BlackBerry UEM

Activation des terminaux

12.20

Contents

Activation de terminaux avec BlackBerry UEM

Lorsque vous ou un utilisateur activez un terminal, celui-ci est associé à BlackBerry UEM. Cela vous permet de gérer et d'attribuer des configurations aux terminaux, et de donner aux utilisateurs l'accès aux données professionnelles sur leurs terminaux.

Lorsqu'un terminal est activé, vous pouvez envoyer des stratégies informatiques et des profils pour contrôler et configurer les fonctionnalités et gérer la sécurité des données professionnelles. Vous pouvez également attribuer à l'utilisateur des applications à installer. Selon le niveau de contrôle lié au type d'activation sélectionné, vous pouvez également protéger le terminal en limitant l'accès à certaines données, en définissant à distance des mots de passe, en verrouillant le terminal ou en supprimant des données.

Vous pouvez attribuer des types d'activation pour répondre aux exigences des terminaux appartenant à votre organisation et à celles des terminaux appartenant aux utilisateurs. Différents types d'activation vous offrent différents degrés de contrôle des données professionnelles et personnelles sur les terminaux, allant du contrôle total de toutes les données au contrôle spécifique des données professionnelles uniquement.

Pour configurer UEM afin de permettre aux utilisateurs d'activer les terminaux, procédez comme suit :

Étape	Action
1	Pour chaque terminal que vous souhaitez activer, vérifiez qu'une licence UEM est disponible. Pour les terminaux iOS, iPadOS et Android, vérifiez que la dernière version de BlackBerry UEM Client est installée sur le terminal à partir de la boutique d'applications appropriée.
2	Configuration des paramètres d'activation par défaut.
3	Passez en revue les informations pertinentes pour votre environnement UEM et les utilisateurs de votre terminal : • Prise en charge des activations Android Enterprise et Android Management • Prise en charge des activations Windows 10 • Prise en charge de l'inscription des utilisateurs d'Apple pour les terminaux iOS et iPadOS • Prise en charge de Samsung Knox DualDAR • Configurer la prise en charge de l'inscription sans intervention Android • Activation de plusieurs terminaux à l'aide de Knox Mobile Enrollment • Activation de terminaux iOS inscrits dans DEP • Activer des terminaux iOS à l'aide de Apple Configurator 2
4	Mettez à jour le modèle d'e-mail d'activation.
5	Créez un profil d'activation et attribuez-le à des comptes d'utilisateur ou à des groupes d'utilisateurs.
6	Envoyer un e-mail d'activation à plusieurs utilisateurs, Envoyez un e-mail d'activation à un utilisateur spécifique ou Autorisez les utilisateurs à définir leur propre mot de passe d'activation dans UEM Self-Service.

Étape	Action
7	Envoyez les instructions d'activation aux utilisateurs : • Activation des terminaux Android • Activation des terminaux iOS • Activation d'un terminal macOS ou Apple TV avec BlackBerry UEM Self-Service • Activation d'une tablette ou d'un ordinateur Windows 10

Types d'activation : terminaux iOS

Type d'activation	Description
Contrôles MDM	Ce type d'activation fournit une gestion de base des terminaux à l'aide des commandes de terminaux mises à disposition par iOS et iPadOS. Il n'existe pas d'espace Travail séparé installé sur le terminal, et aucune sécurité ajoutée pour les données professionnelles. Vous pouvez contrôler le terminal à l'aide de commandes et de stratégies informatiques. Lors de l'activation, les utilisateurs disposant d'un terminal doivent installer un profil de gestion des terminaux mobiles. Pour spécifier si BlackBerry UEM peut limiter l'activation par ID de terminal, sélectionnez Autoriser uniquement les ID de terminal approuvés.

Type d'activation	Description
Confidentialité de l'utilisateur	Ce type d'activation permet un contrôle de base des terminaux tout en garantissant la confidentialité des données personnelles des utilisateurs. Aucun conteneur distinct n'est installé sur le terminal, et aucune sécurité supplémentaire n'est fournie pour les données professionnelles. Les terminaux peuvent utiliser des services tels que Trouver mon téléphone et Détection du statut débridé, mais les administrateurs ne peuvent pas contrôler les stratégies des terminaux. **Remarque :** Pour le modèle de licence SIM, vous devez sélectionner l'option « Autoriser l'accès à la carte SIM et aux informations matérielles du terminal pour activer le modèle de licence SIM » dans le profil d'activation. Les utilisateurs doivent installer un profil MDM qui peut uniquement accéder à la carte SIM et aux informations matérielles du terminal qui sont requises pour déterminer si une licence SIM appropriée est disponible (par exemple, ICCID et IMEI). Ce type d'activation n'est pris en charge que par les terminaux Apple TV. Lorsque vous autorisez les activations Confidentialité de l'utilisateur, vous sélectionnez les profils que vous souhaitez gérer sur le terminal en fonction des besoins de votre organisation. Vous pouvez choisir l'une des options suivantes : • Autoriser l'accès à la carte SIM et aux informations matérielles du terminal pour activer les licences SIM : cette option spécifie si UEM peut accéder aux informations matérielles de la carte SIM et du terminal, telles que les numéros ICCID et IMEI, pour vérifier si une licence SIM appropriée est disponible. • Autoriser la gestion des applications : cette option vous permet de déterminer si vous souhaitez installer ou supprimer des applications professionnelles sur le terminal, et afficher la liste des applications professionnelles installées sur l'écran Détails utilisateur. Vous pouvez également spécifier si vous souhaitez autoriser les raccourcis d'application. • Autoriser la gestion des stratégies informatiques : cette option vous permet de définir si vous souhaitez appliquer un ensemble limité de règles de stratégie informatiques au terminal (stratégies de mot de passe, autoriser les captures d'écran, autoriser les documents issus de sources gérées dans les destinations non gérées et autoriser les documents issus de sources non gérées dans les destinations gérées). • Autoriser la gestion des e-mails : cette option vous permet de définir si les paramètres de profil de messagerie qui sont affectés à l'utilisateur doivent être appliqués au terminal. • Autoriser la gestion du profil Wi-Fi : cette option vous permet de déterminer si les paramètres de profil Wi-Fi qui sont attribués à l'utilisateur doivent être appliqués au terminal. • Autoriser la gestion des VPN : cette option vous permet de définir si les paramètres de profil VPN qui sont affectés à l'utilisateur doivent être appliqués au terminal.

Type d'activation	Description
Confidentialité de l'utilisateur - Inscription de l'utilisateur	Ce type d'activation peut être utilisé pour les terminaux iOS et iPadOS afin de veiller à ce que les données utilisateur restent privées et séparées des données professionnelles. Un espace Travail distinct est installé sur le terminal pour les applications professionnelles et les applications natives Notes, iCloud Drive, Mail (pièces jointes et corps d'e-mail complets), Calendrier (pièces jointes) et iCloud Keychain. Ce type d'activation permet la gestion des applications, la gestion des stratégies informatiques, les profils de messagerie, les profils Wi-Fi et le VPN par application. Les administrateurs peuvent gérer les données professionnelles (par exemple, supprimer des données professionnelles) sans affecter les données personnelles. Ce type d'activation est pris en charge sur les terminaux iPhone et iPad supervisés.
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 UEM. Ce type d'activation ne permet pas de gérer ou de contrôler les terminaux, mais il leur permet 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. Il n'est pas pris en charge par les terminaux Apple TV. Pour plus d'informations, reportez-vous au contenu relatif à BlackBerry 2FA.

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 (Samsung Knox) en premier et Travail et Personnel - Confidentialité des données de l'utilisateur (Android Enterprise) en second, les terminaux qui prennent en charge Samsung Knox Workspace reçoivent le premier type d'activation et les terminaux qui ne prennent pas en charge Samsung Knox Workspace reçoivent le second.

Terminaux Android Management

Avant d'activer des terminaux avec des types d'activation Android Management, consultez Considérations relatives aux types d'activation Android Management.

Type d'activation	Description
Travail et Personnel - Confidentialité des données de l'utilisateur (Android Management 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. Un profil professionnel est créé sur le terminal qui sépare les données professionnelles et personnelles. Les données professionnelles et personnelles sont protégées à l'aide du cryptage et de l'authentification par mot de passe.
Travail et Personnel - Contrôle total (terminal Android Management entièrement géré avec un 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. Un profil professionnel est créé sur le terminal qui sépare les données professionnelles et 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 journalisation de l'activité du terminal (SMS, MMS et appels téléphoniques) dans les fichiers journaux UEM. Après l'activation, les terminaux Travail et Personnel - Contrôle total ne disposent que d'un ensemble limité d'applications standard préinstallées, telles qu'Appareil photo, Téléphone et Paramètres, dans l'espace Personnel. La liste des applications préinstallées conservées dépend du fournisseur du terminal et de la version du système d'exploitation. Pour ce type d'activation, vous devez réinitialiser le terminal aux paramètres d'usine par défaut avant de l'activer. Si BlackBerry UEM Client est supprimé ou si le profil professionnel est supprimé du terminal, il est automatiquement réinitialisé aux paramètres d'usine par défaut.
Espace Travail uniquement (terminal Android Management 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. Lors de l'activation, le terminal installe automatiquement UEM Client et lui accorde des autorisations d'administrateur. Les utilisateurs ne peuvent pas révoquer les autorisations d'administrateur ni désinstaller l'application. Après l'activation, les terminaux Espace Travail uniquement disposent uniquement d'un ensemble limité d'applications standard préinstallées, telles qu'Appareil photo, Téléphone et Paramètres, ainsi que les applications que vous avez vous-même attribuées avec une disposition requise. La liste des applications préinstallées conservées dépend du fournisseur du terminal et de la version du système d'exploitation. Pour ce type d'activation, vous devez réinitialiser le terminal aux paramètres d'usine par défaut avant de l'activer. Si UEM Client est supprimé ou si le profil professionnel est supprimé du terminal, il est automatiquement réinitialisé aux paramètres d'usine par défaut.

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. Un profil professionnel est créé sur le terminal qui sépare les données professionnelles et 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 des applications Google Play pour les terminaux Android Enterprise, sélectionnez Ajouter Google Play à l'espace Travail dans le profil d'activation (activé par défaut). Si le terminal n'a pas accès à Google Play, l'utilisateur doit télécharger la dernière version de UEM Client à partir d'une autre source. Pour télécharger le fichier .apk UEM Client le plus récent, consultez l'article KB 42607. 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 dans le profil d'activation. Les utilisateurs ne sont pas tenus d'octroyer des autorisations d'administrateur à UEM Client.

Type d'activation	Description
Travail et Personnel - Contrôle total (terminal Android Enterprise entièrement géré avec un 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. Un profil professionnel est créé sur le terminal qui sépare les données professionnelles et 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 journalisation de l'activité du terminal (SMS, MMS et appels téléphoniques) dans les fichiers journaux UEM. Pour permettre la gestion des applications Google Play pour les terminaux Android Enterprise, sélectionnez Ajouter Google Play à l'espace Travail dans le profil d'activation (activé par défaut). Après l'activation, les terminaux Travail et Personnel - Contrôle total ne disposent que d'un ensemble limité d'applications standard préinstallées, telles qu'Appareil photo, Téléphone et Paramètres, dans l'espace Personnel. La liste des applications préinstallées conservées dépend du fournisseur du terminal et de la version du système d'exploitation. 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 dans le profil d'activation. Pour spécifier si UEM peut limiter l'activation par ID de terminal, sélectionnez Autoriser uniquement les ID de terminal approuvés dans le profil d'activation. Pour ce type d'activation, vous devez réinitialiser le terminal aux paramètres d'usine par défaut avant de l'activer. Si UEM Client est supprimé ou si le profil professionnel est supprimé du terminal, il est automatiquement réinitialisé aux paramètres d'usine par défaut. Lors de l'activation, les utilisateurs doivent octroyer les autorisations d'administrateur à UEM Client.

Type d'activation	Description
Espace Travail uniquement (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. Il 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 des applications Google Play pour les terminaux Android Enterprise, sélectionnez Ajouter Google Play à l'espace Travail dans le profil d'activation (activé par défaut). Si le terminal n'a pas accès à Google Play, l'utilisateur peut télécharger UEM Client à l'aide d'un fichier .apk de l'application. Vous pouvez configurer et inclure un QR Code qui contient l'emplacement du fichier source UEM Client dans l'e-mail d'activation que vous envoyez aux utilisateurs. Lorsqu'un utilisateur scanne le code QR Code, UEM Client est automatiquement téléchargé. Pour configurer et inclure un QR Code dans l'e-mail d'activation, vous devez cocher la case Autoriser les QR Codes pour l'activation des terminaux sur la page Paramètres d'activation par défaut (Paramètres > Paramètres généraux > Paramètres d'activation par défaut). Vous devez également cocher la case Autoriser le QR Code à contenir l'emplacement du fichier source de l'application UEM Client et spécifier l'emplacement du fichier source de l'application UEM Client. Pour obtenir le fichier .apk de la dernière version de UEM Client, reportez-vous à l'article KB 42607. Lors de l'activation, le terminal installe automatiquement UEM Client et lui accorde des autorisations d'administrateur. Les utilisateurs ne peuvent pas révoquer les autorisations d'administrateur ni désinstaller l'application. Après l'activation, les terminaux Espace Travail uniquement disposent uniquement d'un ensemble limité d'applications standard préinstallées, telles qu'Appareil photo, Téléphone et Paramètres, ainsi que les applications que vous avez vous-même attribuées avec une disposition requise. La liste des applications préinstallées conservées dépend du fournisseur du terminal et de la version du système d'exploitation. 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 dans le profil d'activation. Pour spécifier si UEM peut limiter l'activation par ID de terminal, sélectionnez Autoriser uniquement les ID de terminal approuvés dans le profil d'activation. Pour ce type d'activation, vous devez réinitialiser le terminal aux paramètres d'usine par défaut avant de l'activer. Si UEM Client est supprimé ou si le profil professionnel est supprimé du terminal, il est automatiquement réinitialisé aux paramètres d'usine par défaut.

Terminaux Android sans profil professionnel

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

Type d'activation	Description
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. Un conteneur distinct n'est pas créé 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. Vous pouvez également utiliser le type d'activation Confidentialité de l'utilisateur pour activer les terminaux Chrome OS afin d'installer et de gérer des applications Android BlackBerry Dynamics.
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 UEM. Ce type d'activation ne permet pas de gérer ou de contrôler les terminaux, mais il leur permet 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

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, consultez l'article KB 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. Un espace Travail distinct est créé sur le terminal et l'utilisateur doit définir un mot de passe pour accéder à l'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 UEM Client.

Type d'activation	Description
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 règles de stratégie informatique Knox MDM et Knox Workspace. Un espace Travail distinct est créé sur le terminal et l'utilisateur doit définir un mot de passe pour accéder à l'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. Lors de l'activation, les utilisateurs doivent octroyer les autorisations d'administrateur à UEM Client.

Types d'activation : terminaux macOS

Type d'activation	Description
Contrôles MDM	Ce type d'activation fournit une gestion de base des terminaux à l'aide des commandes de terminaux mises à disposition par macOS. Lorsqu'un utilisateur active un terminal macOS, le terminal et l'utilisateur sont configurés en tant qu'entités distinctes sur BlackBerry UEM. Des canaux de communication séparés sont établis entre UEM et le terminal et UEM et le compte d'utilisateur, ce qui vous permet de gérer l'appareil et l'utilisateur séparément. Certains profils sont affectés à l'utilisateur uniquement (par exemple les profils de messagerie). Certains profils sont affectés au terminal uniquement (par exemple les profils de proxy). Certains profils vous permettent de choisir d'appliquer le profil au terminal ou à l'utilisateur (par exemple les profils Wi-Fi). Vous pouvez contrôler le terminal à l'aide de commandes et de stratégies informatiques. Les utilisateurs activent les terminaux macOS à l'aide de BlackBerry UEM Self-Service.

Types d'activation : terminaux Windows 10

Remarque : Les terminaux Windows 10 Mobile ne sont plus pris en charge par Microsoft et leur prise en charge est limitée sur UEM.

Type d'activation	Description
Contrôles MDM	Ce type d'activation fournit une gestion de base des terminaux à l'aide des commandes mises à disposition par les terminaux Windows 10. Il n'existe pas d'espace Travail séparé installé sur le terminal, et aucune sécurité ajoutée pour les données professionnelles. Vous pouvez contrôler le terminal à l'aide de commandes et de stratégies informatiques. Les utilisateurs Windows 10 activent les terminaux grâce à l'application d'accès de travail Windows 10.

Gérer les paramètres d'activation

Vous pouvez gérer la manière dont les utilisateurs activent les terminaux, notamment s'ils ont besoin d'un mot de passe d'activation ou s'ils peuvent scanner un QR Code, la durée de validité d'un mot de passe d'activation ou QR Code et si les utilisateurs peuvent activer plusieurs terminaux avec le même mot de passe ou QR Code.

Configuration des paramètres d'activation par défaut

1. Sur la barre de menus de la console de gestion, cliquez sur **Paramètres > Paramètres généraux > Paramètres d'activation par défaut**.
2. Dans la section **Paramètres d'activation de terminal par défaut**, spécifiez le mot de passe d'activation et les options QR Code.
3. Si vous souhaitez que BlackBerry UEM avertisse un utilisateur par e-mail chaque fois qu'un terminal est activé sur son compte, cochez la case **Envoyer une notification d'activation de terminal**.
4. Pour autoriser les utilisateurs à activer des applications BlackBerry Dynamics avec un QR Code, dans la section **Contrôle des applications BlackBerry Dynamics par défaut**, cochez la case **Utiliser les QR Codes pour déverrouiller les applications BlackBerry Dynamics**. Pour plus d'informations, consultez Générer des clés d'accès, des mots de passe d'activation ou des QR Codes pour les applications BlackBerry Dynamics.
5. Pour simplifier la façon dont les utilisateurs activent leurs terminaux mobiles, dans la section **BlackBerry Infrastructure**, cochez la case **Activer l'inscription auprès de BlackBerry Infrastructure**. Si vous décochez cette case, les utilisateurs seront invités à indiquer l'adresse du serveur pour UEM lors de l'activation de leurs terminaux.
6. Pour importer ou exporter une liste d'ID de terminal approuvés, dans la section **Importer ou exporter des ID de terminal**, cliquez sur **Parcourir**. Accédez au fichier .csv qui contient la liste des ID de terminal approuvés et sélectionnez-le. Pour plus d'informations, reportez-vous à la section Importer ou exporter une liste d'ID de terminal approuvés.
7. Cliquez sur **Enregistrer**.

Définir un mot de passe d'activation et envoyer un e-mail d'activation

Vous pouvez définir un mot de passe d'activation et envoyer à un utilisateur un e-mail d'activation contenant des instructions pour activer un ou plusieurs terminaux. Dans les environnements sur site, l'e-mail est envoyé depuis l'adresse électronique que vous avez configurée dans les paramètres de serveur SMTP.

Avant de commencer : Créer un modèle d'e-mail d'activation.

1. Sur la barre de menus de la console de gestion, cliquez sur **Utilisateurs > Terminaux gérés**.
2. Recherchez et cliquez sur le nom d'un compte d'utilisateur.
3. Dans la section **Détails de l'activation**, cliquez sur **Définir le mot de passe d'activation**.
4. Dans la liste déroulante **Option d'activation**, effectuez l'une des opérations suivantes :
   - Si vous souhaitez que l'utilisateur active son terminal via le profil d'activation qui lui est actuellement attribué, sélectionnez **Activation du terminal par défaut**.
   - Si vous souhaitez associer un mot de passe d'activation à un profil d'activation spécifique, sélectionnez **Activation du terminal avec un profil d'activation spécifique**. Pour plus d'informations, reportez-vous à Permettre aux utilisateurs d'activer des terminaux utilisant des types d'activation différents.
5. Dans la liste déroulante **Mot de passe d'activation**, effectuez l'une des opérations suivantes :

- Si vous souhaitez que le mot de passe soit généré automatiquement, sélectionnez **Générer automatiquement le mot de passe d'activation du terminal et envoyer un e-mail contenant des instructions d'activation**. Lorsque vous sélectionnez cette option, vous devez choisir un modèle d'e-mail pour envoyer les informations à l'utilisateur.
- Si vous souhaitez définir un mot de passe d'activation pour l'utilisateur et (facultatif) envoyer un e-mail d'activation, sélectionnez **Définir le mot de passe d'activation du terminal** et saisissez un mot de passe.

6. Si vous le souhaitez, vous pouvez modifier la durée de validité du mot de passe d'activation.
7. Pour que le mot de passe d'activation ne s'applique qu'à une seule activation, sélectionnez **La période d'activation expire à l'issue de l'activation du premier terminal**.
8. Dans la liste déroulante **Modèle d'e-mail d'activation**, sélectionnez le modèle d'e-mail que vous souhaitez utiliser.
9. Cliquez sur **Submit**.

Envoyer un e-mail d'activation à plusieurs utilisateurs

Vous pouvez envoyer des e-mails d'activation à plusieurs utilisateurs à la fois. Lorsque vous envoyez un e-mail d'activation à plusieurs utilisateurs, le mot de passe d'activation est généré automatiquement. L'e-mail est envoyé depuis l'adresse électronique que vous avez configurée dans les paramètres de serveur SMTP.

Avant de commencer : Créer un modèle d'e-mail d'activation.

1. Sur la barre de menus de la console de gestion, cliquez sur **Utilisateurs > Terminaux gérés**.
2. Cochez la case en regard de chaque utilisateur auquel vous souhaitez envoyer un e-mail d'activation.
3. Cliquez sur .
4. Dans la liste déroulante **Option d'activation**, effectuez l'une des opérations suivantes :
   - Si vous souhaitez que les utilisateurs activent leurs terminaux via le profil d'activation qui leur est actuellement attribué, sélectionnez **Activation du terminal par défaut**.
   - Si vous souhaitez associer un mot de passe d'activation à un profil d'activation spécifique, sélectionnez **Activation du terminal avec un profil d'activation spécifique**. Pour plus d'informations sur l'association de mots de passe d'activation à des profils d'activation, reportez-vous à Permettre aux utilisateurs d'activer des terminaux utilisant des types d'activation différents.
5. Dans la liste déroulante **Mot de passe d'activation**, sélectionnez **Générer automatiquement le mot de passe d'activation du terminal et envoyer un e-mail contenant des instructions d'activation**.
6. Pour spécifier la durée de validité du mot de passe d'activation, modifiez l'expiration de la période d'activation.
7. Pour que le mot de passe d'activation ne s'applique qu'à une seule activation, sélectionnez **La période d'activation expire à l'issue de l'activation du premier terminal**.
8. Dans la liste déroulante **Modèle d'e-mail d'activation**, sélectionnez le modèle d'e-mail que vous souhaitez utiliser.
9. Cliquez sur **Envoyer**.

Autoriser les utilisateurs à définir des mots de passe d'activation BlackBerry UEM Self-Service

Vous pouvez autoriser les utilisateurs de terminaux iOS, Android et Windows à créer leurs propres mots de passe d'activation à l'aide de BlackBerry UEM Self-Service.

1. Dans la barre de menus de la console de gestion, cliquez sur **Paramètres > Self-Service > Paramètres Self-Service**.
2. Cochez la case **Autoriser les utilisateurs à activer des terminaux dans la console Self-Service** et procédez comme suit :
3. Spécifiez la durée pendant laquelle un utilisateur doit activer un terminal avant l'expiration du mot de passe d'activation.
4. Spécifiez le nombre minimum de caractères requis dans le mot de passe d'activation.
5. Dans la liste déroulante **Complexité minimale des mots de passe**, sélectionnez le niveau de complexité requis.
6. Pour envoyer automatiquement un e-mail d'activation aux utilisateurs lorsqu'ils créent un mot de passe d'activation, cochez la case **Envoyer un e-mail d'activation**. Dans la liste déroulante **Modèle d'e-mail d'activation**, sélectionnez un modèle d'e-mail.
7. Pour envoyer des messages d'activation personnalisés aux utilisateurs, cochez la case **Envoyer des messages d'activation personnalisés**. Sélectionnez un modèle de message pour chaque type de terminal dans la liste déroulante appropriée.
8. Pour envoyer des e-mails de notification de connexion aux utilisateurs chaque fois qu'ils se connectent à UEM Self-Service, cochez la case **Envoyer une notification de connexion Self-Service**.
9. Cliquez sur **Enregistrer**.

Permettre aux utilisateurs d'activer des terminaux utilisant des types d'activation différents

Vous pouvez créer différents mots de passe d'activation et les associer à des profils d'activation spécifiques pour permettre aux utilisateurs d'activer des terminaux aux types d'activation différents.

Par exemple, vous pouvez permettre aux utilisateurs d'activer des terminaux professionnels avec un type d'activation qui vous offre un contrôle total sur ces terminaux tout en les autorisant à activer leurs terminaux personnels en mode Confidentialité de l'utilisateur. En associant un mot de passe d'activation à un profil d'activation qui offre un contrôle total sur les terminaux et un deuxième mot de passe d'activation au profil d'activation Confidentialité de l'utilisateur, les utilisateurs pourront activer chaque terminal avec des résultats différents. Vous pouvez créer des modèles d'e-mail décrivant l'usage de chaque mot de passe.

Pour associer un mot de passe d'activation à un profil d'activation spécifique, lors de la création d'un compte d'utilisateur ou de l'envoi d'un e-mail d'activation, sélectionnez l'option Activation du terminal avec un profil d'activation spécifique.

Vous pouvez disposer de deux mots de passe d'activation associés à des profils d'activation spécifiques. Chaque mot de passe peut être utilisé pour activer plusieurs terminaux. Veuillez noter que pour les mots de passe d'activation associés à des profils d'activation spécifiques, l'option Nombre de terminaux qu'un utilisateur peut activer ne s'applique pas dans le profil d'activation.

Si vous supprimez un profil d'activation auquel est associé un mot de passe d'activation, ce dernier expire automatiquement. Si nécessaire, vous pouvez à tout moment faire expirer les mots de passe d'activation d'un utilisateur.

Dans BlackBerry UEM Self-Service, les utilisateurs ne peuvent pas créer de mots de passe d'activation associés à des profils d'activation spécifiques.

Cette option n'est pas prise en charge par les terminaux iOS qui sont inscrits dans DEP.

Forcer l‘expiration du mot de passe d‘activation

Vous pouvez forcer manuellement l‘expiration d‘un mot de passe d‘activation précédemment généré pour un utilisateur.

1. Sur la barre de menus de la console de gestion, cliquez sur **Utilisateurs > Terminaux gérés**.
2. Recherchez et cliquez sur le nom d‘un compte d‘utilisateur.
3. Dans la section **Détails d‘activation**, sous le mot de passe d‘activation que vous souhaitez faire expirer, cliquez sur **Expirer**.

Le mot de passe d‘activation expire immédiatement. Si vous forcez l‘expiration d‘un mot de passe d‘activation classique, la date et l‘heure auxquelles le mot de passe a expiré s‘affichent. Si vous forcez l‘expiration d‘un mot de passe d‘activation associé à un profil d‘activation spécifique, les détails relatifs au mot de passe d‘activation du terminal ne sont plus affichés.

Prise en charge des activations Android Enterprise et Android Management

La manière dont vous activez les terminaux Android Enterprise et Android Management des utilisateurs peut dépendre de plusieurs facteurs, notamment de la version du système d'exploitation Android du terminal et du niveau de contrôle que votre organisation souhaite exercer sur les terminaux des utilisateurs. Elle peut également dépendre du fait que votre organisation interagisse avec les services Google en utilisant des comptes Google Play gérés, des domaines Google Workspace ou des domaines Google Cloud, ou qu'elle n'utilise pas les services Google.

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

Si votre organisation n'a pas de domaine Google ou si vous ne souhaitez pas connecter BlackBerry UEM à votre domaine Google, vous pouvez activer les terminaux Android Enterprise et Android Management à l'aide de comptes Google Play gérés. Les comptes Google Play gérés vous permettent d'ajouter à Google Play des applications internes que les utilisateurs de terminaux Android Enterprise peuvent télécharger.

Pour utiliser des comptes Google Play gérés avec UEM, vous devez utiliser un compte Google ou Gmail afin de connecter UEM à Google. Aucune information personnelle identifiable concernant vos utilisateurs n'est envoyée à Google. Après avoir connecté UEM à Google, vous pouvez autoriser les utilisateurs à activer des terminaux Android Enterprise et Android Management et à télécharger des applications professionnelles à l'aide de Google Play. Pour plus d'informations sur la configuration d'UEM à des fins de prise en charge des terminaux Android Enterprise et Android Management, consultez Configuration de BlackBerry UEM pour la prise en charge des terminaux Android Enterprise et Configuration de BlackBerry UEM pour la prise en charge des terminaux Android Management.

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

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

Avant de commencer : Configurez BlackBerry UEM pour qu'il prenne en charge les terminaux Android Enterprise.

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

   Ce paramètre est obligatoire pour les terminaux auxquels seront attribués les types d'activation Espace Travail uniquement et Travail et Personnel - Contrôle total, et fortement recommandé pour les terminaux associés à 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. Dans 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 Google Workspace correspondant.
4. Dans UEM, attribuez un profil de messagerie et des applications de productivité à des utilisateurs, des groupes d'utilisateurs ou des groupes 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 qu'il prenne en charge les terminaux Android Enterprise. Lorsque vous configurez UEM pour qu'il se connecte à un domaine Google Cloud, vous devez choisir d'autoriser ou non 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.

1. Dans UEM, créez des comptes d'utilisateur associés à l'annuaire pour vos utilisateurs Android Enterprise.
2. Si vous choisissez de ne pas autoriser UEM à créer des comptes d'utilisateurs dans votre domaine Google Cloud, vous devez créer des comptes d'utilisateurs dans votre domaine Google Cloud et dans 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 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 UEM, attribuez un profil de messagerie et des applications de productivité à des utilisateurs, des groupes d'utilisateurs ou des groupes de terminaux.

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

Pour activer les terminaux qui n'ont pas accès à Google Play, les utilisateurs doivent télécharger la dernière version de BlackBerry UEM Client à partir d'une autre source. Les méthodes disponibles pour télécharger UEM Client dépendent de la version du système d'exploitation et du type d'activation :

- Pour les terminaux qui seront activés avec les types d'activation Espace Travail uniquement ou Travail et Personnel - Contrôle total, le terminal doit être défini sur les paramètres d'usine par défaut avant d'installer UEM Client. Vous pouvez inclure un emplacement de téléchargement spécifique dans un QR Code.
- Les terminaux activés avec le type d'activation Travail et Personnel - Confidentialité des données de l'utilisateur n'ont pas besoin d'être réinitialisés à leurs paramètres d'usine par défaut. Pour ces terminaux, une fois la configuration prête à l'emploi terminée, les utilisateurs peuvent installer UEM Client.

Pour télécharger le fichier .apk UEM Client le plus récent, consultez l'article KB 42607.

Si vous souhaitez activer des terminaux qui n'ont pas accès à Google Play, vérifiez les points suivants :

Configuration requise	Description
Environnement BlackBerry UEM	Si vous souhaitez prendre en charge des terminaux qui n'ont pas accès à Google Play, vous n'êtes pas tenu d'intégrer votre environnement UEM à Android Enterprise. Si vous souhaitez prendre en charge une combinaison de terminaux qui n'ont pas accès à Google Play, vous devez intégrer votre environnement à Android Enterprise.
Paramètres d'activation par défaut	Si vous souhaitez inclure l'emplacement UEM Client dans un QR Code, dans les paramètres d'activation par défaut, sélectionnez Autoriser le QR Code à contenir l'emplacement du fichier source de l'application UEM Client et Utiliser l'emplacement par défaut. Ces options permettent aux utilisateurs de scanner le QR Code figurant dans l'e-mail d'activation pour télécharger UEM Client à partir du site de téléchargement de BlackBerry. Ces options sont disponibles uniquement si votre environnement UEM est intégré à Android Enterprise.
Paramètres du profil d'activation	Vérifiez les paramètres suivants dans le profil d'activation : • Décochez l'option Ajouter un compte Google Play à l'espace Travail. • 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. Vous devez télécharger l'application BlackBerry Connectivity en tant qu'application interne et l'attribuer aux utilisateurs.
Règles de stratégie informatique	Pour les utilisateurs auxquels est attribué le type d'activation Travail et Personnel - Confidentialité des données de l'utilisateur (Android Enterprise), pour autoriser l'installation d'applications en dehors de Google Play, activez la règle de stratégie informatique Autoriser l'installation d'applications autres que Google Play.
Applications non-BlackBerry Dynamics	Pour les applications non-BlackBerry Dynamics, ajoutez les applications à UEM en tant qu'applications internes et attribuez-les aux utilisateurs. 1. Obtenez les fichiers .apk des applications que vous souhaitez attribuer. 2. Sur la barre de menus de la console de gestion, cliquez sur **Applications**. 3. Cliquez sur > **Applications internes**. 4. Cliquez sur **Parcourir**, puis sélectionnez le fichier .apk. 5. Dans le champ **Envoyer à**, sélectionnez **Tous les terminaux Android**. 6. Décochez **Publier l'application dans le domaine Google**. 7. Cliquez sur **Ajouter**. 8. Répétez les étapes précédentes pour chaque application que vous souhaitez ajouter. 9. Attribuez les applications aux utilisateurs. La disposition de l'application doit être définie sur **Obligatoire**.

Configuration requise	Description
Applications BlackBerry Dynamics	Pour les applications BlackBerry Dynamics, téléchargez le fichier source d'application interne et attribuez l'application aux utilisateurs. Pour installer ou mettre à jour des applications internes sur les terminaux qui n'ont pas accès à Google Play, procédez comme suit : **1.** Obtenez les fichiers .apk des applications BlackBerry Dynamics que vous souhaitez attribuer. **2.** Sur la barre de menus de la console de gestion, cliquez sur **Applications**. **3.** Cliquez sur une application BlackBerry Dynamics. **4.** Cliquez sur l'onglet **Android**. **5.** Cliquez sur **Ajouter un fichier source d'application interne**. **6.** Cliquez sur **Parcourir**, puis sélectionnez le fichier .apk. **7.** Cliquez sur **Ajouter**. **8.** Cliquez sur **Enregistrer**. **9.** Répétez les étapes précédentes pour chaque application que vous souhaitez ajouter. **10.** Attribuez les applications aux utilisateurs. La disposition de l'application doit être définie sur **Obligatoire**.
Mise à jour de l'application BlackBerry UEM Client	Pour mettre à jour l'application UEM Client sur les terminaux, les utilisateurs doivent télécharger manuellement la dernière version du fichier .apk et l'installer.

Prise en charge des activations Windows 10

Vous pouvez aider les utilisateurs à activer les terminaux Windows 10 selon les manières suivantes :

- Créer ou modifier un modèle d'e-mail d'activation pour fournir les informations d'activation Windows 10. Pour plus d'informations, consultez Création d'un modèle d'e-mail d'activation.
- Intégration d'UEM avec une jonction Entra ID : lorsqu'une jonction Entra ID est configurée, les utilisateurs peuvent activer leurs terminaux en utilisant uniquement leur nom d'utilisateur et leur mot de passe Entra ID.
- Configurer Windows Autopilot : lorsque vous configurez Windows Autopilot, l'inscription fait partie de la première expérience de configuration et le terminal est automatiquement activé lorsque l'utilisateur l'effectue en utilisant uniquement son nom d'utilisateur et son mot de passe Entra ID.
- Déploiement d'un service de détection Vous pouvez utiliser une application Web Java de BlackBerry comme service de détection afin de simplifier le processus d'activation pour les utilisateurs dotés de terminaux Windows 10. Si vous utilisez le service de détection, les utilisateurs n'auront plus besoin de saisir l'adresse du serveur lors du processus d'activation.

Prise en charge de l‘inscription des utilisateurs d‘Apple pour les terminaux iOS et iPadOS

Vous pouvez utiliser le type d‘activation Confidentialité de l'utilisateur - Inscription de l'utilisateur pour les terminaux iOS et iPadOS afin de vous assurer que les données utilisateur restent privées et séparées des données professionnelles. Avec ce type d‘activation, un espace Travail distinct est installé sur le terminal pour les applications professionnelles et les applications natives Notes, iCloud Drive, Mail (pièces jointes et corps d‘e-mail complets), Calendrier (pièces jointes) et iCloud Keychain. Ce type d‘activation permet la gestion des applications, la gestion des stratégies informatiques, les profils de messagerie, les profils Wi-Fi et le VPN par application. Les administrateurs peuvent gérer les données professionnelles (par exemple, effacer des données professionnelles) sans affecter les données personnelles. Ce type d‘activation est pris en charge sur les terminaux iPhone et iPad non supervisés exécutant des versions prises en charge d‘iOS ou iPadOS.

Si vous souhaitez prendre en charge l‘inscription des utilisateurs d‘Apple, procédez comme suit :

- Vérifiez que les terminaux que vous allez activer à l‘aide de ce type d‘activation ne sont pas supervisés.
- Créez un compte Apple ID géré pour chaque utilisateur. L‘adresse e-mail du compte Apple ID géré doit correspondre à celle de l‘utilisateur dans BlackBerry UEM.
- Lorsque vous définissez le mot de passe d‘activation du terminal pour un utilisateur, sélectionnez le modèle d‘e-mail d‘activation de l‘inscription des utilisateurs d‘Apple.
- Si vous souhaitez permettre aux utilisateurs d‘activer facilement d‘autres applications BlackBerry Dynamics, d‘importer des certificats, d‘utiliser les fonctionnalités BlackBerry 2FA, d‘utiliser CylancePROTECT et de vérifier leur état de conformité, attribuez BlackBerry UEM Client à l‘aide d‘une licence VPP. Si vous définissez la disposition sur Requis, l‘utilisateur est invité à installer l‘application. Si vous définissez la disposition sur Facultatif, l‘utilisateur doit télécharger manuellement l‘application depuis les applications professionnelles.

Prise en charge de Samsung Knox DualDAR

Les terminaux prenant en charge le cryptage Samsung Knox DualDAR peuvent disposer de données de travail sécurisées à l'aide de deux couches de cryptage. La couche externe de Knox DualDAR est basée sur le cryptage de fichiers Android et est améliorée par Samsung pour répondre aux exigences MDFPP. Dans le profil d'activation, vous pouvez spécifier si vous souhaitez utiliser l'application de cryptage intégrée par défaut ou une application interne que vous souhaitez utiliser pour la couche interne de cryptage dans le profil professionnel.

Si vous choisissez d'utiliser l'application par défaut, le profil de travail est sécurisé à l'aide d'un module cryptographique certifié FIPS 140-2 inclus dans la structure de Samsung Knox. L'application de cryptage interne est un module cryptographique spécialement conçu, développé par votre organisation ou un tiers et qui doit être certifié FIPS 140-2. Lorsque l'utilisateur n'utilise pas le terminal, toutes les données du profil de travail sont verrouillées et les applications qui s'exécutent en arrière-plan ne peuvent pas y accéder.

Configuration requise	Description
Terminaux pris en charge	Les modèles phares Samsung sont pris en charge.
Application de cryptage	Si vous souhaitez utiliser une application de cryptage pour le cryptage de Knox DualDAR, vous devez l'ajouter en tant qu'application interne dans la console de gestion . Vous sélectionnez cette application de cryptage lorsque vous créez un profil d'activation pour les terminaux prenant en charge Knox DualDAR. Vous pouvez également choisir d'utiliser l'application de cryptage par défaut.
Profil d'activation	Si vous activez le cryptage de Knox DualDAR dans le profil d'activation, vous devez attribuer le profil uniquement aux terminaux qui le prennent en charge. Si votre organisation prend en charge une combinaison de terminaux qui peuvent ou non prendre en charge Knox DualDAR, vous devez attribuer le profil d'activation à un groupe de terminaux. Si vous appliquez l'activation Knox DualDAR pour un terminal non pris en charge, l'activation ne s'effectuera pas correctement. Pour prendre en charge le cryptage de Knox DualDAR, créez un profil d'activation avec les paramètres suivants pour les terminaux Android : • Sélectionnez le type d'activation Travail et Personnel - Contrôle total (terminal Android Enterprise entièrement géré avec un profil professionnel). • Sélectionnez l'option Lors de l'activation de terminaux Android Enterprise, activez une fonctionnalité UEM Premium telle que BlackBerry Secure Connect Plus. • Sélectionnez l'option Activer Samsung KNOX DualDAR Workspace. • Pour utiliser l'application de cryptage par défaut, sélectionnez l'option Application de cryptage intégrée par défaut. Pour utiliser une autre application de cryptage, sélectionnez l'option Sélectionner une application interne pour cryptage et choisissez l'application de cryptage souhaitée dans la liste des applications.
BlackBerry UEM Client	La dernière version de BlackBerry UEM Client pour Android est recommandée.

Création de profils d'activation

Vous pouvez contrôler la manière dont les terminaux sont activés et gérés à l'aide des profils d'activation. Un profil d'activation spécifie le nombre de terminaux et les types de terminaux qu'un utilisateur peut activer, ainsi que le type d'activation à utiliser pour chaque type de terminal. Le type d'activation détermine le niveau de contrôle dont vous disposez sur les terminaux activés.

Le profil d'activation attribué ne s'applique qu'aux terminaux que l'utilisateur active après l'attribution du profil. Les terminaux déjà activés ne sont pas automatiquement mis à jour pour correspondre au profil d'activation nouveau ou mis à jour.

Lorsque vous ajoutez un utilisateur à BlackBerry UEM, le profil d'activation par défaut est attribué au compte d'utilisateur. Vous pouvez modifier le profil d'activation par défaut selon vos besoins ou créer un profil d'activation personnalisé et l'attribuer à des utilisateurs ou à des groupes.

Créer un profil d'activation

1. Sur la barre de menus de la console de gestion, cliquez sur **Stratégies et profils > Stratégie > Activation**.
2. Cliquez sur +.
3. Saisissez le nom et la description du profil.
4. Dans le champ **Nombre de terminaux qu'un utilisateur peut activer**, spécifiez le nombre maximum de terminaux qu'un utilisateur peut activer.
5. Dans la liste déroulante **Propriété du terminal**, sélectionnez l'une des options suivantes :
   - Si certains utilisateurs activent des terminaux personnels et d'autres des terminaux professionnels, sélectionnez **Non spécifié**.
   - Si la plupart des utilisateurs activent des terminaux professionnels, sélectionnez **Professionnel**.
   - Si la plupart des utilisateurs activent des terminaux personnels, sélectionnez **Personnel**.
6. Vous pouvez également sélectionner un avis d'entreprise dans la liste déroulante **Attribuer un avis d'entreprise**. Si vous affectez un avis d'entreprise, les utilisateurs activant des terminaux iOS, iPadOS, macOS ou Windows 10 doivent accepter l'avis pour terminer le processus d'activation.
7. Dans la section **Types de terminaux que les utilisateurs peuvent activer**, sélectionnez les types de système d'exploitation de terminal que les utilisateurs sont autorisés à activer.
8. Pour chaque type de terminal que vous incluez dans le profil d'activation, procédez comme suit :
   a) Cliquez sur l'onglet correspondant au type de terminal.
   b) Dans la liste déroulante **Restrictions relatives au modèle de terminal**, sélectionnez l'une des options suivantes :
      - **Aucune restriction** : les utilisateurs peuvent activer n'importe quel modèle de terminal.
      - **Autoriser les modèles de terminaux sélectionnés** : les utilisateurs peuvent activer uniquement les modèles de terminaux que vous spécifiez.
      - **Ne pas autoriser les modèles de terminaux sélectionnés** : les utilisateurs ne peuvent pas activer les modèles de terminaux que vous spécifiez.

      Si vous limitez les modèles de terminaux que les utilisateurs peuvent activer, cliquez sur **Modifier** pour sélectionner les terminaux que vous souhaitez autoriser ou restreindre, puis cliquez sur **Enregistrer**.
   c) Dans la liste déroulante **Version minimale autorisée**, sélectionnez la version de système d'exploitation minimale autorisée.
   d) Sélectionnez les types d'activation pris en charge.

Pour les terminaux Android, vous pouvez sélectionner plusieurs types d'activation et les classer. Pour tous les autres types de terminaux, vous ne pouvez sélectionner qu'un seul type d'activation.

Remarque : Vous devez créer des profils d'activation distincts pour Android Enterprise et Android Management. Si Android Enterprise et les types d'activation Android Management sont spécifiés dans le même profil, le type Android Management est prioritaire, même s'il est classé plus bas que Android Enterprise. Seuls le mot de passe et les informations d'activation pour le type d'activation Android Management seront intégrés au QR Code.

9. Pour les terminaux iOS et iPadOS, effectuez les actions suivantes :
   a) Si vous sélectionnez le type d'activation Confidentialité de l'utilisateur et que vous voulez activer le modèle de licence SIM, vous devez sélectionner l'option **Autoriser l'accès à la carte SIM et aux informations matérielles du terminal pour activer la gestion de licences basée sur la carte SIM**.
   b) Si vous avez sélectionné le type d'activation Confidentialité de l'utilisateur et que vous souhaitez gérer des fonctions spécifiques, cochez les cases appropriées.
   c) Si vous avez sélectionné les types d'activation Contrôles MDM ou Confidentialité de l'utilisateur (avec des licences SIM), et que vous souhaitez uniquement activer les terminaux supervisés, sélectionnez **Ne pas autoriser l'activation des terminaux non supervisés**.
   d) Dans la section **Vérification de l'intégrité des applications iOS**, vous pouvez sélectionner l'une des méthodes d'attestation suivantes :

      - **Exécuter une vérification de l'intégrité des applications lors de l'activation des applications BlackBerry Dynamics** : utilisez cette méthode pour vérifier les terminaux lorsqu'ils sont activés pour contrôler l'intégrité des applications professionnelles iOS.
      - **Exécuter des vérifications périodiques de l'intégrité des applications** : utilisez cette méthode pour vérifier les terminaux afin de contrôler l'intégrité des applications professionnelles iOS.

      Pour contrôler l'intégrité de l'application iOS, vous devez activer CylancePROTECT dans votre domaine UEM. Pour plus d'informations, consultez Activation de CylancePROTECT Mobile dans votre domaine UEM.
   e) Dans la section **Attestation de terminal géré**, vous pouvez sélectionner l'une des méthodes d'attestation suivantes :

   - **Exécuter une attestation de terminal géré à l'activation du terminal** : utilisez cette méthode pour vérifier les terminaux lorsqu'ils sont activés pour contrôler l'intégrité des propriétés du terminal.
   - **Exécuter une attestation périodique du terminal géré**: utilisez cette méthode pour réaliser des vérifications régulières pour contrôler l'intégrité des propriétés du terminal.

   Pour exécuter une attestation de terminal géré sur les terminaux iOS, vous devez activer la fonctionnalité. Pour plus d'informations, reportez-vous à la section Configurer l'attestation relative aux terminaux iOS du contenu relatif à l'administration.

   L'attestation du terminal géré s'applique aux types d'activation Contrôles MDM et Confidentialité de l'utilisateur, mais pas au type d'activation Confidentialité de l'utilisateur - Inscription de l'utilisateur. Lorsque vous sélectionnez le type d'activation Confidentialité de l'utilisateur, vous devez sélectionner au moins une des options de gestion (par exemple « Autoriser la gestion VPN »).
10. Pour les terminaux Android, effectuez les actions suivantes :
   a) Si vous avez sélectionné plusieurs types d'activation, cliquez sur les flèches vers le haut et vers le bas pour les classer. Les terminaux reçoivent le profil le mieux classé qu'ils prennent en charge.
   b) Si vous sélectionnez l'un des types d'activation Samsung Knox et que vous souhaitez utiliser Google Play pour gérer les applications professionnelles, sélectionnez **Gestion de l'application Google Play pour les appareils Samsung Knox Workspace**. Cette option est disponible uniquement si vous avez configuré une connexion à un domaine Google.

      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.

c) Si vous avez sélectionné un type d'activation Android Enterprise, sélectionnez les options Android Enterprise appropriées :

- Pour activer BlackBerry Secure Connect Plus et les fonctionnalités Knox Platform for Enterprise (pour les terminaux prenant en charge Samsung Knox) sur les terminaux dotés d'une licence appropriée, sélectionnez **Lors de l'activation de terminaux Android Enterprise, activez une fonctionnalité UEM Premium telle que BlackBerry Secure Connect Plus**.
- Pour activer le cryptage Samsung Knox DualDAR pour les terminaux qui le prennent en charge, sélectionnez **Activer Samsung KNOX DualDAR Workspace**.
- Pour permettre la gestion d'applications Google Play dans l'espace Travail, sélectionnez **Ajouter Google Play à l'espace Travail**.
- Pour autoriser UEM à limiter l'activation par ID de terminal, sélectionnez **Autoriser uniquement les ID de terminal approuvés**. Cette option est uniquement prise en charge pour les terminaux Espace Travail uniquement et Travail et Personnel - Contrôle total.
- Pour spécifier le type de réseau sur lequel les utilisateurs peuvent activer un terminal, sélectionnez un réseau dans la liste déroulante **Inscription par QR Code**. Cette option est uniquement prise en charge pour les terminaux Espace Travail uniquement et Travail et Personnel - Contrôle total.

d) Dans la section **Options d'attestation SafetyNet ou Play Integrity**, vous pouvez sélectionner l'une des méthodes d'attestation suivantes :

- **Exécuter l'attestation SafetyNet ou Play Integrity pour le terminal** : utilisez cette méthode pour vérifier l'authenticité et l'intégrité des terminaux.
- **Effectuer l'attestation SafetyNet lors de l'activation du terminal (s'applique uniquement aux versions UEM client qui ne prennent pas en charge Play Integrity)** : utilisez cette méthode pour tester l'authenticité et l'intégrité des terminaux lorsqu'ils sont activés.
- **Exécuter l'attestation SafetyNet ou Play Integrity lors de l'activation des applications BlackBerry Dynamics** : utilisez cette méthode pour vérifier l'authenticité et l'intégrité des applications BlackBerry Dynamics lorsqu'elles sont activées.

e) Si vous souhaitez qu'UEM teste les terminaux pour s'assurer que le niveau de correctif de sécurité requis est installé, dans la section **Options d'attestation matérielle**, sélectionnez **Appliquer les règles de conformité d'attestation lors de l'activation**.

11. Pour les terminaux Windows 10, sélectionnez l'une des options de facteur de forme ou les deux.

12. Cliquez sur **Ajouter**.

À la fin :

- Si nécessaire, classez les profils d'activation.
- Attribuez le profil aux comptes d'utilisateur et groupes.

Activation des terminaux Android

La procédure suivie par les utilisateurs pour installer BlackBerry UEM Client et lancer l'activation des terminaux Android dépend de plusieurs facteurs, notamment de la version du système d'exploitation de Android, du fabricant du terminal, de la manière dont votre organisation utilise les services Google, du type d'activation spécifié dans le profil d'activation du terminal et des préférences de votre organisation. Vous pouvez fournir des instructions d'activation du terminal dans l'e-mail d'activation que vous envoyez aux utilisateurs. Pour plus d'informations sur la création d'un modèle d'e-mail d'activation, consultez Création d'un modèle d'e-mail d'activation.

Les terminaux Android Management prennent en charge les méthodes d'activation suivantes :

Méthode d'activation	Description
Activation pour la confidentialité de l'utilisateur Android Management	Pour les terminaux qui seront activés avec le type d'activation Travail et Personnel - Confidentialité des données de l'utilisateur, les utilisateurs peuvent configurer un profil professionnel et utiliser un QR Code fourni pour télécharger UEM Client depuis Google Play et activer le terminal sur UEM. Pour plus d'informations, reportez-vous à Activation d'un terminal Android Management avec le type d'activation Travail et Personnel - Confidentialité des données de l'utilisateur.
Activation pour le contrôle total de Android Management et un espace Travail uniquement	Pour les terminaux qui seront activés avec les types d'activation Travail et Personnel - Contrôle total et Espace Travail uniquement, l'utilisateur doit réinitialiser le terminal aux paramètres d'usine par défaut et utiliser un QR Code fourni pour télécharger UEM Client depuis Google Play et activer le terminal sur UEM. Pour plus d'informations, reportez-vous à Activation d'un terminal Android Management à l'aide d'un compte géré Google Play.

Les terminaux Android Enterprise prennent en charge les méthodes d'activation suivantes :

Méthode d'activation	Description
Installez UEM Client depuis Google Play.	Les terminaux qui seront activés avec le type d'activation Travail et Personnel - Confidentialité des données de l'utilisateur n'ont pas besoin d'être réinitialisés aux paramètres d'usine par défaut avant d'être activés. Pour activer ces terminaux, les utilisateurs peuvent télécharger UEM Client depuis Google Play. Pour plus d'informations, reportez-vous à Activer un terminal Android Enterprise avec le type d'activation Travail et Personnel - Confidentialité des données de l'utilisateur.
Téléchargez le fichier .apk UEM Client depuis le site de téléchargement BlackBerry.	Si les utilisateurs Android n'ont pas accès à Google Play, pour les terminaux qui seront activés avec le Travail et Personnel - Confidentialité des données de l'utilisateur type d'activation, ils peuvent télécharger le fichier .apk UEM Client depuis le site de téléchargement BlackBerry. Vous pouvez également télécharger le fichier depuis BlackBerry et le placer à un emplacement auquel vos utilisateurs peuvent accéder. Pour obtenir le fichier .apk de la dernière version de UEM Client, reportez-vous à l'article KB 42607.

Méthode d'activation	Description
Utilisez les informations d'identification du domaine Google lors de la configuration du terminal.	Si BlackBerry UEM est connecté au Google Workspace de votre organisation ou au domaine Google Cloud, pour activer les terminaux auxquels le type d'activation Espace Travail uniquement ou Travail et Personnel - Contrôle total a été attribué, lorsque les utilisateurs saisissent leurs informations d'identification professionnelles Google pendant la configuration du terminal, le terminal télécharge le UEM Client et commence le processus d'activation. Pour plus d'informations, reportez-vous à Activation d'un terminal Android Enterprise lorsque BlackBerry UEM est connecté à un domaine Google.
Scannez un QR Code UEM Client contenant l'emplacement de téléchargement.	BlackBerry UEM vous permet d'inclure l'emplacement de téléchargement de UEM Client dans un QR Code que vous pouvez inclure dans l'e-mail d'activation que vous envoyez aux utilisateurs. Les utilisateurs attribués à Espace Travail uniquement ou Travail et Personnel - Contrôle total peuvent scanner le QR Code pour télécharger UEM Client. Pour plus d'informations, reportez-vous à Activation d'un terminal Android Enterprise à l'aide d'un compte géré Google Play.
Inscription sans intervention Android ou Samsung Knox Mobile Enrollment.	L'inscription sans intervention Android vous permet de déployer simultanément un grand nombre de terminaux Android Enterprise. Knox Mobile Enrollment vous permet de déployer un grand nombre de terminaux Samsung Knox avec des activations Android Enterprise. Pour utiliser cette option, les terminaux doivent être configurés pour une inscription sans intervention ou Knox Mobile Enrollment lorsqu'ils sont achetés auprès d'un revendeur agréé. Pour plus d'informations, reportez-vous à Configurer la prise en charge de l'inscription sans intervention Android ou Activation de plusieurs terminaux à l'aide de Knox Mobile Enrollment.

Pour les terminaux Android Enterprise, chaque option d'activation n'est prise en charge que par certains types d'activation. Pour les types d'activation Espace Travail uniquement et Travail et Personnel - Contrôle total, les options prises en charge dépendent également de la manière dont votre organisation utilise les services Google.

Type d'activation	Confidentialité de l'utilisateur AE	Contrôle total AE			AE Espace Travail uniquement		
Méthode		Domaine Google	Google Play géré	Aucun accès Google	Domaine Google	Google Play géré	Aucun accès Google
Installer UEM Client depuis Google Play ou télécharger par l'utilisateur	Oui	Non	Non	Non	Non	Non	Non

Type d'activation	Confidentialité de l'utilisateur AE	Contrôle total AE			AE Espace Travail uniquement		
Méthode		**Domaine Google**	**Google Play géré**	**Aucun accès Google**	**Domaine Google**	**Google Play géré**	**Aucun accès Google**
Informations d'identification du domaine Google	Oui	Oui	Non	Non	Oui	Non	Non
Scanner le QR Code	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Inscription sans intervention Android/Samsu Knox Mobile Enrollment	Non	Oui	Oui	Oui	Oui	Oui	Oui

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

Pour activer les terminaux à l'aide du type d'activation Travail et Personnel - Confidentialité des données de l'utilisateur (Android Enterprise), envoyez les instructions suivantes aux utilisateurs concernés. Les terminaux dotés de ce type d'activation n'ont pas besoin d'être réinitialisés aux paramètres d'usine par défaut avant d'être activés.

Avant de commencer : L'administrateur de votre terminal vous a envoyé un ou plusieurs e-mails contenant les informations dont vous avez besoin pour activer votre terminal. Si l'e-mail contient un QR Code d'activation, vous pouvez l'utiliser pour activer votre terminal. Si vous n'avez pas reçu de QR Code, assurez-vous de disposer des informations suivantes :

- Votre adresse électronique professionnelle
- Votre nom d'utilisateur UEM (généralement votre nom d'utilisateur professionnel)
- Votre mot de passe d'activation UEM
- Adresse du serveur UEM (si nécessaire)

1. Sur le terminal, installez BlackBerry UEM Client depuis Google Play.

   Si le terminal n'a pas accès à Google Play, vous pouvez télécharger manuellement le UEM Client à l'aide d'un fichier .apk. Pour obtenir le fichier .apk de la dernière version de UEM Client, consultez l'article KB 42607.
2. Ouvrez le UEM Client.
3. Lisez le contrat de licence et cochez la case **J'accepte le contrat de licence**.
4. Effectuez l'une des opérations suivantes :

Tâche	Étapes
Scannez un QR Code pour activer le terminal.	**a.** Sélectionnez . **b.** Appuyez sur **Autoriser** pour permettre à UEM Client de prendre des photos et d'enregistrer des vidéos. **c.** Scannez le QR Code fourni par votre administrateur dans l'e-mail d'activation.
Activez manuellement le terminal.	**a.** Saisissez votre adresse électronique professionnelle et appuyez sur **Suivant**. **b.** Saisissez votre mot de passe d'activation et sélectionnez **Activer mon terminal**. **c.** Si nécessaire, saisissez l'adresse du serveur, puis sélectionnez **Suivant**. **d.** Si nécessaire, saisissez votre nom d'utilisateur et votre mot de passe d'activation, puis appuyez sur **Suivant**.

5. Appuyez sur **Autoriser** pour permettre à UEM Client de passer et de gérer des appels téléphoniques.
6. Sur l'écran **Configurer votre profil**, appuyez sur **Configurer**. La configuration du profil professionnel peut prendre un certain temps.
7. Si vous y êtes invité, connectez-vous à votre compte Google, saisissez votre adresse e-mail et votre mot de passe Google.
8. Choisissez une méthode de déverrouillage de l'écran.
9. Si vous y êtes invité sur l'écran **Démarrage sécurisé**, sélectionnez **Oui** pour demander un mot de passe au démarrage du terminal.
10. Saisissez un mot de passe, puis saisissez-le à nouveau pour le confirmer. Sélectionnez **OK**.
11. Sélectionnez le mode d'affichage des notifications. Sélectionnez **Terminé**.
12. Créez un mot de passe UEM Client et appuyez sur **OK**. Si vous utilisez des applications BlackBerry Dynamics, vous utiliserez également ce mot de passe pour vous connecter à toutes vos applications BlackBerry Dynamics.
13. Appuyez sur **S'inscrire**.
14. Si vous souhaitez configurer l'authentification par empreinte digitale pour les applications UEM Client et BlackBerry Dynamics, suivez les instructions indiquées sur l'écran. Sinon, appuyez sur **Annuler**.
15. Si vous êtes déconnecté de votre terminal, déverrouillez-le pour terminer l'activation UEM.
16. Si vous êtes invité à autoriser la connexion à BlackBerry Secure Connect Plus, appuyez sur **OK** et attendez que la connexion soit établie.
17. Si vous y êtes invité, suivez les instructions qui s'affichent à l'écran pour installer des applications professionnelles sur votre terminal.

À la fin : Pour vérifier que le processus d'activation s'est bien déroulé, effectuez l'une des opérations suivantes :

- Dans 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 la console 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.

Activation d'un terminal Android Enterprise lorsque BlackBerry UEM est connecté à un domaine Google

Ces étapes s'appliquent aux terminaux auxquels est attribué le type d'activation Espace Travail uniquement (Android Enterprise) ou Travail et Personnel - Contrôle total (Android Enterprise) lorsque BlackBerry UEM est connecté à un Google Workspace ou à un domaine Google Cloud. Pour activer les terminaux connectés à un domaine Google avec le type d'activation Travail et Personnel - Confidentialité des données de l'utilisateur, consultez 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 : L'administrateur de votre terminal vous a envoyé un ou plusieurs e-mails contenant les informations dont vous avez besoin pour activer votre terminal. Si l'e-mail contenait un QR Code d'activation, vous pouvez l'utiliser pour activer votre terminal. Vous n'avez alors aucune information à saisir. Si vous n'avez pas reçu de QR Code, assurez-vous d'avoir reçu les informations suivantes :

- Votre adresse électronique professionnelle
- Votre nom d'utilisateur UEM (généralement votre nom d'utilisateur professionnel)
- Votre mot de passe d'activation UEM
- L'adresse de votre serveur UEM (si 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 de connexion à votre compte Google, saisissez votre adresse e-mail Google professionnelle et votre mot de passe.
3. Sur le terminal, sélectionnez **Installer** pour installer BlackBerry UEM Client.
4. Lisez le contrat de licence et cochez la case **J'accepte le contrat de licence**.
5. Effectuez l'une des opérations suivantes :

Tâche	Étapes
Utiliser un QR Code pour activer le terminal	**a.** Sélectionnez . **b.** Appuyez sur **Autoriser** pour permettre à UEM Client de prendre des photos et d'enregistrer des vidéos. **c.** Scannez le QR Code figurant dans l'e-mail d'activation que vous avez reçu.
Activez manuellement le terminal.	**a.** Saisissez votre adresse électronique professionnelle. Appuyez sur **Suivant**. **b.** Saisissez votre mot de passe d'activation. Appuyez sur **Activer mon terminal**. **c.** Si nécessaire, entrez l'adresse du serveur. Vous trouverez l'adresse du serveur dans l'e-mail d'activation que vous avez reçu ou dans BlackBerry UEM Self-Service. Appuyez sur **Suivant**. **d.** Si nécessaire, saisissez votre nom d'utilisateur et votre mot de passe d'activation. Appuyez sur **Suivant**.

6. Attendez la fin du transfert des profils et paramètres.
7. Sur l'écran **Configurer votre profil**, appuyez sur **Configurer**. La configuration du profil professionnel peut prendre un certain temps.

8. Si vous y êtes invité, connectez-vous à votre compte Google avec votre adresse e-mail et votre mot de passe Google.
9. Sur l'écran Déverrouiller la sélection, sélectionnez une méthode de déverrouillage d'écran.
10. Si vous y êtes invité sur l'écran **Démarrage sécurisé**, sélectionnez **Oui** pour demander un mot de passe lorsque le terminal démarre.
11. Saisissez un mot de passe, puis saisissez-le à nouveau pour le confirmer. Sélectionnez **OK**.
12. Sélectionnez une option pour l'envoi des notifications. Sélectionnez **Terminé**.
13. Créez un mot de passe UEM Client et appuyez sur **OK**. Si vous utilisez des applications BlackBerry Dynamics, vous utiliserez également ce mot de passe pour vous connecter à toutes vos applications BlackBerry Dynamics.
14. Sur l'écran suivant, appuyez sur **S'inscrire** et suivez les instructions qui s'affichent à l'écran si vous souhaitez configurer l'authentification par empreinte digitale pour UEM Client et toutes les applications BlackBerry Dynamics dont vous disposez. Sinon, appuyez sur **Annuler**.
15. Si vous êtes déconnecté de votre terminal, déverrouillez-le pour terminer l'activation UEM.
16. Si vous y êtes invité, sélectionnez **OK** pour vous connecter à BlackBerry Secure Connect Plus et attendez que la connexion soit établie.
17. Si vous y êtes invité, suivez les instructions à l'écran pour installer des applications professionnelles sur votre terminal.

À la fin : Pour vérifier que le processus d'activation s'est bien déroulé, effectuez l'une des opérations suivantes :

- Dans 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 la console 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.

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

Les instructions d'activation suivantes s'appliquent aux terminaux Android pris en charge auxquels est attribué le type d'activation Espace Travail uniquement (Android Enterprise) ou Travail et Personnel - Contrôle total (Android Enterprise). Pour activer les terminaux connectés à un compte Google Play géré avec le type d'activation Android Enterprise Travail et Personnel - Confidentialité des données de l'utilisateur, consultez Activer un terminal Android Enterprise avec le type d'activation Travail et Personnel - Confidentialité des données de l'utilisateur.

Vous pouvez configurer et inclure un QR Code contenant l'emplacement du fichier source de l'application UEM Client dans l'e-mail d'activation que vous envoyez aux utilisateurs. Lorsqu'un utilisateur scanne le code QR Code, UEM Client est automatiquement téléchargé. Pour configurer et inclure un QR Code dans l'e-mail d'activation, vous devez cocher la case Autoriser les QR Codes pour l'activation des terminaux sur la page Paramètres d'activation par défaut (Paramètres > Paramètres généraux > Paramètres d'activation par défaut). Vous devez également cocher la case Autoriser le QR Code à contenir l'emplacement du fichier source de l'application UEM Client et spécifier l'emplacement du fichier source de l'application UEM Client. Pour obtenir le fichier .apk de la dernière version de UEM Client, reportez-vous à l'article KB 42607.

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

Avant de commencer : L'administrateur de votre terminal vous a envoyé un ou plusieurs e-mails contenant les informations dont vous avez besoin pour activer votre terminal. L'e-mail comprend un QR Code contenant les informations nécessaires à l'installation de UEM Client et à l'activation du terminal.

1. Sur le terminal que vous souhaitez activer, si l'écran du programme d'installation ne s'affiche pas, réinitialisez votre terminal avec ses paramètres d'usine par défaut.
2. Pour ouvrir le lecteur QR Code du terminal, appuyez sept fois sur l'écran.
3. Pour télécharger UEM Client, scannez le QR Code fourni par votre administrateur dans l'e-mail d'activation.
4. Ouvrez le UEM Client.
5. Lisez le contrat de licence et cochez la case **J'accepte le contrat de licence**.
6. Sur l'écran **Configurer votre profil**, appuyez sur **Configurer**. La configuration du profil professionnel peut prendre un certain temps.
7. Choisissez une méthode de déverrouillage de l'écran.
8. Si vous y êtes invité sur l'écran **Démarrage sécurisé**, sélectionnez **Oui** pour demander un mot de passe au démarrage du terminal.
9. Saisissez le mot de passe du terminal, resaisissez-le pour le confirmer, puis sélectionnez **OK**.
10. Sélectionnez le mode d'affichage des notifications. Sélectionnez **Terminé**.
11. Créez un mot de passe UEM Client et appuyez sur **OK**. Si vous utilisez des applications BlackBerry Dynamics, vous utiliserez également ce mot de passe pour vous connecter à toutes vos applications BlackBerry Dynamics.
12. Appuyez sur **S'inscrire**.
13. Si vous souhaitez configurer l'authentification par empreinte digitale pour les applications UEM Client et BlackBerry Dynamics, suivez les instructions affichées à l'écran. Sinon, appuyez sur **Annuler**.
14. Si vous êtes déconnecté de votre terminal, déverrouillez-le pour terminer l'activation UEM.
15. Si vous y êtes invité, sélectionnez **OK** pour vous connecter à BlackBerry Secure Connect Plus et attendez que la connexion soit établie.
16. Si vous y êtes invité, suivez les instructions qui s'affichent à l'écran pour installer des applications professionnelles sur votre terminal.

À la fin : Pour vérifier que le processus d'activation s'est bien déroulé, effectuez l'une des opérations suivantes :

- Dans 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 la console 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.

Activation d'un terminal Android Enterprise sans accès à Google Play

Les instructions d'activation suivantes s'appliquent aux terminaux attribués aux types d'activation Espace Travail uniquement (Android Enterprise) et Travail et Personnel - Contrôle total (Android Enterprise) qui n'ont pas accès à Google Play. L'utilisateur peut télécharger BlackBerry UEM Client à l'aide d'un fichier .apk de l'application. Vous pouvez configurer et inclure un QR Code qui contient l'emplacement du fichier source UEM Client dans l'e-mail d'activation que vous envoyez aux utilisateurs. Lorsqu'un utilisateur scanne le code QR Code, UEM Client est automatiquement téléchargé.

Pour configurer et inclure un QR Code dans l'e-mail d'activation, vous devez cocher la case Autoriser les QR Codes pour l'activation des terminaux sur la page Paramètres d'activation par défaut (Paramètres > Paramètres généraux > Paramètres d'activation par défaut). Vous devez également cocher la case Autoriser le QR Code à contenir l'emplacement du fichier source de l'application UEM Client et spécifier l'emplacement du fichier source de l'application UEM Client. Pour obtenir le fichier .apk de la dernière version de UEM Client, reportez-vous à l'article KB 42607.

Envoyez les instructions d'activation suivantes aux utilisateurs du terminal.

Avant de commencer : L'administrateur de votre terminal vous a envoyé un ou plusieurs e-mails contenant les informations dont vous avez besoin pour activer votre terminal. Si vous avez reçu un QR Code d'activation de la part de votre administrateur, vous pouvez l'utiliser pour activer votre terminal. Si vous n'avez pas reçu de QR Code, assurez-vous de disposer des informations suivantes :

- Votre adresse électronique professionnelle
- Votre nom d'utilisateur UEM (généralement votre nom d'utilisateur professionnel)
- Votre mot de passe d'activation UEM
- L'adresse de votre serveur UEM (si nécessaire)

1. Sur le terminal que vous souhaitez activer, si l'écran du programme d'installation ne s'affiche pas, réinitialisez votre terminal avec ses paramètres d'usine par défaut.
2. Pour ouvrir le lecteur QR Code du terminal, appuyez sept fois sur l'écran.
3. Pour télécharger UEM Client, scannez le QR Code fourni par votre administrateur dans l'e-mail d'activation. UEM Client est automatiquement téléchargé sur le terminal.
4. Ouvrez le UEM Client.
5. Lisez le contrat de licence et cochez la case **J'accepte le contrat de licence**.
6. Effectuez l'une des opérations suivantes :

Tâche	Étapes
Utiliser un QR Code pour activer le terminal	**a.** Dans UEM Client, appuyez sur . **b.** Appuyez sur **Autoriser** pour permettre à UEM Client de prendre des photos et d'enregistrer des vidéos.
Activez manuellement le terminal.	**a.** Saisissez votre adresse électronique professionnelle et appuyez sur **Suivant**. **b.** Saisissez votre mot de passe d'activation et sélectionnez **Activer mon terminal**. **c.** Si nécessaire, saisissez l'adresse du serveur, puis sélectionnez **Suivant**. **d.** Si nécessaire, saisissez votre nom d'utilisateur et votre mot de passe d'activation, puis appuyez sur **Suivant**.

7. Sur l'écran **Configurer votre profil**, appuyez sur **Configurer**. La configuration du profil professionnel peut prendre un certain temps.
8. Choisissez une méthode de déverrouillage de l'écran.
9. Si vous y êtes invité sur l'écran **Démarrage sécurisé**, sélectionnez **Oui** pour demander un mot de passe au démarrage du terminal.
10. Saisissez un mot de passe, puis saisissez-le à nouveau pour le confirmer. Sélectionnez **OK**.
11. Sélectionnez le mode d'affichage des notifications. Sélectionnez **Terminé**.
12. Créez un mot de passe UEM Client et appuyez sur **OK**. Si vous utilisez des applications BlackBerry Dynamics, vous utiliserez également ce mot de passe pour vous connecter à toutes vos applications BlackBerry Dynamics.
13. Sur l'écran suivant, appuyez sur **Inscrire**.
14. Si vous souhaitez configurer l'authentification par empreinte digitale pour les applications UEM Client et BlackBerry Dynamics, suivez les instructions indiquées à l'écran. Sinon, appuyez sur **Annuler**.
15. Si vous êtes déconnecté de votre terminal, déverrouillez-le pour terminer l'activation UEM.
16. Si vous y êtes invité, sélectionnez **OK** pour vous connecter à BlackBerry Secure Connect Plus et attendez que la connexion soit établie.

17. Si vous y êtes invité, suivez les instructions qui s'affichent à l'écran pour installer des applications professionnelles sur votre terminal.
18. Si nécessaire, ouvrez l'application de messagerie que votre organisation souhaite que vous utilisiez et suivez les instructions pour configurer la messagerie électronique sur votre téléphone.

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

Vous pouvez inclure un QR Code dans l'e-mail d'activation que vous envoyez aux utilisateurs. Lorsqu'un utilisateur scanne le code QR Code, UEM Client est automatiquement téléchargé. Pour configurer et inclure un QR Code dans l'e-mail d'activation, vous devez cocher la case Autoriser les QR Codes pour l'activation des terminaux sur la page Paramètres d'activation par défaut (Paramètres > Paramètres généraux > Paramètres d'activation par défaut). Utilisez le modèle d'e-mail d'activation par défaut d'Android Management (ou un équivalent personnalisé).

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

Avant de commencer : L'administrateur de votre terminal vous a envoyé un ou plusieurs e-mails contenant les informations dont vous avez besoin pour activer votre terminal. L'e-mail comprend un QR Code contenant les informations nécessaires à l'installation de UEM Client et à l'activation du terminal.

1. Sur votre terminal, accédez à **Paramètres > Services et préférences Google**.
2. Sélectionnez **Configurer et restaurer**.
3. Sélectionnez **Configurer votre profil professionnel**.
4. Appuyez sur **Suivant**.
5. Dans la boite de dialogue **Autoriser la stratégie de terminal pour prendre des photos et enregistrer des vidéos**, sélectionnez **Seulement cette fois**.
6. Scannez le QR Code que vous avez reçu de votre administrateur.
7. Sélectionnez **Accepter**.
8. Appuyez sur **Suivant**.
9. Selon la façon dont votre administrateur a configuré l'activation, vous pouvez être invité à définir un verrou pour votre terminal ou pour l'espace Travail.
10. Sur l'écran **Votre liste de contrôle professionnelle**, sous **Installer des applications professionnelles**, sélectionnez **Installer**.
11. Une fois UEM Client installé, sélectionnez **Terminé**.
12. Sélectionnez **Configurer BlackBerry UEM**.
13. Lisez l'accord de licence et sélectionnez **J'accepte**.

Votre terminal finalise la configuration de votre profil professionnel.

À la fin : Si vous souhaitez désactiver votre terminal et le retirer d'UEM, vous pouvez le faire à partir de UEM Client.

Activation d'un terminal Android Management à l'aide d'un compte géré Google Play

Les instructions d'activation suivantes s'appliquent aux terminaux Android auxquels est attribué le type d'activation Travail et Personnel - Contrôle total (Android Management) ou Espace Travail uniquement (Android Management). Pour activer les terminaux connectés à un compte Google Play géré avec le type d'activation Android Management Travail et Personnel - Confidentialité des données de l'utilisateur, consultez Activation d'un terminal Android Management avec le type d'activation Travail et Personnel - Confidentialité des données de l'utilisateur.

Vous pouvez inclure un QR Code dans l'e-mail d'activation que vous envoyez aux utilisateurs. Lorsqu'un utilisateur scanne le code QR Code, UEM Client est automatiquement téléchargé. Pour configurer et inclure un QR Code dans l'e-mail d'activation, vous devez cocher la case Autoriser les QR Codes pour l'activation des terminaux sur la page Paramètres d'activation par défaut (Paramètres > Paramètres généraux > Paramètres d'activation par défaut). Utilisez le modèle d'e-mail d'activation par défaut d'Android Management (ou un équivalent personnalisé).

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

Avant de commencer : L'administrateur de votre terminal vous a envoyé un ou plusieurs e-mails contenant les informations dont vous avez besoin pour activer votre terminal. L'e-mail comprend un QR Code contenant les informations nécessaires à l'installation de UEM Client et à l'activation du terminal.

1. Sur le terminal que vous souhaitez activer, si l'écran du programme d'installation ne s'affiche pas, réinitialisez votre terminal avec ses paramètres d'usine par défaut.
2. Pour ouvrir le lecteur QR Code du terminal, appuyez sept fois sur l'écran.
3. Pour télécharger UEM Client, scannez le QR Code fourni par votre administrateur dans l'e-mail d'activation. Le UEM Client est automatiquement téléchargé.
4. Ouvrez le UEM Client.
5. Lisez le contrat de licence et cochez la case **J'accepte le contrat de licence**.
6. Sur l'écran **Configurer votre profil**, appuyez sur **Configurer**. La configuration du profil professionnel peut prendre un certain temps.
7. Choisissez une méthode de déverrouillage de l'écran.
8. Si vous y êtes invité sur l'écran **Démarrage sécurisé**, sélectionnez **Oui** pour demander un mot de passe au démarrage du terminal.
9. Saisissez le mot de passe du terminal, resaisissez-le pour le confirmer, puis sélectionnez **OK**.
10. Sélectionnez le mode d'affichage de vos notifications, puis appuyez sur **Terminé**.
11. Créez un mot de passe UEM Client et appuyez sur **OK**. Si vous utilisez des applications BlackBerry Dynamics, vous utiliserez également ce mot de passe pour vous connecter à toutes vos applications BlackBerry Dynamics.
12. Sur l'écran suivant, appuyez sur **Inscrire**.
13. Si vous souhaitez configurer l'authentification par empreinte digitale pour les applications UEM Client et BlackBerry Dynamics, suivez les instructions affichées à l'écran. Sinon, appuyez sur **Annuler**.
14. Si vous êtes déconnecté de votre terminal, déverrouillez-le pour terminer l'activation BlackBerry UEM.
15. Si vous y êtes invité, sélectionnez **OK** pour vous connecter à BlackBerry Secure Connect Plus et attendez que la connexion soit établie.
16. Si vous y êtes invité, suivez les instructions qui s'affichent à l'écran pour installer des applications professionnelles sur votre terminal.

À la fin : Pour vérifier que le processus d'activation s'est bien déroulé, effectuez l'une des opérations suivantes :

- Dans 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 la console 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.

Activation des terminaux iOS

Les étapes que les utilisateurs doivent suivre pour installer BlackBerry UEM Client et activer les terminaux iOS et iPadOS peuvent être différentes selon la version du système d'exploitation du terminal et selon que le type d'activation inclut ou non des contrôles MDM. Vous pouvez fournir des instructions d'activation du terminal dans l'e-mail d'activation que vous envoyez aux utilisateurs. Pour plus d'informations sur la création d'un modèle d'e-mail d'activation, consultez Création d'un modèle d'e-mail d'activation.

Activer un terminal iOS ou iPadOS avec le type d'activation Contrôles MDM

Pour activer des terminaux avec le type d'activation Contrôles MDM ou Confidentialité de l'utilisateur avec les options MDM du type d'activation activé, envoyez les instructions d'activation suivantes aux utilisateurs du terminal.

Lors de l'activation, les utilisateurs doivent quitter BlackBerry UEM Client pour installer manuellement le profil MDM.

Avant de commencer : Si le mode Verrouiller est activé sur votre terminal (iOS et iPadOS version 16 ou ultérieure), vous devez le désactiver pour activer le terminal. Le mode Verrouiller empêche l'installation des profils de configuration requis pour l'activation. Le mode Verrouiller empêche l'installation des profils de configuration requis pour l'activation.

1. Sur le terminal, installez UEM Client depuis l'App Store.
2. Ouvrez UEM Client et acceptez le contrat de licence.
3. Effectuez l'une des opérations suivantes :

Tâche	Étapes
Scannez un QR Code pour activer le terminal.	**a.** Sélectionnez . **b.** Appuyez sur **Autoriser** pour permettre à UEM Client de prendre des photos et d'enregistrer des vidéos. **c.** Scannez le QR Code figurant dans l'e-mail d'activation que vous avez reçu.
Activez manuellement le terminal.	**a.** Saisissez votre adresse électronique professionnelle et votre mot de passe d'activation. **b.** Si nécessaire, entrez l'adresse du serveur. Vous trouverez l'adresse du serveur dans l'e-mail d'activation que vous avez reçu ou dans BlackBerry UEM Self-Service. **c.** Appuyez sur **Suivant**.

4. Appuyez sur **Autoriser** pour autoriser l'envoi de notifications par UEM Client. Si vous choisissez **Ne Pas Autoriser**, le terminal ne pourra pas être activé.
5. Lorsque vous êtes invité à installer un profil de configuration, appuyez sur **OK**.
6. Lorsque vous êtes invité à télécharger le profil de configuration, sélectionnez **Autoriser**.
7. Une fois le téléchargement terminé, ouvrez **Paramètres**.
8. Appuyez sur **Général** et accédez à **VPN et Gestion des terminaux**.
9. Pour installer le profil, appuyez sur **Profil BlackBerry UEM** et suivez les instructions à l'écran.

10. Une fois l'installation terminée, revenez à UEM Client pour terminer l'activation.
11. Si vous y êtes invité, suivez les instructions qui s'affichent à l'écran pour installer des applications professionnelles sur votre terminal.

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

- Sur le terminal, ouvrez 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.

Activer un terminal iOS ou iPadOS avec l'inscription des utilisateurs d'Apple

L'inscription de l'utilisateur Apple est prise en charge sur les terminaux exécutant les versions iOS et iPadOS prises en charge. Pour activer des terminaux à l'aide de l'inscription de l'utilisateur Apple, envoyez les instructions suivantes à l'utilisateur du terminal.

Avant de commencer :

- Vérifiez que vous avez reçu un e-mail d'activation contenant le QR Code pour l'inscription des utilisateurs d'Apple. Si vous n'avez pas reçu l'e-mail, contactez un administrateur.
- Si votre terminal est déjà activé avec BlackBerry UEM, vous devez le désactiver.
- Désinstallez BlackBerry UEM Client.
- Vous devez disposer d'un compte Apple ID géré par votre organisation.
- Votre terminal ne doit pas être supervisé. Si votre terminal est supervisé, il est noté dans l'application Paramètres près de votre Apple ID.
- Si le mode Verrouiller est activé sur votre terminal (iOS et iPadOS version 16 ou ultérieure), vous devez le désactiver pour activer le terminal. Le mode Verrouiller empêche l'installation des profils de configuration requis pour l'activation. Le mode Verrouiller empêche l'installation des profils de configuration requis pour l'activation.

1. Ouvrez l'e-mail d'activation qui contient le QR Code pour l'inscription des utilisateurs d'Apple. Si le QR Code a déjà expiré, vous pouvez demander un nouveau code d'activation à BlackBerry UEM Self-Service ou contacter votre administrateur.
2. Ouvrez l'application d'appareil photo de votre terminal et scannez le QR Code figurant dans l'e-mail d'activation. Lorsque vous y êtes invité, sélectionnez la notification pour ouvrir l'URL dans Safari.
3. Lorsque vous êtes invité à télécharger le profil de configuration UEM, sélectionnez **Autoriser**.
4. Une fois le téléchargement terminé, sélectionnez **Fermer**.
5. Accédez à **Paramètres > Général > Profil**.
6. Sélectionnez **Profil UEM**.
7. Sur l'écran Inscription des utilisateurs, sélectionnez **Inscrire mon iPhone** ou **Inscrire mon iPad**.
8. Saisissez votre mot de passe.
9. Connectez-vous à Apple ID à l'aide de vos informations d'identification Apple ID.
10. Si votre administrateur vous a attribué UEM Client, sélectionnez **Installer** lorsque vous y êtes invité ou ouvrez Applications professionnelles.
11. Pour configurer l'application UEM Client, ouvrez-la et acceptez le contrat de licence. Suivez les instructions à l'écran pour terminer le processus d'activation.

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

- Sur le terminal, ouvrez 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.

Activation d'un terminal macOS ou Apple TV avec BlackBerry UEM Self-Service

Les utilisateurs activent les terminaux macOS et Apple TV à l'aide de BlackBerry UEM Self-Service. Pour plus d'informations et d'instructions, reportez-vous au Guide de l'utilisateur UEM Self-Service.

Activation d'une tablette ou d'un ordinateur Windows 10

Pour activer des terminaux Windows 10, envoyez les instructions suivantes à leurs utilisateurs. Veuillez noter que si vous souhaitez gérer des terminaux Windows 10 auxquels est attribué le type d'activation Contrôles MDM, ils ne pourront pas être gérés par Microsoft System Center Configuration Manager.

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

Avant de commencer : Vérifiez que vous avez reçu un e-mail d'activation contenant l'adresse d'un serveur de certificats. Si vous n'avez pas reçu l'e-mail, contactez votre administrateur.

1. Dans le navigateur de votre terminal, saisissez ou collez l'adresse du serveur de certificats.
2. Cliquez sur **Enregistrer**.
3. Dans la notification de téléchargement du certificat, cliquez sur **Ouvrir**.
4. Cliquez sur **Ouvrir**.
5. Cliquez sur **Installer le certificat**.
6. Sélectionnez l'option **Utilisateur actuel** et cliquez sur **Suivant**.
7. Sélectionnez l'option **Placer tous les certificats dans le magasin suivant** et cliquez sur **Parcourir**.
8. Sélectionnez **Autorités de certification racine approuvées** et cliquez sur **OK**.
9. Cliquez sur **Suivant > Terminer > OK > OK**.
10. Cliquez sur le bouton **Démarrer**.
11. Effectuez l'une des opérations suivantes :

Version du SE du terminal	Étapes
Windows 10 version 1607 ou ultérieure	**a.** Sélectionnez **Paramètres > Comptes > Accès professionnel ou scolaire**. **b.** Sélectionnez **S'inscrire uniquement dans la gestion des terminaux**.
Version de Windows 10 antérieure à la version 1607	**a.** Sélectionnez **Paramètres > Comptes > Accès professionnel**. **b.** Sélectionnez **Se connecter**.

12. Dans le champ **Adresse e-mail**, saisissez votre adresse électronique et sélectionnez **Continuer**.
13. Si vous y êtes invité, dans le champ **Serveur**, saisissez le nom du serveur, puis sélectionnez **Continuer**. Vous trouverez le nom du serveur dans l'e-mail d'activation que vous avez reçu de votre administrateur ou dans BlackBerry UEM Self-Service lors de la définition de votre mot de passe d'activation.
14. Dans le champ **Mot de passe d'activation**, saisissez votre mot de passe d'activation, puis sélectionnez **Continuer**. Vous trouverez votre mot de passe d'activation dans l'e-mail d'activation que vous avez reçu de votre administrateur. Vous pouvez aussi définir votre propre mot de passe d'activation dans UEM Self-Service.
15. Sélectionnez **Terminé**.

À la fin :

- Pour vérifier que le processus d'activation s'est bien déroulé, effectuez l'une des opérations suivantes :
  - Sur votre terminal, cliquez sur Paramètres > Comptes > Accès professionnel ou scolaire (ou Accès professionnel) pour vérifier que votre terminal est connecté à UEM.
  - Dans 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.
- Si votre administrateur vous y invite, ajoutez votre compte professionnel aux Comptes utilisés par d'autres applications afin d'avoir accès aux applications en ligne requises.

- Pour Windows 10 1607 ou version ultérieure, cliquez sur Paramètres > Comptes > Accès professionnel ou scolaire > Se connecter. Saisissez votre adresse électronique professionnelle et votre mot de passe.
- Pour les versions de Windows 10 antérieures à la version 1607, cliquez sur Paramètres > Comptes > Votre e-mail et vos comptes. Sous Comptes utilisés par d'autres applications, cliquez sur Ajouter un compte professionnel ou scolaire, puis saisissez votre adresse électronique professionnelle et votre mot de passe.

Configurer la prise en charge de l'inscription sans intervention Android

Vous pouvez utiliser l'inscription sans intervention Android de BlackBerry UEM pour déployer simultanément un grand nombre de terminaux Android Enterprise. Les terminaux doivent prendre en charge l'inscription sans intervention.

Lorsque votre entreprise achète des terminaux pris en charge auprès d'un revendeur d'entreprise agréé, il configure un compte d'inscription sans intervention et ajoute les terminaux à ce compte. Lorsqu'un utilisateur définit l'un de ces terminaux pour la première fois ou réinitialise les paramètres d'usine d'un terminal, le terminal télécharge automatiquement BlackBerry UEM Client et démarre le processus d'activation d'UEM.

Notez que si l'utilisateur redémarre le terminal avant la fin de l'activation, annule l'activation ou laisse la batterie se décharger avant la fin de l'activation, le terminal rétablit automatiquement les paramètres d'usine et le processus d'activation redémarre.

1. Dans la barre de menus de la console de gestion, cliquez sur **Paramètres > Intégration externe**.
2. Cliquez sur **Android Enterprise**.
3. Cliquez sur **Lancer la console d'inscription sans intervention**.
4. Si c'est la première fois que vous vous connectez à Android Zero Touch avec UEM, cliquez sur **Suivant** et connectez-vous à Google en utilisant l'adresse associée au compte d'inscription sans intervention de votre organisation.
5. Créez ou gérez les configurations d'inscription et attribuez-les aux terminaux.

   Vous pouvez également utiliser le portail d'inscription sans intervention Android pour y gérer les configurations d'inscription.

À la fin :

- Dans UEM, vérifiez que les profils et les stratégies informatiques appropriés sont attribués aux utilisateurs. Pour utiliser l'inscription sans intervention, vous devez attribuer un profil d'activation avec le type d'activation Travail et Personnel - Contrôle total (Android Enterprise) ou Espace Travail uniquement (Android Enterprise) activé.
- Distribuez les terminaux aux utilisateurs.

Activation de plusieurs terminaux à l'aide de Knox Mobile Enrollment

Samsung Knox Mobile Enrollment permet de déployer simultanément un grand nombre de terminaux Samsung Knox. Votre entreprise achète les terminaux auprès d'un revendeur agréé ou d'un revendeur qui souhaite partager les IMEI des terminaux directement avec Samsung afin que le terminal puisse utiliser Knox Mobile Enrollment. Lorsqu'un utilisateur définit l'un de ces terminaux pour la première fois ou réinitialise les paramètres d'usine d'un terminal, le terminal télécharge automatiquement BlackBerry UEM Client et démarre le processus d'activation BlackBerry UEM.

Notez que si l'utilisateur redémarre le terminal avant la fin de l'activation, annule l'activation ou laisse la batterie se décharger avant la fin de l'activation, le terminal rétablit automatiquement les paramètres d'usine et le processus d'activation redémarre.

Remarque : Knox Mobile Enrollment ne prend pas en charge l'inscription basée sur l'administration du terminal sur les terminaux exécutant Android 11 ou version ultérieure. Pour plus d'informations, reportez-vous aux notes de mise à jour KNOX Mobile Enrollment 1.36.

1. Sur la barre de menus de la console de gestion, cliquez sur **Paramètres > Intégration externe > KNOX Mobile Enrollment**.
2. Téléchargez le fichier JSON UEM.
3. Suivez les instructions qui s'affichent à l'écran.

À la fin : Une fois l'activation terminée, à l'aide du fichier JSON que vous avez téléchargé, comparez l'entrée de la section CFPrint à l'entrée que vous avez ajoutée lorsque vous avez configuré Knox Mobile Enrollment. Si ces entrées sont différentes, dans le champ **Données JSON personnalisées** de la page Knox Mobile Enrollment, copiez l'intégralité du texte du fichier .json.

Activation de terminaux iOS inscrits dans DEP

Vous pouvez inscrire des terminaux iOS et iPadOS dans le Programme d'inscription des terminaux (DEP) Apple et leur attribuer des configurations d'inscription dans la console de gestion BlackBerry UEM. Les configurations d'inscription comprennent des règles supplémentaires attribuées aux terminaux lors de l'inscription MDM.

Vous pouvez utiliser un compte Apple Business Manager pour synchroniser UEM avec le DEP. Apple Business Manager est un portail Web qui vous permet d'inscrire et de gérer des terminaux iOS dans le DEP, et de gérer des comptes VPP Apple. Si votre organisation utilise DEP ou VPP, vous pouvez effectuer une mise à niveau vers Apple Business Manager.

Pour activer des terminaux inscrits dans le DEP, procédez comme suit :

Étape	Action
1	Enregistrer les terminaux iOS dans DEP et les attribuer au serveur BlackBerry UEM.
2	Ajout d'une configuration d'inscription DEP.
3	Pour ajouter BlackBerry UEM Client à la liste des applications et l'attribuer à des comptes d'utilisateur ou à des groupes d'utilisateurs, vous pouvez également consulter Ajout d'une application iOS à la liste des applications.
4	Si vous ne souhaitez pas utiliser le profil d'activation par défaut, créez un profil d'activation et attribuez-le aux terminaux DEP (Utilisateurs > Terminaux DEP Apple).
5	Choisissez la manière dont vous souhaitez que les utilisateurs activent leurs terminaux : • Envoyer un e-mail d'activation à plusieurs utilisateurs ou envoyez un e-mail d'activation à un utilisateur spécifique à l'aide du modèle d'e-mail Apple DEP. • Si vous avez connecté UEM à votre répertoire d'entreprise, les utilisateurs peuvent utiliser leurs noms d'utilisateur et mots de passe de répertoire d'entreprise. Les utilisateurs doivent saisir leurs noms d'utilisateur au format domaine\nom d'utilisateur (les informations d'identification correspondent aux variables de domaine et de nom d'utilisateur de votre organisation ("%UserDomain%/%UserName%"). • Vous pouvez Attribution d'un utilisateur à un terminal iOS. Lorsque vous attribuez un utilisateur au terminal dans UEM, celui-ci n'est pas invité à saisir un nom d'utilisateur ou un mot de passe lors de l'activation du terminal.
6	Distribuez les terminaux aux utilisateurs et demandez-leur de terminer l'activation. À l'issue de l'activation, les utilisateurs doivent installer et ouvrir UEM Client.

Enregistrer les terminaux iOS dans DEP et les attribuer au serveur BlackBerry UEM

Pour enregistrer les terminaux iOS dans le DEP (Device Enrollment Program) Apple, vous devez saisir les numéros de série de ces terminaux dans le portail Apple Business Manager DEP et attribuer les terminaux au serveur BlackBerry UEM. Pour saisir les numéros de série, vous pouvez saisir chaque numéro, sélectionner

le numéro de commande attribué par Apple aux terminaux lorsque vous les avez achetés, ou télécharger un fichier .csv contenant les numéros de série.

Avant de commencer : Configuration de BlackBerry UEM pour DEP.

1. Connectez-vous au portail Apple Business Manager ou DEP.
2. Dans la section **Programme d'inscription de terminaux**, cliquez sur **Gérer les terminaux**.
3. Pour saisir les numéros de série du terminal, suivez les étapes indiquées à l'écran.
4. Attribuez les numéros de série au serveur UEM.

À la fin : Ajout d'une configuration d'inscription DEP.

Ajout d'une configuration d'inscription DEP

La configuration d'inscription vous permet de déterminer la configuration des terminaux inscrits dans le DEP lorsqu'ils sont activés avec BlackBerry UEM. Vous pouvez créer autant de configurations d'inscription que nécessaires à votre entreprise.

Avant de commencer : Enregistrer les terminaux iOS dans DEP et les attribuer au serveur BlackBerry UEM.

1. Sur la barre de menus de la console de gestion, cliquez sur **Paramètres > Intégration externe > Programme d'inscription de terminaux Apple**.
2. Cliquez sur le nom d'un compte DEP.
3. Dans la section **Configurations d'inscription DEP**, cliquez sur +.
4. Saisissez un nom pour la configuration.
5. Si vous souhaitez qu'UEM attribue automatiquement la configuration d'inscription lorsque les terminaux DEP sont synchronisés avec UEM, cochez la case **Attribuer automatiquement tous les nouveaux terminaux à cette configuration**.

   UEM est synchronisé avec Apple DEP sur une base quotidienne et à chaque fois que vous affichez la page de terminaux DEP Apple. Vous ne pouvez sélectionner qu'une seule configuration d'inscription à attribuer aux nouveaux terminaux DEP. Si vous avez déjà créé une configuration d'inscription avec ce paramètre, ce dernier est supprimé de la configuration précédente et ajouté à la nouvelle. Si vous avez déjà créé une configuration d'inscription avec ce paramètre et que cette configuration a été appliquée aux terminaux, UEM n'attribue pas la nouvelle configuration d'inscription.
6. Vous avez la possibilité de saisir un nom de service et le numéro de téléphone de l'assistance qui s'afficheront sur les terminaux au cours de la configuration.
7. Dans la section **Configuration du terminal**, sélectionnez l'une des options suivantes :
   - **Autoriser le couplage** : les utilisateurs peuvent coupler le terminal à un ordinateur.
   - **Obligatoire** : les utilisateurs ne sont pas invités à accepter la configuration d'inscription.
   - **Autoriser la suppression du profil MDM** : les utilisateurs peuvent désactiver les terminaux.
   - **Attendre que le terminal soit configuré** : les utilisateurs ne peuvent pas annuler la configuration du terminal tant que le processus d'activation n'est pas terminé.
8. Dans la section **Ignorer pendant la configuration**, sélectionnez les éléments que vous ne souhaitez pas inclure dans la configuration des terminaux :

Option	Impact si sélectionné
Mot de passe	Les utilisateurs ne sont pas invités à créer un mot de passe pour le terminal.

Option	Impact si sélectionné
Services de localisation	Les services de localisation sont désactivés sur le terminal.
Restaurer	Les utilisateurs ne peuvent pas restaurer les données à partir d'un fichier de sauvegarde.
Déplacer depuis Android	Les données ne peuvent pas être restaurées depuis un terminal Android.
ID Apple	Les utilisateurs ne peuvent pas se connecter avec Apple ID et iCloud.
Conditions d'utilisation	Les utilisateurs ne voient pas les conditions d'utilisation iOS.
Siri	Siri est désactivé sur les terminaux.
Diagnostics	Les informations de diagnostic ne sont pas envoyées automatiquement par le terminal lors de la configuration.
Biométrique	Les utilisateurs ne peuvent pas configurer Touch ID.
Paiement	Les utilisateurs ne peuvent pas configurer Apple Pay.
Zoom	Les utilisateurs ne peuvent pas configurer Zoom.
Configuration de l'icône de l'écran d'accueil	Les utilisateurs ne peuvent pas régler le clic sur l'icône de l'écran d'accueil.
Temps d'écran	L'option de configuration du temps d'écran est ignorée lors de l'inscription DEP.
Mise à jour logicielle	Les utilisateurs ne voient pas l'écran de mise à jour obligatoire du logiciel sur le terminal.
iMessage et FaceTime	Les utilisateurs ne voient pas iMessage et l'écran FaceTime sur le terminal.
Ton d'affichage	Les utilisateurs ne voient pas l'écran Ton d'affichage sur le terminal.
Confidentialité	Les utilisateurs ne voient pas l'écran Confidentialité sur le terminal.
Intégration	Les utilisateurs ne voient pas l'écran d'intégration sur le terminal.
Migration Watch	Les utilisateurs ne voient pas l'écran Migration Watch sur le terminal.
Configuration SIM	Les utilisateurs ne voient pas l'écran permettant de configurer un forfait cellulaire sur le terminal.
Migration terminal à terminal	Les utilisateurs ne voient pas l'écran Migration terminal à terminal sur le terminal.

9. Cliquez sur **Enregistrer**. Si vous avez coché la case **Attribuer automatiquement de nouveaux terminaux à cette configuration**, cliquez sur **Oui**.

À la fin :

- Si vous n'avez pas coché la case **Attribuer automatiquement de nouveaux terminaux à cette configuration**, vous devez attribuer la configuration d'inscription qui convient aux terminaux. Sous **Utilisateurs > Terminaux DEP Apple**, sélectionnez les terminaux inscrits sur le même compte DEP et cliquez sur . Sélectionnez et attribuez la configuration d'inscription.
- Si vous ne souhaitez pas utiliser le profil d'activation par défaut, créez un profil d'activation et attribuez-le aux terminaux inscrits dans Apple DEP. Sous **Utilisateurs > Terminaux DEP Apple**, sélectionnez les terminaux inscrits sur le même compte DEP et cliquez sur . Sélectionnez et attribuez le profil.
- Lors de l'activation du terminal, les utilisateurs peuvent être invités à saisir un nom d'utilisateur et un mot de passe. Choisissez la manière dont vous souhaitez que les utilisateurs activent leurs terminaux :
  - Envoyer un e-mail d'activation à plusieurs utilisateurs ou envoyez un e-mail d'activation à un utilisateur spécifique à l'aide du modèle d'e-mail Apple DEP.
  - Si vous avez connecté UEM à votre répertoire d'entreprise, les utilisateurs peuvent utiliser leurs noms d'utilisateur et mots de passe de répertoire d'entreprise. Les utilisateurs doivent saisir leurs noms d'utilisateur au format domaine\nom d'utilisateur (les informations d'identification correspondent aux variables de domaine et de nom d'utilisateur de votre organisation ("%UserDomain%/%UserName%").
  - Vous pouvez Attribution d'un utilisateur à un terminal iOS. Lorsque vous attribuez un utilisateur au terminal dans UEM, celui-ci n'est pas invité à saisir un nom d'utilisateur ou un mot de passe lors de l'activation du terminal.
- Distribuez les terminaux aux utilisateurs et demandez-leur de terminer l'activation. À l'issue de l'activation, les utilisateurs doivent installer et ouvrir BlackBerry UEM Client.

Attribution d'un utilisateur à un terminal iOS

Vous pouvez attribuer un utilisateur directement à un terminal enregistré dans Apple DEP avant l'activation du terminal. Lorsque vous attribuez un utilisateur directement au terminal, il n'est pas invité à saisir un nom d'utilisateur ou un mot de passe lors de l'activation du terminal.

1. Sur la barre de menus, cliquez sur **Utilisateurs > Terminaux DEP Apple**.
2. Dans la colonne **Association d'utilisateurs** du terminal que vous souhaitez attribuer, cliquez sur **Sélectionner**.
3. Dans la zone de recherche **Sélectionner un utilisateur**, recherchez l'utilisateur que vous souhaitez attribuer au terminal.
4. Dans la liste des résultats de la recherche, cliquez sur le compte d'utilisateur.
5. Cliquez sur **Enregistrer**.

À la fin :

- Pour afficher le propriétaire d'un terminal activé, dans la colonne **Association d'utilisateurs**, cliquez sur le lien du nom d'utilisateur.
- Pour supprimer un utilisateur d'un terminal iOS, dans la colonne **Association d'utilisateurs**, cliquez sur le lien du nom d'utilisateur du terminal à partir duquel vous souhaitez supprimer l'utilisateur. Cliquez sur **Désattribuer**.

Activer des terminaux iOS à l'aide de Apple Configurator 2

Si vous disposez de BlackBerry UEM sur site, vous pouvez utiliser Apple Configurator 2 pour préparer les terminaux iOS et iPadOS à l'activation. Les utilisateurs peuvent activer les terminaux préparés sans utiliser BlackBerry UEM Client. Les utilisateurs ont uniquement besoin de leur nom d'utilisateur et du mot de passe d'activation.

Apple Configurator n'est pas pris en charge par UEM Cloud.

Remarque : Certaines fonctionnalités UEM impliquent l'attribution de UEM Client à des utilisateurs. Les utilisateurs doivent lancer UEM Client après avoir activé le terminal. Pour plus d'informations, consultez l'article KB 39313.

Pour activer les terminaux iOS à l'aide de Apple Configurator 2, procédez comme suit :

Étape	Action
1	Vous pouvez également ajouter UEM Client à la liste des applications et l'attribuer à des groupes ou comptes d'utilisateurs. Consultez la section Ajouter une application iOS à la liste des applications.
2	Ajouter les informations relatives au serveur BlackBerry UEM dans Apple Configurator 2.
3	Préparer les terminaux iOS à l'aide de Apple Configurator 2.
4	Créez un profil d'activation et attribuez-le à un compte d'utilisateur ou à un groupe d'utilisateurs.
5	Envoyer un e-mail d'activation à plusieurs utilisateurs ou envoyez un e-mail d'activation à un utilisateur spécifique.
6	Distribuez les terminaux aux utilisateurs et demandez-leur de terminer l'activation. Pour appliquer un profil de conformité, les utilisateurs doivent installer et ouvrir UEM Client à l'issue de l'activation.

Ajouter les informations relatives au serveur BlackBerry UEM dans Apple Configurator 2

Avant de commencer : Téléchargez et installez la dernière version de Apple Configurator 2 à partir de Apple.

1. Dans le menu de Apple Configurator 2, sélectionnez **Préférences > Serveurs**.
2. Cliquez sur + > **Suivant**.
3. Dans le champ **Nom**, saisissez un nom pour le serveur.
4. Dans le champ **Nom d'hôte ou URL**, saisissez l'URL du serveur UEM au format *<http or https>://<servername>:<port>*, sachant que le numéro de port par défaut est 8885.

5. Cliquez sur **Suivant**.
6. Fermez la fenêtre **Serveur**.

À la fin : Préparer les terminaux iOS à l'aide de Apple Configurator 2.

Préparer les terminaux iOS à l'aide de Apple Configurator 2

Lorsque vous préparez un terminal, Apple Configurator 2 le nettoie et procède à une mise à niveau du système d'exploitation vers la version la plus récente.

Avant de commencer : Ajouter les informations relatives au serveur BlackBerry UEM dans Apple Configurator 2.

1. Ouvrez Apple Configurator 2.
2. Connectez un ou plusieurs terminaux iOS à votre ordinateur.
3. Cliquez sur **Préparer**.
4. Dans la liste déroulante **Configuration**, sélectionnez **Manuelle**. Cliquez sur **Suivant**.
5. Dans la liste déroulante **Serveur**, sélectionnez le serveur BlackBerry UEM. Cliquez sur **Suivant**.
6. Vous pouvez également cocher la case **Superviser les terminaux**. Cliquez sur **Suivant**.
7. Si vous avez sélectionné **Superviser les terminaux**, entrez les informations relatives à l'entreprise.
8. Cliquez sur **Préparer** et attendez que le terminal soit prêt. Le processus peut prendre une quinzaine de minutes.

À la fin : Distribuez les terminaux aux utilisateurs à des fins d'activation.

Importer ou exporter une liste d'ID de terminal approuvés

Vous pouvez importer et exporter une liste d'identifiants de terminaux uniques pour limiter les terminaux pouvant être inscrits auprès de BlackBerry UEM. Actuellement, le seul identifiant unique pris en charge par UEM est le numéro de série du terminal.

Avant de commencer : Pour importer une liste, assurez-vous que vous disposez d'un fichier .csv contenant une liste d'identifiants de terminal uniques.

1. Sur la barre de menus de la console de gestion, cliquez sur **Paramètres > Paramètres généraux > Paramètres d'activation par défaut**.
2. Dans la section **Importer ou exporter des ID de terminal**, en regard du champ **Charger les ID de terminal approuvés (.csv)**, cliquez sur **Parcourir**.
3. Accédez au fichier .csv.
4. Cliquez sur **Ouvrir**.
5. Cliquez sur **Enregistrer**.

À la fin : Pour exporter la liste, cliquez sur **Exporter les ID de terminal approuvés (.csv)**.

Désactivation des terminaux

Lorsqu'un terminal est désactivé, la connexion entre le compte d'utilisateur et lui est supprimée dans BlackBerry UEM. 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.

Un terminal peut être désactivé à l'aide de l'une des méthodes suivantes :

- Les administrateurs peuvent désactiver un terminal à partir de la console de gestion UEM à l'aide de la commande Supprimer uniquement les données professionnelles ou Supprimer toutes les données du terminal.
- UEM peut désactiver un terminal si celui-ci enfreint les règles du profil de conformité attribué et si la mesure d'application configurée consiste à désactiver le terminal.
- Les utilisateurs peuvent désactiver un terminal à partir d'UEM Self-Service à l'aide de la commande Supprimer uniquement les données professionnelles ou Supprimer toutes les données du terminal.
- Les utilisateurs peuvent utiliser UEM Client pour désactiver les terminaux iOS et Android.
- Les utilisateurs peuvent désactiver les terminaux Windows 10 à partir de Paramètres > Comptes > Accès professionnel > Supprimer.

Tenez compte des considérations suivantes lorsque vous désactivez des terminaux auxquels sont attribués les types d'activation spécifiés :

Type d'activation	Considérations
Terminaux Android Enterprise avec un profil professionnel uniquement	Vous avez la possibilité de supprimer toutes les données de la carte SD et de supprimer la protection contre la réinitialisation aux paramètres d'usine.
Terminaux Android Enterprise auxquels est attribué le type d'activation Travail et Personnel - Contrôle total	• La commande Supprimer toutes les données du terminal est uniquement prise en charge pour Android 10. À partir de janvier 2024, UEM ne prendra plus en charge Android 10. • La commande Supprimer uniquement les données professionnelles est prise en charge pour Android 11. Cette commande supprime toutes les données et applications professionnelles, mais permet à l'utilisateur de conserver ses données et applications personnelles et de continuer à utiliser le terminal non géré.
Terminaux Android Enterprise avec 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 spécifier un motif qui apparait dans la notification sur le terminal de l'utilisateur. Si le terminal est désactivé pour violation des règles de conformité, la notification spécifie la raison pour laquelle le terminal n'est pas conforme.
Knox MDM	• Les applications internes sont désinstallées. • L'option de désinstallation devient disponible pour toutes les applications publiques qui ont été installées à partir de la liste des applications.
Terminaux Samsung Knox Workspace avec Travail et Personnel - Contrôle total	La désactivation du terminal supprime toutes les données du terminal. Vous pouvez spécifier les données qui seront effacées à l'aide de la règle de stratégie informatique Effacement des données à la désactivation.

Résolution des problèmes d'activation des terminaux

Lorsque vous résolvez des problèmes liés à l'activation d'un terminal, vérifiez systématiquement ce qui suit :

- Vérifiez que les licences sont disponibles pour le type de terminal et le type d'activation.
- Vérifiez que le profil d'activation attribué au terminal prend en charge ce type de terminal.
- Vérifiez la connectivité réseau sur le terminal.
  - Vérifiez que le réseau mobile ou Wi-Fi est actif et dispose d'une couverture suffisante.
  - Si vous utilisez un profil Wi-Fi professionnel, vérifiez que le chemin réseau du terminal est disponible.
  - Si l'utilisateur doit configurer manuellement un profil VPN ou Wi-Fi professionnel pour accéder au contenu situé derrière le pare-feu de votre organisation, vérifiez que les profils de l'utilisateur sont correctement configurés sur le terminal.
- Si vous avez configuré des règles de conformité pour les terminaux dotés d'un système d'exploitation cracké ou débridé, de versions limitées du système d'exploitation ou de modèles de terminaux restreints, vérifiez que le terminal est conforme.
- Si UEM est installé sur site et que le terminal tente de se connecter à UEM ou BlackBerry Infrastructure via le pare-feu de votre organisation, vérifiez que les ports appropriés du pare-feu sont ouverts.
- Collectez les journaux des terminaux. Pour plus d'informations sur la récupération des journaux des terminaux, consultez l'article KB 36986 pour iOS et l'article KB 32516 pour Android.

Terminaux Android Management

- Vous devez créer des profils d'activation distincts pour Android Enterprise et Android Management. Si Android Enterprise et les types d'activation Android Management sont spécifiés dans le même profil, le type Android Management est prioritaire, même s'il est classé plus bas que Android Enterprise. Seuls le mot de passe et les informations d'activation pour le type d'activation Android Management seront intégrés au QR Code.
- Sur certains terminaux, un écran Configuration et restauration inutile peut s'afficher une fois le processus d'activation terminé avec succès.

Terminaux Knox Workspace et Android Enterprise

Lorsque vous résolvez les problèmes d'activation des terminaux Samsung utilisant Samsung Knox Workspace, vérifiez que la version du conteneur Knox est prise en charge. Knox Workspace requiert Knox Container 2.0 ou version ultérieure.

Lorsque vous résolvez les problèmes d'activation des terminaux Android Enterprise, vérifiez que le compte d'utilisateur UEM possède la même adresse e-mail que dans le domaine Google. Si ces adresses électroniques ne correspondent pas, le terminal affichera l'erreur : Impossible d'activer le terminal - Type d'activation non pris en charge.

Dépannage : erreurs et problèmes d'activation

Erreurs d'activation

Erreur	Solution possible
Impossible de terminer l'activation du terminal en l'absence de licences suffisantes sur le serveur. Pour obtenir de l'aide, contactez votre administrateur.	Dans la console de gestion UEM, vérifiez que les licences sont disponibles. Si nécessaire, activez les licences ou achetez des licences supplémentaires.
Impossible d'installer le profil. Le certificat AutoMDMCert.pfx n'a pas pu être importé.	Cette erreur s'affiche sur un terminal iOS présentant déjà un profil. Accédez à **Paramètres > Général > Profils** sur le terminal et vérifiez qu'un profil existe déjà. Supprimez le profil et essayez de l'activer à nouveau. Si le problème persiste, vous devrez peut-être réinitialiser le terminal car il est possible que des données aient été mises en cache.
Échec de l'installation du profil : la nouvelle charge utile MDM ne correspond pas à l'ancienne charge utile.	Cette erreur s'affiche sur un terminal iOS présentant déjà un profil. Accédez à **Paramètres > Général > Profils** sur le terminal et vérifiez qu'un profil existe déjà. Supprimez le profil et essayez de l'activer à nouveau. Si le problème persiste, vous devrez peut-être réinitialiser le terminal car il est possible que des données aient été mises en cache.
Erreur 3007 : le serveur n'est pas disponible	Cette erreur peut se produire si le certificat utilisé par UEM pour signer le profil MDM envoyé à un terminal iOS n'est pas approuvé par celui-ci (l'utilisateur est invité à approuver ce certificat lorsqu'il active le terminal). Dans un environnement sur site, installez le certificat racine de l'autorité de certification qui a émis le certificat. Consultez Modification des certificats utilisés par BlackBerry UEM pour l'authentification dans le contenu relatif à la configuration. Cette erreur peut se produire si vous configurez un proxy transparent tel que Blue Coat et qu'il surveille le port 443 afin de détecter tout trafic non standard et que UEM Client ne peut pas passer les appels HTTP CONNECT et HTTP OPTIONS requis auprès d'UEM. Vérifiez que votre configuration de proxy n'empêche pas UEM Client de passer ces appels.
Impossible de contacter le serveur. Vérifiez la connectivité ou l'adresse du serveur.	Cette erreur peut se produire si le nom d'utilisateur (ou l'adresse du client si l'enregistrement auprès de BlackBerry Infrastructure a été désactivé) n'a pas été saisi correctement ou si le mot de passe d'activation n'a pas été défini ou a expiré. Vérifiez que le nom d'utilisateur, le mot de passe et l'adresse du client (le cas échéant) sont corrects, ou définissez un nouveau mot de passe d'activation avec UEM Self-Service et réessayez.

Problèmes d'activation

Problème	Solution possible
Les activations des terminaux iOS ou macOS échouent en présence d'un certificat APNs non valide.	Le certificat APNs peut ne pas être correctement installé. Effectuez une ou plusieurs des opérations suivantes : • Sur la barre de menus de la console de gestion, cliquez sur **Paramètres > Intégration externe > Apple Push Notification**. Vérifiez que l'état du certificat APNs indique Installé. Si cet état est incorrect, essayez à nouveau d'enregistrer le certificat APNs. • Pour tester la connexion entre UEM et le serveur APNs, cliquez sur **Certificat APNs test**. • Si nécessaire, procurez-vous un nouveau fichier CSR signé auprès de BlackBerry, et demandez et enregistrez un nouveau certificat APNs. Pour plus d'informations, consultez Obtention d'un certificat APNs pour gérer les terminaux iOS et macOS dans le contenu relatif à la configuration.
Les utilisateurs ne reçoivent pas d'e-mail d'activation.	Si les utilisateurs ont recours à un serveur de messagerie tiers, les e-mails provenant de UEM peuvent être marqués comme spams et finir dans le dossier des spams ou le dossier du courrier indésirable.
L'écran de détails utilisateur d'UEM montre plus de terminaux Windows activés que prévu.	Lorsqu'un utilisateur installe BlackBerry Access et BlackBerry Work pour Windows sur un ordinateur, ces applications s'affichent en tant que terminal Windows sur l'écran de détails utilisateur. Ce comportement est normal.

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