldav1</string>
                    <key>PayloadOrganization</key>
                    <string></string>
                    <key>PayloadType</key>
                    <string>com.apple.caldav.account</string>
                    <key>PayloadUUID</key>
                    <string>9ADCF5D6-397C-4E14-848D-FA04643610A3</string>
                    <key>PayloadVersion</key>
                    <integer>1</integer>
                </dict>
        </array>
        <key>PayloadDescription</key>
        <string>Profile description.</string>
        <key>PayloadDisplayName</key>
        <string>Profile Name</string>
        <key>PayloadOrganization</key>
        <string></string>
        <key>PayloadRemovalDisallowed</key>
        <false/>
        <key>PayloadType</key>
        <string>Configuration</string>
        <key>PayloadUUID</key>
        <string>7A5F8391-5A98-46EA-A3CF-C0D6EDC74632</string>
        <key>PayloadVersion</key>
        <integer>1</integer>
    </dict>
    </plist>
```

7. Dans le champ **Charge utile personnalisée**, collez le code XML d'Apple Configurator.
8. Cliquez sur **Ajouter**.

# Gestion de la protection contre la réinitialisation définie en usine pour les terminaux Android Enterprise

Vous pouvez utiliser le profil de protection contre la réinitialisation définie en usine pour contrôler la fonction de protection contre la réinitialisation définie en usine pour les terminaux Android Enterprise de votre organisation qui ont été activés à l'aide des types d'activation Espace Travail uniquement et Travail et Personnel - Contrôle total.

La protection contre la réinitialisation définie en usine nécessite que l'utilisateur d'un terminal Android saisisse ses informations d'identification de compte Google pour déverrouiller un terminal qui a été réinitialisé aux paramètres d'usine. Elle est activée par défaut lorsqu'un utilisateur ajoute un compte Google au terminal. Ce profil vous permet de désactiver la protection contre la réinitialisation définie en usine ou de spécifier un compte d'utilisateur qui peut être utilisé pour déverrouiller un terminal une fois qu'il a été réinitialisé aux paramètres d'usine.

Ce profil offre trois options :

- Vous pouvez désactiver la protection contre la réinitialisation définie en usine. Si vous désactivez la protection contre la réinitialisation définie en usine, toute personne peut réinitialiser les paramètres d'usine d'un terminal perdu ou volé et commencer à l'utiliser. Cette option est utile si un utilisateur connu a oublié ses informations d'identification de compte Google ou si vous devez réinitialiser un terminal appartenant à votre organisation qui vous a été renvoyé.
- Les utilisateurs peuvent utiliser les informations d'identification de compte Google déjà associées au terminal après une réinitialisation définie en usine. Il s'agit du comportement par défaut. Si un terminal est réinitialisé aux paramètres d'usine, l'utilisateur doit se connecter au terminal à l'aide des informations d'identification du compte Google qui se trouvent déjà sur le terminal. Dès lors, une personne ayant perdu ou volé un terminal ne peut pas elle-même le réinitialiser et l'utiliser.
- Vous pouvez spécifier les informations d'identification de compte Google qu'un utilisateur peut utiliser pour se connecter au terminal après sa réinitialisation aux paramètres d'usine. Cette option permet à votre entreprise de contrôler qui peut se connecter à un terminal après sa réinitialisation aux paramètres d'usine. BlackBerry recommande d'utiliser cette option uniquement si vous comprenez parfaitement l'expérience utilisateur du terminal.

## Créer un profil de protection contre la réinitialisation définie en usine

1. Sur la barre de menus, cliquez sur **Stratégies et profils > Terminaux gérés > Protection > Protection contre la réinitialisation définie en usine**.
2. Saisissez le nom et la description du profil.
3. Choisissez un **Paramètre de protection contre la réinitialisation définie en usine**. Sélectionnez l'une des options suivantes :
    - **Supprimer la protection contre la réinitialisation définie en usine** : si vous désactivez la protection contre la réinitialisation définie en usine, les utilisateurs ne sont pas invités à saisir un ID utilisateur Google une fois que le terminal est réinitialisé sur les paramètres d'usine.
    - **Activer et utiliser les informations d'identification du précédent compte Google lorsque le terminal est réinitialisé sur les paramètres d'usine** : option par défaut. Si l'utilisateur réinitialise le terminal sur les paramètres d'usine à l'aide d'une méthode non fiable et qu'un compte Google existait sur le terminal avant sa réinitialisation, le compte doit être vérifié après la réinitialisation du terminal sur les paramètres d'usine. Notez que si votre entreprise utilise une structure de compte géré Google , il n'y aura pas de compte Google sur le terminal et la protection contre la réinitialisation définie en usine ne sera pas disponible sur le terminal.

- **Activer et spécifier les informations d'identification de compte Google lorsque le terminal est réinitialisé sur les paramètres d'usine** : sélectionnez cette option pour spécifier le compte Google qui doit être utilisé pour se connecter au terminal après une réinitialisation non sécurisée aux paramètres d'usine. Si vous sélectionnez cette option, les informations d'identification du compte Google personnel de l'utilisateur ne peuvent pas être utilisées après une réinitialisation aux paramètres d'usine.

4. Si vous avez sélectionné **Activer et spécifier les informations d'identification de compte Google lorsque le terminal est réinitialisé sur les paramètres d'usine**, cliquez sur **+** > **Ajouter à l'aide de l'authentification Google**, puis connectez-vous au compte Google que vous souhaitez utiliser pour vous connecter aux terminaux qui ont été réinitialisés.

   Vous pouvez ajouter jusqu'à 20 comptes. Vous pouvez également spécifier le compte manuellement. Pour plus d'informations, reportez-vous à Obtenir manuellement un ID utilisateur pour un compte Google.
5. Si vous avez sélectionné l'option **Activer et spécifier les informations d'identification de compte Google lorsque le terminal est réinitialisé sur les paramètres d'usine** et que votre entreprise possède un domaine G Suite ou Google Cloud, sélectionnez **Ajouter un compte Google créé par BlackBerry UEM** si vous souhaitez inclure le compte Google professionnel de l'utilisateur dans la liste des comptes pouvant déverrouiller le terminal après une réinitialisation aux paramètres d'usine.
6. Cliquez sur **Enregistrer**.

# Obtenir manuellement un ID utilisateur pour un compte Google

Vous pouvez utiliser un compte Google existant ou en créer un spécialement dans le cadre de la protection contre la réinitialisation définie en usine. Si vous choisissez d'ajouter un compte manuellement plutôt que d'utiliser l'authentification Google, vous devez obtenir l'ID utilisateur associé au compte.

1. Rendez-vous sur le site People API réservé aux développeurs Google (https://developers.google.com/people/api/rest/v1/people/get).
2. Dans le champ **resourceName**, saisissez : people/me
3. Dans le champ **personalFields**, saisissez : metadata
4. Cliquez sur **Execute**.
5. Sur l'écran **Choose an account**, sélectionnez un compte à utiliser pour configurer le profil de protection contre la réinitialisation définie en usine.
6. Sur l'écran **Google APIs Explorer wants to access your Google Account**, cliquez sur **Allow**.
7. À droite de la page People ID, l'ID utilisateur à 21 chiffres s'affiche dans le champ ID. Notez que l'identifiant s'affiche sous l'en-tête vert avec le nombre 200.

# Réponses de la protection contre la réinitialisation définie en usine aux réinitialisations des terminaux

Il existe plusieurs façons de réinitialiser un terminal aux paramètres d'usine par défaut. Selon la manière dont le terminal est réinitialisé, la protection contre la réinitialisation définie en usine réagit différemment. Pour plus d'informations sur les réinitialisations fiables et non approuvées, rendez-vous sur support.blackberry.com/community pour lire l'article KB56972.

- La désactivation du BlackBerry UEM Client n'est pas considérée comme une réinitialisation fiable car l'utilisateur du terminal n'est pas vérifié avant que le terminal ne soit désactivé. Par conséquent, la protection contre la réinitialisation définie en usine est déclenchée lorsque le terminal se réinitialise et que la désactivation est terminée.

- L'envoi de la commande « Supprimer toutes les données du terminal » depuis la console de gestion peut être une réinitialisation fiable ou non approuvée. Si vous sélectionnez l'option « Supprimer la protection contre la réinitialisation définie en usine » lors de l'envoi de la commande, la protection en question n'est pas déclenchée lorsque le terminal est réinitialisé.
- La réinitialisation du terminal à partir des paramètres du terminal nécessite que l'utilisateur s'authentifie avant la réinitialisation. Ceci est considéré comme une réinitialisation fiable et la protection contre la réinitialisation définie en usine n'est pas déclenchée.
- Les outils d'amorçage/restauration ou de débogage de terminal (ADB) peuvent être utilisés pour réinitialiser le terminal aux paramètres d'usine et sont considérés comme non intrusifs, car l'identité de l'utilisateur n'est pas validée avant que la réinitialisation n'ait lieu. C'est pourquoi la protection contre la réinitialisation définie en usine est déclenchée lorsque le terminal se réinitialise.

# Considérations relatives à l'utilisation d'un compte Google Play géré spécifique lors de la configuration d'un profil de protection contre la réinitialisation définie en usine

Si votre organisation utilise un compte Google Play géré, vous pouvez utiliser l'option Activer et spécifier les informations d'identification de compte Google lorsque le terminal est réinitialisé sur les paramètres d'usine dans le profil de protection contre la réinitialisation définie en usine, car il n'existe pas de compte Google sur les terminaux de votre organisation que vous utilisez pour réinitialiser le terminal ; et la protection contre la réinitialisation définie en usine n'est donc pas disponible sur ce terminal.

Si vous décidez d'utiliser l'option Activer et spécifier les informations d'identification de compte Google lorsque le terminal est réinitialisé sur les paramètres d'usine, vous devez prendre en compte plusieurs facteurs :

- Assurez-vous que l'ID utilisateur à 21 chiffres que vous saisissez dans le profil est correct. Si ce numéro ne correspond pas au compte Google de votre organisation que vous souhaitez utiliser, il n'existe aucun moyen d'effacer la protection contre la réinitialisation définie en usine sur le terminal après son déclenchement. Pour plus d'informations, reportez-vous à Obtenir manuellement un ID utilisateur pour un compte Google.
- Dans la stratégie informatique pour les utilisateurs de votre organisation auxquels vous attribuez le profil de protection contre la réinitialisation définie en usine, BlackBerry vous recommande de désélectionner l'option Autoriser la réinitialisation définie en usine. Le fait de désélectionner l'option désactive l'option de réinitialisation définie en usine dans les paramètres du terminal et désactive le bouton de désactivation dans BlackBerry UEM Client. Cela garantit que les utilisateurs n'utilisent pas l'option de désactivation non fiable d'UEM Client qui déclenche toujours la protection contre la réinitialisation définie en usine sur le terminal. Lorsque cette option est activée, les utilisateurs doivent contacter l'administrateur BlackBerry UEM de leur organisation pour faire réinitialiser leur terminal.
- Fournissez aux utilisateurs de votre organisation des informations sur l'expérience de la protection contre la réinitialisation définie en usine sur le terminal et sur la procédure qu'ils doivent suivre pour désactiver cette protection lorsqu'elle est déclenchée sur le terminal. Pour plus d'informations, reportez-vous à la section Désactiver la protection contre la réinitialisation définie en usine sur un terminal. L'administrateur BlackBerry UEM doit choisir s'il veut fournir les détails du compte aux utilisateurs pour désactiver la protection contre la réinitialisation définie en usine ou si les utilisateurs devront contacter un membre du personnel de l'assistance locale pour déverrouiller le terminal.

# Désactiver la protection contre la réinitialisation définie en usine d'un terminal

Lorsque la protection contre la réinitialisation définie en usine est déclenchée sur le terminal, l'activation Entreprise sur BlackBerry UEM ne fonctionne plus. Vous devez d'abord désactiver la protection contre la réinitialisation définie en usine à l'aide de l'expérience Android  prête à l'emploi.

1. Si vous utilisez une forme quelconque de système d'activation automatisé (comme l'inscription sans contact ou Samsung Knox Mobile Enrollment), vous devez le désactiver pour que le terminal puisse passer à l'étape d'expérience prête à l'emploi.
2. Une fois que le terminal est connecté, sur le premier écran du compte Android, l'utilisateur est invité à saisir les informations d'identification du compte Google associées au terminal. Si vous avez configuré un compte Google spécifique dans le profil de protection contre la réinitialisation définie en usine, l'utilisateur doit saisir l'adresse e-mail et le mot de passe associés au compte.
3. Une fois que l'utilisateur a saisi l'adresse e-mail et le mot de passe du compte Google, il lui est demandé s'il souhaite ajouter cet utilisateur au terminal. L'utilisateur doit sélectionner l'option pour utiliser un nouvel utilisateur pour le terminal.
    - Sur les terminaux non-Samsung qui n'utilisent pas d'inscription sans intervention : les utilisateurs peuvent saisir 'afw#blackberry' ou les détails du compte Google de l'entreprise pour installer BlackBerry UEM Client et réactiver le terminal contre BlackBerry UEM.
    - Sur les terminaux Samsung qui n'utilisent pas l'inscription sans intervention ou Samsung Knox Mobile Enrollment : terminez l'expérience prête à l'emploi et utilisez les paramètres du terminal pour réinitialiser celui-ci. Lorsque le terminal redémarre, il peut être réactivé avec Entreprise.
    - Terminaux utilisant l'inscription sans intervention ou Samsung Knox Mobile Enrollment : si vous utilisez une forme quelconque de système d'activation automatisé (comme l'inscription sans intervention ou Samsung Knox Mobile Enrollment), vous pouvez le réactiver pour le terminal, compléter l'expérience prête-à-l'emploi et utiliser les paramètres du terminal pour réinitialiser celui-ci. Le terminal doit maintenant redémarrer et utiliser le système d'activation automatique que vous avez configuré.

# Configuration de la fonction Protection des informations Windows pour les terminaux Windows 10

Vous pouvez configurer la fonction Protection des informations Windows (WIP) pour les terminaux Windows 10 lorsque vous souhaitez effectuer les opérations suivantes :

- Séparer les données personnelles et professionnelles sur les terminaux et être en mesure d'effacer uniquement les données professionnelles
- Empêcher les utilisateurs de partager les données professionnelles en dehors des applications professionnelles protégées ou avec des personnes extérieures à votre organisation
- Protéger les données même si elles sont déplacées ou partagées sur d'autres terminaux, tels qu'une clé USB
- Surveiller le comportement de l'utilisateur et prendre les mesures appropriées pour éviter toute fuite de données

Lorsque vous configurez la fonction WIP pour les terminaux, vous spécifiez les applications que vous souhaitez protéger avec WIP. Les applications protégées sont en mesure de créer des fichiers professionnels et d'y accéder, tandis qu'il est possible de bloquer l'accès des applications non protégées aux fichiers professionnels. Vous pouvez choisir le niveau de protection pour les applications protégées en fonction de la manière dont vous souhaitez que les utilisateurs se comportent lorsqu'ils partagent des données professionnelles. Lorsque la fonction WIP est activée, toutes les pratiques de partage des données sont surveillées. Pour plus d'informations sur la fonction WIP, consultez le site https://technet.microsoft.com/itpro/windows/keep-secure/protect-enterprise-data-using-wip.

Les applications que vous spécifiez peuvent être compatibles ou non. Les applications compatibles peuvent créer des données professionnelles et personnelles, mais aussi y accéder. Les applications non compatibles peuvent uniquement créer des données professionnelles et y accéder. Pour plus d'informations sur les applications compatibles et non compatibles, consultez le site https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/enlightened-microsoft-apps-and-wip.

## Créer un profil de protection des données Windows

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Protection > Protection des informations Windows**.
3. Cliquez sur +.
4. Saisissez le nom et la description du profil.
5. Configurez les valeurs qui conviennent pour chaque paramètre de profil. Pour plus de détails sur chaque paramètre de profil, reportez-vous à la section Windows 10 : paramètres de profil de protection des données Windows.
6. Cliquez sur **Ajouter**.

# Windows 10 : paramètres de profil de protection des données Windows

| Windows 10 : paramètre de profil de protection des données Windows | Description |
|---|---|
| Paramètres de protection des données Windows | Ce paramètre indique si la protection des données Windows est activée et son degré d'application. Lorsque ce paramètre est défini sur « Désactivé », les données ne sont pas cryptées et la journalisation des audits est désactivée. Lorsque ce paramètre est défini sur « Silencieux », les données sont cryptées et toute tentative de partage de données protégées est consignée. Lorsque ce paramètre est défini sur « Remplacer », les données sont cryptées, l'utilisateur reçoit une invite lorsqu'il tente de partager des données protégées, et toute tentative de partage de données protégées est consignée. Lorsque ce paramètre est défini sur « Bloquer », les données sont cryptées, les utilisateurs ne peuvent pas partager des données protégées, et toute tentative de partage de données protégées est consignée.<br><br>Valeurs possibles :<br><br>• 0<br>• Silencieux<br>• Remplacer<br>• Bloquer<br><br>La valeur par défaut est « Off ». |
| Noms de domaines d'entreprise protégés | Ce paramètre spécifie les noms des domaines du réseau professionnel que votre entreprise utilise pour les identités de ses utilisateurs. Vous pouvez séparer plusieurs domaines avec des barres verticales (\|). Le premier domaine est utilisé comme une chaine pour marquer les fichiers protégés par des applications qui utilisent WIP.<br><br>Par exemple : `example.com\|example.net`. |
| Fichier de certificat de récupération de données (.der, .cer) | Ce paramètre spécifie le fichier de certificat de récupération de données. Le fichier que vous spécifiez doit être un certificat codé PEM ou DER, avec une extension de fichier.der ou .cer.<br><br>Vous utilisez le fichier de certificat de récupération de données pour récupérer des fichiers qui étaient protégés localement sur un terminal. Par exemple, si votre entreprise souhaite récupérer des données protégées par WIP depuis un terminal.<br><br>Pour plus d'informations sur la création d'un certificat de récupération des données, consultez la documentation relative à la protection des données Microsoft Windows. |
| Supprimer les paramètres de protection des données Windows lorsqu'un terminal est supprimé de BlackBerry UEM | Ce paramètre spécifie si les paramètres WIP doivent être révoqués lorsqu'un terminal est désactivé. Lors les paramètres WIP sont révoqués, l'utilisateur ne peut plus accéder aux fichiers protégés. |

| Windows 10 : paramètre de profil de protection des données Windows | Description |
|---|---|
| Afficher un filigrane de protection des données Windows sur les fichiers et applications protégés autorisés à créer du contenu d'entreprise | Ce paramètre spécifie si une icône de superposition est affichée sur les icônes de fichier et d'application pour indiquer si un fichier ou une application est protégé(e) par WIP. |
| Portée IP du réseau professionnel | Ce paramètre spécifie la plage d'adresses IP au travail avec laquelle une application protégée par WIP peut partager des données.<br>Utilisez un tiret pour indiquer une plage d'adresses. Utilisez une virgule pour séparer les adresses. |
| Les plages d'adresses IP de réseau professionnel font autorité. | Ce paramètre spécifie si seules les plages d'adresses IP du réseau professionnel sont acceptées dans ce réseau professionnel. Lorsque ce paramètre est activé, aucune tentative n'est effectuée pour détecter d'autres réseaux professionnels.<br>Par défaut, cette option n'est pas sélectionnée. |
| Serveurs proxy internes d'entreprise | Ce paramètre spécifie les serveurs proxy internes qui sont utilisés lors de la connexion à des emplacements de réseaux professionnels. Ces serveurs proxy sont utilisés uniquement lors de la connexion à des domaines répertoriés dans les paramètres des ressources Enterprise Cloud. |
| Ressources d'entreprise dans le cloud | Ce paramètre spécifie la liste des domaines de ressources d'entreprise hébergés dans le cloud qui doivent être protégés. Les données de ces ressources sont considérées comme des données d'entreprise et sont donc protégées. |
| Domaine de ressources dans le cloud | Ce paramètre spécifie le nom du domaine. |
| Proxy couplé | Ce paramètre spécifie un proxy qui est associé à une ressource dans le cloud. Le trafic vers la ressource dans le cloud sera acheminé pour tout le réseau d'entreprise via le serveur proxy indiqué (sur le port 80).<br>Un serveur proxy utilisé à cette fin doit également être configuré dans le champ Serveurs proxy internes de l'entreprise. |
| Serveurs proxy d'entreprise | Ce paramètre spécifie la liste des serveurs proxy Internet. |
| Les serveurs proxy d'entreprise font autorité. | Ce paramètre indique si le client doit accepter la liste configurée de proxies et ne pas essayer de détecter d'autres proxies d'entreprise. |
| Ressources neutres | Ce paramètre spécifie les domaines pouvant être utilisés pour les ressources personnelles ou professionnelles. |

| Windows 10 : paramètre de profil de protection des données Windows | Description |
|---|---|
| Noms de domaines de réseau d'entreprise | Ce paramètre répertorie les domaines (séparés par des virgules) compris dans les limites de l'entreprise. Lorsque les données d'un de ces domaines seront envoyées à un terminal, elles seront considérées comme des données d'entreprise protégées. Ces emplacements seront considérés comme une destination sécurisée pour le partage des données d'entreprise.<br><br>Par exemple, `example.com`, `example.net`. |
| Code de charge utile d'application de bureau | Spécifiez les clés et les valeurs des applications de bureau qui sont utilisées pour configurer les restrictions de lancement d'application sur les terminaux Windows 10. Vous devez utiliser les clés définies par Microsoft pour le type de charge utile que vous souhaitez configurer.<br><br>Pour spécifier les applications, copiez le code XML du fichier .xml de la stratégie AppLocker et collez-le dans ce champ. Lors de la copie du texte, copiez uniquement les éléments présentés dans l'exemple de code suivant :<br><br>`<RuleCollection Type="Appx" EnforcementMode="Enabled">`<br>`  <FilePublisherRule Id="0c9781aa-bf9f-4352-`<br>`b4ba-64c25f36f558"`<br>`  Name="WordMobile" Description="`<br>` UserOrGroupSid="S-1-1-0" Action="Allow">`<br>`    <Conditions>`<br>`      <FilePublisherCondition`<br>`      PublisherName="CN=Microsoft Corporation, O=Microsoft`<br>` Corporation, L=Redmond, S=Washington, C=US"`<br>`      ProductName="Microsoft.Office.Word" BinaryName="*">`<br>`        <BinaryVersionRange LowSection="*"`<br>` HighSection="*" />`<br>`      </FilePublisherCondition>`<br>`    </Conditions>`<br>`  </FilePublisherRule>`<br>`</RuleCollection>`<br><br>Pour plus d'informations sur l'utilisation d'AppLocker, consultez la documentation relative à Applocker sous Microsoft. |

| Windows 10 : paramètre de profil de protection des données Windows | Description |
|---|---|
| Code de charge utile de l'application de la plateforme Windows universelle | Spécifiez les clés et valeurs d'application de la plateforme Windows universelle utilisées pour configurer WIP sur les terminaux Windows 10. Vous devez utiliser les clés définies par Microsoft pour le type de charge utile que vous souhaitez configurer.<br><br>Pour spécifier les applications, copiez le code XML du fichier .xml de la stratégie AppLocker et collez-le dans ce champ. Lors de la copie du texte, copiez uniquement les éléments présentés dans l'exemple de code suivant :<br><br>`<RuleCollection Type="Exe" EnforcementMode="Enabled">`<br>`  <FilePathRule Id="921cc481-6e17-4653-8f75-050b80acca20"`<br>`  Name="(Default Rule)`<br>`  All files" Description="" UserOrGroupSid="S-1-1-0"`<br>`  Action="Allow">`<br>`  <Conditions>`<br>`  <FilePathCondition Path="*" />`<br>`  </Conditions>`<br>`  </FilePathRule>`<br>`  <FilePublisherRule Id="ddd0bc90-`<br>`dada-4002-9e2f-0fc68e1f6af0" Name="WORDPAD.EXE,`<br>`  from O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON,`<br>`  C=US" Description=""`<br>`  UserOrGroupSid="S-1-1-0" Action="Deny">`<br>`  <Conditions>`<br>`  <FilePublisherCondition PublisherName="O=MICROSOFT`<br>`  CORPORATION`<br>`  L=REDMOND, S=WASHINGTON, C=US" ProductName="*"`<br>`  BinaryName="WORDPAD.EXE">`<br>`  <BinaryVersionRange LowSection="*"`<br>`  HighSection="*" />`<br>`  </FilePublisherCondition>`<br>`  </Conditions>`<br>`  </FilePublisherRule>`<br>`  <FilePublisherRule Id="c8360d06-f651-4883-`<br>`abdd-9c3a95a415ff" Name="NOTEPAD.EXE,`<br>`  from O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON,`<br>`  C=US" Description=""`<br>`  UserOrGroupSid="S-1-1-0" Action="Allow">`<br>`  <Conditions>`<br>`  <FilePublisherCondition PublisherName="O=MICROSOFT`<br>`  CORPORATION,`<br>`  L=REDMOND, S=WASHINGTON, C=US" ProductName="*"`<br>`  BinaryName="NOTEPAD.EXE">`<br>`  <BinaryVersionRange LowSection="*"`<br>`  HighSection="*" />`<br>`  </FilePublisherCondition>`<br>`  </Conditions>`<br>`  </FilePublisherRule>`<br>`</RuleCollection>`<br><br>Pour plus d'informations sur l'utilisation d'AppLocker, consultez la documentation relative à Applocker sous Microsoft. |

| Windows 10 : paramètre de profil de protection des données Windows | Description |
| --- | --- |
| Profil VPN associé | Ce paramètre spécifie le profil VPN utilisé par un terminal pour se connecter à un réseau VPN lorsqu'une application protégée par WIP est utilisée.<br>Ce paramètre est valide uniquement si l'option « Utiliser un profil VPN » est sélectionnée pour la « Connexion sécurisée utilisée avec WIP ». |
| Collecter les journaux d'audit du terminal | Ce paramètre spécifie si la collecte des journaux d'audit du terminal est requise. |

# Autoriser le cryptage BitLocker sur les terminaux Windows 10

BitLocker Drive Encryption est une fonctionnalité de protection des données du système d'exploitation qui permet de limiter l'accès non autorisé aux données en cas de perte ou de vol d'un terminal. Vous pouvez autoriser le cryptage BitLocker sur les terminaux Windows 10 et la protection est renforcée si le terminal est également équipé d'un standard cryptographique TPM (Trusted Platform Module), ce qui vous permet de demander une authentification supplémentaire au démarrage (par exemple, une clé de démarrage, un code PIN ou un lecteur USB amovible). Dans BlackBerry UEM, vous pouvez également créer un profil de conformité afin d'empêcher les utilisateurs de désactiver BitLocker pour imposer son utilisation sur les terminaux nécessitant un cryptage.

Vous pouvez configurer les options de récupération pour accéder à un système d'exploitation ou à des lecteurs de données protégés par BitLocker. Les utilisateurs peuvent accéder aux clés de récupération à partir de la console Active Directory et, s'ils sont activés, les mots de passe de récupération peuvent être sauvegardés sur Active Directory Domain Services afin qu'un administrateur puisse les récupérer à l'aide de l'outil BitLocker Recovery Password Viewer.

Configurez les règles de stratégie informatique UEM suivantes pour prendre en charge le cryptage BitLocker sur les terminaux Windows 10 :

- Méthode de cryptage BitLocker pour le bureau
- Autoriser les invites de cryptage de la carte de stockage sur le terminal
- Autoriser BitLocker Device Encryption à activer le cryptage sur le terminal
- Définir les méthodes de cryptage par défaut pour chaque type de lecteur
- Exiger une authentification supplémentaire au démarrage
- Exiger une longueur de code PIN minimum pour le démarrage
- URL et message de récupération avant démarrage
- Options de récupération de lecteurs du SE BitLocker
- Options de récupération de lecteurs fixes BitLocker
- Exiger la protection BitLocker pour les lecteurs de données fixes
- Exiger la protection BitLocker pour les lecteurs de données amovibles
- Autoriser l'invite de l'emplacement de la clé de récupération
- Activer le cryptage pour les utilisateurs standard

Pour plus d'informations sur les règles de stratégie informatique BitLocker, consultez la Fiche de référence des stratégies.

# Gestion de l'attestation des terminaux

Lorsque vous activez l'attestation, BlackBerry UEM envoie des défis pour tester l'authenticité et l'intégrité des terminaux. Vous pouvez activer l'attestation pour les terminaux suivants :

- Terminaux Samsung Knox
- Terminaux Android
- Terminaux Windows 10

## Gestion de l'attestation des terminaux Samsung Knox

Lorsque vous activez l'attestation, BlackBerry UEM vérifie l'authenticité et l'intégrité des terminaux Samsung Knox activés avec les types d'activation suivants :

- Travail et Personnel - Contrôle total (Samsung Knox)
- Espace Travail uniquement (Samsung Knox)
- Travail et Personnel - Confidentialité des données de l'utilisateur (Samsung Knox)

1. Dans la barre de menus, cliquez sur **Paramètres > Paramètres généraux > Attestation**.
2. Pour activer l'attestation pour les terminaux Samsung Knox, sélectionnez **Activer les vérifications d'attestation périodiques pour les terminaux KNOX Workspace**.
3. Dans la section **Fréquence des vérifications**, spécifiez la fréquence, en jours ou en heures, à laquelle le terminal doit renvoyer une réponse d'attestation à BlackBerry UEM.
4. Dans la section **Période de grâce**, spécifiez une période de grâce. Après l'expiration du délai de grâce sans réponse d'attestation, un terminal est considéré comme non conforme et le terminal est soumis aux conditions spécifiées dans le profil de conformité attribué à l'utilisateur. Notez que si le terminal d'un utilisateur se trouve en dehors de la zone de couverture, est éteint ou déchargé, celui-ci ne pourra pas répondre aux vérifications d'attestation que BlackBerry UEM envoie et BlackBerry UEM considérera le terminal comme non conforme. Si vous avez défini la politique de conformité de votre organisation pour effacer le terminal lorsqu'il n'est pas conforme, lorsque le terminal ne répond pas avant l'expiration du délai de grâce, les données du terminal seront supprimées.
5. Cliquez sur **Enregistrer**.

**À la fin :** Créez un profil de conformité définissant les actions prises si un terminal est considéré comme débridé. Pour obtenir des instructions, reportez-vous à Application des règles de conformité aux terminaux

## Gestion de l'attestation des terminaux Android et des applications BlackBerry Dynamics à l'aide de SafetyNet

Lorsque vous utilisez l'attestation Android SafetyNet, BlackBerry UEM envoie des défis pour tester l'authenticité et l'intégrité des terminaux Android et des applications BlackBerry Dynamics dans l'environnement de votre entreprise. SafetyNet vous aide à évaluer la sécurité et la compatibilité des environnements dans lesquels les applications de votre entreprise s'exécutent. Vous pouvez utiliser l'attestation SafetyNet en plus de la détection d'exploitation et de racine existante BlackBerry. Pour plus d'informations sur SafetyNet, reportez-vous aux informations de Google.

BlackBerry UEM effectue une attestation SafetyNet dans les circonstances suivantes :

- Après l'activation du terminal lorsque BlackBerry UEM Client est installé
- Pendant l'activation du terminal lorsque BlackBerry UEM Client est installé

- Pendant l'activation des applications BlackBerry Dynamics
- Après l'activation de l'application pour les applications BlackBerry Dynamics
- À la demande en utilisant les API REST
- Au redémarrage de terminal si BlackBerry UEM Client est activé

## Considérations sur la configuration de l'attestation SafetyNet

- L'option Échec de l'attestation Google SafetyNet est un paramètre du profil de conformité pour les terminaux Android et les applications BlackBerry Dynamics qui permet de spécifier les actions qui se produisent si les terminaux ou les applications n'obtiennent pas l'attestation SafetyNet. Pour définir cette option, accédez à **Stratégies et profils > Conformité > onglet Android**.
- Si vous n'activez pas la règle de conformité Échec de l'attestation Google SafetyNet, les applications qui sont déjà activées ne seront pas soumises aux mesures de conformité.
- Lorsque vous activez SafetyNet, l'attestation est exécutée pendant l'activation. Vous ne pouvez pas utiliser de stratégie pour appliquer l'attestation lors de l'activation.
- BlackBerry UEM Client n'est pas nécessaire pour activer l'attestation SafetyNet.
- BlackBerry UEM Client n'apparait pas dans la liste des applications BlackBerry Dynamics que vous pouvez configurer pour l'attestation SafetyNet. BlackBerry UEM envoie des vérifications d'attestation à BlackBerry UEM Client, qui lui répond.
- BlackBerry UEM envoie des vérifications d'attestation à chaque application BlackBerry Dynamics que vous configurez.
- BlackBerry UEM n'a pas confiance dans les anciennes versions des applications. Par exemple, si vous souhaitez activer les vérifications d'attestation pour BlackBerry Work, vous devez vous assurer que la version de BlackBerry Work des terminaux de votre entreprise est la plus récente ou les nouvelles activations échoueront. Notez qu'à moins d'activer l'option Échec de l'attestation Google SafetyNet dans le profil de conformité de votre entreprise, même si les utilisateurs activés existants utilisent d'anciennes versions des applications, aucune action défavorable ne sera exécutée sur les applications et les terminaux.
- En plus de l'activation et de l'attestation périodique, BlackBerry UEM utilise les nouvelles API REST qui permettent de créer des flux de serveur personnalisés. Par exemple, si une application a besoin d'accéder à un élément distant sécurisé, avant d'accorder l'accès, le serveur d'application communique avec BlackBerry UEM pour appliquer l'attestation SafetyNet sur l'application ou le terminal.
- Si le terminal d'un utilisateur se trouve en dehors de la zone de couverture, est éteint ou déchargé, celui-ci ne pourra pas répondre aux vérifications d'attestation que BlackBerry UEM envoie et BlackBerry UEM considérera le terminal comme non conforme. Si vous avez défini la politique de conformité de votre entreprise afin d'effacer le terminal lorsqu'il n'est pas conforme, lorsque le terminal ne répond pas avant l'expiration du délai de grâce, les données du terminal sont supprimées lorsque le terminal se connecte au réseau sans fil.
- Si vous définissez un délai dans le champ Période de grâce de l'application, seules les applications qui ne répondent pas dans le délai que vous avez défini seront soumises à une action. Par exemple, si vous définissez la valeur de la période de grâce de l'application sur 7 jours et que vos utilisateurs se servent de BlackBerry Work tous les jours, mais n'utilisent pas BlackBerry Tasks dans les 7 jours, seul BlackBerry Tasks est soumis à une action.
- Si vous ajoutez une nouvelle application à BlackBerry UEM et qu'elle n'obtient pas l'attestation pendant l'activation, l'application n'est pas activée quelle que soit l'option que vous avez configurée dans la section Échec de l'attestation Google SafetyNet du profile de conformité de votre entreprise. Si une application est déjà activée, elle est soumise aux règles que vous avez spécifiées dans le profil de conformité.
- Les utilisateurs de votre entreprise doivent posséder la version la plus récente des services Google Play.
- Si un terminal n'obtient pas l'attestation, l'échec n'est pas indiqué dans la colonne Système d'exploitation compromis de la page Terminaux gérés.
- Pour plus d'informations sur le développement d'applications BlackBerry Dynamics pour Android, reportez-vous au contenu destiné aux développeurs.

## Configuration de l'attestation des terminaux Android et des applications BlackBerry Dynamics à l'aide de SafetyNet

1. Dans la barre de menus, cliquez sur **Paramètres > Paramètres généraux > Attestation**.
2. Pour activer l'attestation pour les terminaux Android, sélectionnez **Activer les vérifications périodiques d'attestation à l'aide de SafetyNet**.
3. Sélectionnez **Activer la correspondance de profil CTS** si vous souhaitez activer Compatibility Test Suite de Google. Pour plus d'informations sur CTS, reportez-vous aux informations à partir de Google.
4. Dans la section **Fréquence des vérifications**, spécifiez la fréquence, en jours ou en heures, à laquelle le terminal doit renvoyer une réponse d'attestation à BlackBerry UEM. Considérations pour la configuration de la fréquence de vérification :
   - Bien que vous puissiez configurer la fréquence à laquelle BlackBerry UEM vérifie l'authenticité et l'intégrité du terminal, l'attestation pendant l'activation de l'application est obligatoire.
   - Si vous avez déployé BlackBerry UEM Client, il est ajouté comme l'une des applications que BlackBerry UEM teste automatiquement pour l'attestation SafetyNet.
   - BlackBerry UEM Client utilise un canal de communication vers BlackBerry UEM différent de celui des autres applications BlackBerry Dynamics, qui doivent être exécutées et autorisées à se connecter à BlackBerry UEM pour recevoir les mises à jour des stratégies. BlackBerry UEM peut communiquer proactivement avec BlackBerry UEM Client et démarrer l'application si elle ne fonctionne pas. Si vous définissez une fréquence de vérification de 3 heures, alors BlackBerry UEM communique avec BlackBerry UEM Client toutes les 3 heures et la vérification de l'attestation est effectuée. Cependant, les commandes de l'application BlackBerry Dynamics sont stockées jusqu'à ce que l'application se connecte à BlackBerry UEM, et seule la dernière commande d'attestation est stockée. Ainsi, si l'application n'est pas utilisée pendant 24 heures, lorsque l'utilisateur la lance, une seule vérification d'attestation est effectuée.
5. Dans la section **Période de grâce**, spécifiez une période de grâce. Après l'expiration du délai de grâce sans réponse d'attestation, un terminal est considéré comme non conforme et le terminal est soumis aux conditions spécifiées dans le profil de conformité attribué à l'utilisateur. De plus, si le terminal d'un utilisateur se trouve en dehors de la zone de couverture, est éteint ou déchargé, celui-ci ne pourra pas répondre aux vérifications d'attestation que BlackBerry UEM envoie et BlackBerry UEM considérera le terminal comme non conforme. Si vous avez défini la politique de conformité de votre entreprise afin d'effacer le terminal lorsqu'il n'est pas conforme, lorsque le terminal ne répond pas avant l'expiration du délai de grâce, les données du terminal sont supprimées lorsque le terminal se connecte au réseau sans fil.
6. Dans la section **Période de grâce de l'application**, spécifiez une période de grâce. Lorsque la période de grâce expire, les applications BlackBerry Dynamics sont soumises aux conditions spécifiées dans le profil de conformité attribué à l'utilisateur. La période de grâce est appliquée pour chaque application. Notez que si vous avez déployé uniquement BlackBerry UEM Client sur le terminal, la période de grâce est ignorée. De plus, BlackBerry UEM Client n'apparaît pas dans la liste des applications BlackBerry Dynamics. Lorsque vous ajoutez des applications BlackBerry Dynamics à la liste des applications qui font l'objet d'une vérification d'attestation, les règles suivantes s'appliquent :
   - Seules les applications de cette liste reçoivent une vérification d'attestation.
   - Seules les applications de cette liste sont évaluées pour le contrôle de la période de grâce des applications.
   - Seules les applications de cette liste font l'objet d'une attestation lors de l'activation de l'application.

   **Remarque :** Seules les applications BlackBerry Dynamics qui ont été développées spécifiquement pour SafetyNet s'affichent dans la liste. Pour plus d'informations, reportez-vous aux contenus relatifs au Développeur.
7. Pour ajouter une application sujette à des vérifications d'attestation, cliquez sur +.
8. Effectuez l'une des opérations suivantes :
   - Cliquez sur le nom d'une application qui figure déjà dans la liste.
   - Recherchez et cliquez sur le nom de l'application.

9. Cliquez sur **Sélectionner**.
10. Cliquez sur **Enregistrer**.

# Gestion de l'attestation des terminaux Windows 10

Lorsque vous activez l'attestation, BlackBerry UEM vérifie l'authenticité et l'intégrité des terminaux Windows 10. Le terminal communique avec le service d'attestation d'intégrité de Microsoft pour vérifier la conformité en fonction des paramètres définis dans le profil de conformité de votre entreprise.

1. Dans la barre de menus, cliquez sur **Paramètres > Paramètres généraux > Attestation**.
2. Pour activer l'attestation pour les terminaux Windows 10, sélectionnez **Activer les vérifications d'attestation périodiques pour les terminaux Windows 10**.
3. Dans la section **Fréquence des vérifications**, spécifiez la fréquence, en jours ou en heures, à laquelle le terminal doit renvoyer une réponse d'attestation à BlackBerry UEM.
4. Dans la section **Période de grâce**, spécifiez une période de grâce. Après l'expiration du délai de grâce sans réponse d'attestation, un terminal est considéré comme non conforme et le terminal est soumis aux conditions spécifiées dans le profil de conformité attribué à l'utilisateur. Autre élément à prendre en compte : si le terminal d'un utilisateur est en dehors de la zone de couverture, éteint ou a une batterie déchargée, celui-ci ne pourra pas répondre aux défis d'attestation que BlackBerry UEM envoie et BlackBerry UEM considèrera le terminal comme non conforme. Si vous avez défini la politique de conformité de votre organisation pour effacer le terminal lorsqu'il n'est pas conforme, lorsque le terminal ne répond pas avant l'expiration du délai de grâce, les données du terminal seront supprimées.
5. Cliquez sur **Enregistrer**.

Vous pouvez afficher les violations de conformité sur la page des détails du terminal.

**À la fin :** Créez un profil de conformité définissant les actions prises si un terminal est considéré comme débridé. Pour obtenir des instructions, reportez-vous à Application des règles de conformité aux terminaux

# Informations juridiques



Cette documentation, y compris la documentation incluse pour référence telle que celle fournie ou mise à disposition sur le site Web BlackBerry, est fournie ou mise à disposition « EN L'ÉTAT » et « TELLE QUELLE », sans condition ni garantie en tout genre de la part de BlackBerry Limited et de ses filiales (« BlackBerry »), et BlackBerry décline toute responsabilité en cas d'erreur ou d'oubli typographique, technique ou autre inexactitude contenue dans ce document. Pour des raisons de protection des informations confidentielles et/ou des secrets commerciaux de BlackBerry, cette documentation peut décrire certains aspects de la technologie BlackBerry en termes généraux. BlackBerry se réserve le droit de modifier périodiquement les informations contenues dans cette documentation. Cependant, BlackBerry ne s'engage en aucune manière à vous communiquer les modifications, mises à jour, améliorations ou autres ajouts apportés à cette documentation.

La présente documentation peut contenir des références à des sources d'informations, du matériel ou des logiciels, des produits ou des services tiers, y compris des composants et du contenu tel que du contenu protégé par copyright et/ou des sites Web tiers (ci-après dénommés collectivement « Produits et Services tiers »). BlackBerry ne contrôle pas et décline toute responsabilité concernant les Produits et Services tiers, y compris, sans s'y limiter, le contenu, la précision, le respect du code de la propriété intellectuelle, la compatibilité, les performances, la fiabilité, la légalité, l'éthique, les liens ou tout autre aspect desdits Produits et Services tiers. La présence d'une référence aux Produits et Services tiers dans cette documentation ne suppose aucunement que BlackBerry se porte garant des Produits et Services tiers ou de la tierce partie concernée.

SAUF DANS LA MESURE SPÉCIFIQUEMENT INTERDITE PAR LES LOIS EN VIGUEUR DANS VOTRE JURIDICTION, TOUTES LES CONDITIONS, GARANTIES OU REPRÉSENTATIONS DE TOUTE NATURE, EXPRESSES OU TACITES, NOTAMMENT (SANS LIMITATIONS) LES CONDITIONS, GARANTIES OU REPRÉSENTATIONS DE DURABILITÉ, D'ADÉQUATION À UNE UTILISATION OU À UN BUT PARTICULIER, DE COMMERCIALISATION, DE QUALITÉ MARCHANDE, DE NON-INFRACTION, DE SATISFACTION DE LA QUALITÉ OU DE TITRE, OU RÉSULTANT D'UNE LOI, D'UNE COUTUME, D'UNE PRATIQUE OU D'UN USAGE COMMERCIAL, OU EN RELATION AVEC LA DOCUMENTATION OU SON UTILISATION, OU LA PERFORMANCE OU NON-PERFORMANCE DES LOGICIELS, DU MATÉRIEL, DES SERVICE OU DES PRODUITS ET SERVICES TIERS CITÉS, SONT EXCLUES. VOUS POUVEZ JOUIR D'AUTRES DROITS QUI VARIENT SELON L'ÉTAT OU LA PROVINCE. CERTAINES JURIDICTIONS N'AUTORISENT PAS L'EXCLUSION OU LA LIMITATION DES GARANTIES ET CONDITIONS IMPLICITES. DANS LA MESURE AUTORISÉE PAR LES LOIS, TOUTE GARANTIE OU CONDITION IMPLICITE RELATIVE À LA DOCUMENTATION, DANS LA MESURE OÙ ELLES NE PEUVENT PAS ÊTRE EXCLUES EN VERTU DES CLAUSES PRÉCÉDENTES, MAIS PEUVENT ÊTRE LIMITÉES, SONT PAR LES PRÉSENTES LIMITÉES À QUATRE-VINGT-DIX (90) JOURS À COMPTER DE LA DATE DE LA PREMIÈRE ACQUISITION DE LA DOCUMENTATION OU DE L'ARTICLE QUI FAIT L'OBJET D'UNE RÉCLAMATION.

DANS LA MESURE MAXIMALE PERMISE PAR LES LOIS EN VIGUEUR DANS VOTRE JURIDICTION, EN AUCUN CAS BLACKBERRY N'EST RESPONSABLE DES DOMMAGES LIÉS À LA PRÉSENTE DOCUMENTATION OU À SON UTILISATION, OU À LA PERFORMANCE OU NON-PERFORMANCE DES LOGICIELS, DU MATÉRIEL, DES SERVICES OU DES PRODUITS ET SERVICES TIERS MENTIONNÉS DANS LES PRÉSENTES, ET NOTAMMENT, SANS S'Y LIMITER, DES DOMMAGES DIRECTS, EXEMPLAIRES, ACCIDENTELS, INDIRECTS, SPÉCIAUX, PUNITIFS OU AGGRAVÉS, DES DOMMAGES LIÉS À UNE PERTE DE PROFITS OU DE REVENUS, UN MANQUE À GAGNER, UNE INTERRUPTION D'ACTIVITÉ, UNE PERTE D'INFORMATIONS COMMERCIALES, UNE PERTE D'OPPORTUNITÉS COMMERCIALES, LA CORRUPTION OU LA PERTE DE DONNÉES, LE NON-ENVOI OU LA NON-RÉCEPTION DE DONNÉES, DES PROBLÈMES LIÉS À DES APPLICATIONS UTILISÉES AVEC DES PRODUITS OU SERVICES BLACKBERRY, DES COUTS D'INDISPONIBILITÉ, LA PERTE D'UTILISATION DES PRODUITS OU SERVICES BLACKBERRY EN TOUT OU EN PARTIE, OU DE TOUT SERVICE DE COMMUNICATION, DU COUT DE BIENS DE

SUBSTITUTION, DES FRAIS DE GARANTIE, DES ÉQUIPEMENTS OU SERVICES, DES COUTS DE CAPITAL, OU AUTRES PERTES FINANCIÈRES SIMILAIRES, PRÉVISIBLES OU NON, MÊME SI BLACKBERRY A ÉTÉ INFORMÉ DE LA POSSIBILITÉ DE TELS DOMMAGES.

DANS LA MESURE MAXIMALE PERMISE PAR LES LOIS APPLICABLES DANS VOTRE JURIDICTION, BLACKBERRY N'EST NULLEMENT TENU PAR DES OBLIGATIONS, DEVOIRS OU RESPONSABILITÉS, CONTRACTUELS, DÉLICTUELS OU AUTRES, PAS MÊME PAR UNE RESPONSABILITÉ EN CAS DE NÉGLIGENCE OU RESPONSABILITÉ STRICTE ET NE VOUS EST REDEVABLE EN RIEN.

LES LIMITATIONS, EXCLUSIONS ET CLAUSES DE NON-RESPONSABILITÉ CONTENUES DANS LES PRÉSENTES S'APPLIQUENT : (A) INDÉPENDAMMENT DE LA NATURE DE LA CAUSE D'ACTION, DE DEMANDE OU D'ACTION ENTREPRISE PAR VOUS, NOTAMMENT, SANS S'Y LIMITER, POUR RUPTURE DE CONTRAT, NÉGLIGENCE, FAUTE, RESPONSABILITÉ STRICTE OU TOUTE AUTRE THÉORIE LÉGALE, ET RESTENT APPLICABLES EN CAS DE RUPTURES SUBSTANTIELLES OU DE MANQUEMENT AU BUT ESSENTIEL DU PRÉSENT CONTRAT OU DE TOUT RECOURS ENVISAGEABLE PAR LES PRÉSENTES ; ET (B) À BLACKBERRY ET À SES FILIALES, LEURS AYANTS DROIT, REPRÉSENTANTS, AGENTS, FOURNISSEURS (NOTAMMENT LES FOURNISSEURS DE SERVICES), REVENDEURS AGRÉÉS BLACKBERRY (NOTAMMENT LES FOURNISSEURS DE SERVICES) ET LEURS DIRECTEURS, EMPLOYÉS ET SOUS-TRAITANTS RESPECTIFS.

OUTRE LES LIMITATIONS ET EXCLUSIONS SUSMENTIONNÉES, EN AUCUN CAS, LES DIRECTEURS, EMPLOYÉS, AGENTS, REVENDEURS, FOURNISSEURS, SOUS-TRAITANTS DE BLACKBERRY OU DE SES FILIALES N'ONT UNE RESPONSABILITÉ CONSÉCUTIVE OU RELATIVE À LA PRÉSENTE DOCUMENTATION.

Avant de vous abonner, d'installer ou d'utiliser des Produits et Services tiers, il est de votre responsabilité de vérifier que votre fournisseur de services prend en charge toutes les fonctionnalités. Certains fournisseurs de services peuvent ne pas proposer de fonctionnalités de navigation Internet avec un abonnement à BlackBerry® Internet Service. Vérifiez auprès de votre fournisseur de services la disponibilité, les accords d'itinérance, les plans de service et les fonctionnalités. L'installation ou l'utilisation de Produits et Services tiers avec des produits et services BlackBerry peuvent nécessiter un ou plusieurs brevets, marques commerciales, licences de copyright ou autres licences à des fins de protection des droits d'autrui. Vous êtes seul responsable de votre décision d'utiliser ou non les Produits et Services tiers et si cela nécessite l'obtention de licences tierces. Si de telles licences sont requises, vous êtes seul responsable de leur acquisition. Vous ne devez pas installer ou utiliser de Produits et Services tiers avant d'avoir acquis la totalité des licences nécessaires. Les Produits et Services tiers fournis avec les produits et services BlackBerry vous sont fournis à toutes fins utiles « EN L'ÉTAT » sans conditions, garanties ou représentations expresses ou tacites d'aucune sorte par BlackBerry, et BlackBerry n'engage aucune responsabilité sur les Produits et Services tiers à cet égard. L'utilisation que vous faites des Produits et Services tiers est régie par et dépendante de votre acceptation des termes des licences et autres accords distincts applicables à cet égard avec d'autres parties, sauf dans la limite couverte expressément par une licence ou autre accord conclu avec BlackBerry.

Les conditions d'utilisation de tout produit ou service BlackBerry sont stipulées dans une licence ou autre accord distinct conclu avec BlackBerry à cet égard. LE CONTENU DE CETTE DOCUMENTATION N'EST PAS DESTINÉ À REMPLACER LES ACCORDS OU GARANTIES EXPRÈS ET ÉCRITS FOURNIS PAR BLACKBERRY POUR UNE PARTIE DES PRODUITS OU SERVICES BLACKBERRY AUTRES QUE CETTE DOCUMENTATION.

BlackBerry Enterprise Software incorpore des éléments logiciels tiers. La licence et les informations de copyright associées à ce logiciel sont disponibles à l'adresse http://worldwide.blackberry.com/legal/thirdpartysoftware.jsp.

BlackBerry Limited
2200 University Avenue Est
Waterloo, Ontario
Canada N2K 0A7

BlackBerry UK Limited
Ground Floor, The Pearce Building, West Street,

Maidenhead, Berkshire SL6 1RL
Royaume-Uni

Publié au Canada