BlackBerry UEM

Gestion des configurations des appareils

12.20

Table des matières

Gestion de la configuration des terminaux..... 6

Utilisation de profils pour gérer les fonctionnalités du terminal..... 8
Profils BlackBerry UEM..... 8
Gestion des profils..... 14

Utilisation de variables dans les profils, les e-mails et les notifications..... 16
Définir des variables personnalisées..... 16

Utilisation de modèles d'e-mail pour envoyer des messages aux utilisateurs... 17
Modifier un modèle d'e-mail..... 17
Créer un modèle d'e-mail d'activation..... 17
Création d'un modèle pour les notifications de conformité..... 18
Créer un modèle d'e-mail de notification d'évènement..... 18
Texte de modèle suggéré..... 18

Gestion de terminaux à l'aide de stratégies informatiques..... 26
Gestion des stratégies informatiques..... 26
Importer manuellement des mises à jour des stratégies informatiques et des métadonnées de terminal... 28

Création de messages de support de terminal pour les fonctionnalités désactivées sur les terminaux Android..... 30

Application des règles de conformité aux terminaux..... 31
Créer un profil de conformité..... 31
Communs : paramètres de profil de conformité..... 32
iOS et iPadOS : paramètres de profil de conformité..... 34
macOS : paramètres de profil de conformité..... 36
Android : paramètres de profil de conformité..... 37
Windows : paramètres de profil de conformité..... 40
Surveiller les évènements de conformité..... 43

Envoi de commandes aux utilisateurs et aux terminaux..... 45
Envoi de commandes aux utilisateurs et aux terminaux..... 45
Définir une heure d'expiration pour les commandes..... 45
Commandes pour terminaux iOS et iPadOS..... 46
Commandes pour terminaux macOS..... 48
Commandes pour terminaux Android..... 49
Commandes pour terminaux Windows..... 53

Contrôle des mises à jour logicielles installées sur les terminaux..... 55
Création d'un profil de configuration logicielle minimale requise du terminal pour les terminaux Android Enterprise et Android Management..... 55
Créer un profil de configuration logicielle minimale requise du terminal pour les terminaux Samsung Knox..... 56
Mettre à jour le système d'exploitation sur les terminaux iOS supervisés..... 58

Configuration de la façon dont les terminaux contactent BlackBerry UEM pour les mises à jour des applications et de la configuration..... 59
Créer un profil Enterprise Management Agent..... 59
iOS : paramètres de profil Enterprise Management Agent..... 59
Android : paramètres de profil Enterprise Management Agent..... 60
Windows : paramètres de profil Enterprise Management Agent..... 60

Affichage des informations d'entreprise sur les terminaux..... 62
Créer des avis d'entreprise..... 62
Créer un profil de terminal..... 63

Utilisation des services de localisation sur les terminaux..... 64
Configurer les paramètres du service de localisation..... 64
Créer un profil de service de localisation..... 64
Localiser un terminal..... 65
Activation du mode Perdu sur les terminaux iOS supervisés..... 66

Activation du verrouillage d'activation pour un terminal iOS..... 67

Gestion des fonctionnalités iOS à l'aide des profils de charge utile personnalisée..... 68
Création d'un profil de charge utile personnalisée..... 68

Gestion de la protection contre la réinitialisation aux paramètres d'usine sur les terminaux Android Enterprise et Android Management..... 70
Création d'un profil de protection contre la réinitialisation aux paramètres d'usine..... 71
Désactiver la protection contre la réinitialisation définie en usine d'un terminal..... 72

Configuration de l'attestation relative aux terminaux..... 74
Configuration de l'attestation relative aux terminaux Android et aux applications BlackBerry Dynamics..... 74
Configuration de l'attestation relative aux terminaux Android et aux applications BlackBerry Dynamics..... 74
Configuration de l'attestation relative aux terminaux iOS..... 75
Configuration de l'attestation relative aux terminaux Samsung Knox..... 76
Configuration de l'attestation relative aux terminaux Windows 10..... 76

Configuration de la Protection des informations Windows sur les terminaux Windows 10..... 77
Paramètres des profils de protection des données Windows.....78

Déplacement des terminaux iOS ou macOS vers un canal renforcé..... 83

Informations juridiques..... 84

Gestion de la configuration des terminaux

Ce guide fournit des instructions sur l'utilisation des profils BlackBerry UEM, des stratégies informatiques et d'autres fonctionnalités clés pour configurer les terminaux professionnels en fonction des besoins et des exigences de sécurité de votre organisation.

Tâche	Description
Utiliser des profils pour gérer les fonctionnalités du terminal	Configurez des profils UEM et attribuez-les à des utilisateurs et à des groupes afin de gérer un large éventail de fonctionnalités pour tous types terminaux.
Utiliser des variables dans les profils, les e-mails et les notifications	Utilisez des variables dans les profils, les notifications de conformité, les e-mails d'activation et les notifications d'évènements afin de personnaliser les configurations et les messages pour les utilisateurs individuels.
Utiliser des modèles d'e-mail pour envoyer des messages aux utilisateurs.	Utilisez des modèles d'e-mail pour personnaliser les e-mails qu'UEM envoie aux utilisateurs, notamment pour leur communiquer les instructions d'activation de leur terminal, les informer des problèmes de conformité et leur fournir des clés d'accès aux applications BlackBerry Dynamics.
Gérer les terminaux à l'aide de stratégies informatiques.	Utilisez des stratégies informatiques pour contrôler les fonctionnalités des terminaux. Par exemple, vous pouvez utiliser des règles de stratégie informatique pour imposer des exigences en matière de mot de passe, empêcher l'utilisation de certaines fonctionnalités du terminal (par exemple, l'appareil photo) et contrôler la disponibilité de certaines applications.
Création de messages de support de terminal pour les fonctionnalités désactivées sur les terminaux Android.	Affichez un message de support sur les terminaux Android lorsqu'une fonctionnalité est désactivée par une stratégie informatique.
Appliquer des règles de conformité aux terminaux	Utilisez des profils de conformité pour encourager les utilisateurs à respecter les normes de votre organisation en matière de terminaux. Un profil de conformité définit ce qui n'est pas acceptable en matière de terminaux au sein de votre organisation et spécifie les mesures à appliquer pour UEM si l'utilisateur ne corrige pas les problèmes de conformité.
Envoyer des commandes aux utilisateurs et aux terminaux	Vous pouvez envoyer diverses commandes pour gérer les comptes utilisateur et les terminaux. Par exemple, vous pouvez envoyer une commande pour verrouiller un terminal ou pour supprimer toutes les données professionnelles d'un terminal.
Contrôler les mises à jour logicielles installées sur les terminaux	Utilisez des profils de configuration logicielle minimale requise pour déterminer comment les mises à jour logicielles doivent être installées sur les terminaux.

Tâche	Description
Configurer la façon dont les terminaux contactent UEM pour les mises à jour des applications et de la configuration	Utilisez des profils Enterprise Management Agent afin de configurer la façon dont les terminaux contactent UEM pour les mises à jour des applications ou de la configuration.
Afficher les informations relatives à l'organisation sur les terminaux	Utilisez des avis d'entreprise et des profils de terminal pour afficher les informations relatives à l'organisation sur les terminaux.
Utiliser des services de localisation sur les terminaux	Utilisez des profils de service de localisation pour demander l'emplacement des terminaux et afficher leur emplacement approximatif sur une carte.
Activation du verrouillage d'activation pour un terminal iOS.	Utilisez la fonctionnalité de verrouillage de l'activation des terminaux iOS pour permettre aux utilisateurs de protéger leurs terminaux en cas de perte ou de vol. Lorsque la fonctionnalité est activée, l'utilisateur doit confirmer son ID et son mot de passe Apple pour désactiver la fonction Localiser mon iPhone, effacer le terminal ou réactiver et utiliser le terminal.
Gérer les fonctionnalités iOS à l'aide de profils de charge utile personnalisée	Utilisez des profils de charge utile personnalisée pour contrôler les fonctionnalités sur les terminaux iOS qui ne sont pas contrôlés par les règles ou profils UEM existants.
Gérer la protection contre la réinitialisation aux paramètres d'usine sur les terminaux Android	Utilisez des profils de protection contre la réinitialisation aux paramètres d'usine pour contrôler la fonctionnalité de protection contre la réinitialisation aux paramètres d'usine sur les terminaux Android Enterprise et Android Management de votre organisation.
Configurer l'attestation relative aux terminaux	Vérifiez l'authenticité et l'intégrité des terminaux Samsung Knox, Android, iOS et Windows 10.
Configuration de la Protection des informations Windows sur les terminaux Windows 10.	Utilisez des profils de protection des données Windows pour protéger et gérer les données professionnelles sur les terminaux Windows 10.
Déplacement des terminaux iOS ou macOS vers un canal renforcé.	Lorsque vous activez des terminaux iOS ou macOS, ceux-ci sont attribués par défaut à un canal de données renforcé. Si certains de vos terminaux iOS ou macOS n'utilisent pas de canal de données renforcé, vous pouvez exporter la liste de ces terminaux et prendre des mesures pour les déplacer vers un canal renforcé.

Utilisation de profils pour gérer les fonctionnalités du terminal

BlackBerry UEM utilise différents types de profils pour gérer une grande variété de fonctionnalités des terminaux iOS, macOS, Android et Windows. Vous pouvez configurer un profil répondant aux besoins de votre organisation, puis l'attribuer à des comptes d'utilisateur, à des groupes d'utilisateurs et à des groupes de terminaux afin d'appliquer cette configuration aux terminaux.

Pour accéder à la liste complète des profils disponibles, consultez Profils BlackBerry UEM.

Les profils peuvent être classés ou non classés. Pour les profils classés, UEM attribue un profil de ce type à un terminal (par exemple, un profil de conformité). Si un profil classé est directement attribué à un utilisateur, il est prioritaire sur tous les profils de ce type attribués aux groupes d'utilisateurs auxquels appartient cet utilisateur. Si un utilisateur appartient à plusieurs groupes d'utilisateurs auxquels différents profils de ce type ont été attribués, le classement est utilisé pour déterminer le profil à attribuer. Si le terminal d'un utilisateur appartient à un groupe de terminaux, le profil attribué au groupe de terminaux est prioritaire sur le même profil de ce type attribué directement à l'utilisateur. Si le terminal appartient à plusieurs groupes de terminaux auxquels différents profils de ce type ont été attribués, le classement est utilisé pour déterminer le profil à attribuer.

Pour les profils non classés, plusieurs profils de ce type peuvent être attribués à un terminal, soit par attribution directe à un compte d'utilisateur, soit par attribution à un groupe (par exemple, un terminal peut se voir attribuer plusieurs profils Wi-Fi).

Pour certains types de profils, un profil doit être attribué aux terminaux. Si un profil n'est pas attribué aux utilisateurs directement ou via l'appartenance à un groupe, UEM attribue un profil par défaut préconfiguré. UEM comprend un profil d'activation par défaut, un profil de conformité par défaut, un profil de connectivité d'entreprise par défaut et un profil Enterprise Management Agent par défaut.

Profils BlackBerry UEM

Nom du profil	Description	Types de terminaux pris en charge	Classé ou non classé	Pour plus d'informations, reportez-vous à
Stratégie				
Knox Service Plugin	Configure Knox Service Plugin.	Android	Classé	Gestion des terminaux Android avec des configurations d'applications OEM
Activation	Configure les paramètres d'activation des terminaux pour les utilisateurs (par exemple, type d'activation, et nombre et types de terminaux).	Tous les terminaux	Classé	Création de profils d'activation

Nom du profil	Description	Types de terminaux pris en charge	Classé ou non classé	Pour plus d'informations, reportez-vous à
BlackBerry Dynamics	Active BlackBerry Dynamics pour les utilisateurs, et configure les normes relatives à l'accès aux applications, à la protection des données et à la journalisation.	Tous les terminaux	Classé	Contrôle de BlackBerry Dynamics sur les terminaux
Mode de verrouillage des applications	Configure un terminal pour qu'il n'exécute que les applications que vous spécifiez.	Terminaux iOS supervisés Terminaux Samsung Knox activés avec MDM Terminaux Windows 10 Education et Windows 10 Enterprise	Classé	Limitation des applications à exécuter sur un terminal
Agent de gestion d'entreprise	Configure la manière dont les terminaux se connectent à UEM pour les mises à jour des applications ou de la configuration.	iOS Android Windows	Classé	Configuration de la façon dont les terminaux contactent BlackBerry UEM pour les mises à jour des applications et de la configuration
iPad partagé	Configure un terminal iPad pour qu'il puisse être partagé par plusieurs utilisateurs.	iOS	Classé	Création et gestion de groupes d'iPad partagés
Conformité				
Conformité	Définit les conditions relatives aux terminaux qui ne sont pas acceptables dans votre organisation, et configure les mesures d'application.	Tous les terminaux	Classé	Application des règles de conformité aux terminaux
Conformité (BlackBerry Dynamics)	Il s'agit d'un profil en lecture seule qui affiche les paramètres de conformité importés de Good Control dans un environnement UEM sur site.	Tous les terminaux	n/d	n/d

Nom du profil	Description	Types de terminaux pris en charge	Classé ou non classé	Pour plus d'informations, reportez-vous à
Configuration logicielle minimale requise du terminal	Configure les versions logicielles qui doivent être installées sur les terminaux.	Android	Classé	Contrôle des mises à jour logicielles installées sur les terminaux
E-mail, calendrier et contacts				
E-mail	Configure 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.	Tous les terminaux	Classé	Créer des profils de messagerie
Messagerie IMAP/POP3	Configure la manière dont les terminaux se connectent à un serveur de messagerie IMAP ou POP3 et synchronisent les e-mails.	Tous les terminaux	Non classé	Créer un profil de messagerie IMAP/POP3
Contrôle	Spécifie les serveurs Microsoft Exchange à utiliser pour le contrôle d'accès automatique.	Tous les terminaux	Classé	Créer un profil de contrôle d'accès
CalDAV	Spécifie les paramètres de serveur que les terminaux peuvent utiliser pour synchroniser les informations de calendrier.	iOS macOS	Non classé	Configuration des profils CardDAV et CalDAV
CardDAV	Spécifie les paramètres de serveur que les terminaux peuvent utiliser pour synchroniser les informations de contact.	iOS macOS	Non classé	Configuration des profils CardDAV et CalDAV
Réseaux et connexions				
Wi-Fi	Configure la manière dont les terminaux se connectent à un réseau Wi-Fi professionnel.	Tous les terminaux	Non classé	Configuration de réseaux Wi-Fi professionnels pour les terminaux

Nom du profil	Description	Types de terminaux pris en charge	Classé ou non classé	Pour plus d'informations, reportez-vous à
VPN	Configure la manière dont les terminaux se connectent à un VPN professionnel.	Tous les terminaux	Non classé	Configuration de réseaux VPN professionnels pour les terminaux
DNS	Spécifie les serveurs DNS à utiliser par les terminaux pour accéder à des domaines spécifiques.	iOS macOS	Classé	Spécification de serveurs DNS pour les terminaux iOS et macOS
Proxy	Configure la manière dont les terminaux utilisent un serveur proxy pour accéder à des services Web sur Internet ou un réseau professionnel.	iOS macOS Android	Classé	Création de profils proxy pour les terminaux
Connectivité d'entreprise	Configure la manière dont les terminaux peuvent se connecter aux ressources de votre organisation à l'aide de la connectivité d'entreprise, et détermine si les terminaux peuvent utiliser BlackBerry Secure Connect Plus.	iOS Android	Classé	Utilisation de BlackBerry Secure Connect Plus pour des connexions sécurisées aux ressources professionnelles
Connectivité BlackBerry Dynamics	Configure 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.	Tous les terminaux	Classé	Configuration de connexions réseau pour les applications BlackBerry Dynamics
BlackBerry 2FA	Active l'authentification à deux facteurs pour les utilisateurs et configure les fonctionnalités de préauthentification et de résolution autonome.	iOS Android	Classé	Créer un profil BlackBerry 2FA
Utilisation du réseau	Détermine si les applications professionnelles installées sur les terminaux iOS peuvent utiliser le réseau mobile ou l'itinérance des données.	iOS	Classé	Contrôle de l'utilisation du réseau pour les applications sur les terminaux iOS

Nom du profil	Description	Types de terminaux pris en charge	Classé ou non classé	Pour plus d'informations, reportez-vous à
Filtre de contenu Web	Limite les sites Web qu'un utilisateur peut consulter sur les terminaux iOS supervisés.	Terminaux iOS supervisés	Non classé	Créer un profil de filtre de contenu Web sur les terminaux iOS
Extension d'identification unique	Permet aux terminaux iOS de s'authentifier automatiquement auprès des domaines et des services Web du réseau de votre organisation.	iOS	Non classé	Activation de l'authentification automatique sur les terminaux iOS
Domaines gérés	Configure les terminaux iOS afin qu'ils avertissent les utilisateurs de l'envoi d'e-mails en dehors des domaines approuvés et limite les applications qui peuvent ouvrir des documents téléchargés à partir de domaines internes.	iOS	Non classé	Spécification des domaines de messagerie et des domaines Web pour les terminaux iOS
AirPrint	Ajoute des imprimantes aux listes d'imprimantes AirPrint des utilisateurs.	iOS	Non classé	Création d'un profil AirPrint sur les terminaux iOS
AirPlay	Ajoute des terminaux aux listes de terminaux AirPlay des utilisateurs.	iOS	Non classé	Créer un profil AirPlay sur les terminaux iOS
Nom du point d'accès	Spécifie les noms de point d'accès que les terminaux doivent utiliser pour se connecter aux opérateurs.	Android	Non classé	Création d'un profil de nom de point d'accès sur les terminaux Android
Protection				
Protection des données Windows	Configure le paramètre Protection des données Windows dans Windows 10.	Windows 10	Classé	Configuration de la Protection des informations Windows sur les terminaux Windows 10
Protection des applications Microsoft Intune	Configure la fonction de protection des données dans les applications Office 365.	iOS Android	Non classé	Gestion des applications protégées par Microsoft Intune

Nom du profil	Description	Types de terminaux pris en charge	Classé ou non classé	Pour plus d'informations, reportez-vous à
Service de localisation	Permet de demander l'emplacement des terminaux et d'afficher l'emplacement approximatif de ceux-ci sur une carte.	iOS Android Windows	Classé	Utilisation des services de localisation sur les terminaux
Ne pas déranger	Bloque les notifications de BlackBerry Work pendant les périodes d'inactivité.	iOS Android	Classé	Désactiver des notifications en dehors des heures de travail à partir de BlackBerry Work
Protection contre la réinitialisation aux paramètres d'usine	Contrôle la fonction de protection contre la réinitialisation aux paramètres d'usine sur les terminaux Android.	Android	Classé	Gestion de la protection contre la réinitialisation aux paramètres d'usine sur les terminaux Android Enterprise et Android Management
CylancePROTECT	Configure les fonctionnalités de sécurité de CylancePROTECT Mobile for BlackBerry UEM.	iOS Android	Classé	CylancePROTECT Mobile pour BlackBerry UEM
Personnalisée				
Terminal	Spécifier les informations à afficher sur les terminaux.	iOS Android Windows	Classé	Affichage des informations d'entreprise sur les terminaux
Disposition de l'écran d'accueil	Configure la disposition des applications sur les terminaux iOS.	iOS	Classé	Configurer la disposition des applications sur les terminaux iOS
Charge utile personnalisée	Spécifie les informations de configuration personnalisée du terminal à l'aide du code de charge utile.	iOS	Non classé	Gestion des fonctionnalités iOS à l'aide des profils de charge utile personnalisée
Notification par application	Configure les paramètres de notification des applications système et des applications que vous gérez avec UEM.	Terminaux iOS supervisés	Classé	Gestion des notifications d'application sur les terminaux iOS supervisés

Nom du profil	Description	Types de terminaux pris en charge	Classé ou non classé	Pour plus d'informations, reportez-vous à
Certificats				
Certificat d'AC	Spécifie un certificat CA que les terminaux peuvent utiliser pour établir une relation de confiance avec un réseau ou un serveur professionnel.	Tous les terminaux	Non classé	Envoi de certificats d'autorité de certification à des terminaux et des applications
Certificat partagé	Spécifie un certificat client que les terminaux peuvent utiliser pour authentifier les utilisateurs auprès d'un réseau ou d'un serveur professionnel.	iOS macOS Android	Non classé	Envoi du même certificat client à plusieurs terminaux
Informations d'identification de l'utilisateur	Spécifie la connexion CA via laquelle les terminaux peuvent obtenir un certificat client d'authentification sur un réseau ou un serveur professionnel.	iOS macOS Android	Non classé	Envoi de certificats clients vers des terminaux et des applications à l'aide de profils d'authentification utilisateur
SCEP	Spécifie le serveur SCEP via lequel les terminaux peuvent obtenir un certificat client d'authentification sur un réseau ou un serveur professionnel.	Tous les terminaux	Non classé	Envoi de certificats client à des terminaux et applications à l'aide de SCEP
OCSP	Permet aux terminaux de vérifier l'état des certificats S/MIME.	iOS Android	Classé	Identification de l'état des certificats S/MIME sur les terminaux
CRL	Configure UEM pour qu'il recherche l'état des certificats S/MIME.	iOS Android	Classé	Identification de l'état des certificats S/MIME sur les terminaux
Profil de mappage des certificats	Spécifie les certificats client que les applications doivent utiliser	Android	Classé	Spécification du certificat à utiliser par une application à l'aide d'un profil de mappage de certificats

Gestion des profils

1. Sur la barre de menus de la console de gestion, cliquez sur **Stratégies et profils**.
2. Cliquez sur le type de profil qui convient.

3. Effectuez l'une des opérations suivantes :

Tâche	Étapes
Copier un profil	**a.** Cliquez sur le nom du profil que vous souhaitez copier. **b.** Cliquez sur . **c.** Saisissez le nom et la description du profil. **d.** Configurez les valeurs qui conviennent pour le profil. Pour plus d'informations sur chaque type de profil, consultez Profils BlackBerry UEM. **e.** Cliquez sur **Enregistrer**. **f.** Attribuez le profil à des utilisateurs et à des groupes.
Modifier un profil	**a.** Cliquez sur le nom du profil que vous souhaitez modifier. **b.** Cliquez sur . **c.** Apportez les modifications souhaitées au profil. **d.** Cliquez sur **Enregistrer**.
Classez les profils.	**a.** Cliquez sur . **b.** Utilisez les flèches pour déplacer les profils vers le haut ou vers le bas du classement. **c.** Cliquez sur **Enregistrer**.
Supprimer un profil dans des comptes d'utilisateur	**a.** Cliquez sur le nom du profil que vous souhaitez supprimer. **b.** Dans l'onglet **Attribué à x utilisateurs**, recherchez et sélectionnez les comptes d'utilisateur à partir desquels vous souhaitez supprimer le profil. **c.** Cliquez sur .
Supprimer un profil dans des groupes d'utilisateurs	**a.** Cliquez sur le nom du profil que vous souhaitez supprimer. **b.** Dans l'onglet **Attribué à x groupes**, recherchez et sélectionnez les groupes à partir desquels vous souhaitez supprimer le profil. **c.** Cliquez sur .
Supprimer un profil	Vous ne pouvez pas supprimer un profil par défaut. Lorsque vous supprimez un profil personnalisé, UEM le supprime des comptes d'utilisateur et des terminaux auxquels il est attribué. **a.** Sélectionnez le profil que vous souhaitez supprimer. **b.** Cliquez sur . **c.** Cliquez sur **Supprimer**.

Utilisation de variables dans les profils, les e-mails et les notifications

BlackBerry UEM prend en charge des variables par défaut et personnalisées que vous pouvez utiliser dans les profils, les notifications de conformité, les e-mails d'activation et les notifications d'évènements afin de personnaliser les configurations et les messages pour des utilisateurs individuels. Les variables par défaut correspondent aux attributs de compte standard (par exemple, le nom d'utilisateur ou l'adresse électronique) et à d'autres attributs prédéfinis (comme l'adresse du serveur utilisée pour l'activation du terminal). Vous pouvez utiliser les variables personnalisées pour définir des attributs supplémentaires.

Vous pouvez utiliser une variable dans tous les champs de texte d'un profil, à l'exception des champs Nom et Description. Par exemple, vous pouvez spécifier « %UserName%@exemple.com » dans le champ Adresse électronique d'un profil de messagerie.

Vous pouvez afficher la liste des variables par défaut disponibles dans la console de gestion à partir de **Paramètres > Paramètres généraux > Variables par défaut.**

Veuillez noter que les stratégies informatiques et les configurations d'applications BlackBerry Dynamics ne prennent pas en charge l'utilisation de variables.

Définir des variables personnalisées

Vous pouvez définir cinq variables de texte personnalisées et cinq variables de texte masqué pour représenter des informations sensibles telles que des mots de passe. Lorsque vous définissez une variable personnalisée, vous lui donnez un libellé (par exemple, mot de passe VPN). Lorsque vous créez ou mettez à jour un compte d'utilisateur, les libellés sont utilisés comme noms de champs dans la section Variables personnalisées et vous pouvez spécifier les valeurs appropriées pour l'utilisateur en question. Tous les comptes d'utilisateur prennent en charge les variables personnalisées, y compris les comptes d'administrateur. Vous pouvez utiliser les variables personnalisées de la même manière que les variables par défaut.

1. Sur la barre de menus de la console de gestion, cliquez sur **Paramètres > Paramètres généraux > Variables personnalisées**.
2. Cochez la case **Afficher les variables personnalisées lors de l'ajout ou de la modification d'un utilisateur**.
3. Spécifiez un libellé pour chaque variable personnalisée que vous souhaitez utiliser.
4. Cliquez sur **Enregistrer**.

Utilisation de modèles d'e-mail pour envoyer des messages aux utilisateurs

Vous pouvez utiliser des modèles d'e-mail pour personnaliser les e-mails envoyés par BlackBerry UEM aux utilisateurs pour diverses raisons, notamment la mise à disposition d'instructions pour l'activation des terminaux, la notification aux utilisateurs de problèmes de conformité et la mise à disposition de clés d'accès pour les applications BlackBerry Dynamics.

Vous pouvez personnaliser les e-mails à l'aide de variables pour des éléments tels que le nom de l'utilisateur, l'adresse e-mail ou le mot de passe d'activation, et vous pouvez personnaliser l'apparence des messages à l'aide de polices, couleurs et images différentes. Vous pouvez créer plusieurs modèles à utiliser pour différents types de terminal ou d'activation. Vous pouvez modifier les modèles d'e-mail par défaut ou en créer de nouveaux.

Lorsque vous effectuez diverses tâches dans la console de gestion (ajout d'un utilisateur, création d'un profil de conformité, par exemple), vous pouvez sélectionner le modèle d'e-mail à utiliser par UEM pour envoyer un message aux utilisateurs du terminal.

Vous pouvez afficher les modèles par défaut disponibles dans la console de gestion sous **Paramètres > Paramètres généraux > Modèles.**

Modifier un modèle d'e-mail

Si vous décidez de modifier un modèle d'e-mail par défaut, il est recommandé d'enregistrer une sauvegarde du texte du modèle d'origine au cas où vous souhaiteriez le restaurer ultérieurement.

1. Sur la barre de menus de la console de gestion, cliquez sur **Paramètres > Paramètres généraux > Modèles**.
2. Cliquez sur le modèle que vous voulez modifier.
3. Modifiez le champ **Nom**, **Objet** ou **Message**, si nécessaire.
4. Cliquez sur **Enregistrer**.

Créer un modèle d'e-mail d'activation

1. Sur la barre de menus de la console de gestion, cliquez sur **Paramètres > Paramètres généraux > Modèles**.
2. Cliquez sur + > **Activation d'un terminal**.
3. Dans le champ **Nom**, saisissez un nom pour le modèle.
4. Dans le champ **Objet**, saisissez la ligne d'objet de l'e-mail d'activation.
5. Dans le champ **Message**, saisissez le corps du texte de l'e-mail d'activation.

   Utilisez l'éditeur HTML pour personnaliser la mise en forme, insérer des images (par exemple, un logo d'entreprise), etc. Vous pouvez insérer des variables pour personnaliser certaines parties de l'e-mail. Reportez-vous à la section Utilisation de variables dans les profils, les e-mails et les notifications.
6. Si vous souhaitez que les utilisateurs activent leur terminal avec un QR Code à la place d'un mot de passe d'activation, cochez la case **Ajouter un code QR aux e-mails d'activation des terminaux iOS et Android**.
7. Pour envoyer le mot de passe d'activation ou le QR Code indépendamment des instructions d'activation, sélectionnez **Envoyer deux e-mails d'activation distincts - Le premier pour les instructions et le second pour le mot de passe** et spécifiez le contenu et les options du deuxième e-mail d'activation. Si vous décidez d'envoyer un seul e-mail d'activation, veillez à inclure le mot de passe d'activation (ou la variable correspondante) ou le QR Code dans le premier e-mail.
8. Cliquez sur **Enregistrer**.

Pour plus d'informations sur l'activation des terminaux, reportez-vous à la section Activation des terminaux.

Création d'un modèle pour les notifications de conformité

Lorsque le terminal d'un utilisateur ne respecte pas les exigences que vous avez configurées dans un profil de conformité attribué, BlackBerry UEM peut envoyer à l'utilisateur un e-mail personnalisé basé sur un modèle spécifié. UEM comprend un modèle par défaut pour les e-mails relatifs aux violations de conformité. Ce modèle peut être modifié, mais pas supprimé. Si vous n'attribuez pas un autre modèle à un compte d'utilisateur, UEM utilise le modèle par défaut.

1. Sur la barre de menus de la console de gestion, cliquez sur **Paramètres > Paramètres généraux > Modèles**.
2. Cliquez sur + > **Violation de conformité**.
3. Dans le champ **Nom**, saisissez un nom pour le modèle.
4. Dans le champ **Objet**, saisissez un objet pour le message.
5. Dans le champ **Message**, saisissez le corps du texte de l'e-mail sur la conformité.

   Utilisez l'éditeur HTML pour personnaliser la mise en forme, insérer des images (par exemple, un logo d'entreprise), etc. Vous pouvez insérer des variables pour personnaliser certaines parties de l'e-mail. Reportez-vous à la section Utilisation de variables dans les profils, les e-mails et les notifications.
6. Cliquez sur **Enregistrer**.

Pour plus d'informations sur la conformité du terminal, consultez Application des règles de conformité aux terminaux.

Créer un modèle d'e-mail de notification d'évènement

Vous pouvez créer un modèle d'e-mail de notification d'évènement que BlackBerry UEM peut utiliser pour envoyer des messages personnalisés aux administrateurs lorsque certains évènements se produisent dans l'environnement UEM de votre organisation.

1. Sur la barre de menus de la console de gestion, cliquez sur **Paramètres > Paramètres généraux > Modèles**.
2. Cliquez sur + > **Notification d'évènement**.
3. Dans le champ **Nom**, saisissez un nom pour le modèle.
4. Dans le champ **Objet**, saisissez une ligne d'objet pour le message. Si vous souhaitez ajouter le type d'évènement à la ligne d'objet, cochez la case **Ajouter le type d'évènement à l'objet de l'e-mail**.
5. Dans le champ **Message**, saisissez le corps du texte de l'e-mail de notification d'évènement.

   Utilisez l'éditeur HTML pour personnaliser la mise en forme, insérer des images (par exemple, un logo d'entreprise), etc. Vous pouvez insérer des variables pour personnaliser certaines parties de l'e-mail. Reportez-vous à la section Utilisation de variables dans les profils, les e-mails et les notifications.
6. Cliquez sur **Enregistrer**.

Pour plus d'informations sur les notifications d'évènement, consultez Création de notifications d'évènement.

Texte de modèle suggéré

Le texte suggéré ci-dessous est utilisé dans les modèles d'e-mail par défaut. Si vous modifiez les modèles d'e-mail par défaut et que vous souhaitez réutiliser le texte par défaut plus tard, vous pouvez le copier et le coller à partir de là.

Nom	Texte suggéré
Code d'activation de profil professionnel Android	**Objet : un code d'activation de profil professionnel Android a été créé pour vous** %UserDisplayName%, Pour activer un terminal Android avec un espace Travail uniquement, votre administrateur a créé un code d'activation de profil professionnel Android pour vous. Vous recevrez votre mot de passe d'activation BlackBerry UEM mot de passe dans un e-mail séparé. Votre code d'activation de profil professionnel Android : %GoogleActivationCode% Votre code d'activation de profil professionnel Android expirera le %ActivationPasswordExpiry%. Si vous avez des questions, contactez votre administrateur.
Identifiant de compte Google géré par défaut	**Objet : un compte Google a été créé pour vous** %UserDisplayName%, Pour activer le profil professionnel sur votre terminal, votre administrateur a créé un compte Google pour vous. Vous aurez besoin du mot de passe de votre compte Google lorsque vous activerez le profil professionnel. Le mot de passe de votre compte Google affiché ici n'est pas le mot de passe que vous utilisez lorsque vous activez votre terminal sur BlackBerry UEM. Vous recevrez votre mot de passe d'activation BlackBerry UEM dans un e-mail séparé. Vous pouvez aussi définir votre mot de passe d'activation BlackBerry UEM dans BlackBerry UEM Self-Service. Vous avez besoin des informations suivantes lorsque vous activez le profil professionnel : • Votre adresse électronique professionnelle: %UserEmailAddress% • Mot de passe de votre compte Google : %Password% Vous pouvez gérer votre compte Google sur https://myaccount.google.com. Si vous modifiez le mot de passe de votre compte Google, le mot de passe inclus dans cet e-mail ne sera plus valide et vous devrez utiliser votre nouveau mot de passe. Veuillez conserver ces informations dans vos dossiers. Si vous avez des questions, contactez votre administrateur.

Nom	Texte suggéré
E-mail d'activation des terminaux DEP Apple Premier e-mail	**Objet : activer votre terminal sur BlackBerry UEM** %UserDisplayName%, Votre administrateur a activé votre terminal iOS pour BlackBerry UEM. L'activation de votre terminal nécessite les informations suivantes : • Votre adresse électronique professionnelle: %UserEmailAddress% • Le mot de passe d'activation de votre terminal : ce mot de passe d'activation vous sera envoyé dans un e-mail séparé. Vous pouvez gérer votre terminal avec BlackBerry UEM Self-Service sur %UserSelfServicePortalURL%. Pour vous connecter, utilisez le nom d'utilisateur suivant : Nom d'utilisateur BlackBerry UEM Self-Service : %UserName% Votre mot de passe BlackBerry UEM Self-Service vous a peut-être été envoyé dans un e-mail séparé. Si vous ne l'avez pas reçu, contactez votre administrateur. Veuillez conserver ces informations dans vos dossiers. Si vous avez des questions, contactez votre administrateur.
E-mail d'activation des terminaux DEP Apple Deuxième e-mail	**Objet : mot de passe d'activation de votre terminal sur BlackBerry UEM** %UserDisplayName%, Votre administrateur a activé votre terminal mobile pour BlackBerry UEM. L'activation de votre terminal nécessite les informations suivantes : Mot de passe d'activation de votre terminal : %ActivationPassword% Votre mot de passe expirera le %ActivationPasswordExpiry%. Suivez les instructions fournies dans l'e-mail « Activation de votre terminal sur BlackBerry UEM » pour activer votre terminal iOS sur BlackBerry UEM. Si vous avez des questions, contactez votre administrateur. Bienvenue dans BlackBerry UEM !

Nom	Texte suggéré
E-mail pour la clé d'accès BlackBerry Dynamics	**Objet : une clé d'accès pour une application BlackBerry Dynamics a été créée pour vous** %UserDisplayName%, Votre administrateur a créé une clé d'accès pour une application BlackBerry Dynamics. Cet e-mail contient la clé d'accès et les instructions nécessaires pour configurer l'application. Si vous avez été autorisé à utiliser plusieurs applications, vous recevrez plusieurs e-mails. Chaque e-mail contient une clé d'accès permettant de configurer une application. Vous pouvez utiliser l'une de vos clés d'accès pour configurer n'importe quelle application, mais chaque clé d'accès n'est valable qu'une fois. Avant de commencer, vérifiez que vous disposez de données mobiles ou d'une couverture Wi-Fi. **1.** Ouvrez l'application BlackBerry Dynamics. **2.** Lorsque vous y êtes invité, saisissez les informations suivantes. • Adresse e-mail : %UserEmailAddress% • Clés d'accès : %AccessKeys% Votre clé d'accès expirera le %AccessKeyExpiry%. **3.** Vous serez peut-être invité à créer un mot de passe, que vous devrez saisir à l'ouverture de l'application. Si vous avez des questions, contactez votre administrateur.

Nom	Texte suggéré
E-mail d'activation par défaut Premier e-mail	**Objet : activer votre terminal sur BlackBerry UEM** %UserDisplayName%, Votre administrateur a activé votre terminal mobile pour BlackBerry UEM. L'activation de votre terminal nécessite tout ou partie des informations suivantes: • Votre adresse électronique professionnelle: %UserEmailAddress% • Nom du serveur: %ActivationURL% • Nom d'utilisateur pour l'activation: %ActivationUserName% • Le mot de passe d'activation de votre terminal : ce mot de passe d'activation vous sera envoyé dans un e-mail séparé. Pour les terminaux Android : Si vous utilisez un terminal Android, vous devez installer BlackBerry UEM Client depuis Google Play. Pour les terminaux iOS : Si vous utilisez un terminal iOS, vous devez installer BlackBerry UEM Client depuis App Store. Pour les terminaux iOS, ouvrez Safari et accédez à workspace://apps pour installer les applications que votre administrateur vous a attribuées. Le cas échéant, vous pouvez également sélectionner Work Apps sur votre terminal. Pour les terminaux macOS : Si vous utilisez un terminal macOS, vous devez l'activer avec BlackBerry UEM Self-Service. Pour les terminaux exécutant Windows 10 ou version ultérieure : Les informations suivantes vous seront nécessaires pour activer votre terminal : • Nom du serveur: %ClientlessActivationURL% • URL du serveur de certificat : %RsaRootCaCertUrl% • Vous devez installer le certificat RSA. Saisissez l'URL du serveur de certificats dans la barre d'adresse du navigateur sur votre terminal. Suivez les instructions et installez le certificat dans le dossier des autorités de certification racine autorisées. • Sur votre terminal, accédez à Paramètres > Comptes > Accès professionnel ou école et sélectionnez S'inscrire uniquement dans la gestion du terminal. Pour gérer vos terminaux Vous pouvez gérer votre terminal avec BlackBerry UEM Self-Service sur %UserSelfServicePortalURL%. Pour vous connecter, utilisez le nom d'utilisateur suivant : Nom d'utilisateur BlackBerry UEM Self-Service : %UserName% Votre mot de passe BlackBerry UEM Self-Service vous a peut-être été envoyé dans un e-mail séparé. Bienvenue dans BlackBerry UEM !

Nom	Texte suggéré
E-mail d'activation par défaut Deuxième e-mail	**Objet : mot de passe d'activation de votre terminal sur BlackBerry UEM** %UserDisplayName%, Votre administrateur a activé votre terminal mobile pour BlackBerry UEM. L'activation de votre terminal nécessite les informations suivantes : • Mot de passe d'activation de votre terminal : %ActivationPassword% • Votre mot de passe expirera le %ActivationPasswordExpiry% Suivez les instructions fournies dans l'e-mail « Activation de votre terminal sur BlackBerry UEM » pour activer votre terminal iOS, Android ou Windows sur BlackBerry UEM. Si vous avez des questions, contactez votre administrateur. Bienvenue dans BlackBerry UEM !
E-mail d'activation Android Management par défaut	**Objet : activer votre terminal sur BlackBerry UEM** %UserDisplayName%, Votre administrateur a activé Android Management sur votre terminal afin de permettre la création d'un profil professionnel. Pour créer le profil professionnel, vous pouvez cliquer sur le lien %ActivationAndroidManagementURL% suivant depuis votre terminal. Vous pouvez également scanner le QR Code sur votre terminal. Accédez à Paramètres > Services Google > Configurer et restaurer > Configurer votre profil professionnel, puis scannez le QR Code suivant. Le lien d'activation et le QR Code expireront le %ActivationPasswordExpiry% %ActivationAndroidManagementQRCode% Veuillez conserver ces informations dans vos dossiers. Si vous avez des questions, contactez votre administrateur.
E-mail de conformité par défaut	**Objet : notification de terminal non conforme** Votre terminal n'est pas conforme aux stratégies de votre organisation. Si cet état persiste, votre administrateur pourra limiter l'accès aux données de l'entreprise depuis votre terminal, supprimer les données de l'entreprise sur votre terminal ou supprimer tout le contenu et tous les paramètres de votre terminal.

Nom	Texte suggéré
E-mail d'activation pour espace Travail par défaut uniquement (Android Enterprise) Premier e-mail	**Objet : activer votre terminal sur BlackBerry UEM** %UserDisplayName%, Votre administrateur a activé votre terminal Android (9.0 et version ultérieure) pour BlackBerry UEM. L'activation de votre terminal nécessite les informations suivantes : • Nom d'utilisateur pour l'activation: %ActivationUserName% • Le mot de passe d'activation de votre terminal : ce mot de passe d'activation vous sera envoyé dans un e-mail séparé. Pour activer votre terminal, procédez comme suit : **1.** Si l'écran d'accueil du programme d'installation n'apparait pas, réinitialisez les paramètres par défaut du terminal. **2.** Lors de la configuration du terminal, sur l'écran Ajouter votre compte, saisissez vos informations d'identification de compte Google. Attendez que le terminal mette à jour certaines applications système importantes et télécharge UEM Client. **3.** Dans BlackBerry UEM Client, suivez les instructions à l'écran pour activer votre terminal. Vous pouvez gérer votre terminal avec BlackBerry UEM Self-Service sur %UserSelfServicePortalURL%. Pour vous connecter, utilisez le nom d'utilisateur suivant : Nom d'utilisateur BlackBerry UEM Self-Service : %UserName% Votre mot de passe BlackBerry UEM Self-Service vous a peut-être été envoyé dans un e-mail séparé. Si vous ne l'avez pas reçu, contactez votre administrateur. Veuillez conserver ces informations dans vos dossiers. Si vous avez des questions, contactez votre administrateur. Bienvenue dans BlackBerry UEM !
E-mail d'activation Espace Travail uniquement (profils professionnels Android) par défaut Deuxième e-mail	**Objet : mot de passe d'activation de votre terminal sur BlackBerry UEM** %UserDisplayName%, Votre administrateur a activé votre terminal Android pour BlackBerry UEM. L'activation de votre terminal nécessite les informations suivantes : • Mot de passe d'activation de votre terminal : %ActivationPassword% • Votre mot de passe expirera le %ActivationPasswordExpiry% Suivez les instructions fournies dans l'e-mail « Activation de votre terminal sur BlackBerry UEM » pour activer votre terminal sur BlackBerry UEM. Si vous avez des questions, contactez votre administrateur. Bienvenue dans BlackBerry UEM !
E-mail de notification d'évènement BlackBerry UEM	**Objet : notification d'évènement BlackBerry UEM** L'évènement suivant est survenu : %AllEventVariables%

Nom	Texte suggéré
Notification d'activation de terminal	**Objet : le terminal a été activé sur BlackBerry UEM** %UserDisplayName%, Votre terminal a été activé sur BlackBerry UEM. Informations sur le terminal Modèle : %DeviceModel% Numéro de série : %SerialNumber% IMEI : %DeviceIMEI% Si vous n'avez pas activé ce terminal, contactez votre administrateur. **Objet : le terminal BlackBerry Dynamics a été activé sur BlackBerry UEM** %UserDisplayName%, Votre terminal BlackBerry Dynamics a été activé sur BlackBerry UEM. Si vous n'avez pas activé ce terminal, contactez votre administrateur.
Notification de connexion Self-Service	**Objet : notification de connexion Self-Service** %UserDisplayName%, Vous vous êtes connecté à BlackBerry UEM Self-Service. Adresse IP : %IPAddress% Heure : %Timestamp% Si vous n'êtes pas parvenu à vous connecter, contactez votre administrateur.

Gestion de terminaux à l'aide de stratégies informatiques

Vous pouvez utiliser des stratégies informatiques pour gérer la sécurité et le comportement des terminaux dans l'environnement BlackBerry UEM de votre organisation. Une stratégie informatique est un ensemble de règles que vous pouvez utiliser pour contrôler les fonctionnalités des terminaux. Par exemple, vous pouvez utiliser des règles de stratégie informatique pour imposer des exigences en matière de mot de passe, empêcher l'utilisation de certaines fonctionnalités du terminal (par exemple, l'appareil photo) et contrôler la disponibilité de certaines applications.

Vous pouvez configurer des règles pour tous les types de terminaux dans la même stratégie informatique. Le système d'exploitation du terminal détermine les fonctionnalités qui peuvent être contrôlées à l'aide de règles de stratégie informatique. Le type d'activation du terminal détermine quelles règles s'appliquent à un terminal spécifique et si vous pouvez utiliser des règles pour contrôler l'ensemble du terminal ou l'espace Travail uniquement. Les terminaux ignorent les règles de stratégie informatique non applicables.

Téléchargez la fiche de référence des règles de stratégie informatique pour obtenir une référence complète de toutes les règles de stratégie informatique disponibles pour chaque type de terminal pris en charge par UEM.

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

UEM attribue une seule stratégie informatique à un terminal et utilise des règles prédéfinies pour déterminer la stratégie informatique à attribuer. Une stratégie informatique directement attribuée à un utilisateur est prioritaire sur une stratégie informatique attribuée via une appartenance à un groupe d'utilisateurs. Si un utilisateur est membre de plusieurs groupes d'utilisateurs dotés de stratégies informatiques différentes, le classement est utilisé pour déterminer la stratégie informatique à attribuer. Si le terminal d'un utilisateur appartient à un groupe de terminaux, la stratégie informatique attribuée au groupe de terminaux est prioritaire sur une stratégie informatique attribuée directement à l'utilisateur. Si le terminal appartient à plusieurs groupes de terminaux dotés de stratégies informatiques différentes, le classement est utilisé pour déterminer la stratégie informatique à attribuer.

Gestion des stratégies informatiques

Vous pouvez modifier la stratégie informatique par défaut ou créer des stratégies informatiques et les attribuer.

1. Dans la barre de menus de la console de gestion, cliquez sur **Stratégies et profils > Stratégie > Stratégies informatiques**.
2. Effectuez l'une des opérations suivantes :

Tâche	Étapes
Créez une stratégie informatique.	**a.** Cliquez sur +. **b.** Saisissez le nom et la description de la stratégie informatique. **c.** Cliquez sur l'onglet de chaque type de terminal et configurez les valeurs appropriées pour les règles de stratégie informatique. Pour plus d'informations sur l'utilisation des règles de stratégie informatique, consultez la fiche de référence des règles de stratégie informatique. **d.** Cliquez sur **Enregistrer**. **e.** Attribuez la stratégie informatique à des utilisateurs et des groupes.
Copiez une stratégie informatique.	**a.** Cliquez sur le nom de la stratégie informatique que vous souhaitez copier. **b.** Cliquez sur . **c.** Saisissez le nom et la description de la stratégie informatique. **d.** Cliquez sur l'onglet de chaque type de terminal et configurez les valeurs appropriées pour les règles de stratégie informatique. Pour plus d'informations sur l'utilisation des règles de stratégie informatique, consultez la fiche de référence des règles de stratégie informatique. **e.** Cliquez sur **Enregistrer**. **f.** Attribuez la stratégie informatique à des utilisateurs et des groupes.
Modifiez une stratégie informatique.	**a.** Cliquez sur le nom de la stratégie informatique que vous souhaitez modifier. **b.** Cliquez sur . **c.** Apportez les modifications dans l'onglet correspondant à chaque type de terminal. **d.** Cliquez sur **Enregistrer**.
Classez les stratégies informatiques.	**a.** Cliquez sur . **b.** Utilisez les flèches pour déplacer les stratégies informatiques vers le haut ou le bas du classement. **c.** Cliquez sur **Enregistrer**.
Supprimez une stratégie informatique de comptes d'utilisateur.	**a.** Cliquez sur le nom de la stratégie informatique que vous souhaitez supprimer. **b.** Sous l'onglet **Attribué à x utilisateurs**, recherchez et sélectionnez les comptes d'utilisateur dont vous souhaitez supprimer la stratégie informatique. **c.** Cliquez sur .

Tâche	Étapes
Supprimez une stratégie informatique de groupes.	**a.** Cliquez sur le nom de la stratégie informatique que vous souhaitez supprimer. **b.** Sous l'onglet **Attribué à x groupes**, recherchez et sélectionnez les groupes dont vous souhaitez supprimer la stratégie informatique. **c.** Cliquez sur .
Supprimez une stratégie informatique.	Vous ne pouvez pas supprimer la stratégie informatique par défaut. Lorsque vous supprimez une stratégie informatique personnalisée, UEM supprime la stratégie informatique des utilisateurs et des terminaux auxquels elle a été attribuée. **a.** Sélectionnez la stratégie informatique que vous souhaitez supprimer. **b.** Cliquez sur . **c.** Cliquez sur **Supprimer**.
Exportez les stratégies informatiques dans un fichier .xml.	**a.** Sélectionnez les stratégies informatiques que vous souhaitez exporter. **b.** Cliquez sur .

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

BlackBerry envoie régulièrement des mises à jour des stratégies informatiques et des métadonnées de terminal à BlackBerry UEM. Par exemple, lorsqu'un fournisseur publie un nouveau modèle de terminal, BlackBerry peut envoyer des métadonnées de terminal mises à jour à UEM afin que les profils d'activation et de conformité incluent le nouveau modèle de terminal. Lorsqu'un fournisseur publie une mise à jour du système d'exploitation, un nouveau pack de stratégies informatiques peut être envoyé à UEM pour vous permettre de gérer les nouvelles fonctionnalités du système d'exploitation.

Par défaut, UEM reçoit et installe ces mises à jour automatiquement. Si la stratégie de sécurité de votre organisation n'autorise pas les mises à jour automatiques et que vous disposez d'un environnement UEM sur site, vous pouvez désactiver les mises à jour automatiques et les importer manuellement. Les fichiers de mise à jour sont cumulatifs. Si vous manquez une mise à jour, la mise à jour suivante installe toutes les règles de stratégie informatique ou les métadonnées de terminal mises à jour précédemment. Vous pouvez configurer des notifications d'évènement pour informer les administrateurs de l'installation des mises à jour des stratégies informatiques et des métadonnées de terminal.

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

1. Sur la barre de menus de la console de gestion de, cliquez sur **Paramètres > Infrastructure > Importer les données de configuration**.
2. Effectuez l'une des opérations suivantes :
   - Pour désactiver les mises à jour automatiques des packs de stratégies informatiques, décochez la case **Mettre à jour automatiquement les données des packs de stratégies informatiques**.
   - Pour désactiver les mises à jour automatiques des métadonnées de terminal, décochez la case **Mettre à jour automatiquement les métadonnées de terminal**.

3. Cliquez sur le bouton **Parcourir** approprié pour accéder au fichier de données à importer et le sélectionner. Cliquez sur **Ouvrir**.

Création de messages de support de terminal pour les fonctionnalités désactivées sur les terminaux Android

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

1. Sur la barre de menus de la console de gestion, cliquez sur **Paramètres > Paramètres généraux > Messages de support de terminal personnalisés**.
2. Dans la liste déroulante **Langue du terminal**, sélectionnez la langue dans laquelle vous souhaitez que la notification s'affiche.
3. Dans le champ **Note de fonctionnalité désactivée**, saisissez le texte que vous souhaitez afficher sur les terminaux lorsqu'une fonctionnalité est désactivée.
4. Dans le champ **Message de support administrateur**, vous pouvez également saisir une note qui s'affiche sur l'écran des paramètres des administrateurs de terminaux.
5. Si vous souhaitez créer un message dans plusieurs langues, cliquez sur **Ajouter une langue supplémentaire** et répétez les étapes précédentes.
6. Si vous avez ajouté des messages dans plusieurs langues, sélectionnez le bouton radio **Langue par défaut** de la langue que vous souhaitez utiliser voir s'afficher sur les terminaux qui n'utilisent pas l'une des langues spécifiées.
7. Cliquez sur **Enregistrer**.

Application des règles de conformité aux terminaux

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

Un profil de conformité spécifie les conditions susceptibles de rendre un terminal non conforme, les notifications qu'un utilisateur reçoit lorsqu'un terminal n'est pas conforme et les actions que BlackBerry UEM doit entreprendre si un problème de conformité n'est pas résolu (par exemple, limiter l'accès d'un utilisateur aux ressources de l'organisation, supprimer les données professionnelles du terminal ou supprimer toutes les données du terminal).

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

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

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

Créer un profil de conformité

Avant de commencer :

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

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

1. Sur la barre de menus de la console de gestion, cliquez sur **Stratégies et profils > Conformité > Conformité**.
2. Cliquez sur +.
3. Saisissez le nom et la description du profil.
4. Dans la liste déroulante **E-mail envoyé lorsqu'une violation est détectée**, sélectionnez un modèle d'e-mail.

Il s'agit de l'e-mail de conformité par défaut que UEM envoie à un utilisateur lorsqu'une violation de conformité est détectée. Lorsque vous activez les règles de conformité à l'étape 7, vous avez la possibilité de sélectionner différents modèles d'e-mail pour chaque règle de conformité, le cas échéant.

5. Dans la liste déroulante **Intervalle d'application**, sélectionnez la fréquence des contrôles de conformité des applications BlackBerry Dynamics. Vous ne pouvez pas configurer d'intervalle d'application pour les contrôles de conformité autres que BlackBerry Dynamics, qui se produisent à intervalles réguliers.
6. Développez la section **Envoi d'une notification de terminal lorsqu'une violation est détectée** et, si nécessaire, modifiez le message. Vous pouvez intégrer des variables dans le message pour ajouter des informations spécifiques sur l'utilisateur, le terminal et la conformité. Reportez-vous à la section Utilisation de variables dans les profils, les e-mails et les notifications.
7. Cliquez sur l'onglet correspondant à chaque type de terminal de votre organisation et configurez les valeurs appropriées pour chaque paramètre de profil. Pour plus de détails sur chaque paramètre de profil, consultez ce qui suit :
   - Communs : paramètres de profil de conformité
   - iOS et iPadOS : paramètres de profil de conformité
   - macOS : paramètres de profil de conformité
   - Android : paramètres de profil de conformité
   - Windows : paramètres de profil de conformité
8. Cliquez sur **Enregistrer**.

À la fin :

- Attribuez le profil à des utilisateurs et à des groupes.
- Si nécessaire, classez le profil.
- Pour surveiller les évènements de conformité détectés par UEM, reportez-vous à Surveiller les évènements de conformité.

Communs : paramètres de profil de conformité

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

paramètre Profil de conformité	Description
Comportement de l'invite	Ce paramètre indique si UEM invite l'utilisateur à corriger un problème de conformité et donne à l'utilisateur le temps de le résoudre avant de prendre des mesures, ou si UEM prend des mesures immédiates.
Méthode d'invite	Ce paramètre spécifie si UEM invite l'utilisateur à corriger un problème de conformité en envoyant une notification de terminal ou un e-mail et une notification de terminal. Les applications BlackBerry Dynamics envoient uniquement des notifications sur les terminaux, quelle que soit la valeur de ce paramètre. Les notifications du terminal ne sont pas prises en charge sur les terminaux Windows 10. Ce paramètre est uniquement valide si le paramètre Comportement de l'invite est défini sur Invite à la conformité.

paramètre Profil de conformité	Description
Modèle d'e-mail utilisé lorsqu'une violation de conformité est détectée	Ce paramètre spécifie le modèle d'e-mail à envoyer à un utilisateur lorsque son terminal n'est pas conforme à la règle de conformité sélectionnée. Si vous sélectionnez « Utiliser le profil par défaut », UEM envoie le modèle d'e-mail par défaut que vous avez configuré pour le profil (e-mail envoyé en cas de détection d'une violation). Ce paramètre est uniquement valide si le paramètre « Méthode d'invite » est défini sur « Notification par e-mail et sur les terminaux ».
Nombre d'invites	Ce paramètre spécifie le nombre de fois où l'utilisateur est invité à corriger un problème de conformité. Ce paramètre est uniquement valide si le paramètre Comportement de l'invite est défini sur Invite à la conformité.
Intervalle entre les invites	Ce paramètre spécifie le délai entre les invites, en minutes, heures ou jours. Ce paramètre est uniquement valide si le paramètre Comportement de l'invite est défini sur Invite à la conformité.
Action d'application pour les terminaux	Ce paramètre spécifie l'action prise par UEM sur les terminaux non conformes. Les options disponibles peuvent varier en fonction du système d'exploitation et du type de règle de conformité : • Surveiller et consigner : UEM identifie la violation de conformité mais n'exécute aucune action d'application sur le terminal. • Ne pas faire confiance : l'utilisateur ne peut pas accéder aux ressources et applications professionnelles du terminal. Les données et les applications ne sont pas supprimées. sur les terminaux iOS et iPadOS, le compte de messagerie professionnel est supprimé de l'application de messagerie d'origine. Les utilisateurs doivent restaurer les paramètres du compte de messagerie de l'application, une fois le terminal redevenu conforme. • Supprimer uniquement les données professionnelles • Supprimer toutes les données • Supprimer du serveur Ce paramètre ne s'applique pas aux terminaux activés avec Confidentialité de l'utilisateur. Sur les terminaux activés avec « Travail et Personnel - Confidentialité des données de l'utilisateur », il vous est impossible de supprimer toutes les données d'un terminal d'utilisateur. Si vous sélectionnez Supprimer toutes les données, UEM exécute la même action qu'avec Supprimer uniquement les données professionnelles. Les actions d'application de la règle Une application interdite est installée ne concernent pas les terminaux iOS et iPadOS supervisés. L'installation d'applications interdites est impossible.

paramètre Profil de conformité	Description
Action d'application pour les applications BlackBerry Dynamics	Ce paramètre spécifie comment traiter les applications BlackBerry Dynamics lorsqu'un terminal n'est pas conforme : • Ne pas autoriser l'exécution d'applications BlackBerry Dynamics • Supprimer les données d'applications BlackBerry Dynamics • Surveiller et consigner : UEM identifie la violation de conformité mais n'exécute aucune action d'application.

iOS et iPadOS : paramètres de profil de conformité

Consultez Communs : paramètres de profil de conformité pour obtenir des descriptions des actions d'application que BlackBerry UEM peut effectuer si un terminal enfreint une règle de conformité.

paramètre Profil de conformité	Description
Système d'exploitation cracké	Ce paramètre crée une règle de conformité qui garantit qu'il ne sera pas possible de cracker les terminaux. Un terminal est cracké lorsqu'un utilisateur ou un utilisateur malveillant contourne différentes restrictions pour modifier le système d'exploitation d'un terminal. Si vous sélectionnez ce paramètre, les utilisateurs ne pourront pas effectuer de nouvelles activations sur un terminal cracké, quelle que soit l'action d'application que vous avez définie.
Échec de l'attestation du terminal géré	Ce paramètre crée une règle de conformité qui spécifie les actions qui se produisent si un terminal ne passe pas l'attestation de terminal géré.
L'application non attribuée est installée	Ce paramètre crée une règle de conformité pour empêcher l'installation d'applications non attribuées sur les terminaux des utilisateurs. Ce paramètre ne s'applique pas aux terminaux utilisant le type d'activation Confidentialité de l'utilisateur.
Une application requise n'est pas installée	Ce paramètre crée une règle de conformité pour veiller à ce que les applications requises soient installées sur les terminaux.
Une version limitée du SE est installée	Ce paramètre crée une règle de conformité pour vérifier qu'aucune version limitée du système d'exploitation n'est installée sur les terminaux. Vous pouvez sélectionner les versions limitées du système d'exploitation. Si vous sélectionnez ce paramètre, les utilisateurs ne peuvent pas effectuer de nouvelles activations pour les terminaux qui ne sont pas conformes, quelle que soit l'action d'application que vous avez définie.

paramètre Profil de conformité	Description
Modèle de terminal interdit détecté	Ce paramètre crée une règle de conformité permettant d'interdire certains modèles de terminaux. Vous pouvez sélectionner les modèles de terminaux autorisés ou interdits. Si vous sélectionnez ce paramètre, les utilisateurs ne peuvent pas effectuer de nouvelles activations pour les terminaux qui ne sont pas conformes, quelle que soit l'action d'application que vous avez définie.
Mise à jour du système d'exploitation non appliquée	Ce paramètre crée une règle de conformité pour exécuter des actions de conformité si un utilisateur n'applique pas une mise à jour du système d'exploitation en attente au cours d'une période que vous spécifiez.
Terminal non joignable	Ce paramètre crée une règle de conformité pour veiller à ce que les terminaux ne restent pas déconnectés de UEM au-delà du laps de temps spécifié. Vous spécifiez le nombre de jours pendant lesquels un terminal peut rester déconnecté UEM avant de ne plus être conforme.
Vérification de la version de la bibliothèque BlackBerry Dynamics	Ce paramètre crée une règle de conformité qui vous permet de sélectionner les versions de la bibliothèque BlackBerry Dynamics ne pouvant pas être activées. Vous pouvez sélectionner les versions bloquées de la bibliothèque.
Vérification de la connectivité BlackBerry Dynamics	Ce paramètre crée une règle de conformité pour veiller à ce que les applications BlackBerry Dynamics ne restent pas déconnectées de UEM au-delà du laps de temps spécifié. L'action de mise en œuvre concerne les applications BlackBerry Dynamics. Le paramètre Baser l'intervalle de connectivité sur des applications de délégation de l'authentification indique que la vérification de la connectivité est basée sur le moment où une application de délégation de l'authentification se connecte à UEM. Ce paramètre s'applique uniquement si une délégation d'authentification est spécifiée dans un profil BlackBerry Dynamics. Le paramètre Heure du dernier contact spécifie le nombre de jours pendant lesquels un terminal peut rester déconnecté de UEM avant de ne plus être conforme. Les applications BlackBerry Dynamics n'invitent pas les utilisateurs à respecter cette règle. Si vous définissez le paramètre Comportement d'invite sur Invite à la conformité, l'utilisateur n'est pas invité à le faire. Si le terminal est en mesure de contacter UEM, il revient en conformité lorsque l'utilisateur ouvre l'application BlackBerry Dynamics.

paramètre Profil de conformité	Description
Détection de capture d'écran BlackBerry Dynamics sur les terminaux iOS	**Remarque :** Cette règle de conformité a été remplacée par l'option « Ne pas autoriser les captures d'écran sur les terminaux iOS » dans les profils BlackBerry Dynamics. BlackBerry recommande d'utiliser le paramètre de profil et de désactiver cette règle de conformité. Cette règle de conformité sera obsolète dans une future version de UEM. Ce paramètre crée une règle de conformité qui réagit aux captures d'écran des applications BlackBerry Dynamics sur les terminaux. Le paramètre Nombre maximal de captures d'écran au cours de la période spécifie le nombre de captures d'écran autorisées dans un délai spécifié. Le paramètre Action d'application pour les applications BlackBerry Dynamics spécifie l'action qui se produit si l'utilisateur dépasse le nombre autorisé de captures d'écran.
Une application interdite est installée	Ce paramètre crée une règle de conformité pour UEM afin de vérifier régulièrement la présence d'applications interdites, y compris les applications Marketplace. Ajoutez des applications à la liste des applications limitées du profil en sélectionnant les applications dans la liste des applications limitées UEM ou en sélectionnant une application intégrée (terminaux supervisés uniquement). Lorsque vous sélectionnez ce paramètre et qu'une application limitée est installée sur un terminal, un message d'avertissement et un lien sont affichés sur l'écran Terminaux gérés de la console. Lorsque vous cliquez sur le lien, la liste des applications qui mettent le terminal hors conformité est affichée. La liste des applications limitées est également envoyée à l'utilisateur dans la notification de conformité. Les actions d'application de cette règle ne concernent pas les terminaux supervisés. L'installation d'applications interdites est impossible. Si des applications limitées (intégrées ou installées par l'utilisateur) sont déjà installées, ces applications sont automatiquement supprimées du terminal.
Afficher les applications autorisées sur le terminal uniquement	Ce paramètre crée une règle de conformité répertoriant les applications qui peuvent être installées sur les terminaux, y compris les applications Marketplace. Toutes les autres applications sont interdites. Ajoutez des applications à la liste des applications limitées du profil en sélectionnant les applications dans la liste des applications limitées UEM ou en sélectionnant des applications intégrées. Par défaut, certaines applications sont incluses dans la liste autorisée. Ce paramètre est valide uniquement pour les terminaux supervisés.

macOS : paramètres de profil de conformité

Consultez Communs : paramètres de profil de conformité pour obtenir des descriptions des actions d'application que BlackBerry UEM peut effectuer si un terminal enfreint une règle de conformité.

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

Android : paramètres de profil de conformité

Consultez Communs : paramètres de profil de conformité pour obtenir des descriptions des actions d'application que BlackBerry UEM peut effectuer si un terminal enfreint une règle de conformité.

paramètre Profil de conformité	Description
OS « flashé » ou échec de l'attestation Knox	Ce paramètre crée une règle de conformité qui spécifie les actions qui se produisent si un utilisateur ordinaire ou un utilisateur malveillant accède au niveau racine d'un terminal Android. Si vous sélectionnez ce paramètre, les utilisateurs ne pourront pas effectuer de nouvelles activations pour les terminaux routés, quelle que soit l'action d'application que vous avez définie. La sélection de l'option « Activer la détection des débogueurs et des émulateurs lors de l'exécution des applications BlackBerry Dynamics » arrête les applications BlackBerry Dynamics si Runtime BlackBerry Dynamics détecte un outil de débogage ou d'émulation actif. La sélection de l'option « Activer la détection des terminaux de démarrage non verrouillés ou non vérifiés pour les applications BlackBerry Dynamics » permet à UEM de vérifier l'état de démarrage du terminal.
Échec d'attestation SafetyNet ou Play Integrity	Ce paramètre crée une règle de conformité qui spécifie les actions qui se produisent si les terminaux ne passent pas l'attestation SafetyNet ou Play Integrity. Lorsque vous utilisez l'attestation SafetyNet ou Play Integrity, UEM vérifie l'authenticité et l'intégrité des terminaux et des applications Android dans l'environnement de votre entreprise. Reportez-vous à la section Configuration de l'attestation relative aux terminaux Android et aux applications BlackBerry Dynamics.
L'application non attribuée est installée	Ce paramètre crée une règle de conformité pour empêcher l'installation d'applications non attribuées sur les terminaux des utilisateurs. Lorsque vous sélectionnez ce paramètre et qu'une application non attribuée est installée sur un terminal Android, un message d'avertissement et un lien sont affichés sur l'écran Terminaux gérés de la console. Lorsque vous cliquez sur ce lien, la liste des applications non attribuées s'affiche. Pour les terminaux Android Enterprise, Android Management et Samsung Knox, les utilisateurs ne peuvent pas installer d'applications non attribuées dans l'espace Travail. Les mesures d'application ne s'appliquent pas. Ce paramètre ne s'applique pas aux terminaux activés en mode Confidentialité de l'utilisateur.
Une application requise n'est pas installée	Ce paramètre crée une règle de conformité pour veiller à ce que les applications requises soient installées sur les terminaux. Lorsque vous sélectionnez ce paramètre et qu'une application requise n'est pas installée sur un terminal Android, un message d'avertissement et un lien sont affichés sur l'écran Terminaux gérés de la console. Pour les terminaux Android Enterprise et Android Management, les actions d'application ne s'appliquent pas. Pour les terminaux Samsung Knox, les applications internes requises sont automatiquement installées. Les mesures d'application s'appliquent uniquement aux applications publiques requises.

paramètre Profil de conformité	Description
Une version limitée du SE est installée	Ce paramètre crée une règle de conformité pour vérifier qu'aucune version limitée du système d'exploitation n'est installée sur les terminaux. Vous pouvez sélectionner les versions limitées du système d'exploitation. Si vous sélectionnez ce paramètre, les utilisateurs ne pourront pas effectuer de nouvelles activations pour les terminaux qui ne sont pas conformes, quelle que soit l'action d'application que vous avez définie.
Modèle de terminal interdit détecté	Ce paramètre crée une règle de conformité permettant d'interdire certains modèles de terminaux. Vous pouvez spécifier les modèles de terminaux autorisés ou interdits. Si vous sélectionnez ce paramètre, les utilisateurs ne pourront pas effectuer de nouvelles activations pour les terminaux qui ne sont pas conformes, quelle que soit l'action d'application que vous avez définie.
Mise à jour du système d'exploitation non appliquée	Ce paramètre crée une règle de conformité pour exécuter des actions de conformité si un utilisateur n'applique pas une mise à jour du système d'exploitation en attente au cours d'une période que vous spécifiez.
Terminal non joignable	Ce paramètre crée une règle de conformité pour veiller à ce que les terminaux ne restent pas déconnectés de UEM au-delà du laps de temps spécifié. Le paramètre Heure du dernier contact spécifie le nombre de jours pendant lesquels un terminal peut rester déconnecté de UEM avant de ne plus être conforme.
Le niveau de correctif de sécurité requis n'est pas installé	Ce paramètre crée une règle de conformité pour veiller à ce que les correctifs de sécurité requis soient installés sur les terminaux. Vous pouvez spécifier les modèles de terminal sur lesquels les correctifs de sécurité doivent être installés, ainsi qu'une date pour ces correctifs. Les terminaux exécutant un correctif de sécurité de date équivalente ou ultérieure aux dates de correctif de sécurité spécifiées sont considérés comme conformes. Après une mise à niveau, si vous avez déjà créé un profil de conformité avec le paramètre Niveau requis du correctif de sécurité manquant activé, l'action d'application est définie sur Surveiller et consigner.
Vérification de la version de la bibliothèque BlackBerry Dynamics	Ce paramètre crée une règle de conformité qui vous permet de sélectionner les versions de la bibliothèque BlackBerry Dynamics ne pouvant pas être activées. Vous pouvez sélectionner les versions bloquées de la bibliothèque.

paramètre Profil de conformité	Description
Vérification de la connectivité BlackBerry Dynamics	Ce paramètre crée une règle de conformité pour veiller à ce que les applications BlackBerry Dynamics ne restent pas déconnectées de UEM au-delà du laps de temps spécifié. L'action de mise en œuvre concerne les applications BlackBerry Dynamics. Le paramètre Baser l'intervalle de connectivité sur des applications de délégation de l'authentification indique que la vérification de la connectivité est basée sur le moment où une application de délégation de l'authentification se connecte à UEM. Ce paramètre s'applique uniquement si une délégation d'authentification est spécifiée dans un profil BlackBerry Dynamics attribué. Le paramètre Heure du dernier contact spécifie le nombre de jours pendant lesquels un terminal peut rester déconnecté de UEM avant de ne plus être conforme.
Une application interdite est installée	Ce paramètre crée une règle de conformité pour vérifier qu'aucune application interdite n'est installée sur les terminaux. Pour limiter les applications, reportez-vous à la section Ajouter une application à la liste des applications limitées. Pour les terminaux Android Enterprise et Android Management, les utilisateurs ne peuvent pas installer d'applications interdites dans l'espace Travail. Les mesures d'application ne s'appliquent pas. Pour les terminaux Samsung Knox, les applications interdites dans l'espace Travail sont automatiquement désactivées. Les mesures d'application ne s'appliquent pas. Pour les terminaux avec le type d'activation Travail et Personnel - Contrôle total (Samsung Knox), sélectionnez Appliquer les mesures de conformité dans l'espace personnel pour appliquer la règle aux applications du profil professionnel et du profil personnel. Ce paramètre ne s'applique pas aux terminaux activés en mode Confidentialité de l'utilisateur. Lorsque vous sélectionnez ce paramètre et qu'une application interdite est installée sur un terminal Android, un message d'avertissement et un lien sont affichés sur l'écran Terminaux gérés de la console. Lorsque vous cliquez sur ce lien, la liste des applications interdites s'affiche.
Le mot de passe ne répond pas aux critères de complexité	Ce paramètre crée une règle de conformité pour faire en sorte que l'utilisateur définisse des mots de passe pour le terminal ou l'espace Travail répondant aux exigences de complexité définies dans la stratégie informatique attribuée.

Windows : paramètres de profil de conformité

Consultez Communs : paramètres de profil de conformité pour obtenir des descriptions des actions d'application que BlackBerry UEM peut effectuer si un terminal enfreint une règle de conformité.

Paramètre Profil de conformité	Description
Une application requise n'est pas installée	Ce paramètre crée une règle de conformité pour veiller à ce que les applications requises soient installées sur les terminaux. Les dispositions des applications internes ne peuvent pas être surveillées.
Une version limitée du SE est installée	Ce paramètre crée une règle de conformité pour vérifier qu'aucune version limitée du système d'exploitation n'est installée sur les terminaux. Vous pouvez sélectionner les versions limitées du système d'exploitation.
Modèle de terminal interdit détecté	Ce paramètre crée une règle de conformité permettant d'interdire certains modèles de terminaux. Vous pouvez sélectionner les modèles de terminaux autorisés ou interdits.
Terminal non joignable	Ce paramètre crée une règle de conformité pour veiller à ce que les terminaux ne restent pas déconnectés de UEM au-delà du laps de temps spécifié.
Vérification de la version de la bibliothèque BlackBerry Dynamics	Ce paramètre crée une règle de conformité qui vous permet de sélectionner les versions de la bibliothèque BlackBerry Dynamics ne pouvant pas être activées. Vous pouvez sélectionner les versions bloquées de la bibliothèque.
Vérification de la connectivité BlackBerry Dynamics	Ce paramètre crée une règle de conformité pour veiller à ce que les applications BlackBerry Dynamics ne restent pas déconnectés de UEM au-delà du laps de temps spécifié. L'action de mise en œuvre concerne les applications BlackBerry Dynamics.
Signature antivirus	Ce paramètre crée une règle de conformité pour veiller à ce qu'une signature antivirus soit activée sur les terminaux.
État de l'antivirus	Ce paramètre crée une règle de conformité pour veiller à ce qu'un logiciel antivirus soit activé sur les terminaux. Vous pouvez sélectionner les fournisseurs autorisés.
État du pare-feu	Ce paramètre crée une règle de conformité pour veiller à ce qu'un pare-feu soit activé sur les terminaux.
État de cryptage	Ce paramètre crée une règle de conformité pour veiller à ce que le cryptage soit activé sur les terminaux.
État des mises à jour Windows	Ce paramètre crée une règle de conformité pour veiller à ce que les terminaux autorisent UEM à installer les mises à jour de Windows OS ou avertissent les utilisateurs lorsque des mises à jour obligatoires sont disponibles.
Une application interdite est installée	Ce paramètre crée une règle de conformité pour vérifier qu'aucune application interdite n'est installée sur les terminaux. Pour limiter les applications, reportez-vous à la section Ajouter une application à la liste des applications limitées.
Attestation d'intégrité du terminal Windows	
Le délai de grâce a expiré	Ce paramètre crée une règle de conformité pour spécifier les actions qui se produisent si l'attestation du délai de grâce a expiré.

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

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

Surveiller les évènements de conformité

Une fois que vous avez configuré et attribué des profils de conformité aux utilisateurs, vous pouvez utiliser l'écran des évènements de conformité pour surveiller et suivre les violations de conformité sur les terminaux iOS Android macOS et Windows des utilisateurs. Cet écran affiche également tous les évènements de conformité liés aux fonctionnalités de CylancePROTECT Mobile pour UEM.

Avant de commencer : Créer et attribuer des profils de conformité.

1. Sur la barre de menus de la console de gestion, cliquez sur **Utilisateurs > Violations de conformité**.
2. Effectuez l'une des opérations suivantes :
   - Par défaut, cet écran affiche les nouveaux évènements de conformité correspondant à la plage de dates indiquée. Pour afficher les alertes résolues ou ignorées ou toutes les alertes, ou pour modifier la plage de dates, cliquez sur **Modifier**. Définissez le statut et la plage de dates, puis cliquez sur **Soumettre**.
   - Dans la section **Filtres**, définissez les filtres appropriés pour les évènements de conformité que vous souhaitez afficher, puis cliquez sur **Soumettre**.
   - Cliquez sur pour définir les colonnes que vous souhaitez afficher.
   - Cliquez sur une colonne pour trier les évènements en fonction de ces critères.
   - Utilisez le champ de recherche pour rechercher des évènements de conformité spécifiques.
3. Si vous souhaitez supprimer un évènement de cette vue, sélectionnez l'évènement et cliquez sur . Le fait d'ignorer un évènement le supprime de cette vue, cela n'affecte pas l'état de conformité du terminal associé.
4. Pour exporter des évènements sélectionnés dans un fichier .csv, sélectionnez les évènements et cliquez sur .

Notez que, quel que soit leur état, les évènements de conformité sont automatiquement supprimés de cette vue au bout de 120 jours. Les évènements dont l'état est ignoré ou résolu sont automatiquement supprimés au bout de 7 jours.

Envoi de commandes aux utilisateurs et aux terminaux

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

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

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

Envoi de commandes aux utilisateurs et aux terminaux

1. Sur la barre de menus de la console de gestion, cliquez sur **Utilisateurs > Terminaux gérés**.
2. Effectuez l'une des opérations suivantes :

Tâche	Étapes
Envoyer une commande à un utilisateur ou à un terminal spécifique	**a.** Recherchez un utilisateur et cliquez dessus. **b.** Sous l'onglet Terminal, accédez à la section **Gérer le terminal** et cliquez sur la commande appropriée.
Envoyer une commande groupée à plusieurs utilisateurs ou terminaux	**a.** Recherchez plusieurs utilisateurs et sélectionnez-les. **b.** Dans le menu de commandes situé au-dessus de la liste des utilisateurs, cliquez sur la commande appropriée.

Pour plus d'informations sur les commandes disponibles, consultez ce qui suit :

- Commandes pour terminaux iOS et iPadOS.
- Commandes pour terminaux macOS.
- Commandes pour terminaux Android.
- Commandes pour terminaux Windows.

À la fin : Si vous souhaitez définir un délai d'expiration pour les commandes Supprimer toutes les données du terminal et Supprimer uniquement les données professionnelles, consultez Définir une heure d'expiration pour les commandes.

Définir une heure d'expiration pour les commandes

Lorsque vous envoyez la commande « Supprimer toutes les données du terminal » ou « Supprimer uniquement des données professionnelles » à un terminal, ce dernier doit être connecté à BlackBerry UEM pour que la commande se termine. Si le terminal ne parvient pas à se connecter à UEM, la commande reste en attente et

le terminal n'est pas supprimé d'UEM, sauf si vous le supprimez manuellement. Sinon, vous pouvez configurer UEM pour supprimer automatiquement les terminaux lorsque les commandes ne se terminent pas après le délai spécifié.

1. Sur la barre de menus de la console de gestion, cliquez sur **Paramètres > Paramètres généraux > Supprimer l'expiration de la commande**.
2. Pour l'une des commandes ou pour les deux, sélectionnez **Supprimer automatiquement le terminal si la commande expire**.
3. Dans le champ **Expiration de la commande**, saisissez le nombre de jours après lequel la commande expire et le terminal est automatiquement retiré de UEM.
4. Cliquez sur **Enregistrer**.

Commandes pour terminaux iOS et 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.	Contrôles MDM Confidentialité de l'utilisateur
Afficher les actions du terminal	Cette commande affiche les actions en cours sur un 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 UEM à l'issue de sa suppression, seules les données professionnelles sont supprimées du terminal. Si vous envoyez la commande à des terminaux dotés de iOS 17 ou une version ultérieure, vous pouvez sélectionner l'option « Activer le retour au service » et sélectionner un profil Wi-Fi à attribuer aux terminaux pour aider l'utilisateur à configurer à nouveau le terminal après la suppression des données. Si des informations eSIM sont détectées sur un ou plusieurs terminaux que vous sélectionnez, vous êtes invité à spécifier si les informations du forfait de données doivent être conservées.	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 UEM lorsque vous envoyez cette commande, vous pouvez annuler la commande ou supprimer le terminal de la console. Si le terminal se connecte à UEM à l'issue de sa suppression, les données professionnelles sont supprimées du terminal.	Contrôles MDM Confidentialité de l'utilisateur
Verrouiller le terminal	Cette commande verrouille un terminal. Apple ajoute la mention « iPhone perdu » ou « iPad perdu » au titre du message que vous indiquez. L'utilisateur doit saisir le mot de passe du terminal existant pour déverrouiller le terminal. 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 d'afficher un numéro de téléphone et un message sur l'écran. Après avoir envoyé cette commande, vous pouvez voir l'emplacement du terminal dans la console de gestion. 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 BlackBerry 2FA	Cette commande désactive les terminaux qui sont activés avec le type d'activation BlackBerry 2FA. Le terminal est supprimé de 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. 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
Redémarrer le terminal	Cette commande force le terminal 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 la désactivation du terminal. 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 efface les données de toutes les applications gérées par Microsoft Intune sur le terminal. Les applications ne sont pas supprimées du terminal.	Contrôles MDM
Mettre à jour les informations du terminal	Cette commande envoie et reçoit des informations mises à jour sur le terminal. Par exemple, vous pouvez envoyer des règles de stratégie informatique ou des profils mis à jour à un terminal et recevoir des informations mises à jour sur un terminal comme la version du système d'exploitation ou le niveau de la batterie.	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 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 UEM, l'utilisateur reçoit une notification et le terminal ne pourra pas communiquer avec UEM s'il n'est pas réactivé.	Contrôles MDM Confidentialité de l'utilisateur
Actualiser une carte eSIM	Pour les terminaux disposant d'un forfait cellulaire basé sur une carte eSIM, cette commande interroge les détails du forfait mis à jour pour le terminal à partir de l'URL de l'opérateur du terminal.	Contrôles MDM

Commandes pour terminaux macOS

Commande	Description
Afficher le rapport de terminal	Cette commande affiche des informations détaillées sur un terminal. Vous pouvez exporter et enregistrer le rapport de terminal.

Commande	Description
Afficher les actions du terminal	Cette commande affiche les actions en cours sur un terminal.
Verrouiller le bureau	Cette commande permet de définir un code PIN et de verrouiller le terminal.
Supprimer uniquement les données professionnelles	Cette commande supprime les données professionnelles, y compris les stratégies informatiques, profils, applications et certificats présents sur le terminal et supprime éventuellement le terminal de BlackBerry UEM.
Supprimer toutes les données du terminal	Cette commande permet de supprimer les informations utilisateur et les données des applications stockées du terminal. Il rétablit les réglages d'usine par défaut du terminal, verrouille le terminal avec un code PIN que vous définissez et supprime éventuellement le terminal du UEM.
Mettre à jour les données du bureau	Cette commande envoie et reçoit des informations mises à jour sur le terminal. Par exemple, vous pouvez envoyer des règles de stratégie informatique ou des profils mis à jour à un terminal et recevoir des informations mises à jour sur un terminal comme la version du système d'exploitation ou le niveau de la batterie.
Supprimer le terminal	Cette commande supprime le terminal de UEM. Le terminal peut continuer à recevoir des e-mails et d'autres données professionnelles.

Commandes pour terminaux Android

Pour les types d'activation Android Management, reportez-vous à la section Considérations relatives aux types d'activation Android Management.

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.	Tous (sauf BlackBerry 2FA)
Afficher les actions du terminal	Cette commande affiche les actions en cours sur un terminal.	Tous (sauf BlackBerry 2FA)

Commande	Description	Types d'activation
Verrouiller le terminal	Cette commande verrouille le terminal. L'utilisateur doit saisir le mot de passe du terminal existant pour déverrouiller le terminal. 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.	Travail et Personnel - Contrôle total (Android Management) Travail et Personnel - Confidentialité des données de l'utilisateur (Android Management) Espace Travail uniquement (Android Management) Travail et Personnel - Contrôle total (Android Enterprise) Travail et Personnel - Confidentialité des données de l'utilisateur (Android Enterprise) Espace Travail uniquement (Android Enterprise) Contrôles MDM
Supprimer toutes les données du terminal	Cette commande supprime toutes les informations utilisateur et données d'application stockées sur le terminal, y compris les informations de l'espace Travail, et rétablit les paramètres d'usine par défaut du terminal. Si le terminal ne parvient pas à se connecter à UEM lorsque vous envoyez cette commande, vous pouvez annuler la commande ou supprimer le terminal de la console. Si le terminal se connecte à UEM après que vous l'avez supprimé, seules les données professionnelles sont supprimées du terminal, y compris de l'espace Travail, le cas échéant.	Travail et Personnel - Contrôle total (Android Management) Espace Travail uniquement (Android Management) Travail et Personnel - Contrôle total (Android Enterprise) Travail et Personnel - Contrôle total (Samsung Knox) Contrôles MDM

Commande	Description	Types d'activation
Supprimer uniquement les données professionnelles	Cette commande supprime les données professionnelles, y compris la stratégie informatique, les profils, les applications et les certificats qui sont sur le terminal, et désactive le terminal. Si le terminal dispose d'un espace Travail, celui-ci est supprimé du terminal, mais toutes les applications et données personnelles sont conservées. Lorsque vous utilisez cette commande sur les terminaux Android Enterprise, vous pouvez saisir une raison qui apparaîtra dans la notification sur le terminal de l'utilisateur pour expliquer pourquoi le profil professionnel a été supprimé. Si le terminal ne parvient pas à se connecter à UEM lorsque vous envoyez cette commande, vous pouvez annuler la commande ou supprimer le terminal de la console. Si le terminal se connecte à UEM après que vous l'avez supprimé, les données professionnelles sont supprimées du terminal, y compris de l'espace Travail, le cas échéant.	Travail et Personnel - Contrôle total (Android Management) Travail et Personnel - Confidentialité des données de l'utilisateur (Android Management) Travail et Personnel - Contrôle total (Android Enterprise) Travail et Personnel - Confidentialité des données de l'utilisateur (Android Enterprise) Travail et Personnel - Contrôle total (Samsung Knox) Travail et Personnel - Confidentialité des données de l'utilisateur (Samsung Knox) Contrôles MDM
Déverrouiller le terminal et effacer le mot de passe	Cette commande déverrouille le terminal et invite l'utilisateur à créer un nouveau mot de passe pour le terminal. Si l'utilisateur ignore le message l'invitant à créer un mot de passe pour le terminal, le mot de passe existant est conservé. Vous pouvez utiliser cette commande si un utilisateur oublie le mot de passe de son terminal. Cette commande n'est pas prise en charge par les terminaux dotés de Samsung Knox SDK 3.2.1 ou version ultérieure.	Travail et Personnel - Contrôle total (Samsung Knox) Travail et Personnel - Confidentialité des données de l'utilisateur (Samsung Knox) Contrôles MDM (terminaux Samsung uniquement)
Spécifier le mot de passe du terminal et verrouiller le terminal	Cette commande vous permet de créer un mot de passe, puis de verrouiller le terminal. Vous devez créer un mot de passe conforme aux règles de mots de passe existantes. Pour déverrouiller le terminal, l'utilisateur doit saisir le nouveau mot de passe.	Travail et Personnel - Confidentialité des données de l'utilisateur (Android Management) Espace Travail uniquement (Android Management) Espace Travail uniquement (Android Enterprise) Travail et Personnel - Contrôle total (Samsung Knox)

Commande	Description	Types d'activation
Réinitialiser le mot de passe de l'espace Travail	Cette commande supprime le mot de passe actuel de l'espace Travail du terminal. Lorsque l'utilisateur ouvre l'espace Travail, le terminal l'invite à définir un nouveau mot de passe de l'espace Travail.	Travail et Personnel - Contrôle total (Samsung Knox) Travail et Personnel - Confidentialité des données de l'utilisateur - (Samsung Knox)
Spécifier le mot de passe de l'espace Travail et verrouiller	Cette commande permet de définir un mot de passe de profil professionnel et de verrouiller le terminal. Lorsque l'utilisateur ouvre une application professionnelle, il doit saisir le mot de passe que vous avez défini.	Travail et Personnel - Contrôle total (Android Enterprise) Travail et Personnel - Confidentialité des données de l'utilisateur (Android Enterprise)
Désactiver/Activer l'espace Travail	Cette commande désactive ou active l'accès aux applications de l'espace Travail sur le terminal.	Travail et Personnel - Contrôle total (Android Management) Travail et Personnel - Confidentialité des données de l'utilisateur (Android Management) Espace Travail uniquement (Android Management) Travail et Personnel - Contrôle total (Samsung Knox) Travail et Personnel - Confidentialité des données de l'utilisateur - (Samsung Knox)
Désactiver BlackBerry 2FA	Cette commande désactive les terminaux qui sont activés avec le type d'activation BlackBerry 2FA. Le terminal est supprimé de UEM et l'utilisateur ne peut pas utiliser la fonction BlackBerry 2FA.	BlackBerry 2FA
Nettoyage des applications	Cette commande efface les données de toutes les applications gérées par Microsoft Intune sur le terminal. Les applications ne sont pas supprimées du terminal.	Tout (sauf BlackBerry 2FA)
Mettre à jour les informations du terminal	Cette commande envoie et reçoit des informations mises à jour sur le terminal. Par exemple, vous pouvez envoyer des règles de stratégie informatique ou des profils mis à jour à un terminal et recevoir des informations mises à jour sur un terminal comme la version du système d'exploitation ou le niveau de la batterie.	Tous (sauf BlackBerry 2FA)

Commande	Description	Types d'activation
Demander un rapport de bogues	Cette commande envoie une requête au terminal pour les journaux du client. L'utilisateur du terminal doit accepter ou refuser la requête.	Espace Travail uniquement (Android Enterprise) Travail et Personnel - Contrôle total (Android Enterprise)
Redémarrer le terminal	Cette commande envoie une requête de redémarrage au terminal. Un message s'affiche pour indiquer à l'utilisateur que le terminal va redémarrer dans une minute. L'utilisateur du terminal peut reporter le redémarrage pour 10 minutes.	Espace Travail uniquement (Android Management) Espace Travail uniquement (Android Enterprise)
Supprimer le terminal	Cette commande supprime le terminal de 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 UEM, l'utilisateur reçoit une notification et le terminal ne pourra pas communiquer avec UEM s'il n'est pas réactivé.	Tous (sauf BlackBerry 2FA)

Commandes pour terminaux Windows

Commande	Description
Afficher le rapport de terminal	Cette commande affiche des informations détaillées sur un terminal. Vous pouvez exporter et enregistrer le rapport de terminal.
Afficher les actions du terminal	Cette commande affiche les actions en cours sur un terminal.
Verrouiller le terminal	Cette commande verrouille un terminal. L'utilisateur doit saisir le mot de passe du terminal existant pour déverrouiller le terminal. 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 est uniquement prise en charge sur les terminaux exécutant Windows 10 Mobile.

Commande	Description
Générer le mot de passe et verrouiller le terminal	Cette commande génère un mot de passe et verrouille le terminal. Le mot de passe généré est envoyé par e-mail à l'utilisateur. Vous pouvez utiliser l'adresse électronique présélectionnée ou spécifier une adresse électronique. Le mot de passe généré est conforme aux règles de mots de passe existantes. Cette commande est uniquement prise en charge sur les terminaux exécutant Windows 10 Mobile.
Supprimer uniquement les données professionnelles	Cette commande supprime les données professionnelles, y compris les stratégies informatiques, profils, applications et certificats présents sur le terminal et supprime éventuellement le terminal de BlackBerry UEM. Le compte d'utilisateur n'est pas supprimé lorsque vous envoyez cette commande. Après avoir envoyé cette commande, vous avez la possibilité de supprimer le terminal de UEM. Si le terminal ne parvient pas à se connecter à UEM, vous pouvez le supprimer de UEM. Si le terminal se connecte à UEM alors que vous l'avez supprimé, seules les données professionnelles sont supprimées du terminal, y compris de l'espace Travail, le cas échéant.
Supprimer toutes les données du terminal	Cette commande permet de supprimer les informations utilisateur et les données des applications stockées sur le terminal. Elle rétablit les paramètres d'usine par défaut sur le terminal et supprime éventuellement le terminal d'UEM. Après avoir envoyé cette commande, vous avez la possibilité de supprimer le terminal de UEM. Si le terminal ne parvient pas à se connecter à UEM, vous pouvez le supprimer de UEM. Si le terminal se connecte à UEM alors que vous l'avez supprimé, seules les données professionnelles sont supprimées du terminal, y compris de l'espace Travail, le cas échéant.
Redémarrer le bureau/ terminal	Cette commande force le terminal à redémarrer.
Mettre à jour les informations du terminal	Cette commande envoie et reçoit des informations mises à jour sur le terminal. Par exemple, vous pouvez envoyer des règles de stratégie informatique ou des profils mis à jour à un terminal et recevoir des informations mises à jour sur un terminal comme la version du système d'exploitation ou le niveau de la batterie. La commande envoie une requête au terminal pour créer une demande de validation de certificat d'intégrité. Le terminal envoie la requête au service d'attestation d'intégrité Microsoft pour en vérifier la conformité. Cette fonctionnalité est uniquement prise en charge dans un environnement sur site.
Supprimer le terminal	Cette commande supprime le terminal de UEM. Le terminal peut continuer à recevoir des e-mails et d'autres données professionnelles.

Contrôle des mises à jour logicielles installées sur les terminaux

Vous pouvez utiliser des profils de configuration logicielle minimale requise du terminal pour déterminer comment les mises à jour logicielles du terminal doivent être installées sur les terminaux Android Enterprise, Android Management et Samsung Knox, et comment les mises à jour d'applications doivent être gérées pour les applications exécutées en avant-plan.

Vous pouvez utiliser des règles de stratégie informatique pour contrôler les mises à jour logicielles appliquées aux terminaux iOS. Pour plus d'informations, reportez-vous à la Feuille de référence des stratégies informatiques. Vous pouvez également utiliser la console de gestion pour mettre à jour le système d'exploitation sur les terminaux iOS supervisés.

Création d'un profil de configuration logicielle minimale requise du terminal pour les terminaux Android Enterprise et Android Management

Les règles de mise à jour du système d'exploitation s'appliquent uniquement aux terminaux Android Enterprise et Android Management avec les types d'activation Espace Travail uniquement et Travail et Personnel - Contrôle total. Les règles de mise à jour de l'application s'appliquent à tous les terminaux Android Enterprise. Actuellement, la suspension des mises à jour du système d'exploitation et des mises à jour automatiques des applications n'est pas prise en charge pour les terminaux Android Management. Reportez-vous à Considérations relatives aux types d'activation de gestion Android.

1. Sur la barre de menus de la console de gestion, cliquez sur **Stratégies et profils > Conformité > Configuration logicielle minimale requise du terminal**.
2. Cliquez sur +.
3. Saisissez le nom et la description du profil.
4. Pour configurer les règles de mise à jour du système d'exploitation pour les terminaux Espace Travail uniquement et Travail et Personnel - Contrôle total, dans la section **Règle de mise à jour du système d'exploitation**, cliquez sur + et procédez comme suit :
   a) Dans la liste déroulante **Modèle du terminal**, sélectionnez un modèle de terminal.
   b) Dans la liste déroulante **Version du système d'exploitation**, sélectionnez la version du système d'exploitation installée.
   c) Dans la liste déroulante **Mettre à jour la règle**, sélectionnez l'une des options suivantes :
      - **Par défaut** : l'utilisateur peut choisir quand installer les mises à jour. Les utilisateurs dotés du type d'activation Espace Travail uniquement (terminal entièrement géré) ne peuvent pas choisir quand installer les mises à jour.
      - **Mise à jour automatique** : les mises à jour sont installées sans que l'utilisateur n'y soit invité.
      - **Mise à jour automatique entre** : les mises à jour sont installées dans le délai que vous spécifiez, sans que l'utilisateur n'y soit invité. L'utilisateur peut choisir d'installer les mises à jour en dehors de cette fenêtre.
      - **Reporter jusqu'à 30 jours** : permet de bloquer l'installation des mises à jour pendant 30 jours. Après 30 jours, l'utilisateur peut choisir le moment d'installer une mise à jour. Selon le fabricant du terminal et le fournisseur de services sans fil, il est possible que les mises à jour de sécurité ne puissent pas être reportées.
   d) Cliquez sur **Ajouter**.

5. Pour spécifier les périodes pendant lesquelles les mises à jour du système d'exploitation pour les terminaux Espace Travail uniquement et Travail et Personnel - Contrôle total ne doivent pas intervenir, dans la section **Suspendre les mises à jour du système d'exploitation**, cliquez sur +. Sélectionnez le mois et le jour de début de la période de suspension, ainsi que la durée de celle-ci.

   Si vous spécifiez plusieurs périodes de suspension, il doit y avoir au moins 60 jours entre les périodes.
6. Pour spécifier une période de mise à jour pour les applications qui s'exécutent en premier plan, sélectionnez **Activer la période de mise à jour pour les applications qui s'exécutent au premier plan**. Sélectionnez l'heure de début et la durée.
7. Pour spécifier la manière dont Google Play applique les modifications aux applications exécutées au premier plan (paramètre Mise à jour automatique des applications dans Google Play), dans la liste déroulante **Stratégie de mise à jour des applications**, sélectionnez l'une des options suivantes :

   - **Toujours** : les applications sont toujours mises à jour. Pour les applications toujours en cours d'exécution (telles que BlackBerry UEM Client, BlackBerry Work ou BlackBerry Connectivity), si vous ne sélectionnez pas l'option **Activer la période de mise à jour pour les applications qui s'exécutent au premier plan**, l'application n'est mise à jour que lorsque l'utilisateur le fait manuellement.
   - **Wi-Fi uniquement** : les applications se mettent à jour uniquement lorsque le terminal est connecté à un réseau Wi-Fi. Pour les applications toujours en cours d'exécution (telles que UEM Client, BlackBerry Work ou BlackBerry Connectivity), si vous ne sélectionnez pas l'option **Activer la période de mise à jour pour les applications qui s'exécutent au premier plan**, l'application n'est mise à jour que lorsque l'utilisateur le fait manuellement.
   - **L'utilisateur peut autoriser** : l'utilisateur est invité à autoriser les applications à se mettre à jour sur l'appareil.
   - **Désactiver** : les applications ne sont jamais mises à jour.

   Si vous sélectionnez **Toujours**, **Wi-Fi uniquement** ou **Désactiver**, l'utilisateur ne peut pas sélectionner une autre option sur le terminal. Les utilisateurs peuvent toujours mettre à jour manuellement les applications dans Google Play.
8. Cliquez sur **Ajouter**.

À la fin :

- Attribuez le profil à des utilisateurs et à des groupes.
- Si nécessaire, classez le profil.
- Pour afficher la liste des utilisateurs qui exécutent une version annulée du logiciel (une version qui n'est plus acceptée par un fournisseur de services), dans **Stratégies et profils > Conformité > Configuration logicielle minimale requise du terminal**, cliquez sur un profil, puis sur l'onglet **x utilisateurs exécutant une version annulée du logiciel**.

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

Sur les terminaux Samsung Knox, vous pouvez utiliser Knox E-FOTA One (Enterprise Firmware Over the Air) pour déterminer quand installer les mises à jour du micrologiciel de Samsung. Si votre organisation utilise Samsung E-FOTA (fin de service le 31 juillet 2022) et que vous devez migrer vers E-FOTA One, consultez l'article KB 69901.

Les terminaux Samsung Knox auxquels sont attribués les types d'activation Travail et Personnel - Contrôle total (Samsung Knox), Espace Travail uniquement (terminal Android Enterprise entièrement géré) et Travail et Personnel - Contrôle total (terminal Android Enterprise entièrement géré avec un profil professionnel) prennent en charge les restrictions logicielles à l'aide d'E-FOTA One.

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

Avant de commencer :

- Sur la barre de menus de la console de gestion, accédez à **Paramètres > Récapitulatif des licences** pour ajouter une licence E-FOTA à BlackBerry UEM.
- Pour utiliser E-FOTA, vous devez activer la règle globale Android Autoriser les mises à jour par liaison radio dans la stratégie informatique que vous attribuez aux terminaux.

1. Sur la barre de menus de la console de gestion, cliquez sur **Stratégies et profils > Conformité > Configuration logicielle minimale requise du terminal**.
2. Cliquez sur +.
3. Saisissez le nom et la description du profil.
4. Si vous souhaitez autoriser l'application des règles de mise à jour du système d'exploitation Android aux terminaux Samsung, cochez la case **Appliquer la restriction à tous les terminaux Android**.

   Les règles relatives au micrologiciel que vous configurerez au cours des étapes suivantes sont prioritaires sur ces règles. Les paramètres de suspension des mises à jour du système d'exploitation ne s'appliquent pas aux terminaux Samsung Knox qui utilisent E-FOTA.
5. Dans la section **Règles relatives aux micrologiciels des terminaux Samsung**, cliquez sur +.
6. Dans la liste déroulante **Modèle du terminal**, saisissez le modèle de terminal, ou sélectionnez un modèle dans la liste.
7. Dans la liste déroulante **Langue**, sélectionnez une langue.
8. Dans le champ **Code de l'opérateur**, saisissez le code CSC du fournisseur de services sans fil.
9. Cliquez sur **Obtenir la version du micrologiciel**.
10. Répétez les étapes précédentes pour chaque règle de micrologiciel que vous souhaitez ajouter.
11. Une fois terminé, cliquez sur **Ajouter**.
12. Si vous souhaitez planifier une mise à jour forcée, cliquez sur **Planifier** en regard d'une version de micrologiciel que vous avez ajoutée. Dans la boîte de dialogue **Planifier une mise à jour forcée**, procédez comme suit :
    a) Dans les champs **Planifier une mise à jour forcée entre**, sélectionnez une plage de dates au cours de laquelle la mise à jour doit être installée.
    b) Dans les listes déroulantes **Planifier une mise à jour forcée pendant les heures de**, précisez le moment où la mise à jour forcée doit être installée.

    Si vous planifiez une mise à jour forcée, le terminal Knox n'est plus limité à la version du micrologiciel et vous pouvez le mettre à jour manuellement si une version ultérieure est disponible.
13. Cliquez sur **Enregistrer**.

À la fin :

- Attribuez le profil à des utilisateurs et à des groupes.
- Si nécessaire, classez le profil.
- Pour afficher la liste des utilisateurs qui exécutent une version annulée du logiciel (une version qui n'est plus acceptée par un fournisseur de services), dans **Stratégies et profils > Conformité > Configuration logicielle minimale requise du terminal**, cliquez sur un profil, puis sur l'onglet **x utilisateurs exécutant une version annulée du logiciel**.

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

Vous pouvez utiliser la console de gestion pour forcer les terminaux supervisés iOS à installer une mise à jour de système d'exploitation disponible.

1. Sur la barre de menus de la console de gestion, cliquez sur **Utilisateurs > Terminaux gérés**.
2. Effectuez l'une des opérations suivantes :

Tâche	Étapes
Mise à jour du système d'exploitation sur un terminal iOS supervisé spécifique	**a.** Recherchez et cliquez sur le nom d'un compte d'utilisateur. **b.** Sous l'onglet du terminal qui convient, si une mise à jour du logiciel est disponible, cliquez sur **Mettre à jour maintenant**. **c.** Configurez les paramètres de mise à jour du système d'exploitation appropriés. **d.** Cliquez sur **Mettre à jour**.
Mise à jour du système d'exploitation sur plusieurs terminaux iOS supervisés	**a.** Sélectionnez les comptes d'utilisateur. **b.** Cliquez sur . **c.** Configurez les paramètres de mise à jour du système d'exploitation appropriés. **d.** Cliquez sur **Mettre à jour**.

Configuration de la façon dont les terminaux contactent BlackBerry UEM pour les mises à jour des applications et de la configuration

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

Dans des environnements sur site, vous pouvez également utiliser le profil Enterprise Management Agent pour permettre à UEM d'établir une liste des applications personnelles sur les terminaux des utilisateurs.

Créer un profil Enterprise Management Agent

1. Sur la barre de menus de la console de gestion, cliquez sur **Stratégies et profils > Stratégie > Enterprise Management Agent**.
2. Cliquez sur +.
3. Saisissez le nom et la description du profil.
4. Configurez les paramètres relatifs à chaque type de terminal. Pour plus d'informations sur les paramètres, reportez-vous à ce qui suit :
   - iOS : paramètres de profil Enterprise Management Agent
   - Android : paramètres de profil Enterprise Management Agent
   - Windows : paramètres de profil Enterprise Management Agent
5. Cliquez sur **Ajouter**.

À la fin :

- Attribuez le profil à des utilisateurs et à des groupes.
- Si nécessaire, classez le profil.

iOS : paramètres de profil Enterprise Management Agent

Paramètre	Description
Fréquence d'interrogation de Enterprise Management Agent	Indiquez la fréquence (en secondes) à laquelle le terminal interroge les commandes du serveur Enterprise Management Agent. Le terminal interroge uniquement lorsque le client UEM Client est ouvert.
Autoriser la collection d'applications personnelles	Indiquez si BlackBerry UEM doit recevoir une liste des applications personnelles installées sur le terminal d'un utilisateur. Ce paramètre n'est pas pris en charge sur les terminaux ayant des activations Confidentialité de l'utilisateur.

Android : paramètres de profil Enterprise Management Agent

Paramètre	Description
Modifications de l'application	Indiquez la fréquence, en secondes, à laquelle le terminal vérifie les changements dans les applications installées.
Seuil de niveau de batterie	Indiquez le pourcentage de changement du niveau de la batterie requis avant que le terminal ne renvoie les informations à BlackBerry UEM.
Seuil d'espace libre RAM	Indiquez le changement nécessaire de la quantité de mémoire libre en mégaoctets avant que le terminal ne renvoie des informations à UEM.
Seuil de stockage interne	Indiquez le changement nécessaire de la quantité d'espace de stockage libre interne en mégaoctets avant que le terminal ne renvoie des informations à UEM.
Seuil de la carte mémoire	Indiquez le changement nécessaire de la quantité d'espace libre externe en mégaoctets avant que le terminal ne renvoie des informations à UEM.
Fréquence d'interrogation de Enterprise Management Agent	Indiquez la fréquence (en secondes) à laquelle le terminal interroge les commandes du serveur Enterprise Management Agent.
Autoriser la collection d'applications personnelles	Indiquez si UEM doit recevoir une liste des applications personnelles installées sur le terminal d'un utilisateur. Ce paramètre n'est pas pris en charge sur les terminaux ayant des activations Confidentialité de l'utilisateur.

Windows : paramètres de profil Enterprise Management Agent

Paramètre	Description
Intervalle d'interrogation des mises à jour de configuration de terminal	Indiquez la fréquence, en minutes, à laquelle le terminal recherche des mises à jour de configuration lorsque la notification Push n'est pas disponible.
Intervalle d'interrogation pour la première série de nouvelles tentatives	Indiquez le temps d'attente, en minutes, entre deux tentatives lors de la première série de tentatives, si l'interrogation des mises à jour de la configuration du terminal échoue.
Nombre de premières nouvelles tentatives	Indiquez le nombre de tentatives de la première série de tentatives.
Intervalle d'interrogation pour la deuxième série de nouvelles tentatives	Indiquez le temps d'attente, en minutes, entre deux tentatives lors de la deuxième série de tentatives, si l'interrogation des mises à jour de la configuration du terminal échoue.
Nombre de secondes nouvelles tentatives	Indiquez le nombre de tentatives de la deuxième série de tentatives.

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

Affichage des informations d'entreprise sur les terminaux

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

Pour les terminaux iOS, macOS, Android et Windows 10, vous pouvez créer des avis d'entreprise personnalisés à afficher lors du processus d'activation (par exemple, vous pouvez afficher un avis sur les conditions qu'un utilisateur doit respecter pour se conformer aux exigences de sécurité de votre entreprise). L'utilisateur doit accepter l'avis pour continuer le processus d'activation. Vous pouvez créer plusieurs avis et créer des versions distinctes de chaque avis pour prendre en charge différentes langues.

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

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

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

Créer des avis d'entreprise

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

À la fin :

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

Créer un profil de terminal

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

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

Tâche	Étapes
Attribuer un avis d'entreprise à afficher sur les terminaux Samsung Knox lorsqu'un utilisateur redémarre le terminal	Sous l'onglet **Android**, sélectionnez l'avis d'entreprise qui convient dans la liste déroulante **Attribuer un avis d'entreprise**.
Pour les terminaux iOS et Android, définir les informations d'entreprise à afficher dans BlackBerry UEM Client Pour Windows 10, définissez le numéro de téléphone et l'adresse e-mail à afficher dans les informations d'assistance sur les terminaux.	Sous l'onglet approprié du système d'exploitation, spécifiez le nom, l'adresse, le numéro de téléphone et l'adresse e-mail.

5. Vous pouvez également effectuer l'une des opérations suivantes :

Tâche	Étapes
Ajouter une image de fond d'écran à l'espace Travail sur les terminaux Samsung Knox	**a.** Sous l'onglet **Android**, accédez à la section **Fond d'écran de l'espace Travail** et cliquez sur **Parcourir**. **b.** Accédez à l'image et sélectionnez-la.
Ajouter un fond d'écran aux terminaux iOS supervisés	Sous l'onglet **iOS**, dans la section **Fond d'écran du terminal**, effectuez l'une des opérations suivantes : • Pour définir le fond pour l'écran de verrouillage, en regard de **Image de l'écran de verrouillage**, cliquez sur **Parcourir**. Accédez à l'image et sélectionnez-la. • Pour définir le fond pour l'écran d'accueil, en regard de **Image de l'écran d'accueil**, cliquez sur **Parcourir**. Accédez à l'image et sélectionnez-la.

6. Cliquez sur **Ajouter**.

À la fin :

- Attribuez le profil à des utilisateurs et à des groupes.
- Si nécessaire, classez le profil.

Utilisation des services de localisation sur les terminaux

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

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

Pour activer et utiliser les services de localisation, procédez comme suit :

Étape	Action
1	Configurer les paramètres du service de localisation.
2	Créer un profil de service de localisation.
3	Localiser un terminal.
4	Vous pouvez également Activation du mode Perdu sur les terminaux iOS supervisés.

Configurer les paramètres du service de localisation

1. Sur la barre de menus de la console de gestion, cliquez sur **Paramètres > Paramètres généraux > Service de localisation**.
2. Si vous disposez d'un environnement sur site, dans le champ **Durée de stockage de l'historique de localisation**, indiquez la durée pendant laquelle BlackBerry UEM doit conserver l'historique de localisation des terminaux. Par défaut, UEM conserve cette historique pendant un mois.
3. Dans la liste déroulante **Unité de vitesse affichée**, cliquez sur **km/h** ou **mph** .
4. Cliquez sur **Enregistrer**.

À la fin : Créer un profil de service de localisation.

Créer un profil de service de localisation

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

1. Sur la barre de menus de la console de gestion, cliquez sur **Stratégies et profils > Protection > Service de localisation**.
2. Cliquez sur +.
3. Saisissez le nom et la description du profil.

4. Vous pouvez également décocher la case correspondant aux types de terminaux pour lesquels vous ne souhaitez pas configurer le profil.
5. Effectuez l'une des tâches suivantes :

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

6. Cliquez sur **Ajouter**.

À la fin :

- Attribuez le profil à des utilisateurs et à des groupes. Les utilisateurs doivent accepter le profil pour que la console de gestion ou BlackBerry UEM Self-Service puisse afficher l'emplacement de terminaux iOS et Android sur une carte. Les terminaux Windows 10 Mobile acceptent automatiquement le profil.
- Si nécessaire, classez le profil.
- Localiser un terminal.

Localiser un terminal

Avant de commencer : Créer un profil de service de localisation.

1. Sur la barre de menus de la console de gestion, cliquez sur **Utilisateurs > Terminaux gérés**.
2. Cochez la case de chaque terminal que vous souhaitez localiser.
3. Cliquez sur .
4. Recherchez les terminaux sur la carte à l'aide de l'icône de position actuelle () et de la dernière icône de position connue (). Si un terminal iOS ou Android ne répond pas avec les dernières informations d'emplacement et que l'historique de localisation est activé dans le profil, la carte affiche le dernier emplacement connu du terminal.
5. Cliquez ou passez le curseur sur une icône pour afficher des informations sur l'emplacement, telles que la latitude et la longitude, ainsi que la date à laquelle l'emplacement a été signalé.
6. Pour afficher l'historique de localisation d'un terminal iOS ou Android, cliquez sur **Afficher l'historique de localisation**, sélectionnez une plage de dates et d'heures, puis cliquez sur **Soumettre**.

Activation du mode Perdu sur les terminaux iOS supervisés

Vous pouvez activer et gérer le mode Perdu sur les terminaux iOS supervisés. En cas de perte d'un terminal, vous pouvez activer le mode Perdu pour verrouiller celui-ci et définir un message à afficher, et vous pouvez afficher l'emplacement actuel du terminal sans avoir recours à un profil de service de localisation.

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

À la fin :

- Pour localiser un terminal en mode Perdu, accédez à l'onglet Terminal et cliquez sur **Obtenir l'emplacement du terminal**.
- Pour désactiver le mode Perdu, accédez à l'onglet Terminal et cliquez sur **Désactiver le mode Perdu**.

Activation du verrouillage d'activation pour un terminal iOS

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

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

Procédez comme suit pour activer le verrouillage d'activation pour chaque terminal individuellement.

Avant de commencer :

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

1. Dans la console de gestion, cliquez sur **Utilisateurs** sur la barre de menu.
2. Recherchez et cliquez sur un compte d'utilisateur.
3. Sous l'onglet Terminal, accédez à la section **Gérer le terminal** et cliquez sur **Activer le verrouillage d'activation**.

À la fin :

- Pour désactiver le verrouillage d'activation d'un terminal, cliquez sur **Désactiver le verrouillage d'activation**. Si le verrouillage d'activation est activé à l'aide de la règle de stratégie informatique, vous ne pouvez pas utiliser cette option pour le désactiver.
- Pour afficher le code de contournement d'un terminal, accédez à **Utilisateurs > Verrouillage d'activation Apple**, puis recherchez et cliquez sur un terminal.

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

Vous pouvez utiliser des profils de charge utile personnalisée pour contrôler les fonctionnalités sur les terminaux iOS qui ne sont pas contrôlés par les règles ou profils BlackBerry UEM existants. Si une fonctionnalité est commandée par une stratégie ou un profil UEM existant, un profil de charge utile personnalisée peut ne pas fonctionner comme prévu. Vous devez utiliser les stratégies ou profils existants chaque fois que cela est possible.

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

Par exemple, vous voulez contrôler une nouvelle fonctionnalité qui sera disponible pour les terminaux lors d'une nouvelle mise à niveau de iOS, mais UEM ne dispose pas de règles de stratégie informatique pour cette nouvelle fonctionnalité avant la prochaine version du logiciel UEM. Pour résoudre ce problème, vous pouvez créer un profil de charge utile personnalisée qui contrôle cette fonctionnalité jusqu'à ce qu'elle doit officiellement prise en charge par UEM.

Création d'un profil de charge utile personnalisée

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

1. Dans Apple Configurator, créez un profil de configuration Apple.
2. Copiez le code XML du profil de configuration Apple. Lorsque vous copiez le texte, copiez uniquement les éléments en caractères gras, comme illustré dans l'exemple de code suivant.

```
<?xml version="1.0" encoding="UTF-8"?>
    <!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
    "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
    <plist version="1.0">
    <dict>
         <key>PayloadContent</key>
         <array>
               <dict>
                    <key>CalDAVAccountDescription</key>
                    <string>CalDAV Account Description</string>
                    <key>CalDAVHostName</key>
                    <string>caldav.server.example</string>
                    <key>CalDAVPort</key>
                    <integer>8443</integer>
                    <key>CalDAVPrincipalURL</key>
                    <string>Principal URL for the CalDAV account</string>
                    <key>CalDAVUseSSL</key>
                    </true>
                    <key>CalDAVUsername</key>
                    <string>Username</string>
                    <key>PayloadDescription</key>
                    <string>Configures CalDAV account.</string>
                    <key>PayloadDisplayName</key>
                    <string>CalDAV (CalDAV Account Description)</string>
                    <key>PayloadIdentifier</key>
                    <string>.caldav1</string>
                    <key>PayloadOrganization</key>
                    <string></string>
```

```
                    <key>PayloadType</key>
                    <string>com.apple.caldav.account</string>
                    <key>PayloadUUID</key>
                    <string>9ADCF5D6-397C-4E14-848D-FA04643610A3</string>
                    <key>PayloadVersion</key>
                    <integer>1</integer>
                </dict>
        </array>
        <key>PayloadDescription</key>
        <string>Profile description.</string>
        <key>PayloadDisplayName</key>
        <string>Profile Name</string>
        <key>PayloadOrganization</key>
        <string></string>
        <key>PayloadRemovalDisallowed</key>
        <false/>
        <key>PayloadType</key>
        <string>Configuration</string>
        <key>PayloadUUID</key>
        <string>7A5F8391-5A98-46EA-A3CF-C0D6EDC74632</string>
        <key>PayloadVersion</key>
        <integer>1</integer>
    </dict>
    </plist>
```

3. Sur la barre de menus de la console de gestion UEM, cliquez sur **Stratégies et profils > Personnaliser > Charge utile personnalisée**.
4. Cliquez sur +.
5. Saisissez le nom et la description du profil.
6. Dans le champ **Charge utile personnalisée**, collez le code XML que vous avez copié à l'étape 2.
7. Cliquez sur **Ajouter**.

À la fin : Attribuez le profil à des utilisateurs et à des groupes.

Gestion de la protection contre la réinitialisation aux paramètres d'usine sur les terminaux Android Enterprise et Android Management

Vous pouvez utiliser le profil de protection contre la réinitialisation aux paramètres d'usine pour contrôler la fonctionnalité de protection contre la réinitialisation aux paramètres d'usine sur les terminaux Android Enterprise et Android Management qui ont été activés à l'aide des types d'activation Espace Travail uniquement et Travail et Personnel - Contrôle total.

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

Les profils de protection contre la réinitialisation aux paramètres d'usine offrent les options suivantes :

Option	Description	Types d'activation pris en charge
Désactiver la protection contre la réinitialisation aux paramètres d'usine	N'importe qui peut rétablir les paramètres d'usine d'un terminal perdu ou volé et commencer à l'utiliser. Cette option est utile si un utilisateur connu a oublié les informations d'identification de son compte Google ou si vous devez réinitialiser un terminal appartenant à votre organisation qui vous a été renvoyé.	Android Enterprise
Activer et utiliser les informations d'identification du précédent compte Google lorsque le terminal est réinitialisé aux paramètres d'usine	Les utilisateurs peuvent utiliser les informations d'identification du compte Google déjà associées au terminal après une réinitialisation aux paramètres d'usine. Il s'agit du comportement par défaut. Si un terminal est réinitialisé aux paramètres d'usine, l'utilisateur doit se connecter à celui-ci à l'aide des informations d'identification du compte Google qui se trouvent déjà sur le terminal. Dès lors, une personne ayant perdu ou volé un terminal ne peut pas elle-même le réinitialiser et l'utiliser.	Android Enterprise

Option	Description	Types d'activation pris en charge
Activer et spécifier les informations d'identification du compte Google lorsque le terminal est réinitialisé aux paramètres d'usine	Vous pouvez spécifier les informations d'identification du compte Google qu'un utilisateur peut utiliser pour se connecter au terminal après sa réinitialisation aux paramètres d'usine. Cette option permet à votre organisation de déterminer qui peut se connecter à un terminal après sa réinitialisation aux paramètres d'usine. BlackBerry vous recommandons de n'utiliser cette option que si vous maitrisez parfaitement l'expérience utilisateur du terminal. Si votre organisation utilise un compte Google Play géré, vous pouvez être amené à utiliser cette option parce qu'il n'existe pas de compte Google sur les terminaux de votre organisation et que la protection contre la réinitialisation aux paramètres d'usine n'y est pas disponible.	Android Enterprise Android Management

Il existe plusieurs façons de réinitialiser un terminal aux paramètres d'usine par défaut. La protection contre la réinitialisation aux paramètres d'usine répond différemment selon la méthode utilisée. Pour plus d'informations sur les réinitialisations fiables et non approuvées, consultez l'article KB 56972.

Création d'un profil de protection contre la réinitialisation aux paramètres d'usine

1. Sur la barre de menus de la console de gestion, cliquez sur **Stratégies et profils > Terminaux gérés > Protection > Protection contre la réinitialisation définie en usine**.
2. Cliquez sur +.
3. Saisissez le nom et la description du profil.
4. Dans la liste déroulante **Paramètre de protection contre la réinitialisation définie en usine**, cliquez sur l'un des éléments suivants :
   - **Supprimer la protection contre la réinitialisation définie en usine** : si vous désactivez la protection contre la réinitialisation définie en usine, les utilisateurs ne sont pas invités à saisir un ID utilisateur Google une fois que le terminal est réinitialisé sur les paramètres d'usine. Cette option est prise en charge pour les terminaux Android Enterprise (Travail et Personnel - Contrôle total et Espace Travail uniquement).
   - **Activer et utiliser les informations d'identification du précédent compte Google lorsque le terminal est réinitialisé sur les paramètres d'usine** : il s'agit de l'option par défaut. Si l'utilisateur réinitialise le terminal sur les paramètres d'usine à l'aide d'une méthode non fiable et qu'un compte Google existait sur le terminal avant sa réinitialisation, le compte doit être vérifié après la réinitialisation du terminal sur les paramètres d'usine. Notez que si votre entreprise utilise une structure de compte géré Google, il n'y aura pas de compte Google sur le terminal et la protection contre la réinitialisation définie en usine ne sera pas disponible sur le terminal. Cette option est prise en charge pour les terminaux Android Enterprise (Travail et Personnel - Contrôle total et Espace Travail uniquement).
   - **Activer et spécifier les informations d'identification de compte Google lorsque le terminal est réinitialisé sur les paramètres d'usine** : sélectionnez cette option pour spécifier le compte Google qui doit être utilisé pour se connecter au terminal après une réinitialisation non sécurisée aux paramètres d'usine. Si vous sélectionnez cette option, les informations d'identification du compte Google personnel de l'utilisateur

ne peuvent pas être utilisées après une réinitialisation aux paramètres d'usine. Cette option est prise en charge pour les terminaux Android Enterprise et les terminaux Android Management (Travail et Personnel - Contrôle total et Espace Travail uniquement).

Si vous souhaitez utiliser un compte Google Play géré, dans la stratégie informatique attribuée aux utilisateurs, désactivez l'option Autoriser la réinitialisation définie en usine. Cela désactive l'option de réinitialisation des paramètres d'usine dans les paramètres du terminal et désactive le bouton de désactivation dans UEM Client. Cela garantit que les utilisateurs n'utilisent pas l'option de désactivation non fiable d'UEM Client qui déclenche la protection contre la réinitialisation définie en usine sur le terminal.

5. Si vous avez sélectionné **Activer et spécifier les informations d'identification du compte Google lorsque le terminal est réinitialisé aux paramètres d'usine**, cliquez sur + et effectuez l'une des opérations suivantes pour ajouter des comptes Google (vous pouvez ajouter jusqu'à 20 comptes) :
   - Pour utiliser l'authentification Google, cliquez sur **Ajouter à l'aide de l'authentification Google** et connectez-vous au compte Google que vous souhaitez utiliser pour vous connecter aux terminaux réinitialisés.
   - Pour spécifier manuellement des comptes, cliquez sur **Manuel**. Spécifiez l'adresse e-mail et l'ID Google. Pour obtenir l'ID Google, procédez comme suit sur le site People API réservé aux développeurs Google :
     a. Pour **resourceName**, saisissez people/me.
     b. Pour **personalFields**, saisissez metadata.
     c. Cliquez sur **Exécuter**.
     d. Sur l'écran **Choisir un compte**, sélectionnez un compte à utiliser pour configurer le profil de protection contre la réinitialisation définie en usine.
     e. Sur l'écran **Google APIs Explorer souhaite accéder à votre compte Google**, cliquez sur **Autoriser**.
     f. Sur la page **People ID**, notez l'ID utilisateur à 21 chiffres.
6. Si vous avez sélectionné l'option **Activer et spécifier les informations d'identification de compte Google lorsque le terminal est réinitialisé sur les paramètres d'usine** et que votre organisation possède un domaine Google Workspace ou Google Cloud, sélectionnez **Ajouter un compte Google créé par BlackBerry UEM** si vous souhaitez inclure le compte Google professionnel de l'utilisateur dans la liste des comptes pouvant déverrouiller le terminal après une réinitialisation aux paramètres d'usine.
7. Cliquez sur **Enregistrer**.

À la fin :

- Attribuez le profil à des utilisateurs et à des groupes.
- Si nécessaire, classez le profil.
- Lorsque la protection contre la réinitialisation définie en usine est déclenchée sur le terminal, l'activation Entreprise sur BlackBerry UEM ne fonctionne pas. Vous devez d'abord désactiver la protection contre la réinitialisation définie en usine à l'aide de l'expérience Android prête à l'emploi. Reportez-vous à la section Désactiver la protection contre la réinitialisation définie en usine d'un terminal.

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

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

1. Si vous utilisez une forme quelconque de système d'activation automatisé (comme l'inscription sans contact ou Samsung Knox Mobile Enrollment), vous devez le désactiver pour que le terminal puisse passer à l'étape d'expérience prête à l'emploi.

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

Configuration de l'attestation relative aux terminaux

Lorsque vous activez l'attestation, BlackBerry UEM envoie des défis pour tester l'authenticité et l'intégrité des terminaux. Vous pouvez activer l'attestation pour les terminaux Samsung Knox, Android, iOS et Windows 10.

Configuration de l'attestation relative aux terminaux Android et aux applications BlackBerry Dynamics

Vous pouvez utiliser SafetyNet ou l'attestation Google Play Integrity pour que BlackBerry UEM vérifie l'authenticité et l'intégrité des terminaux Android et des applications BlackBerry Dynamics. SafetyNet et Play Integrity vous aident à évaluer la sécurité et la compatibilité des environnements dans lesquels les applications de votre entreprise s'exécutent. Vous pouvez utiliser l'attestation SafetyNet ou Play Integrity en plus de la détection d'exploitation et de racine existante de BlackBerry. Vous pouvez configurer et attribuer un profil de conformité UEM afin d'exécuter les actions de conformité appropriées lorsque les terminaux ou les applications échouent à l'attestation.

UEM utilise l'API Play Integrity avec les versions UEM Client qui le prennent en charge pour fournir une protection supplémentaire contre la falsification d'applications. Play Integrity remplacera SafetyNet selon le calendrier de migration établi par Google. SafetyNet restera pris en charge par les anciennes versions de UEM Client. Pour plus d'informations sur la migration depuis SafetyNet, consultez Google Play : Migrer depuis l'API SafetyNet Attestation.

UEM effectue une attestation SafetyNet ou Play Integrity dans les circonstances suivantes :

- Après l'activation du terminal lorsque BlackBerry UEM Client est installé.
- Pendant et après l'activation des applications BlackBerry Dynamics. Veuillez noter qu'UEM n'accepte pas les anciennes versions des applications. Pour réussir les vérifications d'attestation, les terminaux doivent disposer de la dernière version disponible des applications BlackBerry Dynamics.
- Sur demande à l'aide des API REST.
- Si UEM Client est activé, lorsqu'un terminal est redémarré.
- Vérifications d'attestation périodiques basées sur la fréquence de vérification que vous spécifiez.

UEM Client n'est pas nécessaire pour activer l'attestation SafetyNet ou Play Integrity. UEM Client ne figure pas dans la liste des applications BlackBerry Dynamics que vous pouvez configurer pour l'attestation SafetyNet ou Play Integrity, mais il reçoit les vérifications d'attestation d'UEM et y répond.

Si le terminal d'un utilisateur se trouve en dehors de la zone de couverture, s'il est éteint ou si sa batterie est déchargée, il ne peut pas répondre aux vérifications d'attestation. Dans ce cas, UEM considère que le terminal n'est pas conforme et exécute les actions que vous avez configurées dans le profil de conformité attribué.

Configuration de l'attestation relative aux terminaux Android et aux applications BlackBerry Dynamics

Avant de commencer : La dernière version des services Google Play doit être installée sur les terminaux des utilisateurs.

1. Sur la barre de menus de la console de gestion, cliquez sur **Paramètres > Paramètres généraux > Attestation**.
2. Cochez la case **Activer les vérifications périodiques d'attestation à l'aide de SafetyNet ou Play Integrity**.
3. Si vous souhaitez activer Google Compatibility Test Suite, cochez la case **Activer la correspondance de profil CTS**.
4. Dans la section **Fréquence des vérifications**, spécifiez la fréquence à laquelle le terminal doit renvoyer une réponse d'attestation à BlackBerry UEM. La valeur par défaut et minimum est de 24 heures.

5. Dans la section **Période de grâce**, spécifiez la période de grâce des terminaux. Après l'expiration de la période de grâce sans réponse d'attestation, un terminal est considéré comme non conforme et soumis aux actions que vous spécifiez dans le profil de conformité attribué.
6. Dans la section **Période de grâce de l'application**, spécifiez une période de grâce pour les applications BlackBerry Dynamics. Après l'expiration de la période de grâce sans réponse d'attestation, une application BlackBerry Dynamics est soumise aux actions que vous spécifiez dans le profil de conformité attribué. La période de grâce est appliquée pour chaque application.
7. Pour spécifier les applications BlackBerry Dynamics soumises à des vérifications d'attestation, cliquez sur +.
8. Sélectionnez les applications, puis cliquez sur **Sélectionner**.
9. Cliquez sur **Enregistrer**.

À la fin :

- Dans le profil de conformité attribué aux terminaux, activez la règle SafetyNet ou échec de l'attestation Play Integrity et configurez les actions qu'UEM doit effectuer lorsque les terminaux ou les applications BlackBerry Dynamics échouent à l'attestation.
- Dans la console de gestion, vous pouvez afficher l'état d'attestation d'un terminal dans les détails qui s'y rapportent.

Configuration de l'attestation relative aux terminaux iOS

Lorsque vous activez l'attestation pour les terminaux iOS, seuls les terminaux autorisés et non compromis peuvent être utilisés dans votre organisation. Lors de l'attestation, les propriétés (par exemple, son numéro de série) ou identifiants du terminal sont vérifiés pour s'assurer qu'ils sont légitimes et non frauduleux. Cette fonctionnalité nécessite que les terminaux non supervisés exécutent iOS 16 ou iPadOS 16.1 ou versions ultérieures. Pour les terminaux supervisés, iOS 17 ou iPadOS 17 ou version ultérieure est nécessaire.

1. Sur la barre de menus de la console de gestion, cliquez sur **Paramètres > Paramètres généraux > Attestation**.
2. Cochez la case **Activer les vérifications d'attestation périodiques pour les terminaux Apple exécutant iOS 16 ou une version ultérieure**.
3. Dans la section **Fréquence des vérifications**, spécifiez la fréquence à laquelle le terminal doit renvoyer une réponse d'attestation à UEM. La fréquence minimale de vérification est de 9 jours.
4. Dans la section **Période de grâce**, spécifiez la période de grâce des terminaux. Après l'expiration de la période de grâce sans réponse d'attestation, un terminal est considéré comme non conforme et soumis aux actions que vous spécifiez dans le profil de conformité attribué.
5. Cliquez sur **Enregistrer**.

À la fin :

- Dans le profil d'activation, indiquez si l'attestation a lieu pendant l'activation du terminal, si elle a lieu périodiquement ou les deux. 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 dans le profil d'activation, vous devez sélectionner au moins une des options de gestion (par exemple « Autoriser la gestion VPN »).
- Dans le profil de conformité, sélectionnez la règle « Échec de l'attestation du terminal géré » et spécifiez les actions de conformité que vous souhaitez effectuer sur les terminaux dont l'attestation échoue.
- Dans la console de gestion, vous pouvez afficher l'état d'attestation d'un terminal dans les détails qui s'y rapportent.

Configuration de l'attestation relative aux terminaux Samsung Knox

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

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

1. Sur la barre de menus de la console de gestion, cliquez sur **Paramètres > Paramètres généraux > Attestation**.
2. Cochez la case **Activer les vérifications périodiques d'attestation pour les terminaux KNOX Workspace**.
3. Dans la section **Fréquence des vérifications**, spécifiez la fréquence à laquelle le terminal doit renvoyer une réponse d'attestation à UEM.
4. Dans la section **Période de grâce**, spécifiez la période de grâce des terminaux. Après l'expiration de la période de grâce sans réponse d'attestation, un terminal est considéré comme non conforme et soumis aux actions que vous spécifiez dans le profil de conformité attribué.
5. Cliquez sur **Enregistrer**.

À la fin : Dans le profil de conformité attribué aux terminaux, activez la règle Système d'exploitation débridé ou échec de l'attestation KNOX et configurez les actions qu'UEM doit effectuer lorsque les terminaux échouent à l'attestation.

Configuration de l'attestation relative aux terminaux Windows 10

Lorsque vous activez l'attestation, BlackBerry UEM vérifie l'authenticité et l'intégrité des terminaux Windows 10. Notez que les paramètres d'attestation Windows 10 ne s'appliquent pas à BlackBerry Desktop (BlackBerry Access + BlackBerry Work).

1. Sur la barre de menus de la console de gestion, cliquez sur **Paramètres > Paramètres généraux > Attestation**.
2. Cochez la case **Activer les vérifications périodiques d'attestation pour les terminaux Windows 10**.
3. Dans la section **Fréquence des vérifications**, spécifiez la fréquence à laquelle le terminal doit renvoyer une réponse d'attestation à UEM.
4. Dans la section **Période de grâce**, spécifiez la période de grâce des terminaux. Après l'expiration de la période de grâce sans réponse d'attestation, un terminal est considéré comme non conforme et soumis aux actions que vous spécifiez dans le profil de conformité attribué.
5. Cliquez sur **Enregistrer**.

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

À la fin :

- Dans le profil de conformité attribué aux terminaux, configurez les règles d'attestation d'intégrité des terminaux Windows et configurez les actions qu'UEM doit effectuer lorsque les terminaux échouent à l'attestation.
- Dans la console de gestion, vous pouvez afficher l'état d'attestation d'un terminal dans les détails qui s'y rapportent.

Configuration de la Protection des informations Windows sur les terminaux Windows 10

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

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

Lorsque vous configurez la fonction WIP sur des terminaux, vous spécifiez les applications que vous souhaitez protéger. Les applications protégées sont en mesure de créer des fichiers professionnels et d'y accéder, tandis qu'il est possible de bloquer l'accès des applications non protégées aux fichiers professionnels. Vous pouvez choisir le niveau de protection pour les applications protégées en fonction de la manière dont vous souhaitez que les utilisateurs se comportent lorsqu'ils partagent des données professionnelles. Lorsque la fonction WIP est activée, toutes les pratiques de partage des données sont surveillées. Les applications que vous spécifiez peuvent être compatibles ou non. Les applications compatibles peuvent créer des données professionnelles et personnelles, mais aussi y accéder. Les applications non compatibles ne peuvent créer et accéder qu'aux données professionnelles.

1. Sur la barre de menus de la console de gestion, cliquez sur **Stratégies et profils > Protection > Protection des informations Windows**.
2. Cliquez sur +.
3. Saisissez le nom et la description du profil.
4. Configurez les valeurs qui conviennent pour chaque paramètre de profil. Reportez-vous à la section Paramètres des profils de protection des données Windows.
5. Cliquez sur **Ajouter**.

À la fin :

- Attribuez le profil à des utilisateurs et à des groupes.
- Si nécessaire, classez le profil.

Paramètres des profils de protection des données Windows

Paramètre de profil	Description
Paramètres de protection des données Windows	Ce paramètre indique si la protection des données Windows est activée et son degré d'application. • Désactivé : les données ne sont pas chiffrées et la journalisation d'audit est désactivée. • Silencieux : les données sont chiffrées et toute tentative de partage de données protégées est consignée. • Remplacer : les données sont chiffrées, l'utilisateur reçoit une invite lorsqu'il tente de partager des données protégées, et toute tentative de partage de données protégées est consignée. • Bloquer : les données sont chiffrées, les utilisateurs ne peuvent pas partager de données protégées, et toute tentative de partage de données protégées est consignée.
Noms de domaines d'entreprise protégés	Ce paramètre spécifie les noms des domaines du réseau professionnel que votre entreprise utilise pour les identités de ses utilisateurs. Séparez plusieurs domaines par des barres verticales (|). Le premier domaine est utilisé comme une chaine pour marquer les fichiers protégés par des applications qui utilisent WIP (par exemple, exemple.com|exemple.net).
Fichier de certificat de récupération de données (.der, .cer)	Ce paramètre spécifie le fichier de certificat de récupération de données que vous utilisez pour récupérer des fichiers qui étaient protégés localement sur un terminal. Ce fichier doit être un certificat codé PEM ou DER, avec une extension de fichier .der ou .cer.
Supprimer les paramètres de protection des données Windows lorsqu'un terminal est supprimé de BlackBerry UEM	Ce paramètre spécifie si les paramètres WIP doivent être révoqués lorsqu'un terminal est désactivé. Lors les paramètres WIP sont révoqués, l'utilisateur ne peut plus accéder aux fichiers protégés.
Afficher un filigrane de protection des données Windows sur les fichiers et applications protégés autorisés à créer du contenu d'entreprise	Ce paramètre spécifie si une icône de superposition est affichée sur les icônes de fichier et d'application pour indiquer si un fichier ou une application est protégé(e) par WIP.
Portée IP du réseau professionnel	Ce paramètre spécifie la plage d'adresses IP au travail avec laquelle une application protégée par WIP peut partager des données. Utilisez un tiret pour indiquer une plage d'adresses. Utilisez une virgule pour séparer les adresses.
Les plages d'adresses IP de réseau professionnel font autorité.	Ce paramètre spécifie si seules les plages d'adresses IP du réseau professionnel sont acceptées dans ce réseau professionnel. Lorsque ce paramètre est activé, aucune tentative n'est effectuée pour détecter d'autres réseaux professionnels.

Paramètre de profil	Description
Serveurs proxy internes d'entreprise	Ce paramètre spécifie les serveurs proxy internes qui sont utilisés lors de la connexion à des emplacements de réseaux professionnels. Ces serveurs proxy sont uniquement utilisés lors de la connexion à des domaines répertoriés dans les paramètres des ressources Enterprise Cloud.
Ressources d'entreprise dans le cloud	Ce paramètre spécifie la liste des domaines de ressources d'entreprise hébergés dans le cloud qui doivent être protégés. Les données de ces ressources sont considérées comme des données d'entreprise et sont donc protégées.
Domaine de ressources dans le cloud	Ce paramètre spécifie le nom du domaine.
Proxy couplé	Ce paramètre spécifie un proxy qui est associé à une ressource dans le cloud. Le trafic vers la ressource dans le cloud sera acheminé pour tout le réseau d'entreprise via le serveur proxy indiqué (sur le port 80). Un serveur proxy utilisé à cette fin doit également être configuré dans le champ Serveurs proxy internes de l'entreprise.
Serveurs proxy d'entreprise	Ce paramètre spécifie la liste des serveurs proxy Internet.
Les serveurs proxy d'entreprise font autorité.	Ce paramètre indique si le client doit accepter la liste configurée de proxies et ne pas essayer de détecter d'autres proxies d'entreprise.
Ressources neutres	Ce paramètre spécifie les domaines pouvant être utilisés pour les ressources personnelles ou professionnelles.
Noms de domaines de réseau d'entreprise	Ce paramètre répertorie les domaines (séparés par des virgules) compris dans les limites de l'entreprise. Lorsque les données d'un de ces domaines seront envoyées à un terminal, elles seront considérées comme des données d'entreprise protégées. Ces emplacements seront considérés comme une destination sécurisée pour le partage des données d'entreprise.

Paramètre de profil	Description

Code de charge utile d'application de bureau	Spécifiez les clés et les valeurs des applications de bureau qui sont utilisées pour configurer les restrictions de lancement d'application sur les terminaux Windows 10. Vous devez utiliser les clés définies par Microsoft pour le type charge utile que vous souhaitez configurer.
	
	Pour spécifier les applications, copiez le code XML du fichier .xml de la stratégie AppLocker et collez-le dans ce champ. Lors de la copie du texte, copiez uniquement les éléments présentés dans l'exemple de code suivant :
	
	`<RuleCollection Type="Appx" EnforcementMode="Enabled">`
	`  <FilePublisherRule Id="0c9781aa-bf9f-4352-`
	`b4ba-64c25f36f558"`
	`  Name="WordMobile" Description="`
	` UserOrGroupSid="S-1-1-0" Action="Allow">`
	`  <Conditions>`
	`  <FilePublisherCondition`
	`  PublisherName="CN=Microsoft Corporation, O=Microsoft`
	` Corporation, L=Redmond, S=Washington, C=US"`
	`  ProductName="Microsoft.Office.Word" BinaryName="*">`
	`  <BinaryVersionRange LowSection="*"`
	` HighSection="*" />`
	`  </FilePublisherCondition>`
	`  </Conditions>`
	`  </FilePublisherRule>`
	`</RuleCollection>`

Paramètre de profil	Description

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

Profil VPN associé	Ce paramètre spécifie le profil VPN utilisé par un terminal pour se connecter à un réseau VPN lorsqu'une application protégée par WIP est utilisée. Ce paramètre est valide uniquement si l'option « Utiliser un profil VPN » est sélectionnée pour la « Connexion sécurisée utilisée avec WIP ».

Paramètre de profil	Description
Collecter les journaux d'audit du terminal	Ce paramètre spécifie si la collecte des journaux d'audit du terminal est requise.

Déplacement des terminaux iOS ou macOS vers un canal renforcé

Lorsque vous activez des terminaux iOS ou macOS, ceux-ci sont attribués par défaut à un canal de données renforcé. Si certains de vos terminaux iOS ou macOS n'utilisent pas de canal renforcé, vous pouvez exporter la liste de ces terminaux et prendre des mesures pour les déplacer vers un canal renforcé. Lorsque vous déplacez des terminaux vers un canal renforcé, ceux-ci doivent être réactivés.

Si vous déplacez un terminal inscrit dans Apple DEP, il perd la configuration d'inscription DEP. Les utilisateurs du terminal devront réinitialiser les paramètres d'usine de celui-ci et l'activer à nouveau avec BlackBerry UEM.

Avant de commencer : Dans les paramètres d'application de toutes les applications applicables, désélectionnez l'option **Supprimer l'application du terminal lorsque celui-ci est supprimé de BlackBerry UEM**. Si vous tentez de déplacer des terminaux vers un canal renforcé sans désélectionner cette option, l'application est supprimée et le terminal peut être désinscrit d'UEM. Notez que même si vous décochez cette case, une application peut toujours être supprimée lors du déplacement si le paramètre n'a pas été transmis au terminal. Pour plus d'informations sur les commandes de suivi transmises à un terminal, consultez l'article KB 102688.

1. Sur la barre de menus de la console de gestion, cliquez sur **Paramètres > Migration > Canal renforcé iOS** ou **Paramètres > Migration > Canal renforcé macOS**.

   Si aucune de ces options de menu n'apparait, cela signifie que votre environnement UEM ne dispose d'aucun terminal iOS ou macOS à déplacer vers un canal renforcé.
2. Cliquez sur **Exporter** pour télécharger une liste de terminaux n'utilisant actuellement pas de canal renforcé.
3. Effectuez l'une des opérations suivantes :

Tâche	Étapes
Déplacez plusieurs terminaux iOS vers un canal renforcé.	Cliquez sur **Parcourir**, accédez au fichier que vous avez téléchargé à l'étape 2 et sélectionnez-le. Les terminaux appartenant à des groupes de terminaux partagés sont inclus dans le fichier à titre d'information uniquement et ne sont pas déplacés vers un canal renforcé à l'aide de cette méthode. Pour tous les terminaux appartenant à des groupes de terminaux partagés, l'utilisateur doit réinitialiser les paramètres d'usine des terminaux et les activer à nouveau avec UEM. Cette méthode peut simultanément traiter un maximum de 1 000 entrées. Si le fichier que vous avez téléchargé contient plus de 1 000 entrées, divisez-les en fichiers distincts contenant chacun un maximum de 1 000 entrées.
Déplacez un terminal iOS spécifique vers un canal renforcé.	**a.** Sur la barre de menus, cliquez sur **Utilisateurs > Terminaux gérés**. **b.** Recherchez et cliquez sur le terminal iOS. **c.** Sous l'onglet du terminal, cliquez sur **Migrer vers le canal renforcé iOS**. **d.** Cliquez sur **Submit**.
Déplacez des terminaux macOS vers un canal renforcé.	Contactez les utilisateurs des terminaux et demandez-leur de réactiver leur terminal avec UEM Self-Service.

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