BlackBerry UEM

Gestion des terminaux iOS

Administration

12.16

Contents

Gestion des terminaux iOS et iPadOS

BlackBerry UEM permet une gestion précise de la façon dont les terminaux iOS et iPadOS se connectent à votre réseau, des capacités des terminaux qui sont activés et des applications qui sont disponibles. Que les terminaux appartiennent à votre organisation ou à vos utilisateurs, vous pouvez fournir un accès mobile aux informations de votre organisation tout en les protégeant des personnes qui ne devraient pas y avoir accès.

Apple a introduit iPadOS en tant que système d'exploitation distinct à partir iPadOS de la version 13. En raison des nombreuses similitudes entre iOS et iPadOS, presque toutes les fonctionnalités BlackBerry UEM et la documentation qui s'appliquent à iOS s'appliquent également à iPadOS.

Ce guide décrit les options à votre disposition pour gérer les terminaux iOS et iPadOS, et vous permet d'obtenir les informations dont vous avez besoin pour tirer pleinement parti de toutes les fonctionnalités disponibles.

Gestion d'autres terminaux Apple

Vous pouvez également activer et gérer les terminaux macOS et Apple TV dans BlackBerry UEM. Apple TV est un lecteur multimédia numérique qui peut recevoir des données et les diffuser sur un téléviseur via un câble HDMI.

BlackBerry UEM prend en charge les versions Apple TV de deuxième génération ou les générations ultérieures. Pour plus d'informations sur les versions macOS prises en charge, reportez-vous à la Matrice de compatibilité. Pour gérer les terminaux Apple TV, suivez les instructions et utilisez les paramètres de profil des terminaux iOS. Les fonctionnalités suivantes BlackBerry UEM sont prises en charge pour Apple TV :

- Activation du terminal à l'aide de BlackBerry UEM Self-Service
- Type d'activation Commandes MDM
- Wi-Fi et profils de certificat
- Profils du mode de verrouillage des applications
- Commandes de terminaux

Pour empêcher les utilisateurs d'activer des terminaux Apple TV, définissez la restriction des modèles de terminaux dans le profil d'activation pour ne pas autoriser les terminaux Apple TV. Pour plus d'informations sur l'activation des terminaux macOS et Apple TV, reportez-vous au contenu relatif à l'activation de terminaux.

Fonctions que vous pouvez contrôler sur les terminaux iOS

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

Niveau de contrôle	Description
Les terminaux non gérés et partiellement gérés (terminaux activés sur BlackBerry UEM mais pas entièrement gérés)	Vous pouvez activer un terminal sur BlackBerry UEM pour sécuriser l'accès à des ressources professionnelles sans gérer entièrement le terminal. Cette option est souvent utilisée pour les terminaux BYOD. Ces activations peuvent permettre aux utilisateurs d'accéder à votre réseau via un VPN en utilisant BlackBerry 2FA, de partager des fichiers de façon sécurisée à l'aide de BlackBerry Workspaces, et d'installer des applications BlackBerry Dynamics comme BlackBerry Work et BlackBerry Access pour accéder aux e-mails et à votre intranet professionnel.
Terminaux partiellement gérés avec profil professionnel	Vous pouvez activer un terminal sur BlackBerry UEM pour sécuriser l'accès à des ressources professionnelles dans un profil professionnel. Cette option est souvent utilisée pour les terminaux BYOD. Avec ce type d'activation, un espace Travail distinct est créé 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.
Terminaux gérés (terminaux gérés par BlackBerry UEM)	Vous pouvez activer un terminal afin de le gérer entièrement par BlackBerry UEM. Cette option est souvent utilisée pour les appareils appartenant à une entreprise. Cette option vous permet de gérer les données professionnelles à l'aide de commandes et de règles de stratégie informatique. Vous pouvez gérer les applications professionnelles sur le terminal, y compris les applications BlackBerry Dynamics. BlackBerry UEM prend en charge la gestion des terminaux iOS surveillés. Certaines règles de stratégie informatique sont prises en charge uniquement sur les terminaux supervisés

Les **activations Confidentialité de l'utilisateur** peuvent fournir des capacités limitées de gestion des terminaux et permettre aux utilisateurs d'accéder aux données professionnelles à l'aide des applications BlackBerry Dynamics, telles que BlackBerry Work et BlackBerry Access. Vous pouvez choisir d'autoriser certaines des fonctions de gestion des terminaux suivantes :

- Accès à la carte SIM et aux informations matérielles du terminal : Permet d'autoriser l'accès BlackBerry UEM aux informations sur la carte SIM et le matériel du terminal pour activer la licence SIM.
- Gestion des applications : permet d'autoriser les administrateurs à installer ou supprimer des applications professionnelles et à afficher une liste des applications professionnelles installées dans l'écran de détails utilisateur.
- Gestion des stratégies informatiques : permet d'autoriser l'application d'un ensemble limité de règles de stratégie informatique au terminal (règles de mot de passe, autoriser les captures d'écran, autoriser les

documents issus de sources non gérées dans les destinations gérées, et autoriser les documents provenant de sources non gérées dans des destinations gérées).
- Gestion des profils de messagerie : permet d'autoriser l'application de profils de messagerie sur le terminal.
- Gestion des profils Wi-Fi : permet d'autoriser l'application de profils Wi-Fi sur le terminal.
- Gestion des profils VPN : permet d'autoriser l'application de profils VPN sur le terminal.

Les activations **Confidentialité de l'utilisateur - Inscription de l'utilisateur** permettent de préserver la confidentialité des données utilisateur et de les séparer des données professionnelles. Avec ce type d'activation, un espace Travail distinct est installé sur le terminal pour les applications professionnelles et certaines applications natives. 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 non supervisés exécutant iOS ou iPadOS OS 13.1 ou versions ultérieures.

Les **activations Contrôles MDM** offrent une prise en charge complète de la gestion des terminaux iOS, y compris les fonctionnalités suivantes :

- Appliquer les exigences de mot de passe
- Contrôler les capacités des terminaux à l'aide de stratégies informatiques (par exemple, vous pouvez désactiver la caméra ou Bluetooth)
- Appliquer les règles de conformité
- Profils de connexion Wi-Fi et VPN (avec proxy)
- Synchroniser les e-mails, contacts et calendriers avec les terminaux
- Envoyer des certificats d'AC et de client aux terminaux pour l'authentification et S/MIME
- Gérer les applications publiques et internes requises et autorisées, y compris les applications BlackBerry Dynamics.
- Prise en charge complète de Apple pour DEP et VPP
- Localiser et protéger les terminaux perdus ou volés

Remarque : Certaines fonctionnalités et applications BlackBerry Dynamics ne sont pas disponibles avec tous les niveaux de licence. Pour plus d'informations sur les licences disponibles, consultez le contenu relatif aux licences.

Procédure de gestion des terminaux iOS

Étape	Action
1	Installez et configurez BlackBerry UEM conformément aux instructions d'installation sur site ou aux instructions de configuration UEM Cloud. Pour gérer des terminaux iOS et iPadOS vous devez obtenir un certificat APNs auprès d'Apple.
2	Si votre entreprise utilise le Programme d'inscription des appareils (DEP) d'Apple, configurez BlackBerry UEM pour pouvoir utiliser ce programme.
3	Configurez des stratégies informatiques pour les terminaux. Attribuez des stratégies informatiques à des groupes d'utilisateurs ou des utilisateurs individuels.
4	Configurez des profils pour les terminaux. Attribuez des profils à des groupes d'utilisateurs ou des utilisateurs individuels.
5	Si votre organisation dispose d'un compte VPP Apple, ajoutez-le à BlackBerry UEM.
6	Spécifiez les applications que les terminaux peuvent ou doivent installer.
7	Activez les terminaux
8	Gérez et surveillez les terminaux.

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

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

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

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

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

- Exigences en matière de mot de passe du terminal
- Autoriser les fonctions du terminal telles que l'appareil photo, Bluetooth et Touch ID
- Autoriser les achats App Store et iTunes Store, et les classements de contenu autorisés pour les achats
- Autoriser les applications système, telles que Safari, Siri et FaceTime
- Autoriser l'utilisation de iCloud

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

Configuration des exigences relatives à iOS et aux mots de passe

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

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

Règle	Description
Mot de passe requis pour le terminal	Spécifiez si l'utilisateur doit définir un mot de passe pour le terminal.
Accepter les valeurs simples	Spécifiez si le mot de passe peut contenir des caractères séquentiels ou répétés, tels que DEFG ou 3333.
Exiger des valeurs alphanumériques	Spécifiez si le mot de passe doit contenir à la fois des lettres et des chiffres.
Longueur minimum du mot de passe	Précisez la longueur minimale du mot de passe. Si vous entrez une valeur inférieure à la valeur minimale requise par le terminal, la valeur minimale du terminal est utilisée.

Règle	Description
Nombre minimal de caractères complexes	Spécifiez le nombre minimum de caractères non-alphanumériques que doit contenir le mot de passe.
Durée maximum du code (1-730 jours, ou aucun)	Spécifiez le nombre maximum de jours pendant lesquels le mot de passe peut être utilisé.
Verrouillage automatique maximum	Spécifiez la valeur maximum à définir par l'utilisateur pour le verrouillage automatique, qui correspond au nombre de minutes d'inactivité à l'issue desquelles le terminal doit se verrouiller. Si vous définissez cette règle sur Aucun, toutes les valeurs prises en charge sont disponibles sur le terminal. Si la valeur sélectionnée se trouve en dehors de la plage prise en charge par le terminal, celui-ci utilisera la valeur la plus proche qu'il prend en charge.
Historique de code (1-50 codes, ou aucun)	Spécifiez le nombre de mots de passe précédents que le terminal vérifie pour empêcher un utilisateur de réutiliser un mot de passe récent.
Délai de grâce maximum pour le verrouillage du terminal	Spécifiez la valeur maximum que l'utilisateur peut définir pour le délai de grâce relatif au verrouillage du terminal. Il s'agit du délai pendant lequel le terminal peut rester verrouillé avant qu'un mot de passe soit requis pour le déverrouiller. Si vous définissez cette règle sur "Aucun", toutes les valeurs sont disponibles sur le terminal. Si vous définissez cette règle sur "Immédiatement", le mot de passe est requis immédiatement après le verrouillage du terminal.
Nombre maximum d'échecs de tentatives de saisie du mot de passe	Spécifiez le nombre de tentatives de saisie du mot de passe possibles avant la réinitialisation du terminal.
Autoriser les modifications de mot de passe (sous supervision uniquement)	Spécifiez si l'utilisateur peut ajouter, modifier ou supprimer le mot de passe.

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

Contrôle des terminaux à l'aide de profils

BlackBerry UEM comprend plusieurs profils que vous pouvez utiliser pour contrôler divers aspects de la fonctionnalité des terminaux iOS et iPadOS. Les plus couramment utilisés comprennent les profils suivants :

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

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

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

Référence sur les profils : terminaux iOS

Le tableau suivant répertorie tous les profils BlackBerry UEM pris en charge par les terminaux iOS et iPadOS :

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

Nom du profil	Description	Configurer
Conformité	Définit les conditions des terminaux non acceptables dans votre organisation, ainsi que les actions d'exécution.	Créer un profil de conformité
Conformité (BlackBerry Dynamics)	Il s'agit d'un profil en lecture seule qui affiche les paramètres de conformité importés de Good Control dans un BlackBerry UEM sur site.	Gestion des profils de conformité BlackBerry Dynamics
E-mail, calendrier et contacts		
E-mail	Spécifie la manière dont les terminaux se connectent à un serveur de messagerie professionnel et synchronisent les e-mails, les entrées de calendrier et les données de l'organiseur à l'aide d'Exchange ActiveSync ou IBM Notes Traveler.	Créer un profil de messagerie
Messagerie IMAP/ POP3	Spécifie la manière dont les terminaux se connectent à un serveur de messagerie IMAP ou POP3 et synchronisent les e-mails.	Créer un profil de messagerie IMAP/POP3
Contrôle	Spécifie les serveurs Microsoft Exchange à utiliser pour le contrôle d'accès automatique.	Créer un profil de contrôle d'accès
CalDAV	Spécifie les paramètres de serveur que les terminaux peuvent utiliser pour synchroniser les informations de calendrier.	Créer un profil CalDAV
CardDAV	Spécifie les paramètres de serveur que les terminaux peuvent utiliser pour synchroniser les informations de contact.	Créer un profil CardDAV
Réseaux et connexions		
Wi-Fi	Spécifie la manière dont les terminaux se connectent à un réseau Wi-Fi professionnel.	Créer un profil Wi-Fi
VPN	Spécifie la manière dont les terminaux se connectent à un VPN professionnel.	Créer un profil VPN
Proxy	Spécifie la manière dont les terminaux utilisent un serveur proxy pour accéder à des services Web sur Internet ou un réseau professionnel.	Créer un profil proxy
Connectivité d'entreprise	Spécifie si les terminaux peuvent utiliser BlackBerry Secure Connect Plus.	Activer BlackBerry Secure Connect Plus

Nom du profil	Description	Configurer
Connectivité BlackBerry Dynamics	Définit les connexions réseau, les domaines Internet, les plages d'adresses IP et les serveurs d'applications auxquels les terminaux peuvent se connecter lorsqu'ils utilisent des applications BlackBerry Dynamics.	Créer un profil de connectivité BlackBerry Dynamics
BlackBerry 2FA	Active l'authentification à deux facteurs pour les utilisateurs et spécifie la configuration de la préauthentification et les fonctionnalités de résolution autonome.	Créer un profil BlackBerry 2FA
Utilisation du réseau	Vous permet de contrôler si les applications professionnelles peuvent utiliser le réseau mobile ou l'itinérance des données.	Créer un profil d'utilisation du réseau
Filtre de contenu Web	Limite les sites Web qu'un utilisateur peut afficher sur des terminaux supervisés. Terminaux supervisés uniquement.	Créer un profil de filtre de contenu Web
Identification unique	Spécifie la manière dont les terminaux s'authentifient automatiquement auprès des domaines sécurisés après que les utilisateurs ont saisi leur nom d'utilisateur et leur mot de passe pour la première fois.	Créer un profil d'identification unique
Extension d'identification unique	Permet aux terminaux de s'authentifier à l'aide de l'identification unique.	Créer un profil d'extension d'identification unique
Domaines gérés	Configure les terminaux afin de notifier aux utilisateurs l'envoi d'e-mails en dehors des domaines approuvés et limite les applications pouvant afficher des documents téléchargés depuis des domaines internes.	Créer un profil de domaines gérés
AirPrint	Vous permet d'ajouter des imprimantes aux listes d'imprimantes AirPrint des utilisateurs.	Créer un profil AirPrint
AirPlay	Vous permet d'ajouter des terminaux aux listes de terminaux AirPlay des utilisateurs.	Créer un profil AirPlay
Protection		
Protection des applications Microsoft Intune	Vous permet de gérer les applications protégées par Microsoft Intune.	Créer un profil de protection d'application Microsoft Intune
Service de localisation	Vous permet de demander l'emplacement de terminaux et d'afficher les emplacements approximatifs sur une carte.	Créer un profil de service de localisation

Nom du profil	Description	Configurer
Ne pas déranger	Vous permet de bloquer les notifications BlackBerry Work for iOS en dehors des jours et heures de travail que vous définissez.	Créer un profil Ne pas déranger
Personnalisée		
Terminal	Vous permet de configurer les informations qui s'affichent sur les terminaux.	Créer un profil de terminal
Charge utile personnalisée	Spécifie les informations de configuration personnalisée à l'aide du code de charge utile pour les terminaux.	Création d'un profil de charge utile personnalisée
Notification par application	Vous permet de configurer les paramètres de notification des applications système et des applications que vous gérez via BlackBerry UEM. Terminaux supervisés uniquement.	Créer un profil de notification par application
Certificats		
Certificat d'AC	Spécifie un certificat d'AC que les terminaux peuvent utiliser pour établir une relation de confiance avec un réseau ou un serveur professionnel.	Créer un profil de certificat d'autorité de certification partagé
Certificat partagé	Spécifie un certificat client que les terminaux peuvent utiliser pour authentifier les utilisateurs avec un réseau ou un serveur professionnel.	Créer un profil de certificat partagé
Informations d'identification de l'utilisateur	Spécifie la connexion d'AC via laquelle les terminaux peuvent obtenir un certificat client d'authentification avec un réseau ou un serveur professionnel.	Créer un profil d'informations d'identification de l'utilisateur
SCEP	Spécifie le serveur SCEP via lequel les terminaux peuvent obtenir un certificat client permettant une authentification via un réseau ou un serveur professionnel.	Créer un profil SCEP

Gestion des applications sur les terminaux

Vous pouvez créer une bibliothèque d'applications que vous souhaitez gérer et surveiller sur les terminaux. BlackBerry UEM fournit les options suivantes pour la gestion des applications sur les terminaux iOS et iPadOS :

- Attribuez des applications publiques à partir de l'App Store comme des applications optionnelles ou requises sur les terminaux.
- Téléchargez des applications personnalisées vers UEM et déployez-les comme des applications optionnelles ou requises.
- Préconfigurez les paramètres d'application, tels que les paramètres de connexion, lorsque l'application le permet.
- Empêchez les utilisateurs d'accéder à des applications spécifiques ou configurer une liste d'applications autorisées et bloquer toutes les autres applications.
- Associez les comptes VPP Apple à UEM afin de pouvoir distribuer les licences achetées pour les applications associées aux comptes VPP.
- Configurez les applications publiques, ISV et BlackBerry Dynamics personnalisées pour permettre aux utilisateurs d'accéder aux ressources professionnelles.
- Connectez UEM à Microsoft Intune, de sorte que vous puissiez définir les stratégies de protection des applications Intune depuis la console de gestion UEM pour déployer et gérer les applications Office 365.
- Affichez la liste des applications personnelles installées sur les terminaux..
- Permettez aux utilisateurs d'évaluer et de commenter les applications d'autres utilisateurs de votre environnement.
- Configurez les paramètres de notification pour les applications système et les applications que vous gérez via UEM.
- Spécifiez l'icône et le libellé de l'icône Applications professionnelles sur les terminaux.

Comportement des applications sur les terminaux iOS avec des activations Contrôles MDM

Pour les terminaux activés pour BlackBerry Dynamics, le catalogue d'applications professionnelles s'affiche dans BlackBerry Dynamics Launcher si vous avez attribué l'autorisation Fonctionnalité - BlackBerry App Store à l'utilisateur. Pour plus d'informations, reportez-vous à la section Ajouter le catalogue d'applications professionnelles à BlackBerry Dynamics Launcher.

Pour les terminaux iOS et iPadOS activés avec Contrôles MDM, voici ce qui se produit :

Type d'application	Lorsque les applications sont attribuées à un utilisateur	Lorsque les applications sont mises à jour	Lorsque des applications sont désattribuées d'un utilisateur	Lorsque le terminal est supprimé de BlackBerry UEM
Applications publiques dotées d'une disposition obligatoire	Sur les terminaux supervisés, les applications sont installées automatiquement. Si l'application est déjà installée, elle est alors gérée par UEM. Sur les terminaux non supervisés, l'utilisateur est invité à installer les applications. Si les applications sont déjà installées, l'utilisateur est invité à autoriser UEM à gérer les applications. Les applications sont supprimées de la liste « Nouvelles/ Mises à jour » lorsque l'utilisateur affiche les détails (même si l'application n'est pas installée), ou lorsque l'utilisateur installe les applications. Vous pouvez utiliser un profil de conformité pour définir les actions prises si les applications requises ne sont pas installées.	iTunes informe les utilisateurs des mises à jour disponibles. Les applications sont supprimées de la liste « Nouvelles/ Mises à jour » lorsque l'application est mise à jour. (peut prendre jusqu'à une heure) Pour les terminaux qui n'ont pas accès à iTunes, les utilisateurs ne sont pas avertis, mais ils peuvent télécharger la mise à jour à partir du catalogue d'applications si une licence VPP Apple est attribuée au terminal.	Les applications sont automatiquement supprimées sans notification. Les applications n'apparaissent plus dans le catalogue d'applications.	Les applications sont supprimées automatiquement.

Type d'application	Lorsque les applications sont attribuées à un utilisateur	Lorsque les applications sont mises à jour	Lorsque des applications sont désattribuées d'un utilisateur	Lorsque le terminal est supprimé de BlackBerry UEM
Applications publiques dotées d'une disposition facultative	Si des applications sont déjà installées sur des terminaux sous supervision, elles sont alors gérées par UEM. Sur les terminaux non supervisés, l'utilisateur est invité à autoriser UEM pour gérer les applications. L'utilisateur est informé d'une modification au catalogue d'applications. Les applications sont supprimées de la liste « Nouvelles/ Mises à jour » uniquement lorsque l'utilisateur affiche les détails (que l'application soit installée ou non). Les utilisateurs peuvent choisir d'installer les applications.	iTunes informe les utilisateurs des mises à jour disponibles. Les applications sont supprimées de la liste « Nouvelles/ Mises à jour » lorsque l'utilisateur affiche les détails (que l'application soit mise à jour ou non).	Les applications sont automatiquement supprimées sans notification. Les applications n'apparaissent plus dans le catalogue d'applications.	Les applications sont supprimées automatiquement.

Type d'application	Lorsque les applications sont attribuées à un utilisateur	Lorsque les applications sont mises à jour	Lorsque des applications sont désattribuées d'un utilisateur	Lorsque le terminal est supprimé de BlackBerry UEM
Applications internes dotées d'une disposition requise	Sur les terminaux supervisés, les applications sont installées automatiquement. Si l'application est déjà installée, elle est alors gérée par UEM. Sur les terminaux non supervisés, l'utilisateur est invité à installer les applications. Si les applications sont déjà installées, l'utilisateur est invité à autoriser UEM à gérer les applications. Si l'utilisateur annule l'installation, il peut installer des applications du catalogue d'applications. Les applications sont supprimées de la liste « Nouvelles/ Mises à jour » lorsque l'utilisateur affiche les détails (même si l'application n'est pas installée), ou lorsque l'utilisateur installe les applications. Vous pouvez utiliser un profil de conformité pour définir les actions prises si les applications	Les applications sont supprimées de la liste « Nouvelles/ Mises à jour » lorsque l'application est mise à jour.	Les applications sont automatiquement supprimées sans notification. Les applications n'apparaissent plus dans le catalogue d'applications.	Les applications sont supprimées automatiquement.

Type d'application	Lorsque les applications sont attribuées à un utilisateur	Lorsque les applications sont mises à jour	Lorsque des applications sont désattribuées d'un utilisateur	Lorsque le terminal est supprimé de BlackBerry UEM
Applications internes dotées d'une disposition facultative	Si des applications sont déjà installées sur des terminaux sous supervision, elles sont alors gérées par UEM. Sur les terminaux non supervisés, l'utilisateur est invité à autoriser UEM pour gérer les applications. Les applications sont supprimées de la liste « Nouvelles/ Mises à jour » lorsque l'utilisateur affiche les détails (même si l'application n'est pas installée), ou lorsque l'utilisateur installe les applications.	Les applications sont supprimées de la liste « Nouvelles/ Mises à jour » lorsque l'application est mise à jour.	Les applications sont automatiquement supprimées des terminaux activés avec Contrôles MDM sans notification. Les applications ne sont pas supprimées des terminaux activés avec Confidentialité de l'utilisateur. Les applications n'apparaissent plus dans le catalogue d'applications.	Les applications sont supprimées automatiquement.

Comportement des applications sur les terminaux iOS avec des activations Confidentialité de l'utilisateur

Pour les terminaux activés pour BlackBerry Dynamics, le catalogue d'applications professionnelles s'affiche dans BlackBerry Dynamics Launcher si vous avez attribué l'autorisation Fonctionnalité - BlackBerry App Store à l'utilisateur. Pour plus d'informations, reportez-vous à la section Ajouter le catalogue d'applications professionnelles à BlackBerry Dynamics Launcher.

Lorsque vous activez des terminaux iOS et iPadOS avec Confidentialité de l'utilisateur, vous pouvez choisir d'autoriser ou non la gestion des applications. Si vous autorisez la gestion des applications, le comportement des applications pour les activations Confidentialité de l'utilisateur est le même que pour les activations Contrôles

MDM. Si vous n'autorisez pas la gestion des applications pour les terminaux activés avec Confidentialité de l'utilisateur, le comportement suivant se produit :

Type d'application	Lorsque les applications sont attribuées à un utilisateur	Lorsque les applications sont mises à jour	Lorsque des applications sont désattribuées d'un utilisateur	Lorsque le terminal est supprimé de BlackBerry UEM
Applications publiques dotées d'une disposition obligatoire	L'utilisateur n'est pas invité à installer des applications. L'utilisateur doit se rendre sur le catalogue d'applications pour installer les applications requises. Les applications sont supprimées de la liste « Nouvelles/ Mises à jour » lorsque l'utilisateur affiche les détails (même si l'application n'est pas installée), ou lorsque l'utilisateur installe les applications.	iTunes informe les utilisateurs des mises à jour disponibles. Les applications sont supprimées de la liste « Nouvelles/ Mises à jour » lorsque l'application est mise à jour. (peut prendre jusqu'à une heure) Pour les terminaux qui n'ont pas accès à iTunes, les utilisateurs ne sont pas notifiés mais ils peuvent télécharger la mise à jour depuis le catalogue d'applications.	Les applications restent sur le terminal. Les applications n'apparaissent plus dans le catalogue d'applications.	Les applications restent sur le terminal.

Type d'application	Lorsque les applications sont attribuées à un utilisateur	Lorsque les applications sont mises à jour	Lorsque des applications sont désattribuées d'un utilisateur	Lorsque le terminal est supprimé de BlackBerry UEM
Applications publiques dotées d'une disposition facultative	Si l'application est déjà installée, il ne se passe rien. L'utilisateur est informé d'une modification au catalogue d'applications. Les applications sont supprimées de la liste « Nouvelles/ Mises à jour » uniquement lorsque l'utilisateur affiche les détails (que l'application soit installée ou non). Les utilisateurs peuvent choisir d'installer les applications.	iTunes informe les utilisateurs des mises à jour disponibles. Les applications sont supprimées de la liste « Nouvelles/ Mises à jour » lorsque l'utilisateur affiche les détails (que l'application soit mise à jour ou non).	Les applications restent sur le terminal. Les applications n'apparaissent plus dans le catalogue d'applications.	Les applications restent sur le terminal.
Applications internes dotées d'une disposition requise	Si les applications sont déjà installées, l'utilisateur est invité à autoriser UEM à gérer les applications. Les applications sont supprimées de la liste « Nouvelles/ Mises à jour » lorsque l'utilisateur affiche les détails (même si l'application n'est pas installée), ou lorsque l'utilisateur installe les applications.	Les applications sont supprimées de la liste « Nouvelles/ Mises à jour » lorsque l'application est mise à jour.	Les applications restent sur le terminal. Les applications n'apparaissent plus dans le catalogue d'applications.	Les applications restent sur le terminal.

Type d'application	Lorsque les applications sont attribuées à un utilisateur	Lorsque les applications sont mises à jour	Lorsque des applications sont désattribuées d'un utilisateur	Lorsque le terminal est supprimé de BlackBerry UEM
Applications internes dotées d'une disposition facultative	Si les applications sont déjà installées, il ne se passe rien. Les applications sont supprimées de la liste « Nouvelles/ Mises à jour » lorsque l'utilisateur affiche les détails (même si l'application n'est pas installée), ou lorsque l'utilisateur installe les applications.	Les applications sont supprimées de la liste « Nouvelles/ Mises à jour » lorsque l'application est mise à jour.	Les applications restent sur le terminal. Les applications n'apparaissent plus dans le catalogue d'applications.	Les applications restent sur le terminal.

Activation des terminaux iOS

Lorsque vous ou un utilisateur active un terminal iOS ou iPadOS avec BlackBerry UEM, le terminal est associé à BlackBerry UEM pour pouvoir gérer les terminaux et permettre aux utilisateurs d'accéder aux données professionnelles sur leurs terminaux.

Vous pouvez activer des terminaux avec BlackBerry UEM, avec ou sans l'utilisation de Apple Configurator 2, pour préparer les terminaux à l'activation. Pour plus d'informations sur l'utilisation de Apple Configurator 2, consultez Activation des terminaux iOS à l'aide de Apple Configurator 2 dans le contenu relatif à l'administration.

Vous pouvez également inscrire des terminaux dans le Programme d'inscription des terminaux Apple et leur attribuer des configurations d'inscription dans la console de BlackBerry UEM. Les configurations d'inscription comprennent des règles supplémentaires, comme Activer le mode supervisé, attribuées aux terminaux lors de l'inscription MDM. Pour plus d'informations, consultez Activation des terminaux iOS inscrits dans le DEP dans le contenu relatif à l'administration.

Si les terminaux ne sont pas inscrits dans le DEP, vous pouvez toujours empêcher l'activation des terminaux non surveillés à l'aide des paramètres du profil d'activation.

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	Vous pouvez utiliser le type d'activation Confidentialité de l'utilisateur afin de fournir une base de contrôle des terminaux tout en veillant à assurer la confidentialité des données personnelles des utilisateurs. Avec ce type d'activation, aucun conteneur séparé n'est installé sur le terminal, et aucune sécurité supplémentaire n'est fournie pour les données professionnelles. Les terminaux activés avec Confidentialité de l'utilisateur sont activés sur BlackBerry UEM et 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. **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 la gestion de licences basée sur la carte SIM** : cette option spécifie si BlackBerry UEM peut accéder à la carte SIM et aux informations matérielles du terminal, telles que les numéros ICCID et IMEI, pour déterminer si une licence SIM appropriée est disponible. • **Autoriser la gestion des applications** : cette option vous permet de définir si vous souhaitez installer ou supprimer des applications professionnelles sur le terminal, et afficher la liste des applications professionnelles installées sur l'écran Informations sur l'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 profils de messagerie** : 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 Wi-Fi** : Cette option vous permet de définir si les paramètres de profil Wi-Fi qui sont affectés 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	Vous pouvez utiliser le type d'activation Confidentialité de l'utilisateur - Inscription de l'utilisateur pour les terminaux iOS et iPadOS pour 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 iOS et iPadOS 13.1, ou versions ultérieures.
Inscription du terminal pour BlackBerry 2FA uniquement	Ce type d'activation prend en charge la solution BlackBerry 2FA pour les terminaux qui ne sont pas gérés par BlackBerry UEM. Ce type d'activation ne fournit aucune gestion ni aucun contrôle des terminaux, mais permet aux terminaux d'utiliser la fonctionnalité BlackBerry 2FA. Pour utiliser ce type d'activation, vous devez également attribuer le profil BlackBerry 2FA aux utilisateurs. Lorsqu'un terminal est activé, vous pouvez afficher des informations de terminal limitées dans la console de gestion, et vous pouvez désactiver le terminal à l'aide d'une commande. Ce type d'activation est pris en charge uniquement pour les utilisateurs Microsoft Active Directory. Ce type d'activation n'est pris en charge que par les terminaux Apple TV. Pour plus d'informations, reportez-vous au contenu BlackBerry 2FA.

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 indique le nombre et le type de terminaux qu'un utilisateur peut activer et le type d'activation à utiliser pour chaque type de terminal.

Le type d'activation vous permet de configurer le niveau de contrôle dont vous disposez sur les terminaux activés. Vous pouvez par exemple disposer d'un contrôle total sur un terminal que vous attribuez à un utilisateur, ou veiller à n'avoir aucun contrôle sur les données personnelles d'un terminal appartenant à un utilisateur et qu'il apporte au travail.

Le profil d'activation attribué ne s'applique qu'aux terminaux activés par l'utilisateur après que vous avez attribué le 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 aux utilisateurs ou groupes d'utilisateurs.

Créer un profil d'activation

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Stratégie > Activation**.
3. Cliquez sur +.
4. Saisissez le nom et la description du profil.
5. Dans le champ **Nombre de terminaux qu'un utilisateur peut activer**, spécifiez le nombre maximum de terminaux que l'utilisateur peut activer.
6. Dans la liste déroulante **Propriété du terminal**, sélectionnez le paramètre par défaut de la propriété du terminal.
   - Si certains utilisateurs activent des terminaux personnels et d'autres des terminaux professionnels, sélectionnez **Non spécifié**.
   - Sélectionnez **Travail** si la plupart des utilisateurs activent des terminaux professionnels.
   - Sélectionnez **Personnel** si la plupart des utilisateurs activent leurs terminaux personnels.
7. Vous pouvez, à votre convenance, 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.
8. 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. Les types de terminaux que vous ne sélectionnez pas ne sont pas inclus dans le profil d'activation et les utilisateurs ne peuvent pas activer ces terminaux.
9. Procédez comme suit pour chaque type de terminal inclus dans le profil d'activation :
   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. Utilisez cette option pour limiter les terminaux autorisés à certains modèles uniquement.
      - **Ne pas autoriser les modèles de terminaux sélectionnés** : les utilisateurs ne peuvent pas activer les modèles de terminaux que vous spécifiez. Utilisez cette option pour bloquer l'activation de certains modèles ou terminaux de fabricants spécifiques.

      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.

      De nombreuses versions de système d'exploitation antérieures ne sont plus prises en charge par BlackBerry UEM. Vous devez sélectionner une version minimale uniquement si vous ne souhaitez pas prendre en charge la version la plus ancienne actuellement prise en charge par BlackBerry UEM. Pour plus d'informations sur les versions prises en charge, reportez-vous à la Matrice de compatibilité.
   d) Sélectionnez les types d'activation pris en charge.
10. 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. Pour plus d'informations sur chaque option, consultez Types d'activation : Terminaux iOS.

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 BlackBerry UEM. Pour en savoir plus, reportez-vous au contenu relatif à BlackBerry Protect Mobile.

11. Cliquez sur **Ajouter**.

À la fin : Si nécessaire, classez les profils.

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

Ces étapes s'appliquent aux terminaux iOS et iPadOS qui sont activés à l'aide de Contrôles MDM ou Confidentialité de l'utilisateur avec les options MDM activées.

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

Envoyez les instructions d'activation suivantes aux utilisateurs de terminaux ou envoyez-leur un lien vers le flux de travail suivant : Activation de votre terminal iOS.

1. Sur le terminal, installez BlackBerry UEM Client. Vous pouvez télécharger BlackBerry UEM Client depuis l'App Store.
2. Sur le terminal, appuyez sur **UEM Client** et acceptez le contrat de licence.
3. 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 BlackBerry 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. Cliquez sur **Autoriser** pour autoriser l'envoi de notifications par UEM Client. Si vous choisissez **Ne Pas Autoriser**, le terminal ne pourra pas être entièrement 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 **Profils 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 l'application BlackBerry UEM Client pour terminer l'activation.
11. 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 a réussi, effectuez l'une des actions suivantes :

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

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

L'inscription des utilisateurs d'Apple est prise en charge sur les terminaux exécutant iPad et iPadOS 13.1 ou versions ultérieures.

Pour commencer l'inscription, les utilisateurs scannent un QR Code fourni dans l'e-mail d'activation de l'inscription des utilisateurs d'Apple à l'aide de l'application d'appareil photo du terminal, afin de télécharger et d'installer manuellement le profil MDM sur le terminal. Pour activer leur terminal, les utilisateurs se connectent à leur compte Apple ID géré qui correspond à l'adresse e-mail du compte d'utilisateur BlackBerry UEM.
Vous devez attribuer UEM Client aux utilisateurs à l'aide d'une licence VPP si vous souhaitez leur permettre d'activer facilement d'autres applications BlackBerry Dynamics, d'importer des certificats, d'utiliser des fonctionnalités BlackBerry 2FA, d'utiliser CylancePROTECT et de vérifier leur état de conformité. La configuration d'UEM Client démarre lorsque l'utilisateur accepte le contrat de licence.

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 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.

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 code QR 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** > **Profils**.
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 l'application BlackBerry UEM Client, sélectionnez **Installer** lorsque vous y êtes invité ou ouvrez Applications professionnelles.
11. Pour configurer l'application BlackBerry 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 l'application BlackBerry UEM Client et sélectionnez **À propos de**. Dans les sections Terminal activé et État de conformité, assurez-vous de la présence des informations sur le terminal et de l'heure et de la date d'activation.
- Dans BlackBerry UEM Self-Service, vérifiez que votre terminal est répertorié en tant que terminal activé. Le statut peut prendre jusqu'à deux minutes pour se mettre à jour après que vous avez activé le terminal.

Gestion et surveillance des terminaux activés

Une fois les terminaux iOS et iPadOS activés et gérés par une stratégie informatique et des profils, vous disposez de plusieurs fonctionnalités pour contrôler les terminaux des utilisateurs.

Vous disposez des options suivantes :

Option	Description
Vérifier les mises à jour logicielles disponibles et mettre à jour le terminal	Vous pouvez afficher les mises à jour du système d'exploitation disponibles pour tous les terminaux gérés. Vous pouvez forcer les terminaux supervisés à installer une mise à jour disponible. Pour plus d'informations, reportez-vous au contenu relatif à l'administration.
Activer les paramètres de localisation et activer le mode Perdu	Vous pouvez activer les paramètres de localisation pour connaitre l'emplacement des terminaux. Vous pouvez également activer le mode Perdu pour trouver un terminal perdu. Pour plus d'informations, reportez-vous au contenu relatif à l'administration.
Activation du verrouillage d'activation	La fonction de verrouillage de l'activation des terminaux demande aux utilisateurs de confirmer l'ID et le mot de passe Apple pour désactiver Localiser mon iPhone, supprimer des données du terminal ou réactiver et utiliser le terminal. Pour gérer la fonctionnalité de verrouillage d'activation dans BlackBerry UEM : • L'appareil doit être supervisé. • Le terminal doit disposer d'un compte iCloud configuré. • La fonction Localiser mon iPhone ou Trouver mon iPad doit être activée sur le terminal. BlackBerry UEM enregistre un code de contournement que vous pouvez utiliser pour annuler le verrouillage afin que les données du terminal puissent être supprimées et réactivées sans l'ID et le mot de passe Apple de l'utilisateur. Pour plus d'informations, reportez-vous au contenu relatif à l'administration.
Récupérer les journaux des terminaux	Vous pouvez récupérer les journaux des terminaux à des fins de surveillance et de dépannage. Pour plus d'informations, reportez-vous au contenu relatif à l'administration.
Désactiver un terminal	Lorsque vous ou un utilisateur désactivez un terminal, la connexion entre le terminal et le compte d'utilisateur dans BlackBerry UEM est supprimée. Vous ne pouvez pas gérer le terminal, et ce dernier ne s'affiche plus dans la console de gestion. L'utilisateur ne peut pas accéder aux données professionnelles du terminal. Vous pouvez désactiver un terminal à l'aide de la commande Supprimer toutes les données du terminal ou Supprimer les données professionnelles uniquement. Les utilisateurs peuvent désactiver un terminal en sélectionnant Désactiver mon terminal dans l'écran À propos de l'application BlackBerry UEM Client.

Envoyer une commande à un terminal

Avant de commencer :

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

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

Commandes pour terminaux iOS

Ces commandes s'appliquent également aux terminaux iPadOS.

Commande	Description	Types d'activation
Afficher le rapport de terminal	Cette commande affiche des informations détaillées sur un terminal. Vous pouvez exporter et enregistrer le rapport de terminal sur votre ordinateur. Pour plus d'informations, reportez-vous à la section Afficher et enregistrer un rapport de terminal.	Contrôles MDM Confidentialité de l'utilisateur
Afficher les actions du terminal	Cette commande affiche les actions en cours sur un terminal. Pour plus d'informations, reportez-vous à la section Affichage des actions du terminal.	Contrôles MDM Confidentialité de l'utilisateur
Supprimer toutes les données du terminal	Cette commande supprime toutes les informations utilisateur et données d'application stockées sur le terminal et rétablit les paramètres d'usine par défaut. Si le terminal ne parvient pas à se connecter à BlackBerry UEM lorsque vous envoyez cette commande, vous pouvez annuler la commande ou supprimer le terminal de la console. Si le terminal se connecte à BlackBerry UEM à l'issue de sa suppression, seules les données professionnelles sont supprimées du terminal. Pour envoyer cette commande à plusieurs terminaux, reportez-vous à la section Envoyer une commande groupée.	Contrôles MDM

Commande	Description	Types d'activation
Supprimer uniquement les données professionnelles	Cette commande supprime les données professionnelles, y compris les stratégies informatiques, profils, applications et certificats présents sur le terminal. Si le terminal ne parvient pas à se connecter à BlackBerry UEM lorsque vous envoyez cette commande, vous pouvez annuler la commande ou supprimer le terminal de la console. Si le terminal se connecte à BlackBerry UEM à l'issue de sa suppression, les données professionnelles sont supprimées du terminal. Pour envoyer cette commande à plusieurs terminaux, reportez-vous à la section Envoyer une commande groupée.	Contrôles MDM Confidentialité de l'utilisateur
Verrouiller le terminal	Cette commande verrouille un terminal. L'utilisateur doit saisir le mot de passe du terminal existant pour déverrouiller le terminal. Si un terminal est temporairement perdu, vous pouvez utiliser cette commande. Lorsque vous envoyez cette commande, le terminal se verrouille uniquement s'il existe un mot de passe de terminal. Sinon, aucune action n'est prise sur le terminal. Cette commande n'est pas prise en charge par les terminaux Apple TV.	Contrôles MDM
Déverrouiller le terminal et effacer le mot de passe	Cette commande déverrouille le terminal et supprime le mot de passe existant. L'utilisateur est invité à créer un mot de passe. Vous pouvez utiliser cette commande si l'utilisateur oublie le mot de passe de son terminal. Cette commande n'est pas prise en charge par les terminaux Apple TV.	Contrôles MDM
Activer le mode Perdu	Cette commande verrouille le terminal et vous permet de définir le numéro de téléphone et le message à afficher sur l'écran. Par exemple, vous pouvez afficher le numéro à appeler par la personne qui trouvera le terminal. Après avoir envoyé cette commande, vous verrez l'emplacement du terminal sur BlackBerry UEM. Cette commande est prise en charge sur les terminaux supervisés uniquement. Cette commande n'est pas prise en charge par les terminaux Apple TV.	Contrôles MDM

Commande	Description	Types d'activation
Désactiver BlackBerry 2FA	Cette commande désactive les terminaux qui sont activés avec le type d'activation BlackBerry 2FA. Le terminal est supprimé de BlackBerry UEM et l'utilisateur ne peut pas utiliser la fonction BlackBerry 2FA. Cette commande n'est pas prise en charge par les terminaux Apple TV.	Contrôles MDM
Mettre à jour le système d'exploitation	Cette commande force les terminaux à installer une mise à jour de système d'exploitation disponible. Pour plus d'informations, reportez-vous à la section Mettre à jour le système d'exploitation sur les terminaux iOS sous supervision. Pour envoyer cette commande à plusieurs terminaux, reportez-vous à la section Envoyer une commande groupée. Cette commande est prise en charge sur les terminaux supervisés uniquement. Cette commande n'est pas prise en charge par les terminaux Apple TV.	Contrôles MDM
Redémarrer le terminal	Cette commande force les terminaux à redémarrer. Cette commande est prise en charge sur les terminaux supervisés uniquement. Cette commande n'est pas prise en charge par les terminaux Apple TV.	Contrôles MDM
Désactiver le terminal	Cette commande force les terminaux à se désactiver. Cette commande est prise en charge sur les terminaux supervisés uniquement. Cette commande n'est pas prise en charge par les terminaux Apple TV.	Contrôles MDM
Nettoyage des applications	Cette commande nettoie les données de toutes les applications gérées par Microsoft Intune sur le terminal. Les applications ne sont pas supprimées du terminal. Pour plus d'informations, reportez-vous à la section Nettoyage des applications gérées par Microsoft Intune.	Contrôles MDM

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

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