BlackBerry UEM

Gestion des terminaux Android

Administration

12.11

Contents

Gestion des terminaux Android

BlackBerry UEM permet de gérer avec précision la façon dont les terminaux Android se connectent à votre réseau, et de choisir les fonctionnalités à activer et les applications disponibles. Que les terminaux appartiennent à votre entreprise ou à vos utilisateurs, vous pouvez fournir un accès mobile aux informations de votre entreprise tout en les protégeant contre toute personne qui ne devrait pas y avoir accès.

Ce guide décrit les options dont vous disposez pour gérer les terminaux Android et vous aide à trouver les informations dont vous avez besoin pour profiter de toutes les fonctionnalités disponibles.

Gestion des terminaux portables

Vous pouvez activer et gérer certains terminaux portables Android dans BlackBerry UEM. Les terminaux portables, tels que les lunettes intelligentes, offrent aux utilisateurs un accès mains libres aux informations visuelles telles que les notifications, les instructions étape par étape, les images et les vidéos et leur permettent d'émettre des commandes vocales, de numériser des codes-barres et d'utiliser la navigation GPS.

BlackBerry UEM prend en charge les terminaux portables suivants :

- Vuzix M300 Smart Glasses

Pour gérer des terminaux portables, suivez les instructions relatives aux terminaux Android. Les fonctions BlackBerry UEM suivantes sont prises en charge pour les terminaux portables :

- Activation du terminal à l'aide d'un QR Code
- Stratégies informatiques
- Profils de connectivité Wi-Fi, VPN ou d'entreprise, Profils de conformité et Profils de certificat
- BlackBerry Secure Connect Service
- Commandes de terminaux
- Gestion des applications
- Groupes de terminaux
- Services de localisation

Les terminaux portables utilisent BlackBerry UEM Client pour l'activation. Vous pouvez activer les terminaux portables à l’aide d’un code QR au lieu d'un mot de passe d'activation. Pour plus d'informations, reportez-vous à Activer un terminal à l'aide de QR Code.

Fonctions que vous pouvez contrôler sur les terminaux Android

BlackBerry UEM offre tous les outils dont vous avez besoin pour contrôler les fonctions que les terminaux Android vous permettent de gérer. Il inclut également des fonctions qui vous permettent de donner aux utilisateurs des terminaux un accès sécurisé aux ressources professionnelles sans gérer entièrement le terminal.

Niveau de contrôle	Description
Terminaux non gérés Activations Confidentialité de l'utilisateur	Vous pouvez activer un terminal sur BlackBerry UEM ayant le type d'activation Confidentialité de l'utilisateur pour sécuriser l'accès à des ressources professionnelles sans gérer le terminal. Cette option est souvent utilisée pour les terminaux BYOD. Ces activations peuvent permettre aux utilisateurs d'accéder à votre réseau via un VPN en utilisant BlackBerry 2FA, de partager des fichiers de façon sécurisée à l'aide de BlackBerry Workspaces, et d'installer des applications BlackBerry Dynamics comme BlackBerry Work et BlackBerry Access pour accéder aux e-mails et à votre intranet professionnel.
Terminaux gérés avec profil professionnel Activations Travail et Personnel - Confidentialité des données de l'utilisateur (Android Enterprise)	Les terminaux Android Enterprise peuvent être gérés mais permettent un usage personnel en créant un profil professionnel sur le terminal qui sépare les données professionnelles et personnelles. Cette option préserve la confidentialité des données personnelles de l'utilisateur dans le profil personnel, mais vous permet de gérer les données professionnelles à l'aide de commandes et de règles de stratégie informatique. Vous pouvez gérer les applications sur le terminal, y compris les applications BlackBerry Dynamics. Vous pouvez effacer du terminal les données professionnelles, mais pas les données personnelles. Les données professionnelles et personnelles sont protégées à l'aide du cryptage et de l'authentification par mot de passe. Cette option est souvent utilisée pour les terminaux appartenant à une société et pouvant être utilisés à des fins personnelles (COPE) et les terminaux BYOD.
Terminaux entièrement gérés avec profil professionnel Activations Travail et Personnel - Contrôle total (Android Enterprise)	Les terminaux Android Enterprise 8.0 peuvent être entièrement gérés, mais permettent une certaine utilisation personnelle en créant un profil professionnel sur le terminal qui sépare les données professionnelles et personnelles, tout en permettant à votre entreprise de garder un contrôle total sur le terminal et d'effacer toutes les données stockées sur celui-ci. Certaines règles de stratégie informatique peuvent être appliquées séparément aux profils professionnels et personnels. Vous pouvez gérer les applications sur le terminal, y compris les applications BlackBerry Dynamics. Vous pouvez enregistrer les SMS, MMS et appels téléphoniques envoyés et reçus sur le terminal. Les données professionnelles et personnelles sont protégées à l'aide du cryptage et de l'authentification par mot de passe. Cette option est souvent utilisée pour gérer les terminaux COPE.

Niveau de contrôle	Description
Terminaux entièrement gérés Activations Espace Travail uniquement (Android Enterprise)	Les terminaux Android Enterprise peuvent être entièrement gérés et ont un profil de professionnel, mais aucun profil personnel. Cette option vous permet de gérer le terminal dans son ensemble à l'aide de commandes et de règles de stratégie informatique. Vous pouvez gérer les applications sur le terminal, y compris les applications BlackBerry Dynamics. Vous pouvez enregistrer les SMS, MMS et appels téléphoniques envoyés et reçus sur le terminal. Toutes les données du terminal sont protégées à l'aide du cryptage et d'une méthode d'authentification de type mot de passe. Cette option est souvent utilisée pour les terminaux appartenant à une société à usage professionnel uniquement (COBO).
Administration des terminaux Activations Contrôles MDM	Vous pouvez gérer les terminaux Android 9.x et versions antérieures à l'aide de commandes et de règles de stratégie informatique. Un espace Travail distinct n'est pas créé sur le terminal, et il n'existe aucune sécurité ajoutée pour les données professionnelles. Pour assurer la sécurité des données professionnelles, vous pouvez installer des applications BlackBerry Dynamics. Ce type d'activation sera obsolète dans une future version. Pour plus d'informations, rendez-vous sur le site Web https://support.blackberry.com/community pour lire l'article 48386.

Android Enterprise offre une prise en charge complète de la gestion des terminaux Android, y compris les fonctions suivantes :

- Appliquer les exigences de mot de passe
- Contrôler les capacités des terminaux à l'aide de stratégies informatiques (par exemple, vous pouvez désactiver la caméra ou Bluetooth)
- Appliquer les règles de conformité
- Créer des profils de connexion VPN et Wi-Fi (avec proxy)
- Synchroniser les e-mails, contacts et calendriers avec les terminaux
- Envoyer des certificats CA et de client aux terminaux pour l'authentification et S/MIME
- Gérer les applications publiques et internes requises et autorisées
- Localiser et protéger les terminaux perdus ou volés

Les terminaux Android Enterprise qui sont activés avec BlackBerry UEM prennent aussi en charge d'autres commandes disponibles uniquement pour les terminaux Samsung KNOX Platform for Enterprise et les terminaux BlackBerry optimisés par Android.

BlackBerry UEM prend également en charge les terminaux dotés d'activations Samsung KNOX Workspace outre la prise en charge de Samsung KNOX Platform for Enterprise. Cependant, les types d'activation Samsung KNOX seront obsolètes dans une future version. Pour plus d'informations, rendez-vous sur le site Web https://support.blackberry.com/community pour lire l'article 54614.

Licences utilisées par les terminaux Android

Lorsque vous ou un utilisateur activez un terminal Android avec BlackBerry UEM, vous l'associez à BlackBerry UEM pour pouvoir gérer les terminaux et l'accès des utilisateurs aux données professionnelles de leurs terminaux. Certains types d'activation Android nécessitent au minimum une licence Silver BlackBerry UEM ou une licence BlackBerry Enterprise Mobility Suite - Management Edition, mais d'autres licences peuvent être nécessaires en fonction des fonctionnalités que vous souhaitez activer pour les utilisateurs.

Fonctionnalité	Licence minimale requise
Contrôles MDM, activation Confidentialité de l'utilisateur ou activation Android Enterprise	Une des licences suivantes : • Silver • BlackBerry Enterprise Mobility Suite - Management Edition
Activation Samsung KNOX Workspace	Une des licences suivantes : • Gold Cross-Platform • Gold - KNOX Workspace • BlackBerry Enterprise Mobility Suite - Collaboration Edition
BlackBerry Secure Connect Plus	Une des licences suivantes : • Gold • BlackBerry Enterprise Mobility Suite - Collaboration Edition Pour plus d'informations sur BlackBerry Secure Connect Plus, reportez-vous au contenu relatif à l'administration de BlackBerry UEM ou au contenu relatif à l'administration de BlackBerry UEM Cloud.
Application BlackBerry Access	BlackBerry Enterprise Mobility Suite - Management Edition
Applications BlackBerry Work et BlackBerry Tasks	BlackBerry Enterprise Mobility Suite - Enterprise Edition
Toutes les autres applications BlackBerry et ISV BlackBerry Dynamics	BlackBerry Enterprise Mobility Suite - Collaboration Edition
Inscription du terminal pour BlackBerry 2FA uniquement	Une des licences suivantes : • BlackBerry 2FA • BlackBerry Enterprise Mobility Suite - Application Edition

Pour plus d'informations sur les licences, reportez-vous au contenu relatif aux licences.

Étapes à suivre pour gérer les terminaux Android

Étape	Action
1	Installez et configurez BlackBerry UEM selon les instructions d'installation.
2	Si votre organisation a l'intention de gérer des terminaux Android Enterprise, configurez un compte Google Play géré ou une connexion à votre domaine Google Cloud ou G Suite.
3	Vérifiez que vous disposez des licences requises pour activer les terminaux Android avec les fonctions souhaitées.
4	Configurez les stratégies informatiques des terminaux. Attribuez des stratégies informatiques à des groupes d'utilisateurs ou à des utilisateurs individuels.
5	Configurez des profils pour les terminaux. Attribuez des profils à des groupes d'utilisateurs ou à des utilisateurs individuels.
6	Spécifiez les applications que les terminaux peuvent ou doivent installer.
7	Activez des terminaux.
8	Gérez et surveillez les terminaux.

Prise en charge des activations Android Enterprise

Les entreprises qui utilisent des terminaux Android Enterprise disposent de plusieurs options pour se connecter aux services Google. La façon dont votre entreprise utilise les services Google détermine comment vous connectez BlackBerry UEM aux services Google et comment vous activez les terminaux. Pour plus d'informations sur la configuration de BlackBerry UEM pour se connecter à un domaine Google ou utiliser des comptes Google Play gérés, consultez le contenu relatif à la configuration.

Votre entreprise peut interagir avec les services Google de la manière suivante :

Connexion aux services Google	Description	Informations complémentaires
Comptes Google Play gérés	BlackBerry UEM n'est pas connecté à un domaine Google. Vous pouvez utiliser les comptes Google Play gérés pour permettre aux utilisateurs de télécharger et d'installer des applications professionnelles à l'aide de Google Play.	Prise en charge des activations Android Enterprise à l'aide de comptes Google Play gérés Activer un terminal Android Enterprise avec le type d'activation Travail et Personnel - Confidentialité des données de l'utilisateur Activer un terminal Android Enterprise à l'aide d'un compte géré Google Play
Domaine G Suite	Votre entreprise possède un domaine G Suite qui prend en charge tous les services G Suite tels que Gmail, Google Calendar et Google Drive.	Prendre en charge les activations Android Enterprise avec un domaine G Suite Activer un terminal Android Enterprise avec le type d'activation Travail et Personnel - Confidentialité des données de l'utilisateur Activer un terminal Android Enterprise lorsque BlackBerry UEM est connecté à un domaine Google
Domaine Google Cloud	Votre entreprise possède un domaine Google Cloud, qui fournit des comptes Google gérés aux utilisateurs. Votre entreprise n'utilise pas les services G Suite tels que Gmail, Google Calendar et Google Drive pour la gestion des e-mails, du calendrier et des données de votre entreprise.	Prendre en charge les activations Android Enterprise avec un domaine Google Cloud Activer un terminal Android Enterprise avec le type d'activation Travail et Personnel - Confidentialité des données de l'utilisateur Activer un terminal Android Enterprise lorsque BlackBerry UEM est connecté à un domaine Google
Aucun service Google	Les stratégies de sécurité de votre entreprise ne vous permettent pas d'utiliser les services Google.	Prise en charge des terminaux Android Enterprise sans accès à Google Play Activer un terminal Android Enterprise sans compte Google Play

Si vous prenez en charge les activations Android Enterprise, vous pouvez fournir BlackBerry Hub aux utilisateurs. Ils pourront ainsi gérer leurs messages électroniques professionnels et personnels ainsi que les données de leur calendrier dans une vue unifiée. Pour plus d'informations, reportez-vous à la section Activer la vue unifiée de BlackBerry Hub.

Prise en charge des activations Android Enterprise à l'aide de comptes Google Play gérés

Si vous n'avez pas ou ne voulez pas connecter BlackBerry UEM à un domaine Google, vous pouvez activer des terminaux Android Enterprise pour utiliser les comptes Google Play gérés. Lorsque vous utilisez des comptes Google Play gérés, vous pouvez utiliser n'importe quel compte Google ou Gmail pour connecter BlackBerry UEM à Google et aucune information personnelle identifiable sur vos utilisateurs n'est envoyée à Google. Pour plus d'informations sur les comptes Google Play gérés, rendez-vous sur https://support.google.com/googleplay/work/.

Une fois que vous avez connecté BlackBerry UEM à Google, vous pouvez permettre aux utilisateurs d'activer des terminaux Android Enterprise et de télécharger des applications professionnelles en utilisant Google Play. Pour plus d'informations sur la configuration de BlackBerry UEM afin de prendre en charge les terminaux Android Enterprise, reportez-vous au contenu relatif à la configuration.

Prendre en charge les activations Android Enterprise avec un domaine G Suite

Si vous avez configuré BlackBerry UEM pour se connecter à un domaine G Suite, vous devez exécuter les tâches suivantes afin de permettre aux utilisateurs d'activer leurs terminaux Android Enterprise.

Avant de commencer : Configurez BlackBerry UEM pour la prise en charge des terminaux Android Enterprise. Pour obtenir des informations sur la configuration de BlackBerry UEM afin de prendre en charge les terminaux Android Enterprise, reportez-vous au contenu relatif à la configuration.

1. Dans votre domaine G Suite, créez des comptes d'utilisateur pour vos utilisateurs Android.
2. Sélectionnez le paramètre **Appliquer la stratégie EMM** dans le domaine G Suite.

   Ce paramètre est obligatoire pour les terminaux avec les types d'activation Espace Travail uniquement et Travail et Personnel - Contrôle total et fortement recommandé pour les terminaux avec d'autres types d'activation. Si ce paramètre n'est pas sélectionné, les utilisateurs peuvent ajouter un compte Google géré au terminal qui peut accéder à ses applications à l'extérieur du profil de travail.
3. Si vous avez l'intention d'attribuer le type d'activation Espace Travail uniquement ou Travail et Personnel - Contrôle total, sélectionnez le paramètre **Appliquer la stratégie EMM** dans le domaine G Suite.
4. Dans BlackBerry UEM, créez des comptes d'utilisateur locaux pour vos utilisateurs Android. L'adresse électronique de chaque compte doit correspondre à l'adresse électronique du compte G Suite correspondant.
5. Assurez-vous que vos utilisateurs connaissent le mot de passe de leurs comptes G Suite.
6. Dans BlackBerry UEM, attribuez un profil de messagerie et des applications de productivité pour les utilisateurs, les groupes d'utilisateurs ou de terminaux.

Prendre en charge les activations Android Enterprise avec un domaine Google Cloud

Si vous avez configuré BlackBerry UEM pour se connecter à un domaine Google Cloud, vous devez exécuter les tâches suivantes afin de permettre aux utilisateurs d'activer leurs terminaux à l'aide de Android Enterprise.

Avant de commencer : Configurez BlackBerry UEM pour prendre en charge Android Enterprise. Lorsque vous configurez BlackBerry UEM pour qu'il se connecte à un domaine Google Cloud, vous devez choisir d'autoriser ou non BlackBerry UEM à créer des comptes d'utilisateur dans ce domaine. Ce choix déterminera les tâches que vous devrez effectuer avant que les utilisateurs puissent activer leurs terminaux Android Enterprise. Pour plus d'informations sur la configuration de BlackBerry UEM afin de prendre en charge les terminaux Android Enterprise, reportez-vous au contenu relatif à la configuration .

1. Dans BlackBerry UEM, créez des comptes d'utilisateur associés à l'annuaire pour vos utilisateurs Android Enterprise.
2. Si vous choisissez de ne pas autoriser BlackBerry UEM à créer des comptes d'utilisateur dans votre domaine Google Cloud, vous devez créer des comptes d'utilisateur dans votre domaine Google Cloud et dans BlackBerry UEM. Effectuez l'une des opérations suivantes :
   - Dans votre domaine Google Cloud, créez des comptes d'utilisateur pour vos utilisateurs Android Enterprise. Chaque adresse électronique doit correspondre à l'adresse électronique du compte d'utilisateur BlackBerry UEM correspondant. Assurez-vous que vos utilisateurs Android Enterprise connaissent le mot de passe de leur compte Google Cloud.
   - Utilisez l'outil Synchronisation de répertoire d'applications Google pour synchroniser votre domaine Google Cloud avec votre répertoire d'entreprise. Ce faisant, vous n'êtes pas tenu de créer de comptes d'utilisateur manuellement dans votre domaine Google Cloud.
3. Si vous affectez les types d'activation Espace Travail uniquement ou Travail et Personnel - Contrôle total, sélectionnez le paramètre **Appliquer la stratégie EMM** dans le domaine Google Cloud.

   Ce paramètre est obligatoire pour les terminaux avec les types d'activation Espace Travail uniquement et Travail et Personnel - Contrôle total, et fortement recommandé pour les terminaux avec d'autres types d'activation. Si ce paramètre n'est pas sélectionné, les utilisateurs peuvent ajouter un compte Google géré au terminal qui peut accéder à ses applications à l'extérieur du profil de travail.
4. Dans BlackBerry UEM, attribuez un profil de messagerie et des applications de productivité pour les utilisateurs, les groupes d'utilisateurs ou les groupes de terminaux.

Prise en charge des terminaux Android Enterprise sans accès à Google Play

Les terminaux qui n'ont pas accès à Google Play (par exemple, en raison de restrictions locales) doivent utiliser l'application BlackBerry UEM Enroll sur un terminal secondaire pour activer leur appareil avec UEM. Il utilise NFC pour lancer le téléchargement de l'application BlackBerry UEM Client sur le terminal que vous souhaitez activer. Vous pouvez installer l'application UEM Enroll sur un certain nombre de terminaux qui peuvent être utilisés pour activer un nombre illimité de terminaux avec UEM. Pour télécharger et installer l'application sur un terminal secondaire, rendez-vous sur le site Web support.blackberry.com/community pour lire l'article 42607.

Pour prendre en charge les terminaux Android Enterprise sans accès à Google Play, vérifiez le profil d'activation suivant :

- Si un terminal n'a pas accès à Google Play ou si vous ne souhaitez pas lui donner accès, désélectionnez l'option **Ajouter un compte Google Play à l'espace Travail**. Par défaut, cette option est sélectionnée.

- Si vous souhaitez activer BlackBerry Secure Connect Plus, sélectionnez l'option **Lors de l'activation de terminaux Android Enterprise, activez une fonctionnalité UEM Premium telle que BlackBerry Secure Connect Plus**.

Pour prendre en charge les terminaux qui ont besoin de BlackBerry Secure Connect Plus mais n'ont pas accès à Google Play, vous devez ajouter l'application BlackBerry Connectivity comme application interne. Pour télécharger la dernière application BlackBerry Connectivity pour les terminaux Android. Rendez-vous sur le site Web support.blackberry.com/community pour lire l'article 42607.

Après l'activation, pour attribuer des applications à des terminaux qui n'ont pas accès à Google Play, vous devez ajouter des applications internes et les attribuer à des terminaux. Procédez comme suit :

1. Sur la console de gestion BlackBerry UEM, dans la barre de menus, cliquez sur **Applications**.
2. Cliquez sur > **Applications internes**.
3. Cliquez sur **Parcourir**, puis sélectionnez le fichier .apk.
4. Dans le champ **Envoyer à**, sélectionnez **Tous les appareils Android**.
5. Désélectionnez **Publier l'application dans un domaine Google**.
6. Cliquez sur **Ajouter**.
7. Attribuez l'application que vous avez ajoutée à l'étape précédente aux utilisateurs de terminaux Android Enterprise qui n'ont pas accès à Google Play. La disposition de l'application doit être définie sur **Obligatoire**.

Contrôle des terminaux Android à l'aide d'une stratégie informatique

BlackBerry UEM envoie une stratégie informatique à chaque terminal. Vous pouvez utiliser une stratégie informatique par défaut ou créer vos propres stratégies informatiques. Vous pouvez créer autant de stratégies informatiques que vous le souhaitez pour différentes situations et différents utilisateurs, mais une seule stratégie informatique est active sur un terminal à la fois.

Les règles de stratégie informatique pour Android sont basées sur les capacités du terminal et les options de configuration du terminal fournies par Apple. Au fur et à mesure que Apple publie de nouvelles mises à jour du système d'exploitation avec de nouvelles fonctionnalités et options de configuration, de nouvelles règles de stratégie informatique sont ajoutées à UEM dès que l'occasion se présente.

Vous pouvez télécharger la fiche de référence des règles de stratégie informatique qui peut être consultée et classée. La fiche de référence contient toutes les règles disponibles dans UEM, y compris le système d'exploitation minimal du terminal qui prend en charge la règle.

Le comportement du terminal que vous contrôlez avec une stratégie informatique inclut les options suivantes :

- Exigences en matière de mot de passe du terminal
- Autoriser les fonctions des terminaux telles que l'appareil photo et, Bluetooth
- Permettre aux applications d'un profil d'accéder aux données d'un autre profil
- Restreindre la fonctionnalité uniquement pour les applications et les données du profil professionnel

Pour plus d'informations sur l'envoi de stratégies informatiques aux terminaux, consultez le contenu relatif à l'administration.

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.

Type d'activation	Règles de mot de passe prises en charge
Contrôles MDM	Utilisez les règles de mot de passe global pour configurer les exigences de mot de passe du terminal. Toutes les autres règles de mot de passe sont ignorées par le terminal. Utilisez un profil de conformité pour appliquer les exigences en matière de mot de passe.
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. Toutes les autres règles de mot de passe sont ignorées par le terminal. Utilisez un profil de conformité pour appliquer les exigences en matière 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. Utilisez les règles de mot de passe du profil professionnel pour définir les exigences en matière de mot de passe pour le profil professionnel. Pour les terminaux BlackBerry optimisés par Android, vous pouvez créer une règle obligeant à créer des mots de passe différents pour le professionnel et le terminal. Toutes les autres règles de mot de passe sont ignorées par le terminal. Utilisez un profil de conformité pour appliquer les exigences en matière de mot de passe.
Contrôles MDM (KNOX MDM)	Utilisez les règles de mot de passe KNOX MDM pour configurer les exigences de mot de passe du terminal. Toutes les autres règles de mot de passe sont ignorées par le terminal. Utilisez un profil de conformité pour appliquer les exigences en matière de mot de passe.
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. Toutes les autres règles de mot de passe sont ignorées par le terminal. Utilisez un profil de conformité pour appliquer les exigences en matière de mot de passe.
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. Utilisez les règles de mot de passe de KNOX Premium - Espace Travail pour définir les exigences de mot de passe pour l'espace Travail. Toutes les autres règles de mot de passe sont ignorées par le terminal. Utilisez un profil de conformité pour appliquer les exigences en matière de mot de passe.
Travail et Personnel - Confidentialité des données de l'utilisateur (Samsung KNOX)	Vous n'avez aucun contrôle sur le mot de passe du terminal. Utilisez les règles de mot de passe de KNOX Premium - Espace Travail pour définir les exigences de mot de passe pour l'espace Travail. Toutes les autres règles de mot de passe sont ignorées par le terminal. Utilisez un profil de conformité pour appliquer les exigences en matière de mot de passe.

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 :

- Contrôles MDM (sans Samsung KNOX)

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

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 : • Non spécifié : aucun mot de passe requis • Quelque chose : l'utilisateur doit définir un mot de passe, mais il n'existe aucune exigence de longueur ni de qualité • Numérique : le mot de passe doit inclure au moins un chiffre • Alphabétique : le mot de passe doit inclure au moins une lettre • Alphanumérique : le mot de passe doit inclure au moins une lettre et un chiffre • 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. Les terminaux activés en mode Commandes MDM sont nettoyés. 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 de minutes d'inactivité de l'utilisateur à l'issue de laquelle le terminal ou l'espace Travail se verrouille. 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 de mot de passe des règles 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 - Contrôle total (Android Enterprise)
- Travail et Personnel - Confidentialité des données de l'utilisateur (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 : • Non spécifié : aucun mot de passe requis • Quelque chose : l'utilisateur doit définir un mot de passe, mais il n'existe aucune exigence de longueur ni de qualité • Numérique : le mot de passe doit inclure au moins un chiffre • Alphabétique : le mot de passe doit inclure au moins une lettre • Alphanumérique : le mot de passe doit inclure au moins une lettre et un chiffre • Complexe : vous pouvez définir des exigences spécifiques pour différents types de caractères • Numérique complexe : le mot de passe doit contenir des caractères numériques, sans répétition (4444) ni séquence ordonnée (1234, 4321, 2468). • Biométrique (faible) : le mot de passe est compatible avec la technologie de reconnaissance biométrique à sécurité faible. 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 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 « Délai d'inactivité maximal avant verrouillage » du système d'exploitation natif, le terminal et l'espace Travail se verrouilleront une fois le délai écoulé.
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.

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

Contrôler les terminaux Android à l'aide de profils

BlackBerry UEM comprend plusieurs profils que vous pouvez utiliser pour contrôler divers aspects de la fonctionnalité du terminal. Les plus couramment utilisés comprennent les profils suivants :

Nom du profil	Description	Configurer
Activation	Spécifie les paramètres d'activation des terminaux pour les utilisateurs, tels que le type d'activation, la méthode, le nombre et les types de terminaux qu'un utilisateur peut activer.	Créer un profil d'activation
Wi-Fi	Spécifie les paramètres des terminaux à connecter à votre réseau Wi-Fi professionnel.	Créer un profil Wi-Fi
VPN	Spécifie les paramètres des terminaux à connecter à un VPN professionnel.	Créer un profil VPN
Proxy	Spécifie la manière dont les terminaux utilisent un serveur proxy pour accéder à des services Web sur Internet ou un réseau professionnel.	Créer un profil proxy
E-mail	Spécifie la manière dont les terminaux se connectent à un serveur de messagerie professionnel et synchronisent les e-mails, les entrées de calendrier et les données de l'organiseur. Si vous installez et configurez BlackBerry Work sur des terminaux, vous n'avez pas besoin de configurer un profil de messagerie.	Créer un profil de messagerie
BlackBerry Dynamics	Autorise les terminaux à accéder aux applications BlackBerry Dynamics, telles que BlackBerry Work, BlackBerry Access et BlackBerry Connect.	Créer un profil BlackBerry Dynamics
Connectivité BlackBerry Dynamics	Définit les connexions réseau, les domaines Internet, les plages d'adresses IP et les serveurs d'applications auxquels les terminaux peuvent se connecter lorsqu'ils utilisent des applications BlackBerry Dynamics.	Créer un profil de connectivité BlackBerry Dynamics
Conformité	Définit les conditions des terminaux non acceptables dans votre organisation, ainsi que les actions d'exécution.	Créer un profil de conformité
Connectivité d'entreprise	Spécifie si les appareils peuvent utiliser BlackBerry Secure Connect Plus.	Activer BlackBerry Secure Connect Plus

Nom du profil	Description	Configurer
Certificat d'AC	Spécifie un certificat d'AC que les terminaux peuvent utiliser pour établir une relation de confiance avec un réseau ou un serveur professionnel.	Créer un profil de certificat d'autorité de certification partagé
Informations d'identification de l'utilisateur	Spécifie comment les terminaux obtiennent les certificats clients utilisés pour s'authentifier auprès d'un réseau ou d'un serveur professionnel.	Créer un profil d'informations d'identification de l'utilisateur
SCEP	Spécifie le serveur SCEP via lequel les terminaux peuvent obtenir un certificat client d'authentification avec un réseau ou un serveur professionnel.	Créer un profil SCEP

Pour plus d'informations sur l'envoi de profils aux terminaux, consultez le contenu relatif à l'administration.

Référence des profils - terminaux Android

Le tableau suivant répertorie tous les profils BlackBerry UEM pris en charge par les terminaux Android :

Nom du profil	Description	Configurer
Stratégie		
Activation	Spécifie les paramètres d'activation des terminaux pour les utilisateurs, comme le type d'activation, le nombre et les types de terminaux.	Créez un profil d'activation
BlackBerry Dynamics	Autorise les terminaux à accéder aux applications BlackBerry Dynamics, telles que BlackBerry Work, BlackBerry Access et BlackBerry Connect.	Créez un profil BlackBerry Dynamics
Mode de verrouillage des applications	Spécifiez une application unique à exécuter sur les terminaux. Terminaux Samsung KNOX activés avec MDM uniquement	Créez un profil du mode de verrouillage des applications
Agent de gestion d'entreprise	Indique lorsque des terminaux se connectent à BlackBerry UEM pour des mises à jour d'applications ou de configuration, lorsqu'une notification push n'est pas disponible.	Créez un profil Enterprise Management Agent
Conformité		

Nom du profil	Description	Configurer
Conformité	Définit les conditions des terminaux non acceptables dans votre organisation, ainsi que les actions d'exécution. BlackBerry UEM inclut un profil de conformité par défaut.	Créez un profil de conformité
Conformité (BlackBerry Dynamics)	Il s'agit d'un profil en lecture seule qui affiche les paramètres de conformité importés de Good Control.	Gestion des profils de conformité BlackBerry Dynamics
Configuration logicielle minimale requise du terminal	Définit les versions du logiciel que les terminaux doivent avoir installées et spécifie une période de mise à jour pour les applications qui sont exécutées au premier plan.	Créez un profil d'exigences SR des terminaux
E-mail, calendrier et contacts		
E-mail	Spécifie la manière dont les terminaux se connectent à un serveur de messagerie professionnel et synchronisent les e-mails, les entrées de calendrier et les données de l'organiseur à l'aide d'Exchange ActiveSync ou IBM Notes Traveler.	Créez un profil de messagerie
Messagerie IMAP/ POP3	Spécifie la manière dont les terminaux se connectent à un serveur de messagerie IMAP ou POP3 et synchronisent les e-mails.	Créez un profil de messagerie IMAP/POP3
Contrôle	Spécifie les serveurs Microsoft Exchange à utiliser pour le contrôle d'accès automatique.	Créez un profil de contrôle d'accès
Réseaux et connexions		
Wi-Fi	Spécifie la manière dont les terminaux se connectent à un réseau Wi-Fi professionnel.	Créez un profil Wi-Fi profil
VPN	Spécifie la manière dont les terminaux se connectent à un VPN professionnel.	Créez un profil VPN
Proxy	Spécifie la manière dont les terminaux utilisent un serveur proxy pour accéder à des services Web sur Internet ou un réseau professionnel.	Créez un profil proxy

Nom du profil	Description	Configurer
Connectivité d'entreprise	Spécifie la manière dont les terminaux se connectent aux ressources de votre entreprise au travers de la connectivité d'entreprise. La connectivité d'entreprise est toujours activée pour les terminaux BlackBerry 10. Pour les terminaux BlackBerry 10 et Samsung KNOX Workspace, et pour les terminaux iOS supervisés avec commandes MDM, le profil de connectivité d'entreprise spécifie si les terminaux peuvent utiliser BlackBerry Secure Connect Plus. BlackBerry UEM inclut un profil de connectivité d'entreprise par défaut.	Créer un profil de connectivité d'entreprise
Connectivité BlackBerry Dynamics	Définit les connexions réseau, les domaines Internet, les plages d'adresses IP et les serveurs d'applications auxquels les terminaux peuvent se connecter lorsqu'ils utilisent des applications BlackBerry Dynamics.	Créez un profil de connectivité BlackBerry Dynamics
BlackBerry 2FA	Active l'authentification à deux facteurs pour les utilisateurs et spécifie la configuration de la préauthentification et les fonctionnalités de résolution autonome.	Créer un profil BlackBerry 2FA
Protection		
Protection des applications Microsoft Intune	Vous permet de gérer les applications protégées par Microsoft Intune.	Créez un profil de protection de l'application Microsoft Intune
Service de localisation	Vous permet de demander l'emplacement de terminaux et d'afficher les emplacements approximatifs sur une carte.	Créez un profil de service de localisation
Ne pas déranger	Vous permet de bloquer les notifications BlackBerry Work for Android en dehors des jours et heures de travail que vous définissez.	Créez un profil Ne pas déranger
Personnalisée		
Terminal	Vous permet de configurer les informations qui s'affichent sur les terminaux.	Créez un profil de terminal
Certificats		
Certificat d'AC	Spécifie un certificat d'AC que les terminaux peuvent utiliser pour établir une relation de confiance avec un réseau ou un serveur professionnel.	Créez un profil de certificat d'autorité de certification partagé

Nom du profil	Description	Configurer
Certificat partagé	Spécifie un certificat client que les terminaux peuvent utiliser pour authentifier les utilisateurs avec un réseau ou un serveur professionnel.	Créez un profil de certificat partagé
Informations d'identification de l'utilisateur	Spécifie la connexion d'AC via laquelle les terminaux peuvent obtenir un certificat client d'authentification avec un réseau ou un serveur professionnel.	Créez un profil d'informations d'identification de l'utilisateur
SCEP	Spécifie le serveur SCEP via lequel les terminaux peuvent obtenir un certificat client d'authentification avec un réseau ou un serveur professionnel.	Créez un profil SCEP
CRL	Spécifie les configurations CRL que BlackBerry UEM peut utiliser pour vérifier l'état des certificats. Terminaux BlackBerry alimentés uniquement par Android	Créez un profil CRL
Profil de mappage des certificats	Indique les certificats client que les applications doivent utiliser	Créez un profil de mappage de certificat

Gestion des applications sur les terminaux Android

Vous pouvez créer une bibliothèque d'applications que vous souhaitez gérer et surveiller sur les terminaux. Pour les terminaux Android Enterprise, seules les applications que vous autorisez peuvent être installées sur le profil professionnel. BlackBerry UEM fournit les options suivantes pour la gestion des applications sur les terminaux Android :

- Attribuer des applications publiques à partir de Google Play comme des applications optionnelles ou requises.
- Télécharger des applications personnalisées sur UEM et les déployer comme applications optionnelles ou requises.
- Préconfigurez les paramètres d'application, tels que les paramètres de connexion, lorsque l'application le permet.
- Bloquer l'accès des utilisateurs aux applications.
- Configurer des applications BlackBerry Dynamics publiques, ISV et personnalisées pour permettre aux utilisateurs d'accéder aux ressources professionnelles.
- Connecter UEM à Microsoft Intune pour définir les stratégies de protection des applications Intune à partir de la console de gestion de UEM afin de déployer et de gérer des applications Office 365 .
- Afficher la liste des applications personnelles installées sur les terminaux.
- Permettre aux utilisateurs d'évaluer et de commenter les applications pour les autres utilisateurs de votre environnement.

Comportement des applications sur les terminaux Android Enterprise

Pour les terminaux activés pour BlackBerry Dynamics, le catalogue d'applications professionnelles s'affiche dans BlackBerry Dynamics Launcher si vous l'avez ajouté à BlackBerry Dynamics Launcher.

Pour les terminaux activés avec « Travail et Personnel - Confidentialité des données de l'utilisateur », « Travail et Personnel - Contrôle total » ou « Espace Travail uniquement », il se produit ce qui suit :

Type d'application	Lorsque l'application est attribuée à un utilisateur	Lorsque les applications sont mises à jour	Lorsque l'application est désattribuée d'un utilisateur	Lorsque le terminal est supprimé de BlackBerry UEM
Applications publiques dotées d'une disposition obligatoire	Les applications sont installées automatiquement.	Les applications sont mises à jour automatiquement.	Les applications sont supprimées automatiquement du terminal.	Le profil professionnel et les applications professionnelles attribuées sont supprimés du terminal.
Applications publiques dotées d'une disposition facultative	L'utilisateur peut choisir d'installer ou non les applications. Les applications s'affichent dans Google Play for Work.	Google Play for Work informe les utilisateurs des mises à jour.	Les applications sont supprimées automatiquement du terminal.	Le profil professionnel et les applications professionnelles attribuées sont supprimés du terminal.

Type d'application	Lorsque l'application est attribuée à un utilisateur	Lorsque les applications sont mises à jour	Lorsque l'application est désattribuée d'un utilisateur	Lorsque le terminal est supprimé de BlackBerry UEM
Applications internes dotées d'une disposition obligatoire hébergées dans BlackBerry UEM	Prise en charge uniquement pour les terminaux Espace Travail uniquement. Les applications sont installées automatiquement.	Prise en charge uniquement pour les terminaux Espace Travail uniquement. Les applications sont installées automatiquement.	Les applications sont supprimées automatiquement du terminal.	Les applications sont supprimées automatiquement du terminal.
Applications internes dotées d'une disposition facultative hébergées dans BlackBerry UEM	L'utilisateur peut choisir d'installer ou non les applications. Les applications s'affichent dans Google Play for Work.	Google Play For Work informe les utilisateurs des mises à jour.	Les applications sont supprimées automatiquement du terminal.	Le profil professionnel et les applications professionnelles attribuées sont supprimés du terminal.
Applications internes dotées d'une disposition obligatoire hébergées dans Google Play	Les applications sont installées automatiquement sur le terminal.	Google Play For Work informe les utilisateurs des mises à jour.	Les applications sont supprimées automatiquement du terminal.	Le profil professionnel et les applications professionnelles attribuées sont supprimés du terminal.
Applications internes dotées d'une disposition facultative hébergées dans Google Play	L'utilisateur peut choisir d'installer ou non les applications. Les applications s'affichent dans Google Play for Work.	Google Play for Work informe les utilisateurs des mises à jour.	Les applications sont supprimées automatiquement du terminal.	Le profil professionnel et les applications professionnelles attribuées sont supprimés du terminal.

Activation des terminaux Android

Lorsque vous ou un utilisateur activez un terminal Android avec BlackBerry UEM, vous l'associez le terminal BlackBerry UEM pour pouvoir gérer les terminaux et l'accès des utilisateurs aux données professionnelles de leurs terminaux.

Types d'activation : terminaux Android

Pour les terminaux Android, vous pouvez sélectionner plusieurs types d'activation et les classer pour vous assurer que BlackBerry UEM attribue le type d'activation le plus approprié à ces terminaux. Par exemple, si vous classez « Travail et Personnel - Confidentialité des données de l'utilisateur (Android Enterprise) » en premier et « Contrôles MDM » en deuxième, les terminaux prenant en charge Android Enterprise reçoivent le premier type d'activation.

Les types d'activation Android sont organisés dans les tableaux suivants :

- Terminaux Android Enterprise
- Terminaux Android sans profil professionnel
- Terminaux Samsung KNOX Workspace

Terminaux Android Enterprise

Les types d'activation suivants s'appliquent uniquement aux terminaux Android Enterprise.

Type d'activation	Description
Travail et Personnel - Confidentialité des données de l'utilisateur (Android Enterprise avec profil professionnel)	Ce type d'activation préserve la confidentialité des données personnelles, mais vous permet de gérer les données professionnelles à l'aide de commandes et de règles de stratégie informatique. Ce type d'activation crée un profil professionnel sur le terminal qui sépare les données professionnelles des données personnelles. Les données professionnelles et personnelles sont protégées à l'aide du cryptage et de l'authentification par mot de passe. Pour permettre la gestion de l'application Google Play pour les terminaux Android Enterprise, sélectionnez **Ajouter Google Play à l'espace Travail**. Ce paramètre est activé par défaut. Si le terminal n'a pas accès à Google Play, vous devez désélectionner ce paramètre et vous devez utiliser l'application BlackBerry UEM Enroll depuis un terminal secondaire pendant le processus d'activation. Pour activer la prise en charge de BlackBerry Secure Connect Plus et de Knox Platform for Enterprise, vous devez sélectionner l'option **Lors de l'activation de terminaux Android Enterprise, activez une fonctionnalité UEM Premium telle que BlackBerry Secure Connect Plus**. Les utilisateurs ne sont pas tenus d'octroyer des autorisations d'administrateur à BlackBerry UEM Client.

Type d'activation	Description
Travail et Personnel - Contrôle total (terminal Android Enterprise entièrement géré avec profil professionnel)	Ce type d'activation vous permet de gérer le terminal dans son ensemble à l'aide de commandes et de règles de stratégie informatique. Ce type d'activation crée un profil professionnel sur le terminal qui sépare les données professionnelles des données personnelles. Les données de l'espace Travail sont protégées à l'aide du cryptage et d'une méthode d'authentification de type mot de passe, PIN, schéma ou empreinte digitale. Ce type d'activation prend en charge la consignation de l'activité du terminal (SMS, MMS et appels téléphoniques) dans les fichiers journaux BlackBerry UEM. Pour permettre la gestion de l'application Google Play pour les terminaux Android Enterprise, sélectionnez **Ajouter Google Play à l'espace Travail**. Ce paramètre est activé par défaut. Si le terminal n'a pas accès à Google Play, vous devez désélectionner ce paramètre et vous devez utiliser l'application BlackBerry UEM Enroll depuis un terminal secondaire pendant le processus d'activation. Pour activer la prise en charge de BlackBerry Secure Connect Plus et de Knox Platform for Enterprise, vous devez sélectionner l'option **Lors de l'activation de terminaux Android Enterprise, activez une fonctionnalité UEM Premium telle que BlackBerry Secure Connect Plus**. Lors de l'activation, les utilisateurs doivent octroyer les autorisations d'administrateur à BlackBerry UEM Client. Ce type d'activation est uniquement pris en charge pour Android 8.0 et versions ultérieures.
Espace Travail uniquement (tout terminal Android Enterprise entièrement géré)	Ce type d'activation vous permet de gérer le terminal dans son ensemble à l'aide de commandes et de règles de stratégie informatique. Ce type d'activation requiert que l'utilisateur restaure les réglages d'usine du terminal avant de procéder à l'activation. Le processus d'activation installe un profil de travail et aucun profil personnel. L'utilisateur doit créer un mot de passe pour accéder au terminal. Toutes les données du terminal sont protégées à l'aide du cryptage et d'une méthode d'authentification de type mot de passe. Pour permettre la gestion de l'application Google Play pour les terminaux Android Enterprise, sélectionnez **Ajouter Google Play à l'espace Travail**. Ce paramètre est activé par défaut. Si le terminal n'a pas accès à Google Play, vous devez désélectionner ce paramètre et vous devez utiliser l'application BlackBerry UEM Enroll depuis un terminal secondaire pendant le processus d'activation. Lors de l'activation, le terminal installe automatiquement BlackBerry UEM Client et lui accorde des autorisations d'administrateur. Les utilisateurs ne peuvent pas révoquer les autorisations d'administrateur ni désinstaller l'application. Pour activer la prise en charge de BlackBerry Secure Connect Plus et de Knox Platform for Enterprise, vous devez sélectionner l'option **Lors de l'activation de terminaux Android Enterprise, activez une fonctionnalité UEM Premium telle que BlackBerry Secure Connect Plus**.

Terminaux Android sans profil professionnel

Les types d'activation suivants s'appliquent à tous les terminaux Android.

Type d'activation	Description
Contrôles MDM	Ce type d'activation vous permet de gérer le terminal à l'aide de commandes et de règles de stratégie informatique. Un espace Travail distinct n'est pas créé sur le terminal, et il n'existe aucune sécurité ajoutée pour les données professionnelles. Si le terminal prend en charge KNOX MDM, ce type d'activation s'applique aux règles de stratégie informatique KNOX MDM. Si vous ne voulez pas appliquer les règles de stratégie KNOX MDM, désactivez la case **Activer Samsung KNOX sur les terminaux Samsung pour lesquels a été attribué le type d'activation Commandes MDM**. Lors de l'activation, les utilisateurs doivent octroyer les autorisations d'administrateur à BlackBerry UEM Client. **Remarque :** Ce type d'activation est uniquement pris en charge par Android 9.x et versions antérieures et sera obsolète pour les terminaux Android dans une prochaine version. Pour plus d'informations, rendez-vous sur le site Web https://support.blackberry.com/community pour lire l'article 48386.
Confidentialité de l'utilisateur	Vous pouvez utiliser le type d'activation Confidentialité de l'utilisateur pour fournir un contrôle de base des terminaux, y compris la gestion des applications professionnelles, tout en vous assurant que les données personnelles des utilisateurs restent privées. Avec ce type d'activation, aucun conteneur séparé n'est installé sur le terminal. Pour assurer la sécurité des données professionnelles, vous pouvez installer des applications BlackBerry Dynamics. Les terminaux activés avec Confidentialité de l'utilisateur peuvent utiliser des services tels que Trouver mon téléphone et Détection du statut débridé, mais les administrateurs ne peuvent pas contrôler les stratégies du terminal.
Inscription du terminal pour BlackBerry 2FA uniquement	Ce type d'activation prend en charge la solution BlackBerry 2FA pour les terminaux qui ne sont pas gérés par BlackBerry UEM. Ce type d'activation ne fournit aucune gestion ni aucun contrôle des terminaux, mais permet aux terminaux d'utiliser la fonctionnalité BlackBerry 2FA. Pour utiliser ce type d'activation, vous devez également attribuer le profil BlackBerry 2FA aux utilisateurs. Lorsqu'un terminal est activé, vous pouvez afficher des informations de terminal limitées dans la console de gestion, et vous pouvez désactiver le terminal à l'aide d'une commande. Ce type d'activation est pris en charge uniquement pour les utilisateurs Microsoft Active Directory. Pour plus d'informations, reportez-vous au contenu BlackBerry 2FA.

Terminaux Samsung KNOX Workspace

Les types d'activation suivants s'appliquent uniquement aux terminaux Samsung prenant en charge KNOX Workspace.

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 en utilisant les types d'activation Android Enterprise. Pour plus d'informations, rendez-vous sur le site Web https://support.blackberry.com/community pour lire l'article 54614.

Type d'activation	Description
Travail et Personnel - Confidentialité des données de l'utilisateur - (Samsung KNOX)	Ce type d'activation préserve la confidentialité des données personnelles, mais vous permet de gérer les données professionnelles à l'aide de commandes et de règles de stratégie informatique. Ce type d'activation ne prend pas en charge les règles de stratégie informatique KNOX MDM. Ce type d'activation crée un espace Travail séparé sur le terminal et l'utilisateur doit créer un mot de passe pour accéder à cet espace Travail. Les données de l'espace Travail sont protégées à l'aide du cryptage et d'une méthode d'authentification de type mot de passe, PIN, schéma ou empreinte digitale. L'utilisateur doit également créer un mot de passe de verrouillage de l'écran pour protéger l'ensemble du terminal et ne sera pas en mesure d'utiliser le mode de débogage USB. Lors de l'activation, les utilisateurs doivent octroyer les autorisations d'administrateur à BlackBerry UEM Client.
Travail et Personnel - Contrôle total (Samsung KNOX)	Ce type d'activation vous permet de gérer le terminal dans son ensemble à l'aide de commandes, de KNOX MDM et de règles de stratégie informatique KNOX Workspace. Ce type d'activation crée un espace Travail séparé sur le terminal et l'utilisateur doit créer un mot de passe pour accéder à cet espace Travail. Les données de l'espace Travail sont protégées à l'aide du cryptage et d'une méthode d'authentification de type mot de passe, PIN, schéma ou empreinte digitale. Ce type d'activation prend en charge la consignation de l'activité du terminal (SMS, MMS et appels téléphoniques) dans les fichiers journaux BlackBerry UEM. Lors de l'activation, les utilisateurs doivent octroyer les autorisations d'administrateur à BlackBerry UEM Client.
Espace Travail uniquement - (Samsung KNOX)	Ce type d'activation vous permet de gérer le terminal dans son ensemble à l'aide de commandes, de KNOX MDM et de règles de stratégie informatique KNOX Workspace. Ce type d'activation supprime l'espace Personnel et installe un espace Travail. L'utilisateur doit créer un mot de passe pour accéder au terminal. Toutes les données du terminal sont protégées à l'aide du cryptage et d'une méthode d'authentification de type mot de passe, PIN, schéma ou empreinte digitale. Ce type d'activation prend en charge la consignation de l'activité du terminal (SMS, MMS et appels téléphoniques) dans les fichiers journaux BlackBerry UEM. Lors de l'activation, les utilisateurs doivent octroyer les autorisations d'administrateur à BlackBerry UEM Client.

Activer un terminal Android Enterprise avec le type d'activation Travail et Personnel - Confidentialité des données de l'utilisateur

Envoyez ces instructions d'activation aux utilisateurs qui activent des terminaux avec le type d'activation Travail et Personnel - Confidentialité des données de l'utilisateur (Android Enterprise). Les étapes d'activation sont les mêmes, que vous utilisiez des comptes Google Play gérés ou que vous soyez connecté à un domaine Google.

Avant de commencer :

- Vous avez besoin des informations suivantes :

    - Mot de passe d'activation BlackBerry UEM
    - Votre adresse électronique professionnelle et votre mot de passe
- Informations éventuellement requises :
    - Adresse du serveur BlackBerry UEM
    - Mot de passe du compte Google

1. Sur le terminal, installez BlackBerry UEM Client. Vous pouvez télécharger UEM Client depuis Google Play.
2. Sur le terminal, sélectionnez **UEM Client**.
3. Lisez le contrat de licence. Sélectionnez **J'accepte**.
4. Sélectionnez **Autoriser** pour permettre à UEM Client de passer et de gérer les appels téléphoniques.
5. Saisissez votre adresse électronique professionnelle. Sélectionnez **Suivant**.
6. Si nécessaire, entrez l'adresse du serveur. Sélectionnez **Suivant**. Vous trouverez l'adresse du serveur dans l'e-mail d'activation que vous avez reçu ou dans BlackBerry UEM Self-Service.
7. Saisissez votre mot de passe d'activation. Sélectionnez **Activer mon terminal**.
8. Attendez la fin du transfert des profils et paramètres.
9. Sélectionnez **Accepter et continuer** pour créer un profil professionnel sur le terminal.
10. Si nécessaire, saisissez votre mot de passe Google. Sélectionnez **Suivant**.
11. Si vous y êtes invité, vous pouvez définir un mot de passe pour le terminal et sélectionner les options de notification.
12. Si vous y êtes invité, sélectionnez **OK** pour vous connecter à BlackBerry Secure Connect Plus et attendez que la connexion soit établie.

Activer un terminal Android Enterprise à l'aide d'un compte géré Google Play

Ces étapes s'appliquent aux terminaux dotés du type d'activation Espace Travail uniquement (Android Enterprise) ou Travail et Personnel - Contrôle total (Android Enterprise) . Si les utilisateurs activent des terminaux Travail et Personnel - Confidentialité des données de l'utilisateur, envoyez-leur des instructions pour Activer un terminal Android Enterprise avec le type d'activation Travail et Personnel - Confidentialité des données de l'utilisateur.

Envoyez les instructions d'activation suivantes à l'utilisateur du terminal.

Avant de commencer : Vérifiez que les informations suivantes vous ont été transmises par e-mail par votre administrateur :

- Nom d'utilisateur d'activation
- Mot de passe d'activation BlackBerry UEM

1. Si l'écran d'accueil du programme d'installation n'apparait pas, réinitialisez les paramètres par défaut du terminal.
2. Lors de la configuration du terminal, sur l'écran **Ajouter votre compte**, saisissez afw#blackberry.
3. Sur l'appareil, sélectionnez **Installer** pour installer BlackBerry UEM Client.
4. Lisez le contrat de licence. Sélectionnez **J'accepte**.
5. Sélectionnez **Autoriser** pour permettre à UEM Client de passer et de gérer les appels téléphoniques.
6. Saisissez votre adresse électronique professionnelle. Sélectionnez **Suivant**.
7. Si nécessaire, entrez l'adresse du serveur. Sélectionnez **Suivant**. Vous trouverez l'adresse du serveur dans l'e-mail d'activation que vous avez reçu ou dans BlackBerry UEM Self-Service.

8. Saisissez votre mot de passe d'activation. Sélectionnez **Activer mon terminal**.
9. Attendez la fin du transfert des profils et paramètres.
10. Sur l'écran **Configurer votre terminal**, sélectionnez **Accepter et continuer** et patientez pendant la configuration du profil professionnel.
11. Sur l'écran **Déverrouiller la sélection**, sélectionnez une méthode de déverrouillage.
12. Sur l'écran **Démarrage sécurisé**, sélectionnez **Oui** pour demander un mot de passe lorsque le terminal démarre.
13. Saisissez un mot de passe, puis saisissez-le à nouveau pour le confirmer. Sélectionnez **OK**.
14. Sélectionnez une option pour l'envoi des notifications. Sélectionnez **Terminé**.
15. Si vous y êtes invité, sélectionnez **OK** pour vous connecter à BlackBerry Secure Connect Plus et attendez que la connexion soit établie.

Activer un terminal Android Enterprise lorsque BlackBerry UEM est connecté à un domaine Google

Ces étapes s'appliquent aux terminaux dotés du type d'activation Espace Travail uniquement (Android Enterprise) ou Travail et Personnel - Contrôle total (Android Enterprise). Si les utilisateurs activent les terminaux Travail et Personnel - Confidentialité des données de l'utilisateur, envoyez-leur les instructions à Activer un terminal Android Enterprise avec le type d'activation Travail et Personnel - Confidentialité des données de l'utilisateur.

Envoyez les instructions d'activation suivantes à l'utilisateur du terminal.

Avant de commencer : Vérifiez que les informations suivantes vous ont été transmises par e-mail par votre administrateur :

- Mot de passe d'activation BlackBerry UEM
- Votre adresse électronique professionnelle et votre mot de passe
- Adresse du serveur BlackBerry UEM (celle-ci ne vous sera peut-être pas nécessaire)

1. Si l'écran d'accueil du programme d'installation n'apparait pas, réinitialisez les paramètres par défaut du terminal.
2. Pendant la configuration du terminal, dans l'écran **Ajouter votre compte**, saisissez votre adresse e-mail professionnelle et votre mot de passe.
3. Si vous êtes invité, cryptez le terminal.
4. Sur le terminal, sélectionnez **Installer** pour installer BlackBerry UEM Client.
5. Lisez le contrat de licence. Sélectionnez **J'accepte**.
6. Sélectionnez **Autoriser** pour permettre à UEM Client de passer et de gérer des appels téléphoniques.
7. Saisissez votre adresse électronique professionnelle. Appuyez sur **Suivant**.
8. Si nécessaire, entrez l'adresse du serveur. Appuyez sur **Suivant**. Vous trouverez l'adresse du serveur dans l'e-mail d'activation que vous avez reçu ou dans BlackBerry UEM Self-Service.
9. Saisissez votre mot de passe d'activation. Sélectionnez **Activer mon terminal**.
10. Attendez la fin du transfert des profils et paramètres.
11. Sur l'écran **Configurer votre terminal**, appuyez sur **Accepter et continuer** et patientez pendant la configuration du profil professionnel.
12. Dans l'écran **Déverrouiller la sélection**, sélectionnez une méthode de déverrouillage.
13. Sur l'écran **Démarrage sécurisé**, sélectionnez **Oui** pour demander un mot de passe lorsque le terminal démarre.
14. Saisissez un mot de passe, puis saisissez-le à nouveau pour le confirmer. Sélectionnez **OK**.

15. Sélectionnez une option pour l'envoi des notifications. Sélectionnez **Terminé**.
16. Si vous y êtes invité, sélectionnez **OK** pour vous connecter à BlackBerry Secure Connect Plus et attendez que la connexion soit établie.

Activer un terminal Android Enterprise sans compte Google Play

Ces étapes s'appliquent aux terminaux qui n'ont pas accès à Google Play. Les terminaux peuvent se voir attribuer le type d'activation Espace Travail uniquement (Android Enterprise), Travail et Personnel - Contrôle total (Android Enterprise) ou Travail et Personnel - Confidentialité des données de l'utilisateur (Android Enterprise).

Un terminal secondaire sur lequel l'application BlackBerry UEM Enroll est installée est nécessaire. Le même terminal peut être utilisé pour activer un nombre illimité de terminaux avec UEM.

Envoyez les instructions d'activation suivantes à l'utilisateur du terminal.

Avant de commencer :

- Vérifiez que les informations suivantes vous ont été transmises par e-mail par votre administrateur :
  - Nom d'utilisateur d'activation
  - Mot de passe d'activation BlackBerry UEM
- Vous devez disposer d'un terminal secondaire sur lequel l'application d'inscription BlackBerry UEM est installée. Pour télécharger et installer l'application sur un terminal secondaire, rendez-vous sur support.blackberry.com/community pour lire l'article 42607.

1. Sur le terminal que vous souhaitez activer, si l'écran d'accueil du programme d'installation ne s'affiche pas, réinitialisez les paramètres par défaut du terminal.
2. Sur le terminal secondaire, ouvrez l'application BlackBerry UEM Enroll. Assurez-vous que la fonction NFC est activée sur le terminal.
3. Appuyez sur **Activer le terminal**.
4. Appuyez conjointement sur l'arrière des deux terminaux.
5. Sur le terminal que vous souhaitez activer, suivez les instructions à l'écran pour télécharger et installer BlackBerry UEM Client.
6. Lisez le contrat de licence. Sélectionnez **J'accepte**.
7. Appuyez sur **Autoriser** pour permettre à UEM Client de passer et de gérer des appels téléphoniques.
8. Saisissez votre adresse électronique professionnelle. Appuyez sur **Suivant**.
9. Si nécessaire, entrez l'adresse du serveur. Appuyez sur **Suivant**. Vous trouverez l'adresse du serveur dans l'e-mail d'activation que vous avez reçu ou dans BlackBerry UEM Self-Service.
10. Saisissez votre mot de passe d'activation. Appuyez sur **Activer mon terminal**.
11. Attendez la fin du transfert des profils et paramètres.
12. Sur l'écran **Configurer votre terminal**, appuyez sur **Accepter et continuer** et attendez pendant la configuration du profil professionnel.
13. Dans l'écran **Déverrouiller la sélection**, sélectionnez une méthode de déverrouillage.
14. Sur l'écran **Démarrage sécurisé**, sélectionnez **Oui** pour demander un mot de passe lorsque le terminal démarre.
15. Saisissez un mot de passe, puis saisissez-le à nouveau pour le confirmer. Sélectionnez **OK**.
16. Sélectionnez une option pour l'envoi des notifications. Sélectionnez **Terminé**.
17. Si vous y êtes invité, sélectionnez **OK** pour vous connecter à BlackBerry Secure Connect Plus et attendez que la connexion soit établie.

18. Si nécessaire, ouvrez l'application de messagerie que votre organisation souhaite que vous utilisiez (BlackBerry Hub, par exemple) et suivez les instructions pour configurer la messagerie électronique sur votre téléphone.

Activer un terminal Android avec le type d'activation Contrôles MDM

Remarque : Ces étapes ne s'appliquent qu'aux terminaux auxquels le type d'activation Contrôles MDM a été attribué. Ce type d'activation sera obsolète dans une future version. Pour plus d'informations, rendez-vous sur le site Web https://support.blackberry.com/community pour lire l'article 48386.

Envoyez les instructions d'activation suivantes à l'utilisateur du terminal.

1. Sur le terminal, installez BlackBerry UEM Client. Vous pouvez télécharger BlackBerry UEM Client depuis Google Play.
2. Sur le terminal, sélectionnez **UEM Client**.
3. Lisez le contrat de licence. Sélectionnez **J'accepte**.
4. Saisissez votre adresse électronique professionnelle. Sélectionnez **Suivant**.
5. Si nécessaire, entrez l'adresse du serveur. Sélectionnez **Suivant**. Vous trouverez l'adresse du serveur dans l'e-mail d'activation que vous avez reçu ou dans BlackBerry UEM Self-Service.
6. Saisissez votre mot de passe d'activation. Sélectionnez **Activer mon terminal**.
7. Sélectionnez **Suivant**.
8. Sélectionnez **Activer**.

À la fin : Pour vérifier que le processus d'activation a réussi, effectuez l'une des actions suivantes :

- Sur le terminal, ouvrez BlackBerry UEM Client. Sélectionnez **À propos de**. Dans la section **Terminal activé**, assurez-vous de la présence des informations sur le terminal et de l'heure et de la date d'activation.
- Dans BlackBerry UEM Self-Service, vérifiez que votre terminal est répertorié en tant que terminal activé. Le statut peut prendre jusqu'à deux minutes pour se mettre à jour après que vous avez activé le terminal.

Activer un terminal à l'aide de QR Code

L'activation QR Code est prise en charge sur les terminaux iOS et Android.

Pour activer un terminal à l'aide de QR Code, envoyez les instructions suivantes à l'utilisateur du terminal.

Avant de commencer : Vous avez besoin du QR Code. Vous le trouverez dans l'e-mail d'activation que votre administrateur vous a envoyé ou vous pouvez en générer un dans BlackBerry UEM Self-Service.

1. Sur le terminal, installez l'application BlackBerry UEM Client. Pour les terminaux iOS, téléchargez l'application depuis App Store. Pour les terminaux Android, téléchargez l'application depuis Google Play.
2. Sur le terminal, sélectionnez **UEM Client**.
3. Lisez l'accord de licence et sélectionnez **J'accepte**.
4. Scannez le QR Code que vous avez reçu dans l'e-mail d'activation ou généré dans BlackBerry UEM Self-Service.
5. Si vous êtes invité à saisir le mot de passe de votre compte de messagerie ou le mot de passe de votre terminal, suivez les instructions à l'écran.

À la fin : Pour vérifier que le processus d'activation a abouti, effectuez l'une des opérations suivantes :

- Sur le terminal, ouvrez l'application BlackBerry UEM Client et sélectionnez **À propos de**. Dans les sections Terminal activé et État de conformité, assurez-vous de la présence des informations sur le terminal et de l'heure et de la date d'activation.

- Dans BlackBerry UEM Self-Service, vérifiez que votre terminal est répertorié en tant que terminal activé. Le statut peut prendre jusqu'à deux minutes pour se mettre à jour après que vous avez activé le terminal.

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 secrets commerciaux et/ou des informations confidentielles et propriétaires 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 D'UN LOGICIEL, MATÉRIEL, 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 LA GARANTIE LIMITÉE APPLICABLE, L'ACCORD DE LICENCE DU LOGICIEL BLACKBERRY ET/OU 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 L'UTILISATION OU NON-UTILISATION DES LOGICIELS, DU MATÉRIEL, DES SERVICES OU DES PRODUITS ET SERVICES TIERS MENTIONNÉS DANS LES PRÉSENTES, ET NOTAMMENT 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, DEMANDE OU ACTION ENTREPRISE PAR VOUS, NOTAMMENT POUR RUPTURE DE CONTRAT, NÉGLIGENCE, FAUTE, RESPONSABILITÉ STRICTE OU TOUT 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 AYANT-DROIT, REPRÉSENTANTS, AGENTS, FOURNISSEURS (NOTAMMENT LES FOURNISSEURS DE SERVICES DE TEMPS DE COMMUNICATION), 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, DISTRIBUTEURS, FOURNISSEURS, SOUS-TRAITANTS INDÉPENDANTS 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 sans fil prend en charge toutes les fonctionnalités. Certains fournisseurs de services sans fil 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 ni garanties expresses ou tacites d'aucune sorte par BlackBerry, et BlackBerry n'engage aucune responsabilité sur les Produits et Services tiers. 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
2 200 University Avenue East
Waterloo, Ontario
Canada N2K 0A7

BlackBerry UK Limited
200 Bath Road

Slough, Berkshire SL1 3XE
Royaume-Uni

Publié au Canada