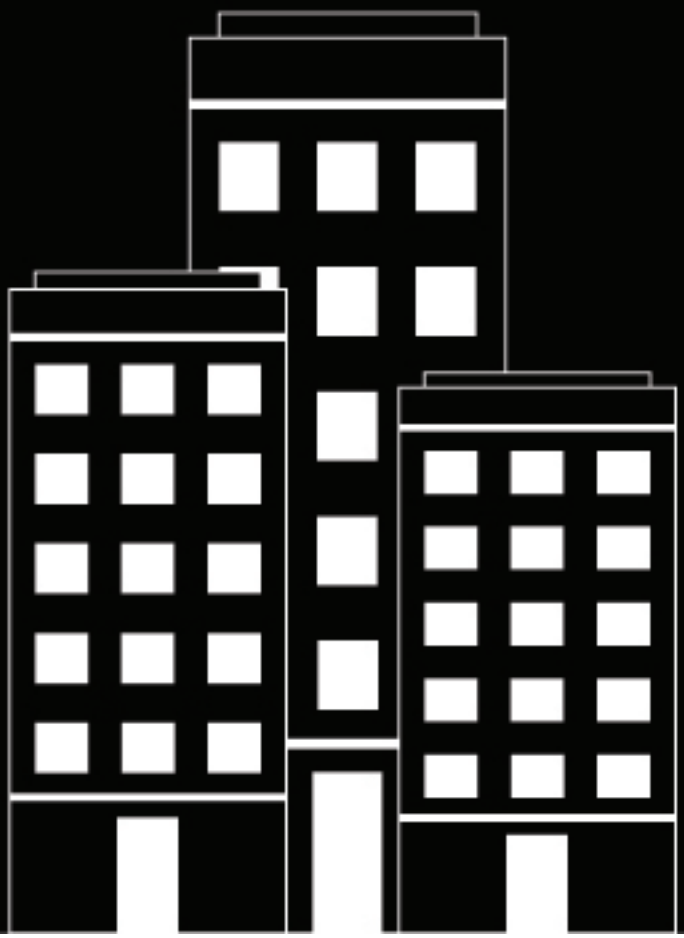

BlackBerry UEM

Guide d'administration

12.9

Table des matières

À propos de ce guide

BlackBerry UEM vous permet de gérer les terminaux de votre organisation. Ce guide explique comment administrer BlackBerry UEM, de la création d'administrateurs à l'ajout d'utilisateur et de terminaux en passant par la gestion et la surveillance de BlackBerry UEM.

Les tâches du présent guide sont présentées dans un ordre particulier pour plus d'efficacité, notamment si vous administrez BlackBerry UEM pour la première fois.

Toutes les tâches décrites dans ce guide ne sont pas obligatoires. Vous pouvez choisir d'activer certains types de terminaux, de séparer les données professionnelles et les données personnelles de différentes manières ou d'utiliser diverses règles de conformité, fonctionnalités et connexions.

Ce guide est destiné aux professionnels de l'informatique qui occupent des fonctions de responsables de la configuration et de l'administration de BlackBerry UEM. Avant d'utiliser ce guide, les professionnels de l'informatique doivent configurer l'environnement de BlackBerry UEM. Pour en savoir plus, consultez le contenu relatif à la configuration.

Mise en route

Étapes de prise en main de BlackBerry UEM

Étape	Action
1	Planifiez votre installation de BlackBerry UEM.
2	Installer BlackBerry UEM ou procéder à une mise à niveau vers la version la plus récente de BlackBerry UEM.
3	Si vous utilisez BlackBerry Work ou BlackBerry Connect, installez ou mettez à niveau et configurez BlackBerry Enterprise Mobility Server.
4	Connectez-vous à BlackBerry UEM.
5	Configurez BlackBerry UEM selon les exigences de votre entreprise.
6	Si vous souhaitez partager les tâches d'administration avec d'autres membres de l'équipe informatique, créez des administrateurs.
7	Configurez des connexions professionnelles. Par exemple, e-mail, Wi-Fi et VPN.
8	Définissez des règles pour gérer la sécurité et le comportement des terminaux à l'aide de stratégies informatiques.
9	Configurez des normes pour les terminaux. Par exemple, règles de conformité.
10	Si votre entreprise utilise BlackBerry Dynamics, configurez les paramètres BlackBerry Dynamics.
11	Déterminez les applications à envoyer aux terminaux et ajoutez-les à BlackBerry UEM.
12	Contrôlez la manière dont les terminaux sont activés et gérés dans BlackBerry UEM à l'aide des profils d'activation.
13	Créez tout groupe d'utilisateurs ou compte d'utilisateur nécessaire.

Étape	Action
14	Attribuez des profils et des stratégies informatiques à des groupes d'utilisateurs ou à des comptes d'utilisateur.
15	Attribuez des applications à des groupes d'utilisateurs ou à des comptes d'utilisateur.
16	Demandez aux utilisateurs d'activer des terminaux sur BlackBerry UEM.

Fonctionnalités prises en charge par type de terminal

Ce guide de référence rapide compare les fonctionnalités prises en charge par les terminaux BlackBerry 10, BlackBerry SE (versions 5.0 à 7.1), iOS, macOS, Android et Windows dans BlackBerry UEM version 12.7.

La prise en charge des terminaux BlackBerry OS requiert une mise à niveau de BES5 vers BlackBerry UEM.

Pour plus d'informations sur les versions de système d'exploitation prises en charge, reportez-vous à la Matrice de compatibilité.

Fonctionnalités des terminaux

Fonctionnalité	BlackBerry 10	BlackBerry OS	iOS	macOS	Android	Windows
Activation sans fil	√	√	√	√	√	√
Activation sans fil à l'aide d'un code QR			√		√	
Activation filaire à l'aide de BlackBerry Wired Activation Tool	√					
Application client requise pour l'activation			√ [1]		√	√ [2]
Personnalisation du contrat des conditions d'utilisation pour l'activation	√		√	√	√	√ [3]
Limitation des activations par modèle de terminal	√		√	√	√	√ [4]

Fonctionnalité	BlackBerry 10	BlackBerry OS	iOS	macOS	Android	Windows
Affichage et exportation du rapport de terminal (par exemple, détails du matériel)	√	√	√	√	√	√
Limiter les terminaux non supervisés			√[5]	√[5]		

[1] Pour les terminaux iOS inscrits dans DEP, l'application client doit être attribuée à des utilisateurs ou des groupes.

[2] Pour terminaux Windows Phone 8.x uniquement.

[3]Pour les terminaux Windows 10 uniquement.

[4] Pour les terminaux Windows Phone 8.x et Windows 10 Mobile uniquement.

[5] Pour les terminaux activés avec des commandes MDM ou Confidentialité de l'utilisateur avec des licences SIM uniquement.

Fonctionnalités de sécurité

Fonctionnalité	BlackBerry 10	BlackBerry OS	iOS	macOS	Android	Windows
Séparation des données professionnelles et personnelles	√	√	√ [1]		√ [2]	√ [4]
Confidentialité de l'utilisateur pour les données personnelles	√	√	√ [1]		√ [2]	
Cryptage des données professionnelles inactives	√	√	√ [1]		√ [2]	√ [4]
Protection du terminal par envoi de commandes informatiques	√	√	√	√	√	√

Fonctionnalité	BlackBerry 10	BlackBerry OS	iOS	macOS	Android	Windows
Contrôle des fonctionnalités du terminal à l'aide de stratégies informatiques	√	√	√	√	√	√
Suppression des données professionnelles après une période d'inactivité	√		√ [1]		√ [1]	
Appliquer les exigences de mot de passe	√	√	√	√	√	√
Cryptage de la carte multimédia	√	√			√ [3]	
Application du cryptage de stockage interne	√	√			√	√

[1] Requiert des applications BlackBerry Dynamics.

[2] Nécessite Samsung KNOX Workspace, un profil professionnel Android ou des applications BlackBerry Dynamics.

[3] Pour terminaux Samsung KNOX uniquement.

[4]Pour les terminaux Windows 10 uniquement.

Envoi de certificats aux terminaux

Fonctionnalité	BlackBerry 10	BlackBerry OS	iOS	macOS	Android	Windows
Profils de certificat d'autorité de certification	√		√	√	√	√
Profils SCEP	√		√	√	√	√ [1]
Profils des certificats partagés			√	√	√	

Fonctionnalité	BlackBerry 10	BlackBerry OS	iOS	macOS	Android	Windows
Profils d'informations d'identification de l'utilisateur	√		√	√	√	

[1] For Windows 10 devices only.

Gestion des connexions professionnelles pour les terminaux

Fonctionnalité	BlackBerry 10	BlackBerry OS	iOS	macOS	Android	Windows
BlackBerry 2FA Profils	√		√		√	
Profils de connectivité BlackBe Dynamics			√	√	√	√
CalDAV Profils			√	√		
CardDAV Profils			√	√		
Profils de récupération de certificat	√					
Connectivité d'entreprise	√					
BlackBerry Secure Connect Plus	√		√ [1]		√ [2]	
Exchange ActiveSync Profils de messagerie	√		√	√	√ [3]	√
BlackBerry Secure Gateway			√			
Profils de messagerie IMAP/ POP3			√	√	√	√
Profils proxy	√		√	√	√	√ [4]

Fonctionnalité	BlackBerry 10	BlackBerry OS	iOS	macOS	Android	Windows
Profils d'identification unique	√		√			
Profils VPN	√	√	√	√	√ [5]	√ [6]
Wi-Fi Profils	√	√	√	√	√	√
Autres profils spécifiques au système d'exploitation	• Profils CRL • Profils OCSP				• Profils CRL[7]	• Profils de protection des données Windows[7]

[1] Uniquement pour les terminaux exécutant iOS version 9.0 et ultérieure.

[2] Uniquement pour les terminaux Android qui sont dotés d'un profil professionnel et les terminaux KNOX Workspace.

[3] Uniquement pour les terminaux Motorola prenant en charge les API EDM, les terminaux Android dotés d'un profil professionnel et les terminaux KNOX.

[4] Uniquement pour les terminaux Windows 10 (configurez les paramètres de proxy dans les profils VPN) et les terminaux Windows 10 Mobile (configurez les paramètres de proxy dans les profils Wi-Fi).

[5]Pour les terminaux KNOX Workspace uniquement.

[6]Pour les terminaux Windows 10 uniquement.

[7] Uniquement pour les terminaux BlackBerry optimisés par Android avec Android version 7.0 et ultérieure.

Gestion des normes de votre entreprise en matière de terminaux

Fonctionnalité	BlackBerry 10	BlackBerry OS	iOS	macOS	Android	Windows
Profils d'activation	√		√	√	√	√
Profils du mode de verrouillage des applications			√ [1]		√ [1]	√ [1]
BlackBerry Dynamics Profils			√	√	√	√
Profils de conformité BlackBerr Dynamics [2]			√	√	√	√
Profils de conformité	√		√		√	√ [3]

Fonctionnalité	BlackBerry 10	BlackBerry OS	iOS	macOS	Android	Windows
Profils des terminaux	√		√		√	√ [4]
Enterprise Management Agent Profils	√		√		√	√
Profils de service de localisation			√		√	√ [5]
Autres profils spécifiques au système d'exploitation	• Profils d'exigences SR des terminaux	• Règles de contrôle d'accès • Configuration logicielle	• AirPlay Profils • AirPrint Profils • Profils de la charge utile personnalisée • Profils des domaines gérés • Profils d'utilisation du réseau • Profils de notification par application [6] • Profils de filtre de contenu Web			

[1] Uniquement pour les terminaux iOS supervisés, les terminaux KNOX activés avec Contrôles MDM, les terminaux Windows 10 Education et les terminaux Windows 10 Enterprise.

[2] Si votre environnement inclut à la fois Good Control et BlackBerry UEM, après mise à niveau et synchronisation de Good Control avec BlackBerry UEM, les profils de conformité existants dans Good Control sont importés dans BlackBerry UEM en tant que profils de conformité BlackBerry Dynamics contenant les paramètres de conformité Good Control.

[3] Pour terminaux Windows Phone 8.x uniquement

[4]Pour les terminaux Windows 10 uniquement.

[5]Pour les terminaux Windows 10 Mobile uniquement.

[6] Uniquement pour les terminaux iOS supervisés exécutant iOS version 9.3 et ultérieure.

Protection des terminaux perdus ou volés

Fonctionnalité	BlackBerry 10	BlackBerry OS	iOS	macOS	Android	Windows
Spécifier un mot de passe de terminal	√	√			√	√ [1]
Verrouiller le terminal	√	√	√	√	√	√ [1]
Verrouillage d'activation			√ [2]			
Spécifier le mot de passe de l'espace Travail et verrouiller					√ [3]	
Déverrouiller le terminal et effacer le mot de passe			√		√	
Supprimer toutes les données du terminal	√	√	√	√	√ [4]	√
Supprimer uniquement les données professionnelles	√	√	√	√	√	√

[1] Pour terminaux Windows Phone 8.x et Windows 10 Mobile uniquement.

[2] Uniquement pour les terminaux exécutant iOS version 7.0 et ultérieure.

[3] Uniquement pour les terminaux Android qui sont dotés d'un profil professionnel et exécutant Android version 7.0 et ultérieure.

[4]Pour les terminaux Motorola prenant en charge l'API EDM, les informations stockées sur la carte multimédia sont également supprimées. Pour les terminaux KNOX Workspace, vous pouvez choisir de supprimer les informations de la carte multimédia.

Configuration de l'itinérance

Fonctionnalité	BlackBerry 10	BlackBerry OS	iOS	macOS	Android	Windows
Désactiver la synchronisation automatique en itinérance	√ [1]		√		√ [2]	
Désactiver les données en itinérance	√		√[3]		√ [4]	√

[1] Pour la synchronisation avec le serveur de messagerie uniquement.

[2] S'applique uniquement aux terminaux KNOX.

[3] Pour les terminaux exécutant iOS version 9.0 ou ultérieure, vous pouvez configurer les paramètres d'itinérance des données dans un profil d'utilisation du réseau.

[4] Pour les terminaux Android qui sont dotés d'un profil professionnel et les terminaux KNOX uniquement.

Gestion des applications

Fonctionnalité	BlackBerry 10	BlackBerry OS	iOS	macOS	Android	Windows
Distribuer les applications publiques à partir de la boutique (BlackBerry World, App Store, Google Play, Windows Store)	√		√		√	√
Gérer le catalogue d'applications professionnelles	√	√	√		√	√
Catalogue d'applications professionnelles de la marque	√		√			
Gestion des applications limitées			√		√ [1]	√ [1]

Fonctionnalité	BlackBerry 10	BlackBerry OS	iOS	macOS	Android	Windows
Distribuer les applications internes	√	√	√		√	√
Ajouter des raccourcis d'application aux terminaux			√	√	√	

[1] La liste des applications interdites n'est pas requise pour les terminaux Android dotés d'un profil professionnel, KNOX Workspace ou les terminaux Windows 10, car seules les applications que l'administrateur attribue peuvent être installées dans l'espace Travail ou sur des terminaux.

Gestion des applications BlackBerry Dynamics dans BlackBerry UEM

Les applications de productivité BlackBerry Dynamics permettent aux utilisateurs d'accéder aux données professionnelles et aux outils de productivité. Les applications BlackBerry Dynamics développées par BlackBerry incluent les applications suivantes :

Application	Description
BlackBerry Work	L'application BlackBerry Work fournit un accès sécurisé à votre messagerie professionnelle et permet aux utilisateurs d'afficher et d'envoyer des pièces jointes, de créer des notifications de contact personnalisées et de gérer leurs messages.
BlackBerry Access	BlackBerry Access est un navigateur sécurisé qui permet aux utilisateurs d'accéder aux intranets professionnels et aux applications Web. BlackBerry Access vous permet également d'activer l'accès à des ressources professionnelles ou de construire et de déployer de riches applications HTML5, tout en maintenant un niveau élevé de sécurité et de conformité.
BlackBerry Connect	BlackBerry Connect permet la communication et la collaboration avec la messagerie instantanée sécurisée, les recherches dans l'annuaire d'entreprise et la présence des utilisateurs à l'aide d'une interface facile à utiliser sur les terminaux des utilisateurs.
BlackBerry Tasks	BlackBerry Tasks permet aux utilisateurs de créer, modifier et gérer les tâches synchronisées avec Microsoft Exchange.
BlackBerry Notes	BlackBerry Notes permet aux utilisateurs de créer, modifier et gérer les notes synchronisées avec Microsoft Exchange sur le terminal mobile de leur choix.

Application	Description
BlackBerry Docs To Go	BlackBerry Docs To Go permet aux utilisateurs de créer, modifier et formater des documents Microsoft Word et des feuilles de calcul Microsoft Excel stockés dans l'application ou partagés avec d'autres applications BlackBerry Dynamics. Les utilisateurs peuvent également afficher, modifier et présenter des diaporamas Microsoft PowerPoint sur leurs terminaux.

Pour plus d'informations sur la gestion d'applications BlackBerry Dynamics, reportez-vous à Gestion des applications BlackBerry Dynamics et aux ressources pour les administrateurs pour chaque application.

Vous pouvez également utiliser les applications BlackBerry Dynamics développées par l'un des nombreux partenaires d'applications tierces de BlackBerry. Pour consulter la liste complète des applications disponibles au public, rendez-vous sur BlackBerry Marketplace for Enterprise Software.

Vous pouvez également développer vos propres applications BlackBerry Dynamics à l'aide du SDK BlackBerry Dynamics. Pour plus d'informations, reportez-vous au contenu relatif à SDK BlackBerry Dynamics.

Terminaux BlackBerry optimisés par Android

PRIV, DTEK et KEYone sont des exemples de terminaux BlackBerry optimisés par Android. Pour gérer ces terminaux avec BlackBerry UEM, vous pouvez suivre les instructions relatives aux terminaux Android.

Les types d'activation suivants sont disponibles sur les terminaux BlackBerry optimisés par Android :

- Travail et Personnel - Confidentialité de l'utilisateur
- Travail et Personnel - Confidentialité de l'utilisateur (Premium)
- Espace Travail uniquement
- Espace Travail uniquement (Premium)
- Contrôles MDM
- Confidentialité de l'utilisateur

Nous vous recommandons d'activer les terminaux BlackBerry optimisés par Android avec un type d'activation « Travail et Personnel » ou « Espace Travail uniquement » pour bénéficier d'une expérience optimale.

Options de gestion de terminaux

BlackBerry UEM prend en charge différentes options de gestion des terminaux. Les options que vous choisissez dépendent des types de terminaux que vous gérez et des exigences de sécurité de votre organisation.

BlackBerry UEM prend en charge les options de gestion suivantes :

- Contrôles MDM
- Travail et personnel
- Confidentialité de l'utilisateur
- Espace Travail uniquement

Pour chaque option de gestion, vous devez disposer du droit de licence disponible et un profil d'activation adapté doit être attribué aux utilisateurs.

Pour plus d'informations sur les profils d'activation, reportez-vous à la section Création de profils d'activation.

Pour plus d'informations sur les licences BlackBerry UEM, consultez le contenu relatif aux licences.

Pour plus d'informations sur la sécurité des différentes options de gestion, consultez le contenu Sécurité.

Gestion des terminaux au-delà des smartphones, tablettes et ordinateurs portables

Vous pouvez activer et gérer plus que des smartphones, tablettes, et ordinateurs portables avec BlackBerry UEM.

BlackBerry UEM gère également les terminaux suivants :

- Certains terminaux portables basés sur Android
- Apple TV

Gestion des terminaux portables

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

BlackBerry UEM prend en charge les terminaux portables suivants :

- Vuzix M300 Smart Glasses

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

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

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

Gestion des terminaux Apple TV

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

BlackBerry UEM prend en charge les versions Apple TV de deuxième génération ou les générations ultérieures.

Pour gérer les terminaux Apple TV, suivez les instructions et utilisez les paramètres de profil des terminaux iOS. Les fonctions BlackBerry UEM suivantes sont prises en charge pour Apple TV :

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

Pour empêcher les utilisateurs d'activer des terminaux Apple TV, définissez la restriction des modèles de terminaux dans le profil d'activation de sorte à interdire tous les terminaux Apple TV.

Pour activer les terminaux Apple TV, vous devez utiliser BlackBerry UEM Self-Service. Pour plus d'informations, reportez-vous à Activer un terminal Apple TV.

Qu'est-ce que BlackBerry UEM Client ?

BlackBerry UEM Client est une application qui permet aux utilisateurs d'activer leurs terminaux sur BlackBerry UEM. UEM Client doit être utilisé pour activer les périphériques suivants :

- iOS
- Android, y compris les appareils portables Android
- Windows Phone 8

Les utilisateurs peuvent télécharger UEM Client depuis : App Store, Google Play ou Windows Store.

Le tableau suivant répertorie les fonctions d'UEM Client :

Fonction de BlackBerry UEM Client	Description
Communication avec BlackBerry UEM	UEM Client permet à BlackBerry UEM de communiquer avec les terminaux à des fins d'activation et de gestion de ceux-ci. Pour plus d'informations sur les flux de données, reportez-vous au contenu relatif à l'architecture.
Activation	Les utilisateurs doivent télécharger la version la plus récente d'UEM Client à partir de la boutique d'applications qui convient et utiliser leur adresse électronique et leur mot de passe d'activation ou QR Code pour activer les terminaux sur BlackBerry UEM. Les utilisateurs n'ont pas besoin de UEM Client pour activer les terminaux dans les cas suivants : • Pour les terminaux iOS, si vous utilisez Apple Configurator 2 ou le Programme d'inscription d'Apple, les utilisateurs n'ont pas besoin d'UEM Client pour activer leurs terminaux. Si vous souhaitez appliquer des règles de conformité, les utilisateurs doivent installer et lancer l'application UEM Client à l'issue de l'activation. • Pour les terminaux iOS et Android qui n'ont pas besoin de MDM, les utilisateurs peuvent activer les applications BlackBerry Dynamics à l'aide de clés d'accès au lieu d'utiliser UEM Client.Toutefois, l'utilisation de UEM Client présente des avantages, en offrant notamment une expérience d'activation cohérente qui ne nécessite pas de clés d'accès, un accès au catalogue d'applications professionnelles de UEM Client ou BlackBerry Dynamics Launcher (si configuré), et la possibilité pour les utilisateurs d'autoriser les services de localisation (si configurés). Pour plus d'informations, reportez-vous à Activation des terminaux.
Désactivation	Les utilisateurs peuvent cliquer sur Désactiver mon terminal dans la section À propos d'UEM Client pour supprimer le terminal de BlackBerry UEM et effacer toutes les données professionnelles du terminal.

Fonction de BlackBerry UEM Client	Description
Applications professionnelles	UEM Client permet aux utilisateurs d'accéder aux applications que vous leur attribuez pour les télécharger. En outre, si le paramètre correspondant est configuré, ils peuvent évaluer les applications et déposer des commentaires sur celles-ci. Pour les terminaux iOS activés en mode Confidentialité de l'utilisateur, les utilisateurs peuvent accéder au catalogue d'applications professionnelles à partir d'un lien disponible dans UEM Client. Pour les terminaux iOS activés en mode MDM, une icône personnalisable est disponible sur l'écran d'accueil afin d'accéder aux applications professionnelles. Pour les terminaux Android, les utilisateurs peuvent accéder au catalogue d'applications professionnelles à partir d'UEM Client. Pour les terminaux Windows Phone 8, les utilisateurs peuvent accéder au catalogue d'applications professionnelles à partir d'UEM Client. Pour plus d'informations, reportez-vous à Applications.
Profils et stratégies	Les profils, stratégies et certificats que vous attribuez aux utilisateurs sont affichés dans UEM Client.
Conformité	Sur l'écran d'accueil d'UEM Client, les utilisateurs peuvent sélectionner Conforme ou Non conforme pour afficher un rapport d'état de leur terminal basé sur le profil de conformité que vous leur avez attribué. Pour les terminaux activés à l'aide d'Apple Configurator 2 ou du Programme d'inscription d'Apple, si vous souhaitez appliquer des règles de conformité, les utilisateurs doivent installer et lancer BlackBerry UEM Client à l'issue de l'activation. Pour plus d'informations, reportez-vous à Application des règles de conformité aux terminaux.
BlackBerry 2FA	S'il est configuré, les utilisateurs peuvent contourner l'authentification à deux facteurs requise par BlackBerry 2FA en se pré-authentifiant dans UEM Client. Pour plus d'informations, reportez-vous au contenu relatif à BlackBerry 2FA.
Service de localisation	Si vous créez un profil de service de localisation et que vous l'attribuez à des comptes d'utilisateur, les utilisateurs sont invités à autoriser UEM Client à accéder à l'emplacement de leur terminal.
Fichiers journaux du terminal	Les utilisateurs peuvent envoyer les fichiers journaux du terminal par e-mail depuis UEM Client. Pour plus d'informations, reportez-vous à Récupérer les journaux des terminaux.

Fonction de BlackBerry UEM Client	Description
À propos de	Dans la section À propos d'UEM Client, les utilisateurs peuvent voir tout ou partie des informations suivantes en fonction du type de terminal et du type d'activation : • Version d'UEM Client • Date et heure auxquelles le terminal a été activé • Informations d'entreprise que vous avez configurées dans le profil du terminal (par exemple, coordonnées de votre entreprise) • URL du serveur BlackBerry UEM • Contrat de licence utilisateur final • Bouton permettant aux utilisateurs de désactiver leur terminal

Qu'est-ce que BlackBerry UEM Self-Service ?

BlackBerry UEM Self-Service est une application Web que vous pouvez mettre à la disposition des utilisateurs pour leur permettre d'effectuer certaines tâches telles que la création de mots de passe d'activation, le verrouillage de leurs terminaux ou la suppression des données de leurs terminaux. Les utilisateurs n'ont aucun logiciel à installer pour utiliser BlackBerry UEM Self-Service.

Vous devez fournir les informations de connexion BlackBerry UEM Self-Service aux utilisateurs. Vous pouvez envoyer ces informations par e-mail ou modifier le modèle d'e-mail d'activation pour les y inclure. Les utilisateurs ont besoin des informations suivantes :

- Adresse Web : l'adresse Web de BlackBerry UEM Self-Service s'affiche dans la console de gestion sous Paramètres > Libre-service.
- Nom d'utilisateur et mot de passe : les utilisateurs des annuaires d'entreprise peuvent se connecter à l'aide de leurs noms d'utilisateur et mots de passe. Pour les utilisateurs locaux, vous devez créer des noms d'utilisateur et des mots de passe temporaires.
- Nom de domaine : le nom de domaine est requis pour les utilisateurs Microsoft Active Directory.

Vous pouvez également créer un avis de connexion que les utilisateurs doivent lire et accepter avant de pouvoir se connecter à BlackBerry UEM Self-Service.

Pour plus d'informations sur l'utilisation de BlackBerry UEM Self-Service, consultez le Guide de l'utilisateur BlackBerry UEM Self-Service.

Tâches connexes

Créer un avis de connexion pour les consoles

Services BlackBerry Enterprise Mobility Suite

Outre les fonctionnalités de sécurité et de productivité fournies par BlackBerry UEM, BlackBerry offre des services supplémentaires qui peuvent apporter de la valeur ajoutée à votre domaine BlackBerry UEM en répondant aux besoins uniques de votre entreprise. Vous pouvez ajouter les services suivants et les gérer via la console de gestion de BlackBerry UEM :

Type de service	Nom et description du service
Services d'entreprise	• BlackBerry Workspaces permet aux utilisateurs d'ouvrir, de synchroniser, de modifier et de partager en toute sécurité des fichiers et dossiers sur des tablettes et ordinateurs Windows et Mac OS ou sur des terminaux Android, iOS et BlackBerry 10. BlackBerry Workspaces protège les fichiers en appliquant des contrôles DRM pour en limiter l'accès, même après leur partage avec des personnes extérieures à votre entreprise. • BlackBerry Enterprise Identity donne aux utilisateurs un accès d'authentification unique à des fournisseurs de services tels que BlackBerry Workspaces, Box, Workday, WebEx, Salesforce, etc. Vous pouvez également ajouter la prise en charge de services SaaS personnalisés. • BlackBerry 2FA protège l'accès aux ressources critiques de votre organisation à l'aide de l'authentification à deux facteurs. BlackBerry 2FA utilise un mot de passe que les utilisateurs doivent saisir et affiche une invite sécurisée sur leur terminal Android iOS ou BlackBerry 10 chaque fois qu'ils tentent d'accéder à des ressources. • BlackBerry UEM Notifications permet aux administrateurs d'envoyer un message aux utilisateurs via SMS, téléphone et e-mail, directement à partir de la console UEM. Cet add-on simplifie les communications pour les utilisateurs finaux et groupes d'utilisateurs, en éliminant la nécessité de solutions de messagerie supplémentaires.
Plate-forme BlackBerry Dynamics	• BlackBerry Enterprise Mobility Server (BEMS) fournit des services supplémentaires aux applications BlackBerry Dynamics. BEMS intègre les services suivants : BlackBerry Mail, BlackBerry Connect, BlackBerry Presence et BlackBerry Docs. Lorsque ces services sont intégrés, les utilisateurs peuvent communiquer les uns avec les autres via une messagerie instantanée sécurisée, afficher la présence en temps réel des utilisateurs dans les applications BlackBerry Dynamics et ouvrir, synchroniser et partager le serveur de fichiers professionnel et les documents Microsoft SharePoint. • Le SDK BlackBerry Dynamics SDK permet aux développeurs de créer des applications sécurisées pour les terminaux Android et iOS et pour les ordinateurs Mac OS et Windows. Il s'agit du côté client de la plate-forme BlackBerry Dynamics.

Type de service	Nom et description du service
Applications de productivité BlackBerry Dynamics	• BlackBerry Workfournit tout ce dont les utilisateurs ont besoin pour travailler en toute sécurité, y compris une messagerie, un calendrier et des contacts (synchronisation complète avec Microsoft Exchange). L'application permet également une collaboration avancée sur les documents.BlackBerry Work sépare les données professionnelles des données personnelles, et permet une intégration transparente avec d'autres applications professionnelles sans qu'aucun profil MDM ne soit nécessaire sur le terminal. • BlackBerry Accesspermet aux utilisateurs d'accéder en toute sécurité à l'intranet de leur entreprise avec le terminal mobile de leur choix. • BlackBerry Connectpermet de communiquer et de collaborer via une messagerie instantanée sécurisée, d'effectuer des recherches dans l'annuaire d'entreprise et d'afficher la présence des utilisateurs grâce à une interface facile à utiliser disponible sur le terminal de l'utilisateur. • BlackBerry Sharepermet aux utilisateurs d'ouvrir, de télécharger et de partager des documents en toute sécurité en intégrant Microsoft SharePoint et d'autres référentiels professionnels au terminal de l'utilisateur. • BlackBerry Taskspermet aux utilisateurs de créer, modifier et gérer les notes synchronisées avec Microsoft Exchange sur leurs terminaux Android et iOS. • BlackBerry Notespermet aux utilisateurs de créer, modifier et gérer les notes synchronisées avec Microsoft Exchange sur le terminal mobile de leur choix.

Pour en savoir plus sur les différents types de licences BlackBerry Enterprise Mobility Suite et la procédure d'activation, consultez le contenu relatif aux licences.

Se connecter à BlackBerry UEM

La console de gestion vous permet d'effectuer des tâches administratives pour les terminaux de votre organisation gérés par BlackBerry UEM.

Avant de commencer :

- Recherchez l'adresse Web (par exemple, https://<*hostname*>/admin/index.jsp.) et les informations de connexion de la console de gestion. Ces informations sont disponibles dans la boite de réception du compte de messagerie associé à votre compte BlackBerry UEM.
- Vous devez connaitre la méthode d'authentification et le domaine (authentification Microsoft Active Directory uniquement).

1. Dans le navigateur, saisissez l'adresse Web de la console de gestion BlackBerry UEM de votre entreprise.
2. Dans le champ **Nom d'utilisateur**, saisissez votre nom d'utilisateur.
3. Dans le champ **Mot de passe**, saisissez votre mot de passe.
4. Si nécessaire, dans la liste déroulante **Connexion via**, procédez comme suit :
   - Cliquez sur **Authentification directe**.
   - Cliquez sur **Authentification LDAP**.
   - Cliquez sur **Authentification Microsoft Active Directory** . Dans le champ **Domaine**, saisissez le domaine Microsoft Active Directory.
5. Cliquez sur **Se connecter**.

À la fin : vous pouvez modifier votre mot de passe de connexion en cliquant sur l'icône utilisateur située en haut à droite de la console de gestion.

Administrateurs

Les administrateurs sont des utilisateurs auxquels un groupe d'utilisateurs ou un compte d'utilisateur a attribué un rôle administratif. Les actions que les administrateurs peuvent effectuer sont définies dans le rôle qui leur est attribué. Vous pouvez attribuer un rôle préconfiguré ou un rôle personnalisé que vous créez. Chaque rôle dispose d'un ensemble d'autorisations qui définit les informations que les administrateurs peuvent afficher et les actions qu'ils peuvent effectuer dans la console de gestion de BlackBerry UEM.

Les rôles permettent à votre organisation de :

- Réduire les risques de sécurité associés en autorisant tous les administrateurs à accéder aux différentes options administratives
- Définir différents types d'administrateurs pour mieux répartir les responsabilités
- Renforcer l'efficacité des administrateurs en limitant les options accessibles à leurs responsabilités

Étapes à suivre pour configurer l'administration UEM

Pour configurer la console de gestion pour l'administration UEM, procédez comme suit :

Étape	Action
1	Si nécessaire, vous pouvez personnaliser la couleur des consoles et personnaliser la page de connexion et la barre de menus.
2	Si nécessaire, créez des signets dans les consoles.
3	Si nécessaire, modifiez la langue pour les e-mails automatisés.
4	Si nécessaire, créez un avis de connexion pour les consoles.
5	Révisez les rôles préconfigurés et, si nécessaire, créez un rôle personnalisé.
6	Classer les rôles.
7	Créer un administrateur.

Personnalisation de l'apparence des consoles

Vous pouvez personnaliser l'apparence des consoles en sélectionnant un jeu de couleurs personnalisé et en modifiant le texte et les images sur l'écran de connexion, ainsi que l'image sur la barre de menus. Les couleurs,

les images et le texte que vous sélectionnez sont utilisés aussi bien dans la console de gestion que dans la console BlackBerry UEM Self-Service.

Personnaliser la couleur des consoles

Vous pouvez sélectionner un jeu de couleurs personnalisé pour les consoles. Les couleurs que vous sélectionnez sont utilisées aussi bien dans la console de gestion que dans la console BlackBerry UEM Self-Service.

1. Dans la barre de menus, cliquez sur **Paramètres > Paramètres généraux**.
2. Cliquez sur **Personnaliser la console**.
3. Sélectionnez deux couleurs pour la console. Effectuez l'une des opérations suivantes :
   - Cliquez sur la case à gauche du code couleur, puis sélectionnez une couleur dans la palette de couleurs.
   - Saisissez des codes couleur au format hexadécimal dans les champs de sélection.
   - Sélectionnez une couleur à partir des échantillons de couleur situés à droite du code couleur.

   Un aperçu du jeu de couleurs s'affiche sur la page.
4. Cliquez sur **Enregistrer**.

À la fin : Déconnectez-vous, puis reconnectez-vous pour afficher le jeu de couleurs mis à jour.

Personnaliser la page de connexion et la barre de menus

Vous pouvez personnaliser l'apparence des consoles en sélectionnant des images personnalisées et un texte d'en-tête pour la page de connexion et une image personnalisée pour la barre de menus. Les images et le texte que vous sélectionnez sont utilisés aussi bien dans la console de gestion que dans la console BlackBerry UEM Self-Service. Les images personnalisées ne peuvent pas dépasser 2 Mo.

1. Dans la barre de menus, cliquez sur **Paramètres > Paramètres généraux**.
2. Cliquez sur **Personnalisation de BlackBerry UEM**.
3. Cliquez sur l'image de la page de connexion ou de la barre de menus que vous souhaitez modifier.
4. Cliquez sur **Parcourir** pour sélectionner une image, puis cliquez sur **Envoyer**.
   L'image d'arrière-plan de la page de connexion s'ajuste à la largeur de la fenêtre du navigateur et conserve le ratio d'aspect de l'image. Les images de la barre de menus et le logo de la société de la page de connexion s'ajustent à la hauteur de la zone et conservent le ratio d'aspect.
5. Cliquez sur le texte d'en-tête de la page de connexion pour le modifier ou le supprimer.
6. Cliquez sur **Enregistrer**.

À la fin : Déconnectez-vous, puis reconnectez-vous pour afficher le texte et les images mis à jour.

Création de signets de site Web dans les consoles

Vous pouvez créer des signets de site Web dans la console de gestion BlackBerry UEM et la console BlackBerry UEM Self-Service. Vous pouvez créer différents signets pour chaque console. Par exemple, vous pouvez créer un signet dans BlackBerry UEM Self-Service pour créer un lien vers les fichiers d'aide personnalisés aux terminaux des utilisateurs.

Avant de commencer : Vous devez être un administrateur de sécurité pour pouvoir créer ou modifier des signets dans les consoles.

1. Connectez-vous à BlackBerry UEM ou BlackBerry UEM Self-Service.
2. Cliquez sur ★ dans l'angle supérieur droit.
3. Sous **Ajouter une adresse web**, ajoutez les informations de signet :

a) Donnez un nom au signet.
b) Saisissez l'URL du site Web. L'URL doit commencer par « http:// » ou « https:// ».

4. Cliquez sur **Enregistrer**.

À la fin : Cliquez sur ★ pour afficher vos signets. Tous les utilisateurs peuvent accéder aux signets, mais seuls les administrateurs de sécurité sont autorisés à créer ou modifier des signets.

Modifier la langue pour les e-mails automatisés

Dans la console de gestion, vous pouvez modifier la langue des e-mails automatisés. BlackBerry UEM utilise la langue que vous spécifiez dans les e-mails que vous ne pouvez pas modifier (par exemple, les notifications à propos de l'accès administrateur et des mots de passe de la console).

1. Sur la barre de menus, cliquez sur **Paramètres**.
2. Dans le volet de gauche, développez **Paramètres généraux.**
3. Cliquez sur **Langue**.
4. Dans la liste déroulante, cliquez sur la langue que vous souhaitez utiliser dans les e-mails automatisés de BlackBerry UEM.
5. Cliquez sur **Enregistrer**.

Créer un avis de connexion pour les consoles

Vous pouvez créer un avis de connexion à afficher pour les administrateurs ou les utilisateurs lorsqu'ils accèdent à la console de gestion ou à BlackBerry UEM Self-Service. Cet avis informe les administrateurs ou les utilisateurs des conditions d'utilisation qu'ils doivent accepter pour pouvoir utiliser la console de gestion ou BlackBerry UEM Self-Service.

1. Sur la barre de menus, cliquez sur **Paramètres**.
2. Dans le volet de gauche, développez **Paramètres généraux.**
3. Cliquez sur **Avis de connexion**.
4. Cliquez sur ✎.
5. Effectuez l'une des tâches suivantes :

Tâche	Étapes
Configurer un avis de connexion pour la console de gestion	**a.** Cochez la case **Activer un avis de connexion pour la console de gestion**. **b.** Entrez les informations que vous souhaitez afficher pour les administrateurs lorsqu'ils accèdent à la console de gestion.
Configurer un avis de connexion pour BlackBerry UEM Self-Service	**a.** Cochez la case **Activer un avis de connexion pour la console en libre-service**. **b.** Entrez les informations que vous souhaitez afficher pour les utilisateurs lorsqu'ils accèdent à BlackBerry UEM Self-Service.

6. Cliquez sur **Enregistrer**.

Création et gestion de rôles d'administrateur

Vous pouvez passer en revue les rôles préconfigurés disponibles dans BlackBerry UEM pour déterminer si vous devez créer des rôles personnalisés ou modifier les paramètres de rôle pour répondre aux besoins de votre entreprise. Vous devez être un administrateur de sécurité pour créer des rôles personnalisés, afficher des informations à propos d'un rôle, modifier les paramètres de rôle, supprimer des rôles et classer des rôles.

Rôles préconfigurés

Dans BlackBerry UEM, le rôle Administrateur de sécurité dispose des autorisations maximales sur la console de gestion, y compris sur la création et la gestion de rôles et d'administrateurs. Au moins un administrateur doit être Administrateur de sécurité.

BlackBerry UEM inclut des rôles préconfigurés, en plus du rôle Administrateur de sécurité. Vous pouvez modifier ou supprimer tous les rôles, à l'exception du rôle Administrateur de sécurité.

Les rôles préconfigurés suivants sont disponibles :

- Administrateur de sécurité : autorisations maximales
- Administrateur d'entreprise : toutes les autorisations, sauf la création et la modification des rôles et administrateurs
- Centre d'assistance senior : autorisations permettant d'effectuer des tâches administratives intermédiaires
- Centre d'assistance junior : autorisations permettant d'effectuer des tâches administratives de base

Autorisations pour les rôles préconfigurés

Les tableaux suivants répertorient les autorisations activées par défaut pour chaque rôle préconfiguré dans BlackBerry UEM. Dans BlackBerry UEM, le rôle Administrateur de sécurité dispose des autorisations maximales sur la console de gestion, y compris sur la création et la gestion de rôles et d'administrateurs.

Remarque : si vous procédez à la mise à niveau de BES5, la configuration des rôles dans BES5 est copiée vers BlackBerry UEM. Les rôles copiés peuvent porter des noms similaires, mais être dotés d'autorisations différentes. Vous devez examiner les autorisations de chaque rôle pour déterminer si vous devez activer ou désactiver des autorisations.

Rôles et administrateurs

Par défaut, le rôle Administrateur de sécurité dans BlackBerry UEM comprend des autorisations pour créer et gérer des rôles et des administrateurs. Ces autorisations ne sont pas disponibles dans la console de gestion et ne peuvent pas être activées pour un autre rôle.

Autorisation	Administrateur de sécurité	Administrateur d'entreprise	Centre d'assistance senior	Centre d'assistance junior
Afficher les rôles	√	NA	NA	NA
Créer et modifier des rôles	√	NA	NA	NA
Supprimer des rôles	√	NA	NA	NA
Classer les rôles	√	NA	NA	NA

Autorisation	Administrateur de sécurité	Administrateur d'entreprise	Centre d'assistance senior	Centre d'assistance junior
Créer des administrateurs	√	NA	NA	NA
Supprimer des administrateurs	√	NA	NA	NA
Modifier des attributs non administratifs d'administrateurs	√	NA	NA	NA
Modifier le mot de passe d'autres administrateurs	√	NA	NA	NA
Modifier l'appartenance de rôle pour les administrateurs	√	NA	NA	NA

Accès aux répertoires

Vous pouvez spécifier les répertoires d'entreprise auxquels l'administrateur peut accéder.

Autorisation	Administrateur de sécurité	Administrateur d'entreprise	Centre d'assistance senior	Centre d'assistance junior
Tous les répertoires d'entreprise	√	√	√	√
Répertoires d'entreprise sélectionnés uniquement				

Gestion des groupes

Vous pouvez indiquer les groupes que l'administrateur peut gérer. Pour gérer les utilisateurs qui n'appartiennent à aucun groupe, les administrateurs doivent être autorisés à gérer tous les groupes et utilisateurs.

Autorisation	Administrateur de sécurité	Administrateur d'entreprise	Centre d'assistance senior	Centre d'assistance junior
Tous les groupes et utilisateurs	√	√	√	√

Autorisation	Administrateur de sécurité	Administrateur d'entreprise	Centre d'assistance senior	Centre d'assistance junior
Groupes sélectionnés				

Utilisateurs et terminaux

Autorisation	Administrateur de sécurité	Administrateur d'entreprise	Centre d'assistance senior	Centre d'assistance junior
Afficher les utilisateurs et les terminaux activés	√	√	√	√
Créer des utilisateurs	√	√	√	
Modifier des utilisateurs	√	√	√	√
Attribuer des rôles d'utilisateur	√	√	√	√
Supprimer des utilisateurs	√	√	√	
Exporter la liste des utilisateurs	√	√		
Générer un mot de passe d'activation et l'envoyer par e-mail	√	√	√	√
Créer des mots de passe d'activation et envoyer des e-mails d'activation à plusieurs utilisateurs	√	√	√	
Spécifier un mot de passe d'activation.	√	√	√	√
Spécifier plusieurs mots de passe d'activation avec des profils d'activation uniques pour un utilisateur	√	√		

Autorisation	Administrateur de sécurité	Administrateur d'entreprise	Centre d'assistance senior	Centre d'assistance junior
Spécifiez si les mots de passe d'activation doivent expirer suite à l'activation du premier terminal.	√	√		
Afficher les clés d'accès et QR codes d'activation de l'utilisateur	√	√		
Spécifier un mot de passe de compte	√	√	√	√
Modifier plusieurs mots de passe de compte	√	√	√	
Définir la pré-authentification BlackBerry 2FA	√	√		
Gérer les terminaux	√	√	√	√
Activer l'espace Travail	√	√	√	√
Désactiver l'espace Travail	√	√	√	√
Verrouiller l'espace Travail	√	√	√	√
Réinitialiser le mot de passe de l'espace Travail	√	√	√	√
Spécifier un mot de passe de terminal	√	√	√	√
Verrouiller le terminal et définir un message	√	√	√	√
Déverrouiller le terminal et effacer le mot de passe	√	√	√	√

Autorisation	Administrateur de sécurité	Administrateur d'entreprise	Centre d'assistance senior	Centre d'assistance junior
Supprimer uniquement les données professionnelles	√	√	√	√
Supprimer uniquement les données professionnelles de plusieurs terminaux	√			
Supprimer toutes les données du terminal	√	√	√	√
Supprimer toutes les données de plusieurs terminaux	√			
Supprimer le terminal	√	√		
Supprimer plusieurs terminaux	√			
Spécifier un mot de passe professionnel et verrouiller	√	√	√	√
Obtenir les journaux du terminal	√	√	√	
Activer le verrouillage d'activation	√	√	√	√
Désactiver le verrouillage d'activation	√	√	√	√
Mode Perdu	√	√	√	√
Activer le mode Perdu	√	√	√	√
Désactiver le mode Perdu	√	√	√	√
Localiser le terminal	√	√	√	√
Enregistrer le terminal	√	√	√	
Redémarrer le terminal	√	√	√	√

Autorisation	Administrateur de sécurité	Administrateur d'entreprise	Centre d'assistance senior	Centre d'assistance junior
Mettre à jour le logiciel iOS	√	√	√	√
Mettre à jour le logiciel iOS sur plusieurs terminaux	√			
Désactiver le terminal	√	√	√	√
Afficher les détails de localisation du terminal	√	√	√	
Afficher l'historique de localisation du terminal	√	√		
Afficher les informations de contrôle d'accès Exchange	√	√		
Afficher les informations sur le terminal du programme d'inscription des appareils Apple	√	√	√	√
Attribuer des configurations d'inscription	√	√		
Afficher les jetons de mot de passe à usage unique	√	√	√	√
Attribuer des jetons de mot de passe à usage unique	√	√		
Envoyer un e-mail aux utilisateurs	√	√	√	
Consulter l'historique de contournement du verrouillage d'activation	√	√	√	

Autorisation	Administrateur de sécurité	Administrateur d'entreprise	Centre d'assistance senior	Centre d'assistance junior
Gérer les applications BlackBerry Dynamics	√	√	√	√
Verrouiller l'application	√	√	√	
Déverrouiller l'application	√	√	√	√
Supprimer les données d'application	√	√	√	√
Contrôler la journalisation d'une application	√	√	√	
Afficher les paramètres du groupe de terminaux partagés	√	√		
Créer et modifier les groupes de terminaux partagés	√	√		
Supprimer les groupes de terminaux partagés	√	√		
Gérer les applications Intune	√	√	√	

Groupes

Autorisation	Administrateur de sécurité	Administrateur d'entreprise	Centre d'assistance senior	Centre d'assistance junior
Afficher les paramètres de groupe	√	√	√	√
Créer et modifier les groupes d'utilisateurs	√	√	√	
Attribuer des rôles d'utilisateur	√	√	√	

Autorisation	Administrateur de sécurité	Administrateur d'entreprise	Centre d'assistance senior	Centre d'assistance junior
Ajouter et supprimer des utilisateurs de groupes d'utilisateurs	√	√	√	
Supprimer des groupes d'utilisateurs	√	√		
Créer et modifier les groupes de terminaux	√	√	√	
Supprimer des groupes de terminaux	√	√		

Stratégies et profils

Autorisation	Administrateur de sécurité	Administrateur d'entreprise	Centre d'assistance senior	Centre d'assistance junior
Afficher les stratégies informatiques	√	√	√	√
Créer et modifier les stratégies informatiques	√	√		
Supprimer des stratégies informatiques	√	√		
Afficher les profils de messagerie	√	√	√	√
Créer et modifier des profils de messagerie	√	√		
Supprimer des profils de messagerie	√	√		
Afficher les profils de messagerie IMAP/POP3	√	√	√	√
Créer et modifier des profils de messagerie IMAP/POP3	√	√		

Autorisation	Administrateur de sécurité	Administrateur d'entreprise	Centre d'assistance senior	Centre d'assistance junior
Supprimer les profils de messagerie IMAP/POP3	√	√		
Afficher les profils de connectivité d'entreprise	√	√	√	√
Créer et modifier des profils de connectivité d'entreprise	√	√		
Supprimer des profils de connectivité d'entreprise	√	√		
Afficher les profils d'exigences SR des terminaux	√	√	√	√
Créer et modifier des profils d'exigences SR des terminaux	√	√		
Supprimer des profils d'exigences SR des terminaux	√	√		
Afficher les profils d'activation	√	√	√	√
Créer et modifier des profils d'activation	√	√		
Supprimer des profils d'activation	√	√		
Afficher les profils Wi-Fi	√	√	√	√
Créer et modifier des profils Wi-Fi	√	√		
Supprimer des profils Wi-Fi	√	√		
Afficher les profils VPN	√	√	√	√

Autorisation	Administrateur de sécurité	Administrateur d'entreprise	Centre d'assistance senior	Centre d'assistance junior
Créer et modifier des profils VPN	√	√		
Supprimer des profils VPN	√	√		
Afficher les profils VPN	√	√	√	√
Créer et modifier des profils VPN	√	√		
Supprimer des profils VPN	√	√		
Afficher les profils de conformité	√	√	√	√
Créer et modifier des profils de conformité	√	√		
Supprimer des profils de conformité	√	√		
Afficher les profils de terminaux	√	√	√	√
Créer et modifier des profils de terminaux	√			
Supprimer des profils de terminaux	√	√		
Afficher les profils proxy	√	√	√	√
Créer et modifier des profils proxy	√	√		
Supprimer des profils proxy	√	√		
Afficher les profils de filtre de contenu Web	√	√	√	√
Créer et modifier des profils de filtre de contenu Web	√	√		

Autorisation	Administrateur de sécurité	Administrateur d'entreprise	Centre d'assistance senior	Centre d'assistance junior
Supprimer des profils de filtre de contenu Web	√	√		
Afficher les profils FileVault	√	√	√	√
Créer et modifier des profils FileVault	√	√		
Supprimer des profils FileVault	√	√		
Afficher les profils de service de localisation	√	√	√	√
Créer et modifier des profils de service de localisation	√	√		
Supprimer des profils de service de localisation	√	√		
Afficher les profils du mode de verrouillage des applications	√	√	√	√
Créer et modifier des profils du mode de verrouillage des applications	√	√		
Supprimer des profils du mode de verrouillage des applications	√	√		
Afficher les profils avec identification unique	√	√	√	√
Créer et modifier des profils avec identification unique	√	√		

Autorisation	Administrateur de sécurité	Administrateur d'entreprise	Centre d'assistance senior	Centre d'assistance junior
Supprimer des profils avec identification unique	√	√		
Afficher les profils de certificat CA	√	√	√	√
Créer et modifier des profils de certificat CA	√	√		
Supprimer des profils de certificat CA	√	√		
Afficher les profils de certificat partagé	√	√	√	√
Créer et modifier des profils de certificat partagé	√	√		
Supprimer des profils de certificat partagé	√	√		
Afficher les profils SCEP	√	√	√	√
Créer et modifier des profils SCEP	√	√		
Supprimer des profils SCEP	√	√		
Afficher les profils OCSP	√	√	√	√
Créer et modifier des profils OCSP	√	√		
Supprimer des profils OCSP	√	√		
Afficher les profils de récupération de certificat	√	√	√	√
Créer et modifier des profils de récupération de certificat	√	√		

Autorisation	Administrateur de sécurité	Administrateur d'entreprise	Centre d'assistance senior	Centre d'assistance junior
Supprimer des profils de récupération de certificat	√	√		
Afficher les profils CRL	√	√	√	√
Créer et modifier des profils CRL	√	√		
Supprimer des profils CRL	√	√		
Afficher des profils de domaines gérés	√	√	√	√
Créer et modifier des profils de domaines gérés	√	√		
Supprimer des profils de domaines gérés	√	√		
Afficher les profils d'identification d'utilisateurs	√	√	√	√
Créer et modifier des profils d'identification d'utilisateurs	√	√		
Supprimer des profils d'identification d'utilisateurs	√	√		
Afficher les profils de charge utile personnalisée	√	√	√	√
Créer et modifier des profils de charge utile personnalisée	√	√		
Supprimer des profils de charge utile personnalisée	√	√		

Autorisation	Administrateur de sécurité	Administrateur d'entreprise	Centre d'assistance senior	Centre d'assistance junior
Attribuer des stratégies informatiques et des profils aux utilisateurs	√	√	√	√
Attribuer des stratégies informatiques et des profils aux groupes d'utilisateurs	√	√	√	√
Attribuer des stratégies informatiques et profils aux groupes de terminaux	√	√	√	√
Attribuer des stratégies informatiques et des profils aux groupes de terminaux partagés	√	√		
Classer les stratégies informatiques et les profils	√	√		
Afficher les profils CardDAV	√	√	√	√
Créer et modifier des profils CardDAV	√	√		
Supprimer des profils CardDAV	√	√		
Afficher les profils AirPrint	√	√	√	√
Créer et modifier des profils AirPrint	√	√		
Supprimer des profils AirPrint	√	√		
Afficher les profils d'utilisation du réseau	√	√	√	√

Autorisation	Administrateur de sécurité	Administrateur d'entreprise	Centre d'assistance senior	Centre d'assistance junior
Créer et modifier les profils d'utilisation du réseau	√	√		
Supprimer les profils d'utilisation du réseau	√	√		
Afficher les profils AirPlay	√	√	√	√
Créer et modifier des profils AirPlay	√	√		
Supprimer des profils AirPlay	√	√		
Afficher les profils Enterprise Management Agent	√	√	√	√
Créer et modifier des profils Enterprise Management Agent	√	√		
Supprimer des profils Enterprise Management Agent	√	√		
Afficher les profils de conformité BlackBerry Dynamics	√	√	√	√
Supprimer des profils de conformité BlackBerry Dynamics	√	√		
Afficher les profils BlackBerry Dynamics	√	√	√	√
Créer et modifier des profils BlackBerry Dynamics	√	√		
Supprimer des profils BlackBerry Dynamics	√	√		

Autorisation	Administrateur de sécurité	Administrateur d'entreprise	Centre d'assistance senior	Centre d'assistance junior
Afficher les profils de connectivité BlackBerry Dynamics	√	√	√	√
Créer et modifier des profils de connectivité BlackBerry Dynamics	√	√		
Supprimer des profils de connectivité BlackBerry Dynamics	√	√		
Afficher les profils Ne pas déranger	√	√	√	√
Créer et modifier des profils Ne pas déranger	√	√		
Supprimer des profils Ne pas déranger	√	√		
Afficher les profils BlackBerry 2FA	√	√	√	√
Créer et modifier des profils BlackBerry 2FA	√	√		
Supprimer des profils BlackBerry 2FA	√	√		
Afficher les profils de protection des données Windows	√	√	√	√
Créer et modifier des profils de protection des données Windows	√	√		
Supprimer des profils de protection des données Windows	√	√		
Afficher les profils de notification par application	√	√	√	√

Autorisation	Administrateur de sécurité	Administrateur d'entreprise	Centre d'assistance senior	Centre d'assistance junior
Créer et modifier les profils de notification par application	√	√		
Supprimer les profils de notification par application	√	√		
Afficher les profils de contrôle	√	√	√	√
Créer et modifier les profils de contrôle	√	√		
Supprimer les profils de contrôle	√	√		
Afficher les profils de protection de l'application Microsoft Intune	√	√	√	√
Créer et modifier les profils de protection de l'application Microsoft Intune	√	√		
Supprimer les profils de protection de l'application Microsoft Intune	√	√		
Afficher les profils de disposition de l'écran d'accueil	√	√	√	√
Créer et modifier des profils de disposition de l'écran d'accueil	√	√		
Supprimer des profils de disposition de l'écran d'accueil	√	√		
Afficher la stratégie d'authentification Enterpı Identity	√	√		

Autorisation	Administrateur de sécurité	Administrateur d'entreprise	Centre d'assistance senior	Centre d'assistance junior
Créer et modifier la stratégie d'authentification Enterprise Identity	√	√		
Supprimer la stratégie d'authentification Enterpı Identity	√	√		
Attribuer la stratégie d'authentification Enterprise Identity à des utilisateurs et groupes	√	√		

Applications

Autorisation	Administrateur de sécurité	Administrateur d'entreprise	Centre d'assistance senior	Centre d'assistance junior
Afficher les applications et groupes d'applications	√	√	√	√
Créer et modifier des applications et groupes d'application	√	√		
Supprimer des applications et groupes d'applications	√	√		
Exporter les données d'application	√	√	√	√
Attribuer des applications et groupes d'applications aux utilisateurs	√	√	√	√
Attribuer des applications et groupes d'applications aux groupes d'utilisateurs	√	√	√	√

Autorisation	Administrateur de sécurité	Administrateur d'entreprise	Centre d'assistance senior	Centre d'assistance junior
Attribuer des applications et groupes d'applications aux groupes de terminaux	√	√	√	√
Attribuer des applications et des groupes d'applications aux groupes de terminaux partagés	√	√		
Modifier les paramètres de note et d'évaluation des applications	√	√		
Supprimer les évaluations et commentaires relatifs aux applications	√	√	√	√
Afficher le classement d'installation de l'application	√	√	√	√
Modifier le classement d'installation de l'application	√	√		
Afficher les licences des applications	√	√	√	√
Créer les licences des applications	√	√		
Modifier les licences des applications	√	√		
Supprimer les licences des applications	√	√		
Attribuer des licences d'application à des applications ou groupes d'applications	√	√	√	√

Applications limitées

Autorisation	Administrateur de sécurité	Administrateur d'entreprise	Centre d'assistance senior	Centre d'assistance junior
Afficher les applications limitées	√	√	√	√
Créer des applications limitées	√	√		
Supprimer des applications limitées	√	√		

Applications personnelles

Autorisation	Administrateur de sécurité	Administrateur d'entreprise	Centre d'assistance senior	Centre d'assistance junior
Afficher les applications personnelles	√	√		

Paramètres

Autorisation	Administrateur de sécurité	Administrateur d'entreprise	Centre d'assistance senior	Centre d'assistance junior
Afficher les paramètres généraux	√	√	√	√
Modifier les paramètres d'activation par défaut	√	√		
Créer et modifier des modèles d’e-mails	√	√		
Supprimer des modèles d’e-mails	√	√		
Modifier les paramètres de la console	√	√		

Autorisation	Administrateur de sécurité	Administrateur d'entreprise	Centre d'assistance senior	Centre d'assistance junior
Modifier la langue des e-mails automatiques	√	√		
Modifier les paramètres de la console en libre-service	√	√		
Créer les paramètres de sauvegarde et restauration de l'espace Travail	√	√		
Supprimer les paramètres de sauvegarde et restauration de l'espace Travail	√	√		
Modifier les variables par défaut	√	√		
Modifier les notifications de connexion	√	√		
Modifier les variables personnalisées	√	√		
Modifier des notes d'entreprise	√	√		
Modifier des domaines de messagerie	√	√		
Modifier les paramètres du service de localisation	√	√		
Modifier les paramètres de la console personnalisée	√	√		
Modifier les paramètres d'expiration de la commande de suppression	√	√		

Autorisation	Administrateur de sécurité	Administrateur d'entreprise	Centre d'assistance senior	Centre d'assistance junior
Modifier les paramètres d'attestation	√	√		
Modifier les paramètres de certificat	√	√		
Créer et modifier les notifications d'événement	√	√		
Supprimer les notifications d'événement	√	√		
Modifier les messages de support de terminal	√	√		
Afficher la gestion des applications	√	√	√	√
Modifier BlackBerry World for Work	√	√		
Modifier le stockage des applications internes	√	√		
Modifier les applications Windows Phone 8	√	√		
Modifier Work Apps pour iOS	√	√		
Modifier les applications Windows 10	√	√		
Modifier les paramètres de note et d'évaluation des applications par défaut	√	√		
Afficher les paramètres d'intégration externe	√	√	√	√

Autorisation	Administrateur de sécurité	Administrateur d'entreprise	Centre d'assistance senior	Centre d'assistance junior
Modifier les paramètres de notification Push Apple	√	√		
Modifier les paramètres de serveur SMTP	√	√		
Modifier les paramètres Apple DEP	√	√		
Modifier les paramètres du serveur BlackBerry 2FA	√	√		
Afficher les jetons de mot de passe à usage unique	√	√	√	√
Créer et modifier les jetons de mot de passe à usage unique	√	√		
Modifier les paramètres de l'annuaire d'entreprise	√	√		
Modifier les paramètres Microsoft Intune	√	√		
Modifier les paramètres de contrôle d'accès Microsoft Exchange	√	√		
Modifier les paramètres de profil professionnel Android	√	√		
Modifier les paramètres d'autorité de certification	√	√		
Modifier les paramètres d'inscription par lot Samsung KNOX	√	√		

Autorisation	Administrateur de sécurité	Administrateur d'entreprise	Centre d'assistance senior	Centre d'assistance junior
Afficher les certificats approuvés	√	√		
Ajouter des certificats approuvés	√	√		
Supprimer les certificats approuvés	√	√		
Afficher les serveurs BlackBerry Connectivity Node	√	√		
Créer et modifier des serveurs BlackBerry Connectivity Node	√	√		
Supprimer des serveurs BlackBerry Connectivity Node	√	√		
Afficher les paramètres BlackBerry Secure Gateway	√	√		
Modifier les paramètres BlackBerry Secure Gateway	√	√		
Afficher les utilisateurs administrateurs et les rôles	√	√	√	√
Afficher le résumé des licences	√	√	√	√
Modifier les paramètres de licences	√	√		
Afficher les paramètres de migration	√	√		
Modifier les paramètres de migration	√	√		

Autorisation	Administrateur de sécurité	Administrateur d'entreprise	Centre d'assistance senior	Centre d'assistance junior
Afficher les paramètres d'infrastructure	√	√	√	
Modifier les paramètres de journalisation	√	√		
Modifier les paramètres proxy côté serveur	√	√		
Afficher les serveurs	√	√		
Modifier des serveurs	√	√		
Supprimer des serveurs	√	√		
Gérer les serveurs	√	√		
Afficher les paramètres d'audit	√	√		
Modifier les paramètres d'audit et purger les données	√	√		
Afficher les paramètres BlackBerry Secure Connect Plus	√	√		
Modifier les paramètres BlackBerry Secure Connect Plus	√	√		
Afficher les certificats de serveur	√	√		
Mettre à jour les certificats de serveur	√	√		
Afficher les paramètres BlackBerry Control	√	√	√	√

Autorisation	Administrateur de sécurité	Administrateur d'entreprise	Centre d'assistance senior	Centre d'assistance junior
Modifier les paramètres BlackBerry Control	√	√		
Afficher les paramètres du serveur proxy BlackBerry Dynamics NOC	√	√	√	√
Modifier les paramètres du serveur proxy BlackBerry Dynamics NOC	√	√	√	√
Modifier les paramètres SNMP	√	√		
Afficher les paramètres Collaboration Service	√	√	√	√
Modifier les paramètres Collaboration Service	√	√		
Afficher les paramètres BlackBerry Dynamics	√	√	√	√
Afficher les services d'application BlackBerry Dynamics	√	√		
Modifier les services d'application BlackBerry Dynamics	√			
Créer des services d'application BlackBerry Dynamics	√			
Supprimer des services d'application BlackBerry Dynamics	√			
Afficher les propriétés du serveur BlackBerry Dynamics	√	√		

Autorisation	Administrateur de sécurité	Administrateur d'entreprise	Centre d'assistance senior	Centre d'assistance junior
Modifier les propriétés du serveur BlackBerry Dynamics	√			
Afficher les paramètres BlackBerry Dynamics Direct Connect	√	√		
Modifier les paramètres BlackBerry Dynamics Direct Connect	√			
Afficher les tâches du serveur BlackBerry Dynamics	√	√		
Supprimer les tâches du serveur BlackBerry Dynamics	√			
Afficher les paramètres de cluster du serveur BlackBerry Dynamics	√	√		
Modifier les paramètres de cluster du serveur BlackBerry Dynamics	√			
Afficher les rapports BlackBerry Dynamics	√	√	√	
Afficher les paramètres de communication BlackBer Dynamics	√	√	√	
Modifier les paramètres de communication BlackBerry Dynamics	√			

Autorisation	Administrateur de sécurité	Administrateur d'entreprise	Centre d'assistance senior	Centre d'assistance junior
Afficher les paramètres Enterprise Identity	√	√		
Afficher les paramètres d'entreprise Enterprise Identity	√	√		
Modifier les paramètres Enterprise Identity	√	√		
Afficher les paramètres de service Enterprise Identity	√	√		
Modifier les paramètres de service Enterprise Identity	√	√		

Planche de bord

Autorisation	Administrateur de sécurité	Administrateur d'entreprise	Centre d'assistance senior	Centre d'assistance junior
Afficher le tableau de bord	√	√	√	√

Audit

Autorisation	Administrateur de sécurité	Administrateur d'entreprise	Centre d'assistance senior	Centre d'assistance junior
Afficher le journal d'audit du système	√	√		
Afficher les journaux de performances du terminal	√	√		

Autorisations BlackBerry OS

Si vous procédez à la mise à niveau de BES5, les autorisations supplémentaires suivantes sont disponibles :

- Afficher les stratégies informatiques BlackBerry OS
- Créer et modifier les stratégies informatiques BlackBerry OS
- Supprimer des stratégies informatiques BlackBerry OS
- Afficher les tâches
- Modifier des tâches
- Afficher les paramètres de distribution par défaut des tâches
- Modifier les paramètres de distribution par défaut des tâches
- Gérer les tâches
- Modifier l'état des tâches

Créer un rôle personnalisé

Si les rôles préconfigurés disponibles dans BlackBerry UEM ne répondent pas aux besoins de votre entreprise, vous pouvez créer des rôles personnalisés pour les administrateurs. Vous pouvez également personnaliser les rôles pour limiter les tâches administratives à une liste définie de groupes d'utilisateurs. Par exemple, vous pouvez créer un rôle pour les nouveaux administrateurs qui limite leurs autorisations à un groupe d'utilisateurs à des fins de formation uniquement.

Avant de commencer : Vous devez être Administrateur de sécurité pour créer un rôle personnalisé.

1. Sur la barre de menus, cliquez sur **Paramètres**.
2. Dans le volet de gauche, développez **Administrateurs**.
3. Cliquez sur **Rôles**.
4. Cliquez sur .
5. Saisissez le nom et la description du rôle.
6. Pour copier les autorisations d'un autre rôle, cliquez sur un rôle de la liste déroulante **Autorisations copiées à partir du rôle**.
7. Effectuez l'une des tâches suivantes :

Tâche	Étapes
Autoriser les administrateurs de ce rôle à rechercher tous les annuaires d'entreprise	a. Sélectionnez l'option **Tous les répertoires d'entreprise**.
Autoriser les administrateurs de ce rôle à rechercher les annuaires d'entreprise sélectionnés	a. Sélectionnez l'option **Répertoires d'entreprise sélectionnés uniquement**. b. Cliquez sur **Sélectionner des répertoires**. c. Sélectionnez un ou plusieurs annuaires et cliquez sur . d. Cliquez sur **Enregistrer**.

8. Effectuez l'une des tâches suivantes :

Tâche	Étapes
Autoriser les administrateurs de ce rôle à gérer tous les utilisateurs et groupes	a. Sélectionnez l'option **Tous les groupes et utilisateurs**.

Tâche	Étapes
Autoriser les administrateurs de ce rôle à gérer les groupes sélectionnés	**a.** Sélectionnez l'option **Groupes sélectionnés uniquement**. **b.** Cliquez sur **Sélectionner des groupes**. **c.** Sélectionnez un ou plusieurs groupes, puis cliquez sur ➔. **d.** Cliquez sur **Enregistrer**.

9. Configurez les autorisations des administrateurs de ce rôle.
10. Cliquez sur **Enregistrer**.

À la fin : classez les rôles.

Tâches connexes

Classer les rôles

Afficher un rôle

Vous pouvez afficher les informations de rôle suivantes :

- Répertoires d'entreprises dans lesquels les administrateurs du rôle peuvent rechercher.
- Groupes d'utilisateurs que les administrateurs du rôle peuvent gérer.
- Autorisations pour les administrateurs du rôle.

Avant de commencer : Vous devez être Administrateur de sécurité pour afficher un rôle.

1. Sur la barre de menus, cliquez sur **Paramètres**.
2. Dans le volet de gauche, développez **Administrateurs**.
3. Cliquez sur **Rôles**.
4. Cliquez sur le nom du rôle que vous souhaitez afficher.

Modifier les paramètres de rôle

Vous pouvez modifier les paramètres de tous les rôles, à l'exception du rôle Administrateur de sécurité.

Avant de commencer : vous devez être Administrateur de sécurité pour modifier les paramètres de rôle.

1. Sur la barre de menus, cliquez sur **Paramètres**.
2. Dans le volet de gauche, développez **Administrateurs**.
3. Cliquez sur **Rôles**.
4. Cliquez sur le nom du rôle que vous souhaitez modifier.
5. Cliquez sur ✎.
6. Pour modifier l'accès aux répertoires, effectuez l'une des tâches suivantes :

Tâche	Étapes
Autoriser les administrateurs de ce rôle à rechercher tous les annuaires d'entreprise	**a.** Sélectionnez l'option **Tous les répertoires d'entreprise**.

Tâche	Étapes
Autoriser les administrateurs de ce rôle à rechercher les annuaires d'entreprise sélectionnés	a. Sélectionnez l'option **Répertoires d'entreprise sélectionnés uniquement**. b. Cliquez sur **Sélectionner des répertoires**. c. Sélectionnez un ou plusieurs annuaires et cliquez sur ➔. d. Cliquez sur **Enregistrer**.

7. Pour modifier la gestion du groupe, effectuez l'une des tâches suivantes :

Tâche	Étapes
Autoriser les administrateurs de ce rôle à gérer tous les utilisateurs et groupes	a. Sélectionnez l'option **Tous les groupes et utilisateurs**.
Autoriser les administrateurs de ce rôle à gérer les groupes sélectionnés	a. Sélectionnez l'option **Groupes sélectionnés uniquement**. b. Cliquez sur **Sélectionner des groupes**. c. Sélectionnez un ou plusieurs groupes, puis cliquez sur ➔. d. Cliquez sur **Enregistrer**.

8. Modifiez les autorisations des administrateurs de ce rôle.
9. Cliquez sur **Enregistrer**.

À la fin : si nécessaire, modifiez le classement du rôle.

Tâches connexes

Classer les rôles

Supprimer un rôle

Vous pouvez supprimer tous les rôles, à l'exception du rôle Administrateur de sécurité.

Avant de commencer :

- Vous devez être Administrateur de sécurité pour supprimer un rôle.
- Supprimez le rôle de tous les comptes d'utilisateur et groupes d'utilisateurs auxquels il est affecté.

1. Sur la barre de menus, cliquez sur **Paramètres**.
2. Dans le volet de gauche, développez **Administrateurs**.
3. Cliquez sur **Rôles**.
4. Cliquez sur le nom du rôle que vous souhaitez supprimer.
5. Cliquez sur 🗑.

Concepts connexes

Comment BlackBerry UEM choisit le rôle à attribuer

Comment BlackBerry UEM choisit le rôle à attribuer

Un seul rôle est attribué à un administrateur. BlackBerry UEM utilise les règles suivantes pour déterminer le rôle à attribuer à un administrateur :

- Un rôle directement attribué à un compte d'utilisateur est prioritaire sur un rôle attribué indirectement par un groupe d'utilisateurs.
- Si un administrateur est membre de plusieurs groupes d'utilisateurs possédant des rôles différents, BlackBerry UEM attribue le rôle avec le rang le plus élevé.

Classer les rôles

Le classement permet de déterminer quel rôle BlackBerry UEM attribue à un administrateur lorsqu'il est membre de plusieurs groupes d'utilisateurs qui possèdent des rôles différents.

Avant de commencer : vous devez être Administrateur de sécurité pour classer les rôles.

1. Sur la barre de menus, cliquez sur **Paramètres**.
2. Dans le volet de gauche, développez **Administrateurs**.
3. Cliquez sur **Rôles**.
4. Utilisez les flèches pour déplacer les rôles vers le haut ou le bas du classement.
5. Cliquez sur **Enregistrer**.

Créer un administrateur

Vous pouvez créer un administrateur en ajoutant un rôle à un compte d'utilisateur ou à un groupe d'utilisateurs. Le groupe d'utilisateurs peut être un groupe lié par annuaire ou un groupe local. Vous pouvez ajouter un rôle à un utilisateur et un rôle à chaque groupe auquel il appartient, et BlackBerry UEM affecte uniquement l'un des rôles de l'utilisateur.

Avant de commencer :

- Vous devez être Administrateur de sécurité pour créer un administrateur.
- Créez un compte d'utilisateur auquel est associée une adresse électronique.
- Si nécessaire, créez un groupe d'utilisateurs.
- Si nécessaire, créez un rôle personnalisé.

1. Sur la barre de menus, cliquez sur **Paramètres**.
2. Dans le volet de gauche, développez **Administrateurs**.
3. Effectuez l'une des tâches suivantes :

Tâche	Étapes
Ajouter un rôle à un compte d'utilisateur	**a.** Cliquez sur **Utilisateurs**. **b.** Cliquez sur . **c.** Si nécessaire, recherchez un compte d'utilisateur. **d.** Cliquez sur le nom du compte d'utilisateur. **e.** Dans la liste déroulante **Rôle**, cliquez sur le rôle que vous souhaitez ajouter. **f.** Cliquez sur **Enregistrer**.

Tâche	Étapes
Ajouter le rôle à un groupe d'utilisateurs	**a.** Cliquez sur **Groupes**. **b.** Cliquez sur . **c.** Si nécessaire, recherchez un groupe d'utilisateurs. **d.** Cliquez sur le nom du groupe d'utilisateurs. **e.** Dans la liste déroulante **Rôle**, cliquez sur le rôle que vous souhaitez ajouter. **f.** Cliquez sur **Enregistrer**.

BlackBerry UEM envoie aux administrateurs un e-mail avec le nom d'utilisateur et un lien vers la console de gestion. BlackBerry UEM envoie également aux administrateurs un e-mail distinct contenant leur mot de passe pour accéder à la console de gestion. Si un administrateur ne dispose pas de mot de passe de compte, BlackBerry UEM génère un mot de passe temporaire et l'envoie à l'administrateur.

À la fin : si nécessaire, ajoutez des comptes d'utilisateur à un groupe d'utilisateurs auquel un rôle a été attribué. Seuls les Administrateurs de sécurité peuvent ajouter ou supprimer un groupe d'utilisateurs auquel un rôle a été attribué.

Concepts connexes

Comment BlackBerry UEM choisit le rôle à attribuer
Création et gestion de groupes d'utilisateurs
Création et gestion de comptes d'utilisateur

Tâches connexes

Créer un rôle personnalisé

Modifier l'appartenance de rôle pour les administrateurs

Vous pouvez modifier le rôle attribué directement à d'autres administrateurs. Vous ne pouvez pas modifier votre propre rôle.

Avant de commencer : Vous devez être Administrateur de sécurité pour modifier l'appartenance au rôle pour les administrateurs.

1. Sur la barre de menus, cliquez sur **Paramètres**.
2. Dans le volet de gauche, développez **Administrateurs**.
3. Effectuez l'une des tâches suivantes :

Tâche	Étapes
Modifier le rôle affecté à un compte d'utilisateur	**a.** Cliquez sur **Utilisateurs**. **b.** Si nécessaire, recherchez un compte d'utilisateur. **c.** Cliquez sur le nom du compte d'utilisateur. **d.** Dans la liste déroulante **Rôle**, cliquez sur le rôle que vous souhaitez attribuer. **e.** Cliquez sur **Enregistrer**.

Tâche	Étapes
Modifier le rôle affecté à un groupe d'utilisateurs	**a.** Cliquez sur **Groupes**. **b.** Si nécessaire, recherchez un groupe d'utilisateurs. **c.** Cliquez sur le nom du groupe d'utilisateurs. **d.** Dans la liste déroulante **Rôle**, cliquez sur le rôle que vous souhaitez attribuer. **e.** Cliquez sur **Enregistrer**.

Concepts connexes

Comment BlackBerry UEM choisit le rôle à attribuer

Définition de la complexité minimale du mot de passe des administrateurs locaux

Vous pouvez définir les exigences minimales en matière de longueur et complexité du mot de passe, pour les comptes d'administrateur local. Ce paramètre prend effet lorsque les administrateurs changent le mot de passe de leur compte.

1. Dans la barre de menus, cliquez sur **Paramètres** > **Paramètres généraux** > **Console**.
2. Dans le champ **Nombre minimal de caractères**, entrez le nombre minimal de caractères pour le mot de passe d'une console.
3. Dans le champ **Complexité minimale du mot de passe**, sélectionnez la complexité minimale pour le mot de passe d'une console :
   - **Aucune restriction**
   - **1 lettre, 1 chiffre**
   - **1 lettre, 1 chiffre, 1 caractère spécial**
   - **1 lettre majuscule et 1 lettre minuscule, 1 chiffre, 1 caractère spécial**
4. Cliquez sur **Enregistrer**.

Définir les paramètres d'expiration de session

1. Dans la barre de menus, cliquez sur **Paramètres > Paramètres généraux > Console**.
2. Dans le champ **Délai d'expiration de la session**, saisissez, en minutes, la durée avant expiration de la session.
3. Dans le champ **Avertissement du délai d'expiration de la session**, saisissez, en minutes, la durée devant s'écouler avant que vous ne soyez déconnecté, à compter de l'affichage du message vous avertissant de l'expiration de la session. Par exemple, si vous définissez ce champ à deux minutes, le message d'avertissement s'affichera deux minutes avant que vous ne soyez déconnecté de votre session.
4. Cliquez sur **Enregistrer**.

Supprimer un administrateur

Vous pouvez supprimer un administrateur en supprimant un rôle attribué directement à un compte d'utilisateur ou à un groupe d'utilisateurs. Lorsque vous supprimez un rôle d'un groupe d'utilisateurs, le rôle est supprimé pour chaque utilisateur appartenant au groupe. Si aucun autre rôle n'est attribué, l'utilisateur n'est plus administrateur. Les comptes d'utilisateur et groupes d'utilisateurs demeurent dans la console de gestion et les terminaux ne sont pas affectés.

Remarque : Au moins un administrateur doit être Administrateur de sécurité.

Avant de commencer : Vous devez être Administrateur de sécurité pour pouvoir supprimer un administrateur.

1. Sur la barre de menus, cliquez sur **Paramètres**.
2. Dans le volet de gauche, développez **Administrateurs**.
3. Effectuez l'une des tâches suivantes :

Tâche	Étapes
Supprimer un rôle d'un compte d'utilisateur	**a.** Cliquez sur **Utilisateurs > Tous les utilisateurs**. **b.** Sélectionnez le compte d'utilisateur duquel vous souhaitez supprimer le rôle. **c.** Cliquez sur 🗑. **d.** Cliquez sur **Supprimer**.
Supprimer un rôle d'un groupe d'utilisateurs	**a.** Cliquez sur **Groupes**. **b.** Sélectionnez le groupe d'utilisateurs duquel vous souhaitez supprimer le rôle. **c.** Cliquez sur 🗑. **d.** Cliquez sur **Supprimer**.

Utilisation de profils, variables et modèles d'e-mail

Les profils, les variables et les modèles d'e-mail vous aident à gérer les comptes d'utilisateur et à communiquer efficacement avec les utilisateurs.

Les profils permettent à votre organisation de configurer efficacement plusieurs terminaux. Ils vous permettent de stocker tous les paramètres d'une configuration spécifique à un même emplacement et de rapidement transférer les paramètres aux terminaux concernés.

Les variables correspondent aux attributs de compte standard (nom d'utilisateur, par exemple) et d'autres attributs prédéfinis (adresse du serveur utilisée pour l'activation du terminal). Vous pouvez utiliser les variables dans les profils, les notifications de conformité, les e-mails d'activation et les notifications d'évènement.

Les modèles d'e-mail vous permettent d'adapter et de personnaliser les e-mails que BlackBerry UEM envoie aux utilisateurs et administrateurs.

Profils

Un profil contient des informations de configuration pour les terminaux et chaque type de profil prend en charge une configuration particulière, comme des certificats, paramètres de connexion professionnelle ou paramètres appliquant certaines normes pour les terminaux. Vous pouvez spécifier les paramètres des terminaux BlackBerry 10,iOS,macOS,Android et Windows dans un même profil, puis distribuer les informations de configuration aux terminaux en attribuant le profil à des comptes d'utilisateur, groupes d'utilisateurs ou groupes de terminaux.

Attribution de profils

Vous pouvez attribuer des profils à des comptes d'utilisateur, groupes d'utilisateurs et groupes de terminaux. Certains types de profil peuvent utiliser le classement pour déterminer le profil envoyé à un terminal.

- Type de profil classé : vous pouvez attribuer un profil à un utilisateur et un profil à chaque groupe auquel il appartient, et BlackBerry UEM envoie un seul des profils attribués au terminal de l'utilisateur.
- Type de profil non classé : vous pouvez attribuer plusieurs profils à un utilisateur et profils multiples à chaque groupe auquel il appartient, et BlackBerry UEM envoie tous les profils attribués au terminal de l'utilisateur.

Remarque : vous ne pouvez pas attribuer de profil d'activation à un groupe de terminaux.

Pour une liste complète des profils, reportez-vous à Référence de profils.

Concepts connexes

Comment BlackBerry UEM choisit les profils à attribuer

Tâches connexes

Attribuer un profil ou une stratégie informatique à un groupe d'utilisateurs
Attribuer un profil ou une stratégie informatique à un compte d'utilisateur
Classer les profils

Comment BlackBerry UEM choisit les profils à attribuer

Pour les types de profils classés, BlackBerry UEMenvoie un seul profil de chaque type à un terminal et utilise des règles prédéfinies pour déterminer le profil à attribuer à un utilisateur et les terminaux que l'utilisateur active.

Attribué à	Règles
Compte d'utilisateur (afficher l'onglet Synthèse)	1. Un profil directement attribué à un compte d'utilisateur est prioritaire sur un profil de même type attribué indirectement par groupe d'utilisateurs. 2. Si un utilisateur est membre de plusieurs groupes d'utilisateurs dotés de différents profils de même type, BlackBerry UEM attribue le profil avec le rang le plus élevé. 3. Le cas échéant, le profil par défaut préconfiguré est attribué si aucun profil n'est attribué à un compte d'utilisateur directement ou par appartenance aux groupes d'utilisateurs. **Remarque :** BlackBerry UEM inclut un profil d'activation par défaut, un profil de conformité par défaut, un profil de connectivité d'entreprise par défaut, un profil Enterprise Management Agent par défaut dotés de paramètres préconfigurés pour chaque type de terminal.
Terminal (afficher l'onglet Terminal)	Par défaut, un terminal hérite du profil attribué par BlackBerry UEM à l'utilisateur qui active le terminal. Si un terminal appartient à un groupe de terminaux, les règles suivantes s'appliquent : 1. Un profil attribué à un groupe de terminaux est prioritaire sur le profil de même type attribué par BlackBerry UEM à un compte d'utilisateur. 2. Si un terminal est membre de plusieurs groupes de terminaux dotés de différents profils de même type, BlackBerry UEM attribue le profil avec le rang le plus élevé.

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

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

Concepts connexes

Attribution de profils

Tâches connexes

Attribuer un profil ou une stratégie informatique à un groupe d'utilisateurs
Attribuer un profil ou une stratégie informatique à un compte d'utilisateur
Classer les profils

Copier un profil

Vous pouvez copier des profils existants afin de créer rapidement des profils similaires pour différents groupes au sein de votre entreprise.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur un type de profil.
3. Cliquez sur le nom du profil que vous souhaitez copier.
4. Cliquez sur .
5. Saisissez le nom et la description du nouveau profil.
6. Apportez les modifications dans l'onglet correspondant à chaque type de terminal.
7. Cliquez sur **Enregistrer**.

À la fin : Si nécessaire, classez les profils.

Afficher un profil

Vous pouvez afficher les informations de profil suivantes :

- Paramètres communs à tous les types de terminaux et spécifiques à chaque type de terminal
- Liste et nombre de comptes d'utilisateur auxquels est attribué le profil (directement et indirectement)
- Liste et nombre de groupes d'utilisateurs auxquels est attribué le profil (directement)

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Développez un type de profil.
3. Cliquez sur le nom du profil que vous souhaitez afficher.

Modifier les paramètres de profil

Si vous mettez à jour un profil d'activation, les nouveaux paramètres du profil s'appliquent uniquement aux terminaux supplémentaires activés par un utilisateur. Les terminaux activés n'utilisent pas les nouveaux paramètres du profil tant que l'utilisateur ne les a pas réactivés.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur un type de profil.
3. Cliquez sur le nom du profil que vous souhaitez modifier.
4. Cliquez sur .
5. Modifiez les paramètres communs.
6. Apportez les modifications dans l'onglet correspondant à chaque type de terminal.
7. Cliquez sur **Enregistrer**.

À la fin : Si nécessaire, classez les profils.

Supprimer un profil de comptes d'utilisateur ou de groupes d'utilisateurs

Si un profil est directement attribué à des comptes d'utilisateur ou à des groupes d'utilisateurs, vous pouvez le supprimer des utilisateurs ou des groupes. Si un profil est indirectement attribué par un groupe d'utilisateurs, vous pouvez supprimer le profil du groupe ou supprimer les comptes d'utilisateur du groupe. Lorsque vous supprimez un profil des groupes d'utilisateurs, le profil est supprimé de chaque utilisateur appartenant aux groupes sélectionnés.

Remarque : Le profil d'activation par défaut, le profil de conformité par défaut, le profil de connectivité d'entreprise par défaut et le profil Enterprise Management Agent par défaut peuvent uniquement être supprimés d'un compte d'utilisateur si vous les avez directement attribués à l'utilisateur.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Sélectionnez un type de profil.
3. Cliquez sur le nom du profil que vous souhaitez supprimer des comptes d'utilisateur ou des groupes d'utilisateurs.
4. Effectuez l'une des tâches suivantes :

Tâche	Étapes
Supprimer un profil de comptes d'utilisateur	**a.** Cliquez sur l'onglet **Attribué aux utilisateurs**. **b.** Si nécessaire, recherchez les comptes d'utilisateur. **c.** Sélectionnez les comptes d'utilisateur desquels vous souhaitez supprimer le profil. **d.** Cliquez sur .
Supprimer un profil de groupes d'utilisateurs	**a.** Cliquez sur l'onglet **Attribué aux groupes**. **b.** Si nécessaire, recherchez les groupes d'utilisateurs. **c.** Sélectionnez les groupes d'utilisateurs desquels vous souhaitez supprimer le profil. **d.** Cliquez sur .

Concepts connexes

Comment BlackBerry UEM choisit les profils à attribuer

Supprimer un profil

Lorsque vous supprimez un profil, BlackBerry UEM supprime le profil des utilisateurs et des terminaux auquel il est attribué. Pour supprimer un profil associé à d'autres profils, vous devez d'abord supprimer toutes les associations existantes. Par exemple, avant de pouvoir supprimer un profil proxy associé à un profil VPN et un profil Wi-Fi, vous devez modifier la valeur du profil proxy associé dans le profil VPN et le profil Wi-Fi.

Remarque : Vous ne pouvez pas supprimer le profil d'activation par défaut, le profil de conformité par défaut, le profil de la connectivité d'entreprise par défaut, ou le profil Enterprise Management Agent par défaut.

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

Concepts connexes

Comment BlackBerry UEM choisit les profils à attribuer

Classer les profils

Le classement est utilisé pour déterminer le profil envoyé par BlackBerry UEM à un terminal dans les scénarios suivants :

- Un utilisateur est membre de plusieurs groupes d'utilisateurs dotés de profils de même type.

- Un terminal est membre de plusieurs groupes de terminaux dotés de profils de même type.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Sélectionnez un type de profil.
3. Cliquez sur ⇅.
4. Utilisez les flèches pour déplacer les profils vers le haut ou le bas du classement.
5. Cliquez sur **Enregistrer**.

Concepts connexes

Attribution de profils
Comment BlackBerry UEM choisit les profils à attribuer

Référence de profils

Le tableau suivant répertorie tous les profils BlackBerry UEM :

Nom du profil	Description	Types de terminaux pris en charge	Type : classé ou non classé[1]	Configurer
Stratégie				
Activation	Spécifie les paramètres d'activation des terminaux pour les utilisateurs, comme le type d'activation, le nombre et les types de terminaux.	• Tous les terminaux	Classé	Créer un profil d'activation
BlackBerry Dynamics	Autorise les terminaux à accéder aux applications BlackBerry Dynamics, comme BlackBerry Work, BlackBerry Access et BlackBerry Connect.	• iOS • macOS • Android • Windows	Classé	Créer un profil BlackBerry Dynamics
Mode de verrouillage des applications	Spécifiez une application unique à exécuter sur les terminaux.	• Terminaux iOS superv • Terminaux Samsung KNOX activés avec MDM • Terminaux Windows 10 Education et Windows 10 Enterprise	Classé	Créer un profil du mode de verrouillage

Nom du profil	Description	Types de terminaux pris en charge	Type : classé ou non classé[1]	Configurer
Agent de gestion d'entreprise	Indique lorsque des terminaux se connectent à BlackBerry UEM pour des mises à jour d'applications ou de configuration, lorsqu'une notification push n'est pas disponible.	• iOS • Android • BlackBerry 10 • Windows	Classé	Créer un profil Enterprise Management Agent
Conformité				
Conformité	Définit les conditions des terminaux non acceptables dans votre organisation, ainsi que les actions d'exécution. BlackBerry UEM inclut un profil de conformité par défaut.	• Tous les terminaux	Classé	Créer un profil de conformité
Conformité (BlackBerry Dynamics)	Il s'agit d'un profil en lecture seule qui affiche les paramètres de conformité importés de Good Control.	• iOS • macOS • Android • Windows	n/d	Gérer les profils de conformité BlackBerry Dynamics
Configuration logicielle minimale requise du terminal	Définit les versions logicielles à installer sur les terminaux BlackBerry 10.	• BlackBerry 10	Classé	Créer un profil de configuration logicielle minimale requise du terminal pour les terminaux BlackBerry 10
E-mail, calendrier et contacts				
E-mail	Spécifie la manière dont les terminaux se connectent à un serveur de messagerie professionnel et synchronisent les e-mails, les entrées de calendrier et les données de l'organiseur à l'aide d'Exchange ActiveSync ou IBM Notes Traveler.	• Tous les terminaux.	Classé	Créer un profil de messagerie

Nom du profil	Description	Types de terminaux pris en charge	Type : classé ou non classé[1]	Configurer
Messagerie IMAP/POP3	Spécifie la manière dont les terminaux se connectent à un serveur de messagerie IMAP ou POP3 et synchronisent les e-mails.	• iOS • Android • Windows • macOS	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	Créer un profil CalDAV
CardDAV	Spécifie les paramètres de serveur que les terminaux peuvent utiliser pour synchroniser les informations de contact.	• iOS • macOS	Non classé	Créer un profil CardDAV
Réseaux et connexions				
Wi-Fi	Spécifie la manière dont les terminaux se connectent à un réseau Wi-Fi professionnel.	• Tous les terminaux	Non classé	Créer un profil Wi-Fi
VPN	Spécifie la manière dont les terminaux se connectent à un VPN professionnel.	• Tous les terminaux	Non classé	Créer un profil VPN
Proxy	Spécifie la manière dont les terminaux utilisent un serveur proxy pour accéder à des services Web sur Internet ou un réseau professionnel.	• iOS • Android • BlackBerry 10 • macOS	Classé	Créer un profil proxy

Nom du profil	Description	Types de terminaux pris en charge	Type : classé ou non classé[1]	Configurer
Connectivité d'entreprise	Spécifie la manière dont les terminaux se connectent aux ressources de votre entreprise au travers de la connectivité d'entreprise. La connectivité d'entreprise est toujours activée pour les terminaux BlackBerry 10. Pour les terminaux BlackBerry 10 et Samsung KNOX Workspace, et pour les terminaux iOS supervisés avec commandes MDM, le profil de connectivité d'entreprise spécifie si les terminaux peuvent utiliser BlackBerry Secure Connect Plus. BlackBerry UEM inclut un profil de connectivité d'entreprise par défaut.	• BlackBerry 10 • iOS • Android	Classé	Créer un profil de connectivité d'entreprise
Connectivité BlackBerry Dynamics	Définit les connexions réseau, les domaines Internet, les plages d'adresses IP et les serveurs d'applications auxquels les terminaux peuvent se connecter lorsqu'ils utilisent des applications BlackBerry Dynamics.	• iOS • macOS • Android • Windows	Classé	Créer un profil de connectivité BlackBerry Dynamics
BlackBerry 2FA	Active l'authentification à deux facteurs pour les utilisateurs et spécifie la configuration de la préauthentification et les fonctionnalités de résolution autonome.	• iOS • Android • BlackBerry 10	Classé	Créer un profil BlackBerry 2FA
Utilisation du réseau	Vous permet de contrôler si les applications professionnelles sur les terminaux exécutant iOS 9 ou version ultérieure peuvent utiliser le réseau mobile ou l'itinérance des données.	• Terminaux iOS exécutant iOS 9 ou version ultérieure	Classé	Créer un profil d'utilisation du réseau
Filtre de contenu Web	Limite les sites Web qu'un utilisateur peut afficher sur des terminaux iOS supervisés.	• Terminaux iOS superv	Non classé	Créer un profil de filtre de contenu Web

Nom du profil	Description	Types de terminaux pris en charge	Type : classé ou non classé[1]	Configurer
Identification unique	Spécifie la manière dont les terminaux s'authentifient automatiquement auprès des domaines sécurisés après que les utilisateurs ont saisi leur nom d'utilisateur et leur mot de passe pour la première fois.	• iOS • BlackBerry 10	Classé	Créer un profil d'identification unique
Domaines gérés	Configure les terminaux iOS afin de notifier aux utilisateurs l'envoi d'e-mails en dehors des domaines approuvés et limite les applications pouvant afficher des documents téléchargés depuis des domaines internes.	• iOS	Non classé	Créer un profil de domaines gérés
AirPrint	Vous permet d'ajouter des imprimantes aux listes d'imprimantes AirPrint des utilisateurs.	• iOS	Non classé	Créer un profil AirPrint
AirPlay	Vous permet d'ajouter des terminaux aux listes de terminaux AirPlay des utilisateurs.	• iOS	Non classé	Créer un profil AirPlay
Protection				
Protection des données Windo\	Spécifie le paramètre Protection des données Windows dans Windows 10.	• Windows 10	Classé	Créer un profil de protection des données Windows
Protection des applications Microsoft Intune	Vous permet de gérer les applications protégées par Microsoft Intune.	• iOS • Android	Non classé	Créer un profil de protection d'application Microsoft Intune
Service de localisation	Vous permet de demander l'emplacement de terminaux et d'afficher les emplacements approximatifs sur une carte.	• iOS • Android • Windows	Classé	Créer un profil de service de localisation

Nom du profil	Description	Types de terminaux pris en charge	Type : classé ou non classé[1]	Configurer
	Vous permet de bloquer les notifications BlackBerry Work for Android et BlackBerry Work for iOS en dehors des jours et heures de travail que vous définissez.	• iOS • Android	Classé	Ne pas déranger
Personnalisée				
Terminal	Vous permet de configurer les informations qui s'affichent sur les terminaux.	• iOS • Android • BlackBerry 10 • Windows	Classé	Créer un profil de terminal
Charge utile personnalisée	Spécifie les informations de configuration personnalisée à l'aide du code de charge utile pour les terminaux.	• iOS	Non classé	Création d'un profil de charge utile personnalisée
Notification par application	Vous permet de configurer les paramètres de notification des applications système et des applications que vous gérez via BlackBerry UEM.	• Terminaux supervisés exécutant iOS 9.3 ou version ultérieure	Classé	Créer un profil de notification par application
Certificats				
Certificat d'AC	Spécifie un certificat d'AC que les terminaux peuvent utiliser pour établir une relation de confiance avec un réseau ou un serveur professionnel.	• Tous les terminaux	Non classé	Créer un profil de certificat d'autorité de certification partagé
Certificat partagé	Spécifie un certificat client que les terminaux peuvent utiliser pour authentifier les utilisateurs avec un réseau ou un serveur professionnel.	• iOS • Android • macOS	Non classé	Créer un profil de certificat partagé
Informations d'identification de l'utilisateur	Spécifie la connexion d'AC via laquelle les terminaux peuvent obtenir un certificat client d'authentification avec un réseau ou un serveur professionnel.	• iOS • Android • macOS • BlackBerry 10	Non classé	Utilisation de profils d'informations d'identification de l'utilisateur pour envoyer des certificats aux terminaux

Nom du profil	Description	Types de terminaux pris en charge	Type : classé ou non classé[1]	Configurer
SCEP	Spécifie le serveur SCEP via lequel les terminaux peuvent obtenir un certificat client d'authentification avec un réseau ou un serveur professionnel.	• Tous les terminaux	Non classé	Créer un profil SCEP
Récupération de certificat	Spécifie la manière dont les terminaux récupèrent les certificats auprès des serveurs LDAP.	• BlackBerry 10	Classé	Créer un profil de récupération de certificat
OCSP	Spécifie les serveurs OCSP que les terminaux BlackBerry 10 peuvent utiliser pour vérifier l'état des certificats.	• BlackBerry 10	Classé	Créer un profil OCSP
CRL	Spécifie les configurations CRL que BlackBerry UEM peut utiliser pour vérifier l'état des certificats.	• BlackBerry 10 • Terminaux BlackBerry optimisés par Android	Classé	Créer un profil CRL

[1] Pour les définitions de profils classés ou non classés, voir Attribution de profils.

Variables

BlackBerry UEM prend en charge les variables par défaut et les variables personnalisées. Les variables par défaut correspondent aux attributs de compte standard (nom d'utilisateur, par exemple) et d'autres attributs prédéfinis (adresse du serveur utilisée pour l'activation du terminal). Vous pouvez utiliser les variables personnalisées pour définir des attributs supplémentaires.

Vous pouvez utiliser les variables dans les profils, les notifications de conformité, les e-mails d'activation et les notifications d'évènement. Utilisez les variables pour faire référence à des valeurs plutôt que de spécifier des valeurs réelles. Lorsque le profil, la notification de conformité, l'e-mail d'activation ou la notification d'évènement sont envoyés aux terminaux, les variables sont remplacées par les valeurs qu'elles représentent.

Remarque : Les stratégies informatiques et les configurations d'application BlackBerry Dynamics ne prennent pas en charge les variables.

Utilisation de variables dans les profils

Les variables des profils vous aident à gérer efficacement les profils des utilisateurs de votre organisation. Les variables offrent plus de flexibilité aux profils et permettent de limiter le nombre de profils dont vous avez besoin pour chaque type de profil. Par exemple, vous pouvez créer un seul profil VPN pour plusieurs utilisateurs spécifiant la variable %UserName% au lieu de créer un profil VPN distinct pour chaque utilisateur spécifiant la valeur de nom d'utilisateur réelle.

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.

Dans les profils de conformité, vous pouvez utiliser des variables pour personnaliser les notifications de conformité envoyées par BlackBerry UEM aux utilisateurs.

Variables par défaut

Les variables par défaut suivantes sont disponibles dans BlackBerry UEM :

Nom de la variable	Description	Utilisation principale
%AccessKeyExpiry%	Date et heure de l'expiration d'une clé d'accès	E-mails d'activation
%AccessKeys%	Clés d'accès générées et utilisées automatiquement pour activer des applications BlackBerry Dynamics	E-mails d'activation
%ActivationPassword%	Mot de passe d'activation généré automatiquement ou défini pour un utilisateur	E-mails d'activation
%ActivationPasswordExpiry%	Date et heure d'expiration d'un mot de passe d'activation	E-mails d'activation
%ActivationQRCode%	QR Code pour l'activation des terminaux	E-mails d'activation
%ActivationURL%	Adresse Web du serveur qui reçoit les demandes d'activation	E-mails d'activation
%ActivationUserName%	Nom d'utilisateur pour les demandes d'activation Équivalent à %UserEmailAddress% (si disponible pour l'utilisateur) ou à SRP ID\ %UserName%	E-mails d'activation
%AdminPortalURL%	Adresse Web de la console de gestion de BlackBerry UEM	E-mails d'accès administrateur (non personnalisables)
%AllEventVariables%	Liste des évènements (telle que configurée dans une notification d'évènement) qui sont survenus dans BlackBerry UEM	Notifications d'événement
%ClientlessActivationURL%	Adresse Web du serveur qui reçoit les requêtes d'activation de terminaux exécutant Windows 10 et versions ultérieures	E-mails d'activation
%CommonName%	Attribut Nom commun (CN) extrait du nom distinctif	Configurations des applications

Nom de la variable	Description	Utilisation principale
%ComplianceApplicationList%	Liste des applications qui violent les règles de conformité (applications non attribuées installées, applications requises non installées ou applications limitées installées)	Notifications de conformité
%ComplianceEnforcementAction%	Action d'application effectuée par BlackBerry UEM en cas de non-conformité d'un terminal	Notifications de conformité
%ComplianceEnforcementAction%	Action d'application effectuée par BlackBerry UEM en cas de non-conformité d'un terminal, avec description de l'action d'application	Notifications de conformité
%ComplianceRuleViolated%	Règle de conformité violée par un terminal	Notifications de conformité
%DeviceIMEI%	Numéro IMEI d'un terminal	Profils
%DeviceModel%	Numéro de modèle d'un terminal	Notifications de conformité
%EmailAddressDomain%	Domaine d'une adresse électronique	Configurations des applications
%EmailAddressLocalPart%	Partie locale de l'adresse électronique (ex. :« nomutilisateur » dans nomutilisateur@exemple.com)	Configurations des applications
%ExchangeAlloweddeviceId%	ID du terminal de contrôle	Configurations des applications
%ICCIdentifier%	Identifiant de carte de circuits intégrée	Configurations des applications
%IMSIdentity%	Identité d'abonné mobile international	Configurations des applications
%IOSUDIdentifier%	Identifiant de terminal unique iOS	Configurations des applications
%MEIdentifier%	Identifiant d'équipement mobile	Configurations des applications
%OrganizationUnit%	Attribut Unité organisationnelle (OU) extrait du nom distinctif	Configurations des applications
%PhoneNumber%	Numéro de téléphone d'un terminal	Configurations des applications

Nom de la variable	Description	Utilisation principale
%RsaRootCaCertUrl%	Adresse Web du certificat racine de l'autorité de certification RSA	E-mails d'activation
%SamAccountName%	Attribut Microsoft sAMAccountName	Configurations des applications
serialNumber	Numéro de série d'un terminal	Paramètre objet dans les profils SCEP
%SSLCertName%	Nom commun du certificat de communication sécurisé	E-mails d'activation
%SSLCertSHA%	Empreinte du certificat de communication sécurisé	E-mails d'activation
%UserDisplayName%	Nom d'affichage d'un utilisateur	E-mails d'activation, profils
%UserDisplayName_RDNValue%	Nom d'affichage d'un utilisateur avec les caractères spéciaux échappés conformément à la spécification DN LDAP	Paramètre objet dans les profils SCEP
%UserDistinguishedName%	Nom distinctif de l'utilisateur d'annuaire avec les caractères spéciaux échappés conformément à la spécification DN LDAP Pour un utilisateur local, correspond à %UserName_RDNValue%	Paramètre objet dans les profils SCEP
%domaine de l'utilisateur%	Domaine Microsoft Active Directory auquel appartient un utilisateur d'annuaire	Profils
%UserDomain_RDNValue%	Domaine Microsoft Active Directory auquel appartient un utilisateur d'annuaire avec les caractères spéciaux échappés conformément à la spécification DN LDAP	Paramètre objet dans les profils SCEP
%adresse électronique utilisateur%	Adresse électronique d'un utilisateur	E-mails d'activation, profils
%UserEmailAddress_RDNValue%	Adresse électronique d'un utilisateur avec les caractères spéciaux échappés conformément à la spécification DN LDAP	Paramètre objet dans les profils SCEP
%UserFirstName%	Prénom d'un utilisateur	Configurations des applications
%UserLastName%	Nom de famille d'un utilisateur	Configurations des applications
%UserLocale%	Langue locale de l'utilisateur (ex. : fr-FR)	Configurations des applications

Nom de la variable	Description	Utilisation principale
%nom d'utilisateur%	Nom d'utilisateur d'un utilisateur	E-mails d'activation, profils
%UserName_RDNValue%	Nom d'utilisateur d'un utilisateur avec les caractères spéciaux échappés conformément à la spécification DN LDAP	Paramètre objet dans les profils SCEP
%UserPrincipalName%	Nom principal de l'utilisateur d'annuaire Pour un utilisateur local, correspond à %UserEmailAddress%	Profils
%UserPrincipalName_RDNValue%	Nom d'utilisateur de l'utilisateur d'annuaire avec les caractères spéciaux échappés conformément à la spécification DN LDAP Pour un utilisateur local, correspond à %UserEmailAddress_RDNValue%	Paramètre objet dans les profils SCEP
%UserSelfServicePortalURL%	Adresse Web de BlackBerry UEM Self-Service	E-mails d'activation
%WIFIMacAddress%	Adresse MAC Wi-Fi	Configurations des applications

Si vous configurez une disponibilité élevée pour les consoles de gestion du domaine BlackBerry UEM, il est recommandé de mettre à jour les variables %AdminPortalURL% et %UserSelfServicePortalURL%. Pour plus d'informations, consultez le contenu relatif à la configuration.

Variables personnalisées

Vous utilisez des libellés pour définir les attributs et les mots de passe représentés par les variables personnalisées. Par exemple, vous pouvez spécifier « Mot de passe VPN » comme libellé d'une variable %custom_pswd1%. Lorsque vous créez ou mettez à jour un compte d'utilisateur, les libellés sont utilisés comme noms de champ et vous spécifiez les valeurs appropriées pour les variables personnalisées utilisées par votre organisation. Tous les comptes d'utilisateur prennent en charge les variables personnalisées, y compris les comptes d'administrateur.

Les variables personnalisées prennent en charge les valeurs de texte et les valeurs de texte masquées. Pour des raisons de sécurité, vous devez utiliser des variables personnalisées prenant en charge les valeurs de texte masquées pour les mots de passe.

Les variables personnalisées suivantes sont disponibles dans BlackBerry UEM :

Nom de la variable	Description
%custom1%, %custom2%, %custom3%, %custom4%, %custom5%	Vous pouvez utiliser jusqu'à cinq variables différentes pour les attributs que vous définissez (valeurs de texte).

Nom de la variable	Description
%custom_pswd1%, %custom_pswd2%, %custom_pswd3%, %custom_pswd4%, %custom_pswd5%	Vous pouvez utiliser jusqu'à cinq variables différentes pour les mots de passe que vous définissez (valeurs de texte masquées).

Définir des variables personnalisées

Vous devez définir des variables personnalisées pour pouvoir les utiliser. Seules les variables personnalisées dotées d'un libellé s'affichent lorsque vous créez ou mettez à jour un compte d'utilisateur.

1. Sur la barre de menus, cliquez sur **Paramètres**.
2. Dans le volet de gauche, développez **Paramètres généraux.**
3. Cliquez sur **Variables personnalisées**.
4. Cochez la case **Afficher les variables personnalisées lors de l'ajout ou de la modification d'un utilisateur**.
5. Spécifiez un libellé pour chaque variable personnalisée que vous prévoyez d'utiliser. Les libellés sont utilisés comme noms de champ dans la section **Variables personnalisées** lorsque vous créez ou mettez à jour un compte d'utilisateur.
6. Cliquez sur **Enregistrer**.

Utilisation de variables personnalisées

Après avoir défini des variables personnalisées, vous devez spécifier les valeurs qui conviennent lorsque vous créez ou mettez à jour un compte d'utilisateur. Vous pouvez ensuite utiliser les variables personnalisées de la même manière que les variables par défaut. Vous spécifiez le nom de la variable lorsque vous créez des profils ou personnalisez les notifications de conformité et les e-mails d'activation.

Exemple : utilisation d'un même profil VPN pour plusieurs utilisateurs disposant de leurs propres mots de passe VPN

Dans l'exemple suivant, « Mot de passe VPN » correspond au libellé que vous spécifiez pour la variable %custom_pswd1% et celle-ci est utilisée en tant que nom de champ dans la section Variables personnalisées lorsque vous mettez à jour un compte d'utilisateur.

1. Sur la barre de menus, cliquez sur **Utilisateurs et terminaux > Terminaux gérés**.
2. Recherchez un compte d'utilisateur.
3. Dans les résultats de la recherche, cliquez sur le nom du compte d'utilisateur.
4. Cliquez sur  .
5. Développez **Variables personnalisées**.
6. Dans le champ **Mot de passe VPN**, saisissez le mot de passe VPN de l'utilisateur.
7. Cliquez sur **Enregistrer**.
8. Répétez les étapes 2 à 7 pour chaque utilisateur qui utilisera le profil VPN.
9. Lorsque vous créez le profil VPN, dans le champ **Mot de passe**, saisissez `%custom_pswd1%`.

Modèles d'e-mail

Les modèles d'e-mail vous permettent de personnaliser les e-mails que vous envoyez aux utilisateurs pour l'une des raisons suivantes :

- Activation du terminal : adressez un premier e-mail aux utilisateurs pour leur communiquer les instructions d'activation de leur terminal, puis un deuxième e-mail contenant leur mot de passe d'activation.
- Conformité : envoyez des e-mails de notification aux utilisateurs lorsque leur terminal n'est pas conforme.
- BlackBerry Dynamics apps activation - send emails to users containing access keys
- Notifications d'évènement : envoyez des e-mails pour informer les administrateurs à propos d'évènements particuliers dans BlackBerry UEM

Vous pouvez personnaliser les e-mails en utilisant des variables dans les modèles d'e-mail pour les éléments tels que le nom d'utilisateur, l'adresse électronique ou le mot de passe d'activation. Utilisez un éditeur HTML pour personnaliser l'apparence de vos e-mails à l'aide de différentes polices, couleurs et images. 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.

Lors de l'ajout d'un utilisateur à BlackBerry UEM, de la création d'un profil de conformité ou de la génération de mots de passe, vous pouvez sélectionner le modèle d'e-mail à utiliser. BlackBerry UEM envoie l'e-mail personnalisé à l'utilisateur en se basant sur le modèle que vous avez sélectionné.

Modèles d'e-mail par défaut

BlackBerry UEM comprend quelques modèles d'e-mail par défaut. Selon votre configuration BlackBerry UEM, vous verrez une partie ou l'ensemble des modèles d'e-mail par défaut suivants dans Paramètres > Modèles d'e-mail :

Type	Modèle d'e-mail par défaut	Description
Activation des terminaux	E-mail d'activation par défaut	Ce modèle contient les instructions dont un utilisateur a besoin pour activer son terminal. Vous pouvez choisir d'envoyer deux e-mails distincts à l'utilisateur, le premier contenant les instructions d'activation et le second uniquement le mot de passe d'activation. Si vous ne sélectionnez pas un autre modèle, BlackBerry UEM utilise ce modèle lorsqu'il envoie un e-mail d'activation à un utilisateur. Vous pouvez modifier ce modèle par défaut, mais vous ne pouvez pas le supprimer.
Identifiant de compte Google géré par défaut	Identifiant de compte Google géré par défaut	Ce modèle est utilisé dans les environnements disposant d'un domaine Google géré. Il fournit le mot de passe du compte Google de l'utilisateur. Les utilisateurs possédant des terminaux Android 6.0 et version ultérieure reçoivent automatiquement cet e-mail s'ils disposent d'un type d'activation de profil professionnel Android. Vous pouvez modifier ce modèle par défaut, mais vous ne pouvez pas le supprimer. Vous devez également envoyer le modèle d'e-mail d'activation par défaut pour fournir aux utilisateurs les instructions leur permettant d'activer leur terminal dans BlackBerry UEM.

Type	Modèle d'e-mail par défaut	Description
Code d'activation de profil professionnel Android par défaut	Code d'activation de profil professionnel Android par défaut	Ce modèle est utilisé dans les environnements pourvus d'un domaine Google géré. Il fournit un code d'activation Google. Les utilisateurs possédant des terminaux Android 5.1 et version antérieure reçoivent automatiquement cet e-mail s'ils disposent d'un type d'activation Espace Travail uniquement. Vous pouvez modifier ce modèle par défaut, mais vous ne pouvez pas le supprimer. Vous devez également envoyer le modèle d'e-mail d'activation par défaut pour fournir aux utilisateurs les instructions leur permettant d'activer leur terminal dans BlackBerry UEM.
Activation de terminal Apple DEP	E-mail d'activation DEP de Apple	Ce modèle contient les instructions dont un utilisateur a besoin pour activer un terminal DEP Apple. Vous pouvez choisir d'envoyer deux e-mails distincts à l'utilisateur, le premier contenant les instructions d'activation et le second uniquement le mot de passe d'activation. Vous pouvez modifier ou supprimer ce modèle.
Clé d'accès BlackBerry Dynamics	E-mail pour la clé d'accès BlackBerry Dynamics	Ce modèle contient les instructions dont un utilisateur a besoin pour activer une application BlackBerry Dynamics à l'aide d'une clé d'accès. Vous pouvez modifier ou supprimer ce modèle.
E-mail d'activation Espace Travail uniquement (profils professionnels Android) par défaut	Activation Espace Travail uniquement (profils professionnels Android) par défaut	Ce modèle est utilisé dans les environnements qui ne disposent pas de domaine Google géré et qui utilisent des profils professionnels Android. Ce modèle contient les instructions dont un utilisateur a besoin pour activer son terminal. Vous pouvez choisir d'envoyer deux e-mails distincts à l'utilisateur, le premier contenant les instructions d'activation et le second uniquement le mot de passe d'activation. Vous pouvez modifier ou supprimer ce modèle.
Violation de conformité	E-mail de conformité par défaut	Ce modèle contient des informations sur la conformité du terminal d'un utilisateur. Vous pouvez associer ce modèle à un profil de conformité. Vous pouvez modifier ce modèle par défaut, mais vous ne pouvez pas le supprimer.

Type	Modèle d'e-mail par défaut	Description
Notification d'événement	E-mail de notification d'évènement BlackBerry UEM	Ce modèle contient des informations destinées aux administrateurs au sujet d'un évènement qui s'est produit dans BlackBerry UEM. Vous pouvez associer ce modèle à une notification d'évènement. Vous pouvez modifier ce modèle par défaut, mais vous ne pouvez pas le supprimer.
Notification d'activation de terminal	E-mail de notification d'activation de terminal	Ce modèle contient des informations sur le terminal qui a été activé par un utilisateur. Un e-mail de notification d'activation de terminal est envoyé lorsque l'utilisateur active son terminal via BlackBerry UEM Client. Un e-mail de notification d'activation de terminal BlackBerry Dynamics est envoyé lorsque l'utilisateur active une application BlackBerry Dynamics son terminal. Vous pouvez modifier ce modèle par défaut, mais vous ne pouvez pas le supprimer.
Notification de connexion Self-Service	E-mail de notification de connexion Self-Service	Ce modèle contient des informations sur l'utilisateur qui est connecté au portail BlackBerry UEM Self-Service (par exemple, l'adresse IP et la date et l'heure). Vous pouvez modifier ce modèle par défaut, mais vous ne pouvez pas le supprimer.

Texte suggéré

Le texte suggéré 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. Si le texte par défaut est actualisé entre les versions de BlackBerry UEM, vous pouvez afficher le texte actualisé ici. Pour obtenir la liste des variables que vous pouvez utiliser dans les modèles d'e-mail, reportez-vous à la section Variables par défaut.

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 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.

Nom	Texte suggéré
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. Les informations suivantes vous seront nécessaires lors de l'activation du profil professionnel : • Votre adresse e-mail professionnelle : %UserEmailAddress% • Le 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.
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.

Nom	Texte suggéré
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 !
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. Vous pouvez consulter une vidéo sur la façon d'activer votre terminal sur la page : http://help.blackberry.com/detectLang/activation-videos/current/ 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 Windows Phone 8.1 Si vous utilisez un terminal exécutant Windows Phone version 8.1 ou antérieure, vous devez installer BlackBerry UEM Client depuis Windows Store. 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 BlackBerry 10, iOS, Android ou Windows sur BlackBerry UEM. Si vous avez des questions, contactez votre administrateur. Bienvenue dans BlackBerry UEM !
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 Espace Travail uniquement (profils professionnels Android) par défaut Premier e-mail	**Objet : activer votre terminal sur BlackBerry UEM** %UserDisplayName%, Votre administrateur a activé votre terminal Android (6.0 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 afw#blackberry. Attendez la fin de la mise à jour des applications système importantes et des téléchargements de 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 !

Nom	Texte suggéré
E-mail de notification d'évènement BlackBerry UEM	**Objet : BlackBerry UEM notification d'évènement** L'évènement suivant est survenu : %AllEventVariables%
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.

Créer un modèle d'e-mail d'activation

1. Dans la barre de menus, cliquez sur **Paramètres** > **Paramètres généraux**.
2. Cliquez sur **Modèles d'e-mail**.
3. Cliquez sur +. Sélectionnez **Activation de terminal**.
4. Dans le champ **Nom**, saisissez un nom pour identifier ce modèle.
5. Dans le champ **Objet**, modifiez le texte pour personnaliser la ligne d'objet du premier e-mail d'activation.
6. Dans le champ **Message**, saisissez le corps du texte de l'e-mail d'activation.
   - Utilisez l'éditeur HTML pour sélectionner le format de police et insérer des images (par exemple, un logo d'entreprise).
   - Insérez des variables dans le texte pour personnaliser le message (par exemple, utilisez la variable %UserDisplayName% pour insérer le nom du destinataire). Pour obtenir la liste des variables disponibles, consultez Variables par défaut.
   - Pour obtenir un échantillon du texte, cliquez sur **Texte suggéré**.

7. 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**.
8. Pour envoyer le mot de passe d'activation ou le QR Code et les instructions d'activation dans des e-mails distincts, sélectionnez **Envoyer deux e-mails d'activation distincts : le premier pour les instructions, le second pour le mot de passe**. 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.
9. Dans le champ **Objet**, saisissez la ligne d'objet du second e-mail d'activation.
10. Personnalisez le texte du modèle du deuxième e-mail d'activation et incluez-y le mot de passe d'activation (ou la variable correspondante) ou cochez la case **Ajouter un code QR aux e-mails**.
11. Cliquez sur **Enregistrer**.

Création d'un modèle pour les notifications d'e-mail de conformité

Vous pouvez créer plusieurs modèles d'e-mail, les personnaliser pour des types de terminal ou groupe d'utilisateurs spécifiques et attribuer un modèle approprié à chaque compte d'utilisateur. Lorsque le terminal d'un utilisateur ne respecte pas avec un profil de conformité, BlackBerry UEM peut envoyer un e-mail personnalisé basé sur le modèle attribué. BlackBerry 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, BlackBerry UEM utilise le modèle par défaut.

1. Dans la barre de menus, cliquez sur **Paramètres** > **Paramètres généraux**.
2. Cliquez sur **Modèles d'e-mail**.
3. Cliquez sur +. Sélectionnez **Violation de conformité**.
4. Dans le champ **Nom**, saisissez un nom pour identifier ce modèle.
5. Dans le champ **Objet**, saisissez un objet pour l'e-mail.
6. Dans le champ **Message**, saisissez le corps du texte de l'e-mail sur la conformité. Utilisez l'éditeur HTML pour sélectionner le format de police et insérer des images (par exemple, un logo d'entreprise). Insérez des variables dans le texte pour personnaliser le message (par exemple, utilisez la variable %UserDisplayName% pour insérer le nom du destinataire). Pour obtenir la liste des variables disponibles, consultez Variables par défaut.
7. Cliquez sur **Enregistrer**.

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

Vous pouvez créer des modèles d'e-mail de notification d'évènement à associer à des notifications d'évènement.

1. Sur la barre de menus, cliquez sur **Paramètres** > **Paramètres généraux**.
2. Cliquez sur **Modèles d'e-mail**.
3. Cliquez sur + et sélectionnez **Notification d'évènement**.
4. Dans le champ **Nom**, saisissez un nom pour identifier ce modèle.
5. Dans le champ **Objet**, effectuez l'une des tâches suivantes :
   - Décochez la case **Ajouter un type d'évènement à l'objet de l'e-mail** et saisissez un objet.
   - Laissez la case **Ajouter un type d'évènement à l'objet de l'e-mail** cochée et saisissez du texte dans le champ objet.
   - Laissez la case **Ajouter un type d'évènement à l'objet de l'e-mail** cochée.
6. Dans le champ **Message**, saisissez le corps du texte de l'e-mail de notification d'évènement.
   - Utilisez l'éditeur HTML pour sélectionner le format de police et insérer des images (par exemple, le logo de votre entreprise).
   - Pour obtenir un échantillon du texte, cliquez sur **Texte suggéré**.
7. Cliquez sur **Enregistrer**.

Concepts connexes

Création de notifications d'évènement

Modifier un modèle d'e-mail

1. Dans la barre de menus, cliquez sur **Paramètres** > **Paramètres généraux**.
2. Cliquez sur **Modèles d'e-mail**.
3. Cliquez sur **E-mail d'activation par défaut** ou sur n'importe quel modèle existant que vous souhaitez modifier.
4. Modifiez les champs **Nom**, **Objet** ou **Message**. Si vous commettez une erreur et que vous souhaitez tout recommencer, cliquez simplement sur **Annuler** pour revenir à la page **Modèles d'e-mail**.
5. Une fois vos modifications terminées, cliquez sur **Enregistrer**.

Wi-Fi, VPN, BlackBerry Secure Connect Plus et autres connexions professionnelles

Vous pouvez utiliser des profils pour configurer et gérer les connexions professionnelles des terminaux de votre organisation. Les connexions professionnelles définissent la manière dont les terminaux se connectent aux ressources professionnelles dans l'environnement de votre entreprise, comme les serveurs de messagerie, serveurs proxy, réseaux Wi-Fi et VPN. Vous pouvez spécifier les paramètres des terminaux BlackBerry 10, iOS, macOS, Android et Windows dans le même profil, puis attribuer le profil à des comptes d'utilisateur, groupes d'utilisateurs ou groupes de terminaux.

Étapes à suivre pour configurer les connexions professionnelles des terminaux

Pour configurer les connexions professionnelles des terminaux, procédez comme suit :

Étape	Action
1	Créez des profils pour configurer la manière dont les terminaux se connectent aux ressources professionnelles. Par exemple, créez un profil de messagerie, un profil Wi-Fi, un profil VPN, un profil de connectivité d'entreprise et un profil de connectivité BlackBerry Dynamics.
2	Si nécessaire, classez les profils.
3	Attribuez les profils aux comptes d'utilisateur, groupes d'utilisateurs ou groupes de terminaux.

Meilleure pratique : création de profils de connexions professionnelles

Certains profils de connexions professionnelles peuvent inclure un ou plusieurs profils associés. Lorsque vous spécifiez un profil associé, vous liez un profil existant à un profil de connexions professionnelles et les terminaux doivent utiliser le profil associé lorsqu'ils utilisent le profil de connexions professionnelles.

Prenez en compte les recommandations suivantes :

- Déterminez les connexions professionnelles requises pour les terminaux de votre organisation.
- Créez des profils que vous pouvez associer à d'autres profils avant de créer les profils de connexions professionnelles qui les utilisent.
- Utilisez des variables, le cas échéant.

Vous pouvez associer des profils de certificat et des profils proxy à différents profils de connexions professionnelles. Vous devez créer ces profils dans l'ordre suivant :

1. Profils de certificat
2. Profils proxy

3. Profils de connexions professionnelles (messagerie, VPN et Wi-Fi , par exemple)

Par exemple, si vous créez un profil Wi-Fi, vous ne pouvez pas associer de profil proxy au profil Wi-Fi lorsque vous le créez. Après avoir créé un profil proxy, vous devez modifier le profil Wi-Fi pour lui associer le profil proxy.

Concepts connexes

Envoi de certificats aux terminaux à l'aide de profils

Référence connexe

Utilisation de variables dans les profils

Configuration de réseaux Wi-Fi professionnels pour les terminaux

Vous pouvez utiliser un profil Wi-Fi pour spécifier la manière dont les terminaux se connectent à un réseau Wi-Fi professionnel derrière le pare-feu. Vous pouvez attribuer un profil Wi-Fi à des comptes d'utilisateur, groupes d'utilisateurs ou groupes de terminaux.

Terminal	Applications et connexions réseau
BlackBerry 10	Par défaut, les applications professionnelles et personnelles peuvent utiliser les profils Wi-Fi stockés sur le terminal pour se connecter au réseau de votre organisation. Les applications professionnelles peuvent également utiliser BlackBerry Infrastructure pour se connecter au réseau de votre organisation. Si les normes de sécurité de votre organisation n'autorisent pas les applications personnelles à accéder au réseau de votre organisation ou si vous souhaitez limiter les options de connectivité des applications professionnelles, vous pouvez limiter les options de connexion.
iOS, macOS, Android et Wir	Les applications professionnelles et personnelles peuvent utiliser les profils Wi-Fi stockés sur le terminal pour se connecter au réseau de votre entreprise.

Créer un profil Wi-Fi

Les paramètres de profil requis varient pour chaque type de terminal et dépendent du type de sécurité Wi-Fi et du protocole d'authentification que vous sélectionnez.

Avant de commencer :

- Si les terminaux utilisent l'authentification basée sur des certificats pour les connexions Wi-Fi professionnelles, créez un profil de certificat d'autorité de certification et attribuez-le aux comptes d'utilisateur, groupes d'utilisateurs ou groupes de terminaux. Pour envoyer les certificats client aux terminaux, créez un profil SCEP, un profil de certificat partagé ou un profil d'informations d'identification de l'utilisateur à associer au profil Wi-Fi.
- Pour les terminaux BlackBerry 10, iOS, macOS, Android dotés d'un profil professionnel ou Samsung KNOX qui utilisent un serveur proxy pour les connexions Wi-Fi professionnelles, créez un profil proxy à associer au profil Wi-Fi.
- Si les terminaux BlackBerry 10 utilisent un réseau VPN pour les connexions Wi-Fi professionnelles, créez un profil VPN à associer au profil Wi-Fi.

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

2. Cliquez sur **Réseaux et connexions > Wi-Fi**.
3. Cliquez sur +.
4. Tapez le nom et la description du profil Wi-Fi. Cette information s'affiche sur les terminaux.
5. Dans le champ **SSID**, saisissez le nom de réseau d'un réseau Wi-Fi.
6. Si le réseau Wi-Fi ne diffuse pas le SSID, cochez la case **Réseau masqué**.
7. Vous pouvez également décocher la case correspondant aux types de terminaux pour lesquels vous ne souhaitez pas configurer le profil.
8. Procédez comme suit :
   a) Cliquez sur l'onglet correspondant à un type de terminal.
   b) Configurez les valeurs qui conviennent pour chaque paramètre de profil afin qu'elles correspondent à la configuration Wi-Fi dans l'environnement de votre organisation. Si votre organisation requiert que les utilisateurs fournissent un nom d'utilisateur et un mot de passe pour se connecter au réseau Wi-Fi et que le profil correspond à plusieurs utilisateurs, dans le champ **Nom d'utilisateur**, saisissez `%UserName%`.

   Pour plus de détails sur chaque paramètre de profil, reportez-vous à la section Paramètres du profil Wi-Fi .
9. Répétez l'étape 7 pour chaque type de terminal de votre organisation.
10. Cliquez sur **Ajouter**.

Concepts connexes

Envoi de certificats aux terminaux à l'aide de profils
Paramètres du profil Wi-Fi

Tâches connexes

Attribuer un profil ou une stratégie informatique à un groupe d'utilisateurs
Attribuer un profil ou une stratégie informatique à un compte d'utilisateur

Configuration de réseaux VPN professionnels pour les terminaux

Vous pouvez utiliser un profil VPN pour spécifier la manière dont les terminaux BlackBerry 10, iOS, macOS, Samsung KNOX Workspace et Windows 10 se connectent à un VPN professionnel. Vous pouvez attribuer un profil VPN à des comptes d'utilisateur, groupes d'utilisateurs ou groupes de terminaux. Pour les terminaux BlackBerry 10, vous pouvez également associer un profil VPN au profil Wi-Fi.

Pour connecter à un VPN professionnel les utilisateurs Windows Phone et le terminal Android, autre que le terminal Samsung KNOX Workspace, les utilisateurs doivent configurer manuellement les paramètres VPN de leurs terminaux.

Terminal	Applications et connexions réseau
BlackBerry 10	• Par défaut, les applications professionnelles et personnelles peuvent utiliser les profils VPN stockés sur le terminal pour se connecter au réseau de votre organisation. Les applications professionnelles peuvent également utiliser BlackBerry Infrastructure pour se connecter au réseau de votre organisation. Si les normes de sécurité de votre organisation n'autorisent pas les applications personnelles à accéder au réseau de votre organisation ou si vous souhaitez limiter les options de connectivité des applications professionnelles, vous pouvez limiter les options de connexion.
iOS	• Les applications professionnelles et personnelles peuvent utiliser les profils VPN stockés sur le terminal pour se connecter au réseau de votre organisation. Vous pouvez activer un VPN par application pour un profil VPN afin de limiter ce dernier aux applications professionnelles que vous spécifiez.
macOS	• Vous pouvez configurer des profils VPN pour permettre aux applications de se connecter au réseau de votre organisation.
KNOX Workspace	• Les applications professionnelles peuvent utiliser les profils VPN stockés sur le terminal pour se connecter au réseau de votre organisation. • Vous pouvez activer un VPN par application afin de limiter ce dernier aux applications professionnelles que vous spécifiez. • Une application client VPN prise en charge doit être installée sur le terminal. Cisco AnyConnect et Juniper sont pris en charge. **Remarque :** L'application Juniper prend uniquement en charge SSL VPN.
Windows 10	• Vous pouvez configurer des profils VPN pour permettre aux applications de se connecter au réseau de votre organisation. Dans le profil VPN, vous pouvez spécifier une liste d'applications que le VPN doit utiliser.

Créer un profil VPN

Les paramètres de profil requis varient pour chaque type de terminal et dépendent du type de connexion VPN et du type d'authentification que vous sélectionnez.

Remarque : certains terminaux peuvent ne pas être en mesure de stocker le mot de passe xAuth. Pour plus d'informations, rendez-vous sur le site support.blackberry.com/kb pour lire l'article KB30353.

Avant de commencer :

- Si les terminaux utilisent l'authentification basée sur des certificats pour les connexions VPN, créez un profil de certificat d'autorité de certification et attribuez-le aux comptes d'utilisateur, aux groupes d'utilisateurs ou aux groupes de terminaux. Pour envoyer des certificats client aux terminaux, créez des informations d'identification utilisateur, un SCEP ou un profil de certificat partagé à associer au profil VPN.
- Pour les terminaux BlackBerry 10, iOS, macOS et Samsung KNOX Workspace qui utilisent un serveur proxy, créez un profil proxy à associer au profil VPN. (Le serveur proxy pour les terminaux Windows 10 est configuré dans le profil VPN.)
- Pour les terminaux KNOX Workspace, ajoutez l'application client VPN qui convient à la liste des applications et attribuez-la aux comptes d'utilisateur, groupes d'utilisateurs ou groupes de terminaux. Les applications client VPN prises en charge sont Cisco AnyConnect et Juniper.

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

2. Cliquez sur **Réseaux et connexions > VPN**.
3. Cliquez sur +.
4. Tapez le nom et la description du VPN. Cette information s'affiche sur les terminaux.
5. Vous pouvez également décocher la case correspondant aux types de terminaux pour lesquels vous ne souhaitez pas configurer le profil.
6. Procédez comme suit :
   a) Cliquez sur l'onglet correspondant à un type de terminal.
   b) Configurez les valeurs qui conviennent pour chaque paramètre de profil afin qu'elles correspondent à la configuration VPN dans l'environnement de votre organisation. Si votre organisation requiert que les utilisateurs fournissent un nom d'utilisateur et un mot de passe pour se connecter au réseau VPN et que le profil correspond à plusieurs utilisateurs, dans le champ **Nom d'utilisateur**, saisissez `%UserName%`.

   Pour plus de détails sur chaque paramètre de profil, reportez-vous à la section Paramètres du profil VPN.
7. Répétez l'étape 5 pour chaque type de terminal de votre organisation.
8. Cliquez sur **Ajouter**.

Concepts connexes

Envoi de certificats aux terminaux à l'aide de profils
Paramètres du profil VPN

Tâches connexes

Attribuer un profil ou une stratégie informatique à un groupe d'utilisateurs
Attribuer un profil ou une stratégie informatique à un compte d'utilisateur

Activation d'un VPN à la demande pour les terminauxiOSoumacOS devices

Le VPN à la demande vous permet de spécifier si un terminaliOSoumacOSse connecte automatiquement à un VPN dans un domaine particulier. Les certificats client assurent l'authentification du terminal de l'utilisateur lors de l'accès au domaine particulier. Par exemple, vous pouvez spécifier le domaine de votre organisation pour permettre aux utilisateurs d'accéder au contenu de votre intranet à l'aide d'un VPN à la demande.

Référence connexe

iOS et macOS : paramètres de profil VPN

Activation d'un VPN par application

Pour les terminaux iOS, Samsung KNOX Workspace et Windows 10, vous pouvez utiliser un VPN par application afin de spécifier les applications professionnelles et sécurisées qui doivent utiliser un VPN pour leurs données en transit. Un VPN par application permet de diminuer la charge du VPN de votre organisation en limitant son utilisation à certaines charges du trafic professionnel (l'accès aux serveurs d'applications ou aux pages Web derrière le pare-feu, par exemple). Cette fonction prend également en charge la confidentialité de l'utilisateur et augmente la vitesse de connexion des applications personnelles en n'acheminant pas le trafic personnel via le VPN.

Pour les terminaux iOS, les applications sont associées à un profil VPN lorsque vous attribuez l'application ou le groupe d'applications à un utilisateur, un groupe d'utilisateurs ou un groupe de terminaux.

Pour les terminaux Samsung KNOX Workspace, les applications sont ajoutées au paramètre « Applications autorisées à utiliser la connexion VPN » dans le profil VPN.

Pour les terminaux Windows 10, les applications sont ajoutées à la « Liste d'applications de déclenchement » dans le profil VPN.

Référence connexe

iOS et macOS : paramètres de profil VPN
Android : paramètres de profil VPN
Windows 10 : paramètres de profil VPN

Comment BlackBerry UEM choisit les paramètres VPN par application à attribuer aux terminaux iOS

Un seul profil VPN peut être attribué à une application ou à un groupe d'applications. BlackBerry UEM utilise les règles suivantes pour déterminer les paramètres VPN d'application à attribuer à une application sur les terminaux iOS :

- Les paramètres VPN d'application directement associés à une application sont prioritaires sur les paramètres VPN d'application indirectement associés via un groupe d'applications.
- Les paramètres VPN d'application directement associés à un utilisateur sont prioritaires sur les paramètres VPN d'application indirectement associés via un groupe d'utilisateurs.
- Les paramètres VPN d'application attribués à une application requise sont prioritaires sur les paramètres VPN d'application attribués à une instance facultative de la même application.
- Les paramètres VPN d'application associés au nom du groupe d'utilisateurs qui apparait en premier dans la liste alphabétique sont prioritaires si les conditions suivantes sont remplies :
  - Une application est attribuée à plusieurs groupes d'utilisateurs
  - La même application apparait dans les groupes d'utilisateurs
  - L'application est attribuée de la même manière, en tant qu'application seule ou groupe d'applications
  - L'application a la même disposition dans toutes les attributions (obligatoire ou facultative)

  Par exemple, vous attribuez Cisco WebEx Meetings en tant qu'application facultative aux groupes d'utilisateurs Développement et Marketing. Lorsqu'un utilisateur est dans les deux groupes, les paramètres VPN d'application du groupe Développement sont appliqués à l'application WebEx Meetings pour cet utilisateur.

Si un profil VPN d'application est attribué à un groupe de terminaux, il est prioritaire sur le profil VPN d'application qui est attribué au compte d'utilisateur des terminaux qui appartiennent au groupe de terminaux.

Création de profils proxy pour les terminaux

Vous pouvez spécifier la manière dont les terminaux utilisent un serveur proxy pour accéder à des services Web sur Internet ou un réseau professionnel. Pour les terminaux BlackBerry 10, iOS, macOS et Android, vous devez créer un profil de proxy. Pour les terminaux Windows 10, vous devez ajouter les paramètres de proxy dans Wi-Fi ou dans le profil VPN.

Sauf note contraire, les profils proxy prennent en charge les serveurs proxy utilisant l'authentification de base ou aucune authentification.

Terminal	Configuration du proxy
BlackBerry 10	Créez un profil proxy et associez-le aux profils utilisés par votre entreprise, notamment : • Wi-Fi • VPN • Connectivité d'entreprise
iOS	Créez un profil proxy et associez-le aux profils utilisés par votre entreprise, notamment : • Wi-Fi • VPN Vous pouvez attribuer un profil proxy à des comptes d'utilisateur, groupes d'utilisateurs ou groupes de terminaux. **Remarque :** Un profil proxy attribué à des comptes d'utilisateur, groupes d'utilisateurs ou groupes de terminaux est un proxy global réservé aux terminaux supervisés et prioritaire sur un profil proxy associé à un profil Wi-Fi ou VPN. Les terminaux supervisés utilisent les paramètres proxy globaux pour toutes les connexions HTTP.
macOS	Créez un profil proxy et associez-le à un profil Wi-Fi ou VPN. macOS applique les profils aux terminaux ou comptes d'utilisateur. Les profils de proxy sont appliqués aux terminaux.
Android	Pour les terminaux Android dotés d'un profil professionnel, créez un profil de proxy associez-le à un profil Wi-Fi. Les terminaux Android 8.0 et version ultérieure dotés des activations Contrôles MDM ou Confidentialité de l'utilisateur ne prennent pas en charge les profils Wi-Fi avec des paramètres de proxy. Si un terminal doté de l'un de ces types d'activation est mis à niveau vers Android 8.0, les profils Wi-Fi associés à un profil de proxy sont supprimés du terminal.

Terminal	Configuration du proxy
Samsung KNOX	Créer un profil proxy et associez-le avec les profils que votre entreprise utilise. Les conditions suivantes s'appliquent : • Pour les profils Wi-Fi, seuls les profils de proxy possédant une configuration manuelle sont pris en charge sur les terminaux KNOX. Les profils proxy que vous associez aux profils Wi-Fi prennent en charge les serveurs proxy utilisant l'authentification de base, NTML ou aucune authentification. • Pour les profils VPN et de connectivité d'entreprise, les profils proxy avec une configuration manuelle sont pris en charge sur les terminaux Samsung KNOX Workspace qui utilisent KNOX 2.5 et versions ultérieures. Les profils proxy avec configuration PAC sont pris en charge sur les terminaux KNOX Workspace qui utilisent une version de KNOX ultérieure à la version 2.5. **Remarque :** Si vous souhaitez utiliser un proxy profil avec un profil de connectivité d'entreprise,BlackBerry Secure Connect Plus doit être activé. Vous pouvez attribuer un profil proxy à des comptes d'utilisateur, groupes d'utilisateurs ou groupes de terminaux. Les conditions suivantes s'appliquent : • Sur les terminaux KNOX Workspace, le profil configure les paramètres de proxy du navigateur de l'espace Travail. • Sur les terminaux Samsung KNOX MDM, le profil configure les paramètres de proxy du navigateur sur le terminal. **Remarque :** la configuration du CCP n'est pas prise en charge sur les terminaux KNOX Workspace qui utilisent KNOX 2.5 et versions antérieures et les terminaux KNOX MDM.
Windows 10	Créez un profil Wi-Fi ou VPN et spécifiez les informations du serveur proxy dans les paramètres du profil. Les conditions suivantes s'appliquent : • Le proxy Wi-Fi prend en charge uniquement la configuration manuelle et est pris en charge uniquement sur les terminaux Windows 10 Mobile. • Le proxy VPN prend en charge la configuration PARC ou manuelle.

Créer un profil proxy

Si votre organisation utilise un fichier PAC pour définir des règles proxy, vous pouvez sélectionner la configuration PAC pour utiliser les paramètres du serveur proxy depuis le fichier PAC que vous spécifiez. Sinon, vous pouvez sélectionner la configuration manuelle et spécifier les paramètres du serveur proxy directement dans le profil.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Réseaux et connexions > Proxy**.
3. Cliquez sur +.
4. Saisissez le nom et la description du profil proxy.
5. Cliquez sur l'onglet correspondant à un type de terminal.
6. Effectuez l'une des tâches suivantes :

Tâche	Étapes
Spécifier les paramètres de configuration PAC	**a.** Dans la liste déroulante **Type**, vérifiez que le paramètre **Configuration PAC** est sélectionné. **b.** Dans le champ **URL du fichier PAC**, saisissez l'URL du serveur Web hébergeant le fichier PAC et indiquez le nom du fichier PAC (par exemple, http://www.exemple.com/PACfile.pac). Le fichier PAC ne doit pas être hébergé sur un serveur qui héberge BlackBerry UEM ou l'un de ses composants. **c.** Dans l'onglet **BlackBerry**, procédez comme suit : **1.** Si votre organisation requiert que les utilisateurs fournissent un nom d'utilisateur et un mot de passe pour se connecter au serveur proxy et que le profil correspond à plusieurs utilisateurs, dans le champ **Nom d'utilisateur**, saisissez `%UserName%`. Si le serveur proxy requiert le nom de domaine pour l'authentification, utilisez le format *<domain>**<username>*. **2.** Dans la liste déroulante **Modifiable par l'utilisateur**, cliquez sur les paramètres proxy que les utilisateurs de terminaux BlackBerry 10 peuvent modifier. La valeur par défaut est **Lecture seule**.
Définir les paramètres de configuration manuelle	**a.** Dans la liste déroulante **Type**, cliquez sur **Configuration manuelle.** **b.** Dans le champ **Hôte**, saisissez le FQDN ou l'adresse IP du serveur proxy. **c.** Dans le champ **Port**, saisissez le numéro de port du serveur proxy. **d.** Si votre entreprise requiert que les utilisateurs fournissent un nom d'utilisateur et un mot de passe pour se connecter au serveur proxy et que le profil correspond à plusieurs utilisateurs, dans le champ **Nom d'utilisateur**, saisissez `%UserName%`. Si le serveur proxy requiert le nom de domaine pour l'authentification, utilisez le format *<domain>**<username>*. **e.** Dans l'onglet **BlackBerry**, procédez comme suit : **1.** Dans la liste déroulante **Modifiable par l'utilisateur**, cliquez sur les paramètres proxy que les utilisateurs de terminaux BlackBerry 10 peuvent modifier. La valeur par défaut est **Lecture seule**. **2.** Vous pouvez également spécifier une liste d'adresses auxquelles les utilisateurs peuvent directement accéder à partir de leurs terminaux BlackBerry 10, sans utiliser le serveur proxy. Dans le champ **Liste d'exclusion**, saisissez les adresses (FQDN ou IP) et utilisez un point-virgule (;) pour séparer les valeurs de la liste. Vous pouvez utiliser le caractère générique (*) dans un nom FQDN ou IP (par exemple, *.exemple.com ou 192.0.2.*).

7. Répétez les étapes 4 et 5 pour chaque type de terminal de votre organisation.
8. Cliquez sur **Ajouter**.

À la fin :

- Associez le profil proxy à un profil Wi-Fi, VPN ou de connectivité d'entreprise.

- Si nécessaire, classez les profils. Le classement que vous spécifiez s'applique uniquement si vous attribuez un profil proxy à des groupes d'utilisateurs ou à des groupes de terminaux.

Tâches connexes

Attribuer un profil ou une stratégie informatique à un groupe d'utilisateurs
Attribuer un profil ou une stratégie informatique à un compte d'utilisateur

Utiliser la connectivité d'entreprise et BlackBerry Secure Connect Plus pour les connexions aux ressources professionnelles

Vous pouvez utiliser un profil de connectivité d'entreprise pour activer la connectivité d'entreprise etBlackBerry Secure Connect Plus sur les terminaux pris en charge.

Connectivité d'entreprise

La connectivité d'entreprise transmet toutes les données professionnelles envoyées entre les terminaux BlackBerry 10 et le réseau de votre entreprise via l'BlackBerry Infrastructure vers BlackBerry UEM. Cette fonctionnalité vous évite de devoir ouvrir une connexion directe à Internet via le pare-feu de votre entreprise pour la gestion des terminaux BlackBerry 10 et des applications qui se connectent à votre serveur de messagerie, à une autorité de certification interne et à d'autres serveurs Web ou serveurs de contenu. La connectivité d'entreprise est toujours activée pour les terminaux BlackBerry 10, même si vous n'utilisez pas BlackBerry Secure Connect Plus. Ces terminaux choisissent le chemin le plus efficace en fonction de la disponibilité du réseau.

BlackBerry Secure Connect Plus

BlackBerry Secure Connect Plus est un composant BlackBerry UEM qui fournit un tunnel IP sécurisé entre des applications et un réseau d'entreprise :

- Pour les terminaux BlackBerry 10 et Android dotés d'un profil professionnel, toutes les applications professionnelles utilisent le tunnel sécurisé.
- Pour les terminaux Samsung KNOX Workspace, vous pouvez autoriser toutes les applications de l'espace Travail à utiliser le tunnel ou spécifier des applications utilisant un VPN par application.
- Pour les terminaux iOS, vous pouvez autoriser toutes les applications à utiliser le tunnel ou spécifier des applications utilisant un VPN par application.

Remarque : Si BlackBerry Secure Connect Plus n'est pas disponible dans votre région, vous devez le désactiver manuellement pour les terminaux Android dans le profil de connectivité d'entreprise.

Le tunnel IP sécurisé permet aux utilisateurs d'accéder aux ressources professionnelles derrière le pare-feu de votre entreprise tout en assurant la sécurité des données à l'aide des protocoles standard et du cryptage de bout en bout.

BlackBerry Secure Connect Plus et un terminal pris en charge établissent un tunnel IP sécurisé s'il s'agit de la meilleure option disponible à des fins de connexion au réseau de l'entreprise. Si un terminal se voit attribuer un profil Wi-Fi ou un profil VPN et que le terminal peut accéder au réseau Wi-Fi professionnel ou VPN, il utilise ces méthodes pour se connecter au réseau. Si ces options ne sont pas disponibles (par exemple, si l'utilisateur est hors de portée du réseau Wi-Fi professionnel), BlackBerry Secure Connect Plus et le terminal établissent un tunnel IP sécurisé.

Pour les terminaux iOS, si vous configurez un VPN par application pour BlackBerry Secure Connect Plus, les applications configurées utilisent toujours un tunnel sécurisé via BlackBerry Secure Connect Plus, même si l'application peut se connecter au réseau Wi-Fi professionnel ou au VPN spécifié dans un profil Wi-Fi ou VPN.

Les terminaux pris en charge communiquent avec BlackBerry UEM pour établir le tunnel sécurisé via BlackBerry Infrastructure. Un tunnel est établi pour chaque terminal. Le tunnel prend en charge les protocoles IPv4 standard (TCP et UDP). Tant que le tunnel est ouvert, les applications peuvent accéder aux ressources du réseau. Lorsque le tunnel n'est plus requis (si, par exemple, l'utilisateur est à portée du réseau Wi-Fi professionnel), il prend fin.

BlackBerry Secure Connect Plus offre les avantages suivants :

- Le trafic IP acheminé entre les terminaux et BlackBerry UEM est crypté de bout en bout à l'aide de l'AES256, ce qui garantit la sécurité des données professionnelles.
- BlackBerry Secure Connect Plus fournit une connexion fiable et sécurisée aux ressources professionnelles lorsqu'un utilisateur de terminal ne peut pas accéder au réseau Wi-Fi professionnel ou VPN.
- BlackBerry Secure Connect Plus est installé derrière le pare-feu de votre entreprise, de sorte que les données transitent via une zone de confiance qui suit les normes de sécurité de votre entreprise.
- BlackBerry Secure Connect Plus offre la possibilité de mettre en œuvre un transcodeur pour les terminaux BlackBerry 10 à des fins de cryptage personnalisé des données qui transitent via le tunnel sécurisé.

Pour plus d'informations sur la méthode utilisée par la connectivité d'entrepriseet BlackBerry Secure Connect Plus pour transférer des données depuis et vers les terminaux, reportez-vous au contenu relatif à l'architecture.

Étapes à suivre pour activer BlackBerry Secure Connect Plus

Pour activer BlackBerry Secure Connect Plus, procédez comme suit :

Étape	Action
1	Vérifiez que le domaine BlackBerry UEM de votre entreprise répond aux conditions d'utilisation de BlackBerry Secure Connect Plus .
2	Vérifiez que BlackBerry Secure Connect Plus est activé dans le profil de connectivité d'entreprise par défaut ou dans un profil personnalisé que vous créez.
3	Vous pouvez également spécifier les paramètres DNS pour l'application BlackBerry Connectivity.
4	Si votre environnement inclut des terminaux Android dotés d'un profil professionnel et des terminaux Samsung KNOX Workspace compatibles BlackBerry Dynamics, optimisez les connexions tunnel sécurisées.
5	Attribuez le profil de connectivité d'entreprise aux utilisateurs et groupes.

Exigences liées au serveur et au terminal

Pour utiliser BlackBerry Secure Connect Plus, l'environnement de votre entreprise doit répondre aux exigences ci-dessous.

Pour le domaine BlackBerry UEM :

- Le pare-feu de votre entreprise doit autoriser les connexions sortantes sur le port 3101 vers <*région*>.turnb.bbsecure.com et <*région*>.bbsecure.com. Si vous configurez BlackBerry UEM pour qu'il utilise un serveur proxy, vérifiez que ce serveur proxy autorise les connexions sur le port 3101 vers ces sous-domaines. Pour connaitre les domaines et les adresses IP à utiliser dans votre configuration de pare-feu, rendez-vous sur http://support.blackberry.com/kb et consultez l'article KB 36470.

- Dans chaque instance de BlackBerry UEM, le composant BlackBerry Secure Connect Plus doit être en cours d'exécution.
- Par défaut, les terminaux Android dotés d'un profil professionnel ne sont pas autorisés à utiliser BlackBerry Secure Connect Plus pour se connecter à Google Play et aux services sous-jacents (com.android.providers.media, com.android.vending et com.google.android.apps.gcs). Google Play ne prend pas en charge le proxy. Les terminaux Android qui sont dotés d'un profil professionnel utilisent une connexion directe sur Internet à Google Play.

  Vérifiez que ces restrictions sont configurées dans le profil de connectivité d'entreprise par défaut ou dans les nouveaux profils de connectivité d'entreprise personnalisés que vous créez. Il est recommandé de maintenir ces restrictions. Si vous supprimez l'une de ces restrictions, vous devez contacter l'assistance Google Play afin de vous renseigner au sujet de la configuration de pare-feu obligatoire pour autoriser les connexions à Google Play à l'aide de BlackBerry Secure Connect Plus.

Remarque : si votre environnement inclut KNOX Workspace et des terminaux Android dotés d'un profil professionnel avec les applications BlackBerry Dynamics, reportez-vous à Optimiser les connexions de tunnel sécurisées pour les terminaux Android qui utilisent des applications BlackBerry Dynamics.

Pour les terminaux pris en charge :

Terminal	Configuration requise

BlackBerry 10	• BlackBerry 10 Système d'exploitation version 10.3.2 ou ultérieure
	• L'un des types d'activation suivants :
	  • Travail et Personnel - Entreprise
	  • Espace Travail uniquement
	  • Travail et Personnel - Régulé

Samsung KNOX Workspace	• Android version 5.0 ou ultérieure
	• Samsung KNOX MDM version 5.0 ou ultérieure
	• Samsung KNOX version 2.3 ou ultérieure
	• L'un des types d'activation suivants :
	  • Espace Travail uniquement (Samsung KNOX)
	  • Travail et Personnel - Contrôle total (Samsung KNOX)
	  • Travail et Personnel - Confidentialité de l'utilisateur (Samsung KNOX)

Terminaux Android dotés d'un profil professionnel	• Android version 5.1 ou ultérieure
	• L'un des types d'activation suivants :
	  • Espace Travail uniquement (Premium)
	  • Travail et Personnel - Confidentialité de l'utilisateur (Premium)

iOS	• iOS version 9 ou ultérieure • Les terminaux doivent être activés à l'aide de l'application BlackBerry UEM Client, disponible à partir de App Store. • Type d'activation Contrôles MDM

Pour plus d'informations sur les licences requises pour utiliser BlackBerry Secure Connect Plus, consultez le contenu relatif aux licences.

Équilibrage des charges et haute disponibilité pour BlackBerry Secure Connect Plus

Si un domaine comprend plusieurs instances de BlackBerry UEM, le composant BlackBerry Secure Connect Plus de chaque instance est exécuté et traite les données. Les données sont équilibrées en termes de charges sur tous les composants BlackBerry Secure Connect Plus du domaine.

Le basculement de haute disponibilité est disponible pour les terminaux BlackBerry 10, Samsung KNOX Workspace, les terminaux Android dotés d'un profil professionnel et les terminaux iOS. Si un terminal utilise un tunnel sécurisé et que le composant BlackBerry Secure Connect Plus actuel devient indisponible, BlackBerry Infrastructure attribue le terminal à un composant BlackBerry Secure Connect Plus sur une autre instance de BlackBerry UEM. Le terminal utilise à nouveau le tunnel sécurisé sans interruption majeure.

BlackBerry Secure Connect Plus et BlackBerry Connectivity Node

Vous pouvez installer une ou plusieurs instances de BlackBerry Connectivity Node pour ajouter des instances supplémentaires de composants de connectivité de terminal au domaine de votre organisation. Chaque BlackBerry Connectivity Node contient une instance active de BlackBerry Secure Connect Plus capable de traiter les données de terminal et d'établir des connexions sécurisées.

Vous pouvez également créer des groupes de serveurs. Un groupe de serveurs contient une ou plusieurs instances de BlackBerry Connectivity Node. Lorsque vous créez un groupe de serveurs, vous spécifiez le chemin de données local que les composants doivent utiliser pour se connecter à BlackBerry Infrastructure. Par exemple, vous pouvez créer un groupe de serveurs pour diriger les connexions des terminaux pour BlackBerry Secure Connect Plus et BlackBerry Secure Gateway afin qu'ils utilisent le chemin pour les États-Unis vers BlackBerry Infrastructure. Vous pouvez associer des profils de messagerie et de connectivité d'entreprise avec un groupe de serveurs. Tout terminal auquel ces profils sont attribués utilise la connexion locale de ce groupe de serveurs à BlackBerry Infrastructure lorsqu'il utilise l'un des composants de BlackBerry Connectivity Node.

Si un groupe de serveurs contient plusieurs instances de BlackBerry Connectivity Node, les terminaux peuvent utiliser toute instance en cours d'exécution. Les connexions des terminaux sont équilibrées sur les différentes instances du groupe. Si aucune instance n'est disponible, les terminaux ne peuvent pas utiliser ces composants pour les connexions sécurisées. Au moins une des instances doit être disponible.

Pour plus d'informations sur la planification et l'installation de BlackBerry Connectivity Node, reportez-vous au contenu relatif à la planification et au contenu relatif à l'installation et à la mise à niveau.

Activer et configurer la connectivité d'entreprise et BlackBerry Secure Connect Plus

Pour activer la connectivité d'entreprise et BlackBerry Secure Connect Plus, vous devez utiliser un profil de connectivité d'entreprise.

- Les terminaux BlackBerry 10 prennent en charge la connectivité d'entreprise avec et sans BlackBerry Secure Connect Plus. Vous ne pouvez pas désactiver la connectivité d'entreprise pour les terminaux BlackBerry 10.
- Les terminaux Android avec un profil professionnel, les terminaux Samsung KNOX Workspace et les terminaux iOS prennent en charge la connectivité d'entreprise par le biais de BlackBerry Secure Connect Plus.

Remarque : Si vous utilisez un profil de messagerie pour activer BlackBerry Secure Gateway pour les terminaux iOS, il est recommandé de configurer un VPN par application pour BlackBerry Secure Connect Plus. Pour plus d'informations sur BlackBerry Secure Gateway, reportez-vous à Protéger les données de la messagerie à l'aide de BlackBerry Secure Gateway.

Remarque : Si votre environnement inclut des terminaux Android avec un profil professionnel et des terminaux Samsung KNOX Workspace avec des applications BlackBerry Dynamics, reportez-vous à Optimiser les connexions de tunnel sécurisées pour les terminaux Android qui utilisent des applications BlackBerry Dynamics.

Créer un profil de connectivité d'entreprise

Si vous souhaitez utiliser un profil de connectivité d'entreprise pour configurer BlackBerry Secure Connect Plus, reportez-vous à Activer BlackBerry Secure Connect Plus et ignorez cette tâche.

Par défaut, BlackBerry UEM attribue le profil de connectivité d'entreprise par défaut à tous les utilisateurs. Vous pouvez modifier le profil par défaut ou créer de nouveaux profils de connectivité d'entreprise.

Avant de commencer : Si nécessaire, créez un profil de proxy.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Réseaux et connexions > Connectivité d'entreprise**.
3. Cliquez sur +.
4. Saisissez le nom et la description du profil. Chaque profil de connectivité d'entreprise doit avoir un nom unique.
5. Procédez comme suit :
   a) Cliquez sur l'onglet correspondant à un type de terminal.
   b) Si la connectivité d''entreprise est activée et que vous utilisez un proxy, sélectionnez un profil proxy.
6. Répétez l'étape 4 pour chaque type de terminal pris en charge de votre organisation.
7. Cliquez sur **Ajouter**.

À la fin : Si nécessaire, classez les profils.

Concepts connexes

Paramètres de profil de connectivité d'entreprise

Tâches connexes

Attribuer un profil ou une stratégie informatique à un groupe d'utilisateurs
Attribuer un profil ou une stratégie informatique à un compte d'utilisateur

Activer BlackBerry Secure Connect Plus

Si vous souhaitez autoriser des terminaux à utiliser BlackBerry Secure Connect Plus, vous devez activer BlackBerry Secure Connect Plus dans un profil de connectivité d'entreprise et attribuer ce profil aux utilisateurs et aux groupes. Par défaut, BlackBerry Secure Connect Plus est activé pour BlackBerry 10 et les terminaux Android pris en charge. Pour les terminaux iOS, BlackBerry Secure Connect Plus n'est pas activé par défaut.

Vous pouvez effectuer l'une des actions suivantes :

- Vérifiez que BlackBerry Secure Connect Plus est activé dans le profil de connectivité d'entreprise par défaut pour les types de terminaux appropriés. Si aucun profil de connectivité d'entreprise personnalisé n'est attribué, directement ou par appartenance aux groupes, à un compte d'utilisateur, BlackBerry UEM attribue le profil par défaut.
- Créez un profil de connectivité d'entreprise personnalisé à l'aide des instructions suivantes et attribuez-le aux utilisateurs et aux groupes.

Lorsque le profil de connectivité d'entreprise est appliqué au terminal après activation, BlackBerry UEM installe l'application BlackBerry Connectivity sur le terminal (pour les terminaux Android dotés d'un profil professionnel, l'application est installée automatiquement depuis Google Play ; pour les terminaux, l'application iOS est installée automatiquement depuis App Store). Sur les terminaux BlackBerry 10, l'application est masquée et ne requiert aucune interaction de l'utilisateur.

BlackBerry publie de nouvelles versions de l'application pour prendre en charge les nouvelles fonctionnalités et améliorations. Pour obtenir des instructions sur la mise à niveau de l'application, et pour en savoir plus sur les derniers problèmes connus et résolus, reportez-vous aux Notes de version de l'application BlackBerry Connectivity.

1. Sur la barre de menus de la console de gestion, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Réseaux et connexions > Connectivité d'entreprise**.
3. Cliquez sur +.
4. Si vous avez créé et configuré un ou plusieurs groupes de serveurs pour diriger le trafic BlackBerry Secure Connect Plus vers un chemin régional spécifique de BlackBerry Infrastructure, dans la liste déroulante **Groupe de serveurs BlackBerry Secure Gateway Service**, cliquez sur le groupe de serveurs approprié.
5. Configurez les valeurs appropriées pour les paramètres de profil pour chaque type de terminal. Pour plus d'informations sur les différents paramètres de profil, reportez-vous à Paramètres de profil de connectivité d'entreprise.
6. Cliquez sur **Ajouter**.
7. Attribuez le profil aux groupes ou comptes d'utilisateur.
8. Si vous avez configuré un VPN par application pour les terminaux iOS, procédez comme suit lorsque vous attribuez une application ou un groupe d'applications : associez cette application ou ce groupe d'applications au profil de connectivité d'entreprise qui convient.

À la fin :

- Sur les terminaux Samsung KNOX Workspace et Android dotés d'un profil professionnel, l'application BlackBerry Connectivity invite les utilisateurs à l'autoriser à s'exécuter en tant que VPN et à autoriser l'accès aux clés privées du terminal. Demandez aux utilisateurs d'accepter ces demandes. Les utilisateurs de terminaux Samsung KNOX Workspace, Android dotés d'un profil professionnel et iOS peuvent ouvrir l'application pour afficher l'état de la connexion. Aucune action supplémentaire n'est requise de la part des utilisateurs.
- Si vous créez plusieurs profils de connectivité d'entreprise, classez-les.
- Si vous souhaitez mettre en œuvre le cryptage personnalisé pour BlackBerry Secure Connect Plus, vous devez exécuter des tâches de configuration supplémentaires pour permettre aux utilisateurs d'activer les terminaux BlackBerry 10. Reportez-vous à la section Mise en œuvre du cryptage personnalisé.
- Si vous dépannez un problème de connexion sur un terminal KNOX Workspace, Android doté d'un profil professionnel ou iOS, l'application autorise l'utilisateur à envoyer les journaux du terminal à l'adresse électronique d'un administrateur (l'utilisateur saisit une adresse électronique que vous devez fournir). Notez que les journaux ne sont pas visibles à l'aide de Winzip. Il est recommandé d'utiliser un autre utilitaire, par exemple 7-Zip.

Concepts connexes

Paramètres de profil de connectivité d'entreprise

Tâches connexes

Attribuer un profil ou une stratégie informatique à un groupe d'utilisateurs
Attribuer un profil ou une stratégie informatique à un compte d'utilisateur
Classer les profils

Spécifier les paramètres DNS pour l'application BlackBerry Connectivity

Vous pouvez spécifier les serveurs DNS que l'application BlackBerry Connectivity doit utiliser pour les connexions de tunnel sécurisées. Vous pouvez également spécifier des suffixes de recherche DNS. Si vous ne spécifiez pas de paramètres DNS, l'application récupère les adresses DNS depuis l'ordinateur qui héberge le composant BlackBerry Secure Connect Plus et le suffixe de recherche par défaut correspond au domaine DNS de cet ordinateur.

Si vous créez et configurez un ou plusieurs groupes de serveurs pour diriger les connexions BlackBerry Secure Connect Plus vers un chemin local spécifique à BlackBerry Infrastructure, vous pouvez définir des paramètres DNS spécifiques à chaque groupe de serveurs. Si vous le faites, les paramètres DNS pour un groupe de serveurs sont prioritaires sur les paramètres DNS mondiaux que vous spécifiez à l'aide de la procédure suivante. Pour plus d'informations sur la création et la configuration de groupes de serveurs, reportez-vous au contenu relatif à l'installation et à la mise à niveau.

1. Sur la barre de menus, cliquez sur **Paramètres**.
2. Cliquez sur **Infrastructure > BlackBerry Secure Connect Plus**.
3. Cochez la case **Configurer manuellement les serveurs DNS** et cliquez sur +.
4. Saisissez l'adresse du serveur DNS secondaire au format décimal séparé par des points (par exemple 192.0.2.0). Cliquez sur **Ajouter**.
5. Si nécessaire, répétez les étapes 3 et 4 pour ajouter d'autres serveurs DNS. Dans le tableau **Serveurs DNS**, cliquez sur les flèches de la colonne **Classement** pour définir la priorité des serveurs DNS.
6. Si vous souhaitez spécifier des suffixes de recherche DNS, procédez comme suit :
   a) Cochez la case **Gérer manuellement les suffixes de recherche DNS** et cliquez sur +.
   b) Saisissez le suffixe de recherche DNS (par exemple, domaine.com). Cliquez sur **Ajouter**.
7. Si nécessaire, répétez l'étape 6 pour ajouter d'autres suffixes de recherche DNS. Dans le tableau **Suffixe de recherche DNS**, cliquez sur les flèches de la colonne **Classement** pour définir la priorité des serveurs DNS.
8. Cliquez sur **Enregistrer**.

Optimiser les connexions de tunnel sécurisées pour les terminaux Android qui utilisent des applications BlackBerry Dynamics

Si vous activez BlackBerry Secure Connect Plus et que votre environnement comprend des applications BlackBerry Dynamics installées sur des terminaux Android dotés d'un profil professionnel ou sur des terminaux Samsung KNOX Workspace, nous vous conseillons de configurer le profil de connectivité BlackBerry Dynamics attribué à ces terminaux pour désactiver BlackBerry Proxy. L'utilisation à la fois de BlackBerry Proxy et de BlackBerry Secure Connect Plus peut retarder l'activité réseau des applications, car les données sont acheminées vers les deux composants de réseau.

1. Dans la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Réseaux et connexions > Connectivité BlackBerry Dynamics**.
3. Sélectionnez le profil attribué aux terminaux Android dotés d'un profil professionnel et aux terminaux Samsung KNOX Workspace.
4. Cliquez sur 
5. Désactivez la case **Acheminer tout le trafic**.
6. Cliquez sur **Enregistrer**.

Référence connexe

BlackBerry Dynamics : paramètres de profil de connectivité

Diriger le trafic de l'espace Travail BlackBerry 10 via BlackBerry Secure Connect Plus lorsqu'un réseau Wi-Fi est disponible

Si vous utilisez BlackBerry UEM pour configurer un profil Wi-Fi et l'attribuer aux terminaux BlackBerry 10, les terminaux hiérarchisent le réseau Wi-Fi professionnel au-dessus de BlackBerry Secure Connect Plus. Si le réseau Wi-Fi professionnel n'est pas disponible et qu'aucun profil VPN n'a été attribué aux terminaux ou qu'ils ne peuvent pas accéder au VPN, les terminaux utilisent BlackBerry Secure Connect Plus. Vous avez la possibilité de diriger tout le trafic de l'espace Travail via BlackBerry Secure Connect Plus même lorsque les terminaux peuvent accéder au réseau Wi-Fi professionnel. Vous pouvez choisir d'utiliser cette option si les normes de sécurité de votre entreprise empêchent les connexions des terminaux aux ressources professionnelles via le réseau Wi-Fi.

Remarque : L'activation de cette fonctionnalité dirige tout le trafic de l'espace Travail qui utilise normalement le réseau Wi-Fi professionnel via une connexion sécurisé à BlackBerry Infrastructure. Cette fonctionnalité peut avoir une incidence sur l'utilisation des données de votre entreprise et les frais de réseau. Vérifier qu'il s'agit de la configuration privilégiée par votre entreprise avant d'activer cette fonctionnalité.

Avant de commencer : dans la stratégie informatique attribuée aux utilisateurs de terminaux BlackBerry 10, vérifiez que la règle de stratégie informatique Forcer le contrôle d'accès au réseau pour les applications professionnelles n'est pas sélectionnée.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Réseaux et connexions > Wi-Fi**.
3. Cliquez sur un profil Wi-Fi qui est attribué aux utilisateurs de terminaux BlackBerry 10.
4. Cliquez sur  .
5. Sur l'onglet **BlackBerry**, dans la section **Profils associés**, cochez la case **Utiliser un profil de connectivité d'entreprise avec connexion BlackBerry Secure Connect Plus pour les données professionnelles**.
6. Cliquez sur **Enregistrer**.

À la fin : si vous avez créé et attribué plusieurs profils Wi-Fi, répétez cette tâche, si nécessaire.

Référence connexe

BlackBerry 10 : paramètres de profil Wi-Fi

Résolution des problèmes BlackBerry Secure Connect Plus

Prenez note des problèmes suivants si vous avez des difficultés à configurer BlackBerry Secure Connect Plus.

L'adaptateur BlackBerry Secure Connect Plus passe à un état « Réseau non identifié » et cesse de fonctionner.

Cause

Ce problème peut survenir si vous redémarrez l'ordinateur qui héberge BlackBerry Secure Connect Plus.

Solution - Windows Server 2008 R2 et Windows Server 2008 R2 SP1

1. Dans le Gestionnaire de serveur, développez **Rôles > Stratégie réseau et services d'accès**. Cliquez avec le bouton droit sur **Accès à distance et routage** et cliquez sur **Désactiver le routage et l'accès à distance**.
2. Cliquez avec le bouton droit sur **Accès à distance et routage** et cliquez sur **Configurer et activer l'accès à distance et le routage**.
3. Exécutez l'Assistant de configuration en sélectionnant les options suivantes :
   a. Sur l'écran **Configuration**, sélectionnez **Network Address Translation (NAT)**.

   b. Sur l'écran **Connexion Internet NAT**, sélectionnez **Utiliser cette interface publique pour se connecter à Internet**. Vérifiez que BlackBerry Secure Connect Plus s'affiche dans la liste des interfaces réseau.
4. Développez **Rôles > Stratégie réseau et services d'accès > Accès à distance et routage > IPv4** et cliquez sur **NAT**. Ouvrez les propriétés de **connexion au réseau local** et sélectionnez **Interface publique connectée à Internet** et **Activer NAT sur cette interface**. Cliquez sur **OK**.
5. Ouvrez les propriétés **BlackBerry Secure Connect Plus** et sélectionnez **Interface privée connectée au réseau privé**. Cliquez sur **OK**.
6. Cliquez avec le bouton droit sur **Accès à distance et routage**, puis sur **Toutes les tâches > Redémarrer**.
7. Dans les services Windows, redémarrez le service **BlackBerry UEM – BlackBerry Secure Connect Plus**.

Dans Connexions réseau, il peut s'écouler quelques minutes avant que l'adaptateur BlackBerry Secure Connect Plus affiche une connexion réussie.

Téléchargez et installez le correctif indiqué dans l'article KB Windows Échec de la fonctionnalité NAT sur un serveur RRAS basé sur Windows Server 2008 R2 SP1.

Solution - Windows Server 2012

1. Dans le Gestionnaire de serveur, cliquez sur **Gérer > Ajouter des rôles et des fonctionnalités**. Cliquez sur **Suivant** jusqu'à accéder à l'écran **Fonctionnalités**. Développez **Outils d'administration de serveur distant > Outils d'administration de rôles** et sélectionnez **Outils de gestion des accès distants**. Exécutez l'Assistant pour installer les outils.
2. Cliquez sur **Outils > Gestion des accès distants**.
3. Sous **Configuration**, cliquez sur **DirectAccess et VPN** .
4. Sous **VPN** , cliquez sur **Ouvrir la gestion RRAS** .
5. Cliquez avec le bouton droit sur Routage et Serveur d'accès à distance, puis cliquez sur **Désactiver le routage et l'accès à distance**.
6. Cliquez avec le bouton droit sur Routage et Serveur d'accès à distance, puis cliquez sur **Configurer et activer l'accès à distance et le routage**.
7. Exécutez l'Assistant de configuration en sélectionnant les options suivantes :
   a. Sur l'écran **Configuration**, sélectionnez **Network Address Translation (NAT)**.
   b. Sur l'écran **Connexion Internet NAT**, sélectionnez **Utiliser cette interface publique pour se connecter à Internet**. Vérifiez que BlackBerry Secure Connect Plus s'affiche dans la liste des interfaces réseau.
8. Ouvrez **Routage et accès à distance >** <*nom_serveur*> **> IPv4** et cliquez sur **NAT**. Ouvrez les propriétés de **connexion au réseau local** et sélectionnez **Interface publique connectée à Internet** et **Activer NAT sur cette interface**. Cliquez sur **OK**.
9. Ouvrez les propriétés **BlackBerry Secure Connect Plus** et sélectionnez **Interface privée connectée au réseau privé**. Cliquez sur **OK**.
10. Cliquez avec le bouton droit sur Routage et serveur d'accès à distance, puis sur **Toutes les tâches > Redémarrer**.
11. Dans les services Windows, redémarrez le service **BlackBerry UEM – BlackBerry Secure Connect Plus**.

Téléchargez et installez le correctif indiqué dans l'article KB Windows Échec de la fonctionnalité NAT sur un serveur RRAS basé sur Windows Server 2012.

BlackBerry Secure Connect Plus ne démarre pas.

Cause possible

Les paramètres TCP/IPv4 pour l'adaptateur BlackBerry Secure Connect Plus sont peut-être incorrects.

Solution possible

Dans**Connexions réseau > Adaptateur BlackBerry Secure Connect Plus > Propriétés > Protocole IPv4 (TCP/IPv4) > Propriétés**, vérifiez que la case**Utiliser l'adresse IP suivante**est cochée, avec les valeurs par défaut suivantes

- Adresse IP : 172.16.0.1
- Masque de sous-réseau : 255.255.0.0

Si nécessaire, corrigez ces paramètres, puis redémarrez le serveur.

BlackBerry Secure Connect Plus cesse de fonctionner après une mise à niveau BlackBerry UEM

Cause

Ce problème peut se produire si le serveur n'a pas redémarré lors d'une mise à jour RRAS avant la mise à niveau de BlackBerry UEM vers la version 12.7, entraînant l'échec de la configuration de routage/NAT pendant la mise à niveau.

Solution

1. Redémarrez le serveur.
2. Dans les services Windows, arrêtez le service **BlackBerry UEM – BlackBerry Secure Connect Plus**.
3. En tant qu'administrateur, démarrez Windows PowerShell (64 bits) ou ouvrez une invite de commande.
4. Accédez à `<drive>:\Program Files\BlackBerry\UEMSecureConnectPlus\config\blackberry\` et exécutez **configureRRAS.bat**
5. Accédez à `<drive>:\Program Files\BlackBerry\UEMSecureConnectPlus\config\` et exécutez **configure-network-interface.cmd**
6. Dans les services Windows, démarrez le service **BlackBerry UEM – BlackBerry Secure Connect Plus**.

Afficher les fichiers journaux pour BlackBerry Secure Connect Plus

Deux fichiers journaux, situés par défaut à l'emplacement *<lecteur>*:\Program Files\BlackBerry\UEM\Logs*<aaaammjj>*, enregistrent les données concernant BlackBerry Secure Connect Plus :

- BSCP : consigne les données sur le composant serveur BlackBerry Secure Connect Plus
- BSCP-TS : consigne les données de connexion avec l'application BlackBerry Connectivity

Sur chaque ordinateur qui héberge une instance de BlackBerry Connectivity Node, les fichiers journaux de BlackBerry Secure Connect Plus se trouvent sous *<lecteur>*:\Program Files\BlackBerry\BlackBerry Connectivity Node\Logs*<aaaammjj>*.

Objectif	Fichier journal	Exemple
Vérifier queBlackBerry Secure Connect Plus est connecté à BlackBerry Infrastructure	BSCP	2015-01-19T13:17:47.540-0500 - BSCP {TcpClientConnectorNio#2} logging.feature.bscp.service|logging.component.bscp.pss.bcp [{}] - DEBUG Received Ping from [id: 0x60bce5a3, /10.90.84.22:28231 => stratos.bcp.bblabs.rim.net/206.53.155.152:3101], responding with Pong.2015-01-19T13:18:22.989-0500 - BSCP {ChannelPinger#1} logging.feature.bscp.service|logging.component.bscp.pss.bcp [{}] - DEBUG Sending Ping to [id: 0xb4a1677a, /10.90.84.22:28232 => stratos.bcp.bblabs.rim.net/206.53.155.152:3101]

Objectif	Fichier journal	Exemple
Vérifier que BlackBerry Secure Connect Plus est prêt à recevoir des appels depuis l'application BlackBerry Connectivity sur les terminaux	BSCP-TS	47: [14:13:21.231312][][3][AsioTurnSocket-1] Connected, host=68-171-243-141.rdns.blackberry.net 48: [14:13:21.239312][][3][AsioTurnSocket-1] Creating TURN allocation 49: [14:13:21.405121][][3][AsioTurnSocket-1] TURN allocation created
Vérifier que les terminaux utilisent le tunnel sécurisé	BSCP-TS	74: [10:39:45.746926][][3][Tunnel-2FFEC51E] Sent: 2130.6 KB (1733), Received: 201.9 KB (1370), Running: 00:07:00.139249
Vérifier que BlackBerry Secure Connect Plus utilise les paramètres de transcodeur personnalisé	BSCP	"configuration_def" : "com.rim.p2e.vpn.server.cipherSuite" }], "TRANSCODER", ["provider", { "configuration_def" : "com.rim.p2e.vpn.transcoder.provider" }, "server_library", { "configuration_def" : "com.rim.p2e.vpn.transcoder.server.library" }, "server_config_blob", { "configuration_def" : "com.rim.p2e.vpn.transcoder.server.configBlob" }]]
Vérifier que les terminaux utilisent un transcodeur personnalisé	BSCP-TS	37: [13:41:39.800371][][3][BlackBerry_1.0.0.1-25B212A5] Connected

Concepts connexes

Utilisation des fichiers journaux

Configuration de connexions réseau pour les applications BlackBerry Dynamics

Les profils de connectivité BlackBerry Dynamics définissent 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.

BlackBerry UEM comprend un profil de connectivité BlackBerry Dynamics par défaut doté de paramètres préconfigurés. Si aucun profil de connectivité BlackBerry Dynamics n'est attribué à un compte d'utilisateur ou à un groupe d'utilisateurs auquel appartient un utilisateur, BlackBerry UEM envoie le profil de connectivité BlackBerry Dynamics par défaut aux terminaux de l'utilisateur. BlackBerry UEM envoie automatiquement un profil de connectivité BlackBerry Dynamics à un terminal lorsqu'un utilisateur l'active, lorsque vous mettez à jour un profil de connectivité BlackBerry Dynamics attribué ou lorsqu'un profil de connectivité BlackBerry Dynamics différent est attribué à un compte d'utilisateur ou à un terminal.

Remarque : Pour les entreprises dotées d'un environnement BlackBerry Dynamics autonome existant, les profils de connectivité qui ont été configurés dans Good Control sont synchronisés de Good Control vers BlackBerry UEM lorsque vous procédez à la synchronisation entre Good Control et BlackBerry UEM. Dans BlackBerry UEM, les profils de connectivité seront automatiquement attribués aux mêmes utilisateurs. Pour plus d'informations sur la synchronisation de Good Control avec BlackBerry UEM, reportez-vous au guide de configuration.

Créer un profil de connectivité BlackBerry Dynamics

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Réseaux et connexions > Connectivité BlackBerrry Dynamics**.
3. Cliquez sur +.
4. Saisissez le nom et la description du profil.
5. Configurez les valeurs qui conviennent dans les paramètres de profil. Pour plus d'informations sur les différents paramètres de profil, reportez-vous à BlackBerry Dynamics : paramètres de profil de connectivité.
6. Pour ajouter un serveur d'applications pour une application BlackBerry Dynamics, reportez-vous à Ajouter un serveur d'applications à un profil de connectivité BlackBerry Dynamics.
7. Cliquez sur **Ajouter**.

À la fin : Si nécessaire, classez les profils.

Tâches connexes

Attribuer un profil ou une stratégie informatique à un groupe d'utilisateurs
Attribuer un profil ou une stratégie informatique à un compte d'utilisateur

Référence connexe

BlackBerry Dynamics : paramètres de profil de connectivité

Acheminement de toutes les données d'une application BlackBerry Dynamics via BlackBerry Proxy

Dans le profil de connectivité BlackBerry Dynamics, vous pouvez spécifier les serveurs auxquels les applications BlackBerry Dynamics de vos utilisateurs sont autorisées à accéder via le pare-feu à l'aide de BlackBerry Proxy.

Si vous sélectionnez l'option Acheminer tout le trafic, toutes les données d'une application BlackBerry Dynamics, quel que soit le domaine ou le sous-réseau, sont acheminées via BlackBerry Proxy.

L'acheminement de l'ensemble du trafic via BlackBerry Proxy présente les avantages suivants :

- Les navigateurs Web et les applications BlackBerry Dynamics sur les terminaux peuvent se connecter à n'importe quel serveur situé derrière le pare-feu et accessible via BlackBerry Proxy.
- Vous pouvez facilement surveiller le trafic de données entre les applications BlackBerry Dynamics et vos ressources.

Tenez compte des éléments suivants si vous sélectionnez l'option Acheminer tout le trafic :

- L'établissement de connexions à des serveurs sur Internet peut prendre plus longtemps.
- Si vous utilisez un proxy Web pour permettre l'accès à des sites externes et que vous avez configuré les paramètres de votre proxy pour limiter l'accès à certains sites, vous devez également définir les propriétés du proxy dans BlackBerry Proxy lorsque vous sélectionnez l'option Acheminer tout le trafic. Sinon, les applications ne pourront pas accéder aux sites externes. Pour plus d'informations sur la configuration des paramètres BlackBerry Proxy, consultez le contenu relatif à la configuration.
- BlackBerry Access peut être configuré avec un fichier PAC qui détermine les sites autorisés. Dans ce cas, le fichier PAC détermine les paramètres du proxy et l'option Acheminer tout le trafic n'a aucun impact. Pour plus d'informations, reportez-vous au Guide d'administration de BlackBerry Access.

Ajouter un serveur d'applications à un profil de connectivité BlackBerry Dynamics

Si vous disposez d'une application BlackBerry Dynamics prise en charge par un serveur d'applications ou par un serveur Web, vous pouvez spécifier le nom de ce serveur et la priorité des clusters BlackBerry Proxy utilisés pour communiquer avec elle.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Réseaux et connexions > Connectivité BlackBerrry Dynamics**.
3. Cliquez sur le profil de connectivité BlackBerry Dynamics auquel vous souhaitez ajouter un serveur d'applications.
4. Cliquez sur .
5. Sous **Serveurs d'applications**, cliquez sur **Ajouter**.
6. Sélectionnez l'application BlackBerry Dynamics à laquelle vous souhaitez ajouter un serveur d'applications.
7. Cliquez sur **Enregistrer**.
8. Dans le tableau de l'application, cliquez sur .
9. Dans le champ **Serveur**, spécifiez le nom de domaine complet (FQDN) du serveur d'applications.
10. Dans le champ **Port**, spécifiez le port du cluster BlackBerry Proxy utilisé pour accéder au serveur.
11. Dans la liste déroulante **Priorité**, spécifiez la priorité du cluster BlackBerry Proxy à utiliser pour accéder au domaine.
12. Dans la liste déroulante **Cluster de proxy BlackBerry principal**, spécifiez le nom du cluster BlackBerry Proxy que vous souhaitez définir comme cluster principal.
13. Dans la liste déroulante **Cluster de proxy BlackBerry secondaire**, spécifiez le nom du cluster BlackBerry Proxy que vous souhaitez définir comme cluster secondaire.
14. Cliquez sur **Enregistrer**.

Utilisation de BlackBerry 2FA pour les connexions sécurisées aux ressources essentielles

BlackBerry 2FA protège l'accès aux ressources critiques de votre organisation à l'aide de l'authentification à deux facteurs. BlackBerry 2FA utilise un mot de passe que les utilisateurs saisissent et une invite sécurisée sur leur terminal mobile chaque fois qu'ils tentent d'accéder à des ressources.

Vous gérez BlackBerry 2FA à partir de la console de gestion BlackBerry UEM, où vous utilisez un profil BlackBerry 2FA afin d'activer l'authentification à deux facteurs pour vos utilisateurs. Pour utiliser la dernière version de BlackBerry 2FA et ses fonctionnalités associées, telles que la pré-authentification et la résolution autonome, le profil BlackBerry 2FA doit être attribué à vos utilisateurs. Pour plus d'informations, consultez le contenu relatif à l'BlackBerry 2FA.

Configuration de l'authentification avec identification unique pour les terminaux

Le profil d'identification unique vous permet d'activer les terminaux BlackBerry 10 ainsi que certains terminaux iOS à des fins d'authentification automatique auprès de domaines et services Web de votre réseau d'entreprise. Une fois le profil d'identification unique attribué, l'utilisateur est invité à saisir un nom d'utilisateur et un mot de passe la première fois qu'il tente d'accéder au domaine que vous avez spécifié. Les informations de connexion sont enregistrées sur le terminal de l'utilisateur et automatiquement utilisées lorsqu'il tente d'accéder

à l'un des domaines sécurisés spécifiés dans le profil. Si l'utilisateur change de mot de passe, celui-ci lui est demandé lorsqu'il tente à nouveau d'accéder à un domaine sécurisé.

Vous pouvez également utiliser un profil d'identification unique pour spécifier les domaines approuvés pour les certificats que vous envoyez aux terminaux BlackBerry 10 à l'aide d'un profil SCEP. Une fois les domaines approuvés spécifiés, les utilisateurs BlackBerry 10 peuvent sélectionner les certificats requis lorsqu'ils accèdent à un domaine approuvé.

Les profils d'identification unique prennent en charge les types d'authentification suivants :

Type d'authentification	OS du terminal	S'applique à
• Kerberos	iOS	• Navigateur et applications • Pour limiter les applications pouvant utiliser le profil
	BlackBerry 10 OS	• Navigateur et applications de l'espace Travail
• NTLM • Spécifier les domaines approuvés pour les certificats SCEP	BlackBerry 10 OS	• Navigateur et applications de l'espace Travail

BlackBerry Dynamics apps also support Kerberos authentication. For more information, see Configuration de Kerberos pour les applications BlackBerry Dynamics.

Conditions préalables : utilisation de l'authentification Kerberos pour les terminaux

Pour les terminaux qui utilisent Kerberos, si un TGT valide est disponible, les utilisateurs ne sont pas invités à saisir leurs informations de connexion s'ils accèdent aux ressources internes de votre entreprise à partir du navigateur et des applications de l'espace Travail.

Pour configurer l'authentification Kerberos pour des domaines spécifiques, vous pouvez télécharger le fichier de configuration Kerberos de votre organisation (krb5.conf). BlackBerry UEM prend en charge l'implémentation Heimdal de Kerberos.

Vérifiez que le fichier de configuration répond aux exigences suivantes :

- La configuration Kerberos utiliser le protocole TCP par défaut au lieu du protocole UDP. Utilisez le préfixe tcp/ pour les hôtes KDC.
- Si votre organisation utilise un réseau VPN, la passerelle VPN doit autoriser le trafic vers les KDC.

Pour plus d'informations sur la configuration de l'authentification Kerberos pour les applications BlackBerry Dynamics, reportez-vous àConfiguration de Kerberos pour les applications BlackBerry Dynamics.

Authentification basée sur des certificats pour iOS 8 ou version ultérieure

Pour les terminaux exécutant iOS 8.0 ou version ultérieure, vous pouvez utiliser les certificats pour authentifier les terminaux iOS auprès des domaines et services Web du réseau de votre organisation. Vous pouvez ajouter un profil de certificat partagé, un profil SCEP ou un profil d'informations d'identification de l'utilisateur existant à un profil d'identification unique. Lorsque le navigateur ou les applications des terminaux iOS utilisent une identification unique basée sur des certificats, les utilisateurs sont automatiquement authentifiés (sous réserve de validité du certificat) et n'ont pas à entrer d'informations de connexion pour accéder aux domaines sécurisés que vous avez spécifiés.

Concepts connexes

Envoi du même certificat client à plusieurs terminaux
Utilisation d'un profil SCEP pour envoyer des certificats client sur des terminaux

Créer un profil d'identification unique

Les profils avec identification unique sont pris en charge pour les terminaux BlackBerry 10 et iOS. Pour configurer l'authentification d'identification unique pour les applications BlackBerry Dynamics, voir Configuration de Kerberos pour les applications BlackBerry Dynamics

Avant de commencer :

- Si vous souhaitez configurer l'authentification Kerberos pour les terminaux BlackBerry 10, localisez le fichier de configuration Kerberos de votre organisation (krb5.conf).
- Si vous souhaitez utiliser l'authentification basée sur des certificats pour les terminaux exécutant iOS 8.0 ou version ultérieure, créez le profil de certificat partagé ou le profil SCEP nécessaire.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Réseaux et connexions > Identification unique**.
3. Cliquez sur +.
4. Saisissez le nom et la description du profil.
5. Effectuez l'une des tâches suivantes :

Tâche	Étapes
Configurer l'authentification Kerberos pour les terminaux iOS	**a.** Cliquez sur l'onglet **iOS**. **b.** Sous **Kerberos**, cliquez sur +. **c.** Dans le champ **Nom**, saisissez le nom de la configuration. **d.** Dans le champ **Nom principal**, saisissez le nom de l'instance principale de Kerberos au format *<primary>*/*<instance>*@*<realm>* (par exemple, `user/admin@blackberry.example.com`). **e.** Dans le champ **Domaine**, saisissez le domaine Kerberos en majuscules (par exemple, **EXEMPLE.COM**). **f.** Dans le champ **Préfixe d'URL**, saisissez le préfixe des URL pour les sites auprès desquels vous souhaitez que les terminaux s'authentifient. Le préfixe doit commencer par http:// ou https:// et peut inclure des caractères génériques (*) (par exemple, **https://www.blackberry.exemple.com/***). **g.** Pour spécifier davantage de préfixes d'URL, cliquez sur + afin d'ajouter plus de champs. **h.** Pour limiter la configuration à des applications spécifiques, cliquez sur + en regard d'**Identificateurs d'applications**. Saisissez l'ID d'offre d'application. Vous pouvez utiliser un caractère générique (*) pour mettre en correspondance l'ID avec plusieurs applications. (par exemple, **com.company.***). **i.** Pour spécifier davantage d'identifiants d'application, cliquez sur + afin d'ajouter plus de champs. **j.** Si vous souhaitez que les terminaux exécutant iOS 8.0 ou version ultérieure utilisent l'authentification basée sur des certificats, dans la liste déroulante **Informations d'identification**, cliquez sur **Certificat**, **SCEP** ou **Informations d'identification de l'utilisateur**. Dans la liste déroulante des certificats, cliquez sur le profil de certificat que vous souhaitez utiliser. **k.** Cliquez sur **Ajouter**. **l.** Si nécessaire, répétez les étapes 2 à 11 pour ajouter une autre configuration Kerberos.
Configurer l'authentification Kerberos pou les terminaux BlackBerry 10	**a.** Cliquez sur l'onglet **BlackBerry**. **b.** Cliquez sur **Parcourir**. Accédez au fichier de configuration Kerberos de votre organisation et sélectionnez-le (krb5.conf).

Tâche	Étapes
Configurer l'authentification NTLM ou les domaines approuvés pour les certificats SCEP des terminaux BlackBerry 10	a. Cliquez sur l'onglet **BlackBerry**. b. Sous **Domaines approuvés**, cliquez sur +. c. Dans le champ **Nom**, saisissez le nom de la configuration. d. Dans le champ **Domaine**, saisissez un sous-domaine approuvé ou un hôte individuel où les informations d'identification pourront être utilisées à des fins d'authentification automatique. Saisissez le nom du serveur en tant que FQDN, nom d'hôte, alias ou adresse IP. Les noms DNS peuvent contenir des caractères génériques (*). e. Pour spécifier davantage de sous-domaines, cliquez sur + afin d'ajouter plus de champs. f. Cliquez sur **Ajouter**. g. Si nécessaire, répétez les étapes 2 à 6 pour ajouter un autre domaine approuvé.

6. Cliquez sur **Ajouter**.

À la fin : Si nécessaire, classez les profils.

Concepts connexes

Envoi du même certificat client à plusieurs terminaux
Utilisation d'un profil SCEP pour envoyer des certificats client sur des terminaux

Tâches connexes

Attribuer un profil ou une stratégie informatique à un groupe d'utilisateurs
Attribuer un profil ou une stratégie informatique à un compte d'utilisateur

Filtrage de contenu Web sur les terminaux iOS

Vous pouvez utiliser les profils de filtre de contenu Web pour limiter les sites Web qu'un utilisateur peut afficher dans Safari ou d'autres applications de navigation sur un terminal iOS. Vous pouvez attribuer des profils de filtre de contenu Web à des comptes d'utilisateur, groupes d'utilisateurs ou groupes de terminaux.

Lorsque vous créez un profil de filtre de contenu Web, vous pouvez choisir l'option de sites Web autorisés répondant aux normes de votre organisation en termes d'utilisation des terminaux mobiles.

Remarque : ce profil s'applique uniquement aux terminaux iOS supervisés.

Sites Web autorisés	Description
Sites Web spécifiques uniquement	Cette option permet d'accéder uniquement aux sites Web que vous spécifiez. Dans Safari, un signet est créé pour chaque site Web autorisé.

Sites Web autorisés	Description
Limiter le contenu pour adultes	Cette option permet le filtrage automatique afin d'identifier et de bloquer tout contenu inapproprié. Vous pouvez également inclure certains sites Web en utilisant les paramètres suivants : • URL autorisées : vous pouvez ajouter une ou plusieurs URL pour autoriser l'accès à certains sites Web. Les utilisateurs peuvent afficher les sites Web de cette liste même si le filtrage automatique en bloque l'accès. • URL non autorisées : vous pouvez ajouter une ou plusieurs URL pour refuser l'accès à certains sites Web. Les utilisateurs ne peuvent pas afficher les sites Web de cette liste même si le filtrage automatique en autorise l'accès.

Créer un profil de filtre de contenu Web

Lorsque vous créez un profil de filtre de contenu Web, chaque URL que vous spécifiez doit commencer par http:// ou https://. Si nécessaire, vous devez ajouter des entrées distinctes pour les versions http:// ou https:// d'une même URL. La résolution DNS n'intervient pas et dès lors, les sites Web limités restent accessibles (par exemple, si vous spécifiez http://www.exemple.com, les utilisateurs seront peut-être en mesure d'accéder au site Web à l'aide de leur adresse IP).

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Réseaux et connexions > Filtre de contenu Web**.
3. Cliquez sur +.
4. Saisissez le nom et la description du profil de filtre de contenu Web.
5. Effectuez l'une des tâches suivantes :

Tâche	Étapes
Autoriser l'accès à des sites Web spécifiques uniquement	a. Dans la liste déroulante **Sites Web autorisés**, vérifiez que le paramètre **Sites Web spécifiques uniquement** est sélectionné. b. Dans la section **Signets de sites Web spécifiques**, cliquez sur +. c. Procédez comme suit : 1. Dans le champ **URL**, saisissez l'adresse Web dont vous souhaitez autoriser l'accès. 2. Dans le champ **Chemin du signet**, vous pouvez également saisir le nom d'un dossier de signets (par exemple, /Work/). 3. Dans le champ **Titre**, saisissez le nom du site Web. 4. Cliquez sur **Ajouter**. d. Répétez les étapes 2 et 3 pour chaque site Web autorisé.

Tâche	Étapes
Limiter le contenu pour adultes	**a.** Dans la liste déroulante **Sites Web autorisés**, cliquez sur **Limiter le contenu pour adultes** pour activer le filtrage automatique. **b.** Vous pouvez également procéder comme suit : 1. Cliquez sur + en regard de **URL autorisées**. 2. Saisissez l'adresse Web dont vous souhaitez autoriser l'accès. 3. Répétez les étapes 2.a et 2.b pour chaque site Web autorisé. **c.** Vous pouvez également procéder comme suit : 1. Cliquez sur + en regard de **URL non autorisées**. 2. Saisissez l'adresse Web dont vous souhaitez refuser l'accès. 3. Répétez les étapes 3.a et 3.b pour chaque site Web limité.

6. Cliquez sur **Ajouter**.

Tâches connexes

Attribuer un profil ou une stratégie informatique à un groupe d'utilisateurs
Attribuer un profil ou une stratégie informatique à un compte d'utilisateur

Gérer les domaines de messagerie et les domaines Web pour les terminaux iOS

Vous pouvez utiliser un profil de domaines gérés pour définir certains domaines de messagerie et domaines Web en tant que « domaines gérés » internes à votre entreprise. Les profils de domaines gérés s'appliquent uniquement aux terminaux exécutant iOS 8 ou version ultérieure avec le type d'activation Contrôles MDM.

Après avoir attribué un profil de domaines gérés :

- Lorsqu'un utilisateur crée un e-mail et ajoute l'adresse électronique d'un destinataire dont le domaine n'est pas spécifié dans le profil de domaines gérés, le terminal affiche l'adresse en rouge pour avertir l'utilisateur que le destinataire est externe à l'entreprise. Le terminal n'empêche pas l'utilisateur d'envoyer des e-mails à des destinataires externes.
- Un utilisateur doit utiliser une application gérée par BlackBerry UEM pour afficher les documents provenant d'un domaine Web géré ou les documents téléchargés depuis un domaine Web géré. Le terminal n'empêche pas l'utilisateur de consulter des documents issus d'autres domaines Web. Le profil de domaines gérés s'applique uniquement au navigateur Safari.

Créer un profil de domaines gérés

Les profils de domaines gérés s'appliquent uniquement aux terminaux exécutant iOS 8 ou version ultérieure avec le type d'activation Contrôles MDM.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Réseaux et connexions > Domaines gérés**.
3. Cliquez sur +.
4. Saisissez le nom et la description du profil.
5. Dans le champ **Description**, tapez la description du profil.

6. Dans la section **Domaines de messagerie gérés**, cliquez sur +.
7. Dans le champ **Domaines de messagerie**, saisissez un nom de domaine de niveau supérieur (par exemple, `exemple.com` plutôt que `example.com/canada`).
8. Cliquez sur **Ajouter**.
9. Dans la section **Domaines Web gérés**, cliquez sur +. Pour obtenir des exemples de formats de domaines Web, reportez-vous à Managed Safari Web Domains in the iOS Developer Library (Domaines Web Safari gérés dans la Bibliothèque du développeur iOS).
10. Dans le champ **Domaines Web**, saisissez un nom de domaine.
11. Si vous souhaitez autoriser le remplissage automatique du mot de passe pour les domaines Web que vous avez spécifiés, cochez la case **Autoriser le remplissage automatique du mot de passe**. Cette option est uniquement prise en charge sur les terminaux iOS supervisés exécutant iOS 9.3 ou version ultérieure.
12. Cliquez sur **Ajouter**.
13. Cliquez sur **Ajouter**.

Tâches connexes

Attribuer un profil ou une stratégie informatique à un groupe d'utilisateurs
Attribuer un profil ou une stratégie informatique à un compte d'utilisateur

Créer un profil AirPrint

Vous pouvez configurer des profils AirPrint et les affecter à des terminaux qui exécutent iOS 7 ou version ultérieure afin que les utilisateurs n'aient pas besoin de configurer les imprimantes manuellement.Les profils AirPrint peuvent aider les utilisateurs à trouver les imprimantes qui prennent en charge AirPrint, qui sont accessibles, et pour lesquelles ils disposent des autorisations requises.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Réseaux et connexions > AirPrint**.
3. Cliquez sur +.
4. Tapez le nom et la description du profil AirPrint.
5. Dans la section **Configuration d'AirPrint**, cliquez sur +.
6. Dans le champ **Adresse IP**, saisissez l'adresse IP de l'imprimante ou du serveur AirPrint.
7. En option, dans le champ **Chemin de ressource**, saisissez le chemin de ressource de l'imprimante. Le chemin de ressource de l'imprimante correspond au paramètre `rp` du dossier Bonjour `_ipps.tcp`. Par exemple :
   - printers/<*gamme de l'imprimante*>
   - printers/<*modèle de l'imprimante*>
   - ipp/print
   - IPP_Printer
8. Cliquez sur **Ajouter**.
9. Cliquez sur **Ajouter**.

Tâches connexes

Attribuer un profil ou une stratégie informatique à un groupe d'utilisateurs

Attribuer un profil ou une stratégie informatique à un compte d'utilisateur

Configuration de profils AirPlay pour les terminaux iOS

Vous pouvez configurerAirPlay les profils et les affecter à des dispositifs qui fonctionnent sous iOS 7 ou version ultérieure. AirPlay est une fonctionnalité iOS qui vous permet d'afficher des photos ou de diffuser de la musique et des vidéos vers des terminaux AirPlay compatibles, tels que Apple TV, AirPort Express ou des haut-parleurs compatibles AirPlay.

Avec un profil AirPlay, vous pouvez définir des mots de passe pour des terminaux AirPlay spécifiques afin de vous assurer que seuls les utilisateurs autorisés peuvent y accéder. Vous pouvez également créer une liste autorisée de terminaux de destination pour vous assurer que les terminaux iOS supervisés ne peuvent se connecter qu'aux terminaux AirPlay que vous spécifiez. Vous pouvez attribuer des profils AirPlay à des comptes d'utilisateur, groupes d'utilisateurs ou groupes de terminaux.

Exemple : Définir un mot de passe pour un terminal AirPlay

Si vous souhaitez limiter l'accès à un terminal AirPlay spécifique, ajoutez le nom du terminal et définissez un mot de passe.Les utilisateurs du terminal iOS possédant ce profil AirPlay devront saisir le mot de passe pour accéder à ce terminal AirPlay. Notez que le mot de passe est requis par le profil AirPlay, et non par le terminal AirPlay lui-même.Les utilisateurs de terminaux iOS qui ne disposent pas de ce profil AirPlay peuvent toujours accéder au terminal AirPlaysans le mot de passe.

Exemple : Créer une liste de terminaux AirPlay pour terminaux iOS supervisés

Si vous souhaitez autoriser les terminaux iOS supervisés à diffuser du contenu uniquement sur certains terminaux, vous pouvez ajouter l'ID du terminal. Les terminaux supervisés ne seront en mesure de diffuser du contenu que sur les terminaux que vous spécifiez. Les terminaux qui ne sont pas supervisés ne seront pas affectés par cette liste.

Créer un profil AirPlay

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Réseaux et connexions > AirPlay**.
3. Cliquez sur +.
4. Tapez le nom et la description du profil AirPlay.
5. Cliquez sur + dans la section **Terminaux de destination autorisés**.
6. Dans le champ **Nom du terminal**, saisissez le nom du terminal AirPlay que vous souhaitez ajouter. Vous pouvez trouver le nom du terminal AirPlay dans les paramètres du terminal ou vous pouvez rechercher le nom du terminal en sélectionnant **AirPlay** dans le centre de contrôle d'un terminal iOS pour afficher la liste des terminaux AirPlay disponibles autour de vous.
7. Dans le champ **Mot de passe**, saisissez un mot de passe.
8. Cliquez sur **Ajouter**.
9. Cliquez sur + dans la section **Terminaux de destination autorisés pour les terminaux supervisés**.
10. Dans le champ **ID du terminal**, saisissez l'ID du terminal AirPlay que vous souhaitez ajouter. Vous trouverez l'ID du terminal AirPlay dans ses paramètres. Pour plus d'informations sur la recherche de l'ID du terminal, reportez-vous à la documentation de votre produit Apple.
11. Cliquez sur **Ajouter**.

Tâches connexes

Attribuer un profil ou une stratégie informatique à un groupe d'utilisateurs
Attribuer un profil ou une stratégie informatique à un compte d'utilisateur

Contrôle de l'utilisation du réseau pour les applications professionnelles sur les terminaux iOS

Vous pouvez utiliser un profil d'utilisation du réseau pour contrôler la façon dont les applications professionnelles sur des terminaux exécutant iOS 9 ou version ultérieure utilisent le réseau mobile.

Pour mieux gérer l'utilisation du réseau, vous pouvez empêcher les applications de transférer des données lorsque des terminaux sont connectés au réseau mobile ou lorsque des terminaux sont en itinérance. Vous pouvez spécifier les mêmes règles d'utilisation du réseau pour toutes les applications professionnelles, ou vous pouvez spécifier les règles pour certaines applications professionnelles. Un profil d'utilisation de réseau peut contenir des règles pour une ou plusieurs applications. Si vous ne spécifiez pas d'applications dans le profil, les règles sont appliquées à toutes les applications professionnelles.

Créer un profil d'utilisation du réseau

Les règles dans un profil d'utilisation de réseau s'appliquent aux applications professionnelles seulement. Si vous n'avez pas attribué d'applications à des utilisateurs ou groupes, le profil d'utilisation du réseau ne possède pas d'effet.

Avant de commencer : ajoutez des applications à la liste d'applications et attribuez-les aux groupes d'utilisateurs ou aux comptes d'utilisateurs.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Réseaux et connexions > Utilisation du réseau**.
3. Cliquez sur +.
4. Saisissez le nom et la description du profil.
5. Cliquez sur +.
6. Effectuez l'une des opérations suivantes :
   - Sélectionnez **Ajouter une application**, puis cliquez sur une application de la liste.
   - Sélectionnez **Spécifier l'ID du package d'applications** et saisissez l'ID. L'ID du package d'applications est également appelé ID d'offre. Vous pouvez trouver l'ID de package de l'application en cliquant sur l'application dans la liste des applications. Utilisez un caractère générique (*) pour mettre en correspondance l'ID avec plusieurs applications. (Par exemple, **com.company.***).
7. Pour empêcher l'application ou les applications d'utiliser des données lorsque le terminal est en itinérance, décochez la case **Autoriser l'itinérance des données**.
8. Pour empêcher l'application ou les applications d'utiliser des données lorsque le terminal est connecté au réseau mobile, décochez la case **Autoriser les données cellulaires**.
9. Cliquez sur **Ajouter**.
10. Répétez les étapes 5 à 8 pour chacune des applications que vous souhaitez ajouter à la liste.

À la fin : Si nécessaire, classez les profils.

Tâches connexes

Attribuer un profil ou une stratégie informatique à un groupe d'utilisateurs
Attribuer un profil ou une stratégie informatique à un compte d'utilisateur

E-mail, calendrier et contacts

Vous pouvez utiliser des profils pour gérer la manière dont les terminaux reçoivent des e-mails, données du calendrier et informations de contact. Vous pouvez spécifier les paramètres des terminaux BlackBerry 10, iOS, macOS, Android et Windows dans le même profil, puis attribuer le profil à des comptes d'utilisateur, groupes d'utilisateurs ou groupes de terminaux.

Si votre entreprise utilise BlackBerry Work pour gérer les e-mails, le calendrier et les contacts pour les terminaux des utilisateurs, configurez l'application BlackBerry Work plutôt que le profil de messagerie. Pour plus d'informations sur la gestion de BlackBerry Work, consultez Gestion des applications BlackBerry Dynamics et le Guide d'administration de BlackBerry Work.

Configuration d'une messagerie professionnelle pour les terminaux

Vous pouvez utiliser les profils de messagerie pour spécifier la manière dont les terminaux se connectent au serveur de messagerie de votre organisation et synchronisent les e-mails, les entrées de calendrier et les données de l'organiseur à l'aide de Exchange ActiveSync ou IBM Notes Traveler.

Si vous souhaitez utiliser Exchange ActiveSync, notez ce qui suit :

- Pour une sécurité renforcée de la messagerie, vous pouvez activer S/MIME pour les terminaux iOS et Android. Vous pouvez activer S/MIME ou PGP pour les terminaux BlackBerry 10. PGP est pris en charge par BlackBerry 10 OS version 10.3.1 ou ultérieure.
- Si vous activez S/MIME, vous pouvez utiliser d'autres profils pour permettre aux terminaux de récupérer automatiquement des certificats S/MIME et en vérifier l'état.

Si vous souhaitez utiliser Notes Traveler, notez ce qui suit :

- Pour utiliser Notes Traveler avec les terminaux iOS, vous devez activer BlackBerry Secure Gateway.
- La synchronisation des données To Do est uniquement prise en charge sur les terminaux BlackBerry 10. Elle utilise le protocole de communication SyncML sur le serveur Notes Traveler.
- Pour une sécurité renforcée de la messagerie sur les terminaux BlackBerry 10, seul le cryptage IBM Notes est pris en charge (S/MIME n'est pas pris en charge).
- Pour utiliser Notes Traveler avec l'application cliente IBM Verse :
  - pour les terminaux Samsung KNOX, vous devez configurer les paramètres de IBM Verse dans le profil de messagerie
  - pour les terminaux Android dotés d’un profil professionnel, vous devez configurer les paramètres de IBM Verse à l’aide de la configuration de l'application

Vous pouvez également utiliser les profils de messagerie IMAP/POP3 pour spécifier la manière dont les terminaux iOS, macOS, Android et Windows se connectent aux serveurs de messagerie IMAP ou POP3 et synchronisent les e-mails. Les terminaux activés pour utiliser KNOX MDM ne prennent pas en charge les protocoles IMAP ou POP3.

Vous pouvez utiliser BlackBerry Work plutôt qu'un profil de messagerie pour gérer les e-mails, le calendrier et les contacts pour les terminaux des utilisateurs. Pour plus d'informations sur la gestion de BlackBerry Work, consultez Gestion des applications BlackBerry Dynamics et le Guide d'administration de BlackBerry Work.

Créer un profil de messagerie

Les paramètres de profil requis varient pour chaque type de terminal et dépendent du serveur de messagerie dans l'environnement de votre entreprise.

Avant de commencer :

- Si vous utilisez l'authentification basée sur des certificats entre les terminaux et le serveur de messagerie, vous devez créer un profil de certificat d'autorité de certification et l'attribuer aux utilisateurs. Vous devez également veiller à ce que les terminaux disposent d'un certificat client approuvé.
- Pour appliquer automatiquement un profil de messagerie à un terminal Android, celui-ci doit respecter l'un des critères suivants. Si le terminal ne satisfait aucun de ces critères, BlackBerry UEM envoie toujours le profil de messagerie aux terminaux Android, mais l'utilisateur doit configurer manuellement la connexion au serveur de messagerie :
  - Terminaux Android dotés d'un profil professionnel
  - Terminaux Samsung KNOX et Samsung KNOX Workspace
  - Motorola
- Si vous prévoyez d'utiliser BlackBerry Secure Gateway pour fournir une connexion sécurisée au serveur de messagerie de votre entreprise par le biais de BlackBerry Infrastructure et BlackBerry UEM pour les terminaux iOS dotés du type d'activation Contrôles MDM, vérifiez que votre entreprise dispose des licences BlackBerry UEM appropriées. Pour plus d'informations, reportez-vous au contenu relatif à la gestion des licences.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **E-mail, calendrier et contacts > E-mail**.
3. Cliquez sur +.
4. Saisissez le nom et la description du profil.
5. Si nécessaire, saisissez le nom de domaine du serveur de messagerie. Si le profil concerne plusieurs utilisateurs pouvant se trouver dans différents domaines Microsoft Active Directory, vous pouvez utiliser la variable `%UserDomain%`.
6. Dans le champ **Adresse électronique**, effectuez l'une des opérations suivantes :
   - Si le profil concerne un utilisateur, saisissez l'adresse électronique de l'utilisateur.
   - Si le profil concerne plusieurs utilisateurs, saisissez `%UserEmailAddress%`.
7. Saisissez le nom d'hôte ou l'adresse IP du serveur de messagerie.
8. Dans le champ **Nom d'utilisateur**, effectuez l'une des opérations suivantes :
   - Si le profil concerne un seul utilisateur, indiquez le nom d'utilisateur.
   - Si le profil concerne plusieurs utilisateurs, saisissez `%UserName%`.
   - Si le profil concerne plusieurs utilisateurs dans un environnement IBM Notes Traveler, saisissez `%UserDisplayName%`.
9. Si vous avez configuré des groupes de serveurs pour diriger le trafic BlackBerry Secure Gateway ou le trafic BlackBerry Gatekeeping Service vers une connexion régionale spécifique de BlackBerry Infrastructure, dans la liste déroulante **Groupe de serveurs BlackBerry Secure Gateway Service**, cliquez sur le groupe de serveurs approprié.

   Pour plus d'informations sur les groupes BlackBerry Connectivity Node et les groupes de serveurs, reportez-vous au contenu relatif à la planification et au contenu relatif à l'installation et à la mise à niveau
10. Cliquez sur l'onglet correspondant à chaque type de terminal de votre organisation et configurez les valeurs appropriées pour chaque paramètre de profil. Pour plus de détails sur chaque paramètre de profil, reportez-vous à la section Paramètres de profil de messagerie.
11. Cliquez sur **Ajouter**.

À la fin : Si nécessaire, classez les profils.

Concepts connexes

Paramètres de profil de messagerie

Envoi de certificats aux terminaux à l'aide de profils

Tâches connexes

Attribuer un profil ou une stratégie informatique à un groupe d'utilisateurs
Attribuer un profil ou une stratégie informatique à un compte d'utilisateur

Créer un profil de messagerie IMAP/POP3

Les paramètres de profil requis varient pour chaque type de terminal et dépendent des paramètres que vous sélectionnez.

Remarque : BlackBerry UEM envoie le profil de messagerie aux terminaux Android, mais l'utilisateur doit configurer manuellement la connexion au serveur de messagerie.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **E-mail, calendrier et contacts > E-mail IMAP/POP3**.
3. Cliquez sur +.
4. Saisissez le nom et la description du profil.
5. Dans le champ **Type de messagerie**, sélectionnez le type de protocole de messagerie.
6. Dans le champ **Adresse électronique**, effectuez l'une des opérations suivantes :
   - Si le profil concerne un utilisateur, saisissez l'adresse électronique de l'utilisateur.
   - Si le profil concerne plusieurs utilisateurs, saisissez `%UserEmailAddress%`.
7. Dans la section **Paramètres du courrier entrant**, saisissez le nom d'hôte ou l'adresse IP du serveur de messagerie pour la réception du courrier.
8. Si nécessaire, saisissez le port pour la réception du courrier.
9. Dans le champ **Nom d'utilisateur**, effectuez l'une des opérations suivantes :
   - Si le profil concerne un seul utilisateur, indiquez le nom d'utilisateur.
   - Si le profil concerne plusieurs utilisateurs, saisissez `%UserName%`.
10. Dans la section **Paramètres du courrier sortant**, saisissez le nom d'hôte ou l'adresse IP du serveur de messagerie pour l'envoi du courrier.
11. Si nécessaire, saisissez le port pour l'envoi du courrier.
12. Si nécessaire, sélectionnez **Authentification requise pour les e-mails sortants** et spécifiez les informations d'identification utilisées pour l'envoi du courrier.
13. 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 Paramètres de profil de messagerie IMAP/POP3.
14. Cliquez sur **Ajouter**.

Concepts connexes

Paramètres de profil de messagerie IMAP/POP3

Tâches connexes

Attribuer un profil ou une stratégie informatique à un groupe d'utilisateurs
Attribuer un profil ou une stratégie informatique à un compte d'utilisateur

Protéger les données de la messagerie à l'aide de BlackBerry Secure Gateway

Par le biais de BlackBerry Infrastructure et BlackBerry UEM, BlackBerry Secure Gateway fournit une connexion sécurisée au serveur de messagerie de votre entreprise pour les terminaux iOS activés via Contrôles MDM.

L'activation de BlackBerry Secure Gateway permet aux terminaux activés via Contrôles MDM d'envoyer et de recevoir des e-mails professionnels sans que vous ayez à exposer votre serveur de messagerie à l'extérieur du pare-feu ou à localiser votre serveur de messagerie dans une zone démilitarisée.

Si vous envisagez d'utiliser BlackBerry Secure Gateway, vérifiez que votre entreprise dispose des licences BlackBerry UEM adéquates. Pour plus d'informations, reportez-vous au contenu relatif à la gestion des licences.

Pour activer BlackBerry Secure Gateway, sélectionnez le paramètre Activer BlackBerry Secure Gateway dans le profil de messagerie.

Si vous avez configuré des groupes de serveurs pour prendre en charge les connexions régionales à BlackBerry Infrastructure, vous pouvez diriger le trafic de BlackBerry Secure Gateway vers une connexion régionale spécifique en associant le profil de messagerie au groupe de serveurs approprié.

Extension de la sécurité de la messagerie à l'aide de S/MIME

Vous pouvez renforcer la sécurité de la messagerie des utilisateurs de terminaux BlackBerry 10, iOS et Android en activant S/MIME. S/MIME propose une méthode standard de cryptage et de signature des e-mails. Les utilisateurs peuvent crypter, signer ou crypter et signer les e-mails à l'aide de la protection S/MIME s'ils utilisent un compte de messagerie professionnel prenant en charge les messages protégés par S/MIME sur les terminaux. S/MIME ne peut pas être activé pour les adresses électroniques personnelles.

Les utilisateurs peuvent stocker les certificats S/MIME des destinataires sur leurs terminaux. Les utilisateurs peuvent stocker leurs clés privées sur leurs terminaux ou sur une carte à puce.

Vous pouvez activer S/MIME pour les utilisateurs dans un profil de messagerie. Vous pouvez contraindre les utilisateurs de terminaux BlackBerry 10 à utiliser S/MIME, mais pas les utilisateurs de terminaux iOS ou Android. Lorsque l'utilisation de S/MIME est facultative, un utilisateur peut activer S/MIME sur le terminal et choisir de crypter, signer ou crypter et crypter et signer les e-mails.

Les paramètres S/MIME sont prioritaires sur les paramètres PGP. Lorsque la prise en charge S/MIME est définie sur Requise, les paramètres PGP sont ignorés.

Récupération des certificats S/MIME

Vous pouvez utiliser les profils de récupération de certificat pour autoriser les terminaux à rechercher et récupérer les certificats S/MIME des destinataires à partir des serveurs de certificats LDAP. Si le certificat S/MIME ne figure pas déjà dans un magasin de certificats du terminal, le terminal le récupère et l'importe automatiquement dans le magasin de certificats.

Type de terminal	Description
BlackBerry 10	Les terminaux recherchent chaque serveur de certificats LDAP que vous spécifiez dans le profil et récupèrent le certificat S/MIME. S'il existe plusieurs certificats S/MIME et si un terminal n'est pas en mesure de déterminer celui qui a la préférence, le terminal affiche tous les certificats S/MIME pour permettre à l'utilisateur de faire son choix. Vous pouvez demander à ce que les terminaux utilisent l'authentification simple ou l'authentification Kerberos pour s'authentifier auprès des serveurs de certificats LDAP. Si vous souhaitez que les terminaux utilisent l'authentification simple, vous pouvez inclure les informations d'authentification requises dans des profils de récupération de certificat pour permettre aux terminaux de s'authentifier automatiquement auprès des serveurs de certificats LDAP. Si vous souhaitez que les terminaux utilisent l'authentification Kerberos, vous pouvez inclure les informations d'authentification requises dans des profils de récupération de certificat pour permettre aux terminaux exécutant BlackBerry 10 OS version 10.3.1 ou ultérieure de s'authentifier automatiquement auprès des serveurs de certificats LDAP. Sinon, le terminal demande à l'utilisateur les informations d'authentification requises la première fois que le terminal tente de s'authentifier auprès d'un serveur de certificats LDAP. Pour les terminaux exécutant BlackBerry 10 OS versions 10.2.1 à 10.3, le terminal invite l'utilisateur à fournir les informations d'authentification requises la première fois que le terminal tente de s'authentifier auprès d'un serveur de certificats LDAP. Si vous mettez en œuvre l'authentification Kerberos pour l'extraction du certificat S/MIME, vous devez attribuer un profil d'identification unique aux utilisateurs ou groupes d'utilisateurs applicables. Pour plus d'informations sur la création et l'attribution d'un profil d'identification unique, reportez-vous à Configuration de l'authentification avec identification unique pour les terminaux.

Si vous ne créez pas de profil de récupération de certificat et ne l'attribuez pas aux comptes d'utilisateur, groupes d'utilisateurs ou de groupes de terminaux, les utilisateurs doivent manuellement importer les certificats S/MIME à partir d'une pièce jointe à un e-mail professionnel ou d'un ordinateur.

Créer un profil de récupération de certificat

Avant de commencer :

- pour permettre aux terminaux d'approuver les serveurs de certificats LDAP lorsqu'ils établissent des connexions sécurisées, vous devrez peut-être distribuer les certificats d'autorité de certification aux terminaux. Si nécessaire, créez des profils de certificat d'autorité de certification et attribuez-les aux comptes d'utilisateur, groupes d'utilisateurs ou groupes de terminaux. Pour plus d'informations sur les certificats CA, reportez-vous à Envoi de certificats CA à des terminaux.
- Si vous mettez en œuvre l'authentification Kerberos pour l'extraction du certificat S/MIME, vous devez attribuer un profil d'identification unique aux utilisateurs ou groupes d'utilisateurs applicables. Pour plus d'informations sur les profils d'identification unique, reportez-vous à Configuration de l'authentification avec identification unique pour les terminaux.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Certificats > Récupération de certificat**.

3. Cliquez sur +.
4. Saisissez le nom et la description du profil de récupération de certificat.
5. Dans la table, cliquez sur +.
6. Dans le champ **URL du service**, saisissez le FQDN d'un serveur de certificats LDAP au format ldap://<*fqdn*>:<*port*>. (Par exemple, ldap://serveur01.exemple.com:389).
7. Dans le champ **Base de recherche**, saisissez le DN de base correspondant au point de départ des recherches effectuées sur le serveur de certificats LDAP.
8. Dans la liste déroulante **Étendue de la recherche**, effectuez l'une des opérations suivantes :
   - Pour rechercher l'objet de base uniquement (DN de base), cliquez sur **Base**. Cette option correspond à la valeur par défaut.
   - Pour rechercher un niveau en-dessous de l'objet de base, mais pas l'objet de base lui-même, cliquez sur **Un niveau**.
   - Pour rechercher l'objet de base et tous les niveaux situés en-dessous, cliquez sur **Sous-arborescence.**
   - Pour rechercher tous les niveaux en-dessous de l'objet de base, mais pas l'objet de base lui-même, cliquez sur **Enfants**.
9. Si une authentification est requise, procédez comme suit :
   a) Dans la liste déroulante **Type d'authentification**, cliquez sur **Simple** ou **Kerberos**.
   b) Dans le champ **ID utilisateur LDAP**, saisissez le DN d'un compte doté d'autorisations de recherche sur le serveur de certificats LDAP (par exemple, cn=admin,dc=exemple,dc=com).
   c) Dans le champ **Mot de passe LDAP**, saisissez le mot de passe du compte doté des autorisations de recherche sur le serveur de certificats LDAP.
10. Si nécessaire, cochez la case **Utiliser une connexion sécurisée**.
11. Dans le champ **Délai de connexion**, saisissez le délai, en secondes, durant lequel le terminal attend la réponse du serveur de certificats LDAP.
12. Cliquez sur **Ajouter**.
13. Répétez les étapes 5 à 11 pour chaque serveur de certificats LDAP.
14. Cliquez sur **Ajouter**.

À la fin :

- Pour permettre aux terminaux BlackBerry 10 de vérifier l'état du certificat, créez un profil OCSP ou CRL.
- Si nécessaire, classez les profils.

Tâches connexes

Créer un profil OCSP
Créer un profil CRL
Attribuer un profil ou une stratégie informatique à un groupe d'utilisateurs
Attribuer un profil ou une stratégie informatique à un compte d'utilisateur

Identification de l'état des certificats S/MIME sur les terminaux

Vous pouvez utiliser des profils OCSP et CRL pour permettre aux terminaux BlackBerry 10 de vérifier l'état des certificats S/MIME. Vous pouvez attribuer un profil OCSP et un profil CRL à des comptes d'utilisateur, groupes d'utilisateurs ou groupes de terminaux.

Les terminaux BlackBerry 10 recherchent chaque répondeur OCSP que vous spécifiez dans un profil OCSP et récupère l'état des certificats S/MIME. Les terminaux exécutant BlackBerry 10 OS version 10.3.1 ou ultérieure

peuvent envoyer des demandes d'état de certificat à BlackBerry UEM, et vous pouvez utiliser des profils CRL pour configurer BlackBerry UEM afin de rechercher l'état des certificats S/MIME via HTTP, HTTPS ou LDAP.

Si vous utilisez Exchange ActiveSync pour obtenir des certificats, les terminaux iOS et Android utilisent Exchange ActiveSync pour vérifier l'état de certificats S/MIME. Si vous utilisez LDAP pour obtenir des certificats, les terminaux iOS et Android utilisent OCSP pour vérifier l'état de certificats.Les terminaux Android et iOS n'utilisent pas de profils OCSP. Les terminaux vérifient le répondeur OCSP du certificat.

Pour plus d'informations sur les indicateurs d'état de certificat, consultez le guide de l'utilisateur du terminal et consultez la section relative aux icônes d'e-mails sécurisés.

Créer un profil OCSP

Les profils OCSP sont pris en charge sur les terminaux BlackBerry 10.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Certificats > OCSP**.
3. Cliquez sur +.
4. Saisissez le nom et la description du profil OCSP.
5. Procédez comme suit :
   a) Dans le tableau, cliquez sur +.
   b) Dans le champ **URL du service**, saisissez l'adresse Web d'un répondeur OCSP.
   c) Dans le champ **Délai de connexion**, saisissez le délai, en secondes, durant lequel le terminal attend la réponse OCSP.
   d) Cliquez sur **Ajouter**.
6. Répétez l'étape 4 pour chaque répondeur OCSP.
7. Cliquez sur **Ajouter**.

À la fin : Si nécessaire, classez les profils.

Tâches connexes

Attribuer un profil ou une stratégie informatique à un groupe d'utilisateurs
Attribuer un profil ou une stratégie informatique à un compte d'utilisateur

Créer un profil CRL

Les profils CRL sont pris en charge sur les terminaux BlackBerry 10 et les terminaux BlackBerry optimisés par Android avec Android version 7.0 et ultérieure.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Certificats > CRL**.
3. Cliquez sur +.
4. Saisissez le nom et la description du profil CRL.
5. Pour permettre aux terminaux d'utiliser les URL définies dans le certificat, cochez la case **Utiliser des répondeurs d'extension de certificat**.
6. Effectuez l'une des tâches suivantes :

Tâche	Étapes
Spécifier une configuration HTTP CRL	**a.** Dans la section **HTTP pour CRL**, cliquez sur +. **b.** Saisissez le nom et la description de la configuration HTTP CRL. **c.** Dans le champ **URL du service**, saisissez l'adresse Web d'un répondeur HTTP ou HTTPS. **d.** Cliquez sur **Ajouter**. **e.** Répétez les étapes 1 à 4 pour chaque serveur HTTP ou HTTPS.
Spécifier une configuration LDAP CRL	**a.** Dans la section **LDAP pour CRL**, cliquez sur +. **b.** Saisissez le nom et la description de la configuration LDAP CRL. **c.** Dans le champ **URL du service**, saisissez le FQDN d'un serveur LDAP au format ldap://<*fqdn*>:<*port*> (par exemple, ldap://server01,exemple.com:389). Pour les connexions sécurisées, utilisez le format ldaps://<*fqdn*>:<*port*>. **d.** Dans le champ **Base de recherche**, saisissez le DN de base correspondant au point de départ des recherches effectuées sur le serveur LDAP. **e.** Si nécessaire, cochez la case **Utiliser une connexion sécurisée**. **f.** Dans le champ **ID utilisateur LDAP**, saisissez le DN d'un compte doté d'autorisations de recherche sur le serveur LDAP (par exemple, cn=admin,dc=example,dc=com). **g.** Dans le champ **Mot de passe LDAP**, saisissez le mot de passe du compte doté des autorisations de recherche sur le serveur LDAP. **h.** Cliquez sur **Ajouter**. **i.** Répétez les étapes 1 à 8 pour chaque serveur LDAP.

7. Cliquez sur **Ajouter**.

À la fin : Si nécessaire, classez les profils.

Tâches connexes

Attribuer un profil ou une stratégie informatique à un groupe d'utilisateurs
Attribuer un profil ou une stratégie informatique à un compte d'utilisateur

Extension de la sécurité de la messagerie avec PGP

Pour les terminaux exécutant BlackBerry 10 OS version 10.3.1 ou ultérieure, vous pouvez étendre la sécurité de la messagerie des utilisateurs de terminaux en activant PGP. PGP protège les e-mails des terminaux utilisant le format OpenPGP. Les utilisateurs peuvent signer, crypter ou signer et crypter des e-mails avec la protection PGP lorsqu'ils utilisent une adresse électronique professionnelle. PGP ne peut pas être activé pour les adresses électroniques personnelles.

Vous pouvez activer PGP pour les utilisateurs dans un profil de messagerie. Vous pouvez contraindre les utilisateurs de terminaux BlackBerry 10 à utiliser PGP, interdire l'utilisation de PGP ou la rendre facultative. Lorsque l'utilisation de PGP est facultative (paramètre par défaut), un utilisateur peut activer PGP sur le terminal et choisir de crypter, signer ou crypter et crypter et signer les e-mails.

Pour signer et crypter les e-mails, les utilisateurs doivent disposer des clés PGP pour chaque destinataire sur leurs terminaux. Les utilisateurs peuvent stocker les clés PGP en important des fichiers depuis un e-mail professionnel.

Vous pouvez configurer PGP à l'aide des paramètres de profil de messagerie qui conviennent.

Référence connexe

BlackBerry 10 : paramètres de profil de messagerie

Application des e-mails sécurisés à l'aide de la classification de messages

La classification de messages permet à votre organisation de spécifier et d'appliquer des stratégies de sécurité des e-mails et d'ajouter des marques visuelles à des e-mails sur des terminaux BlackBerry 10. Vous pouvez utiliser BlackBerry UEM pour fournir aux utilisateurs de terminaux BlackBerry 10 des options de classification de messages similaires à celles que vous avez mises à leur disposition pour les applications de messagerie de leur ordinateur. Vous pouvez définir les règles suivantes pour qu'elles s'appliquent aux messages sortants, en fonction des classifications des messages :

- Ajouter une étiquette pour identifier la classification de message (par exemple : confidentiel)
- Ajouter un marqueur visuel à la fin de la ligne d'objet (par exemple : [C])
- Ajouter du texte au début ou à la fin du corps d'un e-mail (par exemple : ce message a été classé comme confidentiel)
- Définir des options S/MIME ou PGP (par exemple : signer et crypter)
- Définir une classification par défaut

Pour les terminaux qui exécutent BlackBerry 10 OS version 10.3.1 ou ultérieure, vous pouvez utiliser la classification de messages pour exiger que les utilisateurs signent, cryptent ou signent et cryptent les e-mails, ou qu'ils ajoutent des marques visuelles aux e-mails qu'ils envoient de leurs terminaux. Vous pouvez utiliser des profils de messagerie pour les fichiers de configuration de classification de messages (avec extensions de noms de fichiers .json) à envoyer aux terminaux des utilisateurs. Lorsque les utilisateurs répondent à des e-mails avec classification de messages ou rédigent des e-mails sécurisés, la configuration de classification de messages détermine les règles de classification que les terminaux doivent appliquer aux messages sortants.

Les options de protection des messages sur un terminal sont limitées aux types de cryptage et de signature numérique autorisés sur le terminal. Lorsqu'un utilisateur applique une classification de messages à un e-mail sur un terminal, il doit sélectionner l'un des types de protection de message autorisés par cette classification ou accepter le type de protection de message par défaut. Si un utilisateur sélectionne une classification de messages nécessitant la signature, le cryptage ou la signature et le cryptage de l'e-mail et si le terminal ne dispose pas d'une configuration S/MIME ou PGP, l'utilisateur ne peut pas envoyer l'e-mail.

Les paramètres S/MIME et PGP sont prioritaires sur la classification de messages. Les utilisateurs peuvent augmenter, mais pas diminuer, les niveaux de classification de messages sur leurs terminaux. Les niveaux de classification de messages sont déterminés par les règles d'e-mails sécurisés de chaque classification.

Lorsque la classification de messages est activée, les utilisateurs ne peuvent pas utiliser BlackBerry Assistant pour envoyer des e-mails à partir de leurs terminaux.

Vous pouvez configurer la classification de messages à l'aide des paramètres de profil de messagerie qui conviennent.

Pour plus d'informations sur la création de fichiers de configuration de classification de messages, rendez-vous sur support.blackberry.com/kb et consultez l'article KB36736.

Référence connexe

BlackBerry 10 : paramètres de profil de messagerie

Configuration des domaines autorisés et limités sur les terminaux avec espace Travail

Pour aider à prévenir la fuite de données, vous pouvez configurer les domaines accessibles aux utilisateurs depuis la messagerie, le calendrier et les données de l'organiseur de l'espace Travail des terminaux iOS et Android.

- Si vous configurez une liste de domaines autorisés, les utilisateurs peuvent accéder aux domaines autorisés sans restrictions. Par exemple, ils peuvent cliquer sur les liens menant aux domaines ou ajouter des destinataires avec adresses électroniques aux domaines pour envoyer des e-mails ou des invitations de calendrier. Si un domaine donné ne se trouve pas sur la liste des domaines autorisés, l'application affiche un message d'avertissement lorsqu'un utilisateur tente d'y accéder. Si l'utilisateur sélectionne OK, il peut accéder au domaine.
- Si vous configurez une liste limitée de domaines, les utilisateurs ne peuvent pas accéder aux domaines de cette liste. S'ils cliquent sur des liens menant aux domaines ou tentent d'ajouter des destinataires avec adresses électroniques aux domaines, l'application affiche un message d'erreur et ne permet pas aux utilisateurs de mener à bien cette opération. Un utilisateur peut accéder aux domaines non répertoriés sur la liste limitée.

Remarque : pour les terminaux BlackBerry 10, vous pouvez configurer les domaines autorisés et limités à l'aide des règles de stratégie informatique « Liste autorisée des domaines de messagerie externes » et « Liste limitée des domaines de messagerie externes ». Pour plus d'informations, téléchargez la Fiche de référence des stratégies

Configurer les domaines autorisés et limités dans l'espace Travail

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **E-mail, calendrier et contacts > E-mail**.
3. Sélectionnez le profil de messagerie que vous souhaitez modifier.
4. Cliquez sur .
5. Cliquez sur l'onglet **iOS** ou **Android**.
6. Dans la section **Domaines de messagerie externes**, ajoutez les domaines que vous souhaitez autoriser et les domaines que vous souhaitez limiter.
7. Cliquez sur **Enregistrer**.

Référence connexe

Android : paramètres de profil de messagerie
iOS : paramètres de profil de messagerie

Utilisation d'Exchange Gatekeeping

Votre organisation peut utiliser BlackBerry Gatekeeping Service pour contrôler quels terminaux peuvent accéder à Exchange ActiveSync.

Pour utiliser le contrôle d'accès dans BlackBerry UEM, procédez comme suit :

- Créez une configuration de contrôle d'accès. Dans le contenu relatif à la configuration, reportez-vous à la section Contrôle des terminaux pouvant accéder à Exchange ActiveSync.
- Créer un profil de contrôle d'accès

Lorsque votre organisation utilise BlackBerry Gatekeeping Service, tous les terminaux ne figurant pas sur la liste blanche pour Microsoft Exchange sont signalés dans la liste des terminaux Exchange ActiveSync restreints BlackBerry UEM.

Si vous ajoutez un compte d'utilisateur et lui attribuez un profil de contrôle d'accès, tous les terminaux précédemment bloqués, mis en quarantaine ou manuellement autorisés liés au compte d'utilisateur s'affichent dans la liste des terminaux Exchange ActiveSync limités.

Autoriser un terminal à accéder à Microsoft ActiveSync

Si BlackBerry UEM ne parvient pas à obtenir l'ID Exchange ActiveSync d'un terminal, il n'est pas ajouté à la liste autorisée pour Microsoft Exchange. Vous pouvez manuellement ajouter ces terminaux à la liste autorisée depuis la liste des terminaux Exchange ActiveSync limités. Par exemple, si un terminal Android est activé via le type d'activation MDM, BlackBerry UEM n'est pas en mesure d'obtenir un ID Exchange ActiveSync et vous devez manuellement autoriser le terminal dans la liste des terminaux Exchange ActiveSync limités.

1. Sur la barre de menus, cliquez sur **Utilisateurs > Exchange Gatekeeping**.
2. Recherchez un terminal.
3. Dans la colonne **Action**, cliquez sur ✓.

Bloquer l'accès d'un terminal à Microsoft ActiveSync

Vous pouvez bloquer manuellement l'accès d'un terminal précédemment autorisé Microsoft ActiveSync. Ce faisant, le terminal empêche l'utilisateur de récupérer des e-mails et d'autres informations depuis Microsoft Exchange Server sur le terminal.

1. Sur la barre de menus, cliquez sur **Utilisateurs**.
2. Cliquez sur **Exchange Gatekeeping**.
3. Recherchez un terminal.
4. Dans la colonne **Action**, cliquez sur ⊘.

Vérification qu'un terminal est autorisé à accéder à la messagerie professionnelle et aux données de l'organiseur

Lorsque votre organisation utilise BlackBerry Gatekeeping Service pour contrôler les terminaux qui peuvent accéder à la messagerie professionnelle et aux données de l'organiseur depuis Exchange ActiveSync, au moins un serveur de contrôle d'accès est configuré sur un profil de messagerie. Lorsque le profil de messagerie avec contrôle d'accès configuré est attribuée à un compte d'utilisateur, vous pouvez vérifier l'état de la connexion entre un terminal et Exchange ActiveSync. Vous pouvez localiser cet état en consultant la page des détails du terminal de la section Stratégie informatique et profils. Les états suivants s'affichent dans les détails du terminal en regard du profil de messagerie.

État	Description
Inconnu	L'état Inconnu s'affiche lorsque BlackBerry UEM ne peut pas déterminer l'ID du terminal. Le terminal est répertorié dans la liste limitée des terminaux et doit être manuellement ajouté à la liste autorisée.
Connexion en attente	L'état Connexion en attente s'affiche lorsque BlackBerry UEM connait l'ID du terminal et que le terminal est mis en file d'attente pour être ajouté à la liste autorisée.

État	Description
Connexion autorisée	L'état Connexion autorisée s'affiche lorsque BlackBerry UEM connait l'ID du terminal et que le terminal se trouve sur la liste autorisée.

Vérifier qu'un terminal est autorisé

1. Sur la barre de menus, cliquez sur **Utilisateurs > Terminaux gérés**.
2. Recherchez un compte d'utilisateur.
3. Dans les résultats de la recherche, cliquez sur le nom d'un compte d'utilisateur.
4. Sélectionnez l'onglet correspondant au terminal que vous souhaitez vérifier.
5. Dans la section **Stratégie informatique et profils**, si le terminal est autorisé, **Connexion autorisée** s'affiche en regard du profil de messagerie.

Création d'un profil de contrôle d'accès

Si vous configurez le BlackBerry Gatekeeping Service, vous devez créer un profil de contrôle d'accès et l'attribuer aux comptes d'utilisateurs, aux groupes d'utilisateurs ou aux groupes de terminaux. Le profil de contrôle d'accès vous permet de sélectionner les serveurs Microsoft Exchange pour un contrôle d'accès automatique.

Créer un profil de contrôle d'accès

Si vous utilisez le contrôle d'accès automatique, créez un profil de contrôle d'accès.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **E-mail, calendrier et contacts > Contrôle**.
3. Cliquez sur +.
4. Saisissez le nom et la description du profil.
5. Cliquez sur **Sélectionner des serveurs**.
6. Sélectionnez un ou plusieurs serveurs et cliquez sur →.
7. Cliquez sur **Enregistrer**.

Configuration des profils CardDAV et CalDAV pour les terminaux iOSet macOS

Vous pouvez utiliser les profils CardDAV et CalDAV pour permettre aux terminaux iOS et macOS d'accéder à Informations de contact et de calendrier sur un serveur distant. Vous pouvez attribuer des profils CardDAV et CalDAV à des comptes d'utilisateur, groupes d'utilisateurs ou groupes de terminaux. Plusieurs terminaux peuvent accéder à la même information.

macOS applique les profils aux terminaux ou comptes d'utilisateur. Les profils CardDAV et CalDAV sont appliqués aux comptes d'utilisateur.

Créer un profil CardDAV

Avant de commencer :

- Vérifiez que le terminal peut accéder à un serveur CardDAV actif.

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

2. Cliquez sur **E-mail, calendrier et contacts > CardDAV**.
3. Cliquez sur +.
4. Saisissez le nom et la description du profil.
5. Tapez l'adresse du serveur pour le profil. C'est le FQDN de l'ordinateur qui héberge l'application Calendrier.
6. Dans le champ **Nom d'utilisateur**, effectuez l'une des opérations suivantes :
   - Si le profil concerne un seul utilisateur, indiquez le nom d'utilisateur.
   - Si le profil concerne plusieurs utilisateurs, saisissez `%UserName%`.
7. Si nécessaire, entrez le port utilisé pour le serveur CardDAV.
8. Si nécessaire, sélectionnez la case **Utiliser SSL** et entrez l'URL du serveur SSL.
9. Cliquez sur **Ajouter**.

À la fin : attribuez le profil aux utilisateurs, aux groupes d'utilisateurs ou aux groupes de terminaux.

Tâches connexes

Attribuer un profil ou une stratégie informatique à un groupe d'utilisateurs
Attribuer un profil ou une stratégie informatique à un compte d'utilisateur

Créer un profil CalDAV

Avant de commencer :

- Vérifiez que le terminal peut accéder à un serveur CalDAV actif.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **E-mail, calendrier et contacts > CalDAV**.
3. Cliquez sur +.
4. Saisissez le nom et la description du profil.
5. Tapez l'adresse du serveur pour le profil. C'est le FQDN de l'ordinateur qui héberge l'application Calendrier.
6. Dans le champ **Nom d'utilisateur**, effectuez l'une des opérations suivantes :
   - Si le profil concerne un seul utilisateur, indiquez le nom d'utilisateur.
   - Si le profil concerne plusieurs utilisateurs, saisissez `%UserName%`.
7. Si nécessaire, entrez le port utilisé pour le serveur CalDAV.
8. Si nécessaire, sélectionnez la case **Utiliser SSL** et entrez l'URL du serveur SSL.
9. Cliquez sur **Ajouter**.

À la fin : Attribuez le profil aux utilisateurs, aux groupes d'utilisateurs ou aux groupes de terminaux.

Tâches connexes

Attribuer un profil ou une stratégie informatique à un groupe d'utilisateurs
Attribuer un profil ou une stratégie informatique à un compte d'utilisateur

Certificats

Un certificat est un document numérique émis par une autorité de certification qui vérifie l'identité de l'objet de certificat et la lie à une clé publique. Chaque certificat dispose d'une clé privée correspondante stockée séparément. La clé publique et clé privée forment une paire de clés asymétriques qui peuvent être utilisées à des fins de cryptage des données et d'authentification de l'identité. Une autorité de certification signe le certificat pour vérifier que les entités qui approuvent l'autorité de certification peuvent également approuver le certificat.

Selon les fonctionnalités et le type d'activation du terminal, les terminaux peuvent utiliser des certificats pour :

- S'authentifier à l'aide du protocole SSL/TLS lorsqu'ils se connectent aux pages Web utilisant le protocole HTTPS
- S'authentifier auprès d'un serveur de messagerie professionnel
- S'authentifier auprès d'un réseau Wi-Fi ou VPN professionnel
- Crypter et signer les e-mails à l'aide de la protection S/MIME

De nombreux certificats utilisés à différentes fins peuvent être stockés sur un terminal. Vous pouvez utiliser les profils de certificat pour envoyer des certificats d'autorité de certification et des certificats client aux terminaux.

Étapes de l'utilisation des certificats avec des terminaux

Pour utiliser des certificats avec des terminaux, vous devez procéder comme suit :

Étape	Action
1	Si nécessaire, connectez BlackBerry UEM au logiciel PKI de votre entreprise.
2	Créez un ou plusieurs profils de certificat d'autorité de certification pour envoyer des certificats d'autorité de certification aux terminaux.
3	Créez des profils SCEP, identifiants de l'utilisateur ou certificat partagé, ou téléchargez les certificats d'un utilisateur spécifique, pour envoyer des certificats client aux terminaux.
4	Si nécessaire, associez les profils de certificat aux profils Wi-Fi , VPN ou e-mail.
5	Si nécessaire, attribuez les profils de certificats aux comptes d'utilisateur, groupes d'utilisateurs ou groupes de terminaux.

Intégration de BlackBerry UEM avec le logiciel PKI de votre organisation

Si votre entreprise utilise une solution PKI, comme les logiciels Entrust ou OpenTrust, vous pouvez émettre des certificats en étendant l'authentification basée sur des certificats fournie par ces services PKI aux terminaux que vous gérez avec BlackBerry UEM.

Les produits Entrust (comme Entrust IdentityGuard et Entrust Authority Administration Services) ainsi que les produits OpenTrust (comme OpenTrust PKI et OpenTrust CMS) fournissent des autorités de certification qui émettent des certificats client. Vous pouvez configurer une connexion au logiciel PKI de votre organisation et utiliser des profils pour envoyer le certificat d'autorité de certification et les certificats client aux terminaux.

Pour les terminaux BlackBerry Dynamics activés, vous pouvez également configurer un connecteur PKI qui crée une connexion entre BlackBerry UEM et un serveur d'autorité de certification pour inscrire les certificats des applications BlackBerry Dynamics ou utiliser une application prenant en charge l'inscription des certificats sur application, comme Purebred.

Connectez BlackBerry UEM au logiciel Entrust de votre organisation.

Pour étendre l'authentification basée sur des certificats Entrust aux terminaux, vous devez ajouter une connexion au logiciel Entrust de votre entreprise (par exemple, Entrust IdentityGuard ou Entrust Authority Administration Services).

Avant de commencer : Contactez l'administrateur Entrust de votre organisation pour obtenir :

- l'URL du service Web MDM de Entrust ;
- les informations de connexion d'un compte d'administrateur Entrust que vous pouvez utiliser pour connecter BlackBerry UEM au logiciel Entrust ;
- le certificat d'autorité de certification Entrust contenant la clé publique (.der, .pem ou .cert). BlackBerry UEM utilise ce certificat pour établir des connexions SSL avec le serveur Entrust

1. Sur la barre de menus, cliquez sur **Paramètres**.
2. Cliquez sur **Intégration externe > Autorité de certification**.
3. Cliquez sur **Ajouter une connexion Entrust**.
4. Dans le champ **Nom de connexion**, saisissez le nom du groupe.
5. Dans le champ **URL**, saisissez l'URL du service Web Entrust.
6. Dans le champ **Nom d'utilisateur**, saisissez le nom d'utilisateur du compte d'administrateur Entrust.
7. Dans le champ **Mot de passe**, saisissez le mot de passe du compte d'administrateur Entrust.
8. Si vous souhaitez charger un certificat d'autorité de certification pour autoriser BlackBerry UEM à établir des connexions SSL avec le serveur Entrust, cliquez sur **Parcourir**. Accédez au certificat d'autorité de certification et sélectionnez-le.
9. Pour tester la connexion, cliquez sur **Tester la connexion**.
10. Cliquez sur **Enregistrer**.

À la fin :

- Créez un profil d'informations d'identification d'utilisateur pour envoyer les certificats de votre logiciel PKI vers les terminaux.

Connecter BlackBerry UEM au serveur Entrust IdentityGuard de votre organisation pour utiliser les informations d'identification intelligentes

Si votre organisation utilise des informations d'identification intelligentes dérivées gérées par Entrust IdentityGuard, vous pouvez utiliser des informations d'identification intelligentes dérivées avec des terminaux gérés par BlackBerry UEM.

Avant de commencer :

- Vérifiez que BlackBerry UEM peut se connecter au serveur Entrust IdentityGuard. Si vous utilisez la version cloud de Entrust IdentityGuard, il vous faudra peut-être ouvrir un port dans votre pare-feu.
- Contactez l'administrateur Entrust de votre organisation pour obtenir les informations suivantes :
  - URL du serveur Entrust IdentityGuard

- Nom des informations d'identification intelligentes à activer sur les terminaux, comme indiqué dans Entrust IdentityGuard
- Certificat CA Entrust pour envoyer le certificat aux terminaux

1. Sur la barre de menus, cliquez sur **Paramètres**.
2. Cliquez sur **Intégration externe > Autorité de certification**.
3. Cliquez sur **Ajouter une connexion pour les informations d'identification intelligentes Entrust**.
4. Dans le champ **Nom des informations d'identification intelligentes**, entrez le nom des informations d'identification intelligentes spécifiées dans Entrust IdentityGuard.
5. Dans le champ **URL Entrust**, saisissez l'URL du serveur Entrust IdentityGuard.
6. Cliquez sur **Ajouter**.

À la fin :

- Créer un profil de certificat d'autorité de certification partagé Pour envoyer le certificat CA Entrust aux terminaux et attribuer le profil aux utilisateurs ou groupes auxquels le profil d'informations d'identification utilisateur sera attribué.
- Créer un profil d'informations d'identification utilisateur pour utiliser les informations d'identification intelligentes Entrust sur les terminaux.

Connectez BlackBerry UEM au logiciel OpenTrust de votre organisation

Pour étendre l'authentification basée sur des certificats OpenTrust aux terminaux, vous devez ajouter une connexion au logiciel OpenTrust de votre entreprise. BlackBerry UEM prend en charge l'intégration avec OpenTrust PKI 4.8.0 et version ultérieure et OpenTrust CMS version 2.0.4 et ultérieure.

Avant de commencer : Contactez l'administrateur OpenTrust de votre organisation pour obtenir l'URL du serveur OpenTrust, le certificat côté client contenant la clé privée (au format .pfx ou .p12) et le mot de passe du certificat.

1. Sur la barre de menus, cliquez sur **Paramètres**.
2. Cliquez sur **Intégration externe > Autorité de certification**.
3. Cliquez sur **Ajouter une connexion OpenTrust**.
4. Dans le champ **Nom de connexion**, saisissez le nom du groupe.
5. Dans le champ **URL**, saisissez l'URL du logiciel OpenTrust.
6. Cliquez sur **Parcourir**. Naviguez jusqu'au et sélectionnez le certificat côté client utilisé par BlackBerry UEM pour authentifier la connexion au serveur OpenTrust.
7. Dans le champ **Mot de passe du certificat**, saisissez le mot de passe du certificat du serveur OpenTrust.
8. Pour tester la connexion, cliquez sur **Tester la connexion**.
9. Cliquez sur **Enregistrer**.

À la fin :

- Créez un profil d'informations d'identification d'utilisateur pour envoyer les certificats de votre logiciel PKI vers les terminaux.
- Si vous utilisez la connexion BlackBerry UEM avec le logiciel OpenTrust pour distribuer des certificats aux terminaux, les certificats peuvent prendre un certain temps pour devenir valables. Ce retard pourrait entrainer des problèmes avec l'authentification par e-mail au cours du processus d'activation du terminal. Pour résoudre ce problème, dans le logiciel OpenTrust, configurez l'autorité de certification OpenTrust et définissez « Antidater les certificats (secondes) » sur 180.

Connecter BlackBerry UEM au connecteur PKI BlackBerry Dynamics de votre entreprise

Si vous souhaitez utiliser le logiciel PKI de votre entreprise pour inscrire les certificats des applications BlackBerry Dynamics, vous pouvez configurer un connecteur PKI BlackBerry Dynamics de manière à ce qu'il communique avec votre autorité de certification et connecte BlackBerry UEM au connecteur PKI.

Avant de commencer : Configurez un connecteur PKI BlackBerry Dynamics. Pour plus d'informations, reportez-vous à la section Configurer les connexions PKI pour les applications BlackBerry Dynamics du contenu relatif à la configuration.

1. Sur la barre de menus, cliquez sur **Paramètres > Intégration externe > Autorité de certification**.
2. Cliquez sur **Ajouter une connexion PKI BlackBerry Dynamics**.
3. Dans le champ **Nom de connexion**, saisissez un nom de connexion.
4. Dans le champ **URL**, saisissez l'URL du connecteur PKI.
5. Sélectionnez l'une des options suivantes :
   - **Authentification avec nom d'utilisateur et mot de passe** : choisissez cette option si BlackBerry UEM s'authentifie auprès du connecteur PKI BlackBerry Dynamics en utilisant l'authentification par mot de passe.
   - **Authentification avec certificat client** : choisissez cette option si BlackBerry UEM s'authentifie auprès du connecteur PKI BlackBerry Dynamics en utilisant l'authentification basée sur les certificats.
6. Si vous avez sélectionné **Authentification avec nom d'utilisateur et mot de passe**, dans les champs **Nom d'utilisateur** et **Mot de passe**, saisissez le nom d'utilisateur et le mot de passe du connecteur PKI BlackBerry Dynamics.
7. Si vous avez sélectionné **Authentification avec certificat client**, cliquez sur **Parcourir** pour sélectionner et télécharger un certificat approuvé par le connecteur PKI BlackBerry Dynamics. Dans le champ **Mot de passe du certificat client**, saisissez le mot de passe du certificat.
8. Pour tester la connexion, cliquez sur **Tester la connexion**.
9. Cliquez sur **Save**.

À la fin :

- Créez un profil d'informations d'identification d'utilisateur pour envoyer les certificats de votre logiciel PKI vers les terminaux.

Connecter BlackBerry UEM à la solution PKI d'application de votre organisation

Pour utiliser la solution PKI d'application de l'organisation (Purebred, par exemple) pour inscrire des certificats pour les applications BlackBerry Dynamics, vous pouvez installer l'application sur les différents terminaux et autoriser les applications BlackBerry Dynamics à utiliser les certificats inscrits par l'application PKI. Cette option est uniquement prise en charge sur les terminaux iOS.

Avant de commencer : Vérifiez que l'application qui récupère les certificats à l'usage des applications BlackBerry Dynamics figure dans la liste des applications dans BlackBerry UEM.

1. Sur la barre de menus, cliquez sur **Paramètres > Intégration externe > Autorité de certification**.
2. Cliquez sur **Ajouter une connexion pour les certificats de terminal**.
3. Sélectionnez l'application qui récupère les certificats de l'application PKI qui seront utilisés par les applications BlackBerry Dynamics. Pour utiliser Purebred, sélectionnez le BlackBerry UEM Client.
4. Cliquez sur **Ajouter**.

À la fin :

- Création de profils d'identification pour les certificats d'application.

Envoi de certificats client aux terminaux

De nombreux certificats utilisés à différentes fins peuvent être stockés sur un terminal. Plusieurs méthodes sont disponibles pour envoyer des certificats client à des terminaux.

Comment le certificat est ajouté	Description	Terminaux pris en charge
Pendant l'activation du terminal	BlackBerry UEM envoie les certificats aux terminaux lors du processus d'activation. Les terminaux utilisent ces certificats pour établir des connexions sécurisées entre le terminal et BlackBerry UEM.	Toutes
Profils SCEP	Vous pouvez créer des profils SCEP que les terminaux utilisent pour se connecter à l'autorité de certification de votre entreprise et en obtenir des certificats client à l'aide d'un service SCEP. Les terminaux peuvent utiliser ces certificats pour l'authentification basée sur certificat à partir du navigateur et pour se connecter à votre réseau Wi-Fi professionnel, VPN professionnel et serveur de messagerie professionnel.	• BlackBerry 10 • iOS • macOS • Android • Windows 10
Connexion à la solution PKI de votre entreprise	Si votre entreprise utilise une solution PKI telle que des produits logiciels Entrust ou OpenTrust pour émettre et gérer les certificats, vous pouvez créer des profils d'informations d'identification d'utilisateur que les terminaux utiliseront pour obtenir les certificats client auprès de l'autorité de certification de votre entreprise. Les terminaux compatibles BlackBerry Dynamics utilisent ces certificats pour l'authentification basée sur certificat à partir des applications BlackBerry Dynamics. Autres terminaux utilisent ces certificats pour l'authentification basée sur certificat à partir du navigateur et pour se connecter à votre réseau Wi-Fi professionnel, VPN professionnel et au serveur de messagerie professionnel.	• BlackBerry 10 • iOS • Android
Profils des certificats partagés	Un profil de certificat partagé spécifie un certificat client que BlackBerry UEM envoie aux terminaux iOS, macOS et Android. BlackBerry UEM envoie le même certificat client à chaque utilisateur auquel le profil est attribué. L'administrateur doit avoir accès au certificat et à la clé privée pour créer un profil de certificat partagé.	• iOS • macOS • Android

Comment le certificat est ajouté	Description	Terminaux pris en charge
Envoi de certificat client à un compte d'utilisateur individuel	Vous pouvez ajouter un certificat client à un compte d'utilisateur. BlackBerry UEM peut envoyer le certificat aux terminaux iOS et Android de l'utilisateur. Si le certificat est associé à un profil d'informations d'identification de l'utilisateur, les terminaux peuvent utiliser ce certificat pour se connecter à votre réseau Wi-Fi professionnel, VPN professionnel et serveurs de messagerie professionnel. L'administrateur doit avoir accès au certificat et à la clé privée pour envoyer le certificat client à l'utilisateur.	• BlackBerry 10 • iOS • Android
Chargement sur UEM Self-Service	Les utilisateurs peuvent charger des certificats sur BlackBerry UEM Self-Service. BlackBerry UEM, puis transférer le certificat sur leur terminal. Si le certificat est associé à un profil d'informations d'identification de l'utilisateur, les terminaux peuvent utiliser ce certificat pour se connecter à votre réseau Wi-Fi professionnel, VPN professionnel et serveurs de messagerie professionnel.	• BlackBerry 10 • iOS • Android
Importation par les utilisateurs	Les utilisateurs peuvent importer des certificats client dans le magasin de certificats du terminal, dans la section « Sécurité et confidentialité » des Paramètres système. Les certificats destinés à être utilisés par le Work Browser ou pour l'envoi de messages protégés par S/MIME à partir du compte de messagerie professionnel peuvent être importés dans le système de fichiers du terminal ou à partir d'un emplacement réseau accessible depuis l'espace Travail.	BlackBerry 10
Cartes à puce	Les utilisateurs peuvent importer des certificats S/MIME et SSL sur leurs terminaux à partir d'une carte à puce.	BlackBerry 10

Envoi de certificats aux terminaux à l'aide de profils

Vous pouvez envoyer des certificats aux terminaux à l'aide des profils suivants, disponibles dans la bibliothèque des stratégies et des profils.

Profil	Description
Certificat d'autorité de certification	Les profils de certificat d'autorité de certification spécifient un certificat d'autorité de certification que les terminaux peuvent utiliser pour approuver l'identité associée à n'importe quel certificat client ou serveur qui a été signé par cette autorité de certification.

Profil	Description
Informations d'identification de l'utilisateur	Les profils d'informations d'identification de l'utilisateur envoient les certificats aux terminaux comme suit : • Ils peuvent spécifier une connexion au logiciel PKI de votre entreprise pour l'envoi des certificats client aux terminaux. • Ils vous permettent de télécharger manuellement les certificats dans BlackBerry UEM et permettre aux utilisateurs de télécharger des certificats à l'aide de BlackBerry UEM Self-Service.
SCEP	Les profils SCEP indiquent comment les terminaux sont connectés à et obtiennent des certificats client de l'autorité de certification de votre entreprise à l'aide d'un service SCEP.
Certificat partagé	Les profils de certificats partagés spécifient un certificat client que BlackBerry UEM envoie aux terminaux iOS et Android. BlackBerry UEM envoie le même certificat client à chaque utilisateur auquel le profil est attribué.

Pour les terminaux iOS et Android, vous pouvez également envoyer un certificat client à un terminal en ajoutant directement ce certificat à un compte d'utilisateur. Pour plus d'informations, reportez-vous à Ajouter un certificat client à un compte d'utilisateur.

Pour les terminaux BlackBerry 10, iOS et Android, si votre organisation utilise des certificats pour S/MIME, vous pouvez également utiliser des profils pour permettre à des terminaux d'obtenir des clés publiques de destinataire et vérifier l'état du certificat. Pour plus d'informations, reportez-vous à Extension de la sécurité de la messagerie à l'aide de S/MIME.

Pour BlackBerry Dynamics, pour utiliser les certificats envoyés par des profils, vous devez sélectionner l'option Autoriser les applications BlackBerry Dynamics à utiliser les certificats utilisateur, les profils SCEP et les profils d'informations d'identification des utilisateurs dans les paramètres de l'application.

Concepts connexes

Extension de la sécurité de la messagerie à l'aide de S/MIME

Tâches connexes

Ajouter un certificat client à un compte d'utilisateur

Choix des profils pour envoyer des certificats client aux terminaux

Vous pouvez utiliser différents types de profils pour fournir des certificats client aux terminaux. Le type de profil que vous choisissez dépend de la façon dont votre organisation utilise les certificats et des types de terminaux pris en charge. Prenez en compte les recommandations suivantes :

- Pour utiliser les profils SCEP, vous devez disposer d'une autorité de certification qui prend en charge le protocole SCEP.
- Si vous avez configuré une connexion entre BlackBerry UEM et la solution PKI de votre entreprise, utilisez les profils d'informations d'identification de l'utilisateur pour envoyer les certificats aux terminaux. Vous pouvez vous connecter directement à une autorité de certification Entrust ou OpenTrust. Vous pouvez également utiliser un connecteur PKI BlackBerry Dynamics afin de vous connecter à un serveur d'AC pour inscrire les certificats pour les terminaux BlackBerry Dynamics activés.

- Pour permettre aux utilisateurs de charger les certificats leur permettant de se connecter à votre réseau Wi-Fi professionnel, VPN professionnel et serveur de messagerie professionnel, utilisez un profil d'informations d'identification de l'utilisateur.
- Pour utiliser des certificats avec les applications BlackBerry Dynamics, vous devez utiliser un profil d'informations d'identification de l'utilisateur ou ajouter les certificats aux comptes d'utilisateur individuels.
- Pour utiliser des certificats client pour une authentification Wi-Fi, VPN et par serveur de messagerie, vous devez associer le profil de certificat avec un profil Wi-Fi, VPN ou de messagerie.

  Remarque : Les terminaux Android dotés d'un profil professionnel ne prennent pas en charge l'utilisation de certificats envoyés aux terminaux par BlackBerry UEM pour l'authentification Wi-Fi.
- Les profils de certificats partagés et les certificats que vous ajoutez aux comptes utilisateur ne garantissent par le caractère privé de la clé, car vous devez avoir accès à cette clé privée. La connexion à une autorité de certification avec des profils SCEP ou des profils d'informations d'identification de l'utilisateur est plus sécurisée, car la clé privée n'est envoyée qu'au terminal auquel le certificat a été émis.

Envoi de certificats CA à des terminaux

Vous devrez peut-être distribuer des certificats d'autorité de certification aux terminaux si votre organisation utilise le protocole S/MIME ou si des terminaux utilisent une authentification basée sur les certificats pour se connecter à un réseau ou à un serveur dans l'environnement de votre organisation.

Lorsque vous envoyez un certificat d'autorité de certification à un terminal, celui-ci approuve l'identité associée à un certificat client ou serveur signé par l'autorité de certification. Lorsque le certificat de l'autorité de certification qui a signé les certificats réseau et serveur de votre organisation est stocké sur les terminaux, ces derniers peuvent approuver vos réseaux et serveurs lorsqu'ils établissent des connexions sécurisées. Lorsque le certificat d'autorité de certification qui a signé les certificats S/MIME de votre organisation est stocké sur des terminaux, ces terminaux peuvent approuver le certificat de l'expéditeur lors de la réception d'un e-mail sécurisé.

De nombreux certificats d'autorité de certification utilisés à des fins différentes peuvent être stockés sur un terminal. Vous pouvez utiliser des profils de certificat CA pour envoyer des certificats CA à des terminaux.

Créer un profil de certificat d'autorité de certification partagé

Avant de commencer : vous devez obtenir le fichier de certificat d'autorité de certification que vous souhaitez envoyer aux terminaux.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Certificats > Certificat CA**.
3. Cliquez sur +.
4. Saisissez le nom et la description du profil. Chaque profil de certificat d'autorité de certification doit avoir un nom unique. Certains noms (par exemple, ca_1) sont réservés.
5. Dans le champ **Fichier de certificat**, cliquez sur **Parcourir** pour localiser le fichier de certificat.
6. Si le certificat d'autorité de certification est envoyé aux terminaux BlackBerry 10, dans l'onglet BlackBerry, spécifiez un ou plusieurs des magasins de certificats suivants auxquels envoyer le certificat sur le terminal :
   - Magasin de certificats du navigateur
   - Magasin de certificats VPN
   - Magasin de certificats Wi-Fi
   - Magasin de certificats d'entreprise
7. Si le certificat d'autorité de certification est envoyé aux terminaux macOS, dans l'onglet macOS, dans la liste déroulante **Appliquer le profil à**, sélectionnez **Utilisateur** ou **Terminal**.
8. Cliquez sur **Ajouter**.

Tâches connexes

Attribuer un profil ou une stratégie informatique à un compte d'utilisateur
Attribuer un profil ou une stratégie informatique à un groupe d'utilisateurs

Magasins de certificats d'autorité de certification sur les terminaux BlackBerry 10

Les certificats d'autorité de certification envoyés aux terminaux BlackBerry 10 sont stockés dans différents magasins de certificats, selon l'objectif du certificat.

Magasin	Description
Magasin de certificats du navigateur	Le navigateur professionnel des terminaux BlackBerry 10 utilise les certificats de ce magasin pour établir des connexions SSL aux serveurs dans l'environnement de votre organisation.
Magasin de certificats VPN	Les terminaux BlackBerry 10 utilisent les certificats de ce magasin pour les connexions VPN. Vous devez définir le paramètre Source du certificat approuvé du profil VPN sur Magasin de certificats approuvé pour utiliser les certificats de ce magasin pour les connexions VPN professionnelles.
Magasin de certificats Wi-Fi	Les terminaux BlackBerry 10 utilisent les certificats de ce magasin pour les connexions Wi-Fi. Vous devez définir le paramètre Source du certificat approuvé du profil Wi-Fi sur Magasin de certificats approuvé pour utiliser les certificats de ce magasin pour les connexions Wi-Fi professionnelles.
Magasin de certificats d'entreprise	Les terminaux BlackBerry 10 utilisent les certificats de ce magasin pour authentifier les e-mails protégés S/MIME reçus.

Utilisation de profils d'informations d'identification de l'utilisateur pour envoyer des certificats aux terminaux

Les profils d'informations d'identification de l'utilisateur permettent aux terminaux de se procurer les certificats client auprès de l'autorité de certification de votre entreprise. Ils peuvent également vous permettre de télécharger manuellement des certificats dans BlackBerry UEM et permettre aux utilisateurs de télécharger des certificats à l'aide de BlackBerry UEM Self-Service.

BlackBerry UEM peut se connecter directement à l'autorité de certification Entrust ou OpenTrust de votre entreprise. Pour les terminaux BlackBerry Dynamics activés, vous pouvez également configurer un connecteur PKI afin de vous connecter à un serveur d'autorité de certification pour inscrire les certificats des applications BlackBerry Dynamics ou utiliser une solution PKI d'application telle que Purebred.

Si les utilisateurs chargent les certificats manuellement dans UEM Self-Service, ceux-ci s'affichent sur la page de l'utilisateur dans la console de gestion. Vous pouvez également supprimer ou remplacer le certificat.

Les profils d'informations d'identification de l'utilisateur sont pris en charge par les terminaux iOS et Android, ainsi que par les terminaux exécutant BlackBerry 10 OS version 10.3.1 et ultérieure. Les solutions PKI d'application sont prises en charge par les terminaux iOS. Le téléchargement manuel des certificats est pris en charge par les terminaux BlackBerry 10 et iOS, les terminaux Android dotés d'un profil professionnel et les terminaux Samsung KNOX Workspace.

Pour plus d'informations sur la connexion de BlackBerry UEM au logiciel PKI de votre entreprise, reportez-vous à Intégration de BlackBerry UEM avec le logiciel PKI de votre organisation.

Vous pouvez également utiliser des profils SCEP pour inscrire les certificats client sur les terminaux. Vous pouvez également charger des certificats directement vers un compte d'utilisateur. Le type de profil que vous choisissez dépend de la manière dont votre organisation utilise le logiciel PKI, des types de terminaux pris en charge par et de la manière dont vous souhaitez gérer les certificats.

Créer un profil d'informations d'identification de l'utilisateur pour télécharger manuellement les certificats

Les profils d'informations d'identification de l'utilisateur vous permettent, ainsi qu'aux utilisateurs, de télécharger manuellement un certificat à envoyer aux terminaux des utilisateurs.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Certificats > Informations d'identification de l'utilisateur**.
3. Cliquez sur +.
4. Saisissez le nom et la description du profil. Chaque profil de certificat doit avoir un nom unique.
5. Dans la liste déroulante **Connexion à l'autorité de certification**, cliquez sur **Certificat chargé manuellement**.
6. Cliquez sur **Ajouter**.

À la fin :

- Si les terminaux utilisent des certificats client pour s'authentifier auprès d'un réseau Wi-Fi, d'un VPN ou d'un serveur de messagerie, associez le profil d'informations d'identification de l'utilisateur à un profil Wi-Fi, VPN ou de messagerie.
- Attribuez le profil aux comptes d'utilisateur et groupes d'utilisateurs.
- Ajouter un certificat client à un profil d'informations d'identification de l'utilisateur Vous pouvez également demander aux utilisateurs d'utiliser BlackBerry UEM Self-Service pour télécharger leur propre certificat.

Tâches connexes

Ajouter un certificat client à un profil d'informations d'identification de l'utilisateur
Modifier un certificat client pour un profil d'informations d'identification de l'utilisateur

Créer un profil d'informations d'identification d'utilisateur pour la connexion au logiciel PKI de votre entreprise

Avant de commencer :

- Contactez l'administrateur Entrust ou OpenTrust de votre organisation pour confirmer quel profil PKI vous devez sélectionner. BlackBerry UEM obtient une liste des profils du logiciel PKI.
- Demandez à l'administrateur Entrust ou OpenTrust quelles sont les valeurs de profil que vous devez fournir. Par exemple, les valeurs correspondant au type de terminal (devicetype), au groupe Entrust IdentityGuard (iggroup) et au nom d'utilisateur Entrust IdentityGuard (igusername).
- Si le système OpenTrust de votre entreprise est configuré pour renvoyer uniquement des clés sous séquestre, l'administrateur de OpenTrust doit vérifier que des certificats sont présents pour chaque utilisateur dans le système OpenTrust. L'attribution d'un profil d'informations d'identification aux utilisateurs dans BlackBerry UEM ne crée pas automatiquement des certificats pour les utilisateurs dans OpenTrust. Dans ce scénario, un profil d'informations d'identification de l'utilisateur peut uniquement distribuer des certificats aux utilisateurs qui ont déjà un certificat dans le système OpenTrust.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Certificats > Informations d'identification de l'utilisateur**.
3. Cliquez sur +.
4. Saisissez le nom et la description du profil. Chaque profil de certificat doit avoir un nom unique.

5. Dans la liste déroulante **Connexion à l'autorité de certification**, cliquez sur la connexion Entrust ou OpenTrust que vous avez configurée.
6. Dans la liste déroulante **Profil**, cliquez sur le profil qui convient.
7. Spécifiez les valeurs du profil.
8. Si nécessaire, vous pouvez spécifier un type et une valeur SAN pour un certificat client Entrust.
   a) Dans le tableau SAN, cliquez sur +.
   b) Dans la liste déroulante **Type SAN**, cliquez sur le type qui convient.
   c) Dans le champ **Valeur SAN**, tapez la valeur SAN.

      Si le type SAN est défini sur Nom RFC822, la valeur doit correspondre à une adresse électronique valide. Si cette option est définie sur URI, la valeur doit correspondre à une URL valide incluant le protocole et le FQDN ou l'adresse IP. Si cette option est définie sur Nom principal, la valeur doit correspondre à un nom principal valide. Si cette option est définie sur Nom DN, la valeur doit correspondre à un FQDN valide.
9. Indiquez la **Période de renouvellement** du certificat. Cette période peut être comprise entre 1 et 120 jours.
10. Si les terminaux BlackBerry 10 utilisent le certificat client pour crypter les e-mails à l'aide de S/MIME et que vous souhaitez que les terminaux conservent les certificats expirés pour permettre aux utilisateurs d'ouvrir d'anciens e-mails, cochez la case **Inclure l'historique des certificats**.
11. Cliquez sur **Ajouter**.

À la fin :

- Si les terminaux utilisent des certificats client pour s'authentifier auprès d'un réseau Wi-Fi, d'un VPN ou d'un serveur de messagerie, associez le profil d'informations d'identification de l'utilisateur à un profil Wi-Fi, VPN ou de messagerie.
- Attribuez le profil aux comptes d'utilisateur et groupes d'utilisateurs. Les utilisateurs Android sont invités à saisir un mot de passe lorsqu'ils reçoivent le profil (le mot de passe est affiché à l'écran).

Tâches connexes

Attribuer un profil ou une stratégie informatique à un groupe d'utilisateurs
Attribuer un profil ou une stratégie informatique à un compte d'utilisateur

Créer un profil d'informations d'identification utilisateur pour utiliser les informations d'identification intelligentes Entrust sur les terminaux

Les informations d'identification intelligentes dérivées Entrust sont prises en charge par les applications suivantes :

- Applications BlackBerry Dynamics sur les terminaux iOS
- Applications BlackBerry Dynamics sur les terminaux Android autres que les terminaux Samsung KNOX Workspace
- Applications sur les terminaux Android dotés d'un profil professionnel, qui utilisent des certificats pour la signature, le cryptage et l'authentification d'identité, tels que BlackBerry Hub et les navigateurs Web pris en charge
- Applications sur les terminaux Samsung KNOX Workspace qui utilisent des certificats pour la signature, le cryptage et l'authentification d'identité, tels que le client de messagerie natif Samsung et les navigateurs Web pris en charge

Remarque : BlackBerry UEM ne prend pas en charge l'historique des clés pour des informations d'identification intelligentes dérivées.

Avant de commencer :

- Connecter BlackBerry UEM au serveur Entrust IdentityGuard de votre organisation pour utiliser les informations d'identification intelligentes.
- Créer un profil de certificat d'autorité de certification partagé pour envoyer le certificat CA Entrust aux terminaux et attribuer le profil aux utilisateurs ou groupes auxquels ce profil d'informations d'identification utilisateur sera attribué.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Certificats > Informations d'identification de l'utilisateur**.
3. Cliquez sur +.
4. Saisissez le nom et la description du profil. Chaque profil de certificat doit avoir un nom unique.
5. Dans la liste déroulante **Connexion à l'autorité de certification**, sélectionnez la connexion via les informations d'identification intelligentes Entrust que vous avez configurée.
6. Dans la liste déroulante **Type de certificat**, spécifiez si les informations d'identification intelligentes seront utilisées pour l'authentification d'identité, la signature ou le cryptage.

   Si vous souhaitez envoyer des informations d'identification intelligentes aux applications dans plusieurs objectifs, créez d'autres profils d'informations d'identification utilisateur.
7. Si les informations d'identification intelligentes sont envoyées à des terminaux Samsung KNOX Workspace ou à d'autres applications que les applications BlackBerry Dynamics sur des terminaux Android dotés d'un profil professionnel, cliquez sur l'onglet **Android** et sélectionnez **Remettre à la clé native**.

   Si ce paramètre n'est pas sélectionné, les informations d'identification intelligentes ne peuvent être utilisées que par des applications BlackBerry Dynamics.
8. Si les informations d'identification intelligentes sont envoyées à des applications BlackBerry Dynamics, cliquez sur l'onglet **BlackBerry Dynamics** et procédez comme suit :
   a) Si vous souhaitez que le terminal supprime les informations d'identification en double, sélectionnez **Supprimer les certificats dupliqués**. Le terminal supprime les informations d'identification qui expirent en premier.
   b) Si vous souhaitez que le terminal supprime les informations d'identification ayant expiré, sélectionnez **Supprimer les certificats ayant expiré**.
   c) Pour permettre à toutes les applications BlackBerry Dynamics d'utiliser les informations d'identification intelligentes, sélectionnez **Autoriser toutes les applications à utiliser des certificats**.
   d) Pour permettre à certaines applications BlackBerry Dynamics d'utiliser les informations d'identification intelligentes, sélectionnez **Autoriser les applications spécifiées à utiliser des certificats** et cliquez sur + pour spécifier les applications. Vous devez inclure BlackBerry UEM Client dans la liste des applications.
9. Cliquez sur **Ajouter**.

À la fin :

- Attribuez le profil aux comptes d'utilisateur et groupes d'utilisateurs.
- Une fois le profil reçu par le terminal, les utilisateurs doivent se connecter au module Entrust IdentityGuard Self-Service pour activer leurs informations d'identification intelligentes et utiliser BlackBerry UEM Client pour lire le code QR présenté par le module Entrust IdentityGuard Self-Service pour ajouter les informations d'identification intelligentes au terminal.
- Pour supprimer des informations d'identification intelligentes Entrust d'un terminal, l'utilisateur doit désactiver les informations d'identification intelligentes dans BlackBerry UEM Client avant de désattribuer le profil ou de supprimer le certificat.

Créer un profil d'informations d'identification d'utilisateur pour la connexion à votre connecteur PKI BlackBerry Dynamics

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Certificats > Informations d'identification de l'utilisateur**.

3. Cliquez sur +.
4. Saisissez le nom et la description du profil. Chaque profil de certificat doit avoir un nom unique.
5. Dans la liste déroulante **Connexion à l'autorité de certification**, sélectionnez la connexion PKI BlackBerry Dynamics que vous avez configurée.
6. Si l'utilisateur doit fournir un mot de passe pour demander un certificat, sélectionnez **Exiger un mot de passe entré par l'utilisateur ou OTP**.
7. Si vous souhaitez permettre au terminal de demander automatiquement un nouveau certificat avant l'expiration du certificat actuel, sélectionnez **Activer le renouvellement du certificat** et indiquez le nombre de jours avant l'expiration pendant lesquels les terminaux peuvent demander un nouveau certificat.
8. Si vous souhaitez que le terminal supprime les certificats ayant expiré, sélectionnez **Supprimer les certificats ayant expiré**.
9. Si vous souhaitez que le terminal supprime les certificats dupliqués, sélectionnez **Supprimer les certificats dupliqués**. Le terminal supprime le certificat qui expire en premier.
10. Cliquez sur **Ajouter**.

À la fin :

- Autorisez les applications BlackBerry Dynamics à utiliser les certificats.
- Attribuez le profil aux comptes d'utilisateur et groupes d'utilisateurs.
- Si vous mettez à jour le connecteur PKI, cliquez sur **Actualiser les fonctionnalités PKI** pour mettre à jour les fonctionnalités PKI prises en charge pour le profil.

Renouveler les certificats qui sont inscrits par le biais du connecteur PKI BlackBerry Dynamics

Si vous avez besoin de mettre à jour les certificats utilisateur pour tous les utilisateurs BlackBerry Dynamics, vous pouvez envoyer une commande pour demander le renouvellement de certificat à tous les terminaux auxquels le profil d'informations d'identification utilisateur est affecté.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Certificats > Informations d'identification de l'utilisateur**.
3. Cliquez sur le nom du profil que vous souhaitez modifier.
4. Cliquez sur **Actualiser les fonctionnalités PKI** pour vous assurer que BlackBerry UEM dispose des détails les plus récents pour le connecteur PKI.
5. Cliquez sur **Renouveler** pour indiquer à tous les terminaux activés BlackBerry Dynamics auxquels le profil est affecté de demander le renouvellement du certificat.

Tâches connexes

Renouveler ou supprimer un certificat BlackBerry Dynamics pour un compte d'utilisateur

Création de profils d'identification pour les certificats d'application

Pour utiliser la solution PKI d'application de l'organisation (Purebred, par exemple) pour inscrire des certificats pour les applications BlackBerry Dynamics, vous pouvez installer l'application sur les différents terminaux et autoriser les applications BlackBerry Dynamics à utiliser les certificats inscrits par l'application PKI. Cette option est uniquement prise en charge sur les terminaux iOS.

Si vous envoyez plusieurs certificats aux terminaux, vous pouvez créer plusieurs profils d'identification renfermant chacun un type de certificat différent. Configurer plusieurs profils offre les avantages suivants :

- Lorsque Microsoft Exchange est configuré pour l'authentification basée sur les certificats client, BlackBerry Work utilise un nom de profil d'informations d'identification de l'utilisateur configuré afin d'identifier sans

ambiguïté le certificat d'authentification. Ceci n'est pas possible si vous utilisez un seul profil d'identification d'utilisateur.
- Avec un seul profil d'identification d'utilisateur pour plusieurs certificats, rien n'indique s'il manque des certificats. Par exemple, si un utilisateur a besoin d'un certificat de chiffrement et que seuls les certificats de signature et d'authentification sont importés, le BlackBerry UEM Client indique que l'importation a réussi. En revanche, si vous configurez trois profils d'identification distincts et que le certificat de chiffrement est manquant, le BlackBerry UEM Client indique à l'utilisateur que ce certificat est manquant.

Conditions préalables : création d'un profil d'informations d'identification de l'utilisateur pour utiliser des certificats d'application

Avant de créer un profil d'informations d'identification de l'utilisateur afin d'utiliser la solution PKI d'application de l'organisation (Purebred, par exemple), effectuez les actions suivantes :

- Créer un profil BlackBerry Dynamics. Dans le profil, sélectionnez Activer, **Autoriser UEM Client à s'inscrire dans BlackBerry Dynamics** et sélectionnez BlackBerry UEM Client pour **Délégation d'authentification d'application**.
- Connecter BlackBerry UEM à la solution PKI d'application de votre organisation
- Configurer BlackBerry UEM Client pour la prise en charge des certificats d'applications
- Configurer les applications BlackBerry Dynamics pour l'utilisation de certificats basés sur les applications
- Vérifiez que l'application PKI (par exemple, Purebred) est installée sur les terminaux des utilisateurs.

Configurer BlackBerry UEM Client pour la prise en charge des certificats d'applications

1. Sur la console de gestion BlackBerry UEM, dans la barre de menu, cliquez sur **Applications**.
2. Dans la liste des applications, sélectionnez BlackBerry UEM Client.
3. Dans la section Configuration application, cliquez sur +.
4. Dans le champ **Nom de l'application**, saisissez le nom de l'application.
5. Dans le champ **UTI schemes**, spécifiez les schémas UTI pour la solution PKI d'application de l'organisation. Par exemple, si vous utilisez l'application Purebred, utilisez les schémas suivants : purebred.zip.all, purebred.zip.no_filter.
6. Cliquez sur **Enregistrer**.
7. Sélectionnez **Autoriser les applications BlackBerry Dynamics à utiliser les certificats et profils d'informations d'identification des utilisateurs**.
8. Attribuez le BlackBerry UEM Client avec la configuration d'application que vous avez créée aux utilisateurs et aux terminaux que vous souhaitez utiliser avec la solution PKI d'application.

Configurer les applications BlackBerry Dynamics pour l'utilisation de certificats basés sur les applications

1. Sur la console de gestion BlackBerry UEM, dans la barre de menu, cliquez sur **Applications**.
2. Dans la liste des applications, sélectionnez l'application (par exemple, BlackBerry Work ou BlackBerry Access).
3. Sélectionnez l'option **Autoriser les applications BlackBerry Dynamics à utiliser les certificats et profils d'informations d'identification des utilisateurs**.
4. Si vous configurez BlackBerry Work, dans la section de configuration de l'application, cliquez sur + et effectuez l'une des tâches suivantes :

Tâche	Étapes
Configurer BlackBerry Work lorsque votre organisation utilise BEMS	**a.** Sur l'onglet Paramètres de configuration, sélectionnez **Clients must have individual login certificates (SSL) uploaded in the GC**. **b.** Pour activer la détection automatique du serveur Microsoft Exchange sur lequel se trouvent les utilisateurs, sélectionnez **Use BEMS to perform Autodiscover of the EAS/EWS endpoint for the user**. **c.** Sur l'onglet **Paramètres Exchange**, dans le champ **Nom du profil d'informations d'identification de l'utilisateur**, entrez le nom du profil d'informations d'identification de l'utilisateur.
Configurer BlackBerry Work lorsque votre entreprise n'utilise pas BEMS	**a.** Sélectionnez l'onglet **Paramètres Exchange**. **b.** Si votre serveur utilise le format de connexion *nom de domaine\utilisateur*, dans le champ **Domaine par défaut**, spécifiez le domaine par défaut Windows NT auquel BlackBerry Work se connecte lorsque les utilisateurs ouvrent une session. **c.** Dans le champ **Active Sync Server**, spécifiez le serveur Exchange ActiveSync par défaut auquel BlackBerry Work se connectera lorsque les utilisateurs se connecteront à BlackBerry Work (par exemple, cas.mydomain.com). **d.** Dans le champ **Auto Discover URL** , spécifiez l'URL de détection automatique si connue. Ceci accélère le processus de configuration de découverte automatique (par exemple, https://autodiscover.mydomain.com). **e.** Dans le champ **Délai d'expiration de la découverte automatique de connexion (iOS seulement)**, spécifiez le délai d'expiration de la détection automatique de connexion en secondes. **f.** Dans le champ **Nom du profil d'informations d'identification de l'utilisateur**, entrez le nom du profil d'informations d'identification de l'utilisateur.

5. Cliquez sur **Enregistrer**.

Créer un profil d'identification d'utilisateur pour utiliser des certificats d'application

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Certificats > Informations d'identification de l'utilisateur**.
3. Cliquez sur +.
4. Saisissez le nom et la description du profil. Chaque profil de certificat doit avoir un nom unique.
5. Dans la liste déroulante **Connexion à l'autorité de certification**, sélectionnez le nom de l'application que vous avez spécifiée lors de la connexion de BlackBerry UEM à votre solution PKI. Si vous utilisez Purebred, sélectionnez le BlackBerry UEM Client
6. Dans la section **Utilisation de la clé**, sélectionnez les opérations prises en charge par le certificat.

   Par exemple, vous pouvez sélectionner **Cryptage de clé** pour un certificat de chiffrement, **Signature numérique** pour un certificat d'authentification et à la fois **Signature numérique** et **Non-reniement** pour un certificat de signature.
7. Dans la section **Utilisation étendue de la clé**, sélectionnez les fonctions pour lesquelles les utilisateurs utiliseront le certificat.
8. Si le certificat doit être utilisé à des fins autres que le courrier électronique, l'authentification client ou l'ouverture de session par carte à puce, sélectionnez **Utilisation d'ID d'objet supplémentaire**, cliquez sur + et spécifiez l'ID objet pour l'utilisation de la clé. Par exemple, si le certificat doit servir à l'authentification du serveur, ajoutez l'OID 1.3.6.1.5.5.7.3.1

9. Si vous souhaitez indiquer l'émetteur du certificat, à côté d'**Organisme certificateur**, cliquez sur + et saisissez le nom de l'organisme certificateur. Le nom de l'organisme certificateur doit correspondre au nom OID abrégé OpenSSL. Vous pouvez copier cette valeur du certificat de l'organisme certificateur. N'insérez pas d'espace avant ou après le signe « = ». Par exemple :

```
CN=Acme_cert SMIME,OU=Acme_Legal,O=Acme,C=Can
CN=Acme_cert SMIME,OU=Acme_Legal,O=Acme
CN=Acme_cert TLS
```

10. Si vous souhaitez que le terminal supprime les certificats ayant expiré, sélectionnez **Supprimer les certificats ayant expiré**.

    Les certificats de chiffrement expirés utilisés pour S/MIME doivent être conservés sur le terminal afin de permettre aux utilisateurs de lire les messages qui ont été chiffrés avant leur expiration.
11. Si vous souhaitez que le terminal supprime les certificats dupliqués, sélectionnez **Supprimer les certificats dupliqués**. Le terminal supprime le certificat qui expire en premier.
12. Cliquez sur **Ajouter**.

À la fin :

- Autorisez les applications BlackBerry Dynamics à utiliser les certificats.
- Attribuez le profil aux comptes d'utilisateur et groupes d'utilisateurs.

Utilisation d'un profil SCEP pour envoyer des certificats client sur des terminaux

Vous pouvez utiliser des profils SCEP pour spécifier la manière dont les terminaux BlackBerry 10, iOS, Android et Windows 10 se procurent les certificats client auprès de l'autorité de certification de votre entreprise via un service SCEP. SCEP est un protocole IETF qui simplifie le processus d'inscription des certificats client sur un grand nombre de terminaux sans nécessiter d'intervention ou d'approbation de l'administrateur pour délivrer chaque certificat. Les terminaux peuvent utiliser le protocole SCEP pour demander et obtenir des certificats client auprès d'une autorité de certification compatible SCEP utilisée par votre organisation. L'autorité de certification que vous utilisez doit prendre en charge les mots de passe de vérification. L'autorité de certification utilise les mots de passe de vérification pour vérifier que le terminal est autorisé à envoyer une demande de certificat.

Selon leurs capacités du terminal et le type d'activation, les terminaux peuvent utiliser des certificats client obtenus à l'aide de SCEP pour l'authentification basée sur des certificats à partir du navigateur ou se connecter à un réseau Wi-Fi professionnel, à un VPN professionnel ou à un serveur de messagerie professionnel.

Si votre organisation utilise une autorité de certification Entrust ou OpenTrust, les profils SCEP ne sont pas pris en charge pour les terminaux Windows 10.

Créer un profil SCEP

Les paramètres de profil requis varient selon le type de terminal et dépendent de la configuration du service SCEP dans l'environnement de votre entreprise.

Remarque : si vous souhaitez utiliser un Profil SCEP pour distribuer les certificats client OpenTrust aux terminaux, vous devez appliquer un correctif à votre logiciel OpenTrust. Pour plus d'informations, contactez votre représentant de support technique OpenTrust et indiquez la référence de support SUPPORT-798.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Certificats > SCEP**.
3. Cliquez sur +.
4. Saisissez le nom et la description du profil. Chaque profil de certificat doit avoir un nom unique.

5. Dans le champ **URL**, saisissez l'URL du service SCEP. L'URL doit inclure le protocole, le FQDN, le numéro de port et le chemin SCEP.
6. Dans le champ **Nom de l'instance**, saisissez le nom de l'instance pour l'autorité de certification.
7. Dans la liste déroulante **Connexion à l'autorité de certification**, effectuez l'une des opérations suivantes :
   - Pour utiliser une connexion Entrust que vous avez configurée, cliquez sur la connexion qui convient. Dans la liste déroulante **Profil**, cliquez sur un profil. Spécifiez les valeurs du profil.
   - Pour utiliser une connexion OpenTrust que vous avez configurée, cliquez sur la connexion qui convient. Dans la liste déroulante**Profil**, cliquez sur un profil. Spécifiez les valeurs du profil.
     - Les paramètres suivants du profil SCEP ne s'appliquent pas aux certificats client OpenTrust : Utilisation de la clé, Utilisation étendue de la clé, Objet et SAN.
   - Pour utiliser une autre autorité de certification, cliquez sur **Générique**. Dans la liste déroulante **Type de challenge SCEP**, sélectionnez **Statique** ou **Dynamique**, puis spécifiez les paramètres requis pour le type de vérification.

     Remarque : Pour les terminaux Windows, seuls les mots de passe Statiques sont pris en charge.
8. Vous pouvez également décocher la case correspondant aux types de terminaux pour lesquels vous ne souhaitez pas configurer le profil.
9. Procédez comme suit :
   a) Cliquez sur l'onglet correspondant à un type de terminal.
   b) Configurez les valeurs qui conviennent pour chaque paramètre de profil afin qu'elles correspondent à la configuration du service SCEP dans l'environnement de votre organisation.
10. Répétez l'étape 8 pour chaque type de terminal de votre organisation.
11. Cliquez sur **Ajouter**.

À la fin : si les terminaux utilisent le certificat client pour s'authentifier auprès d'un réseau Wi-Fi professionnel, d'un VPN professionnel ou d'un serveur de messagerie professionnel, associez le profil SCEP à un profil Wi-Fi, un profil VPN ou un profil de messagerie.

Concepts connexes

Paramètres du profil SCEP

Envoi du même certificat client à plusieurs terminaux

Vous pouvez utiliser des profils de certificat partagés pour envoyer des certificats client aux terminaux iOS, macOS et Android

Les profils de certificats partagés envoient la même paire de clés à chaque utilisateur affecté au profil. Utilisez uniquement les profils de certificat partagé pour autoriser plusieurs utilisateurs à partager un certificat client.

macOS applique les profils aux terminaux ou comptes d'utilisateur. Vous pouvez configurer un profil de certificat partagé à appliquer à l'un ou à l'autre.

Tâches connexes

Ajouter un certificat client à un compte d'utilisateur

Créer un profil de certificat partagé

Avant de commencer : vous devez obtenir le fichier de certificat client que vous souhaitez envoyer aux terminaux. Le nom du fichier de certificat doit comprendre l'extension .pfx ou .p12.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Certificats > Certificat partagé**.
3. Cliquez sur +.
4. Saisissez le nom et la description du profil. Chaque profil de certificat doit avoir un nom unique. Certains noms (par exemple, ca_1) sont réservés.
5. Dans le champ **Mot de passe**, indiquez un mot de passe pour le profil de certificat partagé.
6. Dans le champ **Fichier de certificat**, cliquez sur **Parcourir** pour localiser le fichier de certificat.
7. Dans l'onglet **macOS**, dans la liste déroulante **Appliquer le profil à**, sélectionnez **Utilisateur** ou **Terminal**.
8. Cliquez sur **Ajouter**.

Tâches connexes

Attribuer un profil ou une stratégie informatique à un groupe d'utilisateurs
Attribuer un profil ou une stratégie informatique à un compte d'utilisateur

Stratégies, normes et conformité des terminaux

Vous pouvez utiliser des stratégies informatiques et des profils pour appliquer certaines normes aux terminaux de votre entreprise. Une stratégie informatique est un ensemble de règles qui contrôlent des fonctions et fonctionnalités sur des terminaux. Différents profils prennent en charge des configurations spécifiques telles que le comportement des applications BlackBerry Dynamics, les règles de conformité, les limites de contenu Web ou les limites des applications. Vous pouvez spécifier les paramètres des terminaux BlackBerry 10, iOS, Android et Windows dans la même stratégie informatique ou le même profil, puis attribuer la stratégie informatique ou le profil à des comptes d'utilisateur, groupes d'utilisateurs ou groupes de terminaux.

Étapes à suivre pour configurer les stratégies et les normes de votre entreprise pour les terminaux

Pour configurer les stratégies et les normes de votre organisation pour les terminaux, procédez comme suit :

Étape	Action
1	Consultez la stratégie informatique par défaut et, si nécessaire, procédez à des mises à jour.
2	Vous pouvez également créer des stratégies informatiques personnalisées.
3	Créez des profils pour appliquer certaines normes aux terminaux. Par exemple, créez un profil de conformité, un profil de contenu Web ou un profil de notification d'entreprise.
4	Si nécessaire, classez les stratégies informatiques et classez les profils.
5	Attribuez les stratégies informatiques et les profils aux comptes d'utilisateur, aux groupes d'utilisateurs ou aux groupes de terminaux.

Gestion de terminaux à l'aide de stratégies informatiques

Vous pouvez utiliser des stratégies informatiques pour gérer la sécurité et le comportement des terminaux de votre organisation. Une stratégie informatique est un ensemble de règles qui contrôlent des fonctions et fonctionnalités sur des terminaux. Vous pouvez configurer des règles pour les terminaux BlackBerry 10,iOS,macOS,Android et Windows dans la même stratégie informatique. Le système d'exploitation du terminal dresse la liste des fonctions qui peuvent être contrôlées à l'aide de stratégies informatiques, et le type d'activation du terminal détermine les règles de stratégie informatique qui s'appliquent à un terminal spécifique. Les terminaux ignorent les règles de stratégie informatique qui ne les concernent pas.

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

vous mettez à jour une stratégie informatique attribuée ou lorsqu'une stratégie informatique différente est attribuée à un compte d'utilisateur ou à un terminal.

BlackBerry UEM se synchronise quotidiennement avec BlackBerry Infrastructure via le port 3101 pour déterminer si des informations de stratégie informatique mises à jour sont disponibles. Si des informations de stratégie informatique mises à jour sont disponibles, BlackBerry UEM les récupère et stocke les mises à jour dans la base de données BlackBerry UEM. Les administrateurs dotés des autorisations Afficher les stratégies informatiques et Créer et modifier les stratégies informatiques sont informés de ces mises à jour lorsqu'ils se connectent.

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

Limiter ou autoriser les fonctionnalités du terminal

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

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

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

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

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

Configuration des exigences de mot de passe du terminal

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

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

Configuration des exigences de mot de passe pour BlackBerry 10

Sur les terminaux BlackBerry 10, les règles de mot de passe affectent le mot de passe de l'espace Travail. Les terminaux "Espace Travail uniquement" doivent avoir un mot de passe et vous pouvez définir les exigences pour ce mot de passe.

Vous pouvez choisir si les terminaux "Travail et Personnel - Entreprise" et "Travail et Personnel - Régulé" doivent avoir un mot de passe pour l'espace Travail. Si vous avez besoin d'un mot de passe pour l'espace Travail, vous pouvez définir des exigences minimum pour ce mot de passe, indiquer si le terminal doit également avoir un mot de passe et spécifier si les mots de passe de l'espace Travail et du terminal peuvent ou doivent être les mêmes.

Règle	Détails
Mot de passe requis pour l'espace Travail	Spécifiez si les terminaux "Travail et Personnel - Entreprise" et "Travail et Personnel - Régulé" nécessitent un mot de passe pour l'espace Travail. Les terminaux "Espace Travail uniquement" doivent avoir un mot de passe.
Longueur minimale du mot de passe	Spécifiez la longueur minimale du mot de passe de l'espace Travail. Le mot de passe doit contenir au moins 4 caractères.
Complexité minimale du mot de passe	Spécifiez la complexité minimale des mots de passe de l'espace Travail. Vous pouvez choisir l'une des options suivantes : • Aucune restriction • 1 lettre et 1 chiffre minimum • 1 lettre, 1 chiffre et 1 caractère spécial minimum • 1 lettre majuscule, 1 lettre minuscule, 1 chiffre et 1 caractère spécial minimum • 1 lettre majuscule, 1 lettre minuscule et 1 chiffre minimum
Délai de sécurité	Spécifiez la période d'inactivité de l'utilisateur avant le verrouillage de l'espace Travail.
Nombre maximum de tentatives de saisie du mot de passe	Spécifiez le nombre de tentatives de saisie du mot de passe possibles avant la réinitialisation de l'espace Travail. Sur les terminaux "Travail et Personnel - Entreprise" et "Travail et Personnel - Régulé", si l'espace Travail et le terminal ont le même mot de passe, le terminal est réinitialisé.
Historique maximum des mots de passe	Spécifiez le nombre de mots de passe précédents que le terminal vérifie pour empêcher un utilisateur de réutiliser de précédents mots de passe pour l'espace Travail. S'il est défini sur 0, le terminal ne vérifie pas les mots de passe précédents.
Délai d'expiration du mot de passe	Spécifiez le nombre maximum de jours pendant lesquels le mot de passe de l'espace Travail peut être utilisé. S'il est défini sur 0, le mot de passe n'expire pas.
Exiger le mot de passe complet du terminal	Spécifiez si les terminaux "Travail et Personnel - Entreprise" et "Travail et Personnel - Régulé" nécessitent un mot de passe pour le terminal ainsi que pour l'espace Travail.
Définir le comportement des mots de passe de l'espace Travail et du terminal	Précisez si le mot de passe de l'espace Travail et le mot de passe du terminal doivent être différents, identiques ou si l'utilisateur peut choisir des mots de passe identiques ou non.

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

Configuration des exigences de mot de passe pour iOS

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

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

Règle	Description
Mot de passe requis pour le terminal	Spécifiez si l'utilisateur doit définir un mot de passe pour le terminal.
Accepter les valeurs simples	Spécifiez si le mot de passe peut contenir des caractères séquentiels ou répétés, tels que DEFG ou 3333.
Exiger des valeurs alphanumériques	Spécifiez si le mot de passe doit contenir à la fois des lettres et des chiffres.
Longueur minimale du mot de passe	Précisez la longueur minimale du mot de passe. Si vous entrez une valeur inférieure à la valeur minimale requise par le terminal iOS, la valeur minimum du terminal est utilisée.
Nombre minimal de caractères complexes	Spécifiez le nombre minimum de caractères non-alphanumériques que doit contenir le mot de passe.
Âge maximal du mot de passe	Spécifiez le nombre maximum de jours pendant lesquels le mot de passe peut être utilisé.
Verrouillage automatique maximum	Spécifiez la valeur maximum à définir par l'utilisateur pour le verrouillage automatique, qui correspond au nombre de minutes d'inactivité à l'issue desquelles le terminal doit se verrouiller. Si vous définissez cette règle sur Aucun, toutes les valeurs prises en charge sont disponibles sur le terminal. Si la valeur sélectionnée se trouve en dehors de la plage prise en charge par le terminal, celui-ci utilisera la valeur la plus proche qu'il prend en charge.
Historique des mots de passe	Spécifiez le nombre de mots de passe précédents que le terminal vérifie pour empêcher un utilisateur de réutiliser un mot de passe récent.
Délai de grâce maximum pour le verrouillage du terminal	Spécifiez la valeur maximum que l'utilisateur peut définir pour le délai de grâce relatif au verrouillage du terminal. Il s'agit du délai pendant lequel le terminal peut rester verrouillé avant qu'un mot de passe soit requis pour le déverrouiller. Si vous définissez cette règle sur "Aucun", toutes les valeurs sont disponibles sur le terminal. Si vous définissez cette règle sur "Immédiatement", le mot de passe est requis immédiatement après le verrouillage du terminal.
Nombre maximum d'échecs de tentatives de saisie du mot de passe	Spécifiez le nombre de tentatives de saisie du mot de passe possibles avant la réinitialisation du terminal.
Autoriser les modifications de mot de passe (sous supervision uniquement)	Spécifiez si l'utilisateur peut ajouter, modifier ou supprimer le mot de passe.

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

Configuration des exigences de mot de passe pour macOS

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

Règle	Description
Cibles de règles de stratégie informatique	Cette règle indique si les règles de stratégie informatique pour le mot de passe s'appliquent uniquement au compte de l'utilisateur attribué ou à l'ensemble du terminal.
Mot de passe requis pour le terminal	Spécifiez si l'utilisateur doit définir un mot de passe pour le terminal.
Autoriser les mots de passe simples	Spécifiez si le mot de passe peut contenir des caractères séquentiels ou répétés, tels que DEFG ou 3333.
Exiger des valeurs alphanumériques	Spécifiez si le mot de passe doit contenir à la fois des lettres et des chiffres.
Longueur minimale du mot de passe	Précisez la longueur minimale du mot de passe.
Nombre minimal de caractères complexes	Spécifiez le nombre minimum de caractères non-alphanumériques que doit contenir le mot de passe.
Délai d'expiration du mot de passe	Spécifiez le nombre maximal de jours pendant lesquels le mot de passe peut être utilisé avant d'expirer et avant que l'utilisateur soit obligé de définir un nouveau mot de passe.
Verrouillage automatique maximum	Spécifiez la durée maximale d'inactivité de l'utilisateur (en minutes) à l'issue de laquelle le terminal doit se verrouiller. Si vous définissez cette période sur « Aucun », l'utilisateur peut sélectionner n'importe quelle valeur.
Historique de mot de passe	Spécifiez le nombre maximal d'anciens mots de passe que le terminal vérifie pour empêcher un utilisateur de réutiliser un mot de passe.
Délai de grâce maximum pour le verrouillage du terminal	Spécifiez la valeur maximum que l'utilisateur peut définir pour le délai de grâce relatif au verrouillage du terminal. Il s'agit du délai pendant lequel le terminal peut rester verrouillé avant qu'un mot de passe soit requis pour le déverrouiller.
Nombre maximum d'échecs de tentatives de saisie du mot de passe	Spécifiez le nombre d'échecs de tentatives de saisie du mot de passe à l'issue desquels le terminal doit être nettoyé.

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

Configuration des exigences de mot de passe pour Android

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

Type d'activation	Règles de mot de passe prises en charge
Contrôles MDM	Utilisez les règles de mot de passe du système d'exploitation natif pour définir les exigences de mot de passe du terminal. Toutes les autres règles de mot de passe sont ignorées par le terminal. Utilisez un profil de conformité pour appliquer les exigences en matière de mot de passe.
Espace Travail uniquement Espace Travail uniquement (Premium)	Utilisez les règles de mot de passe du système d'exploitation natif pour définir les exigences relatives au mot de passe du terminal. Dans la mesure où le terminal dispose uniquement d'un espace Travail, le mot de passe est aussi celui de l'espace Travail. Toutes les autres règles de mot de passe sont ignorées par le terminal. Utiliser un profil de conformité pour faire appliquer les exigences en matière de mot de passe.
Travail et Personnel - Confidentialité de l'utilisateur Travail et Personnel - Confidentialité de l'utilisateur (Premium)	Utilisez les règles de mot de passe du système d'exploitation natif pour définir les exigences de mot de passe du terminal. Utilisez les règles de mot de passe des profils professionnels Android pour définir les exigences de mot de passe pour l'espace Travail. Pour les terminaux BlackBerry optimisés par Android, vous pouvez obliger l'utilisateur à définir des mots de passe différents pour l'espace Travail et le terminal. Toutes les autres règles de mot de passe sont ignorées par le terminal. Utiliser un profil de conformité pour faire appliquer les exigences en matière de mot de passe.
Contrôles MDM (KNOX MDM)	Utilisez les règles de mot de passe KNOX MDM pour configurer les exigences de mot de passe du terminal. Toutes les autres règles de mot de passe sont ignorées par le terminal. Utiliser un profil de conformité pour faire appliquer les exigences en matière de mot de passe.
Espace Travail uniquement (Samsung KNOX)	Utilisez les règles de mot de passe de KNOX Premium - Espace Travail pour définir les exigences de mot de passe pour l'espace Travail. Toutes les autres règles de mot de passe sont ignorées par le terminal. Utiliser un profil de conformité pour faire appliquer les exigences en matière de mot de passe.

Type d'activation	Règles de mot de passe prises en charge
Travail et Personnel - Contrôle total (Samsung KNOX)	Utilisez les règles de mot de passe KNOX MDM pour configurer les exigences de mot de passe du terminal. Utilisez les règles de mot de passe de KNOX Premium - Espace Travail pour définir les exigences de mot de passe pour l'espace Travail. Toutes les autres règles de mot de passe sont ignorées par le terminal. Utiliser un profil de conformité pour faire appliquer les exigences en matière de mot de passe.
Travail et Personnel - Confidentialité de l'utilisateur (Samsung KNOX)	Vous n'avez aucun contrôle sur le mot de passe du terminal. Utilisez les règles de mot de passe de KNOX Premium - Espace Travail pour définir les exigences de mot de passe pour l'espace Travail. Toutes les autres règles de mot de passe sont ignorées par le terminal. Utiliser un profil de conformité pour faire appliquer les exigences en matière de mot de passe.

Android : règles de mot de passe du système d'exploitation natif

Les règles de mot de passe du système d'exploitation natif définissent les exigences de mot de passe des terminaux dotés des types d'activation suivants :

- Contrôles MDM (sans Samsung KNOX)
- Espace Travail uniquement
- Espace Travail uniquement (Premium)
- Travail et Personnel - Confidentialité de l'utilisateur
- Travail et Personnel - Confidentialité de l'utilisateur (Premium)

Règle	Description
Exigences en matière de mot de passe	Précisez les exigences minimum pour le mot de passe. Vous pouvez choisir l'une des options suivantes : • Non spécifié : aucun mot de passe requis • Quelque chose : l'utilisateur doit définir un mot de passe, mais il n'existe aucune exigence de longueur ni de qualité • Numérique : le mot de passe doit inclure au moins un chiffre • Alphabétique : le mot de passe doit inclure au moins une lettre • Alphanumérique : le mot de passe doit inclure au moins une lettre et un chiffre • Complexe : vous pouvez définir des exigences spécifiques pour différents types de caractères

Règle	Description
Nombre maximum d'échecs de tentatives de saisie du mot de passe	Spécifiez le nombre d'échecs de tentatives de saisie du mot de passe à l'issue desquels le terminal doit être nettoyé ou désactivé. Les terminaux activés en mode Commandes MDM sont nettoyés. Les terminaux dotés des types d'activation « Travail et Personnel - confidentialité de l'utilisateur » et « Travail et Personnel - confidentialité de l'utilisateur (Premium) » sont désactivés et le profil professionnel est supprimé.
Délai d'inactivité maximal avant verrouillage	Spécifiez le nombre de minutes d'inactivité de l'utilisateur à l'issue de laquelle le terminal ou l'espace Travail se verrouille. Cette règle est ignorée si aucun mot de passe n'est requis.
Délai d'expiration du mot de passe	Spécifiez le délai maximum pendant lequel le mot de passe peut être utilisé. Passé ce délai, l'utilisateur doit définir un nouveau mot de passe. S'il est défini sur 0, le mot de passe n'expire pas.
Restriction d'historique du mot de passe	Spécifiez le nombre maximum de mots de passe précédents que le terminal vérifie pour empêcher un utilisateur de réutiliser un mot de passe numérique, alphabétique, alphanumérique ou complexe récent. S'il est défini sur 0, le terminal ne vérifie pas les mots de passe précédents.
Longueur minimale du mot de passe	Spécifiez le nombre minimal de caractères pour un mot de passe numérique, alphabétique, alphanumérique ou complexe.
Nombre minimum de lettres majuscules requises dans le mot de passe	Spécifiez le nombre minimum de lettres majuscules que doit contenir un mot de passe complexe.
Nombre minimum de lettres minuscules requises dans le mot de passe	Spécifiez le nombre minimum de lettres minuscules que doit contenir un mot de passe complexe.
Nombre minimum de lettres requises dans un mot de passe	Spécifiez le nombre minimum de lettres que doit contenir un mot de passe complexe.
Nombre minimum de caractères non alphabétiques requis dans le mot de passe	Spécifiez le nombre minimum de caractères non alphabétiques (nombres ou symboles) que doit contenir un mot de passe complexe.
Nombre minimum de chiffres requis dans un mot de passe	Spécifiez le nombre minimum de chiffres que doit contenir un mot de passe complexe.
Nombre de symboles minimum requis dans un mot de passe	Spécifiez le nombre minimum de caractères non-alphanumériques que doit contenir un mot de passe complexe.

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

Android : règles de mot de passe des profils professionnels Android

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

- Travail et Personnel - Confidentialité de l'utilisateur
- Travail et Personnel - Confidentialité de l'utilisateur (Premium)

Règle	Description
Exigences en matière de mot de passe	Spécifiez les exigences minimales à appliquer au mot de passe de l'espace Travail. Vous pouvez choisir l'une des options suivantes : • Non spécifié : aucun mot de passe requis • Quelque chose : l'utilisateur doit définir un mot de passe, mais il n'existe aucune exigence de longueur ni de qualité • Numérique : le mot de passe doit inclure au moins un chiffre • Alphabétique : le mot de passe doit inclure au moins une lettre • Alphanumérique : le mot de passe doit inclure au moins une lettre et un chiffre • Complexe : vous pouvez définir des exigences spécifiques pour différents types de caractères • Numérique complexe : le mot de passe doit contenir des caractères numériques, sans répétition (4444) ni séquence ordonnée (1234, 4321, 2468). • Biométrique (faible) : le mot de passe est compatible avec la technologie de reconnaissance biométrique à sécurité faible. Pour les terminaux BlackBerry optimisés par Android, vous pouvez forcer l'utilisateur à définir des mots de passe différents pour l'espace Travail et le terminal en utilisant la règle des terminaux BlackBerry « Forcer la différence entre le mot de passe de l'espace Travail et celui du terminal ».
Nombre maximum d'échecs de tentatives de saisie du mot de passe	Spécifiez le nombre de tentatives de saisie possibles pour le mot de passe de l'espace Travail avant la désactivation du terminal et la suppression du profil professionnel.
Délai d'inactivité maximal avant verrouillage	Spécifiez le nombre de minutes d'inactivité de l'utilisateur à l'issue desquelles le terminal et l'espace Travail se verrouilleront. Si vous définissez cette règle et la règle « Délai d'inactivité maximal avant verrouillage » du système d'exploitation natif, le terminal et l'espace Travail se verrouilleront une fois le délai écoulé.
Délai d'expiration du mot de passe	Spécifiez la durée de validité maximale du mot de passe de l'espace Travail. Passé ce délai, l'utilisateur devra définir un nouveau mot de passe. S'il est défini sur 0, le mot de passe n'expire pas.
Restriction d'historique du mot de passe	Spécifiez le nombre maximum de mots de passe d'espace Travail précédents que le terminal doit vérifier pour empêcher un utilisateur de réutiliser un mot de passe numérique, alphabétique, alphanumérique ou complexe récent. S'il est défini sur 0, le terminal ne vérifie pas les mots de passe précédents.

Règle	Description
Longueur minimale du mot de passe	Spécifiez le nombre minimal de caractères pour un mot de passe d'espace Travail numérique, alphabétique, alphanumérique ou complexe.
Nombre minimum de lettres majuscules requises dans le mot de passe	Spécifiez le nombre minimum de lettres majuscules que doit contenir un mot de passe d'espace Travail complexe.
Nombre minimum de lettres minuscules requises dans le mot de passe	Spécifiez le nombre minimum de lettres minuscules que doit contenir un mot de passe d'espace Travail complexe.
Nombre minimum de lettres requises dans un mot de passe	Spécifiez le nombre minimum de lettres que doit contenir un mot de passe d'espace Travail complexe.
Nombre minimum de caractères non alphabétiques requis dans le mot de passe	Spécifiez le nombre minimum de caractères non alphabétiques (chiffres ou symboles) que doit contenir un mot de passe d'espace Travail complexe.
Nombre minimum de chiffres requis dans un mot de passe	Spécifiez le nombre minimum de chiffres que doit contenir un mot de passe d'espace Travail complexe.
Nombre de symboles minimum requis dans un mot de passe	Spécifiez le nombre minimum de caractères non alphanumériques que doit contenir un mot de passe d'espace Travail complexe.

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

Android : règles de mot de passe de KNOX MDM

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

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

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

Règle	Description
Exigences en matière de mot de passe	Précisez les exigences minimum pour le mot de passe. Vous pouvez choisir l'une des options suivantes : • Numérique : le mot de passe doit inclure au moins un chiffre • Alphabétique : le mot de passe doit inclure au moins une lettre • Alphanumérique : le mot de passe doit inclure au moins une lettre et un chiffre • Complexe : vous pouvez définir des exigences spécifiques pour différents types de caractères
Longueur minimale du mot de passe	Précisez la longueur minimale du mot de passe. Le mot de passe doit contenir au moins 4 caractères.
Nombre minimum de lettres minuscules requises dans le mot de passe	Spécifiez le nombre minimum de lettres minuscules que doit contenir un mot de passe complexe.
Nombre minimum de lettres majuscules requises dans le mot de passe	Spécifiez le nombre minimum de lettres majuscules que doit contenir un mot de passe complexe.
Nombre minimum de caractères complexes requis dans un mot de passe	Spécifiez le nombre minimum de caractères complexes (par exemple, nombres ou symboles) que doit contenir un mot de passe complexe. Si vous définissez cette valeur sur 1, au moins un chiffre est requis. Si vous spécifiez une valeur supérieure à 1, au moins un chiffre et un symbole sont requis.
Longueur maximum de la séquence de caractères	Spécifiez la longueur maximale d'une séquence alphabétique autorisée dans un mot de passe alphabétique, alphanumérique ou complexe. Par exemple, si la longueur est définie sur 5, la séquence alphabétique "abcde" est autorisée, mais pas la séquence "abcdef". Si elle est définie sur 0, il n'y a aucune restriction de séquence alphabétique.
Délai d'inactivité maximal avant verrouillage	Spécifiez le délai d'inactivité à l'issue duquel le terminal doit se verrouiller. Si le terminal est géré par plusieurs solutions EMM, la valeur la plus faible est utilisée comme délai d'inactivité. Si le terminal utilise un mot de passe, l'utilisateur doit saisir celui-ci pour le déverrouiller. Si ce délai est défini sur 0, le terminal ne dispose d'aucun délai d'inactivité.
Nombre maximum d'échecs de tentatives de saisie du mot de passe	Spécifiez le nombre d'échecs de tentatives de saisie du mot de passe à l'issue desquels le terminal doit être nettoyé.
Restriction d'historique du mot de passe	Spécifiez le nombre maximum de mots de passe précédents que le terminal vérifie pour empêcher un utilisateur de réutiliser un mot de passe récent. S'il est défini sur 0, le terminal ne vérifie pas les mots de passe précédents.
Délai d'expiration du mot de passe	Spécifiez le délai maximum pendant lequel le mot de passe du terminal peut être utilisé. Passé ce délai, le mot de passe expire et l'utilisateur doit en définir un nouveau. S'il est défini sur 0, le mot de passe n'expire pas.

Règle	Description
Autoriser la visibilité du mot de passe	Spécifiez si le mot de passe du terminal est visible lorsque l'utilisateur le saisit. Si cette règle n'est pas sélectionnée, les utilisateurs et les applications tierces ne peuvent pas modifier la configuration de la visibilité.
Autoriser l'authentification par empreinte digitale	Spécifiez si l'utilisateur peut utiliser l'authentification par empreintes digitales pour le terminal.

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

Android : KNOX Premium - Règles de mot de passe de l'espace Travail

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

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

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

Règle	Description
Exigences en matière de mot de passe	Précisez les exigences minimum pour le mot de passe. Vous pouvez choisir l'une des options suivantes : • Numérique : le mot de passe doit inclure au moins un chiffre • Numérique complexe : le mot de passe doit inclure au moins un chiffre, sans séquences répétées (4444) ni dans l'ordre (1234, 4321, 2468) • Alphabétique : le mot de passe doit inclure au moins une lettre • Alphanumérique : le mot de passe doit inclure au moins une lettre et un chiffre • Complexe : vous pouvez définir des exigences spécifiques pour différents types de caractères
Nombre minimum de lettres minuscules requises dans le mot de passe	Spécifiez le nombre minimum de lettres minuscules que doit contenir un mot de passe complexe.
Nombre minimum de lettres majuscules requises dans le mot de passe	Spécifiez le nombre minimum de lettres majuscules que doit contenir un mot de passe complexe.
Nombre minimum de caractères complexes requis dans un mot de passe	Spécifiez le nombre minimum de caractères complexes (par exemple, nombres ou symboles) que doit contenir un mot de passe complexe. Au moins trois caractères complexes sont requis, y compris au moins un nombre et un symbole.

Règle	Description
Longueur maximum de la séquence de caractères	Spécifiez la longueur maximale d'une séquence alphabétique autorisée dans un mot de passe alphabétique, alphanumérique ou complexe. Par exemple, si la longueur est définie sur 5, la séquence alphabétique "abcde" est autorisée, mais pas la séquence "abcdef". Si elle est définie sur 0, il n'y a aucune restriction de séquence alphabétique.
Longueur minimale du mot de passe	Précisez la longueur minimale du mot de passe. Si vous saisissez une valeur inférieure au minimum requis par KNOX Workspace, la valeur minimum de KNOX Workspace est utilisée.
Délai d'inactivité maximal avant verrouillage	Spécifiez la période d'inactivité de l'utilisateur dans l'espace Travail avant le verrouillage de l'espace Travail. Si elle est définie sur 0, l'espace Travail ne dispose d'aucune période d'inactivité.
Nombre maximum d'échecs de tentatives de saisie du mot de passe	Spécifiez le nombre de tentatives de saisie du mot de passe possibles avant la réinitialisation de l'espace Travail. S'il est défini sur 0, il n'existe aucune restriction du nombre de tentatives de saisie du mot de passe pour un utilisateur.
Restriction d'historique du mot de passe	Spécifiez le nombre maximum de mots de passe précédents que le terminal vérifie pour empêcher un utilisateur de réutiliser un mot de passe récent. S'il est défini sur 0, le terminal ne vérifie pas les mots de passe précédents.
Délai d'expiration du mot de passe	Spécifiez le nombre maximum de jours pendant lesquels le mot de passe peut être utilisé. Passé ce délai, le mot de passe expire et l'utilisateur doit en définir un nouveau. S'il est défini sur 0, le mot de passe n'expire pas.
Nombre minimum de caractères modifiés pour les nouveaux mots de passe	Spécifiez le nombre minimum de caractères modifiés que doit contenir un nouveau mot de passe par rapport au précédent. Si vous définissez cette règle sur 0, aucune restriction ne s'applique.
Autoriser les verrouillages personnalisés	Spécifiez si le terminal est autorisé à utiliser des verrouillages personnalisés, comme des agents d'approbation. Si cette règle n'est pas sélectionnée, les verrouillages personnalisés sont désactivés.
Autoriser les agents d'approbation de verrouillage	Spécifiez si l'utilisateur peut maintenir l'espace Travail déverrouillé pendant 2 heures à l'issue du délai d'inactivité maximum de l'espace Travail. Si vous ne définissez aucune valeur de délai d'inactivité, l'utilisateur peut effectuer cette action par défaut.
Autoriser la visibilité du mot de passe	Spécifiez si le mot de passe du terminal est visible lorsque l'utilisateur le saisit. Si cette règle n'est pas sélectionnée, les utilisateurs et les applications tierces ne peuvent pas modifier la configuration de la visibilité.
Appliquer l'authentification à deux facteurs	Spécifiez si l'utilisateur doit utiliser l'authentification à deux facteurs pour accéder à l'espace Travail. Par exemple, vous pouvez utiliser cette règle si vous souhaitez que l'utilisateur s'authentifie à l'aide d'une empreinte et d'un mot de passe.

Règle	Description
Autoriser l'authentification par empreinte digitale	Spécifiez si l'utilisateur peut utiliser l'authentification par empreintes digitales pour accéder à l'espace Travail.

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

Configuration des exigences de mot de passe pour Windows

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

Règle	Description
Mot de passe requis pour le terminal	Spécifiez si l'utilisateur doit définir un mot de passe pour le terminal.
Autoriser les mots de passe simples	Spécifiez si le mot de passe peut contenir des caractères séquentiels ou répétés, tels que DEFG ou 3333.
Longueur minimale du mot de passe	Précisez la longueur minimale du mot de passe. Le mot de passe doit contenir au moins 4 caractères.
Complexité du mot de passe	Spécifiez la complexité du mot de passe. Vous pouvez choisir les options suivantes : • Alphanumérique : le mot de passe doit contenir des lettres et des chiffres • Numérique : le mot de passe doit contenir uniquement des chiffres
Nombre minimum de types de caractères	Spécifiez le nombre minimum de types de caractères que doit contenir un mot de passe alphanumérique. Vous avez le choix entre les options suivantes : **1.** Chiffres requis **2.** Chiffres et lettres minuscules requis **3.** Chiffres, lettres minuscules et lettres majuscules requis **4.** Chiffres, lettres minuscules, lettres majuscules et caractères spéciaux requis Les exigences relatives aux caractères du mot de passe pour les tablettes et ordinateurs Windows 10 dépendent du type de compte d'utilisateur, et non de ce paramètre.
Expiration du mot de passe	Spécifiez le nombre maximum de jours pendant lesquels le mot de passe peut être utilisé. S'il est défini sur 0, le mot de passe n'expire pas.
Historique de mot de passe	Spécifiez le nombre de mots de passe précédents que le terminal vérifie pour empêcher un utilisateur de réutiliser un mot de passe récent. S'il est défini sur 0, le terminal ne vérifie pas les mots de passe précédents.

Règle	Description
Nombre maximum d'échecs de tentatives de saisie du mot de passe	Spécifiez le nombre de tentatives de saisie du mot de passe possibles avant la réinitialisation du terminal. S'il est défini sur 0, le terminal n'est pas réinitialisé, quel que soit le nombre de fois où l'utilisateur saisit un mot de passe incorrect. Cette règle ne s'applique pas aux terminaux qui autorisent plusieurs comptes d'utilisateur, y compris les tablettes et ordinateurs Windows 10.
Délai d'inactivité maximal avant verrouillage	Spécifiez la période d'inactivité de l'utilisateur à l'issue de laquelle le terminal se verrouille. S'il est défini sur 0, le terminal ne se verrouille pas automatiquement.
Autoriser l'accès sans mot de passe	Spécifiez si l'utilisateur doit saisir le mot de passe à l'issue de la période de grâce associée au délai d'inactivité. Si cette règle est sélectionnée, l'utilisateur peut définir la période de grâce du mot de passe sur le terminal. Cette règle ne s'applique pas aux ordinateurs et tablettes Windows 10.

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

Comment BlackBerry UEM choisit la stratégie informatique à attribuer

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

Attribué à	Règles
Compte d'utilisateur (afficher l'onglet Synthèse)	1. Une stratégie informatique directement attribuée à un compte d'utilisateur est prioritaire sur une stratégie informatique attribuée indirectement par groupe d'utilisateurs. 2. Si un utilisateur est membre de plusieurs groupes d'utilisateurs dotés de stratégies informatiques différentes, BlackBerry UEM attribue la stratégie informatique avec le rang le plus élevé. 3. La stratégie informatique par défaut est attribuée si aucune stratégie informatique n'est attribuée à un compte d'utilisateur directement ou par appartenance aux groupes d'utilisateurs.
Terminal (afficher l'onglet Terminal)	Par défaut, un terminal hérite de la stratégie informatique attribuée par BlackBerry UEM à l'utilisateur qui active le terminal. Si un terminal appartient à un groupe de terminaux, les règles suivantes s'appliquent : 1. Une stratégie informatique attribuée à un groupe de terminaux est prioritaire sur la stratégie informatique attribuée par BlackBerry UEM à un compte d'utilisateur. 2. Si un terminal est membre de plusieurs groupes de terminaux dotés de stratégies informatiques différentes, BlackBerry UEM attribue la stratégie informatique avec le rang le plus élevé.

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

- Attribuer une stratégie informatique à un compte d'utilisateur, groupe d'utilisateurs ou groupe de terminaux
- Supprimer une stratégie informatique d'un compte d'utilisateur, groupe d'utilisateurs ou groupe de terminaux

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

Tâches connexes

Classer les stratégies informatiques

Création et gestion des stratégies informatiques

Vous pouvez utiliser la stratégie informatique par défaut ou créer des stratégies informatiques personnalisées (pour spécifier les règles de stratégie informatique pour différents groupes d'utilisateurs de votre organisation, par exemple). Si vous prévoyez d'utiliser la stratégie informatique par défaut, il vous est conseillé de l'examiner et, si nécessaire, de la mettre à jour pour veiller à ce que les règles respectent les normes de sécurité de votre organisation.

Créer une stratégie informatique

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

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

À la fin : classez les stratégies informatiques.

Tâches connexes

Attribuer un profil ou une stratégie informatique à un compte d'utilisateur
Attribuer un profil ou une stratégie informatique à un groupe d'utilisateurs

Copier une stratégie informatique

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

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

À la fin : classez les stratégies informatiques.

Tâches connexes

Attribuer un profil ou une stratégie informatique à un compte d'utilisateur
Attribuer un profil ou une stratégie informatique à un groupe d'utilisateurs

Classer les stratégies informatiques

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

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

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

Concepts connexes

Comment BlackBerry UEM choisit la stratégie informatique à attribuer

Afficher une stratégie informatique

Vous pouvez afficher les informations suivantes sur une stratégie informatique :

- Règles de stratégie informatique spécifiques à chaque type de terminal
- Liste et nombre de comptes d'utilisateur auxquels est attribuée la stratégie informatique (directement et indirectement)
- Liste et nombre de groupes d'utilisateurs auxquels est attribuée la stratégie informatique (directement)

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

Modifier une stratégie informatique

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

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

Tâches connexes

Classer les stratégies informatiques

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

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

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

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

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

Concepts connexes

Comment BlackBerry UEM choisit la stratégie informatique à attribuer

Supprimer une stratégie informatique

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

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

Concepts connexes

Comment BlackBerry UEM choisit la stratégie informatique à attribuer

Exporter des stratégies informatiques

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

Remarque :

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

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

Contrôle des fonctionnalités du terminal BlackBerry OS à l'aide de stratégies informatiques

Si le domaine BlackBerry UEM prend en charge les terminaux BlackBerry OS (versions 5.0 à 7.1), vous pouvez utiliser les stratégies informatiques BlackBerry OS pour contrôler et gérer les terminaux BlackBerry OS, BlackBerry Desktop Software et BlackBerry Web Desktop Manager dans l'environnement de votre entreprise.

Pour plus d'informations sur la création ou la mise à jour des stratégies informatiques pour les terminaux BlackBerry OS, téléchargez le Guide d'administration à l'adresse help.blackberry.com/detectLang/bes5-for-exchange/.

Tâches connexes

Attribuer une stratégie informatique BlackBerry OS, un profil ou une configuration logicielle à un groupe d'utilisateurs
Attribuer une stratégie informatique BlackBerry OS, un profil ou une configuration logicielle à un compte d'utilisateur

Contrôle de BlackBerry Dynamics sur les terminaux des utilisateurs

Le profil BlackBerry Dynamics active BlackBerry Dynamics pour les utilisateurs et définit les normes pour l'accès aux applications BlackBerry Dynamics, la protection des données et la journalisation.

BlackBerry UEM comprend un profil BlackBerry Dynamics par défaut doté de paramètres préconfigurés. Si aucun profil BlackBerry Dynamics n'est attribué à un compte d'utilisateur, à un groupe d'utilisateurs auquel appartient un utilisateur ou à un groupe de terminaux auquel appartiennent les terminaux d'un utilisateur, BlackBerry UEM envoie le profil BlackBerry Dynamics par défaut aux terminaux de l'utilisateur. BlackBerry UEM envoie automatiquement un profil BlackBerry Dynamics à un terminal lorsqu'un utilisateur l'active, lorsque vous mettez à jour un profil BlackBerry Dynamics attribué ou lorsqu'un profil BlackBerry Dynamics différent est attribué à un compte d'utilisateur ou à un terminal.

Vous pouvez attribuer le profil BlackBerry Dynamics à des comptes d'utilisateur, groupes d'utilisateurs ou groupes de terminaux.

Référence connexe

Gérer les profils de conformité BlackBerry Dynamics

Créer un profil BlackBerry Dynamics

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Stratégie > BlackBerrry Dynamics**
3. Cliquez sur +.
4. Saisissez le nom et la description du profil.
5. Configurez les valeurs qui conviennent dans les paramètres de profil. Pour plus d'informations sur les différents paramètres de profil, reportez-vous à Paramètres de profil BlackBerry Dynamics.
6. Cliquez sur **Ajouter**.

À la fin : Si nécessaire, classez les profils.

Tâches connexes

Attribuer un profil ou une stratégie informatique à un groupe d'utilisateurs
Attribuer un profil ou une stratégie informatique à un compte d'utilisateur

Référence connexe

Paramètres de profil BlackBerry Dynamics

Application des règles de conformité aux terminaux

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

Un profil de conformité spécifie les informations suivantes :

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

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

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

Créer un profil de conformité

Avant de commencer :

- Si vous définissez des règles pour autoriser ou interdire certaines applications, ajoutez ces applications à la liste des applications interdites. Pour plus d'informations, reportez-vous à Ajouter une application à la liste des applications limitées. Notez que ceci ne s'applique pas aux applications intégrées pour les terminaux iOS supervisés 9.3.2 et les versions ultérieures. Pour restreindre les applications intégrées, vous devez créer un profil de conformité et ajouter les applications à la liste d'applications limitées dans le profil. Pour plus d'informations, reportez-vous à iOS : paramètres de profil de conformité.
- Pour surveiller les applications dans les profils de conformité pour les terminaux Windows Phone, vous devez télécharger un jeton d'inscription d'application (AET). Pour plus d'informations, reportez-vous à Télécharger un jeton d'inscription d'application pour les terminaux Windows Phone .
- Si vous souhaitez envoyer une notification par e-mail aux utilisateurs lorsque leurs terminaux ne sont pas conformes, modifiez l'e-mail de conformité par défaut ou créez un nouveau modèle d'e-mail. Pour plus d'informations, reportez-vous à Création d'un modèle pour les notifications d'e-mail de conformité.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Conformité > Conformité**.
3. Cliquez sur +.
4. Saisissez le nom et la description du profil de conformité.
5. Si vous souhaitez envoyer un message de notification aux utilisateurs lorsque leurs terminaux ne sont plus conformes, effectuez l'une des opérations suivantes :
   - Dans la liste déroulante **E-mail envoyé lorsqu'une violation est détectée**, sélectionnez un modèle d'email. Pour afficher l'e-mail de conformité par défaut, cliquez sur Paramètres > Paramètres généraux > Modèles d'e-mail.
   - Dans la liste déroulante **Intervalle d'application**, sélectionnez l'intervalle des vérifications de conformité à effectuer par BlackBerry UEM.
   - Développez la section **Envoi d'une notification de terminal lorsqu'une violation est détectée**. Modifiez l'e-mail, si nécessaire.

   Si vous souhaitez utiliser des variables pour renseigner les informations sur l'utilisateur, le terminal et la conformité dans les notifications, reportez-vous à la sectionVariables. Vous pouvez également définir et utiliser vos propres variables personnalisées via la console de gestion. Pour plus d'informations, reportez-vous àVariables personnalisées.
6. Cliquez sur l'onglet correspondant à chaque type de terminal de votre organisation et configurez les valeurs appropriées pour chaque paramètre de profil. Pour plus de détails sur chaque paramètre de profil, reportez-vous à la section Paramètres des profils de conformité.
7. Cliquez sur **Ajouter**.

À la fin : Si nécessaire, classez les profils.

Tâches connexes

Attribuer un profil ou une stratégie informatique à un groupe d'utilisateurs
Attribuer un profil ou une stratégie informatique à un compte d'utilisateur

Création d'un modèle pour les notifications d'e-mail de conformité

Vous pouvez créer plusieurs modèles d'e-mail, les personnaliser pour des types de terminal ou groupe d'utilisateurs spécifiques et attribuer un modèle approprié à chaque compte d'utilisateur. Lorsque le terminal d'un utilisateur ne respecte pas avec un profil de conformité, BlackBerry UEM peut envoyer un e-mail personnalisé

basé sur le modèle attribué. BlackBerry 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, BlackBerry UEM utilise le modèle par défaut.

1. Dans la barre de menus, cliquez sur **Paramètres** > **Paramètres généraux**.
2. Cliquez sur **Modèles d'e-mail**.
3. Cliquez sur +. Sélectionnez **Violation de conformité**.
4. Dans le champ **Nom**, saisissez un nom pour identifier ce modèle.
5. Dans le champ **Objet**, saisissez un objet pour l'e-mail.
6. Dans le champ **Message**, saisissez le corps du texte de l'e-mail sur la conformité. Utilisez l'éditeur HTML pour sélectionner le format de police et insérer des images (par exemple, un logo d'entreprise). Insérez des variables dans le texte pour personnaliser le message (par exemple, utilisez la variable %UserDisplayName% pour insérer le nom du destinataire). Pour obtenir la liste des variables disponibles, consultez Variables par défaut.
7. Cliquez sur **Enregistrer**.

Gérer les profils de conformité BlackBerry Dynamics

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

Pour plus d'informations sur la création de profils de conformité dans BlackBerry UEM, reportez-vous à Création d'un profil de conformité.

Paramètre	Description
Système d'exploitation cracké	Ce paramètre spécifie les actions prises si un utilisateur ou un utilisateur malveillant contourne diverses restrictions sur un terminal pour modifier le système d'exploitation, installer des applications non approuvées ou obtenir des autorisations élevées, ainsi que les actions prises pour les applications BlackBerry Dynamics si un système d'exploitation cracké est utilisé.
Vérification du système d'exploitation	Ce paramètre spécifie les versions autorisées et interdites du système d'exploitation ainsi que les actions prises pour les applications BlackBerry Dynamics si un système d'exploitation interdit est installé sur un terminal.
Vérification du modèle de matériel	Ce paramètre spécifie les modèles de matériel autorisés et interdits ainsi que les actions prises pour les applications BlackBerry Dynamics si un modèle de matériel interdit est utilisé.
Vérification de la version de la bibliothèque BlackBerry Dynamics	Ce paramètre spécifie les bibliothèques BlackBerry Dynamics qui peuvent être utilisées ainsi que les actions prises pour les applications BlackBerry Dynamics si un terminal utilise une version non autorisée de la bibliothèque.

Paramètre	Description
Vérification de la connectivité	Ce paramètre spécifie si un terminal doit se connecter à BlackBerry UEM sous un certain nombre de jours ainsi que les actions prises pour les applications BlackBerry Dynamics si un terminal ne se connecte pas à BlackBerry UEM. Le sous-paramètre Baser l'intervalle de connectivité sur des applications de délégation de l'authentification détermine si l'application définie comme délégué d'authentification gère l'intervalle de connectivité. Si vous utilisez le délégué d'authentification pour gérer l'intervalle de connectivité, les applications les moins utilisées ne seront pas bloquées ni nettoyées si elles ne s'y connectent pas. BlackBerry UEM.

Concepts connexes

Contrôle de BlackBerry Dynamics sur les terminaux des utilisateurs

Configuration de Enterprise Management Agent

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

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

Pour les terminaux BlackBerry 10, le profil Enterprise Management Agent vous permet de définir quelles suites de codes de la bibliothèque SSL sont prises en charge par le terminal. Le fait de limiter les suites de codes prises en charge n'affecte pas la communication du terminal avec BlackBerry UEM mais peut avoir un impact sur la communication avec les autres serveurs de votre entreprise, en fonction des besoins de ces serveurs.

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

Créer un profil Enterprise Management Agent

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

À la fin : Si nécessaire, classez les profils.

Concepts connexes

Paramètres du profil Enterprise Management Agent

Tâches connexes

Attribuer un profil ou une stratégie informatique à un groupe d'utilisateurs
Attribuer un profil ou une stratégie informatique à un compte d'utilisateur

Limiter les terminaux à une application

Sur les terminauxiOSsupervisés, les terminauxAndroidgérés avecSamsung KNOXMDM ouWindows 10Enterprise et les terminauxWindows 10Education gérés avec MDM, vous pouvez utiliser un profil du mode de verrouillage des applications pour limiter les terminaux à une seule application. Par exemple, vous pouvez limiter l'accès à une seule application pour les formations ou les démonstrations en points de vente. Sur les terminauxiOS, le bouton d'accueil d'un terminal est désactivé et le terminal ouvre automatiquement l'application lorsque l'utilisateur sort le terminal de veille ou le redémarre.

Créer un profil du mode de verrouillage

Spécifiez une seule application à exécuter sur les terminaux, puis sélectionnez les paramètres de terminal que vous souhaitez activer pour l'utilisateur. Pour les terminaux iOS supervisés, vous pouvez sélectionner une application dans la liste des applications, spécifier l'identifiant d'offre de l'application ou sélectionner une application intégrée. Pour les terminaux Android gérés à l'aide de Samsung KNOX MDM, spécifiez l'identifiant du package d'application que vous souhaitez définir en tant qu'écran d'accueil. Pour les terminaux Windows 10 gérés avec MDM, spécifiez le compte et l'ID du modèle d'utilisateur de l'application (AUMID). Rendez-vous sur docs.microsoft.com pour trouver l'AUMID.

Remarque : si l'utilisateur n'installe pas l'application sur un terminal, lors de l'attribution du profil à un utilisateur ou à un groupe d'utilisateurs, le terminal n'est pas limité à l'application.

Avant de commencer : pour les terminaux iOS, si vous prévoyez d'utiliser la liste des applications pour sélectionner une application, vérifiez qu'elle y est bien disponible.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Stratégie > Mode de verrouillage des applications**.
3. Cliquez sur +.
4. Saisissez le nom et la description du profil.
5. Spécifiez les types de terminaux auxquels le profil s'applique.
6. Effectuez l'une des tâches suivantes :

Tâche	Étapes
Spécifier l'application à exécuter sur les terminaux iOS	Dans la section **Spécifier l'application à exécuter sur le terminal**, effectuez l'une des opérations suivantes : • Cliquez sur **Ajouter une application**, puis sur une application de la liste. • Cliquez sur **Spécifier l'ID d'offre d'une application** et saisissez l'ID d'offre (par exemple, <*com.company.appname* >). Vous pouvez utiliser les majuscules, les minuscules, les chiffres de 0 à 9, le tiret (-) et le point (.). • Cliquez sur **Sélectionner une application iOS intégrée** et sélectionnez une application dans la liste déroulante.
Spécifier l'application à exécuter sur les terminaux Android	Dans le champ **Spécifier l'application à exécuter sur le terminal**, saisissez l'identifiant du package d'application que vous souhaitez définir en tant qu'écran d'accueil. Par exemple, si vous souhaitez BBM Meetings comme application, saisissez `com.blackberry.bbm.meetings`.
Spécifier l'application à exécuter sur les terminaux Windows 10	• Dans le champ **Compte**, saisissez le nom d'un compte d'utilisateur qui inclut le nom de domaine et le nom d'utilisateur. Pour un utilisateur local, utilisez le nom du terminal à la place du nom de domaine. • Dans le champ **ID du modèle d'utilisateur d'application**, saisissez l'AUMID de l'application (par exemple, l'AUMID de l'application Calculette est `Microsoft.WindowsCalculator_8wekyb3d8bbwe!App`).

7. Pour les terminaux iOS et Android, dans **Paramètres administrateur**, sélectionnez les options que vous souhaitez activer pour l'utilisateur lors de l'utilisation de l'application.
8. Pour les terminaux iOS, dans **Paramètres utilisateur**, sélectionnez les options que l'utilisateur peut activer.
9. Cliquez sur **Ajouter**.

À la fin : Si nécessaire, classez les profils.

Tâches connexes

Ajouter une application Android à la liste des applications si BlackBerry UEM n'est pas configuré pour les profils professionnels Android
Ajouter une application Android à la liste des applications si BlackBerry UEM est configuré pour les profils professionnels Android
Ajouter une application iOS à la liste des applications
Attribuer un profil ou une stratégie informatique à un groupe d'utilisateurs
Attribuer un profil ou une stratégie informatique à un compte d'utilisateur

Contrôle des versions du logiciel qui sont installées sur les terminaux

Vous pouvez contrôler les versions logicielles des terminaux qui sont installées sur les terminaux Android avec des activations Espace Travail uniquement, les terminaux Samsung KNOX et les terminaux BlackBerry 10.

Sur les terminaux exécutant Android 6.0 et versions ultérieures et activés avec Espace Travail uniquement, vous pouvez spécifier si l'utilisateur peut choisir le moment où les mises à jour logicielles disponibles seront installées ou si elles sont automatiquement installées. Vous pouvez spécifier différentes règles en fonction du modèle du terminal et de la version du SE actuellement installée.

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

Pour les terminaux exécutant BlackBerry 10 OS version 10.3.1 ou ultérieure activés avec Travail et Personnel - Régulé ou Espace Travail uniquement, vous avez la possibilité de limiter les versions du logiciel que les terminaux BlackBerry 10 peuvent installer à l'aide d'un profil d'exigences SR des terminaux. Vous pouvez également ajouter des exceptions aux paramètres globaux pour certains modèles de terminaux spécifiques. Par exemple, vous pouvez tester une version de logiciel avant de l'utiliser dans votre organisation.

Pour appliquer une action particulière en cas d'installation d'une version restreinte du logiciel sur un terminal, vous devez créer un profil de conformité et l'attribuer aux utilisateurs, groupes d'utilisateurs ou groupes de terminaux. Le profil de conformité spécifie les actions que seront prises si l'utilisateur ne supprime pas la version restreinte du logiciel du terminal.

Créer un profil d'exigences SR pour les terminaux Android avec des activations Espace Travail uniquement

Avant de commencer : Vérifiez qu'une licence E-FOTA a été ajoutée à BlackBerry UEM. Pour ajouter une licence E-FOTA, reportez-vous à la section Ajouter une licence E-FOTA dans le contenu relatif à la configuration.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Conformité > Configuration logicielle minimale requise du terminal**
3. Cliquez sur +.
4. Saisissez le nom et la description du profil.
5. Cliquez sur l'onglet **Android**.
6. Dans le tableau **Règle de mise à jour de système d'exploitation Espace Travail uniquement**, cliquez sur +.
7. Dans la liste déroulante **Modèle du terminal**, sélectionnez un modèle de terminal.
8. Dans la liste déroulante **Version du système d'exploitation**, sélectionnez la version du système d'exploitation installée.
9. Dans la liste **Mettre à jour la règle**, sélectionnez l'une des options suivantes.
   - Sélectionnez **Par défaut** pour permettre à l'utilisateur de choisir le moment où les mises à jour seront installées.
   - Sélectionnez **Mettre automatiquement à jour** pour installer les mises à jour sans demander à l'utilisateur.
   - Sélectionnez **Mettre automatiquement à jour entre** pour installer les mises à jour entre les heures que vous avez définies, sans demander à l'utilisateur. L'utilisateur peut choisir d'installer les mises à jour en dehors de cette fenêtre.
   - Sélectionnez **Reporter jusqu'à 30 jours** pour bloquer l'installation des mises à jour pendant 30 jours. Après 30 jours, l'utilisateur peut choisir le moment d'installer une mise à jour. Selon le fabricant du terminal et

le fournisseur de services sans fil, il est possible que les mises à jour de sécurité ne puissent pas être reportées.

10. Une fois terminé, cliquez sur **Ajouter**.
11. Répétez les étapes 6 à 10 pour chacune des règles que vous souhaitez ajouter.
12. Cliquez sur **Ajouter**.

À la fin : Si nécessaire, classez les profils.

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

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Conformité > Configuration logicielle minimale requise du terminal**
3. Cliquez sur +.
4. Saisissez le nom et la description du profil.
5. Cliquez sur l'onglet **Android**.
6. Dans le tableau **Règles relatives aux micrologiciels des terminaux Samsung**, cliquez sur +.
7. Dans le champ **Modèle du terminal**, saisissez le modèle de terminal ou sélectionnez-le dans la liste déroulante.
8. Dans la liste déroulante **Langue**, sélectionnez une langue.
9. Dans le champ **Code de l'opérateur**, saisissez le code CSC du fournisseur de services sans fil pour le terminal.
10. Cliquez sur **Obtenir la version du micrologiciel**.
11. Répétez les étapes 5 à 8 pour chaque règle de micrologiciel que vous souhaitez ajouter.
12. Une fois terminé, cliquez sur **Ajouter**.
13. Dans le tableau **Règles relatives aux micrologiciels des terminaux Samsung**, cliquez sur **Planifier** en regard de la version du micrologiciel que vous avez ajoutée.
14. Dans la boîte de dialogue **Planifier une mise à jour forcée**, procédez comme suit :
    a) Dans les champs **Planifier une mise à jour forcée entre**, sélectionnez une plage de dates au cours de laquelle la mise à jour doit être installée. La plage de dates doit contenir de 3 à 7 jours. La valeur par défaut est de 7 jours.
    b) Dans les listes déroulantes **Planifier une mise à jour forcée pendant les heures de**, précisez le moment où la mise à jour forcée doit être installée et le fuseau horaire de l'utilisateur. La durée doit être comprise entre 1 et 12 heures.
15. Cliquez sur **Enregistrer**.

À la fin : Si nécessaire, classez les profils.

Créer un profil de configuration logicielle minimale requise du terminal pour les terminaux BlackBerry 10

Avant de commencer : Créez ou modifiez un profil de conformité définissant les actions prises si une application limitée est installée sur un terminal.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Conformité > Configuration logicielle minimale requise du terminal**
3. Cliquez sur +.
4. Saisissez le nom et la description du profil.
5. Cliquez sur l'onglet **BlackBerry**.

6. Pour afficher la liste de toutes les versions logicielles des terminaux BlackBerry 10 ainsi que le fournisseur de services, le modèle de terminal, l'ID de matériel, la version du logiciel et les informations d'état de révocation correspondants, cliquez sur **Afficher une liste des versions logicielles des terminaux**.
7. Cochez la case **Mise à jour requise** pour contraindre les utilisateurs à mettre à jour leurs terminaux vers une version du logiciel définie dans le profil.
8. Dans le champ **Période de grâce**, saisissez le laps de temps, en heures, pouvant s'écouler avant que les utilisateurs doivent mettre à jour leurs terminaux. Si les utilisateurs ne mettent pas à jour leurs terminaux durant la période de grâce ou si vous définissez la période de grâce sur 0, la mise à jour du logiciel est automatiquement installée sur les terminaux.
9. Dans la liste déroulante **Version minimale du logiciel**, sélectionnez la version minimale du logiciel qu'un terminal BlackBerry 10 doit exécuter.
10. Dans la liste déroulante **Version maximale du logiciel**, sélectionnez la version maximale du logiciel qu'un terminal BlackBerry 10 doit exécuter.
11. Pour ignorer le paramètre global d'un modèle de terminal, procédez comme suit :
    a) Dans le tableau **Exceptions**, cliquez sur +.
    b) Dans la liste déroulante **Disposition**, sélectionnez si vous souhaitez autoriser ou interdire des versions du logiciel. Si vous spécifiez une plage interdite et n'avez pas spécifié de plage autorisée pour un modèle de terminal, une deuxième colonne apparait pour vous permettre de le faire. Si une plage autorisée n'est pas spécifiée, les paramètres globaux ne s'appliquent plus au modèle de terminal et toutes les versions du logiciel, sauf l'exception, sont automatiquement autorisées.
    c) Dans la liste déroulante **Modèle de terminal**, sélectionnez le modèle de terminal pour lequel vous souhaitez définir l'exception.
    d) Dans la liste déroulante **Minimale**, sélectionnez la version minimale du logiciel que vous souhaitez autoriser ou interdire.
    e) Dans la liste déroulante **Maximale**, sélectionnez la version maximale du logiciel que vous souhaitez autoriser ou interdire.
    f) Si vous avez interdit une version du logiciel, sélectionnez la version minimale du logiciel que vous souhaitez autoriser.
    g) Si vous avez interdit une version du logiciel, sélectionnez la version maximale du logiciel que vous souhaitez autoriser.
12. Cliquez sur **Enregistrer**.
13. Cliquez sur **Ajouter**.

À la fin : Si nécessaire, classez les profils.

Tâches connexes

Attribuer un profil ou une stratégie informatique à un groupe d'utilisateurs
Attribuer un profil ou une stratégie informatique à un compte d'utilisateur

Afficher les utilisateurs exécutant une version annulée du logiciel

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

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Conformité > Configuration logicielle minimale requise du terminal**.
3. Cliquez sur le nom du profil que vous souhaitez afficher.

4. Cliquez sur l'onglet **x utilisateurs exécutant une SR annulée** pour afficher la liste des utilisateurs qui exécutent une version annulée du logiciel.

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

Vous pouvez créer des profils de terminaux pour afficher des informations relatives à votre entreprise sur les terminaux. Pour les terminaux iOS, Android et Windows Phone, les informations sur l'entreprise s'affichent dans BlackBerry UEM Client sur le terminal. Sous Windows 10, le numéro de téléphone et l'adresse e-mail sont indiqués dans les informations d'assistance technique du terminal. Pour les terminaux BlackBerry 10 et 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 BlackBerry 10, Samsung KNOX et les terminaux 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 BlackBerry 10 et Samsung KNOX, le fond d'écran s'affiche dans l'espace Travail.

Emplacement des informations sur l'entreprise	Configuration des informations sur l'entreprise
Afficher un avis d'entreprise lors de l'activation des terminaux BlackBerry 10, iOS, macOS, Android et Windows 10	Créez un avis d'entreprise et attribuez-le à un profil d'activation.
Afficher un avis d'entreprise lors du redémarrage des terminaux Samsung KNOX	Créez un avis d'entreprise et attribuez-le dans l'onglet Android du profil de terminal. Pour modifier l'avis qui s'affiche au redémarrage du terminal, vous devez mettre à jour le profil du terminal.
Afficher une organisation avis sur Redémarrer pour BlackBerry 10 les périphériques	Créez un avis d'entreprise et attribuez-le dans l'onglet BlackBerry du profil d'un terminal. Vérifiez que la règle de stratégie informatique « Afficher l'avis d'entreprise après redémarrage du terminal » est sélectionnée. Pour modifier l'avis qui s'affiche au redémarrage du terminal, vous devez mettre à jour le profil du terminal. **Remarque :** la règle de stratégie informatique s'applique uniquement aux types d'activation Espace Travail uniquement et Travail et personnel - Réglementé des terminaux exécutant BlackBerry 10 OS version 10.3.1 ou ultérieure.

Emplacement des informations sur l'entreprise	Configuration des informations sur l'entreprise
Afficher des informations sur l'entreprise dans BlackBerry UEM Client sur les terminaux iOS, Android ou Windows Phone, ou dans les informations d'assistance sur les terminaux Windows 10.	Saisissez les informations que vous voulez afficher dans l'onglet approprié du profil de terminal.
Dans une image en fond d'écran sur les terminaux BlackBerry 10, Samsung KNOX ou iOS supervisés	Sélectionnez un fichier image dans l'onglet approprié du profil de terminal.

Créer des avis d'entreprise

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

Les terminaux BlackBerry 10 et Samsung KNOX peuvent également afficher les avis d'entreprise lorsqu'un utilisateur redémarre le terminal.

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

À la fin :

- Pour afficher l'avis d'organisation pendant l'activation, attribuez l'avis d'organisation à un profil d'activation.
- Pour afficher l'avis d'entreprise lors du redémarrage d'un terminal Samsung KNOX, associez l'avis d'entreprise à un profil de terminal.
- Pour afficher l'avis d'organisation lorsqu'un terminal BlackBerry 10 redémarre, attribuez l'avis d'organisation à un profil de terminal et sélectionnez l'option de stratégie informatique « Afficher l'avis d'organisation après le redémarrage du terminal ».

Créer un profil de terminal

Avant de commencer : Pour les terminaux BlackBerry 10 et Samsung KNOX, créez des avis d'entreprise.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Personnaliser > Terminal**.

3. Cliquez sur +.
4. Saisissez le nom et la description du profil. Chaque profil de terminal doit avoir un nom unique.
5. Effectuez l'une des tâches suivantes :

Tâche	Étapes
Attribuer un avis d'entreprise à afficher sur les terminaux BlackBerry 10 ou Samsung KNOX au redémarrage du terminal	a. Cliquez sur **BlackBerry** ou **Android**. b. Dans la liste déroulante **Attribuer un avis d'entreprise**, sélectionnez l'avis d'entreprise vous que vous souhaitez afficher sur les terminaux.
Pour iOS, Android ou Windows Phone, définissez les informations d'entreprise à afficher dans l'application 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.	a. Cliquez sur **iOS**, **Android** ou **Windows**. b. Saisissez le nom, l'adresse, le numéro de téléphone et l'adresse électronique de votre organisation.

6. Si nécessaire, effectuez les opérations suivantes :

Tâche	Étapes
Ajoutez une image de fond d'écran à l'espace Travail sur les terminaux BlackBerry 10 ou Samsung KNOX	a. Cliquez sur **BlackBerry** ou **Android**. b. Dans la section **Fond d'écran de l'espace Travail**, cliquez sur **Parcourir.** c. Sélectionnez l'image que vous souhaitez utiliser comme fond d'écran. d. Cliquez sur **Ouvrir**.
Ajouter un fond d'écran aux terminaux iOS supervisés	a. Cliquez sur **iOS**. b. Dans la zone **Fond d'écran du terminal**, sélectionnez si le fond d'écran s'affiche sur l'**écran d'accueil**, l'**écran de verrouillage** ou **les deux**. c. Cliquez sur **Parcourir** et sélectionnez l'image que vous souhaitez utiliser comme fond d'écran. d. Cliquez sur **Ouvrir**. e. Dans le champ **Définir le fond d'écran pour**, sélectionnez l'endroit où vous voulez que le fond d'écran s'affiche.

7. Cliquez sur **Ajouter**.

À la fin :

- Pour afficher l'avis d'entreprise lorsqu'un terminal BlackBerry 10 redémarre, sélectionnez l'option de stratégie informatique Afficher l'avis d'entreprise après le redémarrage du terminal.
- Si nécessaire, classez les profils.

Tâches connexes

Attribuer un profil ou une stratégie informatique à un groupe d'utilisateurs
Attribuer un profil ou une stratégie informatique à un compte d'utilisateur

Utilisation des services de localisation sur les terminaux

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

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

Configurer les paramètres du service de localisation

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

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

Créer un profil de service de localisation

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

Avant de commencer : Configurer les paramètres du service de localisation

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

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

7. Cliquez sur **Ajouter**.

À la fin : Si nécessaire, classez les profils.

Tâches connexes

Attribuer un profil ou une stratégie informatique à un groupe d'utilisateurs
Attribuer un profil ou une stratégie informatique à un compte d'utilisateur
Localiser un terminal

Désactivation des notifications en dehors des heures de travail

Vous pouvez utiliser des profils Ne pas déranger pour bloquer les notifications de terminal en dehors des heures de travail dans BlackBerry Work for Android et BlackBerry Work for iOS. Cette fonction nécessite BEMS 2,8 ou une version ultérieure.

Créer un profil Ne pas déranger

Avant de commencer :

- BEMS version 2.8 ou ultérieure est installé et configuré dans votre environnement. Pour obtenir des instructions, reportez-vous aux BEMS guides d'installation et de configuration.
- BlackBerry Work est ajouté au profil de connectivité BlackBerry Dynamics. Reportez-vous à la section Configurer les paramètres de connexion BlackBerry Work dans le contenu relatif à l'administration de BlackBerry Work.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Protection > Ne pas déranger**.
3. Cliquez sur +.
4. Saisissez le nom et la description du profil.

5. Saisissez un message à afficher sur les terminaux lorsque des notifications BlackBerry Work sont bloquées. Si vous laissez ce champ vide, un message par défaut est affiché.
6. Effectuez l'une des opérations suivantes :

Tâche	Étapes
Indiquez les jours et les heures de travail standard.	**a.** Cliquez sur l'option **Sélectionner les jours et les heures de travail standard**. **b.** Dans les listes déroulantes **De**, indiquez l'heure à laquelle commencent ces jours de travail. **c.** Dans les listes déroulantes **À**, indiquez l'heure à laquelle finissent ces jours de travail. **d.** Dans la liste **Jours de travail**, sélectionnez les jours de la semaine qui sont des jours ouvrés.
Spécifiez des heures de travail personnalisées pour certains jours.	**a.** Cliquez sur l'option **Sélectionner les jours et les heures de travail personnalisés**. **b.** Sélectionnez un jour de la semaine. **c.** Dans les listes déroulantes **De**, indiquez l'heure à laquelle commence le jour de travail. **d.** Dans les listes déroulantes **À**, indiquez l'heure à laquelle finit le jour de travail. **e.** Répétez les étapes 2 à 4 pour chaque jour de la semaine correspondant à un jour ouvré.

7. Cliquez sur **Ajouter**.

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.

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

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

- Contrôlez une fonctionnalité iOS existante qui n'est pas comprise dans les politiques et les profils BlackBerry UEM. Par exemple, avec BES10, l'assistant du PDG a pu accéder à la fois à son propre compte de messagerie et au compte du PDG sur un iPhone. Dans BlackBerry UEM, vous pouvez attribuer un seul profil de messagerie à un terminal, de sorte que l'assistant peut uniquement accéder à son propre compte de messagerie. Pour résoudre ce problème, vous pouvez attribuer un profil de messagerie pour permettre à l'iPhone de l'assistant d'accéder au compte de messagerie de l'assistant et un profil personnalisé pour permettre à l'iPhone de l'assistant d'accéder au compte de messagerie du PDG.
- Contrôlez une nouvelle fonctionnalité iOS, lancée après la dernière version du logiciel BlackBerry UEM. Par exemple, vous souhaitez contrôler une nouvelle fonctionnalité qui sera disponible sur les terminaux lors de leur mise à niveau à iOS 9, mais BlackBerry UEM ne dispose pas encore d'un profil pour cette nouvelle fonction, jusqu'à la prochaine version du logiciel BlackBerry UEM. Pour résoudre ce problème, vous pouvez

créer un profil de charge utile personnalisée qui contrôle cette fonction jusqu'à la prochaine version du logiciel BlackBerry UEM.

Création d'un profil de charge utile personnalisée

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

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

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/
DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
     <key>PayloadContent</key>
     <array>
          <dict>
               <key>CalDAVAccountDescription</key>
               <string>CalDAV Account Description</string>
               <key>CalDAVHostName</key>
               <string>caldav.server.example</string>
               <key>CalDAVPort</key>
               <integer>8443</integer>
               <key>CalDAVPrincipalURL</key>
               <string>Principal URL for the CalDAV account</string>
               <key>CalDAVUseSSL</key>
               </true>
               <key>CalDAVUsername</key>
               <string>Username</string>
               <key>PayloadDescription</key>
               <string>Configures CalDAV account.</string>
               <key>PayloadDisplayName</key>
               <string>CalDAV (CalDAV Account Description)</string>
               <key>PayloadIdentifier</key>
               <string>.caldav1</string>
               <key>PayloadOrganization</key>
               <string></string>
               <key>PayloadType</key>
               <string>com.apple.caldav.account</string>
               <key>PayloadUUID</key>
               <string>9ADCF5D6-397C-4E14-848D-FA04643610A3</string>
               <key>PayloadVersion</key>
               <integer>1</integer>
          </dict>
     </array>
     <key>PayloadDescription</key>
     <string>Profile description.</string>
     <key>PayloadDisplayName</key>
     <string>Profile Name</string>
     <key>PayloadOrganization</key>
     <string></string>
     <key>PayloadRemovalDisallowed</key>
```

```
      <false/>
      <key>PayloadType</key>
      <string>Configuration</string>
      <key>PayloadUUID</key>
      <string>7A5F8391-5A98-46EA-A3CF-C0D6EDC74632</string>
      <key>PayloadVersion</key>
      <integer>1</integer>
</dict>
</plist>
```

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

Tâches connexes

Attribuer un profil ou une stratégie informatique à un groupe d'utilisateurs
Attribuer un profil ou une stratégie informatique à un compte d'utilisateur

Configurer la disposition des applications sur les terminaux iOS supervisés

Vous pouvez contrôler l'ordre dans lequel les applications s'affichent sur le terminal iOS d'un utilisateur. Ce profil peut être utilisé uniquement avec des terminaux iOS 9.3 et version ultérieure, supervisés.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Personnaliser > Disposition de l'écran d'accueil**.
3. Cliquez sur +.
4. Dans la liste **Type d'application**, sélectionnez le type d'application que vous souhaitez glisser-déposer sur l'écran (par exemple, les applications intégrées).
5. Glissez-déposez les icônes de la liste d'applications vers l'écran d'accueil.
6. Cliquez sur **Ajouter**.

Configurer la fonction Protection des informations Windows pour les terminaux Windows 10

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

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

Lorsque vous configurez la fonction WIP pour les terminaux, vous spécifiez les applications que vous souhaitez protéger avec WIP. Les applications protégées sont en mesure de créer des fichiers professionnels et d'y accéder, tandis qu'il est possible de bloquer l'accès des applications non protégées aux fichiers professionnels. Vous

pouvez choisir le niveau de protection pour les applications protégées en fonction de la manière dont vous souhaitez que les utilisateurs se comportent lorsqu'ils partagent des données professionnelles. Lorsque la fonction WIP est activée, toutes les pratiques de partage des données sont surveillées. Pour plus d'informations sur la fonction WIP, consultez le site https://technet.microsoft.com/itpro/windows/keep-secure/protect-enterprise-data-using-wip.

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

Créer un profil de protection des données Windows

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

Concepts connexes

Paramètres des profils de protection des données Windows

Tâches connexes

Attribuer un profil ou une stratégie informatique à un groupe d'utilisateurs
Attribuer un profil ou une stratégie informatique à un compte d'utilisateur

Applications

Vous pouvez créer une bibliothèque des applications que vous souhaitez gérer et surveiller sur les terminaux BlackBerry 10, iOS, Android et Windows. Pour gérer les applications, vous pouvez les ajouter à la liste des applications et les attribuer à des comptes d'utilisateur, groupes d'utilisateurs ou groupes de terminaux.

Pour gérer des applications, procédez comme suit :

Étape	Action
1	Ajoutez les applications publiques et internes que vous souhaitez gérer à la liste des applications.
2	Créer des groupes d'applications pour gérer simultanément plusieurs applications.
3	Attribuez des applications ou des groupes d'applications aux comptes d'utilisateur, groupes d'utilisateurs ou groupes de terminaux pour permettre aux utilisateurs de les installer.

Ajout d'applications à la liste des applications

La liste des applications contient les applications que vous pouvez attribuer aux utilisateurs, groupes d'utilisateurs et groupes de terminaux. Les applications accompagnées d'une icône de verrouillage sont des applications BlackBerry Dynamics.

Remarque : Si votre entreprise utilise des applications Microsoft Intune for MAM telles que Office 365, au lieu d'ajouter les applications à la liste d'applications, créez un profil de protection d'application Microsoft Intune pour attribuer des applications protégées par Intuneaux utilisateurs.

Ajout d'applications publiques à la liste des applications

Une application publique est à une application disponible auprès de la boutique BlackBerry World, de la boutique en ligne App Store, de la boutique Google Play ou de Windows Store.

Ajouter une application BlackBerry à la liste des applications

1. Sur la barre de menus, cliquez sur **Applications**.
2. Cliquez sur .
3. Cliquez sur **BlackBerry World**.
4. Dans le champ de recherche, recherchez l'application que vous souhaitez ajouter. Vous pouvez rechercher une application par nom, fournisseur ou URL BlackBerry World.
5. Dans la liste déroulante, sélectionnez le pays du magasin dans lequel vous souhaitez effectuer la recherche.
6. Cliquez sur **Rechercher**.
7. Dans les résultats de la recherche, cliquez sur **Ajouter** pour ajouter une application.
8. Pour filtrer par catégorie les applications BlackBerry dans la liste d'applications, vous pouvez sélectionner une catégorie pour l'application. Dans la liste déroulante **Catégorie**, effectuez l'une des opérations suivantes :

Option	
Sélectionner une catégorie pour l'application	**a.** Dans la liste déroulante, sélectionnez une catégorie.
Créer une catégorie pour l'application	**a.** Saisissez un nom pour la catégorie. La nouvelle catégorie apparait dans la liste déroulante avec la mention « Nouvelle catégorie ». **b.** Appuyez sur la touche **Entrée**. **c.** Appuyez sur la touche **Entrée**.

9. Dans l'écran d'informations sur l'application, cliquez sur **Ajouter**.

Tâches connexes

Attribuer une application à un groupe d'utilisateurs
Attribuer une application à un compte d'utilisateur

Ajouter une application iOS à la liste des applications

1. Sur la barre de menus, cliquez sur **Applications**.
2. Cliquez sur .
3. Cliquez sur **Boutique d'applications**.
4. Dans le champ de recherche, recherchez l'application que vous souhaitez ajouter. Vous pouvez rechercher une application par nom, fournisseur ou URL App Store.
5. Dans la liste déroulante, sélectionnez le pays du magasin dans lequel vous souhaitez effectuer la recherche.
6. Cliquez sur **Rechercher**.
7. Dans les résultats de la recherche, cliquez sur **Ajouter** pour ajouter une application.
8. Pour filtrer, par catégorie, les applications figurant dans la liste des applications et les organiser en catégories dans la liste Applications professionnelles sur les terminaux des utilisateurs, vous pouvez sélectionner une catégorie pour l'application. Dans la liste déroulante **Catégorie**, effectuez l'une des opérations suivantes :

Option	
Sélectionner une catégorie pour l'application	**a.** Dans la liste déroulante, sélectionnez une catégorie.
Créer une catégorie pour l'application	**a.** Saisissez un nom pour la catégorie. La « nouvelle catégorie » apparait dans la liste déroulante, accompagnée de l'étiquette « nouvelle catégorie ». **b.** Appuyez sur la touche **Entrée**. **c.** Appuyez sur la touche **Entrée**.

9. Dans la liste déroulante **Évaluation et commentaires sur l'application**, effectuez l'une des opérations suivantes. Lorsqu'il existe plusieurs versions de l'application, le paramètre spécifié s'applique à toutes les versions.
   - Si vous souhaitez que les utilisateurs puissent évaluer l'application, déposer des commentaires et consulter les avis d'autres utilisateurs de votre environnement, sélectionnez **Mode public**.

- Si vous souhaitez uniquement autoriser les utilisateurs à évaluer et déposer des commentaires sur l'application, sélectionnez **Mode privé**. Les utilisateurs n'auront pas accès aux avis des autres utilisateurs. Ces avis seront disponibles dans la console de gestion BlackBerry UEM.
- Si vous ne souhaitez pas que les utilisateurs puissent évaluer les applications, déposer des commentaires ou consulter les avis d'autres utilisateurs, sélectionnez **Désactivé**.

10. Dans la liste déroulante **Facteur de forme du terminal pris en charge**, sélectionnez les facteurs de forme sur lesquels l'application peut être installée. Par exemple, vous pouvez empêcher l'accès à l'application dans les applications professionnelles pour iPad.
11. Si vous souhaitez supprimer l'application du terminal lorsque celui-ci est supprimé de BlackBerry UEM, sélectionnez **Supprimer l'application du terminal lorsque celui-ci est supprimé de BlackBerry UEM**. Cette option s'applique uniquement aux applications dotées d'une disposition marquée comme requise et l'installation par défaut des applications requises est définie sur une seule demande.
12. Si vous souhaitez empêcher la sauvegarde des applications des terminaux iOS sur le service en ligne iCloud, sélectionnez **Désactiver la sauvegarde iCloud pour l'application**. Cette option s'applique uniquement aux applications dotées d'une disposition marquée comme requise. Vous pouvez définir la disposition de l'application lorsque vous attribuez l'application à un utilisateur ou à un groupe.
13. Dans la liste déroulante **Installation par défaut des applications requises**, effectuez l'une des opérations suivantes :

    - Si vous souhaitez que les utilisateurs reçoivent une demande d'installation de l'application sur leurs terminaux iOS, sélectionnez **Demander une fois**. Si les utilisateurs rejettent cette demande, ils peuvent installer l'application ultérieurement via l'écran Applications professionnelles de l'application BlackBerry UEM Client ou l'icône Applications professionnelles du terminal.
    - Si vous ne souhaitez pas que les utilisateurs reçoivent d'invite, sélectionnez **Aucune invite**.

    La méthode d'installation par défaut s'applique uniquement aux applications dotées d'une disposition marquée comme requise. Vous pouvez définir la disposition de l'application lorsque vous attribuez l'application à un utilisateur ou à un groupe.
14. Dans la liste déroulante **Convertissez une application personnelle installée en application professionnelle**, sélectionnez l'une des options suivantes :

    - Pour convertir l'application en application professionnelle, si elle est déjà installée sur des terminaux iOS 9 ou versions ultérieures, sélectionnez **Convertir**. Une fois que vous avez affecté l'application à un utilisateur, celle-ci est convertie en application professionnelle et peut être gérée par BlackBerry UEM.
    - Si vous ne souhaitez pas convertir l'application en application professionnelle, si elle est déjà installée sur des terminaux iOS 9 ou version ultérieure, sélectionnez **Ne pas convertir**. Une fois que vous avez affecté l'application à un utilisateur, celle-ci ne peut pas être gérée par BlackBerry UEM.
15. S'il est possible de préconfigurer les paramètres de l'application (informations de connexion, par exemple), et si vous souhaitez le faire, obtenez les détails de configuration auprès de l'éditeur et effectuez les opérations suivantes :

    a) Dans le tableau **Configuration d'application**, effectuez l'une des opérations suivantes :

Tâche	Étapes
Créer une configuration d'application à partir d'un modèle XML	1. Cliquez sur + > **Créer à partir d'un modèle**. 2. Cliquez sur **Parcourir** et sélectionnez le modèle que vous souhaitez ajouter. 3. Cliquez sur **Télécharger**. 4. Pour chaque paramètre, entrez la valeur que vous souhaitez définir. Pour plus d'informations sur les modèles .xml de configuration d'application, rendez-vous surhttp://www.appconfig.org/ios/.
Copier une autre configuration d'application	1. Cliquez sur + > **Copier depuis une configuration d'application**. 2. Dans la liste déroulante **Copier depuis**, sélectionnez la configuration d'application que vous souhaitez copier. 3. Pour chaque paramètre, modifiez le nom ou la valeur de la clé.
Créer une configuration d'application manuellement	1. Cliquez sur + > **Configurer manuellement**. 2. Pour chaque paramètre que vous souhaitez ajouter, cliquez sur +, puis sélectionnez un type de valeur pour le paramètre. 3. Pour chaque paramètre, entrez le nom et la valeur de la clé que vous souhaitez définir.

b) Saisissez un nom dans le champ **Nom de la configuration de l'application**.
c) Cliquez sur **Enregistrer**.
d) Si nécessaire, utilisez les flèches pour déplacer les profils vers le haut ou vers le bas du classement. Lorsqu'une application est attribuée plusieurs fois avec différentes configurations d'application, la configuration au classement le plus élevé s'applique.

16. Cliquez sur **Ajouter**.

Tâches connexes

Attribuer une application à un groupe d'utilisateurs
Attribuer une application à un compte d'utilisateur

Ajouter une application Android à la liste des applications si BlackBerry UEM n'est pas configuré pour les profils professionnels Android

Ajoutez uniquement les applications à la liste des applications disponibles. Les films, la musique et les journaux ne peuvent pas être remis aux terminaux. Si vous attribuez un support à un utilisateur et définissez la disposition de ce support sur requis, le terminal est soumis à l'action d'application définie dans le profil de conformité qui lui est attribué.

Si BlackBerry UEM est configuré pour prendre en charge les profils professionnels Android, reportez-vous à la section Ajouter une application Android à la liste des applications si BlackBerry UEM est configuré pour les profils professionnels Android.

1. Sur la barre de menus, cliquez sur **Applications**.
2. Cliquez sur .
3. Cliquez sur **Google Play**.
4. Cliquez sur **Ouvrir Google Play** et recherchez l'application que vous souhaitez ajouter. Vous pouvez ensuite copier et coller les informations depuis Google Play dans les étapes suivantes et télécharger des icônes et captures d'écran.
5. Dans le champ **Nom de l'application**, saisissez le nom de l'application.
6. Dans le champ **Description de l'application**, saisissez la description de l'application.
7. Pour filtrer, par catégorie, les applications figurant dans la liste des applications et les organiser en catégories dans la liste Applications professionnelles sur les terminaux des utilisateurs, vous pouvez sélectionner une catégorie pour l'application. Dans la liste déroulante **Catégorie**, effectuez l'une des opérations suivantes :

Option	
Sélectionner une catégorie pour l'application	**a.** Dans la liste déroulante, sélectionnez une catégorie.
Créer une catégorie pour l'application	**a.** Saisissez un nom pour la catégorie. La « nouvelle catégorie » apparait dans la liste déroulante, accompagnée de l'étiquette « nouvelle catégorie ». **b.** Appuyez sur la touche **Entrée**. **c.** Appuyez sur la touche **Entrée**.

8. Dans la liste déroulante **Évaluation et commentaires sur l'application**, effectuez l'une des opérations suivantes. Lorsqu'il existe plusieurs versions de l'application, le paramètre spécifié s'applique à toutes les versions.
   - Si vous souhaitez que les utilisateurs puissent évaluer l'application, déposer des commentaires et consulter les avis d'autres utilisateurs de votre environnement, sélectionnez **Mode public**.
   - Si vous souhaitez uniquement autoriser les utilisateurs à évaluer et déposer des commentaires sur les applications, sélectionnez **Mode privé**. Les utilisateurs n'auront pas accès aux avis des autres utilisateurs. Ces avis seront disponibles dans la console de gestion BlackBerry UEM.
   - Si vous ne souhaitez pas que les utilisateurs puissent évaluer les applications, déposer des commentaires ou consulter les avis d'autres utilisateurs, sélectionnez **Désactivé**.
9. Dans le champ **Éditeur**, indiquez le nom du fournisseur de l'application.
10. Dans le champ **Icône de l'application**, cliquez sur **Parcourir**. Localisez une icône pour l'application et sélectionnez-la. Les formats .png, .jpg, .jpeg ou .gif sont pris en charge N'utilisez pas Google Chrome pour télécharger l'icône car l'image .webp téléchargée n'est pas compatible.
11. Dans le champ **Adresse Web de l'application sur Google Play**, saisissez l'adresse Web de l'application dans Google Play.
12. Pour ajouter les captures d'écran de l'application, cliquez sur **Ajouter** et accédez aux captures d'écran. Les formats .jpg, .jpeg, .png ou .gif sont pris en charge
13. Dans la liste déroulante **Envoyer à**, effectuez l'une des opérations suivantes :
    - Si vous souhaitez que l'application soit envoyée à tous les terminaux Android, sélectionnez **Tous les appareils Android** .

- Si vous souhaitez que l'application soit uniquement envoyée aux terminaux Android utilisant Samsung KNOX Workspace, sélectionnez **Terminaux KNOX Workspace uniquement**.

14. Cliquez sur **Ajouter**.

Tâches connexes

Attribuer une application à un groupe d'utilisateurs
Attribuer une application à un compte d'utilisateur

Ajouter une application Android à la liste des applications si BlackBerry UEM est configuré pour les profils professionnels Android

Si vous avez configuré la prise en charge des activations de profil professionnel Android, la connexion à Google que vous avez configurée permet à BlackBerry UEM d'obtenir des informations sur l'application auprès de Google Play. Pour plus d'informations sur la configuration de BlackBerry UEM afin de prendre en charge les profils professionnels Android, reportez-vous au contenu relatif à la configuration.

Si BlackBerry UEM n'est pas configuré pour prendre en charge les profils professionnels Android, reportez-vous à la section Ajouter une application Android à la liste des applications si BlackBerry UEM n'est pas configuré pour les profils professionnels Android.

Pour utiliser Google Play afin de gérer les applications dans Samsung KNOX Workspace,Samsung KNOX 2.7.1 ou version ultérieure doit être installé sur les terminaux et vous devez autoriser la gestion d'application Google Play pour les terminaux Samsung KNOX Workspace dans le profil d'activation.

Remarque : Dans une prochaine version de BlackBerry UEM, les paramètres applicables à BlackBerry Hub + et Divide Productivity seront supprimés du profil de messagerie et seront uniquement disponibles au niveau de la configuration de l'application (paramètres de l'application). Dans la version actuelle, si vous configurez les paramètres de l'application à la fois dans le profil de messagerie et au niveau de la configuration de l'application, les paramètres définis au niveau de la configuration de l'application sont prioritaires.

1. Sur la barre de menus, cliquez sur **Applications**.
2. Cliquez sur .
3. Cliquez sur **Google Play**.
4. Recherchez l'application que vous souhaitez ajouter.
5. Cliquez sur **Approuver**.
6. Pour accepter les autorisations d'application au nom des utilisateurs, cliquez sur **Approuver**. Vous devez accepter les autorisations des applications pour permettre l'installation automatique des applications requises sur les terminaux Android dotés d'un profil professionnel ou dans KNOX Workspace. Si vous n'acceptez pas les autorisations des applications au nom des utilisateurs, l'application ne peut pas être gérée dans BlackBerry UEM.
7. Choisissez la manière dont vous souhaitez gérer les nouvelles demandes d'autorisation d'application lorsqu'une mise à jour d'application est disponible.
   - Pour accepter automatiquement les nouvelles autorisations ajoutées par le fournisseur de l'application, sélectionnez **Keep approved when app requests new permissions**.
   - Pour accepter à nouveau manuellement les nouvelles autorisations d'application ajoutées par le fournisseur de l'application pour que l'application puisse être envoyée aux nouveaux terminaux, sélectionnez **Revoke app approval when this app requests new permissions**. Pour plus d'informations sur la mise à jour des autorisations d'application, reportez-vous à Mettre à jour les autorisations des applications du profil professionnel Android.
8. Cliquez sur **Enregistrer**.

9. Dans le champ **Description de l'application**, saisissez la description de l'application.
10. Pour ajouter les captures d'écran de l'application, cliquez sur **Ajouter** et accédez aux captures d'écran. Les formats .jpg, .jpeg, .png ou .gif sont pris en charge
11. Dans la liste déroulante **Envoyer à**, effectuez l'une des opérations suivantes :
    - Si vous souhaitez que l'application soit envoyée à tous les terminaux Android, sélectionnez **Tous les appareils Android** .
    - Si vous souhaitez que l'application soit uniquement envoyée aux terminaux Android utilisant Samsung KNOX Workspace, sélectionnez **Terminaux Samsung KNOX Workspace**.
    - Si vous souhaitez que l'application soit envoyée uniquement aux terminaux Android dotés d'un profil professionnel, sélectionnez **Terminaux Android avec profil professionnel**.
12. Pour les applications prenant en charge les paramètres de configuration, un tableau **Configuration de l'application** s'affiche. Si vous souhaitez créer une configuration d'application, procédez comme suit :
    a) Cliquez sur + pour ajouter une configuration d'application.
    b) Saisissez le nom de la configuration d'application et spécifiez les paramètres de configuration à utiliser.
    c) Cliquez sur **Enregistrer**.
    d) Si nécessaire, utilisez les flèches pour déplacer les profils vers le haut ou vers le bas du classement. Lorsqu'une application est attribuée plusieurs fois avec différentes configurations d'application, la configuration au classement le plus élevé s'applique.
13. Pour filtrer, par catégorie, les applications figurant dans la liste des applications et les organiser en catégories dans la liste Applications professionnelles sur les terminaux des utilisateurs, vous pouvez sélectionner une catégorie pour l'application. Dans la liste déroulante **Catégorie**, effectuez l'une des opérations suivantes :

Option	
Sélectionner une catégorie pour l'application	**a.** Dans la liste déroulante, sélectionnez une catégorie.
Créer une catégorie pour l'application	**a.** Saisissez un nom pour la catégorie. La nouvelle catégorie apparait dans la liste déroulante, accompagnée de l'étiquette « nouvelle catégorie ». **b.** Appuyez sur la touche **Entrée**. **c.** Appuyez sur la touche **Entrée**.

14. Dans la liste déroulante **Évaluation et commentaires sur l'application**, effectuez l'une des opérations suivantes. Lorsqu'il existe plusieurs versions de l'application, le paramètre spécifié s'applique à toutes les versions.
    - Si vous souhaitez que les utilisateurs puissent évaluer l'application, déposer des commentaires et consulter les avis d'autres utilisateurs de votre environnement, sélectionnez **Mode public**.
    - Si vous souhaitez uniquement autoriser les utilisateurs à évaluer et déposer des commentaires sur l'application, sélectionnez **Mode privé**. Les utilisateurs n'auront pas accès aux avis des autres utilisateurs. Ces avis seront disponibles dans la console de gestion BlackBerry UEM.
    - Si vous ne souhaitez pas que les utilisateurs puissent évaluer les applications, déposer des commentaires ou consulter les avis d'autres utilisateurs, sélectionnez **Désactivé**.
15. Cliquez sur **Ajouter**.

Tâches connexes

Attribuer une application à un groupe d'utilisateurs
Attribuer une application à un compte d'utilisateur

Ajouter une application Windows Phone à la liste des applications

1. Sur la barre de menus, cliquez sur **Applications**.
2. Cliquez sur .
3. Cliquez sur **Windows Store** > **8**.
4. Cliquez sur **Ouvrir Windows Store** et recherchez l'application que vous souhaitez ajouter. Vous pouvez ensuite copier et coller les informations depuis Windows Store dans les étapes suivantes et télécharger des icônes et captures d'écran.
5. Dans le champ **Nom de l'application**, saisissez le nom de l'application.
6. Dans le champ **Description de l'application**, saisissez la description de l'application.
7. Dans la liste déroulante **Évaluation et commentaires sur l'application**, effectuez l'une des opérations suivantes. Lorsqu'il existe plusieurs versions de l'application, le paramètre spécifié s'applique à toutes les versions.
   - Si vous souhaitez que les utilisateurs puissent évaluer l'application, déposer des commentaires et consulter les avis d'autres utilisateurs de votre environnement, sélectionnez **Mode public**.
   - Si vous souhaitez uniquement autoriser les utilisateurs à évaluer et déposer des commentaires sur l'application, sélectionnez **Mode privé**. Les utilisateurs n'auront pas accès aux avis des autres utilisateurs. Ces avis seront disponibles dans la console de gestion BlackBerry UEM.
   - Si vous ne souhaitez pas que les utilisateurs puissent évaluer les applications, déposer des commentaires ou consulter les avis d'autres utilisateurs, sélectionnez **Désactivé**.
8. Dans le champ **Éditeur**, indiquez le nom du fournisseur de l'application.
9. Dans le champ **Icône de l'application**, cliquez sur **Parcourir**. Localisez une icône pour l'application et sélectionnez-la. Les formats .png, .jpg, .jpeg ou .gif sont pris en charge
10. Dans le champ **Adresse Web de l'application sur Windows Store**, saisissez l'adresse Web de l'application dans Windows Store. L'adresse Web doit commencer par « https ».
11. Pour ajouter les captures d'écran de l'application, cliquez sur **Ajouter** et accédez aux captures d'écran. Les formats .jpg, .jpeg, .png ou .gif sont pris en charge
12. Cliquez sur **Ajouter**.

Ajouter une application Windows 10 à la liste des applications

Pour ajouter des applications Windows 10 à la liste d'applications, vous devez gérer votre catalogue d'applications dans Windows Store pour Entreprises, puis synchroniser les applications avec BlackBerry UEM. Lorsque de nouvelles applications sont ajoutées à votre catalogue d'applications, vous pouvez synchroniser les applications avec BlackBerry UEM immédiatement ou attendre que BlackBerry UEM se synchronise automatiquement. BlackBerry UEM synchronise le catalogue d'applications toutes les 24 heures.

Vous pouvez autoriser les utilisateurs à installer des applications en ligne ou hors ligne à partir du catalogue d'applications Windows Store pour Entreprises. Les applications hors ligne sont téléchargées par BlackBerry UEM lorsque vous les synchronisez avec le catalogue d'applications. Il est recommandé d'utiliser les applications hors ligne étant donné qu'il est possible de les gérer depuis BlackBerry UEM et que les utilisateurs peuvent les installer sans se connecter à Windows Store pour Entreprises. Une fois les applications installées, les terminaux reçoivent des mises à jour des applications de Windows Store.

Les applications en ligne sont téléchargées directement à partir de Windows Store pour Entreprises. Pour pouvoir envoyer les applications en ligne requises aux terminaux, demandez à vos utilisateurs d'ajouter leur compte professionnel aux **Comptes utilisés par d'autres applications** dans Windows 10.

Avant de commencer :

- Spécifier l'emplacement réseau partagé où stocker des applications internes afin de stocker des applications hors ligne.
- Configurer BlackBerry UEM pour une synchronisation avec Windows Store pour Entreprises Pour obtenir des instructions, consultez le contenu relatif à la configuration.

1. Sur la barre de menus, cliquez sur **Applications**.
2. Cliquez sur .
3. Cliquez sur **Windows Store** > **10**.
4. Cliquez sur **Synchroniser les applications**.

Autorisation des utilisateurs à installer des applications Windows 10 en ligne

Pour que vous puissiez autoriser des utilisateurs à installer des applications Windows 10 en ligne, ces utilisateurs doivent déjà exister dans votre annuaire Microsoft Azure et leur adresse électronique dans BlackBerry UEM doit correspondre à leur adresse électronique dans Microsoft Azure AD. Vous pouvez synchroniser votre annuaire avec Microsoft Azure à l'aide de Microsoft Azure AD Connect. Pour obtenir des instructions, consultez le contenu relatif à la configuration

Remarque : Pour pouvoir envoyer les applications en ligne requises aux terminaux, demandez à vos utilisateurs d'ajouter leur compte professionnel aux **Comptes utilisés par d'autres applications** dans Windows 10.

Ajout d'une catégorie d'application pour une application Windows 10

Après avoir défini une catégorie pour une application, vous pouvez filtrer par catégorie des applications dans la liste d'applications et organiser en catégories les applications figurant sur la liste des applications professionnelles sur les terminaux d'utilisateurs. Lorsqu'une application Windows 10 est synchronisée avec BlackBerry UEM, vous pouvez lui attribuer une catégorie d'application.

Avant de commencer : Ajouter une application Windows 10 à la liste des applications.

1. Sur la barre de menus, cliquez sur **Applications**.
2. Cliquez sur l'application à laquelle vous souhaitez attribuer une catégorie d'application.
3. Dans la liste déroulante **Catégorie**, effectuez l'une des opérations suivantes :

Étape	Description
Sélectionner une catégorie pour l'application	a. Dans la liste déroulante, sélectionnez une catégorie.
Créer une catégorie pour l'application	a. Saisissez un nom pour la catégorie. Le message « Nouvelle catégorie » apparait dans la liste déroulante avec l'étiquette de la nouvelle catégorie à côté. b. Appuyez sur la touche **Entrée**. c. Appuyez sur la touche **Entrée**.

4. Cliquez sur **Enregistrer**.

Ajouter des applications BlackBerry Dynamics publiques à la liste des applications

Pour ajouter des applications BlackBerry Dynamics publiques à la liste des applications de BlackBerry UEM, votre entreprise doit être autorisée à utiliser les applications dans BlackBerry Marketplace for Enterprise Software.

BlackBerry Marketplace for Enterprise Software contient un catalogue d'applications BlackBerry Dynamics. Une fois votre entreprise autorisée à utiliser l'application, vous pouvez mettre à jour la liste des applications pour la synchroniser immédiatement avec BlackBerry UEM ou attendre que BlackBerry UEM le fasse automatiquement. BlackBerry UEM synchronise les applications BlackBerry Dynamics toutes les 24 heures.

Remarque : Les utilisateurs doivent activer les applications Dynamics sur le même environnement BlackBerry UEM à partir duquel les applications sont attribuées. L'activation d'applications BlackBerry Dynamics avec des clés d'accès à partir d'un environnement externe BlackBerry Dynamics n'est pas prise en charge.

1. Connectez-vous à votre compte sur https://apps.good.com/pce/#/apps.
2. Recherchez l'application dans BlackBerry Marketplace for Enterprise Software et demandez une version d'essai. L'application sera mise à la disposition de votre entreprise et pourra être attribuée aux utilisateurs dès qu'elle aura été synchronisée avec BlackBerry UEM.
3. Pour acheter l'application, suivez les instructions du développeur.

À la fin :

- Procédez à la mise à jour de la liste des applications pour synchroniser les applications avec BlackBerry UEM.

Afficher les autorisations d'application BlackBerry Dynamics publiques

1. Connectez-vous à https://account.good.com/pce/#/a/organization//servers.
2. Développez **Autorisations**.

Ajout d'applications internes à la liste des applications

Les applications internes comprennent les applications propriétaires développées par votre organisation ou des applications mises exclusivement à la disposition de votre organisation. Les applications internes ne sont pas ajoutées à partir des boutiques d'applications publiques.

Les applications BlackBerry doivent correspondre à des fichiers .bar, les applications iOS à des fichiers .ipa, les applications Android à des fichiers .apk et les applications Windows Phone à des fichiers .xap ou .appx. Les applications internes doivent également être signées et non modifiées.

Les utilisateurs peuvent accéder aux applications internes sur leurs terminaux comme suit :

- Sur les terminaux BlackBerry 10, dans l'onglet Applications d'entreprise de BlackBerry World for Work
- Sur les terminaux iOS, Android et Windows Phone, dans la liste Applications professionnelles attribuées de l'application BlackBerry UEM Client

Étapes à suivre pour ajouter des applications internes à la liste des applications

Pour ajouter des applications internes, procédez comme suit :

Étape	Action
1	Spécifier l'emplacement réseau partagé où stocker des applications internes.
2	Si vous ajoutez des applications Windows Phone, téléchargez un AET.
3	Si l'application n'est pas une application BlackBerry Dynamics, ajoutez une application interne à la liste des applications.

Étape	Action
4	Si l'application est une application BlackBerry Dynamics, ajoutez une attribution d'application BlackBerry Dynamics interne, puis téléchargez les fichiers source de l'application BlackBerry Dynamics.
5	Si vous ajoutez une application interne que vous souhaitez rendre disponible sur les terminaux Android dotés d'un profil professionnel, procédez comme suit pour héberger l'application dans Google Play ou dans BlackBerry UEM.

Spécifier l'emplacement réseau partagé où stocker des applications internes

Avant d'ajouter des applications internes à la liste des applications, vous devez spécifier un emplacement réseau partagé où stocker les fichiers source des applications. Pour veiller à ce que les applications internes restent disponibles, cet emplacement réseau doit disposer d'une solution haute disponibilité et régulièrement sauvegardé. De même, veillez à ne pas créer de dossier réseau partagé dans le dossier d'installation BlackBerry UEM car celui-ci serait supprimé en cas de mise à niveau de BlackBerry UEM.

Avant de commencer :

- Créez un dossier réseau partagé pour stocker les fichiers source des applications internes sur le réseau hébergeant BlackBerry UEM.
- Vérifiez que le compte de service de l'ordinateur qui héberge BlackBerry UEM dispose d'un accès en lecture et en écriture sur le dossier réseau partagé.

1. Sur la barre de menus, cliquez sur **Paramètres**.
2. Dans le volet de gauche, développez **Gestion des applications**.
3. Cliquez sur **Stockage d'applications internes**.
4. Dans le champ **Emplacement réseau**, saisissez le chemin du dossier réseau partagé au format suivant :

   \\<*computer_name*>\<*shared_network_folder*>

   Le chemin du réseau partagé doit être au format UNC (par exemple, \\NomOrdinateur\Applications \ApplicationInternes).
5. Cliquez sur **Enregistrer**.

Télécharger un jeton d'inscription d'application pour les terminaux Windows Phone

Un jeton d'inscription d'application (AET - Application Enrollment Token) doit être téléchargé pour permettre aux utilisateurs d'installer des applications internes sur les terminaux Windows Phone. Les applications que vous souhaitez que les utilisateurs installent doivent partager un certificat avec l'AET que vous avez téléchargé. Pour plus d'informations sur la génération d'un jeton d'inscription d'application, rendez-vous sur msdn.microsoft.com pour consulter le document *Génération d'un jeton d'inscription d'application pour Windows Phone*. Il vous faut également un jeton d'inscription d'application pour surveiller les applications Windows internes ou publiques dans les profils de conformité.

1. Sur la barre de menus, cliquez sur **Paramètres**.
2. Dans le volet de gauche, développez **Gestion des applications**.
3. Cliquez sur **Applications Windows Phone**.
4. Cliquez sur **Parcourir** et accédez au fichier d'inscription d'application que vous souhaitez télécharger.
5. Cliquez sur **Enregistrer**.

Ajouter une application interne à la liste des applications

Avant de commencer :

- Spécifier l'emplacement réseau partagé où stocker des applications internes.
- Si vous ajoutez des applications Windows Phone, téléchargez un AET.

1. Sur la barre de menus, cliquez sur **Applications**.
2. Cliquez sur .
3. Cliquez sur **Applications internes**.
4. Cliquez sur **Parcourir**. Accédez à l'application que vous souhaitez ajouter ou mettre à jour.
5. Cliquez sur **Ouvrir**.
6. Cliquez sur **Ajouter**.
7. Vous pouvez également ajouter le nom du fournisseur et la description de l'application.
8. Pour ajouter des captures d'écran de l'application, cliquez sur **Ajouter**. Accédez aux captures d'écran. Les formats .jpg, .jpeg, .png ou .gif sont pris en charge
9. Pour filtrer, par catégorie, les applications figurant dans la liste des applications et les organiser en catégories dans la liste Applications professionnelles sur les terminaux des utilisateurs, vous pouvez sélectionner une catégorie pour l'application. Dans la liste déroulante **Catégorie**, effectuez l'une des opérations suivantes :

Option	
Sélectionner une catégorie pour l'application	**a.** Dans la liste déroulante, sélectionnez une catégorie.
Créer une catégorie pour l'application	**a.** Saisissez un nom pour la catégorie. La « nouvelle catégorie » apparait dans la liste déroulante, accompagnée de l'étiquette « nouvelle catégorie ». **b.** Appuyez sur la touche **Entrée**. **c.** Appuyez sur la touche **Entrée**.

10. Dans la liste déroulante **Évaluation et commentaires sur l'application**, effectuez l'une des opérations suivantes : Lorsqu'il existe plusieurs versions de l'application, le paramètre spécifié s'applique à toutes les versions.
    - Si vous souhaitez que les utilisateurs puissent évaluer l'application, déposer des commentaires et consulter les avis d'autres utilisateurs de votre environnement, sélectionnez **Mode public**.
    - Si vous souhaitez uniquement autoriser les utilisateurs à évaluer et déposer des commentaires sur l'application, sélectionnez **Mode privé**. Les utilisateurs n'auront pas accès aux avis des autres utilisateurs. Ces avis seront disponibles dans la console de gestion BlackBerry UEM.
    - Si vous ne souhaitez pas que les utilisateurs puissent évaluer les applications, déposer des commentaires ou consulter les avis d'autres utilisateurs, sélectionnez **Désactivé**.
11. Si vous ajoutez une application iOS, procédez comme suit :
    a) Dans la liste déroulante **Facteur de forme du terminal pris en charge**, sélectionnez les facteurs de forme sur lesquels l'application peut être installée. Par exemple, vous pouvez empêcher l'accès à l'application dans les applications professionnelles pour iPad.
    b) Si vous souhaitez supprimer l'application du terminal lorsque celui-ci est supprimé de BlackBerry UEM, sélectionnez **Supprimer l'application du terminal lorsque celui-ci est supprimé de BlackBerry UEM**. Cette option s'applique uniquement aux applications dotées d'une disposition marquée comme requise et l'installation par défaut des applications requises est définie sur une seule demande.

c) Si vous souhaitez empêcher la sauvegarde des applications des terminaux iOS sur le service en ligne iCloud, sélectionnez **Désactiver la sauvegarde iCloud pour l'application**. Cette option s'applique uniquement aux applications dotées d'une disposition marquée comme requise. Vous pouvez définir la disposition de l'application lorsque vous attribuez l'application à un utilisateur ou à un groupe.
d) Dans la liste déroulante **Méthode d'installation par défaut des applications requises**, si vous souhaitez que les utilisateurs reçoivent une demande d'installation de l'application sur leurs terminaux iOS, sélectionnez **Demander une fois**. Si les utilisateurs ignorent l'invite, ils peuvent installer l'application ultérieurement à partir de la liste Applications professionnelles de l'application BlackBerry UEM Client ou à l'aide de l'icône Applications professionnelles du terminal.

12. Si vous ajoutez une application Android, dans la liste déroulante **Envoyer à**, effectuez l'une des opérations suivantes :
    - Si vous souhaitez que l'application soit envoyée à tous les terminaux Android, sélectionnez **Tous les appareils Android** .
    - Si vous souhaitez que l'application soit uniquement envoyée aux terminaux Android utilisant Samsung KNOX Workspace, sélectionnez **Terminaux Samsung KNOX Workspace**.
    - Si vous souhaitez que l'application soit envoyée uniquement aux terminaux Android dotés d'un profil professionnel, sélectionnez **Terminaux Android avec profil professionnel**.
13. Pour permettre l'installation de l'application sur des terminaux Android dotés d'un profil professionnel, sélectionnez **Activer l'application pour les profils professionnels**.
14. Pour les applications prenant en charge les paramètres de configuration, un tableau **Configuration de l'application** s'affiche. Cliquez sur + pour ajouter une configuration d'application. Pour plus d'informations, reportez-vous à Ajout ou modification d'une configuration d'application.
15. Cliquez sur **Ajouter**. Si vous prévoyez d'héberger l'application dans BlackBerry UEM à l'aide d'un fichier .json, copiez et collez l'URL affichée.

À la fin : Si vous avez sélectionné l'option **Activer l'application pour les profils professionnels Android**, effectuez l'une des opérations suivantes :

- Héberger une application interne pour les terminaux dotés d'un profil professionnel Android dans Google Play à l'aide du fichier .apk
- Héberger une application interne pour les terminaux Android dotés d'un profil professionnel dans BlackBerry UEM à l'aide d'un fichier .json

Ajouter une autorisation d'application BlackBerry Dynamics interne

Pour ajouter une application BlackBerry Dynamics interne, une autorisation est nécessaire. Une fois l'autorisation attribuée, vous pouvez télécharger les fichiers source de l'application.

Avant de commencer :

- Spécifier l'emplacement réseau partagé où stocker des applications internes.
- Si vous ajoutez des applications Windows Phone, téléchargez un AET.
- Vous devez disposer d'une licence Application Edition ou Content Edition pour pouvoir ajouter une autorisation d'application BlackBerry Dynamics interne

1. Sur la barre de menus, cliquez sur **Applications**.
2. Cliquez sur .
3. Cliquez sur **Autorisations d'application BlackBerry Dynamics interne**.
4. Dans le champ Nom, saisissez le nom de l'application que vous souhaitez ajouter.
5. Dans le champ **ID d'autorisation BlackBerry Dynamics**, saisissez l'ID d'autorisation de l'application que vous souhaitez ajouter. Si vous ne connaissez pas l'ID d'autorisation de l'application, contactez le développeur de

l'application. Pour plus d'information sur les ID d'autorisation, reportez-vous à la documentation relative à BlackBerry Dynamics SDK. L'ID d'autorisation doit être au format suivant :

- Nom de domaine inversé, par exemple, `com.votre_entreprise.nom_application`.
- Ne doit pas commencer par l'un des éléments suivants
  - com.blackberry
  - com.good
  - com.rim
  - net.rim
- Ne doit pas contenir de majuscules
- Doit être conforme au format du <sous-domaine> défini dans la section 2.3.1 de la norme RFC 1035, telle qu'amendée par la section 2.1 de la norme RFC 1123.

6. Dans le champ **Version de l'autorisation BlackBerry Dynamics**, saisissez la version de l'autorisation. Si vous ne connaissez pas la version de l'autorisation, contactez le développeur de l'application. La version de l'autorisation doit être au format suivant :
   - Un à quatre segments de chiffres, séparés par des points, par exemple, 100 ou 1.2.3.4.
   - Pas de zéro non significatif dans les segments numériques. Par exemple, vous ne pouvez pas utiliser 0100 ou 01.02.03.04.
   - Les segments numériques peuvent comprendre un à trois caractères, par exemple, 100.200.300.400.
7. Vous pouvez également ajouter une description de l'application.
8. Cliquez sur **Ajouter**.

À la fin :

- Télécharger les fichiers source d'une application BlackBerry Dynamics
- Pour les applications à installer sur les terminaux Android disposant d'un profil professionnel, procédez comme suit :
  - Héberger une application interne pour les terminaux disposant d'un profil professionnel Android dans Google Play à l'aide du fichier .apk
  - Héberger une application interne pour les terminaux Android disposant d'un profil professionnel dans BlackBerry UEM à l'aide d'un fichier .json

Télécharger les fichiers source d'une application BlackBerry Dynamics

Lorsqu'une attribution d'application BlackBerry Dynamics a été créée, vous pouvez télécharger les fichiers source des plates-formes de terminaux qui conviennent.

Remarque : Les utilisateurs doivent activer les applications Dynamics sur le même environnement BlackBerry UEM à partir duquel les applications ont été attribuées. L'activation d'applications BlackBerry Dynamics avec des clés d'accès à partir d'un environnement externe BlackBerry Dynamics n'est pas prise en charge.

Avant de commencer :

- Ajouter une autorisation d'application BlackBerry Dynamics interne

1. Sur la barre de menus, cliquez sur **Applications**.
2. Cliquez sur l'application pour laquelle vous souhaitez télécharger des fichiers source.
3. Cliquez sur l'onglet de la plateforme de terminaux pour laquelle vous souhaitez télécharger un fichier source.
4. Dans la section **Fichier source de l'application**, cliquez sur **Ajouter.**
5. Cliquez sur **Parcourir**. Naviguez jusqu'à l'application que vous souhaitez ajouter ou mettre à jour.
6. Cliquez sur **Ajouter**.

7. Si nécessaire, mettez à jour les paramètres de l'application. Pour plus d'informations, reportez-vous à Gérer les paramètres d'une application BlackBerry Dynamics.

Héberger une application interne pour les terminaux dotés d'un profil professionnel Android dans Google Play à l'aide du fichier .apk

Lorsque vous hébergez une application dans Google Play, vous pouvez utiliser les paramètres de configuration pour modifier les comportements de l'application et la définir en tant qu'obligatoire ou facultative. Pour héberger une application dans Google Play, vous devez la publier dans Google Play de sorte que les utilisateurs puissent installer l'application interne sur leurs terminaux.

Avant de commencer :

- Dans BlackBerry UEM, ajoutez le fichier .apk interne à la liste des applications. Sélectionnez l'option **Activer l'application pour les profils professionnels Android**, et dans la liste déroulante **L'application sera hébergée par**, cliquez sur **Google Play**.
  Remarque : Vous devez sélectionner **Activer l'application pour les profils professionnels Android** même si vous hébergez l'application pour tous les terminaux Android.
- Vous devez disposer d'un compte pour vous connecter à Google Developers Console. Si un profil professionnel Android est configuré, utilisez l'adresse électronique du compte de développeur que vous avez utilisée pour configurer le profil professionnel. Pour chaque domaine BlackBerry UEM, vous devez utiliser un compte de développeur différent.

Rendez-vous sur https://support.blackberry.com/kb et consultez l'article KB 47873 concernant les instructions d'hébergement d'une application interne pour les terminaux Android avec un profil professionnel dans BlackBerry UEM à l'aide d'un fichier .apk.

Tâches connexes

Ajouter une application interne à la liste des applications

Héberger une application interne pour les terminaux Android dotés d'un profil professionnel dans BlackBerry UEM à l'aide d'un fichier .json

Pour héberger une application interne pour des terminaux Android dotés d'un profil professionnel dans BlackBerry UEM, vous devez générer un fichier .json pour l'application, télécharger le fichier sur Google Play et obtenir la clé de licence pour l'application publiée. Les applications qui sont hébergées dans BlackBerry UEM peuvent être définies comme facultatives uniquement, et vous ne pouvez pas utiliser les paramètres de configuration pour modifier les comportements et fonctionnalités de l'application.

Avant de commencer :

- Vérifiez qu'OpenSSL, JDK, Python 2.x et Android Asset Packaging Tool (aapt) sont installés dans un chemin sur l'ordinateur.
- Vous devez disposer d'un compte pour vous connecter à Google Developers Console. Si vous avez configuré la prise en charge des profils professionnels Android, utilisez l'adresse électronique du compte de développeur que vous avez utilisée pour configurer les profils professionnels Android. Pour chaque domaine BlackBerry UEM, vous devez utiliser un compte de développeur différent.
- Dans BlackBerry UEM, ajoutez une application interne à la liste des applications. Sélectionnez l'option **Activer l'application pour les profils professionnels Android**, et dans la liste déroulante **L'application sera hébergée par**, cliquez sur **BlackBerry UEM**. Copiez et enregistrez l'URL qui s'affiche dans BlackBerry UEM.
  Remarque : Vous devez sélectionner **Activer l'application pour les profils professionnels Android** même si vous hébergez l'application pour tous les terminaux Android.

Rendez-vous sur http://support.blackberry.com/kb et consultez l'article KB 47768 concernant les instructions d'hébergement d'une application interne pour les terminaux avec un profil professionnel Android dans BlackBerry UEM à l'aide d'un fichier .json.

Tâches connexes

Ajouter une application interne à la liste des applications

Mettre à jour une application interne

Lorsque vous mettez à jour une application interne, l'application mise à jour remplacera l'application actuellement attribuée aux utilisateurs et aux groupes. Les terminaux BlackBerry mettent automatiquement à jour la version de l'application. Les autres terminaux inviteront peut-être l'utilisateur à installer la nouvelle version de l'application.

Avant de commencer : Si vous mettez à jour une application qui est hébergée dans Google Play pour les terminaux Android dotés d'un profil professionnel, ajoutez la version mise à jour de l'application à Google Play et attendez que Google publie l'application avant de la mettre à jour dans BlackBerry UEM.

1. Sur la barre de menus, cliquez sur **Applications**.
2. Cliquez sur l'application interne que vous souhaitez mettre à jour.
3. Dans le coin supérieur droit, cliquez sur .
4. Dans la boite de dialogue **Mettre à jour l'application interne**, cliquez sur **Parcourir** et naviguez jusqu'à l'application que vous souhaitez mettre à jour.
5. Cliquez sur **Ajouter** jusqu'à ce que le bouton **Enregistrer** s'affiche.
6. Cliquez sur **Save**.

Mettre à jour une application interne pour les terminaux Android dotés d'un profil professionnel dans BlackBerry UEM à l'aide d'un fichier .json

Rendez-vous sur https://support.blackberry.com/kbet consultez l'article KB 47768 concernant les instructions de mise à jour d'une application interne pour les terminaux Android dotés d'un profil professionnel dans BlackBerry UEM à l'aide d'un fichier .json.

Ajout ou modification d'une configuration d'application

Les configurations d'application vous permettent de préconfigurer certains paramètres avant d'attribuer des applications aux utilisateurs. Lorsque vous préconfigurez les paramètres d'une application, son téléchargement, sa configuration et son utilisation sont plus faciles pour les utilisateurs. Par exemple, les utilisateurs doivent souvent saisir une URL, une adresse électronique ou d'autres informations avant de pouvoir utiliser une application. En ajoutant une configuration d'application, vous pouvez configurer certains de ces paramètres à l'avance. Vous pouvez créer plusieurs configurations pour une même application avec différents paramètres pour des usages différents, puis classer ces configurations. Si une application est attribuée plusieurs fois à un utilisateur avec différentes configurations, l'application au classement le plus élevé s'applique.

Dans BlackBerry UEM, vous pouvez créer une configuration d'application pour les applications suivantes :

- Applications iOS (publiques ou internes) développées avec des fonctionnalités Configuration gérée. Reportez-vous à la section Ajouter une application iOS à la liste des applications.
- Applications Android (publiques ou internes) développées avec des fonctionnalités Restrictions d'application Android. BlackBerry UEM doit être configuré pour prendre en charge les profils professionnels Android. Reportez-vous à la section Ajouter une application Android à la liste des applications si BlackBerry UEM est configuré pour les profils professionnels Android.

Pour plus d'informations sur les paramètres des applications, contactez leur fournisseur.

Pour plus d'informations sur la configuration des applications, rendez-vous sur http://www.appconfig.org/.

Ajout de raccourcis d'application

Vous pouvez utiliser les raccourcis d'application pour ajouter un raccourci personnalisé vers le terminal ou BlackBerry Dynamics Launcher. Par exemple, vous pouvez ajouter un raccourci au site Web interne de votre entreprise. Pour chaque raccourci d'application, vous pouvez configurer les attributs suivants :

- Adresse Web qui s'ouvre lorsque l'utilisateur sélectionne l'icône
- Icône et étiquette du raccourci
- Emplacement pour ajouter le raccourci de l'application (par exemple, BlackBerry Dynamics Launcher)
- Si l'adresse Web s'ouvre dans le navigateur sécurisé BlackBerry Access

Remarque : Les profils d'icône Web sont maintenant des raccourcis d'applications. Dans BlackBerry UEM version 12.7 et ultérieure, tout profil d'icône Web de BlackBerry UEM version 12.6 ou antérieure est automatiquement converti en un raccourci d'application. Les raccourcis d'application se trouvent dans la liste Applications de la console de gestion.

Créer un raccourci d'application

Vous devez créer un raccourci d'application pour chaque raccourci à afficher sur les terminaux des utilisateurs. Pour les terminaux activés avec BlackBerry Dynamics, vous avez la possibilité d'ajouter le raccourci au BlackBerry Dynamics Launcher.

Avant de commencer :

- Vérifiez qu'une autorisation d'application est affectée aux utilisateurs pour Fonctionnalité - App Store BlackBerry (com.blackberry.feature.appstore).
- vérifiez que l'image que vous prévoyez d'utiliser pour l'icône du raccourci répond aux exigences suivantes :
  - L'image est au format .png, .jpg ou .jpeg.
  - L'image ne possède pas d'éléments transparents. Tout élément transparent s'affichera en noir sur le terminal.
  - La taille maximale de l'image est de 120 x 120.

1. Sur la barre de menus, cliquez sur **Applications**.
2. Cliquez sur .
3. Cliquez sur **Raccourci d'application**.
4. Saisissez le nom et la description du raccourci d'application. Le nom est utilisé en tant que libellé pour le raccourci d'application.
5. Dans le champ **Icône de raccourci**, cliquez sur **Parcourir**. Localisez et sélectionnez une image pour l'icône du raccourci d'application. Les formats d'image pris en charge sont les suivants : .png, .jpg ou .jpeg.
6. Sélectionnez les types de terminaux pour lesquels vous souhaitez configurer ce raccourci d'application.
7. Dans chacun des onglets du type de terminal que vous avez sélectionné, procédez comme suit :
   - Pour ajouter un raccourci à un site Web, dans le champ URL, saisissez l'adresse Web du raccourci. L'adresse Web doit commencer par http:// ou https://.
8. Sélectionnez l'emplacement où vous voulez ajouter le raccourci. Pour les terminaux avec BlackBerry Dynamics, indiquez si vous souhaitez que le raccourci s'ouvre dans le navigateur BlackBerry Access.
9. Cliquez sur **Ajouter**.

Tâches connexes

Attribuer une application à un groupe d'utilisateurs

Attribuer une application à un compte d'utilisateur

Empêcher les utilisateurs d'installer des applications spécifiques

Pour empêcher les utilisateurs d'installer des applications spécifiques, vous pouvez créer une liste d'applications interdites et utiliser des profils de conformité pour faire appliquer ces restrictions. Par exemple, vous pouvez empêcher les utilisateurs d'installer des applications malveillantes ou nécessitant une grande quantité de ressources.

Interdire des applications spécifiques

Pour iOS, Android ou Windows Phone, vous pouvez créer un profil de conformité afin de sélectionner des applications de la liste d'applications interdites et définir une mesure d'application telle que Envoyer un message à l'utilisateur ou Supprimer les données professionnelles si l'une de ces applications est installée.

Pour les terminaux suivants, vous n'avez pas besoin de spécifier une mesure d'application car l'installation des applications que vous spécifiez dans un profil de conformité est automatiquement bloquée :

- Pour les terminaux Windows Phone 8.1 et Samsung KNOX, si un utilisateur tente d'installer une application non autorisée, le terminal affiche un message indiquant que l'application est interdite et qu'elle ne peut pas être installée. Si une application interdite est déjà installée, elle est désactivée. Pour les terminaux Samsung KNOX, vous pouvez sélectionner une option dans le profil de conformité afin d'empêcher l'installation d'applications dans l'espace Personnel ainsi que dans l'espace Travail.
- Pour les terminaux iOS 9.3.2 et versions ultérieures sous supervision, si un utilisateur tente d'installer une application interdite, celle-ci est masquée. Si une application interdite est déjà installée, elle est automatiquement masquée sans en notifier l'utilisateur. Pour restreindre les applications intégrées, vous devez créer un profil de conformité et ajouter les applications à la liste d'applications limitées dans le profil. Pour plus d'informations, reportez-vous à iOS : paramètres de profil de conformité.
- Pour les terminaux BlackBerry 10 et Android dotés d'un profil professionnel, il n'est pas nécessaire de créer un profil de conformité pour interdire des applications car les utilisateurs peuvent uniquement installer les applications de l'espace Travail que vous leur avez attribué. Si une application interdite est déjà installée sur un terminal, elle n'est pas désactivée.
- Pour les terminaux Android dotés d'un profil professionnel, il n'est pas nécessaire de créer un profil de conformité pour interdire des applications, autres que celles du système, car les utilisateurs peuvent uniquement installer les applications de l'espace Travail que vous leur avez attribué. Si une application interdite est déjà installée sur un terminal, elle n'est pas désactivée. Si vous souhaitez restreindre une application système (comme la calculatrice, le réveil, ou l'appareil photo), vous devez ajouter l'application système à un profil de conformité afin d'appliquer la restriction.

Autoriser des applications spécifiques

Pour les terminaux iOS 9.3.2 et versions ultérieures sous supervision, vous pouvez créer un profil de conformité incluant une liste d'applications autorisées. Toutes les autres applications, à l'exception des applications Téléphone et Préférences, seront automatiquement masquées sur le terminal. Les applications non autorisées déjà installées seront automatiquement masquées sans en notifier l'utilisateur. Les applications suivantes sont incluses par défaut dans la liste des applications autorisées pour permettre la gestion des terminaux dans BlackBerry UEM :

- BlackBerry UEM Client
- Icônes du clip Web
- BlackBerry Secure Connect Plus

Remarque : Si la même application iOS est à la fois attribuée à la liste des applications interdites et à la liste des applications autorisées d'un profil de conformité, elle est considérée comme interdite.

Pour plus d'informations sur la création de profils de conformité, reportez-vous à Créer un profil de conformité.

Étapes à suivre pour empêcher les utilisateurs d'installer des applications spécifiques

Pour empêcher les utilisateurs d'installer des applications, procédez comme suit :

Étape	Action
1	Ajouter une application à la liste des applications limitées. **Remarque :** Que vous souhaitiez interdire ou autoriser des applications spécifiques, vous devez les ajouter à la liste des applications interdites. **Remarque :** Cette étape ne s'applique pas aux applications intégrées pour les terminaux iOS supervisés 9.3.2 et versions ultérieures. Pour restreindre les applications intégrées, vous devez créer un profil de conformité et ajouter les applications à la liste d'applications limitées dans le profil. Pour plus d'informations, reportez-vous à iOS : paramètres de profil de conformité.
2	Créer ou modifier un profil de conformité.
3	Attribuez le profil de conformité à un utilisateur, à un groupe d'utilisateurs ou à un groupe de terminaux.

Ajouter une application à la liste des applications limitées

La liste des applications interdites est une bibliothèque d'applications que vous pouvez sélectionner lorsque vous souhaitez appliquer l'une des règles de conformité suivantes :

- Une application interdite est installée (pour les terminaux iOS, Android ou Windows Phone)
- Afficher les applications autorisées sur le terminal uniquement (pour les terminaux iOS 9.3.2 et versions ultérieures sous supervision)

1. Sur la barre de menus, cliquez sur **Applications**.
2. Cliquez sur **Applications limitées**.
3. Cliquez sur +.
4. Effectuez l'une des tâches suivantes :

Tâche	Étapes
Ajouter une application iOS à la liste des applications limitées	a. Cliquez sur **Boutique d'applications**. b. Dans le champ de recherche, recherchez l'application que vous souhaitez ajouter. Vous pouvez rechercher une application par nom, fournisseur ou URL App Store. c. Cliquez sur **Rechercher**. d. Dans les résultats de la recherche, cliquez sur **Ajouter** pour ajouter une application.

Tâche	Étapes
Ajouter une application Android à la liste des applications limitées	**a.** Cliquez sur **Google Play**. **b.** Dans le champ **Nom de l'application**, saisissez le nom de l'application. **c.** Dans le champ **Adresse Web de l'application sur Google Play**, saisissez l'adresse Web de l'application dans Google Play. **d.** Cliquez sur **Ajouter** pour ajouter l'application ou sur **Ajouter et Nouveau** pour ajouter une autre application après avoir ajouté l'application en cours.
Ajouter une application Windows Phone à la liste des applications limitées	**a.** Cliquez sur **Windows Store**. **b.** Dans le champ **Nom de l'application**, saisissez le nom de l'application. **c.** Dans le champ **Adresse Web de l'application sur Windows Store**, saisissez l'adresse Web de l'application dans Windows Store. **d.** Cliquez sur **Ajouter** pour ajouter l'application ou sur **Ajouter et Nouveau** pour ajouter une autre application après avoir ajouté l'application en cours.

Tâches connexes

Créer un profil de conformité
Attribuer un profil ou une stratégie informatique à un groupe d'utilisateurs
Attribuer un profil ou une stratégie informatique à un compte d'utilisateur
Créer un groupe de terminaux

Gestion des applications à l'aide de la liste des applications

La liste des applications contient les applications que vous pouvez attribuer aux utilisateurs, groupes d'utilisateurs et groupes de terminaux. La liste des applications fournit les informations suivantes :

- Nom et icône de l'application
- Fournisseur de l'application
- Système d'exploitation pris en charge
- Nombre d'utilisateurs appliqués
- Nombre de terminaux sur lesquels l'application est installée
- Évaluation d'application
- Source d'application

Vous pouvez cliquer sur le nombre d'utilisateurs appliqués pour afficher les informations sur l'état d'installation de l'application.

Vous pouvez cliquer sur le nombre de terminaux sur lesquels l'application est installée pour afficher le nombre d'installations confirmées et non confirmées. Les installations non confirmées incluent les installations effectuées sur les terminaux iOS utilisant le type d'activation Confidentialité de l'utilisateur, car UEM ne peut pas confirmer si l'application est toujours installée sur le terminal.

Les applications accompagnées d'une icône de verrouillage sont des applications BlackBerry Dynamics. Pour plus d'informations, reportez-vous à Gestion des applications BlackBerry Dynamics.

Remarque : Les applications attribuées aux utilisateurs par un profil de protection de l'application Microsoft Intune n'apparaissent pas dans la liste des applications.

Supprimer une application de la liste des applications

Lorsque vous supprimez une application de la liste des applications, l'application est désattribuée des utilisateurs ou des groupes concernés et n'apparait plus dans le catalogue des applications professionnelles du terminal.

1. Sur la barre de menus, cliquez sur **Applications**.
2. Cochez la case en regard des applications que vous souhaitez supprimer de la liste des applications.
3. Cliquez sur 🗑.
4. Cliquez sur **Supprimer**.

Spécifier si une application est requise ou facultative

Vous pouvez spécifier si une application est requise ou facultative Les actions prises lorsqu'une application est définie sur Requise ou Facultative dépendent du type d'application, du terminal et du type d'activation.

1. Sur la barre de menus, cliquez sur **Utilisateurs et terminaux**.
2. Si l'application que vous souhaitez modifier est attribuée à un compte d'utilisateur, dans les résultats de la recherche, cliquez sur le nom d'un compte d'utilisateur.
3. Si l'application que vous souhaitez modifier est attribuée à un groupe, dans le volet de gauche, cliquez sur **Groupes** pour développer la liste des groupes d'utilisateurs, puis cliquez sur le nom du groupe.
4. Dans la section **Applications attribuées à des groupes et utilisateurs**, cliquez sur la disposition de l'application que vous souhaitez modifier.
5. Dans la liste déroulante **Disposition**, sélectionnez **Facultative** ou **Obligatoire**.
6. Cliquez sur **Attribuer**.

Référence connexe

Comportement des applications sur les terminaux Android
Comportement des applications sur les terminaux iOS
Comportement de l'application sur les terminaux BlackBerry

Notifications de terminal pour les nouvelles applications et les applications mises à jour

Dans la plupart des cas, les utilisateurs reçoivent des notifications sur leurs terminaux lorsque vous affectez de nouvelles applications, ou lorsque des mises à jour sont disponibles pour les applications installées. En plus des notifications de terminal, toute nouvelle application ou mise à jour d'application s'affiche dans la liste « Nouvelles/Mises à jour » du catalogue d'applications dans le BlackBerry UEM Client ou dans les Applications professionnelles.

Les applications (requises ou facultatives) s'affichent dans la liste « Nouvelles/Mises à jour » dans les situations suivantes :

- Une application est attribuée à un utilisateur et elle n'est pas déjà installée sur son terminal
- Une application est attribuée à un utilisateur et elle est automatiquement installée
- Une mise à niveau d'une application installée est disponible

BlackBerry UEM renverra régulièrement des notifications aux terminaux si les applications restent dans la liste « Nouvelles/Mises à jour ».

Dans la liste d'applications « Nouvelles/Mises à jour », si un utilisateur clique sur une nouvelle application pour en afficher les détails, l'application est retirée de la liste « Nouvelles/Mises à jour », que l'utilisateur l'installe ou non.

Si un utilisateur clique sur une mise à jour d'application, l'application reste dans la liste jusqu'à ce que la mise à jour soit installée.

Pour plus d'informations sur les notifications d'application, reportez-vous à .

- Comportement des applications sur les terminaux iOS
- Comportement des applications sur les terminaux Android
- Comportement de l'application sur les terminaux Android dotés d'un profil professionnel
- Comportement de l'application sur les terminaux Samsung KNOX

Comportement des applications sur les terminaux iOS

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

Pour les terminaux iOS activés avec Contrôles MDM et Confidentialité de l'utilisateur, il se produit ce qui suit :

Type d'application	Lorsque les applications sont attribuées à un utilisateur	Lorsque les applications sont mises à jour	Lorsque des applications sont désattribuées d'un utilisateur	Comportement lorsque le terminal est supprimé de BlackBerry UEM
Applications publiques dotée d'une disposition requise	• Si les applications sont déjà installées, l'utilisateur est invité à autoriser BlackBerry UEM à gérer les applications. • Sur les terminaux supervisés, les applications sont installées automatiquement. • Sur les terminaux non supervisés, les utilisateurs ne sont pas invités à installer les applications. Les utilisateurs doivent se rendre sur le catalogue de l'application pour installer les applications requises. • Les applications sont supprimées de la liste « Nouvelles/ Mises à jour » lorsque l'utilisateur affiche les détails (même si l'application n'est pas installée), ou lorsque l'utilisateur installe les applications. • Vous pouvez utiliser un profil de conformité pour définir les actions prises si les applications requises ne sont pas installées.	• iTunes informe les utilisateurs des mises à jour disponibles. • Les applications sont supprimées de la liste « Nouvelles/ Mises à jour » lorsque l'application est mise à jour. (peut prendre jusqu'à une heure) • Pour les terminaux qui n'ont pas accès à iTunes, les utilisateurs ne sont pas notifiés mais ils peuvent télécharger la mise à jour depuis le catalogue d'applications.	• Les applications sont automatiquement supprimées du terminal sans notification. • Les applications n'apparaissent plus dans le catalogue d'applications.	• Pour les terminaux activés avec Contrôles MDM, les applications sont automatiquement supprimées. • Pour les terminaux activés avec Confidentialité de l'utilisateur, les utilisateurs sont invités à supprimer les applications.

Type d'application	Lorsque les applications sont attribuées à un utilisateur	Lorsque les applications sont mises à jour	Lorsque des applications sont désattribuées d'un utilisateur	Comportement lorsque le terminal est supprimé de BlackBerry UEM
Applications publiques dotée d'une disposition facultative	• Si l'application est déjà installée, il ne se passe rien. • L'utilisateur est informé d'une modification au catalogue d'applications. • Les applications sont supprimées de la liste Nouvelles/ Mises à jour uniquement lorsque l'utilisateur affiche les détails (que l'application soit installée ou non). • Les utilisateurs peuvent choisir d'installer les applications.	• iTunes informe les utilisateurs des mises à jour disponibles. • Les applications sont supprimées de la liste « Nouvelles/ Mises à jour » lorsque l'utilisateur affiche les détails (que l'application soit mise à jour ou non).	• Les applications sont supprimées automatiquement du terminal. • Les applications n'apparaissent plus dans le catalogue d'applications.	• Pour les terminaux activés avec Contrôles MDM, les applications sont automatiquement supprimées. • Pour les terminaux activés avec Confidentialité de l'utilisateur, les utilisateurs sont invités à supprimer les applications.

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

Type d'application	Lorsque les applications sont attribuées à un utilisateur	Lorsque les applications sont mises à jour	Lorsque des applications sont désattribuées d'un utilisateur	Comportement lorsque le terminal est supprimé de BlackBerry UEM
Applications internes dotées d'une disposition facultative	• Si les applications sont déjà installées, il ne se passe rien. • Les applications sont supprimées de la liste « Nouvelles/ Mises à jour » lorsque l'utilisateur affiche les détails (même si l'application n'est pas installée), ou lorsque l'utilisateur installe les applications.	• Les applications sont supprimées de la liste « Nouvelles/ Mises à jour » lorsque l'application est mise à jour.	• Les applications sont automatiquement supprimées du terminal sans notification. • Les applications n'apparaissent plus dans le catalogue d'applications.	• Pour les terminaux activés avec Contrôles MDM, les applications sont automatiquement supprimées. • Pour les terminaux activés avec Confidentialité de l'utilisateur, les utilisateurs sont invités à supprimer les applications.

Comportement des applications sur les terminaux Android

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

Pour les terminaux Android activés avec Contrôles MDM et Confidentialité de l'utilisateur, il se produit ce qui suit :

Type d'application	Lorsque les applications sont attribuées à un utilisateur	Lorsque les applications sont mises à jour	Lorsque les applications sont désattribuées d'un utilisateur	Lorsque le terminal est supprimé de BlackBerry UEM
Applications publiques dotée d'une disposition requise	• L'utilisateur est informé qu'une modification a été apportée sur le catalogue d'applications. • Les applications sont supprimées de la liste Nouvelles/Mises à jour lorsque l'utilisateur affiche les détails (même si l'application n'est pas installée), ou lorsque l'utilisateur installe les applications. • Vous pouvez utiliser un profil de conformité pour définir les actions prises si les applications requises ne sont pas installées.	L'utilisateur est informé par Google Play.	• L'utilisateur est invité à supprimer les applications. • Les applications n'apparaissent plus dans le catalogue d'applications.	• L'utilisateur est invité à supprimer les applications.
Applications publiques dotée d'une disposition facultative	• L'utilisateur peut choisir d'installer les applications.	L'utilisateur est informé par Google Play.	• L'utilisateur est invité à supprimer les applications. • Les applications n'apparaissent plus dans le catalogue d'applications.	• L'utilisateur est invité à supprimer les applications.

Type d'application	Lorsque les applications sont attribuées à un utilisateur	Lorsque les applications sont mises à jour	Lorsque les applications sont désattribuées d'un utilisateur	Lorsque le terminal est supprimé de BlackBerry UEM
Applications internes dotées d'une disposition requise	• L'utilisateur est informé qu'une modification a été apportée sur le catalogue d'applications. • Les applications sont installées automatiquement. • Les applications sont supprimées de la liste Nouvelles/Mises à jour lorsque l'utilisateur affiche les détails ou lorsque l'application est installée. • Vous pouvez utiliser un profil de conformité pour définir les actions prises si les applications requises ne sont pas installées.	• L'utilisateur est informé qu'une modification a été apportée sur le catalogue d’applications. • Les mises à jour sont installées automatiquement. • Les applications sont supprimées de la liste « Nouvelles/ Mises à jour » lorsque l'utilisateur affiche les détails ou lorsque l'application est mise à jour.	• L'utilisateur est invité à supprimer les applications. • Les applications n'apparaissent plus dans le catalogue d’applications.	• L'utilisateur est invité à supprimer les applications.
Applications internes dotées d'une disposition facultative	• L'utilisateur peut choisir d'installer les applications. • Les applications apparaissent dans la liste Nouvelles/Mises à jour.	• Les applications apparaissent dans la liste « Nouvelles/ Mises à jour ».	• L'utilisateur est invité à supprimer les applications. • Les applications n'apparaissent plus dans le catalogue d’applications.	• L'utilisateur est invité à supprimer les applications.

Comportement de l'application sur les terminaux Samsung KNOX

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

Pour les terminaux Samsung KNOX activés avec « Contrôles MDM », il se produit ce qui suit :

Type d'application	Lorsque l'application est attribuée à un utilisateur	Lorsque les applications sont mises à jour	Lorsque l'application est désattribuée à un utilisateur	Lorsque le terminal est supprimé de BlackBerry UEM
Applications publiques dotée d'une disposition requise	• L'utilisateur est invité à installer les applications. • Les applications attribuées apparaissent dans BlackBerry UEM Client. Lorsque l'utilisateur clique sur le bouton Installer, Google Play s'ouvre et l'application est installée. • Vous pouvez utiliser un profil de conformité pour définir les actions prises si les applications requises ne sont pas installées.	• Google Play informe les utilisateurs des mises à jour. • L'application s'affiche dans la liste « Nouvelles/ Mises à jour ».	• L'utilisateur est invité à désinstaller les applications.	• L'utilisateur est invité à désinstaller les installations professionnelles attribuées.
Applications publiques dotées d'une disposition facultative	• L'utilisateur peut choisir d'installer les applications. • Les applications attribuées apparaissent dans BlackBerry UEM Client. Lorsque l'utilisateur clique sur le bouton Installer, Google Play s'ouvre et les applications sont installées.	• Google Play informe les utilisateurs des mises à jour. • L'application s'affiche dans la liste « Nouvelles/ Mises à jour ».	• L'utilisateur est invité à désinstaller les applications.	• L'utilisateur est invité à désinstaller les installations professionnelles attribuées.

Type d'application	Lorsque l'application est attribuée à un utilisateur	Lorsque les applications sont mises à jour	Lorsque l'application est désattribuée à un utilisateur	Lorsque le terminal est supprimé de BlackBerry UEM
Applications internes dotées d'une disposition requise	• Les applications sont automatiquement installées sur les terminaux. L'utilisateur ne peut pas désinstaller les applications.	• Les applications sont mises à jour automatiquement.	• Les applications sont supprimées automatiquement du terminal.	• Les applications sont supprimées automatiquement du terminal.
Applications internes dotées d'une disposition facultative	• L'utilisateur peut choisir d'installer les applications. • L'utilisateur installe les applications depuis BlackBerry UEM Client.	• L'utilisateur peut choisir de mettre à jour les applications. • L'utilisateur met à jour les applications depuis BlackBerry UEM Client.	• Les applications sont supprimées automatiquement du terminal.	• Les applications sont supprimées automatiquement du terminal.

Pour les terminaux activés avec l'espace Travail uniquement (Samsung KNOX), il se produit ce qui suit :

Type d'application	Lorsque l'application est attribuée à un utilisateur	Lorsque les applications sont mises à jour	Lorsque l'application est désattribuée à un utilisateur	Lorsque le terminal est supprimé de BlackBerry UEM
Applications publiques dotée d'une disposition requise	• Par défaut, toutes les applications publiques sont restreintes dans l'espace Travail. • Les applications attribuées apparaissent dans la liste « Nouvelles/ Mises à jour », mais doivent être installées depuis Google Play. • Les applications sont supprimées de la liste « Nouvelles/ Mises à jour » lorsque l'utilisateur affiche les détails ou lorsque l'application est mise à jour. • Google Play doit être activé dans la stratégie informatique attribuée à l'utilisateur. • Vous pouvez utiliser un profil de conformité pour définir les actions prises si les applications requises ne sont pas installées.	• Google Play informe les utilisateurs des mises à jour. • Les applications apparaissent dans la liste « Nouvelles/ Mises à jour ». • Les applications sont supprimées de la liste « Nouvelles/ Mises à jour » lorsque l'utilisateur affiche les détails ou lorsque l'application est mise à jour.	• Les applications sont supprimées du terminal et ne peuvent plus être installées depuis Google Play.	• L'espace Travail et toutes les applications professionnelles sont automatiquement supprimées. • Les applications ne sont plus automatiquement restreintes dans Google Play.

Type d'application	Lorsque l'application est attribuée à un utilisateur	Lorsque les applications sont mises à jour	Lorsque l'application est désattribuée à un utilisateur	Lorsque le terminal est supprimé de BlackBerry UEM
Applications publiques dotées d'une disposition facultative	• Par défaut, toutes les applications publiques sont restreintes dans l'espace Travail. • Les applications attribuées apparaissent dans la liste « Nouvelles/ Mises à jour », mais doivent être installées depuis Google Play. • Les applications sont supprimées de la liste « Nouvelles/ Mises à jour » lorsque l'utilisateur affiche les détails ou lorsque l'application est mise à jour. • Google Play doit être activé dans la stratégie informatique attribuée à l'utilisateur.	• Google Play informe les utilisateurs des mises à jour. • Les applications apparaissent dans la liste « Nouvelles/ Mises à jour ». • Les applications sont supprimées de la liste « Nouvelles/ Mises à jour » lorsque l'utilisateur affiche les détails ou lorsque l'application est mise à jour.	• Les applications sont supprimées du terminal et ne peuvent plus être installées depuis Google Play.	• Les applications sont supprimées automatiquement. • Les applications ne sont plus automatiquement restreintes dans Google Play.
Applications internes dotées d'une disposition requise	• Les applications sont automatiquement installées sur les terminaux. L'utilisateur ne peut pas désinstaller les applications.	• Les applications sont mises à jour automatiquement sur le terminal.	• Les applications sont supprimées automatiquement du terminal.	• Les applications sont supprimées automatiquement du terminal.

Type d'application	Lorsque l'application est attribuée à un utilisateur	Lorsque les applications sont mises à jour	Lorsque l'application est désattribuée à un utilisateur	Lorsque le terminal est supprimé de BlackBerry UEM
Applications internes dotées d'une disposition facultative	• Les utilisateurs peuvent choisir d'installer les applications. • Les utilisateurs installent les applications depuis BlackBerry UEM Client.	• Les utilisateurs peuvent choisir de mettre à jour les applications. • Les utilisateurs mettent à jour les applications depuis BlackBerry UEM Client.	• Les applications sont supprimées automatiquement du terminal.	• Les applications sont supprimées automatiquement du terminal.

Pour les terminaux activés avec « Travail et Personnel - Contrôle total (Samsung KNOX) » et « Confidentialité de l'utilisateur (Samsung KNOX) », il se produit ce qui suit :

Type d'application	Lorsque l'application est attribuée à un utilisateur	Lorsque les applications sont mises à jour	Lorsque l'application est désattribuée à un utilisateur	Lorsque le terminal est supprimé de BlackBerry UEM
Applications publiques dotée d'une disposition requise	• Par défaut, toutes les applications publiques sont restreintes dans l'espace Travail. • L'utilisateur est invité à installer les applications. • Les applications attribuées apparaissent dans BlackBerry UEM Client. Lorsque l'utilisateur clique sur le bouton Installer, Google Play s'ouvre et l'application est installée. • Vous pouvez utiliser un profil de conformité pour définir les actions prises si les applications requises ne sont pas installées.	• Google Play envoie une notification	• Les applications restent dans l'espace Personnel, mais sont supprimées de l'espace Travail.	• L'espace Travail est supprimé et les applications restent dans l'espace Personnel.

Type d'application	Lorsque l'application est attribuée à un utilisateur	Lorsque les applications sont mises à jour	Lorsque l'application est désattribuée à un utilisateur	Lorsque le terminal est supprimé de BlackBerry UEM
Applications publiques dotées d'une disposition facultative	• Par défaut, toutes les applications sont restreintes dans l'espace Travail. • Les applications attribuées apparaissent dans BlackBerry UEM Client, mais doivent être installées depuis Google Play. • Google Play doit être activé dans la stratégie informatique attribuée à l'utilisateur.	• Google Play envoie une notification	• Les applications restent dans l'espace Personnel, mais sont supprimées de l'espace Travail.	• L'espace Travail est supprimé et les applications restent dans l'espace Personnel.
Applications internes dotées d'une disposition requise	• Les applications sont automatiquement installées dans l'espace Travail. L'utilisateur ne peut pas désinstaller les applications.	• Les mises à jour sont automatiquement installées.	• Les applications sont supprimées automatiquement du terminal.	• L'espace Travail est supprimé et les applications restent dans l'espace Personnel.
Applications internes dotées d'une disposition facultative	• Les utilisateurs peuvent choisir d'installer les applications. • Les utilisateurs installent les applications depuis BlackBerry UEM Client et les applications sont installées dans l'espace Travail.	• Les utilisateurs peuvent choisir de mettre à jour les applications. • Les utilisateurs mettent à jour les applications depuis BlackBerry UEM Client.	• Les applications sont supprimées automatiquement du terminal.	• L'espace Travail est supprimé et les applications restent dans l'espace Personnel.

Comportement de l'application sur les terminaux Android dotés d'un profil professionnel

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

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

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

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

Comportement de l'application sur les terminaux BlackBerry

Pour les terminaux BlackBerry activés avec Travail et Personnel - Entreprise (Espace Travail uniquement) ou Travail et Personnel - Régulé, il se produit ce qui suit :

Type d'application	Comportement lorsque des applications sont attribuées à un utilisateur	Comportement lorsque des applications sont désattribuées d'un utilisateur	Comportement lorsque le terminal est supprimé de BlackBerry UEM
Applications publiques dotée d'une disposition requise	• Non pris en charge.	• Non pris en charge.	• Non pris en charge.
Applications publiques dotée d'une disposition facultative	• L'utilisateur peut choisir d'installer les applications. • Les applications apparaissent dans l'onglet Applications publiques de BlackBerry World for Work.	• L'utilisateur est invité à désinstaller les applications.	• L'espace Travail et toutes les applications professionnelles sont automatiquement supprimées.

Type d'application	Comportement lorsque des applications sont attribuées à un utilisateur	Comportement lorsque des applications sont désattribuées d'un utilisateur	Comportement lorsque le terminal est supprimé de BlackBerry UEM
Applications internes dotées d'une disposition requise	• Les applications sont automatiquement installées sur les terminaux. • L'utilisateur ne peut pas désinstaller les applications.	• Les applications sont automatiquement supprimées du terminal.	• L'espace Travail et toutes les applications professionnelles sont automatiquement supprimées.
Applications internes dotées d'une disposition facultative	• Les applications sont automatiquement installées sur les terminaux. • L'utilisateur ne peut pas désinstaller les applications.	• Les applications sont automatiquement supprimées du terminal.	• L'espace Travail et toutes les applications professionnelles sont automatiquement supprimées.

Comportement de l'application sur les terminaux Windows 10

Type d'application	Comportement lorsque des applications sont attribuées à un utilisateur	Comportement lorsque des applications sont désattribuées d'un utilisateur	Comportement lorsque le terminal est supprimé de BlackBerry UEM
Applications Windows Store hors ligne dotée d'une disposition requise	• Les applications sont automatiquement installées sur les terminaux. Les utilisateurs ne peuvent pas désinstaller les applications.	• Les applications sont automatiquement supprimées des terminaux.	• Les applications sont automatiquement supprimées des terminaux.
Applications Windows Store en ligne dotée d'une disposition requise	• Les applications sont automatiquement installées sur les terminaux. Les utilisateurs ne peuvent pas désinstaller les applications.	• Les applications sont automatiquement supprimées des terminaux.	• Les applications sont automatiquement supprimées des terminaux.

Type d'application	Comportement lorsque des applications sont attribuées à un utilisateur	Comportement lorsque des applications sont désattribuées d'un utilisateur	Comportement lorsque le terminal est supprimé de BlackBerry UEM
Applications Windows Store hors ligne dotée d'une disposition facultative	• Les utilisateurs peuvent choisir d'installer les applications. • Pour les applications hors ligne, les utilisateurs installent l'application depuis BlackBerry UEM App Catalog. • Non pris en charge sur les terminaux Windows 10 Mobile.	• Les utilisateurs ne sont pas invités à désinstaller les applications.	• Les utilisateurs ne sont pas invités à désinstaller les applications attribuées.
Applications Windows Store en ligne dotée d'une disposition facultative	• Les utilisateurs peuvent choisir d'installer les applications. • Pour les applications en ligne, les utilisateurs installent l'application à partir de l'application Windows Store sur leurs terminaux. • Non pris en charge sur les terminaux Windows 10 Mobile.	• Les utilisateurs ne sont pas invités à désinstaller les applications.	• Les utilisateurs ne sont pas invités à désinstaller les applications.
Applications internes dotées d'une disposition requise	• Non pris en charge	• Non pris en charge	• Non pris en charge
Applications internes dotées d'une disposition facultative	• Non pris en charge	• Non pris en charge	• Non pris en charge

Gestion des groupes d'applications

Les groupes d'applications vous permettent de créer un ensemble d'applications à attribuer à des utilisateurs, groupes d'utilisateurs ou groupes de terminaux. Les groupes d'applications permettent une gestion plus efficace et plus cohérente des applications. Par exemple, vous pouvez utiliser les groupes d'applications pour grouper la même application pour plusieurs types de terminaux ou pour grouper des applications pour des utilisateurs dotés du même rôle au sein de votre organisation.

BlackBerry UEM fournit des groupes d'applications préconfigurées appelés « Applications recommandées pour les terminaux Android avec profil professionnel » et « BlackBerry Productivity Suite ».

Créer un groupe d'applications

Avant de commencer : Ajoutez les applications à la liste des applications.

1. Sur la barre de menus, cliquez sur **Applications > Groupes d'applications**.
2. Cliquez sur .
3. Saisissez le nom et la description du profil du groupe d'applications.
4. Cliquez sur .
5. Recherchez et sélectionnez les applications que vous souhaitez ajouter.
6. Pour les applications iOS et Android, si une configuration d'application est disponible, sélectionnez-la pour l'attribuer à l'application.
7. Si vous ajoutez des applications iOS, effectuez l'une des tâches suivantes :

Tâche	Étapes
Si vous n'avez pas ajouté de compte VPP	**a.** Cliquez sur **Ajouter**.
Si vous avez ajouté au moins un compte VPP	**a.** Cliquez sur **Ajouter**. **b.** Sélectionnez **Oui** si vous souhaitez attribuer une licence à l'application iOS. Sélectionnez **Non** si vous ne souhaitez pas attribuer une licence à l'application ou n'avez pas de licence à lui attribuer. **c.** Si vous attribuez une licence à l'application, dans la liste déroulante **Licences d'applications**, sélectionnez le compte VPP à associer à l'application. **d.** Dans la liste déroulante **Attribuer une licence à**, attribuez la licence à l'**utilisateur** ou au **terminal**. Si aucune valeur n'est spécifiée dans la liste déroulante **Licence d'application**, la liste déroulante **Attribuer une licence à** n'est pas disponible. **e.** Cliquez sur **Ajouter**, puis de nouveau sur **Ajouter**. Les utilisateurs doivent suivre les instructions qui s'affichent sur leurs terminaux pour inscrire le compte VPP de leur entreprise avant de pouvoir installer des applications prépayées. Les utilisateurs doivent effectuer cette tâche une seule fois. **Remarque :** si vous autorisez l'accès à plusieurs licences dont vous disposez, les premiers utilisateurs à accéder aux licences disponibles peuvent installer l'application.

8. Cliquez sur **Ajouter**, puis de nouveau sur **Ajouter**.

Tâches connexes

Attribuer une application à un groupe d'utilisateurs
Attribuer une application à un compte d'utilisateur

Modifier un groupe d'applications

1. Sur la barre de menus, cliquez sur **Applications > Groupes d'applications**.
2. Cliquez sur le groupe d'applications que vous souhaitez modifier.
3. Procédez aux modifications nécessaires.
4. Cliquez sur **Enregistrer**.

Afficher l'état des applications et des groupes d'applications attribués à des comptes d'utilisateur

1. Sur la barre de menus, cliquez sur **Applications**.
2. Sous **Utilisateurs appliqués** pour l'application ou le groupe d'applications que vous souhaitez afficher, cliquez sur le chiffre.
3. Cliquez sur **Attribué à *x* utilisateurs** pour afficher les comptes d'utilisateur auxquels est attribuée cette application.
4. Affichez la colonne **Attribution** pour vérifier si l'application ou le groupe d'applications a été directement attribué au compte d'utilisateur ou à un groupe.
5. Affichez la colonne **État** pour vérifier si une application est installée sur un terminal. Les états possibles sont les suivants :
   - **Installée** : l'application est installée sur le terminal de l'utilisateur. Pour les terminaux iOS utilisant le type d'activation Confidentialité de l'utilisateur, cet état indique uniquement que l'installation a été lancée. BlackBerry UEM ne peut pas confirmer que l'application reste installée sur le terminal.
   - **Non installée** : l'application n'a pas été installée sur le terminal de l'utilisateur ou en a été supprimée.
   - **Ne peut pas être installée** : l'application n'est pas prise en charge sur le terminal de l'utilisateur.
   - **Non pris en charge** : le système d'exploitation du terminal ne prend pas en charge cette application.

Afficher les applications attribuées à des groupes d'utilisateurs

1. Sur la barre de menus, cliquez sur **Applications**.
2. Sous **Attribué aux utilisateurs** pour l'application que vous souhaitez afficher, cliquez sur le chiffre.
3. Cliquez sur **Attribué aux utilisateurs** *x* pour afficher les groupes d'utilisateurs auxquels est attribuée cette application.

Afficher et personnaliser la liste des applications

Vous pouvez personnaliser la liste des applications et sélectionner les informations à afficher. Vous pouvez utiliser des filtres pour afficher uniquement les informations utiles à votre tâche. Vous pouvez sélectionner et réorganiser les colonnes de la liste des applications. Vous pouvez ajouter et supprimer des colonnes dans la liste des applications. Vous pouvez utiliser un ou plusieurs filtres pour sélectionner les applications à afficher. Par exemple, vous pouvez filtrer la liste des applications par type d'application, par système d'exploitation, par catégorie, par type sécurisé et par évaluation.

Sélectionner les informations à afficher dans la liste des applications

1. Sur la barre de menus, cliquez sur **Applications > Toutes les applications**.
2. Cliquez sur + en haut de la liste des applications et effectuez l'une des opérations suivantes :
   - Cliquez sur **Sélectionner tout** ou sélectionnez la case de chaque colonne que vous souhaitez afficher.
   - Décochez la case de chaque colonne que vous souhaitez supprimer.
   - Cliquez sur **Réinitialiser** pour rétablir les sélections par défaut.
3. Pour réorganiser les colonnes, cliquez sur l'en-tête d'une colonne et faites-le glisser vers la gauche ou vers la droite.

Filtrer la liste des applications

Lorsque vous activez la sélection multiple, vous pouvez sélectionner plusieurs filtres avant de les appliquer et vous pouvez choisir plusieurs filtres sous chaque catégorie. Lorsque vous désactivez la sélection multiple, chaque filtre est appliqué lorsque vous le sélectionnez et vous ne pouvez choisir qu'un seul filtre sous chaque catégorie.

1. Sur la barre de menus, cliquez sur **Applications > Toutes les applications**.
2. Cliquez sur pour activer ou désactiver la sélection multiple.
3. Sous **Filtres**, développez une ou plusieurs catégories.

   Chaque catégorie comprend uniquement des filtres qui affichent les résultats et chaque filtre indique le nombre de résultats à afficher lorsque vous l'appliquez.
4. Effectuez l'une des opérations suivantes :
   - Si vous avez activé la sélection multiple, cochez la case en regard de chaque filtre que vous souhaitez appliquer et cliquez sur **Soumettre**.
   - Si vous avez désactivé la sélection multiple, cliquez sur le filtre que vous souhaitez appliquer.
5. Dans le volet de droite, vous pouvez également cliquer sur **Effacer tout** ou cliquer sur pour chaque filtre que vous souhaitez supprimer.

Mise à jour de la liste des applications

Vous pouvez mettre à jour la liste des applications pour vérifier que vous disposez des informations les plus récentes sur les applicationsBlackBerry 10,iOS,Windows 10etBlackBerry Dynamicsde la liste.

Si vous disposez d'une configuration BlackBerry UEM pour prendre en charge les profils professionnels Android, vous pouvez également mettre à jour les informations relatives aux applications Android. Si vous avez ajouté des applications Android avant d'avoir configuré la prise en charge des profils professionnels Android ou que les autorisations des applications ont changé, vous devez mettre à jour les informations relatives aux applications pour qu'elles soient disponibles sur les terminaux Android dotés d'un profil professionnel. Cela s'applique également si vous apportez des modifications à votre configuration de profil professionnel Android.

Si vous n'avez pas configuré la prise en charge des profils professionnels Android ou des applications Windows Phone, les informations relatives aux applications Google Play doivent être mises à jour manuellement. Mettre à jour les informations de l'application ne signifie pas que celle-ci est mise à jour sur le terminal d'un utilisateur. Les utilisateurs reçoivent des notifications de mise à jour pour leurs applications professionnelles de la même façon qu'ils reçoivent des notifications de mise à jour pour leurs applications personnelles.

Si vous avez configuré votre compte VPN Apple pour mettre automatiquement à jour les informations des applications iOS, vous devez mettre à jour les applications de la liste.

1. Sur la barre de menus, cliquez sur **Applications**.
2. Cliquez sur.

Mettre à jour les autorisations des applications du profil professionnel Android

Si vous n'acceptez pas les autorisations d'applications au nom des utilisateurs, l'application ne peut pas être attribuée aux terminaux Android dotés d'un profil professionnel. Vous devez accepter les autorisations d'applications lorsque vous ajoutez l'application à la liste d'applications, et vous pouvez devoir les accepter à nouveau ultérieurement si elles changent.

Les applications peuvent également être non approuvées ou supprimées depuis la console Google Play mais toujours apparaitre comme disponibles dans BlackBerry UEM. Vous devez mettre à jour les informations sur les applications dans BlackBerry UEM pour synchroniser les autorisations avec Google Play.

1. Sur la barre de menus, cliquez sur **Applications**.
2. Cliquez sur .
3. Dans la liste des applications, les applications dont les autorisations ont changé sont indiquées par une icône d'avertissement et un message d'état. Les états suivants peuvent survenir après la mise à jour de la liste d'applications. Effectuez l'une des tâches suivantes pour résoudre le problème :

État	Étapes
Accepter à nouveau les autorisations des applications	Les autorisations d'application ont été modifiées dans la console Google Play. Pour pouvoir gérer l'application, vous devez réaccepter les autorisations de l'application. Pour réaccepter les autorisations, procédez comme suit : **a.** Cliquez sur **Réaccepter les autorisations de l'application**. **b.** Cliquez sur **Accepter**.
Supprimer l'application de BlackBerry UEM	L'application a été non approuvée dans la console Google Play mais n'a pas été supprimée de BlackBerry UEM. Si vous souhaitez continuer à gérer cette application sur les terminaux, vous devez approuver l'application dans la console Google Play. Si vous ne souhaitez plus gérer l'application, procédez comme suit : **a.** Cliquez sur **Supprimer l'application depuis BlackBerry UEM**. **b.** Cliquez sur **Supprimer**.
Approuver l'application dans Google Play	L'application a été non approuvée dans la console Google Play. Pour pouvoir gérer l'application, vous devez l'approuver dans la console Google Play. Pour approuver l'application, procédez comme suit : **a.** Cliquez sur **Approuver l'application dans Google Play**. **b.** Acceptez les autorisations d'application. **c.** Cliquez sur **Accepter**.
L'application a été ajoutée dans Google Play et est en train d'être ajoutée à BlackBerry UEM	Les applications qui ont été ajoutées à la console Google Play for Work, mais pas à BlackBerry UEM, sont automatiquement synchronisées avec BlackBerry UEM lorsque vous mettez à jour la liste des applications. Vous n'avez aucune action à effectuer.

4. Cliquez sur **Fermer**.

Accepter les autorisations des applications du profil professionnel Android

Vous devez accepter les autorisations d'application pour pouvoir gérer des applications sur les terminaux Android dotés d'un profil professionnel. Vous pouvez accepter des autorisations d'applications lorsque vous ajoutez l'application à BlackBerry UEM ou après la mise à jour de la liste d'applications. Si vous n'acceptez pas les autorisations d'applications dans ces cas, vous pouvez également les accepter à partir de l'écran d'informations de l'application. Les applications qui possèdent des changements d'autorisations présentent une icône d'avertissement dans la liste des applications.

Avant de commencer :

- Mettez à jour la liste d'applications.

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

2. Cliquez sur l'application pour laquelle vous voulez accepter des autorisations.
3. Cliquez sur **Accepter les autorisations des applications** pour exécuter cette action.
4. Sélectionnez **Accepter**.
5. Cliquez sur **Enregistrer**.

Gestion des applications BlackBerry Dynamics

Si votre entreprise utilise des applications BlackBerry Dynamics, vous pourriez avoir à configurer d'autres paramètres d'application. Par exemple, si votre entreprise utilise BlackBerry Work, vous configurez les paramètres pour que l'application envoie des e-mails à des terminaux plutôt que d'utiliser le profil de messagerie. Vous devez également configurer les paramètres de connectivité et autres options qui s'appliquent uniquement à des applications BlackBerry Dynamics.

Pour plus d'informations sur les fonctions et paramètres pris en charge par des applications BlackBerry Dynamics spécifiques, consultez les ressources administrateur de l'application.

Pour utiliser des applications BlackBerry Dynamics dans votre entreprise, procédez comme suit :

Étape	Action
1	Vérifiez les paramètres de connectivité BlackBerry Dynamics et modifiez-les si nécessaire.
2	Créez un profil BlackBerry Dynamics ou mettez à jour le profil BlackBerry Dynamics par défaut.
3	Ajoutez des applications BlackBerry Dynamics à BlackBerry UEM.
4	Si nécessaire, modifiez les paramètres d'application BlackBerry Dynamics.
5	Ajouter le catalogue d'applications professionnelles à BlackBerry Dynamics Launcher.
6	Attribuez le profil BlackBerry Dynamics et le profil de connectivité BlackBerry Dynamics à un groupe d'utilisateurs ou à un compte d'utilisateur.
7	Attribuez des applications BlackBerry Dynamics à des groupes d'utilisateurs ou des comptes d'utilisateur.
8	Pour les utilisateurs qui souhaitent activer des applications BlackBerry Dynamics sur des terminaux sans UEM Client, générez une clé d'accès pour les applications.

Gérer les paramètres d'une application BlackBerry Dynamics

Vous pouvez gérer les configurations d'application, les configurations de serveur et les paramètres d'application.

1. Sur la barre de menus, cliquez sur **Applications**.
2. Cliquez sur l'application BlackBerry Dynamics que vous souhaitez modifier.

3. Dans l'onglet **Paramètres > BlackBerry Dynamics**, effectuez l'une des opérations suivantes :

Tâche	Étapes
Spécifiez un profil BlackBerry Dynamics pour l'application.	Si vous souhaitez que l'application utilise un profil BlackBerry Dynamics spécifique à la place du profil BlackBerry Dynamics attribué à l'utilisateur, sélectionnez-le dans la liste déroulante **Remplacer le profil BlackBerry Dynamics**.
Spécifiez un profil de conformité pour l'application.	Si vous souhaitez que l'application utilise un profil de conformité spécifique à la place du profil attribué à l'utilisateur, sélectionnez-le dans la liste déroulante **Remplacer le profil de conformité**.
Ajoutez ou modifiez la configuration d'application pour une application interne.	**a.** En regard de **Configuration de l'application**, cliquez sur **Charger un modèle** pour ajouter un nouveau modèle de configuration d'application. **b.** Accédez à l'emplacement du modèle. **c.** Cliquez sur **Enregistrer**.
Ajouter ou modifier la configuration d'application pour une application publique	**a.** Dans le tableau **Configuration de l'application**, cliquez sur +. **b.** Saisissez le nom de la configuration d'application. **c.** Modifiez les paramètres de configuration. **d.** Cliquez sur **Enregistrer**. **e.** Si nécessaire, utilisez les flèches pour déplacer la configuration d'application vers le haut ou vers le bas afin de modifier sa priorité. Pour plus d'informations, reportez-vous à Paramètres de configuration d'application BlackBerry UEM Client. Pour plus d'informations sur les paramètres de configuration d'application BlackBerry Work, BlackBerry Notes et BlackBerry Tasks reportez-vous à Configurer les paramètres d'application BlackBerry Work et Configurer les paramètres d'application BlackBerry Notes et BlackBerry Tasks dans le contenu administratif, les notes et les tâches de BlackBerry Work.
Ajoutez ou modifiez la charge utile de la configuration de serveur afin de spécifier les clés et valeurs utilisées pour configurer les paramètres de l'application.	Si l'application dispose de stratégies personnalisées, celles-ci sont ajoutées à la zone Charge utile de la configuration du serveur. **a.** Dans la section **Charge utile de la configuration du serveur**, cliquez sur **Ajouter**. **b.** Dans la zone de texte, saisissez le code XML ou JSON de la charge utile de la configuration.
Autoriser les applications BlackBerry Dynamics à utiliser les certificats utilisateur, les profils SCEP et les profils d'informations d'identification des utilisateurs	Indiquez si l'application peut utiliser des certificats utilisateur comme option d'authentification. Pour plus d'informations sur la configuration de votre environnement à l'aide de certificats avec des applications BlackBerry Dynamics, reportez-vous à Envoi de certificats aux terminaux à l'aide de profils.

4. Cliquez sur l'onglet de la plate-forme de terminaux que vous souhaitez gérer et définissez les options appropriées.

5. Cliquez sur **Enregistrer**.

iOS et macOS : paramètres d'application BlackBerry Dynamics

La plupart des paramètres suivants sont pris en charge uniquement pour les terminaux iOS et n'apparaissent pas dans l'onglet macOS.

iOS Paramètres et macOS	Description
ID de package de l'application iOS ou macOS	Ce paramètre spécifie l'ID de package pour l'application.
Nom de l'application	Ce paramètre indique le nom de l'application qui apparaît dans la liste des applications.
Fournisseur	Ce paramètre indique le fournisseur de l'application.
Description de l'application	Ce paramètre indique la description de l'application.
Catégorie	Ce paramètre indique une catégorie pour filtrer les applications par catégorie dans la liste des applications et pour organiser les applications en catégories dans la liste des applications professionnelles sur les terminaux des utilisateurs. Vous pouvez sélectionner une catégorie ou saisir un nom pour créer une nouvelle catégorie.
Captures d'écran	Ce paramètre indique les captures d'écran pour l'application. Cliquez sur « Ajouter » pour sélectionner les images. Les formats d'image .jpg, .jpeg, .png ou .gif sont pris en charge.
Facteur de forme de terminal pris en charge	Ce paramètre indique les facteurs de forme sur lesquels l'application peut être installée. Par exemple, vous pouvez empêcher l'accès à l'application Work Apps dans iPad terminaux.
Supprimer l'application du terminal lorsque celui-ci est supprimé de BlackBerry UEM	Ce paramètre indique si l'application est supprimée du terminal lorsque celui-ci est supprimé de BlackBerry UEM. Ce paramètre s'applique uniquement aux applications dotées d'une disposition marquée comme « Requise » et si l'installation par défaut des applications requises est définie sur « Inviter une fois ».
Désactiver la sauvegarde iCloud pour l'application	Ce paramètre indique si l'application peut être sauvegardée sur le service en ligne iCloud. Cette option s'applique uniquement aux applications dotées d'une disposition marquée comme « Requise ».

iOS Paramètres et macOS	Description
Installation par défaut pour les applications requises	Ce paramètre indique si les utilisateurs sont invités à installer les applications nécessaires. Sélectionnez l'une des options suivantes : • **Inviter une fois** : les utilisateurs reçoivent une demande d'installation de l'application sur leurs terminaux iOS. Si les utilisateurs rejettent cette demande, ils peuvent installer l'application ultérieurement via l'écran Work Apps de l'application BlackBerry UEM Client ou l'icône Work Apps du terminal. • **Aucune invitation** : les utilisateurs ne reçoivent pas de demande pour installer l'application. Ce paramètre s'applique uniquement aux applications dont la mise à disposition est définie sur « Requise ». Vous définissez la mise à disposition de l'application lors de son attribution à un utilisateur ou à un groupe.
Convertir une application personnelle installée en application professionnelle	Ce paramètre indique si vous devez convertir l'application en application professionnelle si elle est déjà installée sur des terminaux iOS 9 ou versions ultérieures. Si vous sélectionnez « Convertir » après avoir attribué l'application à un utilisateur, celle-ci est convertie en application professionnelle et peut être gérée par BlackBerry UEM.
Versions limitées	Ce paramètre indique les versions de l'application que les utilisateurs ne doivent pas installer sur leurs terminaux. Si vous ajoutez plusieurs versions, utilisez la virgule comme séparateur.

Android : paramètres d'application BlackBerry Dynamics

Paramètres Android	Description
ID de package de l'application Android	Ce paramètre spécifie l'ID de package pour l'application.
Nom de l'application	Ce paramètre indique le nom de l'application qui apparaît dans la liste d'applications.
Éditeur	Ce paramètre indique le fournisseur de l'application.
Description de l'application	Ce paramètre indique la description de l'application.
Catégorie	Ce paramètre indique une catégorie pour filtrer les applications par catégorie dans la liste d'applications et pour organiser les applications en catégories dans la liste des applications professionnelles sur les terminaux des utilisateurs. Vous pouvez sélectionner une catégorie ou saisir un nom pour créer une nouvelle catégorie.
Envoyer à	Ce paramètre permet de définir si l'application est envoyée à tous les terminaux Android, uniquement aux terminaux Android dotés d'un profil professionnel ou uniquement aux terminaux Samsung KNOX Workspace.

Paramètres Android	Description
Versions limitées	Ce paramètre indique les versions de l'application que les utilisateurs ne doivent pas installer sur leurs terminaux. Si vous ajoutez plusieurs versions, utilisez la virgule comme séparateur.

Windows : paramètres d'application BlackBerry Dynamics

Paramètres Windows	Description
ID de package d'applications Windows Phone 8.1	Ce paramètre spécifie l'ID de package pour une application Windows Phone 8.1.
Nom de famille du package Windows 10 (UWP)	Ce paramètre indique le nom de famille du package pour une application Windows 10.
Nom de l'application	Ce paramètre indique le nom de l'application qui apparaît dans la liste des applications.
Fournisseur	Ce paramètre indique le fournisseur de l'application.
Description de l'application	Ce paramètre indique la description de l'application.
Catégorie	Ce paramètre indique une catégorie pour filtrer les applications par catégorie dans la liste des applications et pour organiser les applications en catégories dans la liste des applications professionnelles sur les terminaux des utilisateurs. Vous pouvez sélectionner une catégorie ou saisir un nom pour créer une nouvelle catégorie.
Captures d'écran	Ce paramètre indique les captures d'écran pour l'application. Cliquez sur « Ajouter » pour sélectionner les images. Les formats d'image .jpg, .jpeg, .png ou .gif sont pris en charge.
Supprimer l'application du terminal lorsque celui-ci est supprimé de BlackBerry UEM	Ce paramètre indique si l'application est supprimée du terminal lorsque celui-ci est supprimé de BlackBerry UEM. Ce paramètre s'applique uniquement aux applications dotées d'une disposition marquée comme « Requise » et si l'installation par défaut des applications requises est définie sur « Inviter une fois ».
Versions limitées	Ce paramètre indique les versions de l'application que les utilisateurs ne doivent pas installer sur leurs terminaux. Si vous ajoutez plusieurs versions, utilisez la virgule comme séparateur.

Paramètres de configuration d'application BlackBerry UEM Client

Option	Description
Autoriser l'utilisation de l'option de déverrouillage du contournement dans UEM Client	Si vous sélectionnez cette option, UEM Client contourne l'écran d'authentification/de verrouillage de l'utilisateur de BlackBerry Dynamics et ce dernier peut ouvrir UEM Client sans avoir à déverrouiller l'application UEM Client. Si vous avez configuré BlackBerry 2FA, l'écran d'acceptation/de refus BlackBerry 2FA s'affiche et l'utilisateur doit cliquer sur Accepter. L'utilisateur est ensuite connecté à l'application ou au service par l'intermédiaire de BlackBerry 2FA.
Nom de l'application	Saisissez un nom pour l'application. Sélectionnez cette option si vous souhaitez utiliser la solution PKI basée sur les applications de votre entreprise, comme Purebred pour inscrire des certificats pour les applications BlackBerry Dynamics. Vous pouvez installer l'application sur les terminaux et autoriser les applications BlackBerry Dynamics à utiliser les certificats inscrits par le biais de l'application PKI. Cette option est prise en charge sur les terminaux iOS seulement.
Schémas UTI	Spécifiez les schémas UTI pour la solution PKI d'application de votre entreprise. Par exemple, si vous utilisez l'application Purebred, utilisez les schémas suivants : purebred.zip.all, purebred.zip.no_filter.

Gérer les services d'application BlackBerry Dynamics

Les services d'application sont des fonctions partagées proposées par une application mobile ou par une application basée sur un serveur. À l'aide des SDK BlackBerry Dynamics, un développeur d'applications peut partager une fonction d'application pour permettre à d'autres développeurs de l'utiliser dans leurs propres applications BlackBerry Dynamics. La console de gestion vous permet d'enregistrer des services d'application de votre entreprise et de fournir la définition du service créée par le développeur. Les développeurs de votre entreprise peuvent consulter les services d'application enregistrés et utiliser les définitions de service disponibles dans les applications BlackBerry Dynamics qu'ils créent.

Les services d'application de certaines applications BlackBerry Dynamics et applications partenaires sont également disponibles, et vous pouvez consulter les définitions de service associées dans la console de gestion. Pour plus d'informations sur le développement de services d'application, rendez-vous sur BlackBerry Dynamics - Communauté de développeurs.

Avant de commencer : Si vous souhaitez enregistrer un service d'application pour votre entreprise, vérifiez que vous disposez de l'ID du service d'application, du numéro de version et de la définition du service.

1. Dans la console de gestion, cliquez sur **Paramètres > BlackBerry Dynamics** à partir de la barre de menus.
2. Cliquez sur **Services d'application**.
3. Effectuez l'une des tâches suivantes :

Tâche	Étapes
Enregistrer le service d'application de votre entreprise	**a.** Cliquez sur +. **b.** Dans la liste déroulante **Type de service**, effectuez l'une des opérations suivantes : • Si le service d'application est proposé par une application mobile, cliquez sur **Application**. • Si le service d'application est proposé par une application basée sur un serveur, cliquez sur **Serveur**. **c.** Dans le champ **ID**, saisissez l'identifiant du service de l'application. L'identifiant doit être une chaine unique (tout en minuscules) en notation DNS inversée (par exemple, com.exemple.service.impression). **d.** Saisissez le nom et la description du service d'application. **e.** Dans le champ **Version**, saisissez la version. Le numéro de version ne doit comporter que des chiffres. Si vous souhaitez ajouter un ou plusieurs sous-numéros de version (par exemple, la version de build), utilisez des points pour séparer les segments. Aucun segment ne doit commencer par 0 (par exemple, 1.1.5 est valide mais 1.1.05 ne l'est pas). **f.** Vous pouvez également saisir une description de la version. **g.** Dans le champ **Définition du service**, saisissez la définition du service au format JSON. **h.** Cliquez sur **Save**.
Modifier un service d'application	Procédez comme suit pour modifier un service d'application enregistré pour votre entreprise (par exemple, pour ajouter une nouvelle version). Vous ne pouvez pas modifier le type ou l'ID du service d'application. Vous ne pouvez pas modifier un service d'application BlackBerry Dynamics ou un service d'application partenaire. **a.** Recherchez le service d'application que vous souhaitez modifier. **b.** Cliquez sur le nom du service d'application. **c.** Si nécessaire, modifiez les détails du service d'application. Pour ajouter une nouvelle version, cliquez sur + et spécifiez le numéro de version, la description et la définition du service. **Remarque :** La suppression d'une version de service d'application n'a aucun impact sur les applications proposées ou utilisées par le service. Elle entraine simplement la suppression de la définition du service dans la console de gestion afin que les développeurs de votre entreprise ne puissent pas s'y référer. **d.** Cliquez sur **Save**.

Tâche	Étapes
Supprimer un service d'application	Vous ne pouvez pas supprimer un service d'application BlackBerry Dynamics ou un service d'application partenaire. La suppression d'un service d'application dans la console de gestion n'a aucun impact sur les applications proposées ou utilisées par le service. Elle entraine simplement la suppression de la définition du service dans la console de gestion afin que les développeurs de votre entreprise ne puissent pas s'y référer. **a.** Recherchez le service d'application que vous souhaitez supprimer. **b.** Cliquez sur ✕ en regard du service. **c.** Cliquez sur **Supprimer**.

À la fin : Vous pouvez également lier une version de service d'application à une application gérée pour que la console de gestion indique que l'application fournit le service. Pour plus d'informations, reportez-vous à Gérer les paramètres d'une application BlackBerry Dynamics.

Configuration de Kerberos pour les applications BlackBerry Dynamics

Les applications BlackBerry Dynamics prennent en charge à la fois la délégation Kerberos contrainte et Kerberos PKINIT. La délégation Kerberos contrainte (KCD, Constrained Delegation) et Kerberos PKINIT sont des implémentations distinctes de Kerberos. Vous pouvez prendre en charge l'un ou l'autre pour les applications BlackBerry Dynamics, mais pas les deux.

La délégation Kerberos contrainte utilise une relation de confiance déjà établie entre BlackBerry UEM et le Centre de distribution de clés (KDC) Windows. BlackBerry UEM communique avec le KDC pour le compte de l'application. La délégation Kerberos contrainte prévaut sur Kerberos PKINIT, même si l'utilisateur a un certificat valide. Pour des informations d'ordre général sur le fonctionnement de la délégation Kerberos contrainte avec les applications BlackBerry Dynamics, voir Délégation Kerberos contrainte avec Good Control.

L'authentification Kerberos PKINIT établit la confiance directement entre l'application BlackBerry Dynamics et Windows KDC. L'authentification de l'utilisateur est basée sur les certificats délivrés par les services de certificats Microsoft Active Directory. Pour pouvoir utiliser PKINIT, la délégation Kerberos contrainte ne doit pas être activée dans les paramètres d'application dans BlackBerry UEM.

Configuration de la délégation Kerberos contrainte

La délégation Kerberos contrainte permet aux utilisateurs d'accéder aux ressources de l'entreprise sans avoir à entrer leurs informations d'identification réseau. La délégation Kerberos contrainte utilise des tickets de service qui sont chiffrés et déchiffrés par des clés ne contenant pas les informations d'identification de l'utilisateur.

Lorsque la délégation Kerberos contrainte est configurée, l'application délègue l'authentification à BlackBerry UEM qui demandera l'accès à une ressource de l'entreprise en son nom.

Pour configurer la délégation Kerberos contrainte, procédez comme suit :

- Activez l'authentification Kerberos (sous Authentification Windows) pour le serveur Web Microsoft Exchange Web Services dans Microsoft Internet Information Services (IIS).
- Dans Microsoft Management Console (MMC) « Utilisateurs et ordinateurs Active Directory », onglet Délégation, ajoutez le service HTTP du serveur Web Microsoft Exchange Web Services pour le compte admin Good.
- Si la délégation Kerberos contrainte est activée, les utilisateurs ne peuvent pas entrer leurs identifiants (utilisateur et mot de passe). L'authentification est déléguée à BlackBerry UEM.

Pour activer la délégation Kerberos contrainte pour une application BlackBerry Dynamics, sélectionnez le paramètre **Autoriser l'utilisation de la délégation Kerberos contrainte** dans les paramètres de configuration de l'application. Pour obtenir des instructions détaillées, reportez-vous au contenu d'administration de l'application.

Configuration de Kerberos PKINIT

BlackBerry UEM prend en charge Kerberos PKINIT pour l'authentification de l'utilisateur BlackBerry Dynamics à l'aide de certificats PKI.

Si vous souhaitez utiliser Kerberos PKINIT pour les applications BlackBerry Dynamics, votre organisation doit remplir les conditions suivantes :

Points clés

- La délégation Kerberos contrainte ne doit pas être activée.
- L'hôte KDC doit être ajouté à la liste des domaines autorisés dans le Profil de connectivité BlackBerry Dynamics.
- L'hôte KDC doit être à l'écoute sur le port TCP 88 (port Kerberos par défaut).
- BlackBerry Dynamics ne prend pas en charge le KDC sur UDP.
- Le KDC doit avoir un enregistrement A (IPv4) ou AAAA (IPv6) dans votre DNS.
- BlackBerry Dynamics n'utilise pas de fichiers de configuration Kerberos (comme `krb5.conf`) pour localiser le KDC approprié.
- Le KDC peut référer le client à un autre hôte KDC. BlackBerry Dynamics suivra l'instruction si l'hôte KDC auquel il est renvoyé a été ajouté à la liste des domaines autorisés dans le Profil de connectivité BlackBerry Dynamics.
- Le KDC peut obtenir le TGT de façon transparente pour BlackBerry Dynamics à partir d'un autre hôte KDC.

Certificats de serveur

- Les certificats de serveur Windows KDC émis via les services de certificats Active Directory doivent provenir exclusivement des versions suivantes de Windows Server. Aucune autre version n'est prise en charge.
  - Internet Information Server avec Windows Server 2008 R2
  - Internet Information Server avec Windows Server 2012 R2
- Des certificats de service KDC valides doivent se trouver soit dans le magasin de certificats BlackBerry Dynamics, soit dans le magasin de certificats du terminal.

Certificats client

- La longueur de clé minimale pour les certificats doit être de 2 048 octets.
- Les certificats clients doivent inclure le nom principal de l'utilisateur (par exemple, user@domain.com) dans Autre nom de l'objet pour l'ID d'objet szOID_NT_PRINCIPAL_NAME 1.3.6.1.4.1.311.20.2.3, comme défini par Microsoft dans l'article https://support.microsoft.com/en-us/kb/287547.
- Le domaine du Nom principal de l'utilisateur doit correspondre au nom de domaine du service KDC Windows.
- La propriété Utilisation de clé étendue du certificat doit avoir la valeur Ouverture de session par carte à puce Microsoft (1.3.6.1.4.1.311.20.2.2).
- Les certificats doivent être valides. Vérifiez leur validité par rapport aux serveurs listés ci-dessus.

Ajouter le catalogue d'applications professionnelles à BlackBerry Dynamics Launcher

Pour les terminaux activés pour BlackBerry Dynamics, vous pouvez ajouter le catalogue d'applications professionnelles à BlackBerry Dynamics Launcher pour permettre aux utilisateurs d'accéder rapidement à la liste des applications professionnelles qui leur ont été attribuées.

1. Sur la barre de menus, cliquez sur **Groupes**.
2. Sélectionnez le groupe **Tous les utilisateurs**.

3. Dans la section **Configuration VPN**, cliquez sur +.
4. Dans le champ de recherche, recherchez **Fonctionnalité - BlackBerry App Store**.
5. Sélectionnez **Fonctionnalité - BlackBerry App Store**.
6. Dans la liste déroulante **Disposition** de l'application, sélectionnez **Obligatoire**.
7. Cliquez sur **Attribuer**.

Générer des clés d'accès pour les applications BlackBerry Dynamics

Les applications BlackBerry Dynamics nécessitent une clé d'accès qui doit être activée sur un terminal. Une clé d'accès BlackBerry UEM Client peut être nécessaire après l'installation d'une application par les utilisateurs de BlackBerry UEM. Vous ou un utilisateur devez générer manuellement des clés d'accès et les envoyer pour activer les applications BlackBerry Dynamics dans les situations suivantes :

- Pour les terminaux Samsung KNOX Workspace
- Pour les terminaux iOS et Android qui n'ont pas besoin de MDM et sur lesquels UEM Client n'est pas installé
- Pour les utilisateurs qui souhaitent activer des applications BlackBerry Dynamics sur des terminaux qui ne requièrent pas BlackBerry UEM Client.

Vous pouvez générer des clés d'accès lorsque vous créez un nouvel utilisateur ou ultérieurement. Les utilisateurs n'ont pas besoin d'activer leurs terminaux dans BlackBerry UEM pour recevoir les clés d'accès. Les utilisateurs peuvent également générer des clés d'accès dans BlackBerry UEM Self-Service.

1. Sur la barre de menus, cliquez sur **Utilisateurs > Terminaux gérés**.
2. Recherchez un compte d'utilisateur.
3. Dans les résultats de la recherche, cliquez sur le nom du compte d'utilisateur.
4. Cliquez sur **Définir le mot de passe d'activation**.
5. Dans la liste déroulante **Option d'activation**, sélectionnez **Génération d'une clé d'accès BlackBerry Dynamics**.
6. Dans la liste déroulante **Nombre de clés d'accès à générer**, sélectionnez le nombre de clés d'accès que vous souhaitez créer pour l'utilisateur.
7. Sélectionnez le nombre de jours de validité de la clé d'accès.
8. Dans la liste déroulante **Modèle d'e-mail**, sélectionnez le modèle d'e-mail que vous souhaitez utiliser. Pour plus d'informations, reportez-vous à Modèles d'e-mail.
9. Cliquez sur **Envoyer**.

Gérer les clés d'accès BlackBerry Dynamics

Une fois les clés d'accès BlackBerry Dynamics générées, leur nombre est répertorié dans la section Détails d'activation de l'écran Résumé utilisateur.

Avant de commencer : Générer des clés d'accès pour les applications BlackBerry Dynamics.

1. Sur la barre de menus, cliquez sur **Utilisateurs > Terminaux gérés**.
2. Recherchez un compte d'utilisateur.
3. Dans les résultats de la recherche, cliquez sur le nom du compte d'utilisateur.
4. Dans la section **Détails d'activation**, sous **Clés d'accès BlackBerry Dynamics**, cliquez sur le lien permettant d'afficher le nombre de clés générées. Si vous ne voyez pas cette section, cela signifie qu'aucune clé d'accès n'a été générée pour l'utilisateur.
5. Dans la boite de dialogue **Clés d'accès BlackBerry Dynamics**, effectuez l'une des opérations suivantes :

Option	
	Renvoyer la clé d'accès à l'utilisateur.

Option	
	Supprimer la clé d'accès.

6. Cliquez sur **Enregistrer**.

Envoyer une clé de déverrouillage d'application BlackBerry Dynamics à un utilisateur

Vous pouvez envoyer des clés de déverrouillage d'application à un utilisateur si l'une de ses applications BlackBerry Dynamics s'est verrouillée.

1. Sur la barre de menus, cliquez sur **Utilisateurs**.
2. Recherchez un compte d'utilisateur.
3. Dans les résultats de la recherche, cliquez sur le nom du compte d'utilisateur.
4. Cliquez sur le terminal de l'utilisateur.
5. Dans la section BlackBerry Dynamics de la ligne **Actions des applications**, sélectionnez « Déverrouiller l'application » pour l'application pour laquelle vous souhaitez envoyer un e-mail à l'utilisateur.
6. Sur la page **Déverrouiller l'application**, dans le champ **Modèle d'e-mail**, sélectionnez l'e-mail de clé de déverrouillage BlackBerry Dynamics.
7. Cliquez sur **Envoyer**.

À la fin :

Vous pouvez modifier le modèle d'e-mail qui est envoyé à l'utilisateur.

Gestion des applications protégées par Microsoft Intune

Microsoft Intune est un service EMM Cloud qui fournit les deux fonctionnalités MDM et MAM. Intune MAM offre des fonctionnalités de sécurité pour les applications, notamment les applications Office 365, afin de protéger les données contenues dans les applications. Par exemple, Intune peut exiger que les données des applications soient chiffrées et empêcher la copie et le collage, l'impression et l'utilisation de la commande Enregistrer sous.

Pour les terminaux iOS et Android, si vous souhaitez utiliser les stratégies de protection des applications Intune pour protéger les données des applications Office 365, vous pouvez le faire lors de l'utilisation de BlackBerry UEM pour la gestion des terminaux. Vous pouvez connecter UEM à Intune pour configurer des stratégies de protection des applications Intune depuis la console de gestion UEM.

Pour déployer des applications protégées par Intune, vous devez d'abord configurer la connexion entre UEM et Intune. Pour plus d'informations, reportez-vous à la section Connexion de BlackBerry UEM à Microsoft Azuredans le contenu relatif à la configuration.

Intune utilise des stratégies de protection des applications pour protéger les applications. Pour protéger les applications depuis la console de gestion UEM, vous pouvez créer un profil de protection d'application Intune. Lorsque vous créez ou mettez à jour un profil de protection d'application UEM, les paramètres sont envoyés à Intune et les paramètres de la stratégie de protection d'application correspondante sont mis à jour.

Remarque : Si vous mettez à jour la stratégie de protection d'application dans Intune, les changements ne sont pas synchronisés avec BlackBerry UEM. Une fois que vous avez créé un profil de protection d'application dans UEM, ne mettez pas à jour la stratégie correspondante depuis Intune.

Créer un profil de protection d'application Microsoft Intune

Lorsque vous créez ou mettez à jour un profil de protection d'application Microsoft Intune dans BlackBerry UEM, les paramètres de profil sont envoyés à Intune pour mettre à jour la stratégie de protection d'application

correspondante. Les profils de protection d'application Microsoft Intune peuvent seulement être affectés à des groupes liés par annuaire.

Avant de commencer :

- Configurez la connexion entre BlackBerry UEM et Microsoft Intune. Le profil de protection d'application Microsoft Intune ne s'affiche pas sur la page Stratégies et profils si la connexion n'est pas configurée.
- Pour les terminaux Android, assurez-vous que l'application Microsoft Company Portal est installée sur les terminaux. Pour plus d'informations, reportez-vous à https://docs.microsoft.com/intune/app-protection-enabled-apps-android.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Protection > Profil de protection de l'application Microsoft Intune**.
3. Cliquez sur +.
4. Saisissez le nom et la description du profil.
5. Configurez les valeurs qui conviennent pour chaque type de terminal.
6. Cliquez sur **Ajouter**.

À la fin : Attribuez le profil de protection d'application Intune à un groupe lié par annuaire.

Concepts connexes

Paramètres du profil de protection des applications Microsoft Intune

Tâches connexes

Attribuer un profil ou une stratégie informatique à un groupe d'utilisateurs

Nettoyage des applications gérées par Microsoft Intune

Vous pouvez utiliser la commande Nettoyage des applications pour supprimer les données provenant d'applications qui sont gérées par Intune sur les terminaux iOS et Android. Les applications ne sont pas désinstallées lorsque la commande est envoyée.

1. Sur la barre de menus, cliquez sur **Utilisateurs**.
2. Recherchez l'utilisateur dont vous souhaitez nettoyer les données, puis sélectionnez-le en cliquant dessus.
3. Cliquez sur l'onglet **<*modèle du terminal*> (Intune)**.
4. Cliquez sur **Nettoyage des applications**.

Gestion des comptes VPP Apple

Le Programme d'achat en volume (Volume Purchase Program - VPP) d'Apple vous permet d'acheter, de distribuer et de mettre à jour des applications iOS installées en bloc. Vous pouvez associer des comptes Apple VPP à un domaine BlackBerry UEM afin de pouvoir distribuer les licences achetées pour les applications iOS associées aux comptes VPP.

Ajouter un compte VPP Apple

1. Sur la barre de menus, cliquez sur **Applications > Licences d'applications iOS**.
2. Cliquez sur **Ajouter un compte d'achat en volume Apple**.

3. Saisissez le nom et les informations du titulaire du compte VPP.
4. Dans le champ **Jeton de service d'achat en volume**, copiez et collez le code 64 bits à partir du fichier de jeton .vpp. Il s'agit du fichier que le détenteur du compte VPP depuis la boutique VPP.
5. Cliquez sur **Suivant**.
6. Sélectionnez les applications que vous souhaitez ajouter à la liste des applications. Si une application a déjà été ajoutée à la liste d'applications, vous ne pouvez pas la sélectionner.
7. Si vous souhaitez que les applications soient automatiquement mises à jour lorsqu'une nouvelle version est disponible sur BlackBerry UEM, sélectionnez **Mettre à jour l'application automatiquement lorsqu'une nouvelle version est disponible**. Ce paramètre s'applique à toutes les applications VPP pour ce compte VPP. Vous pouvez modifier ce paramètre ultérieurement.
8. Si vous souhaitez supprimer des applications des terminaux lors de leur suppression de BlackBerry UEM, sélectionnez **Supprimer l'application du terminal lorsque le terminal est supprimé du système**.
9. Pour empêcher la sauvegarde des applications des terminaux iOS sur le service en ligne iCloud, sélectionnez **Désactiver la sauvegarde iCloud pour l'application**. Cette option s'applique uniquement aux applications dotées d'une disposition marquée comme requise. Vous pouvez définir la disposition de l'application lorsque vous attribuez l'application à un utilisateur ou à un groupe.
10. Dans la liste déroulante **Méthode d'installation par défaut**, effectuez l'une des opérations suivantes :
    - Si vous souhaitez que les utilisateurs reçoivent une demande d'installation des applications sur leurs terminaux iOS, sélectionnez **Inviter une fois**. Si les utilisateurs ignorent l'invite, ils peuvent installer les applications ultérieurement à partir de la liste Applications professionnelles de l'application BlackBerry UEM Client ou à l'aide de l'icône Applications professionnelles du terminal.
    - Sélectionnez **Aucune invite**. Les utilisateurs ne sont pas notifiés. Ils peuvent installer les applications à partir de la liste Applications professionnelles de l'application BlackBerry UEM Client ou à l'aide de l'icône Applications professionnelles du terminal.
11. Cliquez sur **Ajouter**.

Tâches connexes

Attribuer une application à un groupe d'utilisateurs
Attribuer une application à un compte d'utilisateur

Modifier un compte VPP Apple

1. Sur la barre de menus, cliquez sur **Applications > Licences d'applications iOS**.
2. Cliquez sur  .
3. Modifiez l'un des paramètres d'informations de compte VPP suivants :
    - Nom du compte d'achat en volume
    - Informations sur le titulaire du compte d'achat en volume
    - Jeton de service d'achat en volume
    - Mettre à jour l'application automatiquement lorsqu'une nouvelle version est disponible.
4. Cliquez sur **Enregistrer**.

Mettre à jour les informations de compte VPP Apple

Lorsque la page Licences des applications est ouverte, les informations de licence les plus actuelles sont automatiquement synchronisées à partir des serveurs VPP Apple. Si nécessaire, vous pouvez aussi mettre à jour manuellement les informations de licence que vous avez ajoutées à BlackBerry UEM.

1. Sur la barre de menus, cliquez sur **Applications**.
2. Cliquez sur **Licences d'applications iOS**.
3. Cliquez sur ⟳.

Supprimer un compte VPP Apple

Avant de commencer : Supprimez les applications dotées de licences associées des utilisateurs avant de supprimer le compte VPP.

1. Sur la barre de menus, cliquez sur **Applications**.
2. Cliquez sur **Licences d'applications iOS**.
3. Cliquez sur 🗑.
4. Cliquez sur **Supprimer**.

Attribution de licences VPP Apple aux terminaux

Vous pouvez attribuer des licences VPP (Volume Purchase Program) Apple aux terminaux exécutant iOS version 9 ou ultérieure. L'attribution de licences VPP à des terminaux plutôt qu'à des utilisateurs simplifie le processus pour les utilisateurs, car ils n'ont plus besoin d'un identifiant Apple pour installer des applications. En outre, les applications n'apparaissent pas dans l'historique d'achat et les installations d'applications des utilisateurs. Lorsque vous modifiez le type d'attribution existant pour une application afin de remplacer « Utilisateur attribué » par « Terminal attribué », l'utilisateur doit réinstaller l'application avant que la nouvelle attribution soit appliquée et affichée dans la console de gestion BlackBerry UEM.

L'attribution de licences VPP à des terminaux n'est prise en charge que sur les terminaux iOS qui sont activés avec Contrôles MDM.

Vous pouvez attribuer des licences VPP à des terminaux lorsque des applications sont ajoutées à l'un des groupes ou comptes suivants :

- Comptes d'utilisateur
- Groupes d'applications
- Groupes d'utilisateurs

L'attribution de licences VPP à des groupes de terminaux n'est pas prise en charge.

Pour plus d'informations, reportez-vous à Gestion des comptes VPP Apple .

Afficher une attribution de licence VPP Apple

Vous pouvez afficher l'état de l'attribution de licence VPP Apple dans votre domaine.

1. Sur la barre de menus, cliquez sur **Applications** > **Licences d'applications iOS**.
2. Si vous possédez plusieurs comptes VPP Apple, cliquez sur celui pour lequel vous souhaitez afficher l'attribution de licence VPP.

   Pour chaque application iOS du domaine, vous pouvez afficher les informations de licence VPP suivantes :

   - Le nombre de licences VPP disponibles
   - Le nombre de licences VPP utilisées
3. Dans la colonne **Licences utilisées** correspondant à l'application, cliquez sur le lien Licences utilisées.

   Pour l'application spécifiée, vous pouvez afficher les informations d'attribution de licence d'application suivantes :

   - Les noms d'utilisateur pour lesquels l'application possède une licence
   - Si la licence d'application est attribuée à un compte d'utilisateur ou à un terminal

- Si une licence VPP est utilisée ou non
- Si l'application est installée ou non

4. Cliquez sur **Fermer**.

Classer l'installation des applications

Vous pouvez classer les applications afin de contrôler l'ordre dans lequel elles seront installées lors de leur attribution à des terminaux. En définissant ce classement, vous vous assurez que toutes les applications de délégation de l'authentification sont d'abord transmises au terminal. Le classement s'applique uniquement aux applications iOS.

1. Sur la barre de menus, cliquez sur **Applications > Classement de l'installation de l'application**.
2. Cliquez sur .
3. Cliquez sur .
4. Cochez la case en regard des applications que vous souhaitez classer.
5. Cliquez sur **Ajouter**.
6. Sur la page Classement de l'installation de l'application, cliquez sur dans la colonne **Classer** pour classer les applications dans l'ordre dans lequel vous souhaitez qu'elles soient installées sur les terminaux.
7. Cliquez sur **Enregistrer**.

Modifier la liste du classement d'installation des applications

Vous pouvez modifier l'ordre d'installation des applications qui seront installées sur les terminaux de votre organisation. Le classement s'applique uniquement aux applications iOS.

1. Sur la barre de menus, cliquez sur **Applications > Classement de l'installation de l'application**.
2. Cliquez sur .
3. Cliquez sur dans la colonne **Classer** pour classer les applications dans l'ordre dans lequel vous souhaitez qu'elles soient installées sur les terminaux.
4. Cliquez sur **Enregistrer**.

Supprimer une application de la liste du classement d'installation des applications

Vous pouvez supprimer une application de la liste du classement d'installation des applications. Le classement s'applique uniquement aux applications iOS.

1. Sur la barre de menus, cliquez sur **Applications > Classement de l'installation de l'application**.
2. Cliquez sur .
3. Dans la liste, cliquez sur en regard de l'application que vous souhaitez supprimer.
4. Cliquez sur **Supprimer**.
5. Cliquez sur **Enregistrer**.

Afficher des listes d'applications personnelles

Par défaut, BlackBerry UEM reçoit une liste des applications personnelles qui sont installées sur les terminaux activés par un type d'activation pris en charge.

Dans la console de gestion BlackBerry UEM vous pouvez afficher la liste des applications sur la page Détails de l'appareil pour un compte d'utilisateur spécifique, ou sur la page applications personnelles pour tous les comptes utilisateur. Reportez-vous à la section Afficher la liste des applications personnelles dans la console de gestion.

Remarque : Vous pouvez également afficher les applications qui ont été installées sur les terminaux avant qu'ils ne soient activés en tant que terminaux KNOX Workspace uniquement.

L'affichage de la liste des applications personnelles n'est pas pris en charge sur les terminaux activés à l'aide des types d'activation suivants :

- iOS et Android : Confidentialité de l'utilisateur
- Android : Travail et Personnel - Confidentialité de l'utilisateur
- Samsung KNOX : Travail et Personnel - Confidentialité de l'utilisateur - (Samsung KNOX)
- BlackBerry 10 : Travail et Personnel - Entreprise
- iOS et Android : inscription du terminal pour BlackBerry 2FA uniquement

Pour désactiver l'ensemble des applications personnelles associées à tous les types d'activation, vous devez désélectionner l'option Autoriser la collection d'applications personnelles du profil d'agent de gestion d'entreprise. Pour plus d'informations, reportez-vous à Désactiver la liste d'applications personnelles.

Afficher la liste des applications personnelles dans la console de gestion

Vous pouvez afficher les informations suivantes sur les applications installées dans l'espace Personnel de l'utilisateur :

- Nom de l'application
- Version de l'application
- Système d'exploitation pris en charge par l'application
- Nombre de comptes d'utilisateur sur lesquels l'application est installée

Avant de commencer : Créez un profil d'activation avec un type d'activation prenant en charge la réception par BlackBerry UEM d'une liste d'applications installées dans l'espace Personnel de l'utilisateur et attribuez-le à des utilisateurs ou à des groupes.

1. Sur la barre de menus, cliquez sur **Applications > Applications personnelles**.
2. Dans la colonne **Nom de l'application**, cliquez sur le nom de l'application.

   Vous pouvez afficher les détails de l'application spécifiée dans la boutique d'applications publique, le cas échéant.
3. Dans la colonne **Nombre installé** de l'application, cliquez sur le nombre installé.

   Pour l'application spécifiée, vous pouvez afficher le compte d'utilisateur et le terminal où l'application est installée.

Désactiver la liste d'applications personnelles

Par défaut, BlackBerry UEM reçoit une liste des applications qui sont installées sur les périphériques activés à l'aide d'une prise en charge type d'activation. Vous pouvez désactiver la liste d'applications personnelles pour tous les types d'activation.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Développez **Enterprise Management Agent**.
3. Cliquez sur le nom du profil que vous souhaitez modifier.
4. Cliquez sur  .
5. Décochez la case **Autoriser la collection d'applications personnelles** pour chaque type de terminal.
6. Cliquez sur **Enregistrer**.

Évaluation et commentaires sur les applications

Vous pouvez déterminer si les utilisateurs de votre entreprise sont autorisés à évaluer et à déposer des commentaires sur les applications iOS, Android et Windows 10 ainsi qu'à consulter les avis déposés par d'autres utilisateurs sur les applications personnalisées internes ou sur les applications téléchargées à partir de boutiques d'applications publiques. Ces évaluations et commentaires ne sont pas accessibles aux utilisateurs extérieurs à votre environnement. Les commentaires ne doivent pas dépasser 1 000 caractères.

Les utilisateurs peuvent évaluer une application sans rédiger de commentaire, mais ils doivent évaluer l'application pour déposer un commentaire. Les évaluations et commentaires déposés par les utilisateurs sont enregistrés et affichés dans la console BlackBerry UEM quasiment en temps réel. Vous pouvez voir l'évaluation moyenne d'une application, le nombre de commentaires déposés, et lire les avis individuels. Vous pouvez aussi supprimer des évaluations et commentaires.

Lorsque vous ajoutez plusieurs versions d'une application personnalisée à BlackBerry UEM et activez les évaluations et commentaires pour une version de l'application, le paramètre spécifié s'applique à toutes les versions de l'application personnalisée. Le nombre moyen d'évaluations et de commentaires ainsi que les évaluations et commentaires déposés pour différentes versions de l'application personnalisée sont identiques pour chaque version.

Par défaut, les nouvelles applications ajoutées à la liste des applications de la console de gestion BlackBerry UEM autorisent les utilisateurs à évaluer l'application, à déposer des commentaires et à consulter les avis d'autres utilisateurs de votre entreprise. Par défaut, les évaluations et commentaires sont désactivés pour des applications existantes, mais si besoin, vous pouvez activer cette fonctionnalité. Lorsque les évaluations et commentaires sont activés pour une application, l'autorisation s'applique à toutes les versions de l'application ajoutées à BlackBerry UEM.

Les évaluations et les commentaires sur les applications ne sont pas pris en charge sur les terminaux suivants :

- BlackBerry
- Windows 8.x
- BlackBerry Dynamics activé(e)
- Terminaux Android dotés d'un profil professionnel
- BlackBerry Enterprise Identity

Pour plus d'informations sur BlackBerry Enterprise Identity, reportez-vous au contenu relatif à BlackBerry Enterprise Identity.

Activer ou désactiver les notes et évaluations pour toutes les applications

Vous pouvez activer ou désactiver les notes et évaluations des applications pour toutes les applications que vous avez ajoutées à BlackBerry UEM et configurer le niveau d'interaction qu'un utilisateur peut avoir avec les notes et évaluations.

Remarque : Les paramètres des notes et évaluations des applications s'appliquent uniquement aux applications que vous ajoutez après avoir enregistré les paramètres.

1. Dans la barre de menus, cliquez sur **Paramètres > Gestion des applications**.
2. Cliquez sur **Notes et évaluations**.
3. Pour activer les notes et évaluations des applications, sélectionnez **Activer les notes et évaluations des applications**.
    - Si vous souhaitez que les utilisateurs puissent évaluer l'application, déposer des commentaires et consulter les avis d'autres utilisateurs de votre environnement, sélectionnez **Mode public**.

- Si vous souhaitez uniquement autoriser les utilisateurs à évaluer et déposer des commentaires sur l'application, sélectionnez **Mode privé**. Les utilisateurs n'auront pas accès aux avis des autres utilisateurs. Ces avis seront disponibles dans la console de gestion BlackBerry UEM.
- Si vous ne souhaitez pas que les utilisateurs puissent évaluer les applications, déposer des commentaires ou consulter les avis d'autres utilisateurs, sélectionnez **Désactivé**.

4. Pour désactiver les notes et évaluations des applications, décochez la case **Activer les notes et évaluations des applications**.
5. Cliquez sur **Enregistrer**.

Activer les évaluations et commentaires sur les applications existantes

Lorsque vous déterminez si les utilisateurs peuvent évaluer une application, déposer des commentaires et consulter les avis d'autres utilisateurs, l'autorisation spécifiée s'applique à toutes les versions de l'application.

1. Sur la barre de menus, cliquez sur **Applications**.
2. Cliquez sur une application.
3. Accédez à l'onglet **Paramètres** et choisissez l'une des actions suivantes dans la liste déroulante **Évaluation et commentaires sur l'application** :
   - Si vous souhaitez que les utilisateurs puissent évaluer l'application, déposer des commentaires et consulter les avis d'autres utilisateurs de votre environnement, sélectionnez **Mode public**.
   - Si vous souhaitez uniquement autoriser les utilisateurs à évaluer et déposer des commentaires sur l'application, sélectionnez **Mode privé**. Les utilisateurs n'auront pas accès aux avis des autres utilisateurs. Ces avis seront disponibles dans la console de gestion BlackBerry UEM.
   - Si vous ne souhaitez pas que les utilisateurs puissent évaluer les applications, déposer des commentaires ou consulter les avis d'autres utilisateurs, sélectionnez **Désactivé**.
4. Cliquez sur **Enregistrer**.

Consulter les commentaires relatifs à une application dans la console de gestion

Vous pouvez consulter l'évaluation moyenne globale ainsi que les évaluations et commentaires individuels déposés par les utilisateurs d'une application.

1. Dans le menu, cliquez sur **Applications**.
2. Vous pouvez également cliquer sur la colonne **Évaluation de l'application** pour classer les applications pour lesquelles les évaluations et commentaires sont activés.

   Les applications pour lesquelles les évaluations et commentaires sont activés apparaissent dans l'ordre suivant :

   a. Applications avec évaluations et commentaires
   b. Applications sans évaluations et commentaires
   c. Évaluation des applications désactivée
   d. Applications ne prenant pas en charge les évaluations et commentaires
3. Cliquez sur une application.
4. Cliquez sur l'onglet **<*nombre de commentaires*> commentaires**.

Spécifier les paramètres relatifs à l'évaluation et au dépôt de commentaires pour plusieurs applications

Lorsque vous déterminez si les utilisateurs peuvent évaluer une application, déposer des commentaires et consulter les avis d'autres utilisateurs, l'autorisation spécifiée s'applique à toutes les versions de l'application.

1. Dans le menu, cliquez sur **Applications**.
2. Effectuez l'une des opérations suivantes :

- Cochez la case située en haut de la liste pour sélectionner toutes les applications.
- Cochez la case de chacune des applications que les utilisateurs pourront évaluer ou commenter.

3. Cliquez sur .
4. Sélectionnez l'une des autorisations suivantes :
   - Si vous souhaitez que les utilisateurs puissent évaluer l'application, déposer un commentaire et consulter les avis d'autres utilisateurs de votre environnement, sélectionnez **Mode public**.
   - Si vous souhaitez uniquement autoriser les utilisateurs à évaluer et déposer des commentaires sur l'application, sélectionnez **Mode privé**. Les utilisateurs n'auront pas accès aux avis des autres utilisateurs. Ces avis seront disponibles dans la console de gestion BlackBerry UEM.
   - Si vous ne souhaitez pas que les utilisateurs puissent évaluer les applications, déposer des commentaires ou consulter les avis d'autres utilisateurs, sélectionnez **Désactivé**.
5. Cliquez sur **Enregistrer**.

Supprimer les évaluations et commentaires relatifs aux applications

Vous pouvez supprimer les évaluations et commentaires relatifs à une application.

1. Dans le menu, cliquez sur **Applications**.
2. Vous pouvez également cliquer sur la colonne **Évaluation de l'application** pour classer les applications pour lesquelles les évaluations et commentaires sont activés.
3. Cliquez sur une application pour laquelle les évaluations et commentaires sont activés.
4. Dans l'écran **Détails de l'application**, cliquez sur l'onglet **<*nombre de commentaires*> commentaires**.
5. Cliquez sur **Sélectionner tout** ou cochez la case de chacun des commentaires que vous souhaitez supprimer.
6. Cliquez sur .
7. Cliquez sur **Supprimer**.
8. Cliquez sur **Enregistrer**.

Gérer l'icône Applications professionnelles pour les terminaux iOS

Lorsque les utilisateurs activent les terminaux iOS avec les types d'activation Contrôles MDM ou Travail et Personnel - Contrôle total, une icône Applications professionnelles s'affiche sur le terminal. Les utilisateurs peuvent toucher l'icône pour voir les applications professionnelles qui leur ont été confiées, et ils peuvent installer ou mettre à jour les applications selon le besoin.

Vous pouvez personnaliser l'apparence de l'icône Applications professionnelles en sélectionnant une image et un nom pour l'icône. Le nom par défaut de l'icône Applications professionnelles est Applications professionnelles et l'icône par défaut affiche le logo BlackBerry.

Personnaliser l'icône Applications professionnelles

Lorsque vous personnalisez l'icône Applications professionnelles, l'icône est mise à jour sur tous les terminaux iOS activés.

Remarque : Cette fonction n'est pas prise en charge sur les terminaux activés en mode Confidentialité de l'utilisateur.

Avant de commencer : vérifiez que l'image que vous prévoyez d'utiliser pour l'icône Applications professionnelles répond aux exigences suivantes :

- Format d'image de type .png, .jpg ou .jpeg.

- Évitez d'utiliser des images .png présentant des éléments transparents. Les éléments transparents s'affichent en noir sur le terminal.
- Pour connaitre les tailles suggérées des images, rendez-vous sur developer.apple.com. et consultez la rubrique Tailles des icônes et des images.

1. Sur la barre de menus, cliquez sur **Paramètres**.
2. Dans le volet de gauche, développez **Gestion des applications**.
3. Cliquez sur **Application Work Apps pour iOS**.
4. Dans le champ **Nom**, saisissez le nom de l'icône personnalisée. Le nom s'affiche sur le terminal juste sous l'icône.
5. Cliquez sur **Parcourir**. Localisez et sélectionnez une image pour l'icône Applications professionnelles. Les formats d'image pris en charge sont les suivants : .png, .jpg ou .jpeg.
6. Sélectionnez **Afficher l'application Work Apps en plein écran** afin de permettre aux utilisateurs d'accéder à l'icône Applications professionnelles pour passer du mode standard au mode plein écran.
7. Cliquez sur **Enregistrer**.

Désactiver l'application Applications professionnelles pour iOS

Si les utilisateurs accèdent à leur catalogue d'applications professionnelles à partir de BlackBerry Dynamics Launcher, vous pouvez désactiver l'application Applications professionnelles.

1. Sur la barre de menus, cliquez sur **Paramètres**.
2. Dans le volet de gauche, développez **Gestion des applications**.
3. Cliquez sur **Applications professionnelles pour iOS**.
4. Cliquez sur **Désactiver l'application Applications professionnelles**.

Gestion des notifications des applications sur les terminaux iOS supervisés

Vous pouvez utiliser un profil de notification par application pour configurer les paramètres de notification des applications système et des applications que vous gérez à l'aide de BlackBerry UEM. Les profils de notification par application sont pris en charge pour les terminaux iOS supervisés exécutant iOS 9.3 ou version ultérieure.

Remarque : Vous devez attribuer un profil de notification par application aux comptes d'utilisateur après que les applications touchées ont déjà été installées sur les terminaux des utilisateurs. Si le profil est appliqué avant que les applications touchées soient installées, les utilisateurs ne seront peut-être pas en mesure d'activer les notifications pour les applications.

Créer un profil de notification par application

Avant de commencer : Vérifiez que les applications pour lesquelles vous souhaitez configurer les paramètres de notification sont déjà installées sur les terminaux des utilisateurs avant d'attribuer le profil de notification par application. Si le profil est appliqué à des terminaux avant que les applications affectées soient installées, les utilisateurs ne seront peut-être pas en mesure d'activer les notifications pour les applications.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Personnaliser > Notification par application**.
3. Cliquez sur +.
4. Saisissez le nom et la description du profil.

5. Dans la section **Paramètres de notification par application**, cliquez sur +. Effectuez l'une des opérations suivantes pour indiquer l'application pour laquelle vous souhaitez configurer les paramètres de notification :
   - Pour sélectionner l'application depuis la liste des applications gérées, cliquez sur **Sélectionner les applications depuis la liste des applications**. Recherchez et sélectionnez l'application.
   - Pour spécifier l'application par son ID de package, cliquez sur **Ajouter un ID de package d'application**. Saisissez le nom de l'application et l'ID de package.
6. Cliquez sur **Suivant**.
7. Dans la liste déroulante **Notification**, cliquez sur **Activé**.
8. Sélectionnez l'une des options de notification suivantes :
   - **Afficher dans le centre de notifications**
   - **Afficher dans l'écran de verrouillage**
9. Dans la liste déroulante **Type d'alerte de notification**, sélectionnez l'une des options suivantes :
   - **Aucune** : les utilisateurs du terminal ne recevront aucune alerte de notification.
   - **Bannière** : les utilisateurs du terminal recevront des alertes de notification dans la bannière.
   - **Alerte modale** : les utilisateurs du terminal recevront des alertes de notification modale.
10. Sélectionnez l'une des options d'alerte de notification suivantes :
    - **Activer les badges** : précisez si l'application affiche un badge.
    - **Activer les sons** : précisez si l'application émet un son.
11. Cliquez sur **Save**.
12. Répétez les étapes 4 à 9 pour ajouter d'autres notifications par application.
13. Cliquez sur **Ajouter**.

À la fin :

- Pour modifier les paramètres de notification d'une application, dans la section **Paramètres de notification par application**, cliquez sur le paramètre de notification pour l'application et modifiez les réglages selon les besoins.
- Si vous avez créé plusieurs profils de notification par application, classez-les.

Tâches connexes

Attribuer un profil ou une stratégie informatique à un groupe d'utilisateurs
Attribuer un profil ou une stratégie informatique à un compte d'utilisateur

Définir le nom d'entreprise pour BlackBerry World

Vous pouvez ajouter le nom de votre organisation à la boutique des applications de BlackBerry World for Work.

1. Sur la barre de menus, cliquez sur **Paramètres**.
2. Développez **Gestion des applications** et cliquez sur **BlackBerry World for Work**.
3. Dans **Nom d'entreprise,** saisissez le nom de votre organisation.
4. Cliquez sur **Enregistrer**.

Gestion des applications sur les terminaux BlackBerry OS

Si le domaine BlackBerry UEM prend en charge les terminaux BlackBerry OS (versions 5.0 à 7.1), vous pouvez utiliser la console de gestion pour installer et gérer les applications BlackBerry Device Software Java et BlackBerry sur les terminaux BlackBerry OS.

Pour envoyer des applications BlackBerry Java aux terminaux BlackBerry OS, vous devez d'abord ajouter ces applications au dossier réseau partagé. Vous pouvez utiliser le dossier réseau partager pour stocker et gérer toutes les versions des applications BlackBerry Java que vous souhaitez installer, mettre à jour ou supprimer des terminaux.

Dans la console de gestion, vous créez des configurations logicielles pour indiquer les versions des applications BlackBerry Device Software et BlackBerry Java que vous souhaitez installer, mettre à jour ou supprimer des terminaux BlackBerry OS. Les configurations logicielles permettent également d'indiquer les applications requises, facultatives ou non autorisées. Lorsque vous créez une configuration logicielle, vous devez également indiquer si les utilisateurs peuvent installer des applications non répertoriées dans cette configuration logicielle.

Lorsque vous ajoutez une BlackBerry Java Application à une configuration logicielle, vous devez attribuer une stratégie de contrôle des applications à l'application pour indiquer les ressources auxquelles elle peut accéder. Vous pouvez utiliser des stratégies de contrôle des applications par défaut ou créer et utiliser des stratégies de contrôle des applications personnalisées. Si vous permettez à des utilisateurs d'installer des applications non répertoriées, vous devez créer une stratégie de contrôle des applications pour les applications non répertoriées, indiquant les ressources auxquelles elles peuvent accéder.

Lorsque vous attribuez une configuration logicielle à un groupe ou à des comptes d'utilisateur individuels, la console de gestion BlackBerry Device Software crée une tâche de déploiement pour installer BlackBerry et les applications Java sur les terminaux, puis appliquer les stratégies de contrôle des applications aux terminaux.

Pour plus d'informations sur l'installation et la gestion de BlackBerry Device Software sur les terminaux BlackBerry OS, téléchargez le Guide de mise à jour de BlackBerry Device Software sur help.blackberry.com/detectLang/bes5.

Préparer la distribution des applications BlackBerry Java

Pour envoyer une BlackBerry Java Application aux terminaux BlackBerry OS (version 5.0 à 7.1), le développeur de l'application doit créer un fichier .zip contenant les fichiers nécessaires à l'application et un fichier .alx contenant des informations sur l'application. Si une structure d'annuaire est décrite dans le fichier .alx, cette structure doit être représentée dans le fichier .zip.

Avant de distribuer les applications BlackBerry Java, vous devez spécifier un dossier réseau partagé pour les applications BlackBerry Java à l'aide de la console de gestion. Pour plus d'informations, reportez-vous à la section Spécifier l'emplacement réseau partagé où stocker des applications internes.

Après avoir ajouté une application au dossier réseau partagé, vous pouvez ajouter l'application à une configuration logicielle, spécifier si l'application est requise, facultative ou non autorisée sur les terminaux BlackBerry OS et lui attribuer une stratégie de contrôle des applications afin de contrôler ses autorisations d'accès. Vous attribuez des configurations logicielles aux comptes d'utilisateur pour installer ou mettre à niveau les applications BlackBerry Java sur les terminaux BlackBerry ou pour supprimer les applications BlackBerry Java des terminaux BlackBerry OS.

Ajouter une BlackBerry Java Application au dossier réseau partagé

Pour envoyer une BlackBerry Java Application aux terminaux BlackBerry OS (versions 5.0 à 7.1), vous devez d'abord ajouter l'offre BlackBerry Java Application à l'emplacement réseau partagé. Pour envoyer une version mise à jour d'une application BlackBerry Java Application aux terminaux BlackBerry OS, vous devez d'abord

ajouter l'offre mise à jour au référentiel d'applications. Pour plus d'informations sur la configuration d'un dossier réseau partagé, reportez-vous à la section Spécifier l'emplacement réseau partagé où stocker des applications internes.

1. Sur la barre de menus, cliquez sur **Paramètres BlackBerry OS**.
2. Cliquez sur **Ajouter ou mettre à jour des applications**.
3. Dans la section **Emplacement des applications**, cliquez sur **Parcourir**. Accédez à l'offre BlackBerry Java Application que vous souhaitez ajouter ou mettre à jour dans le référentiel d'applications.
4. Cliquez sur **Suivant**.
5. Cliquez sur **Ajouter une application**.

Spécifier des mots clés pour une BlackBerry Java Application

Vous pouvez spécifier des mots-clés pour une BlackBerry Java Application. Vous pouvez utiliser des mots-clés pour rechercher l'application dans le référentiel d'applications.

1. Sur la barre de menus, cliquez sur **Paramètres BlackBerry OS**.
2. Cliquez sur **Gérer les applications**.
3. Recherchez une application.
4. Dans les résultats de la recherche, cliquez sur le nom d'une application.
5. Cliquez sur **Modifier l'application**.
6. Dans le champ **Mots-clés de l'application**, saisissez un mot-clé.
7. Cliquez sur l'icône **Ajouter**.
8. Répétez les étapes 6 et 7 pour chaque mot-clé que vous souhaitez ajouter.
9. Cliquez sur **Enregistrer tout**.

Configuration des stratégies de contrôle des applications

Lorsque vous ajoutez une BlackBerry Java Application à une configuration logicielle pour installer l'application sur BlackBerry OS (versions 5.0 à 7.1), vous devez indiquer la stratégie de contrôle des applications que vous souhaitez appliquer à BlackBerry Java Application. Les stratégies de contrôle des applications contrôlent les données et les API auxquelles les applications BlackBerry Java peuvent accéder sur des terminaux BlackBerry OS et les sources de données externes et connexions réseau auxquelles les applications BlackBerry Java peuvent accéder.

BlackBerry UEM inclut une stratégie de contrôle des applications standard pour les applications BlackBerry Java que vous classez comme requises, facultatives ou non autorisées. Vous pouvez modifier les paramètres par défaut des stratégies de contrôle des applications standard ou créer des stratégies de contrôle d'applications personnalisées pour une BlackBerry Java Application.

Pour plus d'informations sur la configuration des paramètres des règles de stratégie de contrôle des applications, téléchargez le Guide de référence des stratégies sur help.blackberry.com/detectLang/bes5.

Stratégies de contrôle des applications standard

BlackBerry UEM comprend les stratégies de contrôle des applications standard suivantes pour les terminaux BlackBerry OS (versions 5.0 à 7.1).

Stratégie de contrôle des applications	Description
Stratégie standard requise	Lorsque vous appliquez la stratégie de contrôle des applications à une BlackBerry Java Application, les paramètres de règle exigent que BlackBerry Java Application soit installée et que son exécution soit autorisée sur les terminaux BlackBerry OS.Les terminaux BlackBerry OS installent automatiquement l'application.
Stratégie standard facultative	Lorsque vous appliquez la stratégie de contrôle des applications à une BlackBerry Java Application, les paramètres de la règle rendent l'application BlackBerry Java Application facultative sur le terminal BlackBerry OS. Les utilisateurs peuvent installer et exécuter BlackBerry Java Application sur leurs terminaux BlackBerry OS.
Stratégie standard non autorisée	Lorsque vous appliquez la stratégie de contrôle des applications à BlackBerry Java Application, les paramètres de la règle empêchent les utilisateurs d'installer BlackBerry Java Application sur les terminaux BlackBerry OS. Les utilisateurs ne peuvent pas installer et exécuter BlackBerry Java Application sur leurs terminaux BlackBerry OS.

Modifier une stratégie de contrôle des applications standard

Lorsque vous ajoutez une application BlackBerry Java Application à une configuration logicielle, vous devez attribuer une stratégie de contrôle des applications à l'application BlackBerry Java Application. Selon les exigences de l'environnement de votre organisation, vous pouvez modifier les paramètres par défaut des stratégies de contrôle des applications standard.

1. Sur la barre de menus, cliquez sur **Paramètres BlackBerry OS**.
2. Cliquez sur **Gérer les stratégies de contrôle des applications par défaut**.
3. Cliquez sur la stratégie de contrôle des applications standard que vous souhaitez modifier.
4. Cliquez sur **Modifier la stratégie de contrôle des applications**.
5. Dans l'onglet **Paramètres d'accès**, dans la section **Paramètres**, modifiez les paramètres de la stratégie de contrôle des applications standard.
6. Cliquez sur **Enregistrer tout**.

Créer des stratégies de contrôle des applications personnalisées pour une BlackBerry Java Application

Après avoir ajouté une BlackBerry Java Application au dossier réseau partagé, vous pouvez configurer l'application de manière à utiliser les stratégies de contrôle d'applications standard ou créer des stratégies de contrôle des applications personnalisées pour l'application. Si vous souhaitez qu'une application BlackBerry Java Application utilise des stratégies de contrôle d'applications personnalisées, vous devez créer ces stratégies de contrôle d'applications personnalisées avant d'ajouter l'application à une configuration logicielle. Lorsque vous ajoutez l'application à une configuration logicielle, vous pouvez sélectionner la stratégie de contrôle des applications personnalisée que vous souhaitez appliquer à l'application.

Si vous ajoutez l'application BlackBerry Java Application à plusieurs configurations logicielles et que vous attribuez différentes stratégies de contrôle des applications personnalisées à l'application BlackBerry Java Application dans différentes configurations logicielles, vous devez définir la priorité des stratégies de contrôle d'applications personnalisées. Cette priorité détermine quelle stratégie de contrôle des applications personnalisée BlackBerry Policy Service applique si vous attribuez plusieurs configurations logicielles à un compte d'utilisateur.

1. Sur la barre de menus, cliquez sur **Paramètres BlackBerry OS**.
2. Cliquez sur **Gérer les applications**.
3. Recherchez une BlackBerry Java Application.
4. Dans les résultats de la recherche, cliquez sur une BlackBerry Java Application.
5. Dans la section **Versions de l'application**, cliquez sur la version de l'application pour laquelle vous souhaitez créer une stratégie de contrôle des applications personnalisée.
6. Cliquez sur **Modifier l'application**.
7. Dans l'onglet **Stratégies de contrôle des applications**, dans la section **Paramètres**, sélectionnez l'option **Utiliser des stratégies de contrôle des applications personnalisées**.
8. Effectuez l'une des tâches suivantes :

Tâche	Étapes
Créer une stratégie de contrôle des applications pour les applications BlackBerry Java requises	a. Dans le champ **Nom de l'application requise**, saisissez un nom pour la stratégie de contrôle des applications. b. Dans la section **Paramètres**, configurez les paramètres de la stratégie de contrôle des applications. c. Cliquez sur l'icône **Ajouter**. d. Répétez les étapes a à c pour chaque stratégie de contrôle des applications que vous souhaitez créer.
Créer une stratégie de contrôle des applications pour les applications BlackBerry Java facult	a. Dans le champ **Nom de l'application facultative**, saisissez un nom pour la stratégie de contrôle des applications. b. Dans la section **Paramètres**, configurez les paramètres de la stratégie de contrôle des applications. c. Cliquez sur l'icône **Ajouter**. d. Répétez les étapes 1 à 3 pour chaque stratégie de contrôle des applications que vous souhaitez créer.
Créer une stratégie de contrôle des applications pour les applications BlackBerry Java interdites	a. Dans le champ **Nom de l'application non autorisée**, saisissez un nom pour la stratégie de contrôle des applications. b. Cliquez sur l'icône **Ajouter**.

9. Si nécessaire, dans chaque section, cliquez sur les flèches haut et bas pour définir la priorité des stratégies de contrôle des applications.
10. Cliquez sur **Enregistrer tout**.

Classement des règles de stratégie informatique sur les terminaux BlackBerry OS

Les paramètres des règles de stratégie informatique remplacent les paramètres des règles de stratégie de contrôle des applications. Par exemple, si vous modifiez la règle de stratégie informatique Autoriser les connexions internes sur Faux sur les terminaux BlackBerry OS (versions 5.0 à 7.1)et si les terminaux disposent d'un ensemble de stratégies de contrôle des applications permettant à une application spécifique d'établir des connexions internes, l'application ne peut pas établir de connexions internes.

Le terminal révoque une stratégie de contrôle des applications et se réinitialise si les autorisations de son application deviennent plus restrictives. Les terminaux permettent aux utilisateurs de rendre les autorisations des applications plus restrictives, mais pas plus permissives que les autorisations que vous définissez.

Stratégies de contrôle des applications pour les applications non répertoriées

Lorsque vous créez une configuration logicielle et que vous l'attribuez à des comptes d'utilisateur pour pouvoir envoyer des applications BlackBerry Device Software, BlackBerry Java et des paramètres d'application standard à BlackBerry OS (versions 5.0 à 7.1), vous devez indiquer si la configuration logicielle permet aux utilisateurs d'installer et d'utiliser les applications qui ne font pas partie de la configuration logicielle (également appelées applications non répertoriées). Lorsque vous indiquez si les applications non répertoriées sont autorisées et facultatives ou non autorisées sur les terminaux BlackBerry OS, vous devez attribuer une stratégie de contrôle des applications pour les applications non répertoriées à la configuration logicielle.

Une stratégie de contrôle d'applications pour les applications non répertoriées détermine les applications non répertoriées autorisées sur les terminaux BlackBerry OS ainsi que les données auxquelles les applications non répertoriées peuvent accéder sur les terminaux BlackBerry OS. Il existe deux stratégies de contrôle des applications standard pour les applications non répertoriées : une stratégie pour les applications non répertoriées facultatives et une stratégie pour les applications non répertoriées non autorisées. Vous pouvez modifier les paramètres par défaut de la stratégie de contrôle des applications standard pour les applications non répertoriées facultatives ou créer des stratégies de contrôle des applications personnalisées pour les applications non répertoriées facultatives.

Modifier la stratégie de contrôle des applications standard pour les applications non répertoriées facultatives

1. Sur la barre de menus, cliquez sur **Paramètres BlackBerry OS**.
2. Développez **Logiciel**.
3. Cliquez sur **Gérer les stratégies de contrôle des applications pour les applications non répertoriées** .
4. Cliquez sur la stratégie de contrôle des applications **Applications non répertoriées facultatives standard**.
5. Cliquez sur **Modifier la stratégie de contrôle des applications**.
6. Dans l'onglet **Paramètres d'accès**, dans la section **Paramètres**, configurez les paramètres de la stratégie de contrôle des applications.
7. Cliquez sur **Enregistrer tout**.

Créer une stratégie de contrôle d'applications pour les applications non répertoriées

Il existe deux stratégies de contrôle des applications par défaut pour les applications non répertoriées : une stratégies pour les applications non répertoriées que vous autorisez sur les terminaux BlackBerry OS (versions 5.0 à 7.1) et une stratégie pour les applications non répertoriées que vous n'autorisez pas sur les terminaux BlackBerry OS. Vous pouvez également créer des stratégies de contrôle des applications personnalisées pour les applications non répertoriées facultatives.

1. Sur la barre de menus, cliquez sur **Paramètres BlackBerry OS**.
2. Développez **Logiciel**.
3. Cliquez sur **Créer une stratégie de contrôle d'applications pour les applications non répertoriées**.
4. Dans la section **Informations sur la stratégie de contrôle des applications**, dans le champ **Nom**, saisissez un nom pour la stratégie de contrôle des applications pour les applications non répertoriées.
5. Cliquez sur **Enregistrer**.
6. Dans le menu **Gestion de la solution BlackBerry**, cliquez sur **Gérer les stratégies de contrôle des applications pour les applications non répertoriées**.
7. Cliquez sur la stratégie de contrôle des applications que vous avez créée.
8. Cliquez sur **Modifier la stratégie de contrôle des applications**.
9. Dans l'onglet **Paramètres d'accès**, dans la section **Paramètres**, configurez les paramètres de la stratégie de contrôle des applications.
10. Cliquez sur **Enregistrer tout**.

Configurer la priorité des stratégies de contrôle des applications pour les applications non répertoriées

Vous pouvez attribuer plusieurs configurations logicielles aux comptes d'utilisateur. Vous pouvez attribuer différentes stratégies de contrôle des applications pour les applications non répertoriées à différentes configurations logicielles. Vous devez configurer la priorité des différentes stratégies de contrôle des applications pour les applications non répertoriées afin de permettre à BlackBerry Policy Service de déterminer les stratégies de contrôle des applications à appliquer aux comptes d'utilisateur lorsque vous attribuez plusieurs configurations logicielles à ces comptes.

1. Sur la barre de menus, cliquez sur **Paramètres BlackBerry OS**.
2. Développez **Logiciel**.
3. Cliquez sur **Gérer les stratégies de contrôle des applications pour les applications non répertoriées** .
4. Cliquez sur **Configurer la priorité des stratégies de contrôle des applications pour les applications non répertoriées**.
5. Cliquez sur les flèches haut et bas pour définir la priorité des stratégies de contrôle des applications pour les applications non répertoriées.
6. Cliquez sur **Enregistrer**.

Création de configurations logicielles

Vous pouvez utiliser des configurations logicielles pour effectuer les opérations suivantes sur les terminaux BlackBerry OS (versions 5.0 à 7.1) :

- attribuer des stratégies de contrôle des applications à des applications BlackBerry Java pour contrôler les autorisations d'application et les données auxquelles les applications peuvent accéder
- spécifier qu'une BlackBerry Java Application n'est pas autorisée
- indiquer si les applications BlackBerry Java exclues de la configuration logicielle sont autorisées ou non
- configurer les autorisations d'accès des applications BlackBerry Java exclues de la configuration logicielle
- installer ou mettre à niveau BlackBerry Device Software sur le réseau sans fil ou à l'aide de BlackBerry Web Desktop Manager
- spécifier des paramètres d'application standard

Étapes à suivre pour créer et attribuer une configuration logicielle

Lorsque vous créez et attribuez une configuration logicielle, vous procédez comme suit :

Étape	Action
1	Créez et partagez un dossier réseau.
2	Ajoutez les applications.
3	Si nécessaire, créez une stratégie de contrôle des applications personnalisée.
4	Créez une configuration logicielle.

Étape	Action
5	Ajoutez des logiciels à la configuration logicielle.
6	Attribuez la configuration logicielle à un compte d'utilisateur ou à un groupe d'utilisateurs.

Créer une configuration logicielle

1. Sur la barre de menus, cliquez sur **Paramètres BlackBerry OS**.
2. Développez **Logiciel**.
3. Cliquez sur **Créer une configuration logicielle**.
4. Dans la section **Informations sur la configuration**, dans le champ **Nom**, saisissez un nom pour la configuration logicielle.
5. Dans la liste déroulante **Disposition pour les applications non répertoriées**, effectuez l'une des opérations suivantes :
   - Pour autoriser les utilisateurs à installer des applications non incluses dans la configuration logicielle de leurs terminaux BlackBerry OS, cliquez sur **Facultatif**.
   - Pour empêcher les utilisateurs d'installer des applications non incluses dans la configuration logicielle de leurs terminaux BlackBerry OS, cliquez sur **Non autorisé**.
6. Dans la liste déroulante **Stratégie de contrôle des applications pour les applications non répertoriées**, cliquez sur la stratégie de contrôle des applications pour les applications non répertoriées que vous souhaitez attribuer à la configuration logicielle.
7. Cliquez sur **Enregistrer**.

À la fin : ajoutez les configurations BlackBerry Device Software et les applications BlackBerry Java à la configuration logicielle.

Ajouter une BlackBerry Java Application à une configuration logicielle

Pour installer BlackBerry Java Application sur les terminaux BlackBerry Java Application OS (versions 5.0 à 7.1) par le biais du réseau sans fil, vous devez ajouter une BlackBerry à une configuration logicielle et attribuer la configuration logicielle aux comptes d'utilisateur. Pour mettre à niveau une application, vous devez ajouter la nouvelle version de l'application à la configuration logicielle qui convient. BlackBerry UEM met à niveau l'application qui se trouve sur les terminaux BlackBerry OS vers la nouvelle version.

1. Sur la barre de menus, cliquez sur **Paramètres BlackBerry OS.**
2. Développez **Logiciel**.
3. Cliquez sur **Gérer les configurations logicielles**.
4. Cliquez sur la configuration logicielle à laquelle vous souhaitez ajouter une BlackBerry Java Application.
5. Cliquez sur **Modifier la configuration logicielle**.
6. Dans l'onglet **Applications**, cliquez sur **Ajouter des applications à la configuration logicielle**.
7. Recherchez les applications BlackBerry Java que vous souhaitez ajouter à la configuration logicielle.
8. Dans les résultats de la recherche, sélectionnez une BlackBerry Java Application que vous souhaitez ajouter à la configuration logicielle.
9. Dans la liste déroulante **Disposition** de BlackBerry Java Application, exécutez l'une des opérations suivantes :

- Pour installer BlackBerry Java Application automatiquement sur les terminaux BlackBerryOS et empêcher les utilisateurs de la supprimer, cliquez sur **Requis.**
- Pour permettre aux utilisateurs d'installer et de supprimer BlackBerry Java Application, cliquez sur **Facultatif**.
- Pour empêcher les utilisateurs d'installer une BlackBerry Java Application sur les terminaux BlackBerry OS, cliquez sur **Non autorisé**.

10. Dans la section **Données d'application**, dans la liste déroulante **Stratégie de contrôle des applications**, cliquez sur une stratégie de contrôle des applications à appliquer à la BlackBerry Java Application.
11. Si nécessaire, dans la liste déroulante **Déploiement**, exécutez l'une des actions suivantes :
    - Pour installer l'application sur des terminaux BlackBerry OS par le biais du réseau sans fil, cliquez sur **Sans fil.**
    - Pour installer l'application sur des terminaux BlackBerry OS à l'aide d'une connexion USB à l'ordinateur de l'utilisateur et à BlackBerry Web Desktop Manager, cliquez sur **Filaire**.
12. Répétez les étapes 6 à 10 pour chaque BlackBerry Java Application que vous souhaitez ajouter à la configuration logicielle.
13. Cliquez sur **Ajouter à la configuration logicielle**.
14. Cliquez sur **Enregistrer tout**.

Installer des applications BlackBerry Java sur un terminal BlackBerry à partir d'un ordinateur central

Si vous ne souhaitez pas installer les applications BlackBerry Java sur un terminal BlackBerry OS (versions 5.0 à 7.1) via le réseau sans fil, et si vous ne souhaitez pas que l'utilisateur installe les applications BlackBerry Java à l'aide de BlackBerry Web Desktop Manager ou BlackBerry Desktop Software, vous pouvez installer les applications BlackBerry Java sur un terminal BlackBerry OS en connectant le terminal BlackBerry OS à un ordinateur central autorisé à accéder à BlackBerry UEM.

Avant de commencer :

- Attribuez au compte d'utilisateur approprié une configuration logicielle avec les applications BlackBerry Java nécessaires.
- Pour permettre à la console de gestion de se connecter à un terminal BlackBerry OS relié à l'ordinateur hébergeant la console de gestion BlackBerry UEM via une connexion USB, ajoutez l'adresse Web de la console de gestion à la liste des sites Web approuvés du navigateur Web. Connectez-vous à nouveau à la console de gestion.
- Vérifiez que l'ordinateur central peut accéder à la console de gestion.
- Connectez le terminal BlackBerry OS associé au compte d'utilisateur à l'ordinateur central.

1. Sur la barre de menus, cliquez sur **Paramètres BlackBerry OS**.
2. Développez **Terminaux associés**.
3. Cliquez sur **Logiciel du terminal**.
4. Cliquez sur **Installation automatique d'applications sur le terminal BlackBerry.**
5. Suivez les instructions qui s'affichent à l'écran.

Afficher les utilisateurs dotés d'une application BlackBerry Java sur leurs terminaux BlackBerry OS

1. Sur la barre de menus, cliquez sur **Paramètres BlackBerry OS**.
2. Développez **Logiciel > Applications**.
3. Cliquez sur **Gérer les applications**.
4. Recherchez une application.
5. Dans les résultats de la recherche, cliquez sur le nom d'une application.

6. Dans la section **Versions de l'application**, cliquez sur la version de l'application.
7. Cliquez sur **Afficher les utilisateurs dotés de l'application**.
8. Recherchez des utilisateurs associés aux terminaux BlackBerry OS sur lesquels vous avez installé l'application BlackBerry Java.

Règles de réconciliation des paramètres en conflit des configurations logicielles

Si vous attribuez plusieurs configurations logicielles aux comptes d'utilisateur ou groupes d'utilisateurs, ces configurations logicielles peuvent présenter des paramètres en conflit. Par exemple, il est possible que vous indiquiez qu'une application BlackBerry Java Application est requise dans une configuration logicielle que vous attribuez à un compte d'utilisateur, mais que vous indiquiez également que cette même application n'est pas autorisée dans une configuration logicielle que vous attribuez à un groupe auquel le compte d'utilisateur appartient. Des conflits peuvent se produire lorsque vous attribuez plusieurs BlackBerry Java, stratégies de contrôle des applications, stratégies de contrôle des applications pour les applications non homologuées, logiciels BlackBerry Device Software, et des paramètres d'application standard dans les configurations BlackBerry Device Software.

BlackBerry UEM utilise les règles de réconciliation prédéfinies pour résoudre les paramètres en conflit de configurations logicielles multiples, et pour déterminer les applications, les logiciels et les paramètres installés ou appliqués à un terminal BlackBerry OS (versions 5.0 à 7.1). BlackBerry UEM résout les paramètres en conflit sous forme d'activité d'arrière-plan asynchrone. Vous pouvez afficher le résultat des activités de réconciliation, les erreurs de réconciliation, et les applications, logiciels et paramètres appliqués par BlackBerry UEM à un terminal BlackBerry OS.

Il est possible que BlackBerry UEM doive réconcilier les paramètres de configuration logicielle en conflit si vous exécutez l'une des actions suivantes :

- Activer un terminal
- attribuer un nouveau terminal BlackBerry OS ou code PIN à un utilisateur
- ajouter un compte d'utilisateur à un groupe ou supprimer un compte d'utilisateur d'un groupe
- ajouter un groupe à un groupe ou supprimer un groupe d'un autre groupe
- ajouter une application à une configuration logicielle ou supprimer une application d'une configuration logicielle
- modifier les paramètres d'une application dans une configuration logicielle
- modifier les paramètres d'une stratégie de contrôle des applications
- modifier le classement des stratégies de contrôle des applications
- installer une nouvelle version de BlackBerry Device Software sur un terminal BlackBerry OS
- ajouter une configuration BlackBerry Device Software ou supprimer une configuration BlackBerry Device Software d'une configuration logicielle
- modifier une configuration BlackBerry Device Software
- modifier les paramètres d'application standard d'une configuration BlackBerry Device Software

Règles de réconciliation : applications BlackBerry Java

Scénario	Règle
Plusieurs configurations logicielles sont attribuées à un compte d'utilisateur ou aux groupes auxquels appartient l'utilisateur. Plusieurs applications BlackBerry Java sont contenues dans chaque configuration logicielle.	Les applications BlackBerry Java de chaque configuration logicielle sont installées sur le terminal BlackBerry OS (versions 5.0 à 7.1). Si BlackBerry Device Software ne prend pas en charge une BlackBerry Java Application spécifique, cette application n'est pas installée sur le terminal BlackBerry OS.
Plusieurs configurations logicielles qui contiennent des versions différentes de la même BlackBerry Java Application sont attribuées à un compte d'utilisateur ou aux groupes auxquels appartient l'utilisateur.	En présence de différentes versions d'une application dans les configurations logicielles attribuées à un compte d'utilisateur, la version la plus récente de l'application prise en charge par BlackBerry Device Software est installée sur le terminal BlackBerry OS. Par exemple, si une configuration logicielle avec la version 1.0 d'une application est attribuée à un compte d'utilisateur, et si une autre configuration logicielle avec la version 2.0 de l'application est attribuée à un compte d'utilisateur, la version 2.0 de l'application est installée sur le terminal BlackBerry. La version d'une BlackBerry Java Application correspondant à une configuration logicielle attribuée à un compte d'utilisateur est prioritaire sur la version d'une BlackBerry Java Application présente dans une configuration logicielle attribuée à un groupe. Par exemple, si la version 1.0 d'une application est dans une configuration logicielle attribuée à un compte d'utilisateur, et une version 2.0 d'une application est dans une configuration logicielle attribuée à un groupe auquel l'utilisateur appartient, la version 1.0 de l'application est installée sur le terminal BlackBerry.

Scénario	Règle
Plusieurs configurations logicielles qui contiennent la même BlackBerry Java Application sont attribuées à un compte d'utilisateur ou aux groupes auxquels l'utilisateur appartient. La disposition de BlackBerry Java Application (requise ou facultative) est différente dans chaque configuration logicielle. La méthode de déploiement (filaire ou par le biais du réseau sans fil) de l'application est différente dans chaque configuration logicielle.	La disposition spécifiée pour une application dans une configuration logicielle attribuée à un compte d'utilisateur est prioritaire sur la disposition de la même application dans une configuration logicielle attribuée à un groupe. Si l'application présente des dispositions différentes dans plusieurs configurations logicielles attribuées au même niveau (compte d'utilisateur ou groupes), la disposition requise est prioritaire sur la disposition facultative et la disposition facultative prioritaire sur la disposition non autorisée. BlackBerry UEM résout la méthode de déploiement après avoir résolu la disposition d'une application. La méthode de déploiement spécifiée pour une application dans une configuration logicielle attribuée à un compte d'utilisateur est prioritaire sur la méthode de déploiement de la même application dans une configuration logicielle attribuée à un groupe. Le paramètre sans fil est prioritaire sur le paramètre filaire.
Une ou plusieurs configurations logicielles qui incluent les applications BlackBerry Java sont attribuées à un compte d'utilisateur ou aux groupes auxquels appartient l'utilisateur, mais une quantité limitée de mémoire disponible reste sur le terminal BlackBerry OS.	BlackBerry UEM vérifie la quantité de mémoire disponible sur le terminal BlackBerry OS après avoir résolu les conflits d'application (résolution des paramètres de disposition et de déploiement en conflit, par exemple) et avant d'installer une BlackBerry Java Application. S'il n'y a pas assez de mémoire disponible sur le terminal BlackBerry pour prendre en charge l'application, celle-ci n'est pas installée. En fonction de la quantité de mémoire disponible, les applications sont installées dans l'ordre suivant : **1.** Applications requises configurées pour le déploiement sans fil **2.** Applications requises configurées pour le déploiement filaire **3.** Applications facultatives configurées pour le déploiement sans fil **4.** Applications facultatives configurées pour le déploiement filaire

Scénario	Règle
Une configuration logicielle est attribuée à un compte d'utilisateur et contient une BlackBerry Java Application qui a une dépendance à une autre BlackBerry Java Application.	Si une BlackBerry Java Application dans une configuration logicielle a une dépendance à une autre application et si l'autre application n'est pas incluse dans une configuration logicielle attribuée au compte d'utilisateur ou à un groupe auquel l'utilisateur appartient, l'application n'est pas installée sur le terminal BlackBerry OS. Si une BlackBerry Java Application dans une configuration logicielle a une dépendance à une autre application, et si l'application dépendante est incluse dans une configuration logicielle attribuée au compte d'utilisateur ou à un groupe auquel l'utilisateur appartient, l'application dépendante est installée en premier. Si l'application dépendante est correctement installée, l'application avec la dépendance est alors installée.
Une configuration logicielle est attribuée à un compte d'utilisateur et contient une BlackBerry Java Application qui a une dépendance à une autre BlackBerry Java Application. L'application dépendante n'est pas prise en charge sur le terminal BlackBerry OS.	Si une application dépendante n'est pas prise en charge par le terminal BlackBerry OS ou n'a pas été installée avec succès sur le terminal BlackBerry OS, l'application avec la dépendance n'est pas installée sur le terminal BlackBerry OS de l'utilisateur.
Plusieurs applications BlackBerry Java ont une dépendance circulaire (par exemple, l'application A est dépendante de l'application B, l'application B est dépendante de l'application C et l'application C est dépendante de l'application A) et sont comprises dans la même offre d'application. L'offre d'application est ajoutée au référentiel d'applications. Les applications sont ajoutées à une configuration logicielle et attribuées à un compte d'utilisateur ou à un groupe auquel appartient l'utilisateur.	Si plusieurs BlackBerry Java sont comprises dans la même offre d'application et ont une dépendance circulaire, les applications ne sont pas installées sur le terminal BlackBerry OS. Si plusieurs applications ont une dépendance circulaire, elles ne peuvent être installées que si elles sont présentes dans des offres d'applications séparées et installées moyennant un déploiement filaire.

Règles de réconciliation : BlackBerry Device Software

Scénario	Règle
Une configuration logicielle qui contient le logiciel BlackBerry Device Software est attribuée à un compte d'utilisateur. Une configuration logicielle contenant une version différente de BlackBerry Device Software est attribuée à un groupe auquel appartient le compte d'utilisateur.	La BlackBerry Device Software d'une configuration logicielle attribuée à un compte d'utilisateur est prioritaire sur la BlackBerry Device Software d'une configuration logicielle attribuée à un groupe.

Scénario	Règle
Plusieurs configurations logicielles contenant des versions différentes de BlackBerry Device Software sont attribuées à un compte d'utilisateur.	La version de BlackBerry Device Software prise en charge par le terminal BlackBerry OS (versions 5.0 à 7.1) et par le fournisseur de services sans fil et à laquelle vous attribuez la plus haute priorité dans la console de gestion BlackBerry UEM est installée sur le terminal BlackBerry OS. BlackBerry UEM n'installe pas une version de BlackBerry Device Software si cette version est classée plus bas que la version de BlackBerry Device Software actuellement installée sur le terminal BlackBerry OS.

Règles de réconciliation : paramètres d'application standard

Scénario	Règle
Une configuration logicielle dotée de paramètres d'application standard est attribuée à un compte d'utilisateur. Une configuration logicielle dotée de différents paramètres d'application standard est attribuée à un groupe auquel appartient le compte d'utilisateur.	Les paramètres d'application standard d'une configuration logicielle attribuée à un compte d'utilisateur sont prioritaires sur les paramètres d'application standard d'une configuration logicielle attribuée à un groupe.
Un compte d'utilisateur appartient à plusieurs groupes. Le paramètre d'affichage initial du calendrier est configuré différemment dans chacune des configurations logicielles attribuées aux groupes.	Le paramètre d'affichage initial du calendrier appliqué au terminal BlackBerry OS (versions 5.0 à 7.1) de l'utilisateur correspond à la plus basse valeur spécifiée dans les différentes configurations logicielles.
Un compte d'utilisateur appartient à plusieurs groupes. Le paramètre de conservation des rendez-vous dans le calendrier est configuré différemment dans chacune des configurations logicielles attribuées aux groupes.	Le paramètre de conservation des rendez-vous dans le calendrier appliqué au terminal BlackBerry OS de l'utilisateur correspondant à la plus haute valeur spécifiée dans les différentes configurations logicielles.
Un compte d'utilisateur appartient à plusieurs groupes. Le paramètre de confirmation de la suppression est défini sur Oui dans une ou plusieurs des configurations logicielles attribuées aux groupes. Le paramètre est défini sur Non dans les configurations logicielles restantes.	Si le paramètre de confirmation de suppression est défini sur Oui dans une configuration logicielle attribuée à un groupe auquel appartient le compte d'utilisateur, le paramètre Oui est appliqué au terminal BlackBerry OS.
Un compte d'utilisateur appartient à plusieurs groupes. Le paramètre de masquage des messages envoyés est défini sur Oui dans une ou plusieurs des configurations logicielles attribuées aux groupes. Le paramètre est défini sur Non dans les configurations logicielles restantes.	Si le paramètre de masquage des messages envoyés est défini sur Non dans une configuration logicielle attribuée à un groupe auquel appartient le compte d'utilisateur, le paramètre Non est appliqué au terminal BlackBerry OS.

Scénario	Règle
Un compte d'utilisateur appartient à plusieurs groupes. Le paramètre de sauvegarde d'une copie dans le dossier des messages envoyés est défini sur Oui dans une ou plusieurs des configurations logicielles attribuées aux groupes. Le paramètre est défini sur Non dans les configurations logicielles restantes.	Si le paramètre de sauvegarde d'une copie dans le dossier des messages envoyés est défini sur Oui dans une configuration logicielle attribuée à un groupe auquel appartient le compte d'utilisateur, le paramètre Oui est appliqué au terminal BlackBerry OS.
Un compte d'utilisateur appartient à plusieurs groupes. Le paramètre de tri du carnet d'adresses est configuré différemment dans chacune des configurations logicielles attribuées aux groupes.	Si le paramètre tri du carnet d'adresses est configuré différemment dans les configurations logicielles attribuées aux groupes auxquels appartient le compte d'utilisateur, le paramètre de prénom est prioritaire sur le paramètre de nom et le paramètre de nom est prioritaire sur le paramètre de nom de l'entreprise.
Un compte d'utilisateur appartient à plusieurs groupes. Les paramètres des attributs des paramètres d'application standard sont configurés différemment dans les configurations logicielles attribuées aux groupes.	Le paramètre Verrouillé et visible est prioritaire sur le paramètre Déverrouillé et visible. Le paramètre Déverrouillé et visible est prioritaire sur le paramètre Déverrouillé et masqué.
Les paramètres d'application standard sont configurés dans une configuration logicielle et attribués aux comptes d'utilisateur avec les terminaux BlackBerry qui exécutent une version du logiciel BlackBerry Device Software antérieure à la version 5.0.	Les paramètres d'application standard s'appliquent uniquement aux terminaux BlackBerry OS exécutant BlackBerry Device Software version 5.0 ou ultérieure.

Règles de réconciliation : stratégies de contrôle des applications

Scénario	Règle
Un utilisateur se voit attribuer plusieurs configurations logicielles contenant chacune la même application. Une stratégie de contrôle des applications différente est attribuée à l'application dans chaque configuration logicielle.	Une stratégie de contrôle des applications pour une application dans une configuration logicielle attribuée à un compte d'utilisateur est prioritaire sur une stratégie de contrôle d'applications pour la même application dans une configuration logicielle attribuée à un groupe. Le paramètre requis est prioritaire sur le paramètre facultatif. Le paramètre facultatif est prioritaire sur le paramètre non autorisé. Si plusieurs configurations logicielles contiennent la même application, et si chaque configuration logicielle se voit attribuer une stratégie de contrôle des applications personnalisée différente avec la même disposition (par exemple, deux stratégies de contrôle des applications requises personnalisées), la stratégie de contrôle des applications que vous avez classée à un rang plus élevé dans la console de gestion BlackBerry UEM est appliquée au terminal BlackBerry OS (versions 5.0 à 7.1) de l'utilisateur.

Règles de réconciliation : stratégies de contrôle des applications pour les applications non répertoriées

Scénario	Règle
Une configuration logicielle présentant une stratégie de contrôle des applications par défaut ou personnalisée pour les applications non répertoriées est attribuée à un compte d'utilisateur. Une configuration logicielle présentant une stratégie de contrôle des applications différente pour les applications non répertoriées est attribuée à un groupe auquel appartient le compte d'utilisateur.	La stratégie de contrôle des applications pour les applications non répertoriées dans une configuration logicielle attribuée à un compte d'utilisateur est prioritaire sur la stratégie de contrôle d'applications pour les applications non répertoriées dans une configuration logicielle attribuée à un groupe.
Une configuration logicielle définissant les applications non répertoriées comme non autorisées est attribuée à un compte d'utilisateur. Une configuration logicielle définissant les applications non répertoriées comme facultatives est également attribuée à un compte d'utilisateur.	Si les applications non répertoriées sont définies comme non autorisées dans une configuration logicielle attribuée à un compte d'utilisateur, les applications non répertoriées ne sont pas autorisées sur le terminal BlackBerry OS (versions 5.0 à 7.1).
Plusieurs configurations logicielles avec différentes stratégies de contrôle d'accès pour les applications non homologuées sont attribuées à un compte d'utilisateur.	La stratégie de contrôle des applications pour les applications non répertoriées que vous avez classées à un rang plus élevé dans la console de gestion BlackBerry UEM est appliquée au terminal BlackBerry OS.

Utilisateurs et groupes

Vous pouvez créer des comptes d'utilisateur, puis des groupes d'utilisateurs pour gérer plus efficacement les utilisateurs et les terminaux.

Procédure de création de groupes et comptes d'utilisateur

Pour gérer les utilisateurs et les terminaux de votre organisation, procédez comme suit :

Étape	Action
1	Créez des rôles d'utilisateurs.
2	Créez des groupes d'utilisateurs.
3	Créez des comptes d'utilisateur.
4	Si vous le souhaitez, créez des groupes de terminaux.

Création de rôles d'utilisateur

Les rôles d'utilisateur vous permettent de spécifier les fonctionnalités mises à la disposition des utilisateurs dans BlackBerry UEM Self-Service.

BlackBerry UEM inclut un rôle d'utilisateur par défaut préconfiguré. Le rôle d'utilisateur par défaut est configuré pour autoriser toutes les fonctionnalités BlackBerry UEM Self-Service. De plus, il est attribué au groupe Tous les utilisateurs. Vous pouvez modifier les fonctionnalités du rôle d'utilisateur par défaut.

Remarque : Renommer, supprimer ou supprimer le rôle d'utilisateur par défaut du groupe Tous les utilisateurs peut entrainer des problèmes avec l'application Wok Apps sur les terminaux iOS.

Si vous souhaitez limiter l'accès des utilisateurs à certaines fonctionnalités BlackBerry UEM Self-Service, vous pouvez créer de nouveaux rôles d'utilisateur ou modifier un rôle d'utilisateur existant. Vous pouvez attribuer des rôles d'utilisateur aux groupes ou directement aux utilisateurs.

Fonctionnalités de BlackBerry UEM Self-Service

Le tableau suivant répertorie les capacités de BlackBerry UEM Self-Service :

Fonctionnalité	Description
Spécifier un mot de passe d'activation	Cette fonctionnalité permet aux utilisateurs de créer des mots de passe d'activation qu'ils peuvent ensuite utiliser pour activer leurs terminaux dans BlackBerry UEM. Vous pouvez configurer le délai d'expiration par défaut et la complexité exigée pour le mot de passe dans Paramètres > Self-Service > Paramètres Self-Service.
Spécifier une clé d'accès	Cette fonctionnalité permet aux utilisateurs de créer des clés d'accès qu'ils peuvent ensuite utiliser pour activer les applications BlackBerry Dynamics.
Supprimer uniquement les données professionnelles	Cette fonctionnalité permet aux utilisateurs d'envoyer la commande « Delete only work data » (Supprimer les données professionnelles uniquement) à un terminal. Cette commande supprime les données professionnelles, y compris les stratégies informatiques, les profils, les applications et les certificats.
Supprimer toutes les données du terminal	Cette fonctionnalité permet aux utilisateurs d'envoyer la commande « Delete all device data » (Supprimer toutes les données du terminal) à un terminal. Cette commande supprime toutes les informations utilisateur et toutes les données d'applications qui sont stockées sur le terminal, y compris les informations de l'espace de travail. Elle rétablit les paramètres d'usine du terminal et supprime ce dernier dans BlackBerry UEM.
Localiser le terminal	Cette fonctionnalité permet aux utilisateurs de visualiser l'emplacement de leurs terminaux iOS, Android ou Windows 10 Mobile sur une carte. Pour que cette fonctionnalité soit disponible, un profil de service de localisation doit être attribué à l'utilisateur. Pour plus d'informations, reportez-vous à Créer un profil de service de localisation.
Gérer les certificats utilisateur	Cette fonctionnalité permet aux utilisateurs de charger des certificats utilisateur pour leurs terminaux. Vous pouvez fournir des instructions aux utilisateurs sur les certificats dont ils ont besoin et sur les emplacements d'où ils peuvent télécharger ces certificats.
Verrouiller et déverrouiller les applications BlackBerry Dynamics	Si des terminaux d'utilisateurs sont activés pour BlackBerry Dynamics, cette fonctionnalité permet aux utilisateurs de verrouiller les applications BlackBerry Dynamics installées sur leurs terminaux ou de générer des codes de déverrouillage pour déverrouiller les applications. Lorsqu'un utilisateur verrouille une application, plus personne ne peut l'ouvrir.
Supprimer les données d'application BlackBerry Dynamics	Si des terminaux d'utilisateurs sont activés pour BlackBerry Dynamics, cette fonctionnalité permet aux utilisateurs de supprimer toutes les données d'une application BlackBerry Dynamics installée sur un terminal. La commande supprime toutes les données stockées par l'application, mais l'application même n'est pas supprimée.

Création d'un rôle d'utilisateur

Vous pouvez créer un rôle d'utilisateur personnalisé et l'attribuer à des utilisateurs ou groupes pour spécifier les fonctionnalités qu'ils peuvent utiliser dans BlackBerry UEM Self-Service.

1. Dans la barre de menus, cliquez sur **Paramètres > Self-Service**.
2. Cliquez sur **Rôles d'utilisateur**.

3. Cliquez sur .
4. Saisissez le nom et la description du rôle d'utilisateur.
5. Pour copier les autorisations d'un autre rôle, cliquez sur un rôle de la liste déroulante **Autorisations copiées à partir du rôle**.
6. Sélectionnez les fonctionnalités que vous souhaitez mettre à la disposition d'un utilisateur.
7. Cliquez sur **Enregistrer**.

Comment BlackBerry UEM choisit-il l'attribution du rôle d'utilisateur ?

Un utilisateur ne peut avoir qu'un seul rôle. BlackBerry UEM utilise les règles suivantes pour déterminer le rôle à attribuer à un utilisateur :

- Un rôle directement attribué à un compte d'utilisateur est prioritaire sur un rôle attribué indirectement par un groupe d'utilisateurs.
- Si un utilisateur est membre de plusieurs groupes d'utilisateurs possédant des rôles d'utilisateur différents, BlackBerry UEM lui attribue le rôle dont le rang est le plus élevé.

Classement des rôles d'utilisateur

Le classement permet de déterminer quel rôle BlackBerry UEM attribue à un utilisateur lorsqu'il est membre de plusieurs groupes d'utilisateurs qui possèdent des rôles différents.

1. Dans la barre de menus, cliquez sur **Paramètres > Self-Service**.
2. Cliquez sur **Rôles d'utilisateur**.
3. Utilisez les flèches pour déplacer les rôles vers le haut ou le bas du classement.
4. Cliquez sur **Enregistrer**.

Attribuer un rôle d'utilisateur à un groupe

Un rôle d'utilisateur spécifie les fonctionnalités mises à la disposition des utilisateurs dans BlackBerry UEM Self-Service.

Avant de commencer : Création d'un rôle d'utilisateur.

1. Sur la barre de menus, cliquez sur **Groupes**.
2. Recherchez un groupe d'utilisateurs.
3. Dans les résultats de la recherche, cliquez sur le nom du groupe d'utilisateurs.
4. Cliquez sur l'onglet **Terminaux gérés**.
5. Dans la section **Rôle d'utilisateur**, cliquez sur +.
6. Dans la liste déroulante, cliquez sur le nom du rôle que vous souhaitez attribuer au groupe.
7. Cliquez sur **Ajouter** ou **Remplacer**.

Attribuer un rôle d'utilisateur à un utilisateur

Un rôle d'utilisateur spécifie les fonctionnalités mises à la disposition des utilisateurs dans BlackBerry UEM Self-Service.

Avant de commencer : Création d'un rôle d'utilisateur.

1. Sur la barre de menus, cliquez sur **Utilisateurs**.
2. Sélectionnez l' **ensemble des utilisateurs** ou l' **onglet appareils gérés** .
3. Recherchez un compte d'utilisateur.
4. Dans les résultats de la recherche, cliquez sur le nom du compte d'utilisateur.

5. Cliquez sur  .
6. Dans la liste déroulante **Attribution directe de rôle**, sélectionnez le rôle que vous souhaitez attribuer. Si vous sélectionnez **Aucun**, le rôle de l'utilisateur sera attribué par un groupe. Si aucune attribution de groupe n'est effectuée, l'utilisateur n'aura pas accès à BlackBerry UEM Self-Service.
7. Cliquez sur **Enregistrer**.

Création et gestion de comptes d'utilisateur

Vous pouvez directement ajouter des comptes d'utilisateur à BlackBerry UEM ou, si vous vous êtes connecté BlackBerry UEM à votre annuaire d'entreprise, ajouter des comptes d'utilisateur depuis celui-ci. Pour obtenir des informations sur la connexion de BlackBerry UEM à un répertoire d'entreprise et sur l'activation de groupes liés par répertoire, reportez-vous au contenu relatif à la configuration.

Vous pouvez également utiliser un fichier .csv pour ajouter simultanément plusieurs comptes d'utilisateur à BlackBerry UEM.

Créer un compte d'utilisateur

Avant de commencer :

- si vous souhaitez ajouter un utilisateur d'annuaire, vérifiez que BlackBerry UEM est connecté à votre annuaire d'entreprise. Pour obtenir des informations sur la connexion de BlackBerry UEM à un répertoire d'entreprise et sur l'activation de groupes liés par répertoire, reportez-vous au contenu relatif à la configuration.
- Si vous souhaitez activer le service BlackBerry Workspaces pour vos utilisateurs, vérifiez que le plug-in Workspaces pour BlackBerry UEM est installé sur chaque instance de BlackBerry UEM dans votre environnement. Pour plus d'informations sur l'installation du service Workspaces, contactez votre gestionnaire de compte Workspaces.

1. Sur la barre de menus, cliquez sur **Utilisateurs > Terminaux gérés**.
2. Cliquez sur **Ajouter un utilisateur**.
3. Effectuez l'une des tâches suivantes :

Tâche	Étapes
Ajouter un utilisateur d'annuaire	**a.** Dans le champ de recherche de l'onglet **Répertoire d'entreprise**, spécifiez les critères de recherche de l'utilisateur d'annuaire que vous souhaitez ajouter. Vous pouvez effectuer une recherche par nom, prénom, nom d'affichage, nom d'utilisateur ou adresse électronique. **b.** Dans les résultats de la recherche, sélectionnez le compte d'utilisateur.

Tâche	Étapes
Ajouter un utilisateur local	**a.** Cliquez sur l'onglet **Local**. **b.** Saisissez le **Prénom** et le **Nom** du compte utilisateur. **c.** Dans le champ **Nom d'affichage**, apportez des modifications, si nécessaire. Le nom d'affichage est automatiquement configuré avec le prénom et le nom que vous avez spécifiés. **d.** Dans le champ **Nom d'utilisateur**, saisissez un nom d'utilisateur unique pour le compte d'utilisateur. **e.** Dans le champ **Adresse électronique**, saisissez une adresse électronique de contact pour le compte d'utilisateur. Une adresse électronique est obligatoire pour le compte d'utilisateur, lorsque vous activez un service comme la gestion de terminal ou Workspaces. **f.** Vous pouvez aussi cliquer sur **Informations complémentaires sur l'utilisateur** et renseigner les champs au besoin.

4. Si des groupes locaux existent dans BlackBerry UEM et que vous souhaitez ajouter le compte d'utilisateur à des groupes, sélectionnez un ou plusieurs groupes dans la liste **Groupes disponibles**, puis cliquez sur ➡.

   Lorsque vous créez un compte d'utilisateur, vous pouvez uniquement l'ajouter aux groupes locaux de BlackBerry UEM. Si le compte d'utilisateur est membre d'un groupe lié par annuaire, il est automatiquement associé à ce groupe lors de la synchronisation entre BlackBerry UEM et votre annuaire d'entreprise.

   Pour ajouter un compte d'utilisateur à des groupes auxquels a été attribué un rôle administratif, vous devez être Administrateur de sécurité.
5. Si vous ajoutez un utilisateur local, créez un mot de passe pour BlackBerry UEM Self-Service dans le champ **Mot de passe du compte**. Si un rôle d'administrateur est attribué à l'utilisateur, il peut également utiliser le mot de passe pour accéder à la console de gestion.
6. Dans la section **Services activés**, sélectionnez l'option **Autoriser l'utilisateur à gérer les terminaux**.
7. Si le plug-in Workspaces pour BlackBerry UEM est installé dans le domaine, procédez comme suit pour activer le service Workspaces :
   a) Dans la section **BlackBerry Workspaces**, cochez la case **Activer BlackBerry Workspaces**. Par défaut, les utilisateurs activés avec le service Workspaces reçoivent le rôle de Visiteur.
   b) Sélectionnez un ou plusieurs rôles de l'utilisateur. Cliquez sur ➡.
8. Effectuez l'une des tâches suivantes :

Tâche	Étapes
Demandez aux utilisateurs d'activer leur terminal avec le profil d'activation qui leur a été attribué.	**a.** Dans la liste déroulante **Option d'activation**, sélectionnez **Activation du terminal par défaut**. **b.** Dans la liste déroulante **Mot de passe d'activation**, choisissez de définir le mot de passe ou de le générer automatiquement. **c.** Vous pouvez également modifier le champ Expiration de la période d'activation. Ce champ spécifie la durée de validité du mot de passe d'activation. **d.** Pour que le mot de passe d'activation ne s'applique qu'à une seule activation, sélectionnez **La période d'activation expire à l'issue de l'activation du premier terminal**. **e.** Dans la liste déroulante **Modèle d'e-mail d'activation**, sélectionnez le modèle à utiliser pour l'e-mail d'activation.

Tâche	Étapes
Associez un mot de passe d'activation à un profil d'activation spécifique.	**a.** Dans la liste déroulante **Option d'activation**, sélectionnez **Activation du terminal avec un profil d'activation spécifique**. **b.** Dans la liste déroulante **Profil d'activation**, sélectionnez le profil d'activation auquel vous souhaitez associer un mot de passe. **c.** Dans la liste déroulante **Mot de passe d'activation**, choisissez de définir le mot de passe ou de le générer automatiquement. **d.** Vous pouvez également modifier le champ Expiration de la période d'activation. Ce champ spécifie la durée de validité du mot de passe d'activation. **e.** Pour que le mot de passe d'activation ne s'applique qu'à une seule activation, sélectionnez **La période d'activation expire à l'issue de l'activation du premier terminal**. **f.** Dans la liste déroulante **Modèle d'e-mail d'activation**, cliquez sur un modèle à utiliser pour l'e-mail d'activation.
Autoriser les utilisateurs à activer uniquement les applications BlackBerry Dynamics	**a.** Dans la liste déroulante **Option d'activation**, sélectionnez **Génération d'une clé d'accès BlackBerry Dynamics**. **b.** Dans la liste déroulante **Nombre de clés d'accès à générer**, sélectionnez le nombre de clés. Chaque clé ne peut être utilisée qu'une seule fois pour activer une application BlackBerry Dynamics. **c.** Sélectionnez le nombre de jours de validité de la clé d'accès. **d.** Dans la liste déroulante **Modèle d'e-mail d'activation**, cliquez sur un modèle à utiliser pour l'e-mail d'activation.
Ajoutez un utilisateur à BlackBerry UEM uniquement.	**a.** Dans la liste déroulante **Option d'activation**, sélectionnez **Ne pas définir**.

9. Si le domaine BlackBerry UEM prend en charge les terminaux BlackBerry OS (versions 5.0 à 7.1), pour activer un terminal BlackBerry pour un utilisateur d'annuaire, procédez comme suit :
   a) Cochez la case **Autoriser un utilisateur à activer un terminal BlackBerry OS**.
   b) Dans la liste déroulante **Serveur de messagerie BlackBerry OS**, cliquez sur le nom d'un serveur.

   Remarque : l'utilisateur d'annuaire doit être présent sur le serveur de messagerie professionnel auquel se connecte le serveur de messagerie BlackBerry OS.
10. Si vous utilisez des variables personnalisées, développez **Variables personnalisées** et spécifiez les valeurs appropriées pour les variables que vous avez définies.
11. Effectuez l'une des opérations suivantes :
    - Pour enregistrer le compte d'utilisateur, cliquez sur **Enregistrer**.
    - Pour enregistrer le compte d'utilisateur et en créer un autre, cliquez sur **Enregistrer et ajouter nouveau**.

Concepts connexes

Permettre aux utilisateurs d'activer des terminaux utilisant des types d'activation différents
Modèles d'e-mail

Référence connexe

Variables personnalisées

Création de comptes d'utilisateur à partir d'un fichier .csv

Vous pouvez manuellement créer le fichier .csv à l'aide du modèle de fichier .csv BlackBerry UEM, disponible au téléchargement dans l'onglet Importer de la fenêtre Ajouter un utilisateur.

À propos du fichier .csv de comptes d'utilisateur

Vous pouvez importer des comptes utilisateur au format fichier .csv dans BlackBerry UEM pour créer simultanément plusieurs comptes utilisateur. Selon vos besoins, vous pouvez également spécifier l'appartenance à un groupe et les paramètres d'activation des comptes d'utilisateur en incluant les colonnes suivantes dans le fichier .csv :

En-tête de colonne	Description
Appartenance à un groupe	Attribuez un ou plusieurs groupes d'utilisateurs à chaque compte d'utilisateur. Utilisez un point-virgule (;) pour séparer plusieurs groupes utilisateur. Si vous n'incluez pas la colonne « Appartenance à un groupe », lorsque vous importez le fichier, vous avez la possibilité de sélectionner le groupe auquel vous souhaitez ajouter tous les comptes d'utilisateur importés. Si vous souhaitez attribuer chaque compte d'utilisateur à un groupe d'utilisateurs spécifique, vous pouvez utiliser cette colonne avant d'importer le fichier.
MDM (BlackBerry UEM)	Précisez si l'utilisateur est activé pour MDM. Pour activer un utilisateur pour MDM, saisissez « Activé ».
Mot de passe d'activation	Saisissez le mot de passe d'activation. Cette valeur est obligatoire si le paramètre Génération du mot de passe d'activation est défini sur Manuelle.
Modèle d'activation	Entrez le nom du modèle d'e-mail d'activation que vous souhaitez envoyer à l'utilisateur. Si vous n'indiquez pas de nom, le modèle d'activation par e-mail par défaut est utilisé.
Expiration du mot de passe d'activation	Saisissez, en secondes, la durée de validité du mot de passe d'activation arrivée à expiration.
Génération du mot de passe d'activation	Saisissiez un des éléments suivants : • Auto Le mot de passe d'activation est automatiquement créé et envoyé à l'utilisateur. • Manuelle Le mot de passe d'activation est défini dans la colonne « Mot de passe d'activation ». Si la valeur est vierge, la valeur par défaut est Auto.

En-tête de colonne	Description
Envoyer un e-mail d'activation	Saisissiez un des éléments suivants : • Vrai. L'e-mail d'activation est envoyé à l'utilisateur. • Faux. L'e-mail d'activation n'est pas envoyé à l'utilisateur. Si le paramètre Génération du mot de passe d'activation est défini sur Auto, l'e-mail d'activation est envoyé à l'utilisateur quelle que soit la valeur de cette colonne. Si le paramètre Génération du mot de passe d'activation est défini sur Manuelle et que cette valeur est vide, la valeur par défaut est Vrai.
Type d'utilisateur	Cette colonne est nécessaire chaque fois que le fichier .csv comprend des comptes locaux et des comptes d'utilisateur associés à l'annuaire. Saisissiez un des éléments suivants : • L pour comptes d'utilisateur locaux • D pour comptes d'utilisateur associés à l'annuaire Les entrées ne sont pas sensibles à la casse.
UID de l'annuaire	(Facultatif) Alternative à la saisie d'une adresse électronique pour les comptes d'utilisateur associés à l'annuaire. Par défaut, l'adresse électronique est utilisée pour valider les comptes d'utilisateur associés à l'annuaire, mais vous pouvez indiquer que l'UID de l'annuaire sera utilisé. Si le compte d'utilisateur ne peut pas être validé par l'UID de l'annuaire, une erreur est signalée. Si vous incluez une valeur UID de l'annuaire pour l'un de vos utilisateurs, l'en-tête de colonne doit inclure l'UID de l'annuaire et toutes les lignes du fichier .csv doivent comporter soit un UID de l'annuaire soit un espace réservé vide pour la colonne UID de l'annuaire.

Pour obtenir un exemple de fichier .csv, cliquez sur **Utilisateurs > Tous les utilisateurs > Ajouter un utilisateur > Importer > Télécharger un modèle de fichier .csv**.

Comment BlackBerry UEM valide le fichier .csv des comptes d'utilisateur

BlackBerry UEM valide le fichier .csv des comptes d'utilisateur avant, pendant et immédiatement après le chargement fichier .csv et signale toutes les erreurs rencontrées.

Voici quelques-unes des erreurs qui empêchent BlackBerry UEM de charger le fichier .csv :

- Format de fichier ou extension de fichier non valide
- Fichier vide
- Le nombre de colonnes ne correspond pas au nombre d'en-têtes dans le fichier

Lorsque BlackBerry UEM rencontre une erreur, il arrête de charger le fichier et affiche un message d'erreur. Vous devez corriger cette erreur et recharger le fichier .csv.

Une fois le fichier .csv chargé, BlackBerry UEM affiche la liste des comptes d'utilisateur qui seront importés et, le cas échéant, les comptes d'utilisateur associés à l'annuaire qui ne seront pas importés suite à une erreur (entrée dupliquée ou adresse électronique incorrecte). Vous pouvez effectuer l'une des actions suivantes :

- Annuler l'opération, corriger les erreurs, puis recharger le fichier .csv.

- Continuer et charger les comptes d'utilisateur valides. Les comptes d'utilisateur associés à l'annuaire comportant des erreurs ne sont pas chargés. Vous devez copier et corriger les comptes d'utilisateur associés à l'annuaire qui n'ont pas été chargés dans un fichier .csv distinct. En effet, le rechargement du même fichier .csv créera des erreurs de duplication au niveau des comptes d'utilisateur correctement chargés précédemment.

BlackBerry UEM effectue une validation finale des comptes d'utilisateur importés juste avant de créer les comptes d'utilisateur afin de vérifier qu'aucune erreur n'est survenue lors de l'importation du fichier (autre utilisateur créant un compte d'utilisateur sous forme de fichier .csv contenant le même compte d'utilisateur que celui importé, par exemple).

Ajouter des comptes d'utilisateur à l'aide d'un fichier .csv

Pour un exemple de fichier .csv, reportez-vous à la section À propos du fichier .csv de comptes d'utilisateur.

Avant de commencer :

- Si le fichier .csv contient des comptes d'utilisateur associés à l'annuaire, vérifiez que BlackBerry UEM est connecté à votre annuaire d'entreprise.
- Vérifiez que le nombre de colonnes correspond au nombre d'en-têtes du fichier .csv.
- Vérifiez que les colonnes obligatoires sont incluses.
- Vérifiez que les informations des colonnes sont correctes.

1. Sur la barre de menus, cliquez sur **Utilisateurs**.
2. Sélectionnez l' **ensemble des utilisateurs** ou l' **onglet appareils gérés** .
3. Cliquez sur **Ajouter un utilisateur**.
4. Cliquez sur l'onglet **Importer**.
5. Cliquez sur **Parcourir** et accédez au fichier .csv contenant les comptes d'utilisateur que vous souhaitez ajouter.
6. Cliquez sur **Charger**.
7. Si des erreurs ont été signalées, procédez comme suit :
   a) Corrigez les erreurs dans le fichier .csv.
   b) Cliquez sur **Parcourir** et accédez au fichier .csv.
   c) Cliquez sur **Charger**.
   d) Répétez l'étape 6 jusqu'à ce que toutes les erreurs soient corrigées.
8. Si le fichier .csv n'utilise pas la colonne « Appartenance à un groupe » et que des groupes locaux sont présents dans BlackBerry UEM, procédez comme suit pour ajouter des comptes d'utilisateur aux groupes :
   a) Dans la liste **Groupes disponibles**, sélectionnez un ou plusieurs groupes, puis cliquez sur ➡.
   b) Cliquez sur **Suivant**.

   Lorsque vous importez le fichier .csv, tous les comptes d'utilisateur sont ajoutés aux groupes locaux que vous sélectionnez. Si le compte d'utilisateur est membre d'un groupe lié par annuaire, il est automatiquement associé à ce groupe lors de la synchronisation entre BlackBerry UEM et votre annuaire d'entreprise.

   Pour ajouter des comptes d'utilisateur à des groupes auxquels a été attribué un rôle administratif, vous devez être Administrateur de sécurité.
9. Examinez la liste des comptes d'utilisateur et effectuez l'une des opérations suivantes :
   - Pour corriger les erreurs liées aux comptes d'utilisateur associés à l'annuaire non valides, cliquez sur **Annuler** et passez à l'étape 6.
   - Pour ajouter les comptes d'utilisateur valides, cliquez sur **Importer**. Les comptes d'utilisateur associés à l'annuaire non valides sont ignorés.

À la fin : si le domaine BlackBerry UEM prend en charge les terminaux BlackBerry OS (versions 5.0 à 7.1), pour activer l'activation des terminaux BlackBerry OS pour les comptes d'utilisateur associés à l'annuaire, procédez comme suit :

Tâches connexes

Modifier les informations de compte d'utilisateur

Afficher un compte d'utilisateur

Vous pouvez afficher des informations sur un compte d'utilisateur dans l'onglet Synthèse. Par exemple, vous pouvez consulter les informations suivantes :

- Terminaux activés
- Groupes d'utilisateurs auxquels appartient un compte d'utilisateur
- Stratégie informatique attribuée, profils et applications

1. Sur la barre de menus, cliquez sur **Utilisateurs**.
2. Recherchez un compte d'utilisateur à l'aide de l'une des options suivantes :
   - Cliquez sur **Tous les utilisateurs** et saisissez votre recherche dans le champ **Rechercher**.
   - Cliquez sur **Terminaux gérés > Recherche d'utilisateur** et saisissez du texte dans le champ de recherche.
3. Dans les résultats de la recherche, cliquez sur le nom du compte d'utilisateur.

Ajouter des notes à un compte d'utilisateur

Vous pouvez ajouter des notes pour garder une trace de toute information liée à un compte utilisateur spécifique. La note d'informations est enregistrée avec le compte utilisateur et non avec le terminal individuel. Si l'utilisateur est supprimé, les informations du champ Notes sont également supprimées. L'utilisation de la fonction Notes est soumise à l'autorisation « Modifier les utilisateurs » des administrateurs.

1. Sur la barre de menus, cliquez sur **Utilisateurs**.
2. Recherchez un compte d'utilisateur.
3. Dans les résultats de la recherche, cliquez sur le nom d'un compte d'utilisateur.
4. Cliquez sur l'icône **Ajouter une note** dans l'angle supérieur droit.
5. Saisissez les notes dans la boîte de dialogue qui s'ouvre. Les notes que vous saisissez sont automatiquement enregistrées et l'icône est modifiée pour indiquer la présence de notes.

Gestion simultanée de plusieurs comptes utilisateur

Vous pouvez effectuer certaines actions pour plusieurs utilisateurs à la fois. Par exemple, vous pouvez envoyer un e-mail au groupe d'utilisateurs de votre choix.

Avant de commencer : Configuration de la vue par défaut ou avancée.

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

Icône	Description
	Envoyer un e-mail aux utilisateurs
	Envoyer un e-mail d'activation à plusieurs utilisateurs
	Ajouter des utilisateurs à des groupes d'utilisateurs
	Exportation d'une liste d'utilisateurs vers un fichier .csv
	Envoyer un mot de passe BlackBerry UEM Self-Service à plusieurs utilisateurs

Envoyer un e-mail aux utilisateurs

Vous pouvez envoyer un e-mail à un ou plusieurs utilisateurs directement depuis la console de gestion. Les utilisateurs doivent posséder une adresse électronique associée à leur compte.

L'e-mail est envoyé depuis l'adresse électronique que vous avez configurée dans les paramètres de serveur SMTP.

Avant de commencer : pour envoyer un e-mail à plusieurs utilisateurs, vous devez disposer d'un rôle administratif possédant l'autorisation Envoyer un e-mail aux utilisateurs.

1. Sur la barre de menus, cliquez sur **Utilisateurs**.
2. Sélectionnez l'onglet **Tous les utilisateurs** ou **Terminaux gérés**.
3. Effectuez l'une des tâches suivantes :

Tâche	Étapes
Envoyer un e-mail à un utilisateur	**a.** Recherchez un compte d'utilisateur. **b.** Dans les résultats de la recherche, cliquez sur le nom du compte d'utilisateur. **c.** Cliquez sur  . **d.** Vous pouvez également cliquer sur **CC** et saisir une ou plusieurs adresses électroniques (séparées par des virgules ou des points-virgules) pour mettre en copie l'e-mail à vous-même ou à d'autres personnes.
Envoyer des e-mails à plusieurs utilisateurs	**a.** Cochez la case pour chaque utilisateur auquel vous souhaitez envoyer un e-mail. **b.** Cliquez sur  . **c.** Vous pouvez également cliquer sur **À** ou **CC** et saisir une ou plusieurs adresses électroniques (séparées par des virgules ou des points-virgules) pour envoyer ou mettre en copie l'e-mail à vous-même ou à d'autres personnes.

4. Saisissez un objet et un message.
5. Cliquez sur **Envoyer**.

Modifier les informations de compte d'utilisateur

Vous pouvez modifier les informations utilisateur suivantes :

- Nom, nom d'utilisateur, nom d'affichage et adresse électronique
- Appartenance aux groupes (L'appartenance aux groupes liés par répertoire ne peut pas être modifiée.)
- Mot de passe de compte pour les comptes d'utilisateur locaux
- Rôle d'utilisateur
- Si vous avez défini des variables personnalisées, vous pouvez modifier les informations de ces variables.
- Si le domaine BlackBerry UEM prend en charge les terminaux BlackBerry OS (versions 5.0 à 7.1), vous pouvez activer ou désactiver l'activation des terminaux BlackBerry OS des comptes d'utilisateur associés à l'annuaire. Vous pouvez désactiver l'activation du terminal BlackBerry uniquement si l'utilisateur n'a pas activé de terminal BlackBerry.

Remarque : Vous ne pouvez pas modifier les détails de l'utilisateur administrateur par défaut ni des utilisateurs qui utilisent leurs BlackBerry informations d'identification de compte.

1. Sur la barre de menus, cliquez sur **Utilisateurs > Terminaux gérés**.
2. Recherchez un compte d'utilisateur.
3. Dans les résultats de la recherche, cliquez sur le nom du compte d'utilisateur.
4. Cliquez sur  .
5. Modifiez les informations du compte d'utilisateur.
6. Cliquez sur **Enregistrer**.

Synchroniser des informations pour un utilisateur d'annuaire

Si vous avez ajouté un compte d'utilisateur à partir de votre annuaire d'entreprise, vous pouvez synchroniser manuellement les informations de cet utilisateur avec votre annuaire d'entreprise, sans attendre la synchronisation automatique.

1. Sur la barre de menus, cliquez sur **Utilisateurs**.
2. Sélectionnez l' **ensemble des utilisateurs** ou l' **onglet appareils gérés** .
3. Recherchez un compte d'utilisateur.
4. Dans les résultats de la recherche, cliquez sur le nom du compte d'utilisateur.
5. Cliquez sur  .

Modifier la synchronisation des données de l'organiseur et la configuration de la messagerie pour un utilisateur de terminal BlackBerry OS

Dans les paramètres avancés de l'onglet Synthèse, vous pouvez modifier les paramètres de synchronisation des données de l'organiseur pour un compte d'utilisateur. Vous pouvez également gérer le transfert de messages, contrôler les dossiers qu'un utilisateur peut synchroniser avec un terminal BlackBerry OS et gérer les signatures et les clauses de non-responsabilité des e-mails.

1. Sur la barre de menus, cliquez sur **Utilisateurs**.
2. Recherchez un compte d'utilisateur.
3. Dans les résultats de la recherche, cliquez sur le nom du compte d'utilisateur.
4. Dans la section **Stratégie informatique, profils et configurations logicielles**, cliquez sur **Paramètres avancés.**
5. Cliquez sur **Modifier l'utilisateur**.
6. Dans la section **Configuration de la messagerie**, cliquez sur **Configuration par défaut** .
7. Apportez des modifications sur les onglets correspondants.

8. Cliquez sur **Accéder à l'écran de modification des informations utilisateur** .
9. Cliquez sur **Enregistrer tout**.

Suppression de services pour un utilisateur

Si BlackBerry UEM est activé pour un ou plusieurs services à valeur ajoutée et qu'un utilisateur est activé pour un service, vous pouvez supprimer ce service pour cet utilisateur. Vous pouvez également supprimer des commandes MDM, sans pour autant supprimer le compte d'utilisateur dans BlackBerry UEM.

Avant de commencer :

- Avant de pouvoir supprimer des commandes MDM, vous devez supprimer les terminaux activés pour un utilisateur.
- Avant de pouvoir supprimer le service Enterprise Identity, vous devez supprimer toutes les attributions de Enterprise Identity.

1. Sur la barre de menus, cliquez sur **Utilisateurs > Tous les utilisateurs**.
2. Recherchez un compte d'utilisateur.
3. Dans les résultats de la recherche, cliquez sur le nom du compte d'utilisateur.
4. Cliquez sur ⛔.
5. Effectuez l'une des tâches suivantes :

Tâche	Étapes
Supprimer des services MDM	a. Cliquez sur ⛔ sur les terminaux gérés. b. Cliquez sur **Enregistrer**.
Supprimer un service Workspaces	a. Cliquez sur ⛔ sur Workspaces. b. Dans la boite de dialogue **Supprimer WatchDox by BlackBerry**, sélectionnez l'une des options suivantes : • Supprimer tous les fichiers appartenant à cet utilisateur et supprimer l'utilisateur de tous les groupes et listes de distribution de l'espace de travail • Transférer les fichiers et l'adhésion des groupes et des listes de distribution de l'espace Travail à une autre adresse électronique Dans le champ **Adresse électronique**, saisissez une adresse électronique. Un nouveau compte d'utilisateur est créé si l'adresse électronique n'est pas associée à un compte d'utilisateur existant. c. Cliquez sur **Supprimer**.
Supprimer un service Enterprise Identity	a. Cliquez sur ⛔ sur Enterprise Identity. b. Cliquez sur **Enregistrer**.

À la fin : Pour activer un service, consultez Activation des services pour un utilisateur.

Activation des services pour un utilisateur

Si BlackBerry UEM est activé pour un ou plusieurs services à valeur ajoutée, vous pouvez activer un service pour un utilisateur.

1. Sur la barre de menus, cliquez sur **Utilisateurs > Tous les utilisateurs**.

2. Recherchez un compte d'utilisateur.
3. Dans les résultats de la recherche, cliquez sur le nom du compte d'utilisateur.
4. Effectuez l'une des tâches suivantes :

Tâche	Étapes
Activer les services MDM	a. Cliquez sur + dans Terminaux gérés. b. Si des groupes locaux existent dans BlackBerry UEM et que vous souhaitez ajouter le compte d'utilisateur à des groupes, sélectionnez un ou plusieurs groupes dans la liste **Groupes disponibles**, puis cliquez sur →. c. Choisissez une option pour le mot de passe d'activation du terminal. d. Cliquez sur **Enregistrer**.
Activer le service Workspaces	a. Cliquez sur + dans Workspaces. b. Attribuez des rôles Workspaces. c. Cliquez sur **Enregistrer**.
Activer le service Enterprise Identity	a. Cliquez sur + dans Enterprise Identity. b. Sélectionnez des groupes d'applications. c. Cliquez sur **Attribuer**.

Supprimer un compte d'utilisateur

Lorsque vous supprimez un compte d'utilisateur, les données professionnelles sont également supprimées de tous les terminaux de l'utilisateur.

Avant de commencer :

- Désactivez tous les terminaux associés au compte d'utilisateur que vous souhaitez supprimer.
- Supprimez tous les services associés au compte d'utilisateur que vous souhaitez supprimer. Pour plus d'informations, reportez-vous à Suppression de services pour un utilisateur.

1. Sur la barre de menus, cliquez sur **Utilisateurs > Terminaux gérés**.
2. Recherchez un compte d'utilisateur.
3. Dans les résultats de la recherche, sélectionnez le nom d'un compte d'utilisateur.
4. Cliquez sur 🗑.
5. Cliquez sur **Supprimer**.

Concepts connexes

Désactivation des terminaux

Ajouter des utilisateurs à des groupes d'utilisateurs

Remarque : pour ajouter un utilisateur auquel a été attribué un rôle administratif à un groupe d'utilisateurs, vous devez être Administrateur de sécurité.

1. Sur la barre de menus, cliquez sur **Utilisateurs > Terminaux gérés**.
2. Cochez la case en regard des utilisateurs que vous souhaitez ajouter aux groupes d'utilisateurs.

3. Cliquez sur .
4. Dans la liste **Groupes disponibles**, sélectionnez un ou plusieurs groupes, puis cliquez sur .

   Remarque : l'appartenance aux groupes de répertoires associés ne peut pas être modifiée.
5. Cliquez sur **Enregistrer**.

Supprimer un utilisateur d'un groupe d'utilisateurs

Vous ne pouvez pas supprimer un utilisateur d'un groupe lié par annuaire.

Remarque : pour supprimer un utilisateur doté d'un rôle administratif d'un groupe d'utilisateurs, vous devez être Administrateur de sécurité.

1. Sur la barre de menus, cliquez sur **Groupes**.
2. Recherchez le groupe d'utilisateurs que vous souhaitez modifier.
3. Cliquez sur le groupe d'utilisateurs.
4. Recherchez l'utilisateur que vous souhaitez supprimer.
5. Sélectionnez l'utilisateur.
6. Cliquez sur .

Modifier les groupes auxquels appartient un utilisateur

Remarque : pour modifier les groupes d'utilisateurs auquel appartient un utilisateur doté d'un rôle administratif, vous devez être Administrateur de sécurité.

1. Sur la barre de menus, cliquez sur **Utilisateurs > Terminaux gérés**.
2. Recherchez un compte d'utilisateur.
3. Dans les résultats de la recherche, cliquez sur le nom du compte d'utilisateur.
4. Dans la section **Appartenance à un groupe**, cliquez sur .
5. Effectuez l'une des actions suivantes :
   - Pour ajouter l'utilisateur aux groupes d'utilisateurs, dans la liste **Groupes disponibles**, sélectionnez un ou plusieurs groupes et cliquez sur .
   - Pour supprimer l'utilisateur des groupes d'utilisateurs, dans la liste **Membre de groupes**, sélectionnez un ou plusieurs groupes et cliquez sur .

   Remarque : l'appartenance aux groupes de répertoires associés ne peut pas être modifiée.
6. Cliquez sur **Enregistrer**.

Attribuer un profil ou une stratégie informatique à un compte d'utilisateur

1. Sur la barre de menus, cliquez sur **Utilisateurs > Terminaux gérés**.
2. Recherchez un compte d'utilisateur.
3. Dans les résultats de la recherche, cliquez sur le nom du compte d'utilisateur.
4. Dans la section **Stratégie informatique et profils**, cliquez sur .
5. Cliquez sur **Stratégie informatique** ou sur un type de profil.
6. Dans la liste déroulante, cliquez sur le nom du profil ou de la stratégie informatique que vous souhaitez attribuer à l'utilisateur.
7. Pour les stratégies informatiques et les types de profils classés, si le type de profil que vous avez sélectionné à l'étape 5 est déjà directement attribué à l'utilisateur, cliquez sur **Remplacer**. Sinon, cliquez sur **Attribuer**.

Concepts connexes

Comment BlackBerry UEM choisit la stratégie informatique à attribuer
Attribution de profils
Comment BlackBerry UEM choisit les profils à attribuer

Tâches connexes

Créer une stratégie informatique
Créer un profil de configuration logicielle minimale requise du terminal pour les terminaux BlackBerry 10
Attribuer un profil ou une stratégie informatique à un groupe d'utilisateurs

Ajouter un certificat client à un compte d'utilisateur

Vous pouvez ajouter un certificat client à un compte d'utilisateur individuel et envoyer ce certificat aux terminaux BlackBerry Dynamics activés ou à d'autres terminaux iOS et Android gérés.

Ajoutez des certificats client aux comptes d'utilisateurs lorsque les terminaux des utilisateurs ont besoin de certificats pour S/MIME ou l'authentification des clients et que le certificat ne peut pas être envoyé aux terminaux par le biais d'un profil d'informations d'identification de l'utilisateur ou d'un profil SCEP.

Le certificat client doit porter une extension .pfx ou .p12. Vous pouvez envoyer plusieurs certificats client aux terminaux.

Vous pouvez également utiliser les profils d'informations d'identification de l'utilisateur pour charger les certifications des utilisateurs individuels. Les profils d'informations d'identification de l'utilisateur peuvent être associés à un profil Wi-Fi, VPN ou de messagerie.

1. Sur la barre de menus, cliquez sur **Utilisateurs > Terminaux gérés**.
2. Recherchez un compte d'utilisateur.
3. Dans les résultats de la recherche, cliquez sur le nom d'un compte d'utilisateur.
4. Dans la section **Stratégie informatique et profils**, cliquez sur +.
5. Cliquez sur **Certificat utilisateur**.
6. Saisissez la description du certificat.
7. Dans la section **Appliquer le certificat à**, sélectionnez l'un des éléments suivants :
   - **Autres terminaux gérés** : choisissez cette option pour envoyer le certificat aux terminaux iOS et Android pour tous les usages pris en charge autres que pour des applications BlackBerry Dynamics.
   - **Terminaux BlackBerry Dynamics activés** : choisissez cette option pour envoyer le certificat aux terminaux aux fins d'utilisation avec des applications BlackBerry Dynamics.
8. Dans le champ **Fichier de certificat**, cliquez sur **Parcourir** pour localiser le fichier de certificat.
9. Si vous avez sélectionné **Autres terminaux gérés**, dans le champ **Mot de passe**, saisissez un mot de passe pour le certificat. Pour les terminaux iOS, un mot de passe est requis. Pour les terminaux Android, vous n'avez pas à fournir de mot de passe dans BlackBerry UEM si le terminal exécute la version la plus récente de BlackBerry UEM Client. Si vous ne définissez aucun mot de passe, l'utilisateur doit saisir le mot de passe du terminal.
10. Cliquez sur **Ajouter**.
    Le certificat est répertorié dans le tableau **Certificats utilisateur** sur la page de résumé de l'utilisateur.

À la fin :

- Pour les terminaux BlackBerry Dynamics activés, configurez la durée pendant laquelle les certificats chargés restent sur le serveur BlackBerry UEMavant d'être supprimés automatiquement du serveur. Le paramètre par défaut est 24 heures.

Concepts connexes

Envoi de certificats aux terminaux à l'aide de profils

Modifier un certificat client pour un compte d'utilisateur

1. Sur la barre de menus, cliquez sur **Utilisateurs > Terminaux gérés**.
2. Recherchez un compte d'utilisateur.
3. Dans les résultats de la recherche, cliquez sur le nom d'un compte d'utilisateur.
4. Dans la section **Profils et stratégies informatiques**, cliquez sur le certificat d'utilisateur que vous souhaitez modifier.
5. Cliquez sur .
6. Procédez aux modifications nécessaires. Vous ne pouvez pas modifier les terminaux auxquels le certificat s'applique.
7. Cliquez sur **Enregistrer**.

À la fin : Si vous modifiez un certificat d'utilisateur BlackBerry Dynamics que vous ou un utilisateur a supprimé d'un terminal, le certificat est renvoyé au terminal.

Renouveler ou supprimer un certificat BlackBerry Dynamics pour un compte d'utilisateur

Vous pouvez envoyer une commande au terminal d'un utilisateur pour demander le renouvellement du certificat de l'AC. Vous pouvez également supprimer un certificat BlackBerry Dynamics du terminal d'un utilisateur. Si vous supprimez un certificat, le connecteur PKI BlackBerry Dynamics envoie une notification à l'AC indiquant que le certificat n'est plus utilisé, mais le certificat n'est pas automatiquement révoqué.

1. Sur la barre de menus, cliquez sur **Utilisateurs > Terminaux gérés**.
2. Recherchez un compte d'utilisateur.
3. Dans les résultats de la recherche, cliquez sur le nom d'un compte d'utilisateur.
4. Effectuez l'une des opérations suivantes dans la section **Certificats utilisateur** :
   - Cliquez sur Pour demander le renouvellement du certificat à partir de l'AC.
   - Cliquez sur pour envoyer le certificat à partir des terminaux de l'utilisateur.

   Remarque : Pour supprimer des informations d'identification intelligentes Entrust d'un terminal, l'utilisateur doit également désactiver les informations d'identification intelligentes dans BlackBerry UEM Client.

Tâches connexes

Renouveler les certificats qui sont inscrits par le biais du connecteur PKI BlackBerry Dynamics

Ajouter un certificat client à un profil d'informations d'identification de l'utilisateur

Vous pouvez télécharger les certificats pour les utilisateurs individuels dans un profil d'informations d'identification de l'utilisateur. Les utilisateurs peuvent également télécharger leur certificat dans le profil d'informations d'identification de l'utilisateur à l'aide de BlackBerry UEM Self-Service. Le téléchargement des certificats dans les profils d'informations d'identification de l'utilisateur est pris en charge pour les terminaux

exécutant BlackBerry 10 OS, version 10.3.1 et ultérieure, les terminaux iOS et les terminaux Android équipés d'un espace Travail.

Le certificat client doit porter une extension .pfx ou .p12. Le nouveau certificat que vous, ou un utilisateur, téléchargez dans le profil d'informations d'identification de l'utilisateur remplace le certificat existant sur les terminaux des utilisateurs.

Avant de commencer :

- Créer un profil d'informations d'identification de l'utilisateur pour télécharger manuellement les certificats.
- Attribuez le profil d'informations d'identification de l'utilisateur aux utilisateurs.

1. Sur la barre de menus, cliquez sur **Utilisateurs > Terminaux gérés**.
2. Recherchez un compte d'utilisateur.
3. Dans les résultats de la recherche, cliquez sur le nom d'un compte d'utilisateur.
4. Dans la section **Stratégie informatique et profils**, en regard du profil d'informations d'identification de l'utilisateur, cliquez sur **Ajouter un certificat**.
5. Cliquez sur **Parcourir** pour localiser le fichier de certificat.
6. Indiquez le mot de passe du certificat. Pour les terminaux iOS, le mot de passe est requis. Pour les terminaux Android, vous n'avez pas à fournir le mot de passe dans BlackBerry UEM si le terminal exécute la version la plus récente de BlackBerry UEM Client. Si vous ne spécifiez aucun mot de passe, l'utilisateur doit saisir le mot de passe du terminal.
7. Cliquez sur **Ajouter**.

Tâches connexes

Créer un profil d'informations d'identification de l'utilisateur pour télécharger manuellement les certificats

Modifier un certificat client pour un profil d'informations d'identification de l'utilisateur

Vous pouvez modifier le certificat que vous ou qu'un utilisateur a ajouté au profil d'informations d'identification de l'utilisateur. Le nouveau certificat remplace le certificat existant sur le terminal.

1. Sur la barre de menus, cliquez sur **Utilisateurs > Terminaux gérés**.
2. Recherchez un compte d'utilisateur.
3. Dans les résultats de la recherche, cliquez sur le nom d'un compte d'utilisateur.
4. Dans la section **Stratégie informatique et profils**, à la ligne du profil d'informations d'identification de l'utilisateur, cliquez sur **Mettre à jour**.
5. Cliquez sur **Parcourir** pour localiser le fichier de certificat.
6. Saisissez un mot de passe (password) pour le certificat. Pour les terminaux iOS, un mot de passe est requis. Pour les terminaux Android, vous n'avez pas à fournir le mot de passe dans BlackBerry UEM si le terminal exécute la version la plus récente de BlackBerry UEM Client. Si vous ne spécifiez aucun mot de passe, l'utilisateur doit saisir le mot de passe du terminal.
7. Cliquez sur **Enregistrer**.

Tâches connexes

Créer un profil d'informations d'identification de l'utilisateur pour télécharger manuellement les certificats

Attribuer une application à un compte d'utilisateur

Si vous devez contrôler les applications au niveau utilisateur, vous pouvez attribuer des applications ou des groupes d'applications à des comptes d'utilisateur. Lorsque vous attribuez une application à un utilisateur, celle-ci est mise à la disposition de tous les terminaux activés par l'utilisateur pour ce type de terminal et l'application est répertoriée dans le catalogue des applications professionnelles du terminal.

Vous pouvez également attribuer des applications aux utilisateurs de certains types de terminaux que l'utilisateur n'a pas encore activés. Si l'utilisateur active ultérieurement un type de terminal différent, les applications qui conviennent seront mises à la disposition du nouveau terminal.

Une même application peut être directement attribuée au compte d'utilisateur ou héritée de groupes d'utilisateurs ou de groupes de terminaux. Les paramètres de l'application (si l'application est requise, par exemple) sont attribués en fonction de la priorité : les groupes de terminaux bénéficient de la priorité la plus élevée, suivis des comptes d'utilisateur, puis des groupes d'utilisateurs.

Avant de commencer :

- Ajouter l'application à la liste des applications disponibles
- Vous pouvez également ajouter des applications à un groupe d'applications

1. Sur la barre de menus, cliquez sur **Utilisateurs > Terminaux gérés**.
2. Recherchez un compte d'utilisateur.
3. Dans les résultats de la recherche, cliquez sur le nom d'un compte d'utilisateur.
4. Dans la section **Applications**, cliquez sur +.
5. Cochez la case en regard des applications ou du groupe d'applications que vous souhaitez attribuer au compte d'utilisateur.
6. Cliquez sur **Suivant**.
7. Dans la liste déroulante **Disposition** de l'application, exécutez l'une des opérations suivantes :
   - Pour demander aux utilisateurs d'installer l'application, sélectionnez **Requis**.
   - Pour autoriser des utilisateurs à installer ou supprimer l'application, sélectionnez **Facultatif**.

     Remarque : Si la même application est attribuée à un compte d'utilisateur, un groupe d'utilisateurs auquel appartient l'utilisateur et au groupe de terminaux auquel appartient le terminal, la disposition de l'application attribuée au groupe de terminaux est prioritaire.
8. Pour les terminaux iOS, pour attribuer des paramètres VPN par application à une application ou à un groupe d'applications, dans la liste déroulante **VPN par application** de l'application ou du groupe d'applications, sélectionnez les paramètres à lui associer.
9. Pour les terminaux iOS et Android, si une configuration d'application est disponible, sélectionnez-la pour l'attribuer à l'application.
10. Si vous ajoutez une application iOS, effectuez l'une des tâches suivantes :

Tâche	Étapes
Si vous n'avez pas ajouté de compte PPV ou n'ajoutez pas d'application iOS	**a.** Cliquez sur **Attribuer**.

Tâche	Étapes
Si vous ajoutez une application iOS et avez ajouté au moins un compte PPV	**a.** Cliquez sur **Suivant**. **b.** Sélectionnez **Oui** si vous souhaitez attribuer une licence à l'application iOS. Sélectionnez **Non** si vous ne souhaitez pas attribuer une licence à l'application ou n'avez pas de licence à lui attribuer. **c.** Si vous avez attribué une licence à l'application, dans la liste déroulante **Licence d'application**, sélectionnez le compte VPP à associer à l'application. **d.** Dans la liste déroulante **Attribuer une licence à**, attribuez la licence à l'**utilisateur** ou au **terminal**. Si aucune valeur n'est spécifiée dans la liste déroulante **Licence d'application**, la liste déroulante **Attribuer une licence à** n'est pas disponible. **e.** Cliquez sur **Attribuer**. Les utilisateurs doivent suivre les instructions qui s'affichent pour inscrire le compte VPP de leur entreprise avant de pouvoir installer des applications prépayées. Les utilisateurs doivent effectuer cette tâche une seule fois. **Remarque :** si vous autorisez l'accès à plusieurs licences dont vous disposez, les premiers utilisateurs à accéder aux licences disponibles peuvent installer l'application. Si l'application est une application requise ne disposant pas de licence disponible, vous devez obtenir la licence avant que l'utilisateur ne puisse installer l'application et ne soit soumis à toutes les règles de conformité que vous avez attribuées aux utilisateurs.

Référence connexe

Comportement des applications sur les terminaux Android
Comportement des applications sur les terminaux iOS
Comportement de l'application sur les terminaux BlackBerry

Attribuer un groupe d'applications à un compte d'utilisateur

Si vous devez contrôler les applications au niveau utilisateur, vous pouvez attribuer des applications ou des groupes d'applications à des comptes d'utilisateur. Lorsque vous attribuez une application à un utilisateur, celle-ci est mise à la disposition de tous les terminaux activés par l'utilisateur pour ce type de terminal et l'application est répertoriée dans le catalogue des applications professionnelles du terminal.

Vous pouvez également attribuer des applications aux utilisateurs de certains types de terminaux que l'utilisateur n'a pas encore activés. Si l'utilisateur active ultérieurement un type de terminal différent, les applications qui conviennent seront mises à la disposition du nouveau terminal.

Une même application peut être directement attribuée au compte d'utilisateur ou héritée de groupes d'utilisateurs ou de groupes de terminaux. Les paramètres de l'application (si l'application est requise, par exemple) sont attribués en fonction de la priorité : les groupes de terminaux bénéficient de la priorité la plus élevée, suivis des comptes d'utilisateur, puis des groupes d'utilisateurs.

Avant de commencer : Ajoutez des applications à un groupe d'applications.

1. Sur la barre de menus, cliquez sur **Utilisateurs > Terminaux gérés**.
2. Recherchez un compte d'utilisateur.
3. Dans les résultats de la recherche, cliquez sur le nom d'un compte d'utilisateur.

4. Dans la section **Applications**, cliquez sur +.
5. Cochez la case en regard des applications ou du groupe d'applications que vous souhaitez attribuer au compte d'utilisateur.
6. Cliquez sur **Suivant**.
7. Dans la liste déroulante **Disposition** de l'application, exécutez l'une des opérations suivantes :
   - Pour demander aux utilisateurs d'installer l'application, sélectionnez **Requis**.
   - Pour autoriser des utilisateurs à installer ou supprimer l'application, sélectionnez **Facultatif**.

   Remarque : Si la même application est attribuée à un compte d'utilisateur, un groupe d'utilisateurs auquel appartient l'utilisateur et au groupe de terminaux auquel appartient le terminal, la disposition de l'application attribuée au groupe de terminaux est prioritaire.
8. Pour les terminaux iOS, pour attribuer des paramètres VPN par application à une application ou à un groupe d'applications, dans la liste déroulante **VPN par application** de l'application ou du groupe d'applications, sélectionnez les paramètres à lui associer.
9. Si vous ajoutez une application iOS, effectuez l'une des tâches suivantes :

Tâche	Étapes
Si vous n'avez pas ajouté de compte VPP ou n'ajoutez pas d'application iOS	**a.** Cliquez sur **Attribuer**.
Si vous ajoutez une application iOS et avez ajouté au moins un compte VPP	**a.** Cliquez sur **Suivant**. **b.** Sélectionnez **Oui** si vous souhaitez attribuer une licence à l'application iOS. Sélectionnez **Non** si vous ne souhaitez pas attribuer une licence à l'application ou n'avez pas de licence à lui attribuer. **c.** Si vous avez attribué une licence à l'application, dans la liste déroulante **Licence d'application**, sélectionnez le compte VPP à associer à l'application. **d.** Dans la liste déroulante **Attribuer une licence à**, attribuez la licence à l'**utilisateur** ou au **terminal**. Si aucune valeur n'est spécifiée dans la liste déroulante **Licence d'application**, la liste déroulante **Attribuer une licence à** n'est pas disponible. **e.** Cliquez sur **Attribuer**. Les utilisateurs doivent suivre les instructions qui s'affichent pour inscrire le compte VPP de leur entreprise avant de pouvoir installer des applications prépayées. Les utilisateurs doivent effectuer cette tâche une seule fois. **Remarque :** si vous autorisez l'accès à plusieurs licences dont vous disposez, les premiers utilisateurs à accéder aux licences disponibles peuvent installer l'application. Si l'application est une application requise ne disposant pas de licence disponible, vous devez obtenir la licence avant que l'utilisateur ne puisse installer l'application et ne soit soumis à toutes les règles de conformité que vous avez attribuées aux utilisateurs.

Référence connexe

Comportement des applications sur les terminaux Android
Comportement des applications sur les terminaux iOS

Comportement de l'application sur les terminaux BlackBerry

Attribuer une stratégie informatique BlackBerry OS, un profil ou une configuration logicielle à un compte d'utilisateur

Avant de commencer :

- Vérifiez que vous avez activé l'activation du terminal BlackBerry OS pour le compte d'utilisateur. Pour plus d'informations, téléchargez le Guide d'administration sur help.blackberry.com/detectLang/bes5-for-exchange/.
- Créez une stratégie informatique BlackBerry OS.
- Créez une configuration logicielle.
- Créez un profil Wi-Fi ou VPN pour les terminaux BlackBerry OS. Pour plus d'informations, téléchargez le Guide d'administration sur help.blackberry.com/detectLang/bes5-for-exchange/.
- Créez une règle de contrôle d'accès Push ou Pull pour les terminaux BlackBerry OS. Pour plus d'informations, téléchargez le Guide d'administration sur help.blackberry.com/detectLang/bes5-for-exchange/.

1. Sur la barre de menus, cliquez sur **Utilisateurs**.
2. Recherchez un compte d'utilisateur.
3. Dans les résultats de la recherche, cliquez sur le nom du compte d'utilisateur.
4. Dans la section **Stratégie informatique, profils et configurations logicielles**, cliquez sur +.
5. Cliquez sur **Stratégie informatique**, **Wi-Fi**, **VPN**, **Règle de contrôle d'accès Push**, **Règle Pull de contrôle d'accès** ou **Configuration logicielle**.
6. Dans la liste déroulante, cliquez sur le nom de la stratégie informatique, du profil, de la règle de contrôle d'accès ou de la configuration logicielle que vous souhaitez attribuer à l'utilisateur.
7. Cliquez sur **Attribuer**.

Concepts connexes

Contrôle des fonctionnalités du terminal BlackBerry OS à l'aide de stratégies informatiques

Tâches connexes

Attribuer une stratégie informatique BlackBerry OS, un profil ou une configuration logicielle à un groupe d'utilisateurs

Afficher les règles de stratégies informatiques BlackBerry OS résolues attribuées à un compte d'utilisateur

Si un utilisateur est membre de plusieurs groupes d'utilisateurs dotés de stratégies informatiques BlackBerry OS différentes, BlackBerry UEM résout les stratégies informatiques ou paramètres de règle de stratégie informatique en conflit à l'aide de la méthode de réconciliation que vous avez spécifiée dans les paramètres BlackBerry OS. Vous pouvez afficher les résultats de la réconciliation des stratégies informatiques BlackBerry OS et les paramètres résolus pour chaque règle dans les paramètres avancés de l'onglet Synthèse. Si une règle de stratégie informatique est identique dans plusieurs stratégies informatiques BlackBerry OS appliquées au compte d'utilisateur, les résultats n'affichent pas la règle de stratégie informatique.

1. Sur la barre de menus, cliquez sur **Utilisateurs**.
2. Recherchez un compte d'utilisateur.
3. Dans les résultats de la recherche, cliquez sur le nom du compte d'utilisateur.
4. Dans la section **Stratégie informatique, profils et configurations logicielles**, cliquez sur **Paramètres avancés.**
5. Cliquez sur l'onglet **Stratégies**.

6. Dans la section **Nom de la stratégie informatique résolue**, cliquez sur le nom de la stratégie informatique BlackBerry OS.

Envoyer un mot de passe BlackBerry UEM Self-Service à plusieurs utilisateurs

Vous pouvez envoyer un mot de passe UEM Self-Service à plusieurs utilisateurs à la fois. Les mots de passe sont générés de manière aléatoire et envoyés aux utilisateurs par e-mail.

L'e-mail est envoyé depuis l'adresse électronique que vous avez configurée dans les paramètres de serveur SMTP.

1. Sur la barre de menus, cliquez sur **Utilisateurs > Terminaux gérés**.
2. Sélectionnez les utilisateurs auxquels vous souhaitez envoyer le mot de passe UEM Self-Service. Notez que les utilisateurs doivent posséder une adresse électronique associée à leurs comptes.
3. Cliquez sur  .
4. Cliquez sur **Continuer**.

Création et gestion de groupes d'utilisateurs

Un groupe d'utilisateurs est un ensemble d'utilisateurs partageant des propriétés communes. L'administration d'utilisateurs sous forme de groupe est plus efficace que l'administration d'utilisateurs individuels car elle permet d'ajouter des propriétés, de les modifier ou de les supprimer simultanément de tous les membres du groupe.

Les utilisateurs peuvent appartenir à plusieurs groupes à la fois. Vous pouvez attribuer une stratégie informatique, des profils et des applications dans la console de gestion lorsque vous créez ou mettez à jour les paramètres d'un groupe d'utilisateurs. Si le domaine BlackBerry UEM prend en charge les terminaux BlackBerry OS (versions 5.0 à 7.1), vous pouvez également attribuer une stratégie informatique BlackBerry OS, des profils et des configurations logicielles.

Vous pouvez créer deux types de groupes d'utilisateurs :

- Les groupes de répertoires associés lient les groupes à votre annuaire d'entreprise. Seuls les comptes d'utilisateur associés à l'annuaire d'entreprise peuvent être membres d'un groupe lié par annuaire.
- Les groupes locaux sont créés et gérés dans BlackBerry UEM et peuvent se voir attribuer des comptes d'utilisateur locaux et des comptes d'utilisateur associés à l'annuaire d'entreprise.

Une fois les groupes d'utilisateurs créés, vous pouvez définir un groupe comme membre d'un autre groupe. Lorsque vous imbriquez un groupe dans un groupe d'utilisateurs, les membres du groupe imbriqué héritent des propriétés du groupe d'utilisateurs. Vous pouvez créer et gérer la structure d'imbrication dans BlackBerry UEM et imbriquer des groupes de répertoires associés et des groupes locaux dans chaque type de groupe d'utilisateurs.

Créer des groupes liés par annuaire

BlackBerry UEM vous permet de créer des groupes liés à un ou plusieurs groupes de votre annuaire d'entreprise. Ces groupes BlackBerry UEM sont appelés « groupes liés par annuaire ». Seuls les comptes d'utilisateur d'annuaire peuvent être membres d'un groupe lié par annuaire.

À l'intervalle spécifié, BlackBerry UEM synchronise automatiquement l'appartenance d'un groupe lié par annuaire avec le ou les groupes d'annuaires d'entreprise associés. Les utilisateurs qui ont été ajoutés ou supprimés du groupe d'annuaires d'entreprise sont ajoutés ou supprimés du groupe lié par annuaire.

Remarque : Lorsque des utilisateurs sont déplacés vers un groupe d'annuaires d'entreprise lié à un groupe lié par annuaire, ils sont affectés aux stratégies, profils et applications attribués à ce groupe. Lorsque des utilisateurs sont supprimés d'un groupe d'annuaires d'entreprise lié à un groupe lié par annuaire, les stratégies, profils et applications correspondants leur sont retirés.

Un groupe lié par répertoire ne peut être lié qu'à un seul répertoire d'entreprise. Par exemple, si BlackBerry UEM a deux connexions Microsoft Active Directory (A et B), et que vous créez un groupe lié par répertoire qui est relié à la connexion A, vous pouvez uniquement relier les groupes de répertoires de la connexion A. Vous devez créer de nouveaux groupes de répertoires associés pour les autres connexions à l'annuaire.

Pour activer cette fonctionnalité, reportez-vous à la section « Activer les groupes liés par annuaire » du contenu relatif à la configuration.

La synchronisation des groupes liés par annuaire n'entraine l'ajout ou la suppression d'aucun utilisateur dans BlackBerry UEM. Pour autoriser BlackBerry UEM à créer des comptes d'utilisateur lorsque de nouveaux utilisateurs d'annuaires d'entreprise sont créés, vous devez activer et configurer l'intégration. Pour plus d'informations, reportez-vous à la section « Activer l'intégration » du contenu relatif à la configuration.

Créer un groupe lié par répertoire

Avant de commencer : Activez les groupes liés par répertoire. Pour obtenir des instructions, consultez le contenu relatif à la configuration.

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

2. Cliquez sur .
3. Saisissez le nom du groupe.
4. Dans la section **Groupes liés par annuaire**, procédez comme suit :
   a) Cliquez sur +.
   b) Saisissez tout ou partie du nom du groupe d'annuaires d'entreprise que vous souhaitez lier.
   c) Si vous disposez de plusieurs connexions au répertoire d'entreprise, sélectionnez la connexion que vous souhaitez rechercher. Lorsque c'est chose faite, le groupe lié par répertoire est définitivement associé à la connexion sélectionnée.
   d) Cliquez sur .
   e) Sélectionnez le groupe d'annuaires d'entreprise dans la liste des résultats de la recherche.
   f) Cliquez sur **Ajouter**. Le groupe d'annuaires d'entreprise s'affiche dans la liste et la connexion à un annuaire d'entreprise auquel le groupe est lié s'affiche en regard du titre de la section.
   g) Si nécessaire, cochez la case **Relier les groupes imbriqués**. Vous pouvez décocher cette case pour relier tous les groupes imbriqués ou la cocher pour permettre aux paramètres de répertoire de contrôler le nombre de groupes imbriqués.
   h) Répétez ces étapes pour lier d'autres groupes.
5. Pour attribuer un rôle d'utilisateur à un groupe lié par répertoire, procédez comme suit :
   a) Dans la section **Rôle d'utilisateur**, cliquez sur +
   b) Dans la liste déroulante, cliquez sur le nom du rôle d'utilisateur que vous souhaitez attribuer au groupe.
   c) Cliquez sur **Ajouter**.
6. Pour attribuer une stratégie informatique ou un profil au groupe lié par annuaire, procédez comme suit :
   a) Dans la section **Profils et stratégies informatiques**, cliquez sur +.
   b) Cliquez sur **Stratégie informatique** ou un type de profil.
   c) Dans la liste déroulante, cliquez sur le nom de la stratégie informatique que vous souhaitez attribuer au groupe.
   d) Cliquez sur **Attribuer**.
7. Pour attribuer une application au groupe lié par annuaire, dans la section **Applications attribuées**, cliquez sur +.
8. Recherchez l'application.
9. Dans les résultats de la recherche, sélectionnez l'application.
10. Cliquez sur **Suivant**.
11. Dans la liste déroulante **Disposition** de l'application, exécutez l'une des opérations suivantes :
    - Pour installer l'application automatiquement sur les terminaux et empêcher les utilisateurs de la supprimer, cliquez sur **Requis**. Cette option n'est pas disponible pour les applications BlackBerry.
    - Pour permettre aux utilisateurs d'installer et de supprimer l'application, sélectionnez **Facultatif**.
12. Pour les terminaux iOS : si vous souhaitez attribuer des paramètres VPN par application à une application ou un groupe d'applications, sélectionnez les paramètres à associer dans la liste déroulante **VPN par application**.
13. Cliquez sur **Attribuer**.
14. Cliquez sur **Ajouter**.

Tâches connexes

Créer un groupe local

Ajouter un groupe d'annuaires d'entreprise à un groupe lié par annuaire existant

1. Sur la barre de menus, cliquez sur **Groupes**.
2. Cliquez sur le groupe lié par annuaire.
3. Cliquez sur l'onglet **Paramètres**.
4. Cliquez sur .
5. Dans la section **Groupes liés par annuaire**, cliquez sur +.
6. Saisissez le nom du groupe d'annuaires d'entreprise.
7. Cliquez sur **Rechercher**.
8. Sélectionnez le groupe d'annuaires d'entreprise dans la liste des résultats de la recherche.
9. Cliquez sur **Ajouter**.
10. Si nécessaire, sélectionnez **Relier les groupes imbriqués**.

Créer un groupe local

1. Sur la barre de menus, cliquez sur **Groupes**.
2. Cliquez sur .
3. Saisissez le nom du groupe d'utilisateurs.
4. Vous pouvez aussi entrer une description du groupe d'utilisateurs.
5. Pour attribuer un rôle d'utilisateur au groupe local, procédez comme suit :
   a) Dans la section **Rôle d'utilisateur**, cliquez sur +.
   b) Dans la liste déroulante, cliquez sur le nom du rôle d'utilisateur que vous souhaitez attribuer au groupe.
   c) Cliquez sur **Ajouter**.
6. Pour attribuer une stratégie informatique ou un profil au groupe local, procédez comme suit :
   a) Dans la section **Profils et stratégies informatiques**, cliquez sur +.
   b) Cliquez sur **Stratégie informatique** ou un type de profil.
   c) Dans la liste déroulante, cliquez sur le nom de la stratégie informatique que vous souhaitez attribuer au groupe.
   d) Cliquez sur **Attribuer**.
7. Pour attribuer une application au groupe d'utilisateurs, dans la section **Applications attribuées**, cliquez sur +.
8. Recherchez l'application.
9. Dans les résultats de la recherche, sélectionnez l'application.
10. Cliquez sur **Suivant**.
11. Dans la liste déroulante **Disposition** de l'application, exécutez l'une des opérations suivantes :
    - Pour installer l'application automatiquement sur les terminaux et empêcher les utilisateurs de la supprimer, cliquez sur **Requis**. Cette option n'est pas disponible pour les applications BlackBerry.
    - Pour autoriser les utilisateurs à installer et à supprimer l'application, sélectionnez **Facultatif**.

      Remarque : si la même application est attribuée à un compte d'utilisateur et au groupe d'utilisateurs auquel appartient l'utilisateur, la disposition de l'application attribuée au compte d'utilisateur est prioritaire
12. Pour les terminaux iOS : si vous souhaitez attribuer des paramètres VPN par application à une application ou un groupe d'applications, sélectionnez les paramètres à associer dans la liste déroulante **VPN par application**.
13. Cliquez sur **Attribuer**.
14. Après avoir spécifié les propriétés du groupe d'utilisateurs, cliquez sur **Ajouter**.

Tâches connexes

Créer un groupe lié par répertoire
Ajouter des utilisateurs à des groupes d'utilisateurs

Afficher un groupe d'utilisateurs

1. Sur la barre de menus, cliquez sur **Groupes**.
2. Recherchez un groupe d'utilisateurs.
3. Dans les résultats de la recherche, cliquez sur le nom du groupe d'utilisateurs.
4. Pour afficher les membres d'un groupe d'utilisateurs, procédez comme suit :
   a) Cliquez sur **Utilisateurs** pour afficher les comptes d'utilisateur attribués.
   b) Cliquez sur **Groupes imbriqués** pour afficher les groupes imbriqués attribués.
5. Cliquez sur **Paramètres** pour afficher les informations suivantes sur un groupe d'utilisateurs :
   - Groupes de répertoires associés (disponibles pour un groupe lié par annuaire)
   - Stratégie informatique BlackBerry OS attribuée, profils et configurations logicielles (disponibles si le domaine BlackBerry UEM prend en charge les terminaux BlackBerry)
   - Stratégie informatique attribuée, profils et applications

Modifier le nom d'un groupe d'utilisateurs

1. Sur la barre de menus, cliquez sur **Groupes**.
2. Recherchez le groupe d'utilisateurs que vous souhaitez afficher.
3. Cliquez sur le groupe d'utilisateurs.
4. Cliquez sur .
5. Modifiez le nom d'un groupe d'utilisateurs.
6. Vous pouvez aussi modifier la description du groupe d'utilisateurs.
7. Cliquez sur **Enregistrer**.

Supprimer un groupe d'utilisateurs

Lorsque vous supprimez un groupe d'utilisateurs, les utilisateurs du groupe ne sont pas supprimés. Les propriétés du groupe attribuées à l'utilisateur sont supprimées ou modifiées.

1. Sur la barre de menus, cliquez sur **Groupes**.
2. Recherchez le groupe d'utilisateurs que vous souhaitez supprimer.
3. Cliquez sur le groupe d'utilisateurs.
4. Cliquez sur .
5. Cliquez sur **Supprimer**.

Ajouter des groupes imbriqués à un groupe d'utilisateurs

Lorsque vous ajoutez un groupe imbriqué à un groupe d'utilisateurs, tous les groupes appartenant au groupe imbriqué sont également ajoutés.

Avant de commencer : Créez des groupes d'utilisateurs. Vous pouvez créer des groupes de répertoires associés ou des groupes locaux.

1. Sur la barre de menus, cliquez sur **Groupes**.
2. Recherchez un groupe d'utilisateurs.

3. Dans les résultats de la recherche, cliquez sur le nom du groupe d'utilisateurs.
4. Cliquez sur l'onglet **Groupes imbriqués**.
5. Cliquez sur +.
6. Sélectionnez un ou plusieurs groupes disponibles.
7. Cliquez sur **Ajouter**.

Supprimer les groupes imbriqués d'un groupe d'utilisateurs

Vous pouvez supprimer les groupes imbriqués directement attribués à un groupe d'utilisateurs.

1. Sur la barre de menus, cliquez sur **Groupes**.
2. Recherchez un groupe d'utilisateurs.
3. Dans les résultats de la recherche, cliquez sur le nom du groupe d'utilisateurs.
4. Cliquez sur l'onglet **Groupes imbriqués**.
5. Cliquez sur ✕ en regard de chaque groupe imbriqué que vous souhaitez supprimer.

Attribuer un profil ou une stratégie informatique à un groupe d'utilisateurs

1. Sur la barre de menus, cliquez sur **Groupes > Utilisateur**.
2. Dans la liste des groupes, cliquez sur le nom du groupe d'utilisateurs.
3. Dans la section **Profil attribué**, cliquez sur +.
4. Cliquez sur **Stratégie informatique** ou un type de profil.
5. Dans la liste déroulante, cliquez sur le nom du profil ou de la stratégie informatique que vous souhaitez attribuer au groupe.
6. Pour les stratégies informatiques et les types de profils classés, si le type de profil que vous avez sélectionné à l'étape 6 est déjà directement attribué au groupe, cliquez sur **Remplacer**. Sinon, cliquez sur **Attribuer**.

Concepts connexes

Comment BlackBerry UEM choisit la stratégie informatique à attribuer
Attribution de profils
Comment BlackBerry UEM choisit les profils à attribuer

Tâches connexes

Créer une stratégie informatique
Créer un profil de configuration logicielle minimale requise du terminal pour les terminaux BlackBerry 10
Attribuer un profil ou une stratégie informatique à un compte d'utilisateur

Attribuer une application à un groupe d'utilisateurs

Lorsque vous attribuez des applications à un groupe d'utilisateurs, ces applications sont mises à la disposition de tous les terminaux concernés que les membres du groupe d'utilisateurs ont activés. Vous pouvez également attribuer des applications à des groupes d'utilisateurs pour des types de terminaux que les membres du groupe d'utilisateurs n'ont pas encore activés. Ainsi, si un membre du groupe active ultérieurement un type de terminal différent, les applications qui conviennent seront mises à la disposition du nouveau terminal.

Si un compte d'utilisateur est membre de plusieurs groupes d'utilisateurs présentant les mêmes applications ou groupes d'applications, seule une instance de l'application ou du groupe d'applications apparait dans la liste

des applications attribuées à ce compte d'utilisateur. Une même application peut être directement attribuée au compte d'utilisateur ou héritée de groupes d'utilisateurs ou de groupes de terminaux. Les paramètres de l'application (si l'application est requise, par exemple) sont attribués en fonction de la priorité. Les groupes de terminaux bénéficient de la priorité la plus élevée, suivis des comptes d'utilisateur, puis des groupes d'utilisateurs.

Avant de commencer :

- Ajoutez l'application à la liste des applications disponibles.
- Vous pouvez également ajouter des applications à un groupe d'applications.

1. Sur la barre de menus, cliquez sur **Groupes > Utilisateur**.
2. Dans la liste des groupes, cliquez sur le nom du groupe d'utilisateurs.
3. Dans la section **Configuration VPN**, cliquez sur +.
4. Dans le champ de recherche, saisissez le nom, le fournisseur ou l'URL de l'application que vous souhaitez ajouter.
5. Cochez la case en regard des applications ou du groupe d'applications que vous souhaitez attribuer au groupe d'utilisateurs.
6. Cliquez sur **Suivant**.
7. Dans la liste déroulante **Disposition** de l'application, exécutez l'une des opérations suivantes :
   - Pour demander aux utilisateurs d'installer l'application, sélectionnez **Requis**.
   - Pour autoriser des utilisateurs à installer ou supprimer l'application, sélectionnez **Facultatif**.

   Remarque : si la même application est attribuée à un compte d'utilisateur, un groupe d'utilisateurs auquel appartient l'utilisateur et au groupe de terminaux auquel appartient le terminal, la disposition de l'application attribuée au groupe de terminaux est prioritaire.
8. Pour les terminaux iOS, pour attribuer des paramètres VPN par application à une application ou à un groupe d'applications, dans la liste déroulante **VPN par application** de l'application ou du groupe d'applications, sélectionnez les paramètres à lui associer.
9. Pour les terminaux iOS et Android, si une configuration d'application est disponible, sélectionnez-la pour l'attribuer à l'application.
10. Effectuez l'une des tâches suivantes :

Tâche	Étapes
Si vous n'avez pas ajouté de compte VPP ou n'ajoutez pas d'application iOS	**a.** Cliquez sur **Attribuer**.

Tâche	Étapes
Si vous ajoutez une application iOS et avez ajouté au moins un compte VPP	**a.** Cliquez sur **Suivant**. **b.** Sélectionnez **Oui** si vous souhaitez attribuer une licence à l'application iOS. Sélectionnez **Non** si vous ne souhaitez pas attribuer une licence à l'application ou n'avez pas de licence à lui attribuer. **c.** Si vous avez attribué une licence à l'application, dans la liste déroulante **Licence d'application**, sélectionnez le compte VPP à associer à l'application. **d.** Dans la liste déroulante **Attribuer une licence à**, attribuez la licence à l'**utilisateur** ou au **terminal**. Si aucune valeur n'est spécifiée dans la liste déroulante **Licence d'application**, la liste déroulante **Attribuer une licence à** n'est pas disponible. **e.** Cliquez sur **Attribuer**. Les utilisateurs doivent suivre les instructions qui s'affichent pour inscrire le compte VPP de leur entreprise avant de pouvoir installer des applications prépayées. Les utilisateurs doivent effectuer cette tâche une seule fois. **Remarque :** si vous autorisez l'accès à plusieurs licences dont vous disposez, les premiers utilisateurs à accéder aux licences disponibles peuvent installer l'application. Si l'application est une application requise ne disposant pas de licence disponible, vous devez obtenir la licence avant que l'utilisateur ne puisse installer l'application et ne soit soumis à toutes les règles de conformité que vous avez attribuées aux utilisateurs.

Référence connexe

Comportement des applications sur les terminaux Android
Comportement des applications sur les terminaux iOS
Comportement de l'application sur les terminaux BlackBerry

Attribuer un groupe d'applications à un groupe d'utilisateurs

Lorsque vous attribuez un groupe d'applications à un groupe d'utilisateurs, les applications de ce groupe sont mises à la disposition des terminaux activés par les membres du groupe d'utilisateurs. Vous pouvez également attribuer des applications à des groupes d'utilisateurs pour des types de terminaux que les membres du groupe d'utilisateurs n'ont pas encore activés. Ainsi, si un membre du groupe active ultérieurement un type de terminal différent, les applications qui conviennent seront mises à la disposition du nouveau terminal.

Si un compte d'utilisateur est membre de plusieurs groupes d'utilisateurs présentant les mêmes applications ou groupes d'applications, seule une instance du groupe d'applications apparait dans la liste des applications attribuées à ce compte d'utilisateur. Une même application peut être directement attribuée au compte d'utilisateur ou héritée de groupes d'utilisateurs ou de groupes de terminaux. Les paramètres de l'application (si l'application est requise, par exemple) sont attribués en fonction de la priorité : les groupes de terminaux bénéficient de la priorité la plus élevée, suivis des comptes d'utilisateur, puis des groupes d'utilisateurs.

Avant de commencer :

- Ajoutez des applications à un groupe d'applications.

1. Sur la barre de menus, cliquez sur **Groupes**.
2. Dans l'onglet **Groupes d'utilisateurs**, cliquez sur le nom d'un groupe.
3. Dans la section **Configuration VPN**, cliquez sur +.

4. Dans le champ de recherche, saisissez le nom du groupe d'applications que vous souhaitez ajouter.
5. Cochez la case en regard des applications ou du groupe d'applications que vous souhaitez attribuer au groupe d'utilisateurs.
6. Cliquez sur **Suivant**.
7. Dans la liste déroulante **Disposition** de l'application, exécutez l'une des opérations suivantes :
   - Pour demander aux utilisateurs d'installer l'application, sélectionnez **Requis**.
   - Pour autoriser des utilisateurs à installer ou supprimer l'application, sélectionnez **Facultatif**.

   Remarque : Si la même application est attribuée à un compte d'utilisateur, un groupe d'utilisateurs auquel appartient l'utilisateur et au groupe de terminaux auquel appartient le terminal, la disposition de l'application attribuée au groupe de terminaux est prioritaire.
8. Pour les terminaux iOS, pour attribuer des paramètres VPN par application à une application ou à un groupe d'applications, dans la liste déroulante **VPN par application** de l'application ou du groupe d'applications, sélectionnez les paramètres à lui associer.
9. Effectuez l'une des tâches suivantes :

Tâche	Étapes
Si vous n'avez pas ajouté de compte VPP ou n'ajoutez pas d'application iOS	**a.** Cliquez sur **Attribuer**.
Si vous ajoutez une application iOS et avez ajouté au moins un compte VPP	**a.** Cliquez sur **Suivant**. **b.** Sélectionnez **Oui** si vous souhaitez attribuer une licence à l'application iOS. Sélectionnez **Non** si vous ne souhaitez pas attribuer une licence à l'application ou n'avez pas de licence à lui attribuer. **c.** Si vous avez attribué une licence à l'application, dans la liste déroulante **Licence d'application**, sélectionnez le compte VPP à associer à l'application. **d.** Dans la liste déroulante **Attribuer une licence à**, attribuez la licence à l'**utilisateur** ou au **terminal**. Si aucune valeur n'est spécifiée dans la liste déroulante **Licence d'application**, la liste déroulante **Attribuer une licence à** n'est pas disponible. **e.** Cliquez sur **Attribuer**. Les utilisateurs doivent suivre les instructions qui s'affichent pour inscrire le compte VPP de leur entreprise avant de pouvoir installer des applications prépayées. Les utilisateurs doivent effectuer cette tâche une seule fois. **Remarque :** si vous autorisez l'accès à plusieurs licences dont vous disposez, les premiers utilisateurs à accéder aux licences disponibles peuvent installer l'application. Si l'application est une application requise ne disposant pas de licence disponible, vous devez obtenir la licence avant que l'utilisateur ne puisse installer l'application et ne soit soumis à toutes les règles de conformité que vous avez attribuées aux utilisateurs.

Référence connexe

Comportement des applications sur les terminaux Android
Comportement des applications sur les terminaux iOS
Comportement de l'application sur les terminaux BlackBerry

Attribuer une stratégie informatique BlackBerry OS, un profil ou une configuration logicielle à un groupe d'utilisateurs

Avant de commencer :

- Créez une stratégie informatique BlackBerry OS. Pour plus d'informations, téléchargez le Guide d'administration sur help.blackberry.com/detectLang/bes5-for-exchange/.
- Créez une configuration logicielle.
- Créez un profil Wi-Fi ou VPN pour les terminaux BlackBerry OS. Pour plus d'informations, téléchargez le Guide d'administration sur help.blackberry.com/detectLang/bes5-for-exchange/.
- Créez une règle de contrôle d'accès Push ou Pull pour les terminaux BlackBerry OS. Pour plus d'informations, téléchargez le Guide d'administration sur help.blackberry.com/detectLang/bes5-for-exchange/.

1. Sur la barre de menus, cliquez sur **Groupes**.
2. Recherchez un groupe d'utilisateurs.
3. Dans les résultats de la recherche, cliquez sur le nom du groupe d'utilisateurs.
4. Cliquez sur l'onglet **Terminaux gérés**.
5. Dans la section **Stratégie informatique, profils et configurations logicielles**, cliquez sur +.
6. Cliquez sur **Stratégie informatique**, **Wi-Fi**, **VPN**, **Règle de contrôle d'accès Push**, **Règle Pull de contrôle d'accès** ou **Configuration logicielle**.
7. Dans la liste déroulante, cliquez sur le nom de la stratégie informatique, du profil, de la règle de contrôle d'accès ou de la configuration logicielle que vous souhaitez attribuer au groupe.
8. Cliquez sur **Attribuer**.

Concepts connexes

Contrôle des fonctionnalités du terminal BlackBerry OS à l'aide de stratégies informatiques

Tâches connexes

Attribuer une stratégie informatique BlackBerry OS, un profil ou une configuration logicielle à un compte d'utilisateur

Création et gestion de groupes de terminaux partagés

Vous pouvez autoriser plusieurs utilisateurs à partager un terminal iOS et configurer des paramètres propres à chaque utilisateur ou identiques pour tous. Vous pouvez personnaliser les conditions d'utilisation que les utilisateurs doivent accepter pour extraire des terminaux partagés. Un utilisateur peut extraire un terminal à l'aide d'une authentification locale ou Microsoft Active Directory. Quand il ne l'utilise plus, il peut l'archiver pour le rendre disponible pour l'utilisateur suivant. Les terminaux partagés restent gérés par BlackBerry UEM pendant les processus d'extraction et d'archivage.

Cette fonctionnalité a été conçue pour des terminaux supervisés avec la configuration suivante :

- Mode de verrouillage des applications activé
- Applications VPP attribuées

Remarque : Cette fonction ne prend pas en charge les applications BlackBerry Dynamics. Ce même profil BlackBerry Dynamics doit être attribué au compte d'utilisateur qui possède le groupe de terminaux partagés, ainsi qu'à ce groupe. Vous devez vérifier que l'option Autoriser UEM Client à s'inscrire dans BlackBerry Dynamics n'est pas sélectionnée dans le profil.

Concepts connexes

Limiter les terminaux à une application
Gestion des comptes VPP Apple

Créer un groupe de terminaux partagés

Lorsque vous créez un groupe de terminaux partagés, un compte d'utilisateur local est créé. Ce compte d'utilisateur local est propriétaire du groupe de terminaux partagés.

1. Sur la barre de menus, cliquez sur **Utilisateurs > Groupes de terminaux partagés**.
2. Cliquez sur + en regard de la barre de recherche.
3. Saisissez le nom du groupe de terminaux partagés.
4. Vous pouvez aussi saisir une description pour le groupe de terminaux partagés.
5. Saisissez le nom d'utilisateur pour l'activation du terminal.
6. Pour demander aux utilisateurs d'accepter les conditions d'utilisation lorsqu'ils extraient un terminal partagé, procédez comme suit :
   a) Sélectionnez **Activer les conditions d'utilisation**.
   b) Saisissez le texte des conditions d'utilisation.
7. Dans la section **Utilisateurs avec accord**, recherchez un utilisateur et cliquez sur son nom dans la liste des résultats de recherche.
8. Répétez l'étape 7 pour chaque utilisateur que vous souhaitez ajouter.
9. Cliquez sur **Enregistrer**.

À la fin : Pour activer le verrouillage des applications UEM Client, modifiez les informations relatives au groupe de terminaux partagés.

Activer un terminal partagé

Pour que les utilisateurs puissent extraire des terminaux partagés, vous devez les activer.

Avant de commencer : Vérifiez que l'option **Autoriser UEM Client à s'inscrire dans BlackBerry Dynamics** n'est pas sélectionnée pour le profil BlackBerry Dynamics affecté au groupe de terminaux partagés. Vérifiez que ce même profil est également affecté au compte d'utilisateur qui possède le groupe de terminaux partagés.

1. Sur la barre de menus, cliquez sur **Utilisateurs > Terminaux partagés**.
2. Recherchez un groupe de terminaux partagés.
3. Dans les résultats de la recherche, cliquez sur le nom du groupe de terminaux partagés.
4. Cliquez sur **Activation du terminal** pour afficher l'adresse du serveur, le nom d'utilisateur et le mot de passe d'activation.
5. Utilisez les données d'activation du terminal pour activer le terminal. Pour obtenir de l'aide concernant l'activation, reportez-vous à Activer un terminal iOS .

À la fin : Vérifiez que le terminal activé est affiché dans la section **Terminaux partagés**. BlackBerry UEM utilise le nom du groupe pour générer le nom du terminal et ajoute un chiffre. Par exemple, si le nom du groupe est Exemple, le premier terminal que vous activez est nommé Exemple 01.

Afficher l'historique de désenregistrement d'un utilisateur

Vous pouvez afficher la liste des terminaux partagés qu'un utilisateur a utilisés. Chaque enregistrement indique l'heure à laquelle un terminal a été extrait et archivé et la liste affiche les 50 derniers enregistrements pour un utilisateur. L'historique de désenregistrement d'un utilisateur est mis à jour lorsqu'il archive un terminal.

1. Sur la barre de menus, cliquez sur **Utilisateurs > Terminaux partagés**.
2. Recherchez un groupe de terminaux partagés.
3. Dans les résultats de la recherche, cliquez sur le nom du groupe de terminaux partagés.
4. Dans la section **Utilisateurs avec accord** , cliquez sur **Afficher** dans la colonne **Historique de désenregistrement** de l'utilisateur.

Modifier l'adhésion des utilisateurs pour un groupe de terminaux partagés

L'adhésion des utilisateurs pour un groupe de terminaux partagés spécifie la liste des utilisateurs autorisés à accéder aux terminaux partagés activés pour le groupe. Les utilisateurs peuvent appartenir à un ou plusieurs groupes de terminaux partagés.

1. Sur la barre de menus, cliquez sur **Utilisateurs > Terminaux partagés**.
2. Recherchez un groupe de terminaux partagés.
3. Dans les résultats de la recherche, cliquez sur le nom du groupe de terminaux partagés.
4. Dans la section **Utilisateurs avec accord**, effectuez l'une des opérations suivantes :
   - Pour ajouter un utilisateur au groupe, recherchez un utilisateur et cliquez sur son nom dans la liste des résultats de recherche.
   - Pour supprimer un utilisateur du groupe, cliquez sur ✕ dans la colonne **Action** pour l'utilisateur et cliquez sur **Envoyer**.
5. Répétez l'étape 4 pour chaque utilisateur que vous souhaitez ajouter ou supprimer.

Supprimer un terminal d'un groupe de terminaux partagés

Lorsque vous supprimez un terminal d'un groupe de terminaux partagés, BlackBerry UEM envoie la commande Supprimer uniquement les données professionnelles au terminal.

1. Sur la barre de menus, cliquez sur **Utilisateurs > Terminaux partagés**.
2. Recherchez un groupe de terminaux partagés.
3. Dans les résultats de la recherche, cliquez sur le nom du groupe de terminaux partagés.

4. Dans la section **Terminaux partagés**, procédez comme suit :
   a) Cliquez sur ✕ dans la colonne **Action** du terminal.
   b) Cliquez sur **Supprimer uniquement les données professionnelles**.
5. Répétez l'étape 4 pour chaque terminal que vous souhaitez supprimer.

Supprimer un groupe de terminaux partagés

Avant de commencer : Retirez tous les terminaux du groupe de terminaux partagés.

1. Sur la barre de menus, cliquez sur **Utilisateurs > Terminaux partagés**.
2. Recherchez un groupe de terminaux partagés.
3. Dans les résultats de la recherche, cliquez sur le nom du groupe de terminaux partagés.
4. Cliquez sur 🗑.
5. Cliquez sur **Supprimer**.

Attribuer une application à un groupe de terminaux partagés

Lorsque vous attribuez des applications ou des groupes d'applications à un groupe de terminaux partagés, les applications sont mises à disposition lorsqu'un utilisateur extrait un terminal qui est activé pour le groupe, et les applications sont supprimées lorsque l'utilisateur archive le terminal. Si vous voulez que des applications restent sur les terminaux lorsqu'ils sont archivés, vous devez également attribuer celles-ci au compte de l'utilisateur qui possède le groupe de terminaux partagés.

Avant de commencer :

- Ajoutez l'application à la liste des applications disponibles.
- Vous pouvez également ajouter des applications à un groupe d'applications.

1. Sur la barre de menus, cliquez sur **Utilisateurs > Terminaux partagés**.
2. Recherchez un groupe de terminaux partagés.
3. Dans les résultats de la recherche, cliquez sur le nom du groupe de terminaux partagés.
4. Dans la section **Applications attribuées**, cliquez sur +.
5. Dans le champ de recherche, saisissez le nom, le fournisseur ou l'URL de l'application que vous souhaitez ajouter.
6. Cochez la case en regard des applications ou du groupe d'applications que vous souhaitez attribuer au groupe d'utilisateurs.
7. Cliquez sur **Suivant**.
8. Dans la liste déroulante **Disposition** de l'application, exécutez l'une des opérations suivantes :
   - Pour demander aux utilisateurs d'installer l'application, sélectionnez **Requis**.
   - Pour permettre aux utilisateurs d'installer et de supprimer l'application, sélectionnez **Facultatif**.
9. Pour attribuer des paramètres VPN par application à une application ou à un groupe d'applications, dans la liste déroulante **VPN par application** de l'application ou du groupe d'applications, sélectionnez les paramètres à lui associer.
10. Si une configuration d'application est disponible, sélectionnez-la pour l'attribuer à l'application.
11. Cliquez sur **Suivant**.
12. Sélectionnez **Oui** si vous souhaitez attribuer une licence à l'application. Sélectionnez **Non** si vous ne souhaitez pas attribuer une licence à l'application ou n'avez pas de licence à lui attribuer.
13. Si vous avez attribué une licence à l'application, dans la liste déroulante **Licence d'application**, sélectionnez le compte VPP à associer à l'application.

14. Dans la liste déroulante **Attribuer une licence à**, attribuez la licence à l'**utilisateur** ou au **terminal**. Si aucune valeur n'est spécifiée dans la liste déroulante **Licence d'application**, la liste déroulante **Attribuer une licence à** n'est pas disponible.
15. Cliquez sur **Attribuer**.

    Les utilisateurs doivent suivre les instructions qui s'affichent pour inscrire le compte VPP de leur entreprise avant de pouvoir installer des applications prépayées. Les utilisateurs doivent effectuer cette tâche une seule fois.

    Remarque : si vous autorisez l'accès à plusieurs licences dont vous disposez, les premiers utilisateurs à accéder aux licences disponibles peuvent installer l'application. Si l'application est une application requise ne disposant pas de licence disponible, vous devez obtenir la licence avant que l'utilisateur ne puisse installer l'application et ne soit soumis à toutes les règles de conformité que vous avez attribuées aux utilisateurs.

Attribuer une stratégie informatique ou un profil à un groupe de terminaux partagés

Lorsque vous attribuez une stratégie informatique ou un profil à un groupe de terminaux partagés, ceux-ci sont envoyés lorsqu'un utilisateur extrait un terminal qui est activé pour le groupe, et supprimés lorsque l'utilisateur archive le terminal. Si vous souhaitez qu'une stratégie informatique ou un profil reste sur les terminaux lorsqu'ils sont archivés, vous devez également les attribuer au compte de l'utilisateur qui possède le groupe de terminaux partagés.

Avant de commencer :

- Si nécessaire, Créer une stratégie informatique.
- Si nécessaire, créez des profils. Pour plus d'informations, reportez-vous aux sections Référence de profils et Utilisation de variables dans les profils.

1. Sur la barre de menus, cliquez sur **Utilisateurs > Terminaux partagés**.
2. Recherchez un groupe de terminaux partagés.
3. Dans les résultats de la recherche, cliquez sur le nom du groupe de terminaux partagés.
4. Dans la section **Stratégie informatique et profils attribués**, cliquez sur +.
5. Cliquez sur **Stratégie informatique** ou un type de profil.
6. Dans la liste déroulante, cliquez sur le nom de la stratégie informatique que vous souhaitez attribuer au groupe.
7. Effectuez l'une des tâches suivantes :

Tâche	Étapes
Attribuer une stratégie informatique	**a.** Si une stratégie informatique est déjà attribuée au groupe, cliquez sur **Remplacer**. Sinon, cliquez sur **Attribuer**.
Attribuer un type de profil classé	**a.** Si le type de profil que vous avez sélectionné à l'étape 5 est déjà directement attribué au groupe, cliquez sur **Remplacer**. Sinon, cliquez sur **Attribuer**.
Attribuer un type de profil non classé	**a.** Cliquez sur **Attribuer**.

Création de groupes de terminaux

Un groupe de terminaux regroupe des terminaux dotés d'attributs communs, comme le modèle et le fabricant du terminal, le type et la version du système d'exploitation, le fournisseur de services et l'appartenance du terminal (entreprise ou utilisateurs). BlackBerry UEM déplace automatiquement les terminaux à l'intérieur ou à l'extérieur des groupes de terminaux selon les attributs que vous définissez.

Vous pouvez utiliser les groupes de terminaux pour appliquer différents ensembles de stratégies, profils et applications aux terminaux attribués à un seul utilisateur. Par exemple, vous pouvez utiliser un groupe de terminaux pour appliquer une stratégie informatique spécifique à tous les terminaux exécutant BlackBerry 10 OS ou tous les terminaux HTC EVO exécutant Android OS 4.0 ou version ultérieure sur le réseau T-Mobile.

Les stratégies, profils et applications attribués à un groupe de terminaux sont prioritaires sur ceux attribués à un utilisateur ou à un groupe d'utilisateurs. Vous ne pouvez cependant pas attribuer de profils d'activation ou certificats d'utilisateur aux groupes de terminaux.

Les groupes de terminaux n'incluent pas les terminaux BlackBerry OS (versions 5.0 à 7.1). Malgré la création d'une demande de groupe de terminaux censée logiquement inclure vos terminaux BlackBerry OS, ceux-ci ne sont pas contenus dans le groupe de terminaux.

Créer un groupe de terminaux

1. Sur la barre de menus, cliquez sur **Groupes > Terminal**.
2. Cliquez sur .
3. Saisissez le nom du groupe de terminaux.
4. Dans la section **Étendre à des groupes d'utilisateurs**, vous pouvez sélectionner un ou plusieurs groupes d'utilisateurs à appliquer au groupe de terminaux. Si vous ne sélectionnez aucun groupe d'utilisateurs, le groupe de terminaux s'applique à tous les terminaux activés.
5. Dans la première liste déroulante de la section **Demande sur les terminaux**, sélectionnez **Un** ou **Tous**.

   Si vous sélectionnez **Tous**, les terminaux doivent satisfaire à tous les attributs que vous définissez pour rejoindre le groupe de terminaux. Si vous sélectionnez **Un**, les terminaux doivent satisfaire à un des attributs que vous définissez pour rejoindre le groupe de terminaux.
6. Dans la section **Demande sur les terminaux**, procédez comme suit :
   - Dans la liste déroulante **Attribut**, cliquez sur un attribut.
   - Dans la liste déroulante **Opérateur**, cliquez sur un opérateur.
   - Dans la liste déroulante **Valeur**, cliquez sur une valeur ou saisissez une valeur.

   Vous pouvez ajouter ou supprimer des lignes mieux définir votre demande.
7. Cliquez sur **Suivant**.
8. Pour attribuer une stratégie informatique ou un profil au groupe de terminaux, procédez comme suit :
   a) Dans la section **Profils et stratégies informatiques**, cliquez sur +.
   b) Cliquez sur **Stratégie informatique** ou un type de profil.
   c) Dans la liste déroulante, cliquez sur le nom de la stratégie informatique que vous souhaitez attribuer au groupe.
   d) Cliquez sur **Attribuer**.
9. Pour attribuer une application ou un groupe d'applications au groupe de terminaux, dans la section **Applications attribuées**, cliquez sur +.

   Remarque : Vous ne pouvez pas ajouter des applications BlackBerry Dynamics à des groupes de terminaux parce que les autorisations peuvent uniquement être accordées aux utilisateurs. Tout BlackBerry Dynamics

inclus dans des groupes d'applications que vous ajoutez aux groupes de terminaux ne sera pas attribué aux utilisateurs.

Remarque : Vous ne pouvez pas ajouter d'applications Android dotées d'une disposition optionnelle à des groupes de terminaux dans un environnement BlackBerry UEM qui prend en charge les profils professionnels Android. Google Play for Work ne peut pas attribuer d'applications à des ID de terminaux. Google Play for Work peut attribuer des applications uniquement à des ID d'utilisateur Google. Si vous ajoutez des applications Android dotées d'une disposition requise à un groupe de terminaux, les applications seront installées, mais elles ne seront pas répertoriées dans Google Play for Work.

10. Recherchez l'application.
11. Dans les résultats de la recherche, sélectionnez l'application.
12. Cliquez sur **Suivant**.
13. Dans la liste déroulante **Disposition** de l'application ou du groupe d'applications, exécutez l'une des opérations suivantes :
    - S'il s'agit d'une application iOS ou Android : pour demander aux utilisateurs de suivre les actions définies pour les applications du profil de conformité correspondant, sélectionnez **Requis**.
    - S'il s'agit d'une application Windows Phone :Pour installer automatiquement une application interne sur des terminaux attribués, sélectionnez**Requis**. Si les utilisateurs désinstallent l'application interne requise, ils doivent suivre les actions définies dans le profil de conformité correspondant.Pour les applications ajoutées depuis Windows Store, sélectionnez**Requis**pour demander aux utilisateurs de suivre les actions définies pour les applications dans le profil de conformité correspondant. Cela s'applique uniquement aux terminaux exécutant Windows Phone 8.1 ou version ultérieure.
    - S'il s'agit d'une application BlackBerry 10 interne : pour installer automatiquement l'application interne sur les terminaux attribués, sélectionnez**Requis**. Cette option est uniquement disponible pour applications BlackBerry 10 internes. Les applications ajoutées depuis la boutique BlackBerry World peuvent uniquement être facultatives.
    - Si le groupe d'applications prend en charge les profils professionnels Android, la disposition ne peut être définie que comme requise.
    - Pour autoriser les utilisateurs à installer et à supprimer l'application, sélectionnez **Facultatif**.

      Remarque : La même application peut être directement attribuée au compte d'utilisateur ou héritée de groupes d'utilisateurs ou de groupes de terminaux. Les paramètres de l'application (si l'application est requise, par exemple) sont attribués en fonction de la priorité : les groupes de terminaux sont prioritaires sur les comptes d'utilisateur et les groupes d'utilisateurs.
14. Pour les terminaux iOS : si vous souhaitez attribuer des paramètres VPN par application à une application ou un groupe d'applications, sélectionnez les paramètres à associer dans la liste déroulante **VPN par application**.
15. Pour les iOS terminaux et Android, si une configuration d'application est disponible, sélectionnez cette configuration d'application pour l'attribuer à l'application.
16. Cliquez sur **Attribuer**.
17. Après avoir spécifié les propriétés du groupe de terminaux, cliquez sur **Ajouter**.

Modifier un groupe de terminaux

1. Sur la barre de menus, cliquez sur **Groupes > Terminal**.
2. Cliquez sur le nom d'un groupe de terminaux que vous souhaitez modifier.
3. Cliquez sur  .
4. Procédez aux modifications nécessaires.
5. Cliquez sur **Enregistrer**.

Définition des paramètres des groupes de terminaux

Lorsque vous créez un groupe de terminaux, vous configurez une demande de terminaux incluant une ou plusieurs instructions d'attribut. Vous pouvez spécifier si un terminal appartient au groupe de terminaux, s'il correspond à une instruction d'attribut ou s'il correspond à toutes les instructions d'attribut. Chaque instruction d'attribut contient un attribut, un opérateur et une valeur.

Attribut	Opérateurs	Valeurs
Opérateur	• = • != • Commence par	Dans le champ de texte, saisissez le nom d'un fournisseur de services, comme T-Mobile ou Bell.
BlackBerry Dynamics activé(e)	• = • !=	Dans la liste déroulante, choisissez l'une des options suivantes : • Désactivée • Activé(e)
Fabricant	• = • != • Commence par	Dans le champ de texte, saisissez le nom d'un fabricant de terminaux, comme Apple ou BlackBerry.
Modèle	• = • != • Commence par	Dans le champ de texte, saisissez le nom d'un modèle de terminal, comme iPhone 5S ou BlackBerry Classic.
Système d'exploitation	• = • !=	Dans la liste déroulante, choisissez l'une des options suivantes : • Android • BlackBerry 10 • iOS • Windows
Version OS	• = • != • >= • <=	Dans le champ de texte, saisissez une version d'OS, comme 7.1.1 ou 10.3. Si vous utilisez cet attribut, vous devez également spécifier l'attribut du système d'exploitation.
Propriété	• = • !=	Dans la liste déroulante, choisissez l'une des options suivantes : • Work • Personnel • Non spécifié
Type d'activation	• = • !=	Dans la liste déroulante, choisissez un type d'activation. La liste contient les mêmes types d'activation que ceux disponibles pour l'affectation dans vos profils d'activation.

Attribut	Opérateurs	Valeurs
KNOX Workspace	• = • != • Commence par	Dans le champ de texte, saisissez une version Samsung KNOX Workspace, comme 2.2.

Afficher un groupe de terminaux

1. Sur la barre de menus, cliquez sur **Groupes > Terminaux**.
2. Recherchez le groupe de terminaux que vous souhaitez afficher.
3. Cliquez sur le groupe de terminaux.
4. Effectuez l'une des opérations suivantes :
   - Pour afficher les terminaux attribués au groupe de terminaux, cliquez sur l'onglet **Terminaux**.
   - Pour afficher les groupes d'utilisateurs, les demandes sur les terminaux, les stratégies informatiques, les profils ou les applications attribués au groupe de terminaux, sélectionnez l'onglet **Paramètres.**

Modifier le nom d'un groupe de terminaux

1. Sur la barre de menus, cliquez sur **Groupes > Terminal**.
2. Recherchez le groupe de terminaux que vous souhaitez afficher.
3. Cliquez sur le groupe de terminaux.
4. Cliquez sur .
5. Modifiez le nom du groupe de terminaux
6. Cliquez sur **Suivant**.
7. Cliquez sur **Enregistrer**.

Supprimer un groupe de terminaux

Pour pouvoir supprimer un groupe de terminaux, vous devez être autorisé à gérer tous les groupes d'utilisateurs auxquels ce groupe de terminaux a été appliqué.

1. Sur la barre de menus, cliquez sur **Groupes > Terminal**.
2. Recherchez le groupe de terminaux que vous souhaitez afficher.
3. Cliquez sur le groupe de terminaux.
4. Cliquez sur .
5. Cliquez sur **Supprimer**.

Affichage et personnalisation de la liste d'utilisateurs

Vous pouvez afficher et personnaliser la liste d'utilisateurs en définissant la vue par défaut ou avancée, puis en sélectionnant les informations à afficher dans la liste d'utilisateurs. Vous pouvez sélectionner et réorganiser les colonnes de la liste d'utilisateurs, des colonnes supplémentaires étant disponibles dans la vue avancée.

Vous pouvez utiliser des filtres pour afficher uniquement les informations utiles à votre tâche. Vous pouvez choisir de filtrer la liste d'utilisateurs en sélectionnant un filtre ou plusieurs filtres à la fois. Dans la vue par défaut, vous pouvez filtrer la liste des utilisateurs par système d'exploitation, fournisseur de services sans fil, groupe, stratégie informatique attribuée, propriété et non-conformité. Plus de catégories sont disponibles dans la vue

avancée. Par exemple, vous pouvez filtrer la liste d'utilisateurs par modèle, version du système d'exploitation et type d'activation.

À des fins d'analyse approfondie et de génération de rapports, vous pouvez exporter la liste d'utilisateurs vers un fichier .csv.

Configuration de la vue par défaut ou avancée

Vous pouvez définir la vue utilisée par votre navigateur pour afficher la liste d'utilisateurs dans BlackBerry UEM. Plusieurs colonnes et catégories de filtre sont disponibles dans la vue avancée.

Remarque : dans les environnements à grande échelle, la vue avancée peut mettre plus de temps à s'afficher que la vue par défaut.

1. Sur la barre de menus, cliquez sur **Utilisateurs > Terminaux gérés**.
2. Dans le coin supérieur droit, cliquez sur **Par défaut** ou sur **Avancé**.

À la fin : Sélection des informations à afficher dans la liste des utilisateurs.

Sélection des informations à afficher dans la liste des utilisateurs

Avant de commencer : Configuration de la vue par défaut ou avancée.

1. Sur la barre de menus, cliquez sur **Utilisateurs > Terminaux gérés**.
2. Cliquez sur + en haut de la liste d'utilisateurs et effectuez l'une des actions suivantes :
   - Cliquez sur **Sélectionner tout** ou sélectionnez la case de chaque colonne que vous souhaitez afficher.
   - Décochez la case de chaque colonne que vous souhaitez supprimer.
   - Cliquez sur **Réinitialiser** pour rétablir les sélections par défaut.
3. Pour trier la liste des utilisateurs, cliquez sur l'en-tête d'une colonne.
4. Pour réorganiser les colonnes, cliquez sur l'en-tête d'une colonne et faites-le glisser vers la gauche ou vers la droite.

Filtrage de la liste d'utilisateurs

Lorsque vous activez la sélection multiple, vous pouvez sélectionner plusieurs filtres avant de les appliquer et vous pouvez choisir plusieurs filtres sous chaque catégorie. Lorsque vous désactivez la sélection multiple, chaque filtre est appliqué lorsque vous le sélectionnez et vous ne pouvez choisir qu'un seul filtre sous chaque catégorie.

Avant de commencer : Configuration de la vue par défaut ou avancée.

1. Sur la barre de menus, cliquez sur **Utilisateurs**.
2. Cliquez sur pour activer ou désactiver la sélection multiple.
3. Sous **Filtres**, développez une ou plusieurs catégories.

   Chaque catégorie comprend uniquement des filtres qui affichent les résultats et chaque filtre indique le nombre de résultats à afficher lorsque vous l'appliquez.
4. Effectuez l'une des opérations suivantes :
   - Si vous avez activé la sélection multiple, cochez la case en regard de chaque filtre que vous souhaitez appliquer et cliquez sur **Soumettre**.
   - Si vous avez désactivé la sélection multiple, cliquez sur le filtre que vous souhaitez appliquer.
5. Dans le volet de droite, vous pouvez également cliquer sur **Effacer tout** ou cliquez sur ✕ pour chaque filtre que vous souhaitez supprimer.

Classer la liste des utilisateurs

Vous pouvez classer la liste des utilisateurs dans l'ordre alphabétique en choisissant l'une des catégories affichées sur les en-têtes de colonne.

Avant de commencer : Configuration de la vue par défaut ou avancée.

1. Sur la barre de menu, cliquez sur **Utilisateurs** et sélectionnez l'onglet que vous souhaitez afficher.
2. Si nécessaire, filtrez la liste des utilisateurs.
3. Sélectionnez un en-tête de colonne. Cliquez à nouveau sur l'en-tête de la colonne pour la classer dans l'ordre inverse.

Exportation d'une liste d'utilisateurs vers un fichier .csv

Lorsque vous exportez la liste d'utilisateurs vers un fichier .csv, le fichier inclut toutes les colonnes disponibles dans la vue par défaut ou avancée.

Avant de commencer : Configuration de la vue par défaut ou avancée.

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

Tâches connexes

Filtrage de la liste d'utilisateurs

Modifier l'étiquette de propriété du terminal

Chaque appareil activé dans BlackBerry UEM dispose d'une étiquette qui indique s'il appartient à votre entreprise ou à l'utilisateur ou si sa propriété n'est pas définie. La valeur par défaut de cette étiquette est déterminée par le paramètre de propriété du terminal dans le profil d'activation. Vous pouvez modifier l'étiquette de propriété à tout moment. Pour modifier ce paramètre pour plusieurs terminaux à la fois, reportez-vous à la section Envoyer une commande groupée.

L'étiquette de propriété du terminal vous permet de filtrer la liste des utilisateurs avec le paramètre de propriété du terminal. Pour plus d'informations, reportez-vous à Filtrage de la liste d'utilisateurs.

1. Sur la barre de menus, cliquez sur **Utilisateurs > Terminaux gérés**.
2. Recherchez un compte d'utilisateur.
3. Dans les résultats de la recherche, cliquez sur le nom du compte d'utilisateur.
4. Cliquez sur l'onglet du terminal.
5. Dans la section Terminal activé, en regard du paramètre de propriété, cliquez sur **Modifier**.
6. Dans la liste déroulante, sélectionnez l'une des options suivantes :
   - Work
   - Personnel
   - Non spécifié
7. Cliquez sur **Enregistrer**.

Activation des terminaux

Lorsque vous activez un terminal, vous pouvez associer ce terminal à BlackBerry UEM pour gérer les terminaux et l'accès des utilisateurs aux données professionnelles de leurs terminaux.

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

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

Étapes à suivre pour activer des terminaux

Pour activer des terminaux, procédez comme suit :

Étape	Action
1	Vérifiez que toutes les conditions d'activation sont remplies.
2	Configurez les paramètres d'activation par défaut.
3	Le cas échéant, consultez les informations suivantes : • Si vous avez l'intention de prendre en charge les terminaux Android dotés d'un profil professionnel, reportez-vous à Prise en charge des activations pour les terminaux Android dotés d'un profil professionnel. • Si vous envisagez de prendre en charge des terminaux Windows 10, reportez-vous à la section Prise en charge des activations Windows 10 .
4	mettez à jour le modèle de l'e-mail d'activation.
5	Créez un profil d'activation et attribuez-le à un compte d'utilisateur ou à un groupe auquel appartient l'utilisateur.
6	Définissez un mot de passe d'activation pour l'utilisateur.

Exigences : Activation

Pour tous les terminaux :

- Une licence disponible dans BlackBerry UEM pour le terminal que vous souhaitez activer. Pour plus d'informations sur les licences, reportez-vous au contenu relatif aux licences.
- Connexion sans fil

Pour les terminaux iOS, Android et Windows Phone 8.0 et 8.1 :

- La dernière version de l'application BlackBerry UEM Client installée sur le terminal

Pour les terminaux Windows 10 et Windows 10 Mobile :

- Un certificat RSA racine BlackBerry Enterprise Server installé sur le terminal
- Pour les terminaux qui utilisent une configuration proxy, un proxy qui ne nécessite pas d'authentification. Pour plus d'informations, reportez-vous à : https://docs.microsoft.com/en-us/windows/client-management/mdm/new-in-windows-mdm-enrollment-management
- Pour les ordinateurs, Windows 10 Home n'offre qu'une prise en charge limitée.

Pour Espace Travail uniquement sur les terminaux Android dotés d'un profil professionnel :

- Un Google code d'activation

Pour les terminaux BlackBerry OS (versions 5.0 à 7.1) :

- Compte d'utilisateur dans un annuaire du serveur de messagerie professionnel auquel le serveur de messagerie BlackBerry OS se connecte
- Activation du terminal BlackBerry OS activée pour le compte d'utilisateur

Remarque : Les utilisateurs peuvent cliquer ici pour regarder une vidéo sur la façon d'activer leurs terminaux : http://help.blackberry.com/detectLang/activation-videos/current/

Gérer les mots de passe d'activation

Vous pouvez bénéficier d'un certain contrôle sur le nombre de terminaux que les utilisateurs peuvent activer en gérant les mots de passe d'activation envoyés aux utilisateurs.

Vous trouverez ci-dessous des exemples de gestion des mots de passe d'activation :

- Lorsque vous définissez des mots de passe d'activation pour les utilisateurs, vous pouvez effectuer les opérations suivantes :
  - Configurez BlackBerry UEM pour qu'il génère automatiquement un mot de passe d'activation. Vous pouvez aussi définir le mot de passe d'activation vous-même.
  - Spécifiez le délai de validité du mot de passe d'activation (en minutes ou en jours).
  - Spécifiez que la période d'activation expirera dès que l'utilisateur aura activé un terminal, ce qui l'empêchera d'activer d'autres terminaux avec le même mot de passe.

  Pour plus d'informations, reportez-vous à Définir un mot de passe d'activation et envoyer un e-mail d'activation.
- Vous pouvez créer plusieurs mots de passe pour un même utilisateur et associer les mots de passe à des profils d'activation spécifiques. Pour plus d'informations, reportez-vous à Permettre aux utilisateurs d'activer des terminaux utilisant des types d'activation différents.
- Si vous autorisez les utilisateurs à définir leurs mots de passe d'activation dans BlackBerry UEM Self-Service, ils pourront créer des mots de passe d'activation en fonction de leurs besoins, mais ils ne pourront activer qu'un nombre spécifique de terminaux, comme défini dans le profil d'activation. Pour plus d'informations, reportez-vous à Autoriser les utilisateurs à définir des mots de passe d'activation BlackBerry UEM Self-Service.
- Vous pouvez faire expirer les mots de passe d'activation d'un utilisateur à tout moment. Pour plus d'informations, reportez-vous à Faire expirer manuellement un mot de passe d'activation.

- Si vous déployez des terminaux à l'aide de Samsung KNOX Mobile Enrollment, vous pouvez autoriser les utilisateurs de ceux-ci à utiliser leurs identifiants Microsoft Active Directory pour les activer. Au lieu de gérer les mots de passe d'activation pour chaque utilisateur, vous pouvez demander aux utilisateurs d'utiliser leurs identifiants Active Directory. Cette option s'applique uniquement aux terminaux inscrits dans le compte KNOX Mobile Enrollment de votre entreprise. Pour plus d'informations, reportez-vous à Spécifier les paramètres par défaut des mots de passe d'activation.

Spécifier les paramètres par défaut des mots de passe d'activation

Vous pouvez spécifier la durée par défaut pendant laquelle un mot de passe d'activation reste valide avant expiration. Vous pouvez également spécifier la longueur des mots de passe générés automatiquement qui sont envoyés aux utilisateurs dans un des e-mails d'activation et spécifier si la période d'expiration expire après la première activation du terminal.

La valeur que vous saisissez pour l'expiration du mot de passe d'activation apparait comme paramètre par défaut dans le champ Mot de passe d'activation des fenêtres Définir le mot de passe d'activation du terminal et Ajouter un utilisateur.

Pour les terminaux qui sont activés à l'aide de Samsung KNOX Mobile Enrollment, vous pouvez également préciser si vous souhaitez autoriser les utilisateurs à utiliser leurs identifiants Microsoft Active Directory pour activer leurs terminaux.

1. Sur la barre de menus, cliquez sur **Paramètres**.
2. Dans le volet de gauche, développez **Paramètres généraux.**
3. Cliquez sur **Paramètres d'activation par défaut.**
4. Dans le champ **Expiration de la période d'activation**, saisissez la durée par défaut pendant laquelle un mot de passe d'activation (ou QR Code) reste valide avant expiration. La valeur doit être comprise entre 1 minute et 30 jours.
5. Si nécessaire, cochez la case **La période d'activation expire à l'issue de l'activation du premier terminal**.
6. Cochez ou décochez la case **Autoriser les codes QR pour l'activation des terminaux**. Si vous la cochez, vous avez la possibilité d'envoyer un QR Code aux utilisateurs à la place du mot de passe d'activation. Dans le cas contraire, l'option d'envoi d'un QR Code n'est pas disponible dans le modèle d'e-mail d'activation.
7. Si nécessaire, pour les terminaux qui sont activés à l'aide de KNOX Mobile Enrollment, sélectionnez **Autoriser l'utilisation du nom d'utilisateur et du mot de passe Microsoft Active Directory**.
8. Cochez ou décochez la case **Envoyer une notification d'activation de terminal**. Si la case est cochée, l'utilisateur reçoit un e-mail lorsqu'un terminal est activé.
9. Dans le champ **Longueur du mot de passe d'activation généré automatiquement**, indiquez la longueur du mot de passe d'activation généré automatiquement. La valeur doit être comprise entre 4 et 16.
10. Dans la section **Complexité du mot de passe généré automatiquement** , sélectionnez une ou plusieurs des options suivantes :
    - Lettres minuscules
    - Lettres majuscules
    - Chiffres
    - Caractères spéciaux ou symboles
11. Cochez ou décochez la case **Activer l'inscription auprès de BlackBerry Infrastructure** pour modifier la manière dont les utilisateurs activent leurs terminaux mobiles. Si vous décochez cette case, les utilisateurs seront invités à indiquer l'adresse du serveur pour BlackBerry UEM lors de l'activation des terminaux. Pour plus d'informations, reportez-vous à Activer l'inscription de l'utilisateur auprès de BlackBerry Infrastructure .
12. Cliquez sur **Enregistrer**.

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

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

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

Sélectionnez l'option Activation du terminal avec un profil d'activation spécifique lorsque vous effectuez l'une des opérations suivantes :

- Créer un compte d'utilisateur
- Définir un mot de passe d'activation et envoyer un e-mail d'activation
- Envoyer un e-mail d'activation à plusieurs utilisateurs

Vous pouvez simultanément disposer de deux mots de passe d'activation associés à des profils d'activation spécifiques. Chaque mot de passe peut être utilisé pour activer plusieurs terminaux.

Remarque : Pour les mots de passe d'activation associés à des profils d'activation spécifiques, le paramètre « Nombre de terminaux qu'un utilisateur peut activer » du profil d'activation ne s'applique pas.

Si vous supprimez un profil d'activation auquel est associé un mot de passe d'activation, ce dernier expire automatiquement.

Si nécessaire, vous pouvez à tout moment faire expirer les mots de passe d'activation d'un utilisateur. Pour plus d'informations, reportez-vous à Faire expirer manuellement un mot de passe d'activation.

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

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

Faire expirer manuellement un mot de passe d'activation

Vous pouvez faire expirer manuellement un mot de passe d'activation précédemment généré pour un utilisateur.

1. Sur la barre de menus, cliquez sur **Utilisateurs > Terminaux gérés**.
2. Recherchez un compte d'utilisateur.
3. Dans les résultats de la recherche, cliquez sur le nom du compte d'utilisateur.
4. Dans la section **Détails d'activation**, recherchez le mot de passe d'activation que vous souhaitez faire expirer. Cliquez sur **Faire expirer**. Le mot de passe d'activation expire immédiatement.

   Si vous faites expirer un mot de passe d'activation ordinaire, la date et l'heure d'expiration apparaissent.

   Si vous faites expirer un mot de passe d'activation associé à un profil d'activation spécifique, les détails du mot de passe d'activation du terminal n'apparaissent plus.

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

Vous pouvez définir un mot de passe d'activation et envoyer à l'utilisateur un e-mail d'activation avec les informations nécessaires à l'activation d'un ou de plusieurs terminaux.

L'e-mail est envoyé depuis l'adresse électronique que vous avez configurée dans les paramètres de serveur SMTP.

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

1. Sur la barre de menus, cliquez sur **Utilisateurs et terminaux > Terminaux gérés**.
2. Recherchez un compte d'utilisateur.
3. Dans les résultats de la recherche, cliquez sur le nom du compte d'utilisateur.
4. Dans le volet Détails de l'activation, cliquez sur **Définir le mot de passe d'activation**.
5. Dans la liste déroulante **Option d'activation**, effectuez l'une des opérations suivantes :
   - Si vous souhaitez que l'utilisateur active son terminal via le profil d'activation qui lui est actuellement attribué, sélectionnez **Activation du terminal par défaut**. Le profil d'activation attribué à l'utilisateur est affiché dans la section Stratégies informatiques et profils de l'onglet Résumé.
   - Si vous souhaitez associer un mot de passe d'activation à un profil d'activation spécifique, sélectionnez **Activation du terminal avec un profil d'activation spécifique**. Pour plus d'informations, reportez-vous à Permettre aux utilisateurs d'activer des terminaux utilisant des types d'activation différents.
6. Dans la liste déroulante **Mot de passe d'activation**, effectuez l'une des opérations suivantes :
   - Si vous souhaitez que le mot de passe soit généré automatiquement, sélectionnez **Générer automatiquement le mot de passe d'activation du terminal et envoyer un e-mail contenant des instructions d'activation**. Lorsque vous sélectionnez cette option, vous devez choisir un modèle d'e-mail pour envoyer les informations à l'utilisateur.
   - Si vous souhaitez définir un mot de passe d'activation pour l'utilisateur et (facultatif) envoyer un e-mail d'activation, sélectionnez **Définir le mot de passe d'activation du terminal**.
7. Vous pouvez également modifier le champ Expiration de la période d'activation. Ce champ spécifie la durée de validité du mot de passe d'activation.
8. Pour que le mot de passe d'activation ne s'applique qu'à une seule activation, sélectionnez **La période d'activation expire à l'issue de l'activation du premier terminal**.
9. Dans la liste déroulante **Modèle d'e-mail d'activation**, sélectionnez le modèle d'e-mail que vous souhaitez utiliser. Pour plus d'informations, reportez-vous à Modèles d'e-mail.
10. Cliquez sur **Envoyer**.

Envoyer un e-mail d'activation à plusieurs utilisateurs

Vous pouvez envoyer des e-mails d'activation à plusieurs utilisateurs à la fois. Lorsque vous envoyez un e-mail d'activation à plusieurs utilisateurs, le mot de passe d'activation est généré automatiquement. Si vous souhaitez définir vous-même le mot de passe d'activation, reportez-vous à Définir un mot de passe d'activation et envoyer un e-mail d'activation.

L'e-mail est envoyé depuis l'adresse électronique que vous avez configurée dans les paramètres de serveur SMTP.

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

1. Sur la barre de menus, cliquez sur **Utilisateurs et terminaux > Terminaux gérés**.
2. Cochez la case pour chaque utilisateur auquel vous souhaitez envoyer un e-mail d'activation.
3. Cliquez sur  .
4. Dans la liste déroulante **Option d'activation**, effectuez l'une des opérations suivantes :
   - Si vous souhaitez que les utilisateurs activent leurs terminaux via le profil d'activation qui leur est actuellement attribué, sélectionnez **Activation du terminal par défaut**.
   - Si vous souhaitez associer un mot de passe d'activation à un profil d'activation spécifique, sélectionnez **Activation du terminal avec un profil d'activation spécifique**. Pour plus d'informations sur l'association de mots de passe d'activation à des profils d'activation, reportez-vous à Permettre aux utilisateurs d'activer des terminaux utilisant des types d'activation différents.
5. Dans la liste déroulante **Mot de passe d'activation**, sélectionnez **Générer automatiquement le mot de passe d'activation du terminal et envoyer un e-mail contenant des instructions d'activation**.

6. Vous pouvez également modifier le champ Expiration de la période d'activation. Ce champ spécifie la durée de validité du mot de passe d'activation.
7. Pour que le mot de passe d'activation ne s'applique qu'à une seule activation, sélectionnez **La période d'activation expire à l'issue de l'activation du premier terminal**.
8. Dans la liste déroulante **Modèle d'e-mail d'activation**, sélectionnez le modèle d'e-mail que vous souhaitez utiliser. Pour plus d'informations, reportez-vous à Modèles d'e-mail.
9. Cliquez sur **Envoyer**.

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

Vous pouvez autoriser les utilisateurs de terminaux BlackBerry 10, iOS, Android et Windows à créer leurs propres mots de passe d'activation à l'aide de BlackBerry UEM Self-Service.

Remarque : Les utilisateurs de terminaux exécutant BlackBerry OS (version 5.0 à 7.1) peuvent créer des mots de passe d'activation à l'aide de BlackBerry Web Desktop Manager.

1. Dans la barre de menus, cliquez sur **Paramètres > Paramètres généraux > Self-Service**.
2. Vérifiez que l'option **Autoriser les utilisateurs à accéder à la console en libre-service** est sélectionnée.
3. Sélectionnez **Autoriser les utilisateurs à activer des terminaux dans la console en libre-service** et procédez comme suit :
   a) Spécifiez le nombre de minutes, d'heures ou de jours pendant lesquels l'utilisateur est autorisé à activer un terminal avant que son mot de passe d'activation expire.
   b) Spécifiez le nombre minimum de caractères requis dans le mot de passe d'activation.
   c) Dans la liste déroulante **Complexité minimale des mots de passe**, sélectionnez le niveau de complexité requis pour les mots de passe d'activation.
4. Cliquez sur **Enregistrer**.

Activer l'inscription de l'utilisateur auprès de BlackBerry Infrastructure

L'inscription avec BlackBerry Infrastructure simplifie la manière dont les utilisateurs activent leurs terminaux mobiles. Une fois l'inscription activée, les utilisateurs n'ont pas besoin de saisir l'adresse du serveur lorsqu'ils activent leurs terminaux. L'inscription est activée par défaut. Si vous modifiez ce paramètre, vous devrez peut-être mettre à jour l'e-mail d'activation à l'aide de la procédure suivie par les utilisateurs pour activer leurs terminaux.

Les terminaux exécutant Windows 10 et Windows 10 Mobile n'utilisent pas la même méthode pour contacter BlackBerry Infrastructure et dès lors, l'activation ou la désactivation de l'inscription de l'utilisateur ne modifient en rien le processus d'activation de ces terminaux.

Les terminaux exécutant BlackBerry OS (versions 5.0 à 7.1) ne contactent pas BlackBerry Infrastructureet dès lors, l'activation ou la désactivation de l'inscription de l'utilisateur ne modifient en rien le processus d'activation de ces terminaux.

1. Sur la barre de menus, cliquez sur **Paramètres**.
2. Dans le volet de gauche, développez **Paramètres généraux.**
3. Cliquez sur **Paramètres d'activation par défaut.**
4. Veillez à cocher la case **Activer l'inscription auprès de BlackBerry Infrastructure**.
5. Cliquez sur **Enregistrer**.

Activer la notification d'utilisateur lorsqu'un terminal a été activé

Vous pouvez configurer UEM de sorte que l'utilisateur soit informé chaque fois qu'un terminal est activé sur son compte. La notification par e-mail est envoyée à l'adresse e-mail du compte d'utilisateur qui a été utilisé pour activer le terminal. Par défaut, l'e-mail comprend le modèle de terminal, le numéro de série et IMEI. Si l'utilisateur reçoit une notification à laquelle il ne s'attendait pas, il doit contacter un administrateur.

1. Sur la barre de menus, cliquez sur **Paramètres** > **Paramètres généraux**.
2. Cliquez sur **Paramètres d'activation par défaut.**
3. Sélectionnez **Envoyer une notification d'activation de terminal**.
4. Cliquez sur **Enregistrer**.

Tâches connexes

Modifier un modèle d'e-mail

Référence connexe

Modèles d'e-mail par défaut
Texte suggéré

Prise en charge des activations pour les terminaux Android dotés d’un profil professionnel

Pour prendre en charge les activations des terminaux Android dotés d’un profil professionnel, procédez comme suit :

- Si vous disposez d'un domaine G Suite, consultez Prendre en charge des activations de profil professionnel Android avec un domaine G Suite.
- Si vous disposez d'un domaine Google Cloud, consultez Prendre en charge des activations de profil professionnel Android avec un domaine Google Cloud.
- Vérifiez que BlackBerry Hub fonctionnera correctement sur les terminaux Android dotés d’un profil professionnel. Reportez-vous à la section Activer un BlackBerry Hub unifié.

Prendre en charge des activations de profil professionnel Android avec un domaine G Suite

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

Avant de commencer : Configurez BlackBerry UEM pour prendre en charge les terminaux Android dotés d’un profil professionnel. Pour plus d'informations sur la configuration de BlackBerry UEM afin de prendre en charge les terminaux Android dotés d’un profil professionnel, reportez-vous au contenu relatif à la configuration.

1. Dans votre domaine G Suite, créez des comptes d'utilisateur pour vos utilisateurs Android.
2. Si les utilisateurs ont des terminaux exécutant Android 6.0 ou ultérieur, vérifiez que le paramètre **Appliquer la stratégie EMM** est activé pour le domaine G Suite.

   Ce paramètre est obligatoire pour les terminaux avec le type d'activation Espace Travail uniquement et fortement recommandé pour les terminaux avec d'autres types d'activation. Si ce paramètre n'est pas

sélectionné, les utilisateurs peuvent ajouter un compte Google géré au terminal qui peut accéder à ses applications à l'extérieur du profil de travail.

3. Si vous prévoyez d'attribuer le type d'activation Espace Travail uniquement et que certains utilisateurs disposent de terminaux exécutant Android 6.0 ou version ultérieure, sélectionnez le paramètre **Appliquer la stratégie EMM** dans le domaine G Suite.
4. Dans BlackBerry UEM, créez des comptes d'utilisateur locaux pour vos utilisateurs Android. L'adresse électronique de chaque compte doit correspondre à l'adresse électronique du compte G Suite correspondant.
5. Assurez-vous que vos utilisateurs connaissent le mot de passe de leurs comptes G Suite.
6. Dans BlackBerry UEM, attribuez un profil de messagerie et des applications de productivité pour les utilisateurs, les groupes d'utilisateurs ou de terminaux.

Prendre en charge des activations de profil professionnel Android avec un domaine Google Cloud

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

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

1. Dans BlackBerry UEM, créez des comptes d'utilisateur associés à l'annuaire pour vos utilisateurs Android ayant un profil professionnel.
2. Si vous choisissez de ne pas autoriser BlackBerry UEM à créer des comptes d'utilisateurs dans votre domaine Google Cloud, vous devez créer des comptes d'utilisateurs dans votre domaine Google Cloud et dans BlackBerry UEM. Effectuez l'une des opérations suivantes :
   - Dans votre domaine Google Cloud, créez des comptes d'utilisateur pour vos utilisateurs Android ayant un profil professionnel. Chaque adresse électronique doit correspondre à l'adresse électronique du compte d'utilisateur BlackBerry UEM correspondant. Assurez-vous que vos utilisateurs ayant un profil professionnel Android connaissent le mot de passe de leur compte Google Cloud.
   - Utilisez l'outil Synchronisation de répertoire d'applications Google pour synchroniser votre domaine Google Cloud avec votre répertoire d'entreprise. Ce faisant, vous n'êtes pas tenu de créer de comptes d'utilisateur manuellement dans votre domaine Google Cloud.
3. Si vous prévoyez d'attribuer le type d'activation Espace Travail uniquement et que certains utilisateurs disposent de terminaux exécutant Android 6.0 ou version ultérieure, sélectionnez le paramètre **Appliquer la stratégie EMM** dans le domaine Google Cloud.
4. Dans BlackBerry UEM, attribuez un profil de messagerie et des applications de productivité pour les utilisateurs, les groupes d'utilisateurs ou de terminaux.

Activer un BlackBerry Hub unifié

BlackBerry Hub est une application qui permet aux utilisateurs d'afficher les messages, les notifications et les évènements dans un seul endroit.

Pour autoriser les utilisateurs disposant de terminaux Android dotés d'un profil professionnel à afficher les messages professionnels et personnels dans BlackBerry Hub, vous devez vérifier certains paramètres dans BlackBerry UEM.

1. Pour la stratégie informatique qui est attribuée aux utilisateurs, dans la section BlackBerry Productivity Suite, vérifiez que la règle de stratégie informatique Autoriser l'affichage unifié des comptes dans BlackBerry Hub est sélectionnée.

2. Effectuez l'une des tâches suivantes :
   - Si vous configurez les paramètres de BlackBerry Hub dans un profil de messagerie, dans l'onglet Android du profil de messagerie, vérifiez que les éléments suivants sont sélectionnés :
     - Autoriser le partage de données entre les profils professionnel et personnel
     - Autoriser les applications personnelles à accéder aux données professionnelles
   - Si vous configurez les paramètres de BlackBerry Hub dans une configuration d'application, vérifiez que les éléments suivants sont sélectionnés :
     - Profils IPC
     - Accéder au contenu professionnel

À la fin :

Pour plus d'informations sur l'utilisation de BlackBerry Hub sur les terminaux (ajout d'un compte de messagerie ou personnalisation des paramètres BlackBerry Hub, par exemple) reportez-vous au contenu relatif à BlackBerry Hub.

Pour obtenir des informations sur la résolution de problèmes, rendez-vous sur le site http://support.blackberry.com/kb et lisez l'article 37721.

Prise en charge des activations Windows 10

Vous pouvez aider les utilisateurs à activer les terminaux Windows 10 de deux manières :

- Déployer un service de repérage pour simplifier les activations Windows 10. Pour plus d'informations, reportez-vous au contenu relatif à la configuration.
- Créer ou modifier un modèle d'e-mail d'activation pour fournir les informations d'activation Windows 10. Pour plus d'informations, reportez-vous à la section « Créer un modèle d'e-mail d'activation ».

Création de profils d'activation

Vous pouvez contrôler la manière dont les terminaux sont activés et gérés à l'aide des profils d'activation. Un profil d'activation indique le nombre et le type de terminaux qu'un utilisateur peut activer et le type d'activation à utiliser pour chaque type de terminal.

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

Le profil d'activation attribué s'applique uniquement aux terminaux activés par l'utilisateur après que vous avez attribué le profil. Les terminaux déjà activés ne sont pas automatiquement mis à jour pour correspondre au profil d'activation nouveau ou mis à jour.

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

Les profils d'activation ne s'appliquent pas aux terminaux BlackBerry OS (versions 5.0 à 7.1).

Créer un profil d'activation

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Stratégie > Activation**.

3. Cliquez sur +.
4. Saisissez le nom et la description du profil.
5. Dans le champ **Nombre de terminaux qu'un utilisateur peut activer**, spécifiez le nombre maximum de terminaux que l'utilisateur peut activer.
6. Dans la liste déroulante **Propriété du terminal**, sélectionnez le paramètre par défaut de la propriété du terminal. Effectuez l'une des opérations suivantes :
   - Si certains utilisateurs activent des terminaux personnels et d'autres des terminaux professionnels, sélectionnez **Non spécifié**.
   - Si les utilisateurs activent généralement des terminaux professionnels, sélectionnez **Professionnel**.
   - Si les utilisateurs activent généralement des terminaux personnels, sélectionnez **Personnel**.
7. Vous pouvez, à votre convenance, sélectionner un avis d'entreprise dans la liste déroulante **Attribuer un avis d'entreprise**. Si vous affectez un avis d'entreprise, les utilisateurs activant des terminaux BlackBerry 10, Windows 10, iOS ou macOS doivent accepter l'avis pour terminer le processus d'activation.
8. Dans la section **Types de terminaux que les utilisateurs peuvent activer**, sélectionnez les types de terminaux, selon les besoins. Les types de terminaux que vous ne sélectionnez pas ne sont pas inclus dans le profil d'activation et les utilisateurs ne peuvent pas activer ces terminaux.
9. Procédez comme suit pour chaque type de terminal inclus dans le profil d'activation :
   - Cliquez sur l'onglet correspondant au type de terminal.
   - Dans la liste déroulante **Limites de modèles de terminaux**, sélectionnez si vous souhaitez autoriser ou restreindre les terminaux spécifiés ou n'appliquer aucune restriction. Cliquez sur **Modifier** pour sélectionner les terminaux que vous souhaitez restreindre ou autoriser, puis cliquez sur **Enregistrer**.
   - Dans la liste déroulante **Version autorisée**, sélectionnez la version minimale autorisée.
   - Dans l'onglet **Windows**, vous pouvez sélectionner l'une des options de facteur de forme ou les deux, et choisir d'autoriser ou d'interdire ces facteurs de forme dans la liste déroulante **Restrictions relatives au modèle de terminal**.
   - Dans la section **Type d'activation**, sélectionnez un type d'activation.
     - Pour les terminaux Android, vous pouvez sélectionner plusieurs types d'activation et les classer selon les besoins de votre entreprise.
     - Pour les terminaux Android, si vous sélectionnez le type d'activation « contrôles MDM » et que vous ne voulez pas que les règles de stratégie MDM KNOX soient appliquées aux terminaux, désactivez la case **Activer Samsung KNOX sur les terminaux Samsung pour lesquels a été attribué le type d'activation contrôles MDM**. Ce paramètre s'applique uniquement aux terminaux qui prennent en charge KNOX MDM.
     - Pour les terminaux Android, si vous sélectionnez l'un des types d'activation Samsung KNOX et que vous souhaitez utiliser Google Play pour gérer les applications de travail, sélectionnez **Gestion de l'application Google Play pour les appareils Samsung Knox Workspace**. Cette option est disponible uniquement si vous avez configuré une connexion à un domaine Google. Pour plus d'informations, consultez le contenu relatif à la configuration.
     - Pour les terminaux iOS, si vous sélectionnez le type d'activation Confidentialité de l'utilisateur et que vous voulez activer le modèle de licence SIM, vous devez sélectionner l'option **Autoriser l'accès à la carte SIM et aux informations matérielles du terminal pour activer le modèle de licence SIM**.
     - Pour les terminaux iOS, si vous sélectionnez les commandes MDM ou les types d'activation Confidentialité de l'utilisateur (avec modèle de licence SIM), vous pouvez bloquer les terminaux non supervisés en sélectionnant Ne pas autoriser l'activation des terminaux non supervisés.
10. Cliquez sur **Ajouter**.

À la fin : Si nécessaire, classez les profils.

Tâches connexes

Attribuer un profil ou une stratégie informatique à un groupe d'utilisateurs
Attribuer un profil ou une stratégie informatique à un compte d'utilisateur
Créer des avis d'entreprise

Types d'activation : terminaux BlackBerry 10

Type d'activation	Description
Travail et Personnel - Entreprise	Ce type d'activation fournit un contrôle des données professionnelles sur les terminaux, tout en veillant à assurer la confidentialité des données personnelles. Lorsqu'un terminal est activé, un espace Travail séparé est créé sur le terminal et l'utilisateur doit définir un mot de passe pour accéder à l'espace Travail. Les données professionnelles sont protégées à l'aide du cryptage et de l'authentification par mot de passe. Toutes les données professionnelles des précédentes activations sont supprimées. Vous pouvez contrôler l'espace Travail sur le terminal à l'aide de commandes et de stratégies informatiques, mais vous ne pouvez contrôler aucun aspect de l'espace Personnel sur le terminal.
Espace Travail uniquement	Ce type d'activation offre un contrôle complet du terminal et ne fournit pas un espace séparé pour les données personnelles. Lorsqu'un terminal est activé, l'espace Personnel et toutes les données professionnelles des précédentes activations sont supprimées. Un espace Travail est installé et l'utilisateur doit créer un mot de passe pour accéder au terminal. Les données professionnelles sont protégées à l'aide du cryptage et de l'authentification par mot de passe. Vous pouvez contrôler le terminal à l'aide de commandes et de stratégies informatiques.
Travail et Personnel - Régulé	Ce type d'activation permet de contrôler à la fois les données professionnelles et personnelles. Lorsqu'un terminal est activé, un espace Travail séparé est créé sur le terminal et l'utilisateur doit définir un mot de passe pour accéder à l'espace Travail. Les données professionnelles sont protégées à l'aide du cryptage et de l'authentification par mot de passe. Toutes les données professionnelles des précédentes activations sont supprimées. Vous pouvez contrôler à la fois l'espace Travail et l'espace Personnel sur le terminal à l'aide de commandes et de stratégies informatiques.

Types d'activation : terminaux iOS

Type d'activation	Description
Contrôles MDM	Ce type d'activation fournit une gestion de base des terminaux à l'aide des commandes de terminaux mises à disposition par iOS. Il n'existe pas d'espace Travail séparé installé sur le terminal, et aucune sécurité ajoutée pour les données professionnelles. Vous pouvez contrôler le terminal à l'aide de commandes et de stratégies informatiques. Lors de l'activation, les utilisateurs disposant d'un terminal doivent installer un profil de gestion des terminaux mobiles.
Confidentialité de l'utilisateur	Vous pouvez utiliser le type d'activation Confidentialité de l'utilisateur afin de fournir une base de contrôle des terminaux tout en veillant à assurer la confidentialité des données personnelles des utilisateurs. Avec ce type d'activation, aucun conteneur séparé n'est installé sur le terminal, et aucune sécurité supplémentaire n'est fournie pour les données professionnelles. Les terminaux activés avec Confidentialité de l'utilisateur sont activés sur BlackBerry UEM et peuvent utiliser des services tels que Trouver mon téléphone et Détection du statut débridé, mais les administrateurs ne peuvent pas contrôler les stratégies du terminal. **Remarque :** Pour le modèle de licence SIM, vous devez sélectionner l'option « Autoriser l'accès à la carte SIM et aux informations matérielles du terminal pour activer le modèle de licence SIM » dans le profil d'activation. Les utilisateurs doivent installer un profil MDM qui peut uniquement accéder à la carte SIM et aux informations matérielles du terminal qui sont requises pour déterminer si une licence SIM appropriée est disponible (par exemple, ICCID et IMEI). Ce type d'activation n'est pris en charge que par les terminaux Apple TV.
Inscription du terminal pour BlackBerry 2FA uniquement	Ce type d'activation prend en charge la solution BlackBerry 2FA pour les terminaux qui ne sont pas gérés par BlackBerry UEM. Ce type d'activation ne fournit aucune gestion ni aucun contrôle des terminaux, mais permet aux terminaux d'utiliser la fonctionnalité BlackBerry 2FA. Pour utiliser ce type d'activation, vous devez également attribuer le profil BlackBerry 2FA aux utilisateurs. Lorsqu'un terminal est activé, vous pouvez afficher des informations de terminal limitées dans la console de gestion, et vous pouvez désactiver le terminal à l'aide d'une commande. Ce type d'activation est pris en charge uniquement pour les utilisateurs Microsoft Active Directory. Ce type d'activation n'est pris en charge que par les terminaux Apple TV. Pour plus d'informations, reportez-vous au contenu BlackBerry 2FA.

Types d'activation : terminaux macOS

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

Types d'activation : terminaux Android

Pour les terminaux Android, vous pouvez sélectionner plusieurs types d'activation et les classer pour vous assurer que BlackBerry UEM attribue le type d'activation le plus approprié à ces terminaux. Par exemple, si vous classez « Espace Travail uniquement (Samsung KNOX) » en premier et « Contrôles MDM » en deuxième, les terminaux prenant en charge Samsung KNOX Workspace reçoivent le premier type d'activation.

Remarque : KNOX MDM permet au terminal d'utiliser les règles de stratégie informatique KNOX MDM dans BlackBerry UEM plutôt que les règles de base disponibles pour tous les terminaux Android. KNOX Workspace crée un espace Travail séparé sur le terminal afin de séparer les données et les applications professionnelles des données et des applications personnelles.

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

- Android
- Terminaux Android dotés d'un profil professionnel
- Samsung KNOX Workspace

terminaux Android

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

Type d'activation	Description
Contrôles MDM	Ce type d'activation vous permet de gérer le terminal à l'aide de commandes et de règles de stratégie informatique. Si le terminal prend en charge KNOX MDM, ce type d'activation s'applique aux règles de stratégie informatique KNOX MDM. Un espace Travail distinct n'est pas créé sur le terminal, et il n'existe aucune sécurité ajoutée pour les données professionnelles. Si vous ne souhaitez pas appliquer les règles de stratégie MDM KNOX, décochez la case **Activer Samsung KNOX sur les terminaux Samsung où le type d'activation Commandes MDM est attribué**. Ce paramètre s'applique uniquement aux terminaux qui prennent en charge KNOX MDM. Lors de l'activation, les utilisateurs doivent octroyer les autorisations d'administrateur à BlackBerry UEM Client. Ce type d'activation sera obsolète dans une future version. Pour plus d'informations, rendez-vous sur http://support.blackberry.com/kb et consultez l'article KB 47875.
Confidentialité de l'utilisateur	Vous pouvez utiliser le type d'activation Confidentialité de l'utilisateur afin de fournir une base de contrôle des terminaux tout en veillant à assurer la confidentialité des données personnelles des utilisateurs. Avec ce type d'activation, aucun conteneur séparé n'est installé sur le terminal, et aucune sécurité supplémentaire n'est fournie pour les données professionnelles. Les terminaux activés avec Confidentialité de l'utilisateur sont activés sur BlackBerry UEM et peuvent utiliser des services tels que Trouver mon téléphone et Détection du statut débridé, mais les administrateurs ne peuvent pas contrôler les stratégies du terminal.
BlackBerry 2FA	Ce type d'activation prend en charge la solution BlackBerry 2FA pour les terminaux qui ne sont pas gérés par BlackBerry UEM. Ce type d'activation ne fournit aucune gestion ni aucun contrôle des terminaux, mais permet aux terminaux d'utiliser la fonctionnalité BlackBerry 2FA. Pour utiliser ce type d'activation, vous devez également attribuer le profil BlackBerry 2FA aux utilisateurs. Lorsqu'un terminal est activé, vous pouvez afficher des informations de terminal limitées dans la console de gestion, et vous pouvez désactiver le terminal à l'aide d'une commande. Ce type d'activation est pris en charge uniquement pour les utilisateurs Microsoft Active Directory. Pour plus d'informations, reportez-vous au contenu BlackBerry 2FA.

Terminaux Android dotés d'un profil professionnel

Les types d'activation suivants s'appliquent uniquement aux terminaux Android dotés d'un profil professionnel.

Type d'activation	Description
Travail et Personnel - Confidentialité de l'utilisateur	Ce type d'activation préserve la confidentialité des données personnelles, mais vous permet de gérer les données professionnelles à l'aide de commandes et de règles de stratégie informatique. Ce type d'activation crée un profil professionnel sur le terminal qui sépare les données professionnelles des données personnelles. Les données professionnelles et personnelles sont protégées à l'aide du cryptage et de l'authentification par mot de passe. Ce type d'activation ne prend pas en charge BlackBerry Secure Connect Plus. Les utilisateurs ne sont pas tenus d'octroyer des autorisations d'administrateur à BlackBerry UEM Client.
Travail et Personnel - Confidentialité de l'utilisateur (Premium)	Ce type d'activation préserve la confidentialité des données personnelles, mais vous permet de gérer les données professionnelles à l'aide de commandes et de règles de stratégie informatique. Ce type d'activation crée un profil professionnel sur le terminal qui sépare les données professionnelles des données personnelles. Les données professionnelles et personnelles sont protégées à l'aide du cryptage et de l'authentification par mot de passe. Les utilisateurs ne sont pas tenus d'octroyer des autorisations d'administrateur à BlackBerry UEM Client. Vous devez utiliser ce type d'activation si vous souhaitez prendre en charge BlackBerry Secure Connect Plus avec les caractéristiques du type d'activation Travail et Personnel - Confidentialité de l'utilisateur.

Type d'activation	Description
Espace Travail uniquement	Si vous attribuez ce type d'activation à un utilisateur, vous devez également attribuer le modèle d'e-mail d'activation Espace Travail uniquement à cet utilisateur. L'attribution de ce modèle permet de s'assurer que l'utilisateur reçoit le code d'activation Google nécessaire pendant le processus d'activation. Ce type d'activation vous permet de gérer le terminal dans son ensemble à l'aide de commandes et de règles de stratégie informatique. Ce type d'activation requiert que l'utilisateur restaure les réglages d'usine du terminal avant de procéder à l'activation. Le processus d'activation installe un profil de travail et aucun profil personnel. L'utilisateur doit créer un mot de passe pour accéder au terminal. Toutes les données du terminal sont protégées à l'aide du cryptage et d'une méthode d'authentification de type mot de passe. Ce type d'activation ne prend pas en charge BlackBerry Secure Connect Plus. Lors de l'activation, le terminal installe automatiquement BlackBerry UEM Client et lui accorde des autorisations d'administrateur. Les utilisateurs ne peuvent pas révoquer les autorisations d'administrateur ni désinstaller l'application. Si le terminal prend en charge KNOX MDM, les stratégies KNOX MDM suivantes s'appliquent également au terminal : • Autoriser l'authentification par iris • Autoriser l'authentification faciale • SSID Wi-Fi non autorisés • Autoriser les MMS entrants • Autoriser les MMS sortants

Type d'activation	Description
Espace Travail uniquement (Premium)	Si vous attribuez ce type d'activation à un utilisateur, vous devez également attribuer le modèle d'e-mail d'activation Espace Travail uniquement à cet utilisateur. L'attribution de ce modèle permet de s'assurer que l'utilisateur reçoit le code d'activation Google nécessaire pendant le processus d'activation. Ce type d'activation vous permet de gérer le terminal dans son ensemble à l'aide de commandes et de règles de stratégie informatique. Ce type d'activation requiert que l'utilisateur restaure les réglages d'usine du terminal avant de procéder à l'activation. Le processus d'activation installe un profil de travail et aucun profil personnel. L'utilisateur doit créer un mot de passe pour accéder au terminal. Toutes les données du terminal sont protégées à l'aide du cryptage et d'une méthode d'authentification de type mot de passe. Ce type d'activation prend en charge la consignation de l'activité du terminal (SMS, MMS et appels téléphoniques) dans les fichiers journaux BlackBerry UEM. Lors de l'activation, le terminal installe automatiquement BlackBerry UEM Client et lui accorde des autorisations d'administrateur. Les utilisateurs ne peuvent pas révoquer les autorisations d'administrateur ni désinstaller l'application. Vous devez utiliser ce type d'activation si vous souhaitez prendre en charge BlackBerry Secure Connect Plus avec les caractéristiques du type d'activation Espace Travail uniquement. Si le terminal prend en charge KNOX MDM, les stratégies KNOX MDM suivantes s'appliquent également au terminal : • Autoriser l'authentification par iris • Autoriser l'authentification faciale • SSID Wi-Fi non autorisés • Autoriser les MMS entrants • Autoriser les MMS sortants • Valider les certificats installés par l'utilisateur final

terminaux Samsung KNOX Workspace

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

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

Types d'activation : terminaux Windows

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

Instructions d'activation destinées aux utilisateurs

Si nécessaire, vous pouvez fournir des instructions pas à pas aux utilisateurs pour les aider à activer leurs terminaux.

Activation des terminaux Android

Les informations que les utilisateurs doivent entrer et les étapes qu'ils doivent suivre pour activer un terminal Android dépendent du type d'activation attribué. Les modèles d'e-mails d'activation contiennent les informations dont les utilisateurs ont besoin. Pour plus d'informations, reportez-vous à Modèles d'e-mail.

Pour les activations deQR Code, consultezActiver un terminal à l'aide de QR Code.

Activer un terminal Android

Remarque : Ces étapes s'appliquent à un terminal doté du type d'activation Contrôles MDM. Les types d'activation qui installent ou activent un espace Travail sur le terminal peuvent nécessiter des étapes supplémentaires.

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

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

À la fin : pour vérifier que le processus d'activation a réussi, effectuez l'une des opérations suivantes.

- Sur le terminal, ouvrez BlackBerry UEM Client. Sélectionnez **À propos de**. Dans la section **Terminal activé**, assurez-vous de la présence des informations sur le terminal et de l'heure et de la date d'activation.

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

Activer un terminal Android doté d'un profil professionnel

Ces étapes s'appliquent aux terminaux utilisant l'un des types d'activation suivants :

- Travail et Personnel - Confidentialité de l'utilisateur
- Travail et Personnel - Confidentialité de l'utilisateur (Premium)

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

Avant de commencer :

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

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

Activer un terminal Android doté d'un profil professionnel avec un espace Travail uniquement

Ces étapes s'appliquent aux terminaux utilisant l'un des types d'activation suivants :

- Espace Travail uniquement
- Espace Travail uniquement (Premium)

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

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

- Mot de passe d'activation BlackBerry UEM
- Code d'activation de profil professionnel Android
- Votre adresse électronique professionnelle et votre mot de passe

- Adresse du serveur BlackBerry UEM (celle-ci ne vous sera peut-être pas nécessaire)

1. Si l'écran d'accueil du programme d'installation n'apparait pas, réinitialisez les paramètres par défaut du terminal.
2. Lors de la configuration du terminal, sur l'écran **Ajouter votre compte**, sélectionnez **Menu > Configuration d'un terminal professionnel**.
3. Si vous êtes invité, cryptez le terminal.
4. Sur le terminal, sélectionnez **UEM Client**.
5. Lisez le contrat de licence. Sélectionnez **J'accepte**.
6. Saisissez votre adresse électronique professionnelle. Sélectionnez **Suivant**.
7. Si nécessaire, entrez l'adresse du serveur. Sélectionnez **Suivant**. Vous trouverez l'adresse du serveur dans l'e-mail d'activation que vous avez reçu ou dans BlackBerry UEM Self-Service.
8. Saisissez votre mot de passe d'activation. Sélectionnez **Activer mon terminal**.
9. Attendez la fin du transfert des profils et paramètres.
10. Sélectionnez **Configurer**.
11. Sélectionnez **OK** et attendez la fin de la configuration du profil professionnel.
12. Saisissez votre mot de passe Google.
13. Sélectionnez **Suivant**.
14. Sur l'écran de **Déverrouiller la sélection**, sélectionnez **Mot de passe**.
15. Vérifiez que le champ **Mot de passe requis pour démarrer le terminal** est sélectionné. Sélectionnez **Continuer**.
16. Saisissez un mot de passe, puis saisissez-le à nouveau pour le confirmer. Sélectionnez **OK**.
17. Sélectionnez une option pour l'envoi des notifications. Sélectionnez **Terminé**.
18. Si vous y êtes invité, sélectionnez **OK** pour vous connecter à BlackBerry Secure Connect Plus et attendez que la connexion soit établie.
19. Dans l'écran d'accueil, ouvrez la liste des applications. Sélectionnez l'application BlackBerry Hub pour valider la configuration.
    a) Sélectionnez **Suivant** pour autoriser les services BlackBerry à accéder à votre terminal et, si vous y êtes invité, sélectionnez **Autoriser** sur chacun des écrans suivants.
    b) Sélectionnez la flèche pour continuer.
    c) Sélectionnez **Accorder les autorisations** pour autoriser BlackBerry Hub à accéder à votre terminal. Si vous êtes invité, sélectionnez **Autoriser** sur chacun des écrans suivants.
    d) Sélectionnez votre adresse électronique.
    e) Saisissez le mot de passe de votre messagerie professionnelle. Sélectionnez **Suivant**.
    f) Sélectionnez **OK**.
    g) Dans l'écran **Administration à distance de la sécurité**, sélectionnez **OK**.
    h) Dans l'écran **Configuration du compte**, sélectionnez **Suivant**.
    i) Dans l'écran **Mise à jour de sécurité**, sélectionnez **OK**.
    j) Sélectionnez **Activer** pour activer l'administrateur du terminal.
    k) Sélectionnez **Terminé**.
20. Rendez-vous sur BlackBerry Hub et attendez que vos e-mails soient synchronisés.

Activation d'un terminal Android en mode Espace Travail uniquement (sans domaine Google)

Ces étapes s'appliquent aux terminaux utilisant l'un des types d'activation suivants :

- Espace Travail uniquement
- Espace Travail uniquement (Premium)

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

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

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

1. Si l'écran d'accueil du programme d'installation n'apparait pas, réinitialisez les paramètres par défaut du terminal.
2. Lors de la configuration du terminal, sur l'écran **Ajouter votre compte**, saisissez afw#blackberry.
3. Attendez la fin de la mise à jour des applications système et des téléchargements de BlackBerry UEM Client.
4. Lisez le contrat de licence. Sélectionnez **J'accepte**.
5. Saisissez votre adresse électronique professionnelle. Sélectionnez **Suivant**.
6. Si nécessaire, entrez l'adresse du serveur. Sélectionnez **Suivant**. Vous trouverez l'adresse du serveur dans l'e-mail d'activation que vous avez reçu ou dans BlackBerry UEM Self-Service.
7. Saisissez votre mot de passe d'activation. Sélectionnez **Activer mon terminal**.
8. Attendez la fin du transfert des profils et paramètres.
9. Sélectionnez **Configurer**.
10. Sélectionnez **OK** et attendez la fin de la configuration du profil professionnel.
11. Saisissez votre mot de passe Google.
12. Sélectionnez **Suivant**.
13. Sur l'écran de **Déverrouiller la sélection**, sélectionnez **Mot de passe**.
14. Vérifiez que le champ **Mot de passe requis pour démarrer le terminal** est sélectionné. Sélectionnez **Continuer**.
15. Saisissez un mot de passe, puis saisissez-le à nouveau pour le confirmer. Sélectionnez **OK**.
16. Sélectionnez une option pour l'envoi des notifications. Sélectionnez **Terminé**.
17. Si vous y êtes invité, sélectionnez **OK** pour vous connecter à BlackBerry Secure Connect Plus et attendez que la connexion soit établie.
18. Dans l'écran d'accueil, ouvrez la liste des applications. Sélectionnez l'application BlackBerry Hub pour valider la configuration.
    a) Sélectionnez **Suivant** pour autoriser les services BlackBerry à accéder à votre terminal et, si vous y êtes invité, sélectionnez **Autoriser** sur chacun des écrans suivants.
    b) Sélectionnez la flèche pour continuer.
    c) Sélectionnez **Accorder les autorisations** pour autoriser BlackBerry Hub à accéder à votre terminal. Si vous y êtes invité, sélectionnez **Autoriser** sur chacun des écrans suivants.
    d) Sélectionnez votre adresse électronique.
    e) Saisissez le mot de passe de votre messagerie professionnelle. Sélectionnez **Suivant**.
    f) Sélectionnez **OK**.
    g) Dans l'écran **Administration à distance de la sécurité**, sélectionnez **OK**.
    h) Dans l'écran **Configuration du compte**, sélectionnez **Suivant**.
    i) Dans l'écran **Mise à jour de sécurité**, sélectionnez **OK**.
    j) Sélectionnez **Activer** pour activer l'administrateur du terminal.
    k) Sélectionnez **Terminé**.
19. Rendez-vous sur BlackBerry Hub et attendez que vos e-mails soient synchronisés.

Activer un terminal iOS

Pour les activations deQR Code, consultezActiver un terminal à l'aide de QR Code.

Pour activer des terminaux à l'aide d'un mot de passe d'activation, envoyez les instructions suivantes à l'utilisateur concerné.

1. Sur le terminal, installez l'application BlackBerry UEM Client. Vous pouvez télécharger l'application BlackBerry UEM Client sur l'App Store.
2. Sur le terminal, sélectionnez **UEM Client**.
3. Lisez l'accord de licence et sélectionnez **J'accepte**.
4. Saisissez votre adresse électronique professionnelle et sélectionnez **Atteindre**.
5. Si nécessaire, saisissez l'adresse du serveur, puis sélectionnez **Atteindre**. Vous trouverez l'adresse du serveur dans l'e-mail d'activation que vous avez reçu ou dans BlackBerry UEM Self-Service.
6. Saisissez votre mot de passe d'activation et sélectionnez **Activer mon terminal**.
7. Sélectionnez **OK** pour installer le certificat requis.
8. Suivez les instructions à l'écran pour procéder à l'installation.
9. Si vous êtes invité à saisir le mot de passe de votre compte de messagerie ou le mot de passe de votre terminal, suivez les instructions à l'écran.

À la fin : pour vérifier que le processus d'activation a réussi, effectuez l'une des opérations suivantes.

- Sur le terminal, ouvrez l'application BlackBerry UEM Client et sélectionnez **À propos de**. Dans les sections Terminal activé et État de conformité, vérifiez que les informations concernant le terminal et l'horodatage d'activation sont présentes.
- Dans BlackBerry UEM Self-Service, vérifiez que votre terminal est répertorié en tant que terminal activé. Après l'activation du terminal, la mise à jour de l'état peut prendre jusqu'à deux minutes.

Activer un terminal BlackBerry 10

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

1. Sur le terminal, accédez à **Paramètres**.
2. Sélectionnez **Comptes**.
3. Si vous disposez déjà de comptes sur ce terminal, sélectionnez **Ajouter un compte**. Sinon, passez à l'étape 4.
4. Sélectionnez **Messagerie, Calendrier et Contacts**.
5. Saisissez votre adresse électronique professionnelle et sélectionnez **Suivant**.
6. Dans le champ **Mot de passe**, saisissez le mot de passe d'activation que vous avez reçu. Sélectionnez **Suivant**.
7. Si vous recevez un avertissement vous indiquant que votre terminal n'a pas pu rechercher les informations de connexion, procédez comme suit :
   a) Sélectionnez **Avancé**.
   b) Sélectionnez **Compte professionnel**.
   c) Dans le champ **Adresse du serveur**, saisissez l'adresse du serveur. Vous trouverez l'adresse du serveur dans l'e-mail d'activation que vous avez reçu ou dans BlackBerry UEM Self-Service.
   d) Sélectionnez **Terminé**.
8. Suivez les instructions à l'écran pour procéder à l'activation.

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

- Sur le terminal, accédez à BlackBerry Hub et vérifiez que l'adresse électronique est présente. Accédez au Calendrier et vérifiez que les rendez-vous sont présents.
- Dans BlackBerry UEM Self-Service, vérifiez que votre terminal est répertorié en tant que terminal activé. Après l'activation du terminal, la mise à jour de l'état peut prendre jusqu'à deux minutes.

Activer un terminal Windows Phone

Notes du formateur: Ces étapes s'appliquent à Windows Phone 8.1. Si les participants utilisent Windows Phone 8.0, après avoir copié l'adresse du serveur, ils doivent accéder manuellement aux applications Windows Phone et revenir ensuite à BlackBerry UEM Client.

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

1. Sur le terminal, installez BlackBerry UEM Client. Vous pouvez télécharger BlackBerry UEM Client depuis Windows Store.
2. Sur le terminal, accédez à la liste des applications et sélectionnez **UEM Client**.
3. Lisez l'accord de licence et sélectionnez **J'accepte**.
4. Saisissez votre adresse électronique professionnelle et sélectionnez **Suivant**.
5. Si nécessaire, saisissez l'adresse du serveur, puis sélectionnez **Suivant**. Vous trouverez l'adresse du serveur dans l'e-mail d'activation que vous avez reçu ou dans BlackBerry UEM Self-Service.
6. Saisissez le mot de passe d'activation que vous avez reçu dans l'e-mail d'activation ou que vous avez défini dans BlackBerry UEM Self-Service et sélectionnez **Activer mon terminal**.
7. Sélectionnez **Copier et continuer** pour copier l'adresse du serveur et accéder à l'application Windows Phone Workplace.
8. Sélectionnez **Ajouter un compte**.
9. Saisissez votre adresse électronique et sélectionnez **Connexion**.
10. Positionnez votre curseur dans le champ Serveur et sélectionnez l'icône **Coller**.
11. Sélectionnez **Connexion**.
12. Si vous recevez un avertissement au sujet d'un certificat, sélectionnez **Continuer**.
13. Ne saisissez rien dans les champs Nom d'utilisateur et Domaine. Dans le champ Mot de passe, saisissez le mot de passe d'activation que vous avez reçu dans l'e-mail d'activation ou que vous avez défini dans BlackBerry UEM Self-Service. Sélectionnez **Connexion**.
14. Sélectionnez **Terminé**.
15. Sélectionnez le bouton **Retour** de votre Windows Phone pour revenir à BlackBerry UEM Client.
16. L'activation est automatique.

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

- Sur le terminal, ouvrez BlackBerry UEM Client, sélectionnez l'icône **Menu** en bas à droite (trois points horizontaux) et sélectionnez **À propos de**. Dans la section Terminal activé, assurez-vous de la présence des informations du terminal et de l'heure et de la date d'activation.
- Dans BlackBerry UEM Self-Service, vérifiez que votre terminal est répertorié en tant que terminal activé. Après l'activation du terminal, la mise à jour de l'état peut prendre jusqu'à deux minutes.

Activer un terminal Windows 10 Mobile

Notes du formateur: Ces étapes s'appliquent aux smartphones utilisant Windows 10 Mobile. Si les participants utilisent des tablettes ou ordinateurs Windows 10, utilisez les étapes permettant d'Activer un terminal Windows 10.

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

1. Dans le navigateur de votre terminal, saisissez ou collez l'adresse du serveur de certificats. Vous trouverez l'adresse du serveur de certificats dans l'e-mail d'activation que vous avez reçu. Si vous n'avez pas reçu de lien vers le certificat, contactez votre administrateur pour obtenir de l'aide.
2. Sélectionnez le certificat.
3. Sélectionnez **Installer**.
4. Sélectionnez **OK**.
5. Sélectionnez le bouton **Windows** pour retourner au menu de démarrage.
6. Faites glisser l'écran vers la gauche pour ouvrir le menu Applications.
7. Effectuez l'une des tâches suivantes :

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

8. Dans le champ **Adresse e-mail**, saisissez votre adresse électronique professionnelle et sélectionnez **Entrée**.
9. Si vous y êtes invité, dans le champ **Serveur**, saisissez le nom du serveur, puis sélectionnez **Continuer**. Vous trouverez le nom du serveur dans l'e-mail d'activation que vous avez reçu de votre administrateur ou dans BlackBerry UEM Self-Service lors de la définition de votre mot de passe d'activation.
10. Dans le champ **Mot de passe d'activation**, saisissez votre mot de passe d'activation, puis sélectionnez **Continuer**. Vous trouverez votre mot de passe d'activation dans un des e-mails que vous avez reçus de votre administrateur. Vous pouvez aussi définir votre propre mot de passe d'activation dans BlackBerry UEM Self-Service.
11. Sélectionnez **Terminé**.
12. Le processus d'activation est terminé.

À la fin :

- Pour vérifier que le processus d'activation a abouti, effectuez l'une des opérations suivantes :
  - Sur le terminal, cliquez sur Paramètres > Comptes > Accès professionnel ou scolaire (ou Accès professionnel) pour vérifier que votre terminal est connecté à BlackBerry UEM. Cliquez sur l'icône en forme de porte-documents pour vérifier l'état de la synchronisation.
  - Dans BlackBerry UEM Self-Service, vérifiez que votre terminal est répertorié en tant que terminal activé. Le statut peut mettre jusqu'à deux minutes pour se mettre à jour après que vous avez activé le terminal.
- Si votre administrateur vous y invite, ajoutez votre compte professionnel aux Comptes utilisés par d'autres applications afin d'avoir accès aux applications en ligne requises.
  - Pour Windows 10 1607 ou version ultérieure, cliquez sur Paramètres > Comptes > Accès professionnel ou scolaire > Se connecter. Saisissez votre adresse électronique professionnelle et votre mot de passe.
  - Pour les versions de Windows 10 antérieures à la version 1607, cliquez sur Paramètres > Comptes > Votre e-mail et vos comptes. Sous Comptes utilisés par d'autres applications, cliquez sur Ajouter un compte professionnel ou scolaire, puis saisissez votre adresse électronique professionnelle et votre mot de passe.

Activer un terminal macOS

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

Avant de commencer : Vous devez disposer des informations de connexion BlackBerry UEM Self-Service suivantes :

- Adresse Web de BlackBerry UEM Self-Service
- Nom d'utilisateur et mot de passe
- Nom de domaine

1. Sur le terminal à activer, connectez-vous à BlackBerry UEM Self-Service à l'aide des informations de connexion que vous avez reçues de votre administrateur.
2. Si des terminaux sont déjà indiqués, cliquez sur **Activer un terminal**.
3. Dans le menu déroulant Terminal, cliquez sur **macOS**.
4. Regardez le didacticiel d'activation.

5. Cliquez sur **Envoyer**.
6. Suivez les instructions pour installer les profils requis et terminer l'activation du terminal. Une fois l'activation terminée, votre terminal s'affiche dans BlackBerry UEM Self-Service.

Activer un terminal Apple TV

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

Avant de commencer :

- Vous avez besoin de l'adresse Web et de vos identifiants de connexion pour BlackBerry UEM Self-Service.
- Vous avez besoin d'un ordinateur macOS où Apple Configurator 2 est installé.
- Vous avez besoin d'un câble USB-C ou Micro-USB (selon la version de Apple TV).
- Vérifiez que le terminal Apple TV est en mode supervisé.
- Débrancher le câble HDMI et le cordon d'alimentation du terminal Apple TV.

1. Connectez le terminal Apple TV à votre ordinateur macOS à l'aide d'un câble USB-C ou Micro-USB.
2. Pour les versions Apple TV de troisième et quatrième générations, branchez le cordon d'alimentation.
3. Sur votre ordinateur macOS, connectez-vous à BlackBerry UEM Self-Service.
4. Selon que vous activez votre premier terminal ou que vous disposez déjà d'un terminal activé, cliquez sur ou sur > **Activer un terminal**.
5. Dans le menu déroulant Terminal, cliquez sur **Apple TV**.
6. Cliquez sur **Submit**.
7. Cliquez sur **Télécharger le profil**.
8. Cliquez sur **Fermer**.
9. Ouvrez Apple Configurator 2.
10. Sélectionnez Apple TV et cliquez sur **Ajouter > Profils**.
11. Sélectionnez le fichier de configuration que vous avez téléchargé à l'étape 7 et cliquez sur **Ajouter**.
12. Une fois l'activation terminée, votre terminal s'affiche dans BlackBerry UEM Self-Service.

Activer une tablette ou un ordinateur Windows 10

Notes du formateur: Ces étapes s'appliquent aux tablettes ou ordinateurs utilisant Windows 10. Si les participants utilisent des smartphones Windows 10 Mobile, utilisez les étapes permettant d'Activer un terminal Windows 10 Mobile.

Remarque : Si vous souhaitez gérer les terminaux Windows 10 à l'aide de MDM, ils ne pourront pas être gérés par Microsoft System Center Configuration Manager.

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

1. Dans le navigateur de votre terminal, saisissez ou collez l'adresse du serveur de certificats. Vous trouverez l'adresse du serveur de certificats dans l'e-mail d'activation que vous avez reçu. Si vous n'avez pas reçu de lien vers le certificat, contactez votre administrateur pour obtenir de l'aide.
2. Cliquez sur **Enregistrer**.
3. Dans la notification de téléchargement du certificat, sélectionnez **Ouvrir**.
4. Cliquez sur **Ouvrir**.
5. Cliquez sur **Installer le certificat**.
6. Sélectionnez l'option **Utilisateur actuel**. Cliquez sur **Suivant**.
7. Sélectionnez l'option **Placer tous les certificats dans le magasin suivant**. Cliquez sur **Parcourir**.
8. Sélectionnez **Autorités de certification racine approuvées**. Cliquez sur **OK**.

9. Cliquez sur **Suivant**.
10. Cliquez sur **Terminer**.
11. Cliquez sur **OK**.
12. Cliquez sur **OK**.
13. Cliquez sur le bouton **Démarrer**.
14. Effectuez l'une des tâches suivantes :

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

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

À la fin :

- Pour vérifier que le processus d'activation a abouti, effectuez l'une des opérations suivantes :
  - Sur le terminal, cliquez sur Paramètres > Comptes > Accès professionnel ou scolaire (ou Accès professionnel) pour vérifier que votre terminal est connecté à BlackBerry UEM. Cliquez sur l'icône en forme de porte-documents pour vérifier l'état de la synchronisation.
  - Dans BlackBerry UEM Self-Service, vérifiez que votre terminal est répertorié en tant que terminal activé. Le statut peut mettre jusqu'à deux minutes pour se mettre à jour après que vous avez activé le terminal.
- Si votre administrateur vous y invite, ajoutez votre compte professionnel aux Comptes utilisés par d'autres applications afin d'avoir accès aux applications en ligne requises.
  - Pour Windows 10 1607 ou version ultérieure, cliquez sur Paramètres > Comptes > Accès professionnel ou scolaire > Se connecter. Saisissez votre adresse électronique professionnelle et votre mot de passe.
  - Pour les versions de Windows 10 antérieures à la version 1607, cliquez sur Paramètres > Comptes > Votre e-mail et vos comptes. Sous Comptes utilisés par d'autres applications, cliquez sur Ajouter un compte professionnel ou scolaire, puis saisissez votre adresse électronique professionnelle et votre mot de passe.

Activer un terminal à l'aide de QR Code

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

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

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

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

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

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

Activer un terminal BlackBerry OS

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

1. Sur le terminal, accédez **Configuration**.
2. Cliquez sur **Comptes de messagerie.**
3. Cliquez sur **Compte d'entreprise**.
4. Dans le champ **E-mail**, saisissez votre adresse électronique professionnelle.
5. Dans le champ **Mot de passe**, saisissez le mot de passe d'activation que vous avez reçu.
6. Cliquez sur **Activer**.
7. Cliquez sur **OK**.

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

- Sur le terminal, accédez à l'application de configuration et cliquez sur **Comptes de messagerie.** Vérifiez que l'adresse électronique est présente.
- Dans BlackBerry Web Desktop Manager, vérifiez que votre terminal est répertorié en tant que terminal activé. Après l'activation du terminal, la mise à jour de l'état peut prendre jusqu'à deux minutes.

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

Samsung KNOX Mobile Enrollment permet d'activer un grand nombre de terminaux dans BlackBerry UEM en une seule fois. Pour plus d'informations, rendez-vous sur https://www.samsungknox.com/en/products/knox-mobile-enrollment.

Avant de commencer : Vous devez acheter des terminaux auprès de l'un des revendeurs suivants :

- Un revendeur agréé
- Un revendeur qui accepte de partager les IMEI des terminaux directement avec Samsung

1. Dans la barre de menus, cliquez sur **Paramètres > Intégration externe**.
2. Cliquez sur **KNOX Mobile Enrollment**.
3. Suivez les instructions qui s'affichent à l'écran.

À la fin : Une fois l'activation effectuée, cliquez sur **Télécharger** pour télécharger le fichier configuration.json. Dans le fichier, comparez l'entrée figurant dans la section CFPrint avec celle que vous avez ajoutée lorsque vous

avez configuré KNOX Mobile Enrollment. Si les entrées sont différentes, copiez tout le texte du fichier .json dans le champ Custom JSON Data sur la page KNOX Mobile Enrollment.

Activer plusieurs terminaux à l'aide de l'inscription Zero Touch pour les terminaux Android

L'inscription sans intervention vous permet de déployer simultanément un grand nombre de terminaux Android.

Votre entreprise achète ces terminaux auprès d'un revendeur d'entreprise agréé, qui configure un compte d'inscription sans intervention et ajoute les terminaux au compte pour les provisionner à des fins de gestion de terminaux. Lorsque des utilisateurs configurent ces terminaux pour la première fois, ces derniers téléchargent automatiquement le BlackBerry UEM Client et lancent le processus d'activation avec BlackBerry UEM. L'utilisateur doit terminer le processus d'activation pour utiliser le terminal.

Pour plus d'informations sur l'inscription sans intervention et la manière de la configurer, reportez-vous à https://www.android.com/intl/en_ca/enterprise/management/zero-touch/ et à https://support.google.com/work/android/answer/7514005.

Pour utiliser l'inscription sans intervention dans BlackBerry UEM, les terminaux doivent exécuter Android 8.0 ou version ultérieure et avoir été activés pour l'inscription sans intervention.

1. Achetez des terminaux pris en charge auprès d'un revendeur d'entreprise agréé. Le revendeur configure un compte d'inscription sans intervention pour votre entreprise.
2. Dans la plate-forme sans intervention, le revendeur ajoute les terminaux que vous avez achetés.
3. Dans la barre de menus de la console de gestion BlackBerry UEM, cliquez sur **Paramètres > Intégration externe**.
4. Cliquez sur **Android enterprise**.
5. Au bas de l'écran, cliquez sur **En savoir plus**.
6. Copiez la chaine générée par cette instance de BlackBerry UEM pour pouvoir l'utiliser lors de la configuration des terminaux dans le portail d'inscription Zero Touch.

   Vous pouvez laisser le champ Nom d'utilisateur vide ou y indiquer un nom d'utilisateur de sorte que seul ce nom d'utilisateur pourra être utilisé pour se connecter au terminal qui utilise la configuration.
7. Dans la plate-forme sans intervention, créez des configurations et attribuez-les aux terminaux que vous avez achetés.
8. Dans BlackBerry UEM, vérifiez que les profils et les stratégies informatiques appropriés sont attribués aux utilisateurs. Pour utiliser l'inscription sans intervention, vous devez attribuer un profil d'activation avec le type d'activation « Espace Travail uniquement » ou « Espace Travail uniquement (Premium) » activé.
9. Distribuez les terminaux aux utilisateurs.

Activation de terminaux iOS inscrits dans DEP

Vous pouvez vous inscrire des terminaux iOS dans le Programme d'inscription des appareils Apple et leur attribuer des configurations d'inscription dans la console de BlackBerry UEM. Les configurations d'inscription comprennent des règles supplémentaires, comme « Activer le mode supervisé », attribuées aux terminaux lors de l'inscription MDM.

Lorsque les terminaux sont activés, BlackBerry UEM envoie les stratégies informatiques et des profils que vous avez attribués aux utilisateurs.

Remarque : Pour que certaines caractéristiques fonctionnent, vous devez attribuer l'application BlackBerry UEM Client aux utilisateurs. Les utilisateurs doivent lancer l'application BlackBerry UEM Client après avoir activé le terminal. Pour plus d'informations concernant l'attribution de l'application BlackBerry UEM Client aux utilisateurs, rendez-vous sur support.blackberry.com/kb/ et consultez l'article KB 39313.

Étapes à suivre pour activer les terminaux inscrits dans DEP

Pour activer des terminaux iOS inscrits dans le Programme d'inscription des appareils Apple, procédez comme suit :

Étape	Action
1	Enregistrer les terminaux iOS dans DEP et les attribuer au serveur BlackBerry UEM.
2	Si vous n'avez pas sélectionné l'option Attribuer automatiquement tous les nouveaux terminaux à cette configuration lors de la création de la configuration d'inscription ou que vous souhaitez attribuer une autre configuration, attribuez une configuration d'inscription.
3	Vous pouvez également, de manière optionnelle, ajouter l'application BlackBerry UEM Client à la liste des applications et l'attribuer à des comptes ou groupes utilisateur. Consultez la section Ajouter une application iOS à la liste des applications.
4	Si vous ne souhaitez pas utiliser le profil d'activation par défaut, reportez-vous à la section Créer un profil d'activation et l'attribuer à un compte d'utilisateur ou à un groupe auquel l'utilisateur appartient.
5	Définissez un mot de passe d'activation pour l'utilisateur et envoyez-lui un e-mail d'activation à l'aide du modèle d'e-mail DEP Apple. Lorsque vous définissez le mot de passe d'activation, vous devez sélectionner Activation du terminal par défaut. Les utilisateurs du répertoire d'entreprise peuvent utiliser le nom d'utilisateur et le mot de passe du répertoire de leur entreprise ; il n'est donc pas nécessaire de créer un mot de passe d'activation. Les utilisateurs doivent saisir leur nom d'utilisateur au format domaine \nomd'utilisateur.
6	Distribuez les terminaux aux utilisateurs et demandez-leur de terminer la configuration. À l'issue de l'installation, les utilisateurs doivent installer et ouvrir l'application BlackBerry UEM Client.

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

Pour enregistrer les terminaux, vous devez saisir les numéros de série de ces terminaux dans le portail Apple DEP et attribuer les terminaux au serveur BlackBerry UEM. Vous pouvez saisir les numéros de série comme suit :

- Saisissez chaque numéro.
- Sélectionnez le numéro de commande attribué par Apple aux terminaux lors de leur achat.
- Téléchargez un fichier .csv contenant les numéros de série.

Avant de commencer : Configurez BlackBerry UEM pour utiliser DEP. Pour plus d'informations, reportez-vous au contenu relatif à la configuration.

1. Dans un navigateur, saisissez **deploy.apple.com**.

2. Connectez-vous à votre compte du programme d'inscription des appareils.
3. Dans la section **Programme d'inscription de terminaux**, cliquez sur **Gérer les terminaux**.
4. Suivez la procédure pour saisir les numéros de série des terminaux.
5. Attribuez les numéros de série au serveur BlackBerry UEM.

À la fin : Attribuez une configuration d'inscription aux terminaux iOS .

Attribuez une configuration d'inscription aux terminaux iOS

Si vous avez créé une configuration d'inscription et sélectionné Attribuer automatiquement tous les nouveaux terminaux à cette configuration, BlackBerry UEM attribue automatiquement la configuration lorsque les terminaux DEP sont synchronisés avec BlackBerry UEM. Sinon, vous devez attribuer une configuration d'inscription aux terminaux. BlackBerry UEM est synchronisé avec DEP sur une base quotidienne et à chaque fois que vous affichez la page de terminaux DEP Apple.

Si l'état d'activation d'un terminal est toujours en attente, vous pouvez supprimer une configuration d'inscription existante et en attribuer une autre.

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

1. Sur la barre de menus, cliquez sur **Utilisateurs > Terminaux DEP Apple**.
2. Cochez les cases en regard des terminaux auxquels vous souhaitez attribuer une configuration d'inscription. Vous devez sélectionner des terminaux qui sont enregistrés sous le même compte DEP.
3. Cliquez sur .
4. Dans la liste déroulante **Configuration d'inscription**, sélectionnez la configuration d'inscription que vous souhaitez attribuer.
5. Cliquez sur **Attribuer**.

À la fin : Distribuez les terminaux iOS aux utilisateurs. Lors de la configuration des terminaux, les terminaux sont activés avec BlackBerry UEM. Les utilisateurs sont invités à saisir un nom d'utilisateur et un mot de passe. Les utilisateurs du répertoire d'entreprise peuvent utiliser le nom d'utilisateur (au format domaine/nomd'utilisateur) et le mot de passe du répertoire de leur entreprise. Les utilisateurs locaux doivent utiliser un mot de passe d'activation. Reportez-vous à la section Définir un mot de passe d'activation pour l'utilisateur.

Ajouter une configuration d'inscription

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

1. Sur la barre de menus, cliquez sur **Paramètres**.
2. Dans le volet de gauche, cliquez sur **Intégration externe > Programme d'inscription des appareils Apple**.
3. Cliquez sur le nom d'un compte DEP.
4. Dans la section **Configurations d'inscription DEP**, cliquez sur +.
5. Saisissez un nom pour la configuration.
6. Effectuez l'une des tâches suivantes :

   - Si vous souhaitez que BlackBerry UEM attribue automatiquement la configuration d'inscription lorsque les terminaux sont synchronisés avec BlackBerry UEM, cochez la case Attribuer automatiquement tous les nouveaux terminaux à cette configuration. BlackBerry UEM est synchronisé avec Apple DEP sur une base quotidienne et à chaque fois que vous affichez la page de terminaux DEP Apple.

     Remarque : Si vous avez déjà créé une configuration d'inscription avec ce paramètre et que cette configuration a été appliquée aux terminaux, BlackBerry UEM n'attribue pas la nouvelle configuration d'inscription.

Remarque : Vous ne pouvez sélectionner qu'une seule configuration d'inscription à attribuer automatiquement aux nouveaux terminaux inscrits dans le DEP. Si vous avez déjà créé une configuration d'inscription avec ce paramètre, ce dernier est supprimé de la configuration précédente et ajouté à la nouvelle.

- Si vous souhaitez attribuer manuellement la configuration d'inscription à des terminaux spécifiques, ne cochez pas la case Attribuer automatiquement tous les nouveaux terminaux à cette configuration.

7. Vous avez la possibilité de saisir un nom de service et le numéro de téléphone de l'assistance qui s'afficheront sur les terminaux au cours de la configuration.
8. Dans la section **Configuration du terminal**, sélectionnez les options suivantes :
   - Autoriser le couplage : cette option permet aux utilisateur de coupler le terminal à un ordinateur.
   - Activer le mode supervisé : cette option permet d'activer le mode supervisé des terminaux. Vous devez sélectionner au moins l'une des deux options suivantes : Activer le mode supervisé ou Autoriser la suppression du profil MDM.
   - Obligatoire : avec cette option, les utilisateurs ne sont pas invités à accepter la configuration d'inscription.
   - Autoriser la suppression du profil MDM : cette option permet aux utilisateurs de désactiver les terminaux. Vous devez sélectionner au moins l'une des deux options suivantes : Activer le mode supervisé ou Autoriser la suppression du profil MDM.
   - Veuillez patienter pendant la configuration du terminal : cette option empêche les utilisateurs d'annuler la configuration des terminaux tant que l'activation avec BlackBerry UEM n'est pas terminée. Ce paramètre n'est disponible que si vous sélectionnez l'option Activer le mode supervisé.
9. Dans la section **Ignorer pendant la configuration**, sélectionnez les éléments que vous ne souhaitez pas inclure dans la configuration des terminaux :
   - Mot de passe : avec cette option, les utilisateurs ne sont pas invités à créer un mot de passe pour le terminal.
   - Services de localisation : cette option permet de désactiver les services de localisation sur le terminal.
   - Restaurer : cette option empêche les utilisateurs de restaurer les données à partir d'un fichier de sauvegarde.
   - Déplacer depuis Android : cette option empêche les utilisateurs de restaurer les données à partir d'un terminal Android.
   - ID Apple : cette option empêche les utilisateurs de se connecter avec leur identifiant Apple et iCloud.
   - Conditions générales : cette option permet de masquer les conditions générales de iOS.
   - Siri : cette option permet de désactiver Siri sur les terminaux.
   - Diagnostics : cette option bloque l'envoi automatique des informations de diagnostic au terminal pendant la configuration.
   - Biométrique : cette option empêche les utilisateurs de configurer Touch ID.
   - Paiement : cette option empêche les utilisateurs de configurer Apple Pay.
   - Zoom : cette option empêche les utilisateurs de configurer le zoom.
   - Configuration de l'icône de l'écran d'accueil : si cette option est sélectionnée, les utilisateurs ne peuvent pas régler le clic de l'icône de l'écran d'accueil
10. Cliquez sur **Enregistrer**.
11. Si vous avez sélectionné "Attribuer automatiquement de nouveaux terminaux à cette configuration", cliquez sur **Oui**.

À la fin : Si vous n'avez pas sélectionné l'option Attribuer automatiquement tous les nouveaux terminaux à cette configuration, reportez-vous à la section Attribuez une configuration d'inscription aux terminaux iOS .

Supprimer une configuration d'inscription attribuée aux terminaux iOS

Si vous avez attribué une configuration d'inscription aux terminaux et que celle-ci ne leur a pas encore été attribuée, vous pouvez supprimer la configuration d'inscription des terminaux.

1. Sur la barre de menus, cliquez sur **Utilisateurs > Terminaux DEP Apple**.
2. Cochez les cases en regard des terminaux dont vous souhaitez supprimer une configuration d'inscription. Vous devez sélectionner les périphériques qui sont enregistrés pour le même compte DEP.
3. Cliquez sur .
4. Cliquez sur **Supprimer**.

À la fin : Attribuez une configuration d'inscription aux terminaux iOS .

Supprimer une configuration d'inscription

Si vous supprimez une configuration d'inscription attribuée aux terminaux avant que celle-ci ne leur soit appliquée, BlackBerry UEM supprime la configuration d'inscription attribuée aux terminaux.

1. Sur la barre de menus, cliquez sur **Paramètres**.
2. Dans le volet de gauche, cliquez sur **Intégration externe > Programme d'inscription des appareils Apple**.
3. Cliquez sur le nom du compte d'utilisateur.
4. Dans la section **Configurations d'inscription DEP**, cliquez sur .
5. Cliquez sur **Supprimer**.

À la fin : si BlackBerry UEM supprime la configuration d'inscription des terminaux, attribuer une configuration d'inscription à ces terminaux.

Modifier les paramètres d'une configuration d'inscription

Si vous avez attribué une configuration d'inscription à des terminaux et que celle-ci ne leur est pas appliquée, BlackBerry UEM met à jour à la configuration d'inscription attribuée aux terminaux lorsque vous enregistrez les modifications apportées à la configuration.

1. Sur la barre de menus, cliquez sur **Paramètres**.
2. Dans le volet de gauche, cliquez sur **Intégration externe > Programme d'inscription des appareils Apple**.
3. Cliquez sur le nom du compte d'utilisateur.
4. Dans la section **Configurations d'inscription DEP**, cliquez sur le nom de la configuration que vous souhaitez modifier.
5. Modifiez les paramètres.
6. Cliquez sur **Enregistrer**.

Afficher les paramètres d'une configuration d'inscription attribuée à un terminal

Si une configuration d'inscription est attribuée à un terminal iOS et que la configuration est en attente, vous pouvez afficher les paramètres de cette configuration d'inscription.

1. Sur la barre de menus, cliquez sur **Utilisateurs > Terminaux DEP Apple**.
2. Dans la colonne **Configuration d'inscription**, cliquez sur le nom d'une configuration d'inscription.

Afficher les détails de l'utilisateur pour un terminal activé

Une fois le terminal correctement activé, vous pouvez afficher les détails associés à l'utilisateur, comme les groupes auxquels l'utilisateur est attribué.

1. Sur la barre de menus, cliquez sur **Utilisateurs > Terminaux DEP Apple**.
2. Dans la colonne **Nom d'affichage**, cliquez sur le nom d'un utilisateur.

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

Vous pouvez utiliser Apple Configurator 2 pour préparer les terminaux iOS à l'activation dans BlackBerry UEM. Les utilisateurs peuvent activer les terminaux préparés sans avoir recours à l'application BlackBerry UEM Client. Ils ont uniquement besoin de leur nom d'utilisateur et du mot de passe d'activation.

Une fois les terminaux activés, BlackBerry UEM leur transmet la stratégie informatique et les profils que vous avez attribués aux utilisateurs.

Remarque : Pour que certaines caractéristiques fonctionnent, vous devez attribuer l'application BlackBerry UEM Client aux utilisateurs. Les utilisateurs doivent lancer BlackBerry UEM Client après avoir activé le terminal. Pour plus d'informations concernant l'attribution de l'application BlackBerry UEM Client aux utilisateurs, rendez-vous sur support.blackberry.com/kb/ et consultez l'article KB 39313.

Étapes à suivre pour activer des terminaux utilisant Apple Configurator 2

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

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

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

1. Dans le menu de Apple Configurator 2, sélectionnez **Préférences > Serveurs**.
2. Cliquez sur + > **Suivant**.
3. Dans le champ **Nom**, saisissez un nom pour le serveur.
4. Dans le champ**Nom d'hôte ou URL**, saisissez l'URL du serveur BlackBerry UEM au format suivant :*<http ou https> ://< nom_serveur>:<port>*, sachant que le numéro de port par défaut est 8885. Pour plus d'informations sur les ports obligatoires, reportez-vous à la section Ports d'écoute BlackBerry UEM du contenu relatif à l'installation et à la mise à niveau.
5. Cliquez sur **Suivant**.
6. Fermez la fenêtre **Serveur**.

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

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

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

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

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

Utilisation du verrouillage d'activation sur les terminaux iOS

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

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

- Le terminal doit être un terminal supervisé exécutant iOS version 7.1 ou ultérieure.
- Le terminal doit disposer d'un compte iCloud configuré.
- La fonction Localiser mon iPhone ou Trouver mon iPad doit être activée sur le terminal.

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

Concepts connexes

Activation de terminaux iOS inscrits dans DEP

Activation du verrouillage d'activation

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

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

Avant de commencer :

- Le terminal doit être un terminal supervisé exécutant iOS version 7.1 ou ultérieure.
- Le terminal doit disposer d'un compte iCloud configuré.

- La fonction Localiser mon iPhone ou Trouver mon iPad doit être activée sur le terminal.

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

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

Désactivation du verrouillage d'activation

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

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

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

Affichage du code de contournement du verrouillage d'activation

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

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

Activation de terminaux BlackBerry 10 à l'aide de BlackBerry Wired Activation Tool

BlackBerry Wired Activation Tool vous permet d'activer simultanément plusieurs terminaux BlackBerry 10 via des connexions USB au lieu de connexions sans fil. Votre entreprise peut être amenée à utiliser cette méthode pour différentes raisons :

- Pour accélérer et faciliter l'activation simultanée de plusieurs terminaux
- Pour continuer de confier le processus d'activation aux administrateurs
- Pour activer les terminaux et configurer leurs fonctions de sécurité, comme les exigences de cryptage de contenu et les profils VPN, avant de les confier aux utilisateurs ou de les connecter au réseau de votre organisation

Vous ne pouvez pas attribuer de profils ou de stratégies à l'aide de BlackBerry Wired Activation Tool. Vous devez attribuer les profils et les stratégies à vos utilisateurs dans la console de gestion BlackBerry UEM avant d'attribuer et d'activer les terminaux à l'aide de BlackBerry Wired Activation Tool. Il n'est cependant pas nécessaire de définir de mots de passe d'activation pour attribuer et activer des terminaux à l'aide de BlackBerry Wired Activation Tool.

Pour activer les terminaux à l'aide de BlackBerry Wired Activation Tool, les terminaux doivent exécuter BlackBerry 10 OS version 10.3 ou ultérieure.

Vous pouvez télécharger BlackBerry Wired Activation Tool ici : Docs.blackberry.com/BES12tools

Installer BlackBerry Wired Activation Tool

Procédez comme suit pour télécharger et installer le BlackBerry Wired Activation Tool

1. Accédez à docs.blackberry.com/bes12tools.
2. Dans la liste déroulante, cliquez sur BlackBerry Wired Activation Tool.
3. Cliquez sur **Suivant**.
4. Cliquez sur **Télécharger**.
5. Sélectionnez l'option Oui ou Non et cliquez sur **Télécharger**.
6. Enregistrez le fichier d'installation sur votre ordinateur.
7. Sur votre ordinateur, accédez à l'emplacement où vous avez enregistré le fichier d'installation.
8. Suivez les instructions qui s'affichent l'écran pour procéder à l'installation.

Configurer BlackBerry Wired Activation Tool et se connecter à une instance de BlackBerry UEM

Avant de pouvoir activer des terminaux avec BlackBerry Wired Activation Tool, vous devez créer une configuration pour chaque instance de BlackBerry UEM à laquelle vous devez accéder. Lorsque c'est chose faite, vous devez également utiliser un compte d'administrateur pour autoriser BlackBerry Wired Activation Tool à accéder à BlackBerry Web Services.

1. Dans le dossier d'installation de BlackBerry Wired Activation Tool, double-cliquez sur le fichier **BWAT.exe**.
2. Dans l'**écran Ajouter un serveur BES12**, dans le champ **Nom**, saisissez un nom pour identifier la configuration que vous créez. Par exemple, si vous disposez de deux instances BlackBerry UEM, vous pouvez créer une configuration pour chacune et les nommer Serveur 1 et Serveur 2.
3. Dans le champ **URL de BlackBerry Web Services**, saisissez l'adresse du composant BlackBerry Web Services. Par défaut, l'adresse est https://<*BlackBerry UEM web address*>:18084.

   Pour changer de port, modifiez le paramètre `tomcat.bws.port` de la base de données BlackBerry UEM.
4. Dans le champ **URL du point de terminaison BCP**, saisissez l'adresse à utiliser pour les activations de terminaux. Ceci est également connu sous le terme d'URL d'activation ou de nom du serveur. Par défaut, l'adresse est : http://*server.name*:8882/*SRP_ID*/mdm.

   Pour rechercher l'adresse, vérifiez que la variable %ActivationURL% se trouve dans le modèle d'e-mail d'activation et cliquez sur **Afficher l'e-mail d'activation** depuis un écran Synthèse des données utilisateur.

   Si nécessaire, vous pouvez également rechercher le port et l'adresse de l'hôte dans la base de données BlackBerry UEM. Dans le tableau `def_cfg_setting_dfn`, recherchez les valeurs `id_setting_definition` pour `bdmi.enroll.bcp.host` et `bdmi.enroll.bcp.port`. Utilisez ensuite les valeurs `id_setting_definition` pour rechercher les valeurs de ces paramètres dans `obj_global_cfg_setting`.
5. Cliquez sur **Envoyer**.
6. Dans l'écran **Connexion**, sélectionnez une configuration BlackBerry UEM dans la liste déroulante.
7. Dans le champ **Nom d'utilisateur**, saisissez le nom d'utilisateur d'un compte d'utilisateur BlackBerry UEM doté d'autorisations d'administrateur.
8. Dans le champ **Mot de passe**, saisissez le mot de passe du compte.
9. Dans la liste déroulante **Répertoire**, sélectionnez une méthode d'authentification.
10. Si nécessaire, dans le champ **Domaine**, saisissez le domaine Microsoft Active Directory.
11. Cliquez sur **Se connecter**.

Activer des terminaux BlackBerry 10 à l'aide de BlackBerry Wired Activation Tool

Avant de commencer :

- Configurez BlackBerry Wired Activation Tool et connectez-vous à une instance de BlackBerry UEM.
- Activez tous les terminaux connectés et vérifiez qu'ils ont terminé le processus de configuration initiale ou qu'ils ne l'ont pas démarré. Vous ne pouvez pas activer les terminaux si le processus de configuration initiale est en cours.

1. Connectez un ou plusieurs terminaux BlackBerry 10 à votre ordinateur à l'aide de câbles USB.
2. Vérifier la colonne **État** pour chaque terminal. Effectuez l'une des opérations suivantes :
   - Si la colonne État indique **Mot de passe requis,** cliquez sur **Mot de passe requis** pour saisir le mot de passe du terminal.
   - Si la colonne État indique **Terminal non pris en charge**, procédez à la mise à niveau de BlackBerry 10 OS vers la version 10.3 ou ultérieure.
   - Si la colonne État indique **Prêt**, attribuez le terminal à un utilisateur.
3. Dans le champ **Rechercher**, recherchez un compte d'utilisateur auquel vous souhaitez attribuer un terminal.
4. Dans la liste des résultats de la recherche, cliquez sur le compte d'utilisateur.
5. Dans la section principale de l'écran, cliquez sur le nom d'un compte d'utilisateur et faites-le glisser vers un terminal pour attribuer le terminal à cet utilisateur. Répétez cette étape pour attribuer des terminaux à plusieurs utilisateurs.
6. Cochez la case en regard des paires d'utilisateurs et de terminaux que vous souhaitez activer.
7. Cliquez sur **Activer les terminaux**.

BlackBerry Wired Activation Tool active tous les terminaux que vous avez sélectionnés. Vérifiez la colonne État pour connaitre la progression et les résultats de chaque terminal. Si l'activation échoue, cliquez sur le message de la colonne État pour plus d'informations sur les erreurs.

Conseils pour résoudre les problèmes relatifs à l'activation des terminaux

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

- Vérifiez que BlackBerry UEM prend en charge ce type de terminal. Pour plus d'informations sur les types de terminaux pris en charge, reportez-vous à la matrice de compatibilité.
- Assurez-vous de la disponibilité de licences pour le type de terminal que l'utilisateur active et vérifiez le type d'activation attribué à l'utilisateur. Pour plus d'informations, reportez-vous au contenu relatif aux licences.
- Vérifiez la connectivité réseau sur le terminal.
  - Vérifiez que le réseau mobile ou Wi-Fi est actif et dispose d'une couverture suffisante.
  - Si l'utilisateur doit configurer manuellement un profil VPN ou Wi-Fi professionnel pour accéder au contenu situé derrière le pare-feu de votre entreprise, assurez-vous que les profils de l'utilisateur sont correctement configurés sur le terminal.
  - Si vous utilisez un Wi-Fi professionnel, assurez-vous que chemin réseau du terminal est disponible. Pour plus d'informations sur la configuration des pare-feu réseau avec BlackBerry UEM, rendez-vous sur http://support.blackberry.com/kb pour consulter l'article 36470.
- Assurez-vous que le profil d'activation attribué à l'utilisateur prend en charge le type de terminal en cours d'activation.

- Si le terminant tente de se connecter à BlackBerry UEM ou BlackBerry Infrastructure via le pare-feu de votre entreprise, vérifiez que les ports du pare-feu qui conviennent sont ouverts. Pour en savoir plus sur les ports obligatoires, reportez-vous au contenu relatif à l'installation et à la mise à niveau.
- Collectez les journaux du terminal :
  - Pour plus d'informations sur la récupération des fichiers journaux des terminaux BlackBerry 10, rendez-vous sur http://support.blackberry.com/kb pour lire l'article 26038.

    Remarque : les fichiers journaux BlackBerry 10 sont cryptés. Pour utiliser les fichiers journaux BlackBerry 10 à des fins de résolution des problèmes, vous devez disposer d'un ticket ouvert avec BlackBerry Technical Support Services. Seuls les agents de l'assistance peuvent décrypter les fichiers journaux.
  - Pour plus d'informations sur la récupération des fichiers journaux des terminaux iOS, rendez-vous sur http://support.blackberry.com/kb pour lire l'article 36986.
  - Pour plus d'informations sur la récupération des fichiers journaux des terminaux Android, rendez-vous sur http://support.blackberry.com/kb pour lire l'article 32516.
  - Pour plus d'informations sur la récupération des journaux des terminaux Windows Phone, rendez-vous sur http://support.blackberry.com/kb pour lire l'article 36984.

Terminaux KNOX Workspace et Android dotés d'un profil professionnel

Lorsque vous résolvez des problèmes liés à l'activation des terminaux Samsung utilisant Samsung KNOX Workspace, vérifiez ce qui suit :

- Vérifiez que le terminal prend en charge KNOX Workspace. Reportez-vous aux informations de Samsung.
- Assurez-vous que le bit de garantie n'a pas été déclenché. Reportez-vous aux informations de Samsung.
- Assurez-vous que la version du conteneur KNOX est prise en charge. KNOX Workspace requiert KNOX Container 2.0 ou version ultérieure. Pour plus d'informations sur les versions Samsung KNOX prises en charge, reportez-vous à la liste de Samsung.

Lorsque vous résolvez des problèmes liés à l'activation de terminaux Android dotés d'un profil professionnel, vérifiez ce qui suit :

- Assurez-vous que le terminal prend en charge les profils professionnels Android. Pour plus d'informations, rendez-vous sur https://support.google.com/work/android/answer/6174145 pour lire l'article 6174145.
- Assurez-vous de la disponibilité d'une licence et vérifiez que le type d'activation est défini sur Travail et Personnel - Confidentialité de l'utilisateur.
- Pour utiliser le type d'activation Travail et Personnel - Confidentialité de l'utilisateur, les terminaux doivent exécuter Android OS version 5.1 ou version ultérieure.
- Assurez-vous que le compte d'utilisateur de BlackBerry UEM dispose de la même adresse électronique que celle du domaine Google. Si ces adresses électroniques ne correspondent pas, le terminal affichera l'erreur suivante : Impossible d'activer le terminal - Type d'activation non pris en charge. Dans le fichier journal Core, recherchez ce qui suit :
  - ```
    ERREUR AfW : impossible de trouver l’utilisateur dans le domaine Google.
     Abandon de la création et de l’activation de l’utilisateur.
    ```
  - ```
    Raison de la mise en quarantaine de la tâche en ERREUR : impossible d'activer
     le terminal - Type d'activation non pris en charge
    ```

Impossible de terminer l'activation du terminal en l'absence de licences suffisantes sur le serveur. Pour obtenir de l'aide, contactez votre administrateur.

Description

Cette erreur s'affiche lors de l'activation du terminal si les licences ne sont pas disponibles ou si elles ont expiré.

Solution possible

Dans BlackBerry UEM, procédez comme suit :

- Vérifier que des licences sont disponibles à des fins d'activation.
- Si nécessaire, activez les licences ou achetez des licences supplémentaires.

Pour plus d'informations, reportez-vous au contenu relatif à la gestion des licences.

Vérifiez votre nom d'utilisateur et votre mot de passe, puis réessayez

Description

Cette erreur s'affiche lors de l'activation d'un terminal si l'utilisateur a saisi un nom d'utilisateur ou un mot de passe erroné, voire les deux.

Solution possible

Saisissez le nom d'utilisateur et le mot de passe qui conviennent.

Impossible d'installer le profil. Le certificat AutoMDMCert.pfx n'a pas pu être importé.

Description

Cette erreur s'affiche lors de l'activation d'un terminal iOS s'il existe déjà un profil sur le terminal.

Solution possible

Accédez à **Paramètres > Général > Profils** sur le terminal et vérifiez qu'un profil existe déjà. Supprimez le profil et procédez à une nouvelle activation. Si le problème persiste, vous devrez peut-être réinitialiser le terminal car il est possible que des données aient été mises en cache.

Erreur 3007 : le serveur n'est pas disponible

Description

Cette erreur peut s'afficher lors de l'activation du terminal pour les raisons suivantes :

- Le certificat utilisé par BlackBerry UEM pour signer le profil MDM envoyé aux terminaux iOS n'est pas approuvé par le terminal. L'utilisateur est invité à approuver ce certificat lorsqu'il active le terminal.
- Si vous configurez un proxy transparent tel que Blue Coat et qu'il surveille le port 443 afin de détecter tout trafic non standard, le BlackBerry UEM Client ne peut pas passer les appels HTTP CONNECT et HTTP OPTIONS requis auprès de BlackBerry UEM.

Solutions possibles

Les solutions possibles sont les suivantes :

- Installez le certificat racine pour l'autorité de certification ayant émis le certificat qui utilise BlackBerry UEM pour signer le profil MDM envoyé au terminal iOS. Pour plus d'informations sur ce certificat, reportez-vous au contenu relatif à la configuration.
- Vérifiez que la configuration de votre proxy n'empêche pas le BlackBerry UEM Client de passer les appels HTTP CONNECT et HTTP OPTIONS auprès de BlackBerry UEM. Pour plus d'informations, rendez-vous sur http://support.blackberry.com/kb et lisez l'article 38644.

Impossible de contacter le serveur. Vérifiez la connectivité ou l'adresse du serveur

Description

Cette erreur peut s'afficher lors de l'activation du terminal pour les raisons suivantes :

- Le nom d'utilisateur n'a pas été correctement saisi sur le terminal.
- L'adresse du client pour l'activation du terminal n'a pas été correctement saisie sur le terminal.

  Remarque : uniquement nécessaire en cas de désactivation de l'inscription auprès de BlackBerry Infrastructure.
- Aucun mot de passe d'activation n'a été défini ou le mot de passe a expiré.

Solutions possibles

Les solutions possibles sont les suivantes :

- Vérifiez le nom d'utilisateur et le mot de passe.
- Vérifiez l'adresse du client pour l'activation du terminal.
- Définissez un nouveau mot de passe d'activation à l'aide de BlackBerry UEM Self-Service.

iOS or macOS device activations fail with an invalid APNs certificate

Cause possible

Si vous n'êtes pas en mesure d'activer les terminauxiOSoumacOS, cela signifie peut-être que le certificat APNs n'est pas correctement installé.

Solution possible

Effectuez une ou plusieurs des opérations suivantes :

- Dans la console de gestion, cliquez sur **Paramètres > Intégration externe > Apple Push Notification** sur la barre de menus. Vérifiez que le certificat APNs affiche l'état « Installé ». Si l'état est incorrect, tentez de réenregistrer le certificat APNs.
- Pour tester la connexion entre BlackBerry UEM et le serveur APNs, cliquez sur **Certificat APNs test**.
- Si nécessaire, procurez-vous un nouveau fichier CSR signé auprès de BlackBerry, et demandez et enregistrez un nouveau certificat APNs.

Les utilisateurs ne reçoivent pas d'e-mail d'activation

Description

Les utilisateurs ne reçoivent pas d'e-mail d'activation, même si tous les paramètres de BlackBerry UEM sont corrects.

Solution possible

Si les utilisateurs ont recours à un serveur de messagerie tiers, les e-mails provenant de BlackBerry UEM peuvent être marqués comme spams et finir dans le dossier des spams ou le dossier du courrier indésirable.

Assurez-vous que les utilisateurs ont vérifié si l'e-mail d'activation se trouve dans leur dossier de spams ou leur dossier de courrier indésirable.

Commandes et contrôles de terminal

BlackBerry UEM permet d'envoyer des commandes aux terminaux via le réseau sans fil pour protéger les données de terminal. Vous pouvez également localiser des terminaux sur une carte et contrôler quels sont les terminaux qui peuvent accéder à Exchange ActiveSync.

Envoi de commandes aux utilisateurs et aux terminaux

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

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

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

Envoyer une commande à un terminal

Avant de commencer :

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

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

Envoyer une commande groupée

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

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

1. Sur la barre de menus, cliquez sur **Utilisateurs > Terminaux gérés**.
2. Si nécessaire, filtrez la liste des utilisateurs.
3. Effectuez l'une des opérations suivantes :
   - Cochez la case en haut de la liste d'utilisateurs pour sélectionner tous les utilisateurs et les terminaux de la liste.

- Cochez la case pour chaque utilisateur et terminal que vous souhaitez inclure. Vous pouvez appuyer sur Maj+Clic pour sélectionner plusieurs utilisateurs.

4. Dans le menu, cliquez sur l'une des icônes suivantes :

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

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

Définir une heure d'expiration pour les commandes

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

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

Référence des commandes

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

Commandes communes à tous les types de terminaux

Commande	Description
Mettre à jour les informations du terminal	Cette commande envoie et reçoit des informations mises à jour sur le terminal. Par exemple, vous pouvez envoyer des règles de stratégie informatique ou des profils mis à jour à un terminal et recevoir des informations mises à jour sur un terminal comme la version du système d'exploitation ou le niveau de la batterie. Pour les terminaux macOS, il s'agit de la commande Mettre à jour les données du bureau. Pour les terminaux Windows 10, 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. Pour envoyer cette commande à plusieurs terminaux, reportez-vous à la sectionEnvoyer une commande groupée.
Afficher les actions du terminal	Cette commande affiche les actions en cours sur un terminal. Pour plus d'informations, reportez-vous à Affichage des actions du terminal.
Afficher le rapport de terminal	Cette commande affiche des informations détaillées sur un terminal. Vous pouvez exporter et enregistrer le rapport de terminal sur votre ordinateur. Pour plus d'informations, reportez-vous à Afficher et enregistrer un rapport de terminal.
Supprimer le terminal	Cette commande supprime le terminal de BlackBerry UEM. Le terminal peut continuer à recevoir des e-mails et d'autres données professionnelles. Pour envoyer cette commande à plusieurs terminaux, reportez-vous à la sectionEnvoyer une commande groupée.

Commandes pour terminaux Android

Commande	Description	Types d'activation
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 BlackBerry UEM lorsque vous envoyez cette commande, vous pouvez annuler la commande ou supprimer le terminal de la console. Si le terminal se connecte à BlackBerry UEM après que vous l'avez supprimé, seules les données professionnelles sont supprimées du terminal, y compris de l'espace Travail, le cas échéant. Pour envoyer cette commande à plusieurs terminaux, reportez-vous à la sectionEnvoyer une commande groupée.	• Contrôles MDM • Travail et Personnel - Contrôle total (Samsung KNOX) • Espace Travail uniquement - (Samsung KNOX)
Supprimer uniquement les données professionnelles	Cette commande supprime les données professionnelles, y compris la stratégie informatique, les profils, les applications et les certificats qui sont sur le terminal, et désactive le terminal. Si le terminal dispose d'un espace Travail, les informations de cet espace Travail et l'espace Travail sont supprimés du terminal. Pour plus d'informations, reportez-vous à Désactivation des terminaux. Si le terminal ne parvient pas à se connecter à BlackBerry UEM lorsque vous envoyez cette commande, vous pouvez annuler la commande ou supprimer le terminal de la console. Si le terminal se connecte à BlackBerry UEM après que vous l'avez supprimé, les données professionnelles sont supprimées du terminal, y compris de l'espace Travail, le cas échéant. Pour envoyer cette commande à plusieurs terminaux, reportez-vous à la sectionEnvoyer une commande groupée.	• Tout (sauf BlackBerry 2FA)

Commande	Description	Types d'activation
Verrouiller le terminal	Cette commande verrouille le terminal. L'utilisateur doit saisir le mot de passe du terminal existant pour déverrouiller le terminal. Si un terminal est temporairement perdu, vous pouvez utiliser cette commande. Lorsque vous envoyez cette commande, le terminal se verrouille uniquement s'il existe un mot de passe de terminal. Sinon, aucune action n'est prise sur le terminal.	• Contrôles MDM • Travail et Personnel - Contrôle total (Samsung KNOX) • Travail et Personnel - Confidentialité de l'utilisateur • Travail et Personnel - Confidentialité de l'utilisateur (Premium) • Espace Travail uniquement • Espace Travail uniquement (Premium)
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. **Remarque :** Cette commande n'est pas prise en charge sur les terminaux non Samsung sous Android version 7.0 et versions ultérieures qui sont activés avec Contrôles MDM.	• Contrôles MDM • Travail et Personnel - Contrôle total (Samsung KNOX) • Travail et Personnel - Confidentialité de l'utilisateur (Samsung KNOX)
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. **Remarque :** Cette commande n'est pas prise en charge sur les terminaux non Samsung exécutant Android 7.0 et versions ultérieures qui sont activés avec Contrôles MDM. **Remarque :** Pour les types d'activation Travail et Personnel - Confidentialité de l'utilisateur, seuls les terminaux BlackBerry optimisés par Android version 8.x et ultérieure prennent en charge cette commande.	• Contrôles MDM • Travail et Personnel - Contrôle total (Samsung KNOX) • Espace Travail uniquement • Espace Travail uniquement (Premium) • Travail et Personnel - Confidentialité de l'utilisateur • Travail et Personnel - Confidentialité de l'utilisateur (Premium)
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 de l'utilisateur - (Samsung KNOX) • Espace Travail uniquement - (Samsung KNOX)

Commande	Description	Types d'activation
Spécifier le mot de passe de l'espace Travail et verrouiller	Pour les terminaux exécutant Android 7.0 ou version ultérieure, vous pouvez spécifier un mot de passe de l'espace Travail et verrouiller le terminal. Lorsque l'utilisateur ouvre une application de profil professionnel Android, il doit saisir le mot de passe que vous avez défini.	• Travail et Personnel - Confidentialité de l'utilisateur • Travail et Personnel - Confidentialité de l'utilisateur (Premium)
Désactiver/Activer l'espace Travail	Cette commande désactive ou active l'accès aux applications de l'espace Travail sur le terminal.	• Travail et Personnel - Contrôle total (Samsung KNOX) • Travail et Personnel - Confidentialité de l'utilisateur - (Samsung KNOX) • Espace Travail uniquement - (Samsung KNOX)
Deactivate BlackBerry 2FA	Cette commande désactive les terminaux qui sont activés avec le type d'activation BlackBerry 2FA. Le terminal est supprimé de BlackBerry UEM et l'utilisateur ne peut pas utiliser la fonction BlackBerry 2FA.	• BlackBerry 2FA
Nettoyage des applications	Cette commande nettoie les données de toutes les applications gérées par Microsoft Intune sur le terminal. Les applications ne sont pas supprimées du terminal. Pour plus d'informations, reportez-vous à : Nettoyage des applications gérées par Microsoft Intune	• Tout (sauf BlackBerry 2FA)

Commandes pour terminaux iOS

Commande	Description	Types d'activation
Supprimer toutes les données du terminal	Cette commande supprime toutes les informations utilisateur et données d'application stockées sur le terminal et rétablit les paramètres d'usine par défaut. Si le terminal ne parvient pas à se connecter à BlackBerry UEM lorsque vous envoyez cette commande, vous pouvez annuler la commande ou supprimer le terminal de la console. Si le terminal se connecte à BlackBerry UEM à l'issue de sa suppression, seules les données professionnelles sont supprimées du terminal. Pour envoyer cette commande à plusieurs terminaux, reportez-vous à la sectionEnvoyer une commande groupée.	• Contrôles MDM

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

Commande	Description	Types d'activation
Activer le mode Perdu	Cette commande verrouille le terminal et vous permet de définir le numéro de téléphone et le message à afficher sur l'écran. Par exemple, vous pouvez afficher le numéro à appeler par la personne qui trouvera le terminal. Après avoir envoyé cette commande, vous verrez l'emplacement du terminal sur BlackBerry UEM. Cette commande est prise en charge sur les terminaux iOS supervisés exécutant iOS 9.3 ou version ultérieure. Cette commande n'est pas prise en charge par les terminaux Apple TV.	• Contrôles MDM
Désactiver BlackBerry 2FA	Cette commande désactive les terminaux qui sont activés avec le type d'activation « BlackBerry 2FA ». Le terminal est supprimé de BlackBerry UEM et l'utilisateur ne peut pas utiliser la fonction BlackBerry 2FA. Cette commande n'est pas prise en charge par les terminaux Apple TV.	• BlackBerry 2FA
Mettre à jour le système d'exploitation	Cette commande force les terminaux à installer une mise à jour de système d'exploitation disponible. Prise en charge sur les terminaux suivants : • terminaux supervisés exécutant iOS 10.3 et version ultérieure • terminaux DEP supervisés exécutant iOS 9.0 et version ultérieure Pour plus d'informations, reportez-vous à Mettre à jour le système d'exploitation sur les terminaux iOS supervisés. Pour envoyer cette commande a plusieurs appareils, voir Envoyer une commande groupée. Cette commande n'est pas prise en charge par les terminaux Apple TV.	• Contrôles MDM
Redémarrer le terminal	Cette commande force les terminaux à redémarrer. Prise en charge sur les terminaux iOS supervisés exécutant les versions 10.3 et ultérieures. Cette commande n'est pas prise en charge par les terminaux Apple TV.	• Contrôles MDM

Commande	Description	Types d'activation
Désactiver le terminal	Cette commande force les terminaux à se désactiver. Prise en charge sur les terminaux iOS supervisés exécutant les versions 10.3 et ultérieures. Cette commande n'est pas prise en charge par les terminaux Apple TV.	• Contrôles MDM
Nettoyage des applications	Cette commande nettoie les données de toutes les applications gérées par Microsoft Intune sur le terminal. Les applications ne sont pas supprimées du terminal. Pour plus d'informations, reportez-vous à : Nettoyage des applications gérées par Microsoft Intune	• Contrôles MDM

Commandes pour terminaux macOS

Commande	Description	Types d'activation
Verrouiller le bureau	Cette commande permet de définir un code PIN et de verrouiller le terminal.	• Contrôles MDM
Supprimer uniquement les données professionnelles	Cette commande supprime les données professionnelles, y compris les stratégies informatiques, profils, applications et certificats présents sur le terminal et supprime éventuellement le terminal de BlackBerry UEM. Pour envoyer cette commande à plusieurs terminaux, reportez-vous à la sectionEnvoyer une commande groupée.	• Contrôles MDM
Supprimer toutes les données du terminal	Cette commande permet de supprimer les informations utilisateur et les données des applications stockées du terminal. Il rétablit les réglages d'usine par défaut du terminal, verrouille le terminal avec un code PIN que vous définissez et supprime éventuellement le terminal du BlackBerry UEM. Cette commande n'est pas prise en charge comme commande groupée.	• Contrôles MDM

Commandes pour terminaux BlackBerry 10

Commande	Description	Types d'activation
Spécifier le mot de passe du terminal, verrouiller le terminal et définir un message	Cette commande vous permet de créer un mot de passe de terminal et de définir un message sur l'écran d'accueil, puis de verrouiller le terminal. Vous devez créer un mot de passe conforme aux règles de mots de passe existantes. Lorsque l'utilisateur déverrouille le terminal, celui-ci l'invite à accepter ou rejeter le nouveau mot de passe. Si une stratégie informatique requiert le même mot de passe pour le terminal et l'espace Travail, cette commande modifie également le mot de passe de l'espace Travail.	• Travail et Personnel - Entreprise • Espace Travail uniquement • Travail et Personnel - Régulé
Supprimer toutes les données du terminal	Cette commande supprime toutes les informations utilisateur et données des applications stockées sur le terminal, y compris les informations de l'espace Travail. Elle rétablit les paramètres d'usine par défaut sur le terminal et supprime éventuellement le terminal de BlackBerry UEM. Si le terminal ne parvient pas à se connecter à BlackBerry UEM lorsque vous envoyez cette commande, vous pouvez annuler la commande ou supprimer le terminal de la console. Si le terminal se connecte à BlackBerry UEM à l'issue de sa suppression, seules les données professionnelles sont supprimées du terminal. Pour envoyer cette commande à plusieurs terminaux, reportez-vous à la sectionEnvoyer une commande groupée.	• Travail et Personnel - Entreprise • Espace Travail uniquement • Travail et Personnel - Régulé
Spécifier le mot de passe de l'espace Travail et verrouiller	Cette commande vous permet de créer un mot de passe pour l'espace Travail sur le terminal et de verrouiller l'espace Travail. Vous devez créer un mot de passe conforme aux règles de mots de passe existantes. Pour déverrouiller l'espace Travail, l'utilisateur doit saisir le nouveau mot de passe que vous créez. Si une stratégie informatique requiert le même mot de passe pour le terminal et l'espace Travail, cette commande modifie également le mot de passe du terminal.	• Travail et Personnel - Entreprise • Travail et Personnel - Régulé

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 et supprime éventuellement le terminal de BlackBerry UEM. Si le terminal dispose d'un espace Travail, les informations de cet espace Travail sont supprimées et l'espace Travail est supprimé du terminal. Si le terminal ne parvient pas à se connecter à BlackBerry UEM lorsque vous envoyez cette commande, vous pouvez annuler la commande ou supprimer le terminal de la console. Si le terminal se connecte à BlackBerry UEM à l'issue de sa suppression, les données professionnelles sont supprimées du terminal. Pour envoyer cette commande à plusieurs terminaux, reportez-vous à la sectionEnvoyer une commande groupée.	• Travail et Personnel - Entreprise • Travail et Personnel - Régulé

Commandes pour terminaux Windows

Commande	Description	Types d'activation
Verrouiller le terminal	Cette commande verrouille un terminal. L'utilisateur doit saisir le mot de passe du terminal existant pour déverrouiller le terminal. Si un terminal est temporairement perdu, vous pouvez utiliser cette commande. Lorsque vous envoyez cette commande, le terminal se verrouille uniquement s'il existe un mot de passe de terminal. Sinon, aucune action n'est prise sur le terminal. Cette commande est uniquement prise en charge sur les terminaux exécutantWindows 10 Mobile etWindows Phone 8.1 ou versions ultérieures.	Contrôles MDM
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 exécutantWindows 10 Mobile etWindows Phone OS version 8.10.14176 ou ultérieure.	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 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 BlackBerry UEM. Si le terminal ne parvient pas à se connecter à BlackBerry UEM, vous pouvez supprimer le supprimer de BlackBerry UEM. Si le terminal se connecte à BlackBerry UEM après que vous l'ayez supprimé, seules les données professionnelles sont supprimées du terminal, y compris de l'espace Travail, le cas échéant. Pour envoyer cette commande à plusieurs terminaux, reportez-vous à la sectionEnvoyer une commande groupée.	Contrôles MDM
Supprimer toutes les données du terminal	Cette commande permet de supprimer les informations utilisateur et les données des applications stockées sur le terminal. Elle rétablit les paramètres d'usine par défaut sur le terminal et supprime éventuellement le terminal de BlackBerry UEM. Après avoir envoyé cette commande, vous avez la possibilité de supprimer le terminal de BlackBerry UEM. Si le terminal ne parvient pas à se connecter à BlackBerry UEM, vous pouvez supprimer le supprimer de BlackBerry UEM. Si le terminal se connecte à BlackBerry UEM après que vous l'avez supprimé, seules les données professionnelles sont supprimées du terminal, y compris de l'espace Travail, le cas échéant. Pour envoyer cette commande a plusieurs appareils, voirEnvoyer une commande groupée.	Contrôles MDM
Redémarrer le bureau/terminal	Cette commande force les terminaux à redémarrer. Cette commande est uniquement prise en charge sur les terminaux Windows 10.	Contrôles MDM

Commandes pour terminaux BlackBerry OS (versions 5.0 à 7.1)

BlackBerry OS (versions 5.0 à 7.1)

Commande	Description
Spécifier le mot de passe du terminal et verrouiller le terminal	Cette commande vous permet de créer un mot de passe de terminal, puis de verrouiller le terminal. Vous devez créer un mot de passe conforme aux règles de mots de passe existantes. Si vous ou un utilisateur avez activé la protection du contenu à deux facteurs, vous ne pouvez pas utiliser cette commande.
Supprimer uniquement les données professionnelles	Cette commande supprime les données professionnelles, y compris la stratégie informatique, les e-mails, les contacts et les annuaires de services professionnels présents sur le terminal. Toutes les données personnelles restent sur le terminal.
Supprimer toutes les données du terminal	Cette commande supprime définitivement toutes les informations d'utilisateur et données des applications stockées sur le terminal et rétablit les paramètres d'usine par défaut sur le terminal. Vous pouvez envoyer cette commande à un terminal que vous souhaitez remettre à un autre utilisateur dans votre organisation, ou à un terminal qui est perdu et que l'utilisateur risque de ne pas retrouver.
Renvoyer les annuaires de services	Cette commande renvoie les annuaires de services à un terminal. Les annuaires de services spécifient les services disponibles sur un terminal BlackBerry OS.
Envoyer de nouveau la stratégie informatique	Cette commande renvoie la stratégie informatique BlackBerry OS attribuée à un terminal.

Désactivation des terminaux

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

Vous pouvez désactiver un terminal à l'aide de la commande Supprimer les données professionnelles uniquement. Les utilisateurs peuvent désactiver leurs terminaux à l'aide des méthodes suivantes :

- Pour les terminaux iOS, Android ou Windows Phone , les utilisateurs peuvent sélectionner Désactiver mon terminal dans l'écran « À propos de » de l'application BlackBerry UEM Client.
- Pour les terminaux Windows 10, les utilisateurs peuvent sélectionner Paramètres > Comptes > Accès professionnel > Supprimer.
- Pour les terminaux BlackBerry 10, les utilisateurs peuvent sélectionner Paramètres > BlackBerry Balance > Supprimer l'espace Travail.

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

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

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

Localiser un terminal

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

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

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

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

Tâches connexes

Créer un profil de service de localisation

Utiliser le mode Perdu sur les terminaux iOS supervisés

Vous pouvez activer et gérer le mode Perdu sur les terminaux iOS supervisés exécutant iOS 9.3 ou version ultérieure. En cas de perte d'un terminal, l'activation du mode Perdu vous permet de :

- verrouiller le terminal et définir le message à afficher (par exemple, vous pouvez afficher le numéro à appeler par la personne qui trouvera le terminal) ;
- afficher l'emplacement actuel du terminal sans avoir recours à un profil de service de localisation ;

- assurer le suivi de tous les terminaux en mode Perdu à partir de la console de gestion.

Activer le mode Perdu

Le mode Perdu est pris en charge sur les terminaux iOS supervisés exécutant iOS 9.3 ou version ultérieure.

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

Localiser un terminal en mode Perdu

Avant de commencer : Activer le mode Perdu

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

Désactiver le mode Perdu

Avant de commencer : Activer le mode Perdu

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

Affichage des mises à jour disponibles pour les terminaux iOS

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

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

Tâches connexes

Envoyer un e-mail aux utilisateurs

Limitation des terminaux iOS non supervisés

Deux méthodes permettent de limiter les terminaux iOS non supervisés dans BlackBerry UEM :

- Pour les terminaux inscrits dans le programme d'inscription des terminaux (DEP), vous pouvez attribuer une configuration d'inscription aux terminaux dont le paramètre « Activer le mode supervisé » est sélectionné. Lorsque les terminaux sont activés, ils sont activés automatiquement en mode supervisé. Pour plus d'informations, reportez-vous à Attribuez une configuration d'inscription aux terminaux iOS .
- Vous pouvez attribuer aux comptes d'utilisateur un profil d'activation dont le paramètre « Ne pas autoriser l'activation des terminaux non supervisés » est sélectionné. Ce paramètre est pris en charge pour les types d'activation « Commandes MDM » et « Confidentialité de l'utilisateur » (avec des licences SIM activées). BlackBerry UEM empêche l'activation des terminaux non supervisés et supprime automatiquement les terminaux qui deviennent non supervisés, que ceux-ci soient activés avec BlackBerry UEM Client ou à l'aide du DEP. Pour plus d'informations, reportez-vous à Créer un profil d'activation.

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

Vous pouvez forcer les terminaux suivants à installer une mise à jour de système d'exploitation disponible :

- terminaux supervisés exécutant iOS 10.3 et version ultérieure
- terminaux DEP supervisés exécutant iOS 9.0 et version ultérieure

Pour mettre à jour le système d'exploitation sur plusieurs terminaux, reportez-vous à la section Envoyer une commande groupée.

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

Création de messages de support de terminal

Pour les terminaux Android 8.0 et version ultérieure, vous pouvez créer un message de support qui s'affiche sur le terminal lorsqu'une fonction est désactivée par une stratégie informatique. Le message s'affiche sur l'écran des paramètres pour la fonction qui est désactivée. Si vous ne créez pas de message de support, le terminal affiche le message par défaut pour le système d'exploitation.

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

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

Créer des messages de support de terminal

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

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

Autorisation des utilisateurs BlackBerry 10 à sauvegarder les données du terminal

Vous pouvez contrôler si les utilisateurs BlackBerry 10 peuvent sauvegarder et restaurer les données d'un terminal. Vous pouvez autoriser les utilisateurs à sauvegarder uniquement les données de l'espace Personnel ou les données des espaces Personnel et Travail. Dans la stratégie informatique que vous attribuez aux utilisateurs, vous pouvez sélectionnez l'une ou les deux règles de stratégie informatique suivantes :

Règle de stratégie informatique	Types d'activation applicables
Autoriser la sauvegarde et la restauration du terminal	• Travail et Personnel - Régulé • Espace Travail uniquement
Autoriser la sauvegarde et la restauration de l'espace Travail	• Travail et Personnel - Entreprise • Travail et Personnel - Régulé **Remarque :** Pour les terminaux activés avec Travail et Personnel - Régulé, cette règle est appliquée uniquement si la règle « Autoriser la sauvegarde et la restauration du terminal » est sélectionnée.

Si la stratégie informatique attribuée aux utilisateurs autorise les sauvegardes du terminal, les utilisateurs peuvent se connecter à BlackBerry Link pour créer ou restaurer des fichiers de sauvegarde.

Lorsque les utilisateurs créent des fichiers de sauvegarde à l'aide de BlackBerry Link, ces fichiers sont cryptés à l'aide de clés de cryptage que BlackBerry UEM envoie aux terminaux BlackBerry 10. Les clés de cryptage initiales sont générées lorsque vous installez BlackBerry UEM 12.4 ou effectuez une mise à niveau vers cette version. Si nécessaire, vous pouvez générer de nouvelles clés de cryptage, importer des clés d'une autre instance de BlackBerry UEM ou en exporter.

Générer des clés de cryptage

Vous pouvez générer les clés de cryptage qui sont utilisées pour crypter les fichiers de sauvegarde lorsque les utilisateurs sauvegardent des données sur leurs terminaux BlackBerry 10. Les clés de cryptage initiales sont automatiquement générées lorsque vous installez ou mettez à niveau vers BlackBerry UEM 12.4.

1. Sur la barre de menus, cliquez sur **Paramètres > Paramètres généraux > Sauvegarde et restauration d'un terminal BB10**.
2. Cliquez sur **Générer une nouvelle clé**.
3. Cliquez sur **Générer**.

À la fin : Les clés de cryptage sont envoyées à tous les terminaux BlackBerry 10 activés dans BlackBerry UEM.

Exporter les clés de cryptage

Vous pouvez exporter des clés de cryptage à partir de BlackBerry UEM de façon à pouvoir importer les clés d'une autre instance BlackBerry UEM.

1. Sur la barre de menus, cliquez sur **Paramètres > Paramètres généraux > Sauvegarde et restauration d'un terminal BB10**.
2. Cliquez sur **Exporter des clés**.
3. Entrez et confirmez le mot de passe du fichier.
4. Cliquez sur **Exporter**.
5. Enregistrez le fichier.

Importer des clés de cryptage

Vous pouvez importer dans BlackBerry UEM des clés de cryptage générées et exportées à partir d'une autre instance BlackBerry UEM.

Avant de commencer : Vérifiez que vous disposez du mot de passe du fichier de clés de cryptage à importer.

1. Sur la barre de menus, cliquez sur **Paramètres > Paramètres généraux > Sauvegarde et restauration d'un terminal BB10**.
2. Cliquez sur **Importer des clés**.
3. Cliquez sur **Parcourir** et accédez au fichier de clés de cryptage. Cliquez sur **Ouvrir**.
4. Indiquez le mot de passe du fichier.
5. Cliquez sur **Importer**.

Supprimer les clés de cryptage

Lorsque vous générez une nouvelle clé de cryptage, toutes les clés générées précédentes ne sont plus utiles qu'à des fins de cryptage. Si vous n'avez plus besoin des clés générées précédemment, vous pouvez les supprimer de BlackBerry UEM. Vous ne pouvez pas supprimer la dernière clé de cryptage générée.

1. Sur la barre de menus, cliquez sur **Paramètres > Paramètres généraux > Sauvegarde et restauration d'un terminal BB10**.
2. Pour supprimer une clé de cryptage, en regard de la clé, cliquez sur ✕.
3. Pour confirmer que vous souhaitez supprimer de façon permanente la clé, entrez « blackberry ». Cliquez sur **Supprimer**.

Maintenance, surveillance et génération de rapports

Vous pouvez surveiller l'état de BlackBerry UEM grâce aux fichiers journaux, journaux d'audit et outils SNMP. De plus, vous pouvez générer des rapports depuis le tableau de bord et la liste d'utilisateurs.

Utilisation des fichiers journaux

Vous pouvez utiliser les fichiers journaux pour identifier et résoudre les problèmes liés aux composants ou terminaux BlackBerry UEM dans l'environnement de votre organisation. Les fonctionnalités de journalisation BlackBerry UEM vous permettent ce qui suit :

- Suivre l'activité des composants BlackBerry UEM à l'aide des journaux du serveur
- Envoyer les données des fichiers journaux BlackBerry UEM vers un serveur syslog ou un fichier texte
- Récupérer les fichiers journaux des terminaux Android et BlackBerry 10
- Vérifier les activités des applications sur les terminaux BlackBerry 10

Gestion des fichiers journaux BlackBerry UEM

La taille des fichiers journaux varie selon le nombre d'utilisateurs et de terminaux de votre environnement BlackBerry UEM et de leur niveau d'activité. Il s'agit d'une méthode recommandée pour surveiller et contrôler la quantité d'espace disque occupé par les fichiers journaux. Pour éviter que les fichiers journaux ne prennent trop de place sur le disque, vous pouvez spécifier une taille de fichier maximale ainsi que le niveau de débogage de ces fichiers journaux..

Vous pouvez configurer les paramètres de journalisation pour les niveaux suivants :

- Paramètres de journalisation globaux : ces paramètres s'appliquent à toutes les instances de BlackBerry UEM de votre organisation qui partagent la même base de données. Ces paramètres comprennent l'emplacement du fichier syslog et la taille maximale des fichiers journaux.
- Paramètres de journalisation de l'instance : ces paramètres s'appliquent uniquement à l'instance de BlackBerry UEM que vous sélectionnez et remplacent les paramètres globaux. Ces paramètres comprennent l'activation de l'option d'emplacement local des fichiers journaux et le niveau de journalisation de ces derniers.

Configurer les paramètres de journalisation globaux

1. Sur la barre de menus, cliquez sur **Paramètres** > **Infrastructure** > **Journalisation**.
2. Configurez les paramètres globaux suivants tels que requis pour l'environnement de votre organisation :

   Remarque : la modification de ces paramètres implique un redémarrage du système.

Paramètre	Étapes
Pour acheminer des événements système vers un serveur syslog	**a.** Cochez la case **SysLog**. Par défaut, cette case est décochée. **b.** Spécifiez le nom d'hôte et le port du serveur syslog où vous souhaitez acheminer les événements des journaux BlackBerry UEM.
Pour spécifier un emplacement sur l'instance du serveur où les fichiers journaux des composants BlackBerry UEM sont stockés	**a.** Cochez la case **Activer la destination du fichier local**.

Paramètre	Étapes
Pour activer la journalisation avancée des communications serveur-terminal à des fins de dépannage	**a.** Cochez la case **Activer la journalisation de charge utile MDM**.
Pour définir une taille maximale pour les fichiers journaux des composants BlackBerry UEM	Dans le champ **Taille maximale du fichier journal**, spécifiez la taille maximale, en Mo, de chaque fichier journal. Lorsqu'un fichier journal atteint la taille maximale, BlackBerry UEMcommence une nouvelle instance du fichier journal.
Pour définir l'ancienneté maximale des fichiers journaux du composant BlackBerry UEM	Dans le champ **Ancienneté maximale des fichiers journaux** , spécifiez le nombre de jours durant lesquels les fichiers journaux du serveur seront conservés avant d'être supprimés. Si vous ne spécifiez aucune valeur, les fichiers journaux ne sont pas supprimés.
Pour spécifier un chemin de destination réseau pour les fichiers journaux des terminaux Android et BlackBerry 10	Dans le champ **Emplacement réseau des journaux des terminaux**, spécifiez le chemin UNC où vous souhaitez stocker les fichiers journaux que vous récupérez depuis les terminaux à l'aide de la console de gestion.
Ancienneté maximale des fichiers journaux d'audit des applications du terminal	Dans le champ **Ancienneté maximale des fichiers journaux d'audit des applications du terminal** , spécifiez le nombre de jours durant lesquels les fichiers journaux d'audit des applications du terminal seront conservés avant d'être supprimés. Si vous ne spécifiez aucune valeur, les fichiers journaux ne sont pas supprimés.

3. Cliquez sur **Enregistrer**.

Définir un niveau de journal pour des composants BlackBerry UEM individuels

Pour aider à faciliter la résolution des problèmes et prévenir l'impact sur les performances du à un excès de génération de fichiers journaux, vous pouvez activer des composants BlackBerry UEM individuels afin d'écrire dans des fichiers journaux à différents niveaux d'information. Par exemple, vous pouvez configurer le BlackBerry UEM Core pour produire des fichiers journaux au niveau de débogage et laisser le reste des composants pour générer des fichiers journaux au niveau des informations.

1. Sur la barre de menus, cliquez sur **Paramètres > Infrastructure > Journalisation**.
2. Développez **Paramètres de journalisation globaux**.
3. Dans la section **Remplacement de la journalisation des services**, cliquez sur +.
4. Sélectionnez un composant UEM.
5. Dans la liste déroulante **Niveau de journalisation**, sélectionnez un niveau de journalisation.
6. Cliquez sur **Enregistrer**.

À la fin : Si nécessaire, vous pouvez remplacer ces paramètres. Pour plus d'informations, reportez-vous aux sections Modifier les paramètres par défaut des instances de BlackBerry Connectivity Node et Créer un groupe de serveurs.

Configurer les paramètres de journalisation de l'instance

1. Sur la barre de menus, cliquez sur **Paramètres** > **Infrastructure** > **Journalisation**.
2. Développez l'instance de serveur que vous souhaitez configurer.
3. Configurez les paramètres suivants tels que requis pour l'environnement de votre organisation :

Paramètre	Étapes
Pour spécifier l'emplacement où les fichiers journaux des composants de BlackBerry UEM sont stockés	**Remarque :** Pour modifier ce paramètre, vous devez d'abord cocher la case **Activer la destination des fichiers locaux** dans les paramètres globaux de journalisation. **a.** Dans le champ **Chemin d'accès au journal du serveur**, entrez le chemin de l'emplacement où vous souhaitez stocker les fichiers journaux. Par défaut, les fichiers journaux sont stockés sous `C:\Program Files\BlackBerry\UEM\Logs\aaaammjj`.
Pour définir le niveau de détails des fichiers journaux	Dans la liste déroulante **Niveaux de débogage des journaux**, sélectionnez l'une des options suivantes : • **Info** : consignez les activités quotidiennes ainsi que les messages d'avertissement et d'erreur dans le fichier journal. • **Avertissement** : consignez les messages d'avertissement et d'erreur dans le fichier journal. Les messages d'avertissement sont des événements imprévus pouvant nécessiter votre intervention. • **Erreur** : consignez tous les messages d'erreur dans le fichier journal. Lorsqu'une condition d'erreur apparait, il vous faut généralement intervenir. • **Débogage** : consignez les informations uniquement requises pour déboguer un problème. • **Suivi** : consignez les informations supplémentaires qu'un développeur peut utiliser à des fins de débogage approfondi. Par défaut, le niveau de débogage est défini sur **Info**.
Pour spécifier le dossier des fichiers journaux d'audit des applications des terminaux Android et BlackBerry 10	Dans le champ **Chemin d'accès au journal d'audit des applications du terminal**, saisissez le chemin du dossier où vous souhaitez stocker les fichiers journaux d'audit des applications du terminal.
Pour définir la taille maximale du fichier journal d'audit des applications du terminal	Dans le champ **Taille maximale du journal d'audit des applications**, spécifiez la taille maximale, en Mo, que les fichiers journaux d'audit des applications du terminal peuvent atteindre. Lorsqu'un fichier journal atteint la taille maximale, BlackBerry UEMcommence une nouvelle instance du fichier journal.

4. Cliquez sur **Enregistrer**.

Modifier la durée de conservation maximale d'un fichier journal

1. Sur la barre de menus, cliquez sur **Paramètres** > **Infrastructure** > **Journalisation**.
2. Développez **Paramètres de journalisation globaux**.
3. Configurez la durée de conservation maximale d'un fichier journal du serveur en jours.

4. Cliquez sur **Enregistrer**.

Modifier le niveau de journal de mise en garde des clients Microsoft Intune

Si vous utilisez Microsoft Intune, nous vous recommandons de modifier le niveau du journal de mise en garde.

1. Sur le serveur BlackBerry UEM où vous souhaitez modifier le niveau de journal, localisez le fichier log4J.xml. Le fichier se trouve par défaut à l'emplacement suivant : `C:\Program Files\BlackBerry\BES\Core \tomcat-core\webapps\ROOT\WEB-INF\classes`
2. Dans le fichier, au-dessus de la valeur <root>, ajoutez les informations suivantes : `<logger name="org.apache.http.wire"> <level value="warn"/> </logger>`
3. Redémarrez le service BlackBerry UEM Core.

Recherche de fichiers journaux

Par défaut, un fichier journal est créé pour chaque composant de BlackBerry UEM et stocké sur l'ordinateur qui héberge le composant. Si vous installez plusieurs instances de BlackBerry UEM, chaque ordinateur crée ses propres fichiers journaux. BlackBerry UEM Nomme les fichiers *<nom_serveur>_<identifiant_composant>_<aaaammjj>_<numéro_journal>.<extension_fichier>* (par exemple, ServeurBB01_MDAT_20140730_0001.txt).

Les fichiers journaux suivants sont disponibles dans une solution BlackBerry UEM :

- Fichiers journaux pour les composants utilisés pour gérer les terminaux BlackBerry 10, iOS, Android et Windows.

  Les fichiers journaux sont les suivants :

  - ACCS - Fichiers journaux avec accès Tomcat
  - AFMGR - Fichiers journaux BlackBerry Affinity Manager
  - BGS - Fichiers journaux BlackBerry Gatekeeping Service
  - BSG - Fichiers journaux BlackBerry Secure Gateway
  - CORE - Fichiers journaux BlackBerry UEM Core
  - DISP - Fichiers journaux BlackBerry Dispatcher
  - EVNT - Fichiers journaux d'événements BlackBerry UEM Core
  - MDAT - Fichiers journaux BlackBerry MDS Connection Service
  - TMCT - Fichiers journaux du serveur Tomcat
  - UI - Fichiers journaux de la console de gestion BlackBerry UEM
  - Fichier <FQDN_serveur>_aaaammjj.csv*<FQDN_Ordinateur>*_aaaammjj.csv utilisé pour la journalisation de BlackBerry MDS Connection Service pour BlackBerry UEM.

    Remarque : Pour en savoir plus sur le fichier journal .csv de BlackBerry MDS Connection Service, rendez-vous sur le site Web support.blackberry.com/kb pour consulter l'article 36936.

  Des fichiers journaux supplémentaires sont créés lors de la première installation de BlackBerry UEM.

  Par défaut, ces fichiers journaux sont stockés à l'emplacement suivant : `<lecteur>:\Program Files \BlackBerry\UEM\Logs\<date ou nom de dossier>`
- Les fichiers journaux utilisés pour BlackBerry Secure Connect Plus sont les suivants :

  - BSCP - Fichiers journaux BlackBerry Secure Connect Plus consignant des données pour les connexions à l'application BlackBerry Secure Connect Plus
  - BSCP-TS - Fichiers journaux principaux BlackBerry Secure Connect Plus consignant des données sur le composant BlackBerry Secure Connect Plus

  Les fichiers journaux BlackBerry Secure Connect Plus sont stockés à l'emplacement suivant : <lecteur>: \Program Files\BlackBerry\UEM\Logs\.

- Les fichiers journaux utilisés pour BlackBerry Work Connect Notification Service sont les suivants :
  - BWCN - Fichiers journaux BlackBerry Work Connect Notification Service

  Les fichiers journaux BlackBerry Work Connect Notification Service sont stockés à l'emplacement suivant : `<lecteur>:\Program Files\BlackBerry\UEM\Logs\BWCN\<nom de fichier>`
- Fichiers journaux pour les composants utilisés pour gérer les terminaux BlackBerry OS (versions 5.0 à 7.1) (le cas échéant)

  Par défaut, ces fichiers journaux quotidiennement sont stockés à l'emplacement suivant : `C:\Program Files\Research In Motion\BlackBerry Enterprise Server\Logs\<date ou nom de dossier>`.

  Pour plus d'informations sur les fichiers journaux pour BES5, reportez-vous au Guide d'administration de BES5.
- Les fichiers des journaux BBM, journaux du téléphone, journaux PIN à PIN, journaux SMS/MMS et journaux de chat vidéo sont stockés au format .csv et utilisés pour vérifier les activités des applications.

  Par défaut, les fichiers journaux d'audit d'application pour les terminaux BlackBerry 10 sont stockés dans *C:\Program Files\BlackBerry\UEM\Logs* et fichiers journaux d'audit d'application pour les terminaux BlackBerry sont stockés dans *C:\Program Files (x86)\Research in Motion\BlackBerry Enterprise Server\Logs*.
- Les fichiers journaux pour Good Control sont stockés dans : *C:\Program Files\BlackBerry\UEM\Logs\gclogs*
- Les fichiers journaux pour Good Proxy sont stockés dans : *C:\Program Files\BlackBerry\UEM\Logs\gpslogs*

Lecture des fichiers journaux

Les fichiers journaux BlackBerry UEM sont enregistrés sous deux formats, fichiers de valeurs séparés par une virgule et fichiers texte.

Les journaux BlackBerry Gatekeeping Service, paquets de journaux BlackBerry UEM, journaux de contacts et de messages, d'appels téléphoniques, de messages PIN, de SMS et de chats vidéos BlackBerry Messenger sont stockés au format CSV.

Tous les autres fichiers journaux sont stockés au format TXT.

Lecture des fichiers journaux .csv

Les fichiers journaux séparés par des virgules contiennent différentes informations selon le composant, le terminal ou l'application faisant l'objet de la journalisation. Les fichiers journaux au format .csv comprennent notamment le fichier journal BlackBerry Gatekeeping Service et les fichiers d'audit des applications du terminal comme les journaux des applications BBM ou Téléphone.

Vous pouvez identifier les informations contenues dans les fichiers journaux .csv car chaque ligne de journal présente des informations de façon simple et cohérente. Par exemple, chaque ligne du fichier journal SMS présente des informations au format suivant :

```
Name.ID,"Email Address","Type of Message","To","From","Callback Phone
 Number","Body","Send/Received Date","Server Log Date","Overall Message
 Status","Command","UID"
```

Chaque ligne du fichier journal Téléphone présente des informations au format suivant :

```
Name.ID,"Type of Call","Name","Phone Number","Start Date","Server Log
 Date","Elapsed Time","Memo","Command","UID","Phone Line"
```

Lecture des fichiers journaux .txt

Les fichiers journaux stockés sous forme de fichiers .txt présentent deux formats de base :

- Le premier format est le plus commun et commence généralement par la date et l'heure, fournissant des informations comme suit :

  ```
  TimeStamp Hostname AppName ProcessId MessageID [StructuredData] Message
  ```

  Par exemple :

  ```
  2015-06-12T12:07:17.634-0400 computer.example.com MDM localhost-startStop-1
   logging.feature.admin.application.management|logging.component.appmgmt
   [{{requestId,543ade23}{myContextInfo,runningContext}}] INFO  Total 2 routes,
   of which 2 is started.
  ```

- Le deuxième format, commençant par un indicateur de niveau numérique, fournit des informations comme suit :

  ```
  Level Date Thread CID Message
  ```

  Par exemple :

  ```
  <#03>[30000] (09/10 00:00:00.122):{0x520} [DIAG] EVENT=Thread_report,
   THREADID=0x1390, THREADNAME="SRPReceiverHandler"
  ```

Des variantes sont possibles, selon le composant ou la fonctionnalité en cours de journalisation, mais tous les fichiers journaux stockés sous forme de fichiers `.txt` contiennent les informations de base suivantes.

Élément	Description
Date ou horodatage	L'horodatage se présente sous la forme <Date><Heure><Différence par rapport à l'UTC>. La Date/Heure indique la date et l'heure d'un événement particulier. **Remarque :** l'horodatage correspond à l'heure du serveur local.
Nom d'hôte ou identification des composants	Identification du composant ou nom d'hôte vous indique le composant sur lequel porte le fichier journal. Dans certains cas, cela semble évident, comme pour CORE ou MDS-CS, mais dans d'autres, cela l'est moins, comme l'utilisateur d'un identifiant numérique.
Nom de l'application	Le nom de l'application est identique pour tous les fichiers journaux et est indiqué en tant que MDM.
IDProcessus ou Thread	Représente l'ID du thread Java qui consigne actuellement un message. Par exemple : `localhost-startStop-1`
IDMessage	L'IDMessage identifie le type de message envoyé au fichier journal. C'est une combinaison de la fonction et du composant enregistrés au format <fonction>|<composant>. Par exemple : `admin.application.management|appmgmt`

Élément	Description
DonnéesStructurées	Zéro paires de valeurs de nom ou plus qui représentent des données structurées. Par exemple : `[{{requestId,543ade23} {myContextInfo,runningContext}}]`
Message	Le message indique l'activité et décrit la nature de l'événement. Un message peut inclure des informations sur le matériel ou le logiciel utilisé ou le problème qui survient. Par exemple : `INFO (2 itinéraires au total, dont 2 ont démarré).`

Niveau	Le niveau d'événement indique le type d'entrée de journal. Les événements sont généralement classés comme suit :
	• ERROR = Erreur
	• WARN = Avertissement
	• INFO = Informations
	ENV = Environnement
	• DEBUG = Débogage
	• Autre
	  • DIAG = Diagnostic
	  • TRAC = Trace
	Dans certains fichiers journaux, le niveau est indiqué par une valeur numérique au format suivant :
	• [10000] = Erreur
	• [20000] = Avertissement
	• [30000] = Informations
	• [40000] = Débogage
	• [50000] = Autre

Niveaux des fichiers journaux

Niveau	Description
DÉBOGAGE	Ce niveau spécifie les informations utiles au débogage des problèmes de codage. Les événements peuvent inclure ce qui suit : • Etats des ressources suspectes dans les conditions d'erreur • Transitions entre les composants internes et externes • Demandes REST envoyées à BlackBerry UEM Core • Demandes envoyées à Microsoft Active Directory

Niveau	Description
ERREUR	Ce niveau spécifie une condition d'erreur nécessitant votre intervention ou celle d'un spécialiste de l'assistance. Les événements peuvent inclure ce qui suit : • Exceptions de codage • Exceptions du niveau de données • Exceptions de codage récupérables
INFO	Ce niveau spécifie les événements système normaux pouvant être attendus par les administrateurs ou les spécialistes de l'assistance. Ce niveau correspond au niveau par défaut pour BlackBerry UEM.
SUIVI	Ce niveau spécifie les informations utiles aux personnes dotées de connaissances de développement, y compris les informations utilisées pour les classes et le traçage des méthodes, les paramètres des méthodes, etc.
AVERTISSEMENT	Ce niveau peut indiquer une condition d'avertissement, une action requise ou la survenue d'un événement inattendu. Les événements peuvent inclure ce qui suit : • Données incohérentes • Demandes inattendues • Échecs d'autorisation • Échecs d'authentification

Utilisation des fichiers journaux à des fins de résolution des problèmes

Identifiant du composant	Composant de journalisation	Description
ACCS	Fichiers journaux d'accès au serveur Apache Tomcat	Les fichiers journaux ACCS Apache Tomcat consignent toutes les demandes d'accès envoyés aux services Web BlackBerry UEM. Vous pouvez utiliser ces fichiers journaux pour vérifier si les demandes d'accès aux services Web BlackBerry UEM ont échoué ou abouti.

Identifiant du composant	Composant de journalisation	Description
AFMGR	BlackBerry Affinity Manager	BlackBerry Affinity Manager contient des informations sur la fonctionnalité et l'état de basculement en présence de plusieurs instances de BlackBerry Affinity Manager dans l'environnement de votre organisation. Vous pouvez également résoudre les problèmes liés à ce qui suit : • Connectivité entre BlackBerry UEM et BlackBerry Infrastructure • Connectivité entre les terminaux BlackBerry UEM et BlackBerry 10 • Problèmes de fonctionnement entrainant la modification de l'instance active de BlackBerry Affinity Manager
BGS	BlackBerry Gatekeeping Service	Vous pouvez utiliser ces fichiers journaux pour résoudre les problèmes liés à ce qui suit : • Non-activation des terminaux dans un environnement où BlackBerry Gatekeeping Service est en cours d'utilisation • Connectivité à BlackBerry Gatekeeping Service • Connectivité entre BlackBerry UEM et BlackBerry Infrastructure • Activations BlackBerry 10 et envoi de stratégies et de profils • Connectivité de iOS, Android et Windows Phone
BSCP	BlackBerry Secure Connect Plus	Consigne des données sur le composant BlackBerry Secure Connect Plus. Vous pouvez utiliser ces fichiers journaux pour vérifier que BlackBerry Secure Connect Plus est connecté à BlackBerry Infrastructure. Par exemple : 2015-01-19T13:17:47.540-0500 - BSCP {TcpClientConnectorNio#2} logging.feature.bscp.service| logging.component.bscp.pss.bcp [{}] - DEBUG Received Ping from [id: 0x60bce5a3, /192.0.2.0:28231 => bcp.example.com/192.0.2.124:3101], responding with Pong. 2015-01-19T13:18:22.989-0500 - BSCP {ChannelPinger#1} logging.feature.bscp.service| logging.component.bscp.pss.bcp [{}] - DEBUG Sending Ping to [id: 0xb4a1677a, /192.0.2.0:28232 => bcp.example.com/192.0.2.124:3101]

Identifiant du composant	Composant de journalisation	Description
BSCP-TS	BlackBerry Secure Connect Plus Core	Consigne les données des connexions au client BlackBerry Secure Connect Plus. Vous pouvez utiliser ces fichiers journaux pour vérifier que BlackBerry Secure Connect Plus est prêt à recevoir des appels à partir du client BlackBerry Secure Connect Plus sur les terminaux. Par exemple : 47: [14:13:21.231312][][3][AsioTurnSocket-1] Connected, host=68-171-243-141.rdns.blackberry.net 48: [14:13:21.239312][][3][AsioTurnSocket-1] Creating TURN allocation 49: [14:13:21.405121][][3][AsioTurnSocket-1] TURN allocation created Pour vérifier que les terminaux utilisent le tunnel sécurisé. Par exemple : 74: [10:39:45.746926][][3][Tunnel-2FFEC51E] Sent: 2130.6 KB (1733), Received: 201.9 KB (1370), Running: 00:07:00.139249
BSG	BlackBerry Secure Gateway	Vous pouvez utiliser ces fichiers journaux pour résoudre les problèmes liés à ce qui suit : • Terminaux iOS ne pouvant ni envoyer ni recevoir des e-mails • Connectivité entre BlackBerry UEM et BlackBerry Infrastructure • Connectivité entre BlackBerry Infrastructure et le serveur de messagerie Microsoft Exchange ou Microsoft Office 365
BWCN	BlackBerry Work Connect Notification Service	Vous pouvez utiliser ces fichiers journaux pour résoudre les problèmes liés aux terminaux iOS ne recevant pas de notifications sur les nouveaux éléments ou les éléments modifiés.
CORE	BlackBerry UEM Core	Vous pouvez utiliser ces fichiers journaux pour résoudre les problèmes liés à ce qui suit : • Services principaux ou transactions • Transactions BlackBerry 2FA • Migration de données à partir de BES10
DISP	BlackBerry Dispatcher	Vous pouvez utiliser ces fichiers journaux pour résoudre les problèmes liés à ce qui suit : • Connectivité entre BlackBerry UEM et BlackBerry Infrastructure • Connectivité entre les terminaux BlackBerry UEM et BlackBerry 10

Identifiant du composant	Composant de journalisation	Description
EVNT	BlackBerry UEM Core	Vous pouvez utiliser ces fichiers journaux pour trouver les notifications relatives à des événements spécifiques dans BlackBerry UEM Core.
MDAT	BlackBerry MDS Connection Service	Vous pouvez utiliser ces fichiers journaux pour résoudre les problèmes liés à ce qui suit : • Applications du terminal BlackBerry 10 • Problèmes de transfert des applications • Problèmes d'authentification de transfert des applications
ROUT	BlackBerry Router	Vous pouvez utiliser ces fichiers journaux pour résoudre les problèmes liés à ce qui suit : • Installation de BlackBerry Router • Connectivité entre BlackBerry UEM et BlackBerry Router • Connectivité entre BlackBerry UEM et BlackBerry Infrastructure • Connectivité entre BlackBerry Router et BlackBerry Infrastructure • Connectivité entre les terminaux et BlackBerry UEM **Remarque :** Les fichiers journaux BlackBerry Router sont uniquement disponibles si vous avez installé BlackBerry Router dans l'environnement de votre organisation.
TMCT	Fichiers journaux du serveur Apache Tomcat	Les fichiers journaux TMCT Apache Tomcat permettent d'enregistrer toutes les activités des services Web Apache Tomcat. Vous pouvez utiliser ces fichiers journaux pour résoudre les problèmes avec la console de gestion.
UI	Console de gestion	Vous pouvez utiliser ces fichiers journaux pour résoudre les problèmes avec la console de gestion.

Vérification des activités des applications sur les terminaux BlackBerry 10 et BlackBerry OS

Vous pouvez utiliser les journaux pour suivre l'activité des applications sur les terminaux BlackBerry 10 avec les types d'activation Travail et Personnel - Entreprise, Travail et Personnel - Régulé et Espace Travail uniquement et les terminaux avec systèmes d'exploitation BlackBerry (versions 5.0 à 7.1).

Vous devez configurer les règles de stratégie informatique suivantes pour générer ces fichiers journaux :

Règle de stratégie informatique pour BlackBerry 10	Règle de stratégie informatique pour les terminaux BlackBerry OS	Description
Synchroniser les journaux BBM	Désactiver la synchronisation sans fil BlackBerry Messenger	Cette règle spécifie si un terminal synchronise des journaux depuis BlackBerry Messenger avec BlackBerry UEM.
Synchroniser les journaux du téléphone	Désactiver la synchronisation sans fil des journaux d'appels téléphoniques	Cette règle spécifie si un terminal synchronise les journaux d'appels téléphoniques avec BlackBerry UEM.
Synchroniser les journaux PIN à PIN	Désactiver la synchronisation sans fil des messages PIN	Cette règle spécifie si un terminal synchronise les journaux des messages PIN avec BlackBerry UEM.
Synchroniser les journaux SMS/MMS	Désactiver la synchronisation mobile des messages SMS	Cette règle spécifie si un terminal synchronise les journaux des messages SMS et MMS avec BlackBerry UEM.
Synchroniser les journaux de chat vidéo	Ne s'applique pas aux terminaux BlackBerry OS	Cette règle spécifie si un terminal BlackBerry 10 synchronise les journaux pour la fonctionnalité BBM Video avec BlackBerry UEM.

Par défaut, les fichiers journaux d'audit d'application des terminaux BlackBerry 10 sont stockés sous *C:\Program Files\BlackBerry\UEM\Logs\<aaaammjj>* et ceux des terminaux BlackBerry sous *C:\Program Files (x86)\Research in Motion\BlackBerry Enterprise Server\Logs\<aaaammjj>*.

Affichage des actions du terminal

Actions prises ou en cours sur un terminal suite aux commandes que vous avez envoyées à partir de la console de gestion BlackBerry UEM, telles que le verrouillage d'un terminal, la désactivation de l'espace Travail ou la suppression des données du terminal.

La disponibilité de ces commandes dépend du terminal et du type d'activation.

Une commande de terminal peut présenter l'état suivant :

- Commande annulée
- Commande terminée par le terminal
- Commande remise au terminal
- Commande reçue par le terminal
- Echec de la commande
- Commande en cours
- Notification reçue par le terminal
- Notification envoyée au terminal
- En file d'attente

Afficher les actions du terminal

1. Sur la barre de menus, cliquez sur **Utilisateurs > Terminaux gérés**.
2. Recherchez un compte d'utilisateur.

3. Dans les résultats de la recherche, cliquez sur le nom d'un compte d'utilisateur.
4. Cliquez sur l'onglet du terminal dont vous souhaitez afficher les actions.
5. Cliquez sur **Afficher les actions du terminal**.

Récupérer les journaux des terminaux

Pour récupérer les fichiers journaux des terminaux, utilisez les méthodes suivantes :

Méthode	Description	Terminaux pris en charge
Obtenir les journaux des terminaux à l'aide d'une commande BlackBerry UEM	Vous pouvez récupérer les fichiers journaux des terminaux à l'aide de la commande « Obtenir les journaux du terminal ». Un instantané des fichiers journaux du terminal est collecté chaque fois que vous utilisez la commande du terminal pour les récupérer. Les utilisateurs sont informés de votre capacité à collecter les fichiers journaux système lors de l'activation des terminaux et peuvent être à nouveau informés lorsque vous envoyez la commande de récupération des fichiers journaux, selon les paramètres des terminaux. Sur les terminaux iOS et Android, BlackBerry UEM Client doit être installé et seuls les fichiers journaux BlackBerry UEM Client sont récupérés. Pour les terminaux BlackBerry 10, tous les journaux du terminal sont récupérés.	• iOS • Android • BlackBerry 10
Envoyer des fichiers journaux depuis BlackBerry UEM Client	Les utilisateurs de terminaux peuvent envoyer des fichiers journaux à leur administrateur par e-mail à l'aide du menu Aide de BlackBerry UEM Client.	• iOS • Android
Envoyer les fichiers journaux des terminaux BlackBerry 10 à BlackBerry Technical Support Services	Vous pouvez envoyer des fichiers journaux BlackBerry 10 à BlackBerry Technical Support Services à l'aide de la règle de stratégie informatique Envoyer des journaux à BlackBerry, afin de spécifier si le terminal peut générer et envoyer des fichiers journaux.	• BlackBerry 10
Envoyer les fichiers journaux depuis le catalogue d'applications BlackBerry UEM	Les utilisateurs de terminaux Windows 10 peuvent envoyer des fichiers journaux à leur administrateur par e-mail à l'aide du menu Aide du catalogue d'applications de BlackBerry UEM.	• Windows 10

Obtenir les journaux des terminaux à l'aide d'une commande BlackBerry UEM

Vous pouvez utiliser une commande BlackBerry UEM pour obtenir les fichiers journaux à partir des types de terminaux suivants :

- iOS
- Android
- BlackBerry 10

Avant de commencer :

- Les terminaux BlackBerry 10 doivent exécuter BlackBerry 10 OS version 10.3.1 ou ultérieure. Pour les terminaux activés via le type d'activation « Travail et Personnel - Entreprise », les utilisateurs doivent activer le paramètre Collecte de journaux à distance. Pour plus d'informations, rendez-vous sur http://support.blackberry.com/kb et lisez l'article KB 36424.
- Les terminaux iOS et Android doivent disposer de BlackBerry UEM Client.
- Par défaut, le rôle Centre d'assistance junior ne permet pas de récupérer des fichiers journaux.

1. Sur la barre de menus, cliquez sur **Utilisateurs > Terminaux gérés**.
2. Recherchez un compte d'utilisateur.
3. Dans les résultats de la recherche, cliquez sur le nom du compte d'utilisateur.
4. Cliquez sur l'onglet du terminal.
5. Dans la fenêtre **Gérer les terminaux**, cliquez sur **Obtenir les journaux du terminal**.
6. Cliquez sur **Demander**.

À la fin :

Récupérez les fichiers journaux du terminal. Par défaut, les fichiers journaux sont stockés sous C:\Program Files \BlackBerry\UEM\Logs\device_logs.

Envoyer les fichiers journaux des terminaux BlackBerry 10 à BlackBerry Technical Support Services

Vous pouvez configurer un terminalBlackBerry 10pour l'autoriser à envoyer des fichiers journaux àBlackBerry Technical Support Services. Vous pouvez utiliser la règle de stratégie informatique**Envoyer des journaux à BlackBerry**pour spécifier si le terminal peut générer et envoyer des fichiers journaux.

L'utilisateur doit disposer d'un ticket ouvert avec BlackBerry Technical Support Services et fournir le numéro de ticket lors de l'envoi des fichiers journaux du terminal. Si l'utilisateur ne fournit pas le numéro de ticket d'assistance, l'adresse électronique qui convient ou le code PIN associé au ticket d'assistance, le terminal affiche un message d'erreur lorsque vous tentez d'envoyer les fichiers journaux du terminal.

Envoyer des fichiers journaux depuis BlackBerry UEM Client

Les utilisateurs peuvent vous envoyer des fichiers journaux depuis BlackBerry UEM Client pour les terminaux suivants :

- iOS
- Android
- Windows Phone 8

1. Sur le terminal, sélectionnez l'icône **UEM Client**.
2. Sélectionnez **Aide**.
3. Sélectionnez **Envoyer les journaux** ou **Rapport de bogues**.
4. Sélectionnez le compte de messagerie du terminal auquel envoyer le fichier journal.
5. Sélectionnez **Envoyer**.
    - Les fichiers journaux iOS et Android sont joints à l'e-mail sous forme de fichier .zip.
    - Les fichiers journaux du terminal Windows Phone 8 sont placés dans le corps de l'e-mail

Exemple de journal d'un terminal Android :

```
[2014-09-29 10:33:50 -0400 ERROR] (262): logging level set to default (warning and
 above)
[2014-09-29 10:33:50 -0400 ERROR] (262): IsCertificateTrusted failed for cert.
 Certificate not trusted.
[2014-09-29 12:10:50 -0400 ERROR] javax.net.ssl.SSLException: Connection closed by
 peer
com.android.org.conscrypt.NativeCrypto.SSL_do_handshake(Native Method)
com.android.org.conscrypt.OpenSSLSocketImpl.startHandshake(OpenSSLSocketImpl.java:405)
com.android.org.conscrypt.OpenSSLSocketImpl
$SSLInputStream.<init>(OpenSSLSocketImpl.java:661)
com.android.org.conscrypt.OpenSSLSocketImpl.getInputStream(OpenSSLSocketImpl.java:632)
org.apache.http.impl.io.SocketInputBuffer.<init>(SocketInputBuffer.java:70)
org.apache.http.impl.SocketHttpClientConnection.createSessionInputBuffer(SocketHttpClientCon
org.apache.http.impl.conn.DefaultClientConnection.createSessionInputBuffer(DefaultClientConn

.....

hoD0R.hoDoR.hodor(SourceFile:149)
hoD0R.Hodor.hodoR(SourceFile:36)
Hod0r.Hodor.executeCommand(SourceFile:29)
hoD0R.hodor.run(SourceFile:70)
hoD0R.hoDor.hodor(SourceFile:119)
hoD0R.Hodor.hodoR(SourceFile:36)
com.rim.mobilefusion.client.service.hodor.hodor(SourceFile:96)
com.rim.mobilefusion.client.GCMIntentService.hodor(SourceFile:99)
com.google.android.gcm.GCMBaseIntentService.onHandleIntent(SourceFile:223)
android.app.IntentService$ServiceHandler.handleMessage(IntentService.java:65)
android.os.Handler.dispatchMessage(Handler.java:102)
android.os.Looper.loop(Looper.java:136)
android.os.HandlerThread.run(HandlerThread.java:61)

[2014-09-29 12:10:51 -0400 ERROR] (321): Error encountered executing server
 command - exiting command processing
```

Envoyer les fichiers journaux depuis le catalogue d'applications BlackBerry UEM

Les utilisateurs de terminaux Windows 10 peuvent vous envoyer les fichiers journaux depuis le catalogue d'applications BlackBerry UEM.

1. Sur le terminal, sélectionnez l'icône **Catalogue d'applications**.
2. Sélectionnez **Aide**.
3. Sélectionnez **Rapport de bogues**.
4. Sélectionnez le compte de messagerie du terminal auquel envoyer le fichier journal.
5. Sélectionnez **Envoyer**. Les fichiers journaux sont joints à l'e-mail sous forme de fichier .zip.

Audit d'évènements dans BlackBerry UEM

BlackBerry UEM conserve les évènements d'audit d'administrateur et de sécurité dans des fichiers journaux que vous pouvez utiliser pour étudier n'importe quelle action ou interaction d'administrateur entre BlackBerry UEM et les terminaux.

BlackBerry UEM enregistre toutes les actions que les administrateurs effectuent dans la console de gestion et les affiche sur l'écran Audit. Vous pouvez filtrer la liste des actions pour afficher uniquement les actions pertinentes

pour votre examen. À des fins d'analyse approfondie et de génération de rapports, vous pouvez exporter la liste filtrée vers un fichier .csv.

Vous pouvez exporter des évènements d'audit de sécurité vers un fichier .csv à partir de l'écran Configuration de l'audit. Les évènements d'audit de sécurité incluent des actions telles que la mise en œuvre de commandes ou stratégies, le démarrage ou l'arrêt d'une instance de BlackBerry UEM, l'initialisation ou la résiliation de canaux approuvés, l'état de validation de certificat et les modifications des paramètres d'audit. Sur l'écran Configuration de l'audit, vous pouvez choisir les types d'évènement de sécurité que vous voulez enregistrer dans le fichier journal. Pour certains évènements, vous pouvez choisir de consigner l'évènement selon son état d'avancement (terminé ou non terminé).

Remarque :

Configurer les paramètres d'audit

Vous pouvez activer ou désactiver l'audit des évènements d'administrateur ou de sécurité dans BlackBerry UEM. Lorsque l'audit est activé, vous pouvez choisir le délai de conservation des enregistrements, le nombre de résultats à afficher et la date de suppression des anciens enregistrements. Lorsque l'audit est désactivé, tous les enregistrements sont supprimés.

Remarque : L'activation de l'audit des évènements de sécurité nécessite d'importantes ressources de base de données. Vous pouvez télécharger le Calculateur de performances et l'utiliser pour estimer les ressources nécessaires.

1. Sur la barre de menus, cliquez sur **Paramètres** > **Infrastructure** > **Configuration de l'audit**.
2. Dans le volet de droite, cliquez sur .
3. Dans la section **Paramètres d'audit des évènements d'administrateur**, effectuez l'une des opérations suivantes :

Tâche	Étapes
Activer l'audit des évènements d'administrateur	**a.** Dans le champ **Audit des évènements de l'administrateur**, cliquez sur **Activé**. **b.** Dans le champ **Durée de conservation des enregistrements d'audit de l'administrateur**, saisissez la durée maximale de conservation d'un enregistrement (en jours). **c.** Dans le champ **Nombre maximum d'enregistrements**, saisissez le nombre maximum d'enregistrements à afficher dans l'interface utilisateur. Si le nombre d'enregistrements dépasse cette valeur, l'administrateur doit raccourcir la plage de dates ou sélectionner une catégorie pour réduire le nombre d'enregistrements. **d.** Dans le champ **Heure de suppression quotidienne (UTC)**, choisissez l'heure de la journée à laquelle les enregistrements doivent être supprimés.
Désactiver l'audit des évènements d'administrateur et purger tous les enregistrements	**a.** Dans le champ **Audit des évènements d'administrateur**, cliquez sur **Désactivé**.

4. Dans la section **Paramètres d'audit des évènements de sécurité**, effectuez l'une des opérations suivantes :

Tâche	Étapes
Activer l'audit des évènements de sécurité	**a.** Dans le champ **Audit des évènements de sécurité**, cliquez sur **Activé**. **b.** Dans le champ **Durée de conservation des enregistrements d'audit de sécurité**, saisissez la durée maximale de conservation d'un enregistrement (en jours). **c.** Dans le champ **Heure de suppression quotidienne (UTC)**, choisissez l'heure de la journée à laquelle les anciens enregistrements sont supprimés. **d.** Pour arrêter l'audit d'un évènement de sécurité, cliquez sur ✕ en regard du type d'évènement. **e.** Pour ajouter des évènements de sécurité à auditer, cliquez sur +. Sélectionnez les évènements, puis cliquez sur **Ajouter**. **f.** Si une liste déroulante est disponible dans la colonne **Paramètre** en regard d'un type d'évènement, vous pouvez choisir l'état des évènements à consigner.
Désactiver l'audit des évènements de sécurité et purger tous les enregistrements	**a.** Dans le champ **Audit des évènements de sécurité**, cliquez sur **Désactivé**.

5. Cliquez sur **Enregistrer**.

À la fin :

- Redémarrez le service BlackBerry UEM Core sur chaque ordinateur hébergeant une instance de BlackBerry UEM.
- Connectez-vous à nouveau à la console de gestion.

Affichage et filtrage des évènements d'audit d'administrateur

La tâche suivante concerne uniquement l'affichage et le filtrage des évènements d'audit d'administrateur. Pour afficher le journal des évènements d'audit de sécurité, consultez Exporter les évènements d'audit de sécurité vers un fichier .csv.

1. Sur la barre de menus, cliquez sur **Audit et journalisation** > **Audit de système**.
2. Cliquez sur **Modifier**.
3. Choisissez une catégorie et une plage de dates. Cliquez sur **Envoyer**.
4. Sous **Filtres**, cliquez sur une catégorie pour la développer.
5. Sélectionnez les filtres que vous souhaitez appliquer et cliquez sur **Envoyer**.
6. Dans le volet de droite, vous pouvez également cliquer sur ⋮. Sélectionnez les colonnes que vous souhaitez afficher.
7. Si nécessaire, effectuez l'une des opérations suivantes :
   - Pour supprimer un filtre, cliquez sur ✕ en regard du filtre que vous souhaitez supprimer.
   - Pour effacer tous les filtres, cliquez sur **Effacer tout.**

À la fin : Si nécessaire, Exportation des évènements d'audit d'administrateur vers un fichier .csv..

Exportation des évènements d'audit d'administrateur vers un fichier .csv.

Lorsque vous exportez des évènements d'audit d'administrateur vers un fichier .csv, ce fichier contient les données que vous filtrez.

1. Sur la barre de menus, cliquez sur **Audit et journalisation** > **Audit de système**.
2. Si nécessaire, dans le volet de gauche, filtrez le journal d'audit pour afficher uniquement les données que vous souhaitez inclure dans le fichier .csv.
3. Cliquez sur et enregistrez le fichier.

Exporter les évènements d'audit de sécurité vers un fichier .csv

Lorsque vous exportez les évènements d'audit de sécurité vers un fichier .csv, ce dernier contient tous les évènements de sécurité enregistrés.

1. Sur la barre de menus, cliquez sur **Paramètres** > **Infrastructure** > **Configuration de l'audit**.
2. Dans la section **Paramètres d'audit des évènements de sécurité**, cliquez sur **Exporter**, puis enregistrez le fichier.

Suppression des enregistrements d'audit

Vous pouvez supprimer les enregistrements d'audit avant l'heure de suppression quotidienne.

1. Sur la barre de menus, cliquez sur **Paramètres** > **Infrastructure** > **Configuration de l'audit**.
2. Dans la section **Paramètres d'audit des évènements d'administrateur** ou **Paramètres d'audit des évènements de sécurité**, cliquez sur **Supprimer**.
3. Cliquez sur **Supprimer**.

Création de notifications d'évènement

Vous pouvez configurer des notifications d'évènement pour alerter les administrateurs par e-mail en cas d'évènements BlackBerry UEM. Voici quelques exemples d'évènements :

- Un compte utilisateur est ajouté
- Un terminal devient non conforme
- Un terminal est désactivé
- Une stratégie informatique est attribuée à un groupe
- Il reste 30 jours avant l'expiration du certificat APNs.

Pour une liste complète des évènements, reportez-vous à la section Types d'évènement.

Chaque notification d'évènement est associée à une liste de distribution par e-mail, un calendrier et un modèle d'e-mail. Vous pouvez créer des listes de distribution qui incluent des adresses électroniques individuelles, des destinataires avec certains rôles d'administrateur ou des destinataires qui appartiennent à certains groupes. Les calendriers définissent les jours de la semaine et les heures de la journée auxquels les notifications sont envoyées. Les modèles d'e-mail définissent le contenu des notifications par e-mail.

Tâches connexes

Créer un modèle d'e-mail de notification d'évènement
Vous pouvez créer des modèles d'e-mail de notification d'évènement à associer à des notifications d'évènement.

Créer une notification d'évènement

Créez une notification d'évènement pour alerter les administrateurs en cas d'évènements dans BlackBerry UEM.

Avant de commencer :

- Si vous ne souhaitez pas utiliser l'e-mail de notification d'évènement par défaut, créez un modèle d'e-mail de notification d'évènement.
- Créer un calendrier pour une notification d'évènement.
- Créer une liste de distribution pour une notification d'évènement.

1. Dans la barre de menus, cliquez sur **Paramètres > Paramètres généraux**.
2. Cliquez sur **Notifications d'évènement**.
3. Sur l'onglet **Notifications d'évènement**, cliquez sur +.
4. Sélectionnez un type d'évènement.
5. Cliquez sur **Suivant**.
6. Dans la liste déroulante **Date/heure d'envoi de la notification par e-mail**, sélectionnez une des options suivantes :
   - **Toujours après un évènement** : les notifications par e-mail sont envoyées dès qu'un évènement se produit.
   - Tout calendrier préconfiguré dans la liste.
   - **Ajouter un nouveau planificateur** : créez un calendrier et cliquez sur **Enregistrer**.
7. Dans le champ **Destinataires**, sélectionnez l'une des options suivantes :
   - **Ajouter une nouvelle liste de distribution** : créez une liste de distribution et cliquez sur **Enregistrer**.
   - Toute liste de distribution préconfigurée.
8. Dans la liste déroulante **Modèle d'e-mail**, sélectionnez le modèle d'e-mail que vous souhaitez utiliser pour la notification d'évènement.
9. Dans la liste déroulante **État**, sélectionnez **Activée** pour activer la notification d'évènement ou **Désactivée** pour désactiver la notification d'évènement.
10. Cliquez sur **Prévisualiser l'e-mail** pour afficher l'e-mail de notification d'évènement et la liste des adresses électroniques des destinataires.
11. Cliquez sur **Enregistrer**.

Créer un calendrier pour une notification d'évènement

Vous pouvez préconfigurer un calendrier à associer à des notifications d'évènement. Les notifications d'évènement sont envoyées uniquement pour des évènements qui se produisent pendant les jours et heures définis dans le calendrier.

1. Dans la barre de menus, cliquez sur **Paramètres > Paramètres généraux**.
2. Cliquez sur **Notifications d'évènement**.
3. Sur l'onglet **Composants de calendrier**, cliquez sur +.
4. Saisissez un nom pour le calendrier.
5. Sélectionnez les jours de la semaine pour l'envoi des notifications. Les notifications sont envoyées uniquement pour des évènements qui se produisent les jours sélectionnés.
6. Sélectionnez l'une des options suivantes :
   - Cochez la case **Journée entière** : les notifications sont envoyées à tout moment.
   - Décochez la case **Journée entière** : sélectionnez les heures d'envoi des notifications chaque jour. Les notifications sont envoyées uniquement pour des évènements qui se produisent aux heures sélectionnées.
7. Cliquez sur **Enregistrer**.

Créer une liste de distribution pour une notification d'évènement

Vous pouvez créer des listes de distribution à associer à des notifications d'évènement. Les listes de distribution peuvent contenir des groupes d'utilisateurs, des rôles d'administrateur et des adresses électroniques individuelles.

1. Dans la barre de menus, cliquez sur **Paramètres > Paramètres généraux**.
2. Cliquez sur **Notifications d'évènement**.
3. Sur l'onglet **Liste de distribution**, cliquez sur +.
4. Saisissez le nom de la liste de distribution.
5. Si vous souhaitez inclure des adresses électroniques individuelles, cliquez sur + dans la section **Destinataires de l'e-mail**, saisissez une adresse électronique et cliquez sur **Enregistrer**.
6. Si vous voulez inclure les administrateurs qui appartiennent à un groupe, sélectionnez un ou plusieurs groupes dans la liste **Groupes d'utilisateurs disponibles** et cliquez sur →.
7. Si vous voulez inclure les administrateurs qui ont un rôle particulier, sélectionnez le ou les rôles concernés dans la liste **Rôles d'utilisateur disponibles** et cliquez sur →.
8. Cliquez sur **Ajouter**.

Désactiver une notification d'évènement

Vous pouvez désactiver une notification d'évènement sans la supprimer.

1. Dans la barre de menus, cliquez sur **Paramètres > Paramètres généraux**.
2. Cliquez sur **Notifications d'évènement**.
3. Dans la colonne **Type de notification**, cliquez sur une notification d'évènement.
4. Dans la liste déroulante **État**, cliquez sur **Désactivé**.
5. Cliquez sur **Enregistrer**.

Types d'évènement

Vous pouvez créer des notifications d'évènement pour les types d'évènement suivants :

Gestion des applications

- Application ajoutée au groupe d'utilisateurs
- Application attribuée à l'utilisateur
- Application supprimée du groupe d'utilisateurs
- Application supprimée de l'utilisateur
- Définition d'application créée
- Définition d'application supprimée
- Définition d'application mise à jour
- Disposition du groupe d'applications mise à jour
- Disposition de l'utilisateur de l'application mise à jour

Signature BDMI

- Échec de la signature BDMI

Conformité

- Violation de conformité
- Restauration de la conformité

Connectivité

- Échec de l'envoi de l'e-mail d'administrateur
- Connexion BlackBerry Infrastructure établie
- Échec de la connexion BlackBerry Infrastructure
- Échec de l’accès à BlackBerry Gatekeeping Service

Terminal

- Terminal supprimé
- Modification du propriétaire du terminal
- Commande envoyée
- Commande émise
- Autoriser BlackBerry Gatekeeping Service
- Échange de carte SIM
- L'état du terminal utilisateur a été modifié

Inscription

- Activation terminée
- Désactivé

Groupe

- Groupe créé
- Groupe supprimé
- Groupe ajouté au groupe d'utilisateurs
- Groupe ajouté à l'utilisateur
- Groupe supprimé du groupe d'utilisateurs
- Utilisateur supprimé du groupe

Stratégies et profils

- Stratégie ou profil créé
- Stratégie ou profil supprimé
- Stratégie ou profil envoyé
- Stratégie ou profil émis
- Stratégie ou profil attribué au groupe
- Stratégie ou profil attribué à l'utilisateur
- Stratégie ou profil désattribué du groupe
- Stratégie ou profil désattribué de l'utilisateur
- Stockage des signatures de stratégies ou de profils
- Validation des signatures de stratégies ou de profils

Performances

- Alerte relative aux performances des terminaux

Utilisateur

- Utilisateur créé
- Utilisateur supprimé

Notification Push Apple

- Expiration de certificat APNs (30 jours avant l'expiration)

Gérer les tâches BlackBerry Dynamics

BlackBerry UEM crée des tâches pour traiter et accomplir des opérations complexes pour les applications BlackBerry Dynamics. BlackBerry UEM gère une file d'attente de tâches et traite celles-ci en fonction de l'ordre dans lequel elles ont été créées. Une instance de BlackBerry UEM doit terminer la tâche en cours avant de traiter la tâche suivante de la file d'attente. Si le domaine comprend plusieurs instances de BlackBerry UEM, toute instance disponible peut démarrer la tâche suivante de la file d'attente.

La console de gestion présente différentes informations sur les tâches en cours ou terminées (par exemple, nom de l'instance qui a traité la tâche, type de tâche, heure de début et de fin, éventuelles erreurs survenues, etc.). Vous pouvez aussi supprimer manuellement les enregistrements de tâche à partir de la console de gestion.

Si vous souhaitez que BlackBerry UEM supprime automatiquement les enregistrements de tâche au bout d'un certain nombre de jours, vous pouvez configurer les propriétés BlackBerry UEM. Pour plus d'informations, consultez le contenu relatif à la configuration.

1. Dans la console de gestion, cliquez sur **Paramètres > BlackBerry Dynamics** à partir de la barre de menus.
2. Cliquez sur **Tâches**.
3. Effectuez l'une des tâches suivantes :

Tâche	Étapes
Affichez les informations relatives à une tâche.	Cliquez sur une tâche.
Supprimez les enregistrements de tâche.	Vous ne pouvez pas récupérer un enregistrement de tâche supprimé. La suppression d'un enregistrement de tâche en cours n'empêche pas la tâche d'aboutir. **a.** Sélectionnez une ou plusieurs tâches. **b.** Cliquez sur 🗑. **c.** Cliquez sur **OK**.

Tâche	Étapes
Supprimez tous les enregistrements de tâche antérieurs au nombre de jours spécifié.	**Remarque :** La tâche suivante supprime tous les enregistrements de tâche antérieurs au nombre de jours spécifié, même s'ils ne sont pas visibles sur l'écran Tâches (par exemple, les tâches de synchronisation Active Directory). **a.** Dans la liste déroulante **Supprimer les tâches après**, cliquez sur le nombre de jours qui convient. **b.** Cliquez sur **Supprimer**.

Utilisation de SNMP pour surveiller BlackBerry UEM

Vous pouvez utiliser des outils SNMP tiers pour surveiller l'activité de BlackBerry UEM.

Pour plus d'informations sur la configuration de SNMP pour surveiller BlackBerry UEM Core,BlackBerry Secure Connect Plus,BlackBerry Secure Gateway et d'autres composants BlackBerry UEM, reportez-vous au contenu relatif à la configuration.

Pour plus d'informations sur certains compteurs SNMP clés pour surveiller les performances et les activités, reportez-vous au contenu HTML.

Utilisation des rapports du tableau de bord

Le tableau de bord utilise des graphiques pour afficher les informations issus des services BlackBerry UEM sur les utilisateurs et les terminaux de votre système. Vous pouvez utiliser le curseur pour pointer un élément spécifique du graphique et afficher des informations sur les utilisateurs ou les terminaux.

Si vous avez besoin de plus d'informations, vous pouvez afficher un rapport à partir du graphique afin d'afficher des informations détaillées sur les utilisateurs ou les terminaux. Un rapport peut contenir un maximum de 2 000 enregistrements. Vous pouvez générer une version .csv d'un rapport et exporter le fichier à des fins d'analyse approfondie ou de génération de rapports.

Pour ouvrir et gérer un compte d'utilisateur, vous pouvez cliquer sur l'utilisateur ou le terminal dans un rapport. Lorsque c'est chose faite, vous pouvez cliquer sur le bouton Précédent de la page (et non du navigateur) pour revenir au rapport.

Le tableau suivant décrit les informations affichées par chaque rapport du tableau de bord.

Rapport du tableau de bord	Description
Terminaux en itinérance et pas en itinérance	Liste des utilisateurs dont les terminaux sont actuellement en itinérance
Activations de terminaux	Représentation dynamique des terminaux activés mensuellement dans votre organisation sur une période de 12 mois, en fonction du moment où les terminaux ont été initialement activés. Ces chiffres évoluent pour refléter les terminaux actuellement activés. Par exemple, si un terminal que vous avez activé en août est désactivé, le nombre de terminaux affichés en août est réduit d'un terminal.

Rapport du tableau de bord	Description
Top 5 des applications gérées installées	Les cinq applications les plus couramment attribuées par votre organisation et installées sur les terminaux
Terminaux par plate-forme	Liste des terminaux de votre organisation, par plate-forme
Conformité du terminal	Liste des problèmes détectés sur les terminaux BlackBerry 10, iOS, Androidet Windows Phone de votre organisation
Terminaux par heure du dernier contact	Nombre de jours passés depuis le dernier contact des terminaux avec le serveur
Terminaux par opérateurs	Liste des terminaux de votre organisation, par fournisseur de service
Top 5 des modèles de terminaux	Les cinq modèles de terminaux mobiles les plus couramment utilisés dans votre organisation

Modifier le type de graphique

Vous pouvez modifier le type de graphique utilisé pour les informations graphiques.

Cliquez sur ⚙ en regard d'un graphique et sélectionnez un type de graphique dans la liste déroulante.

Exporter un rapport du tableau de bord au format .csv

1. Pour ouvrir un rapport, cliquez sur un graphique.
2. Pour trier les enregistrements en fonction de la colonne sélectionnée, cliquez sur un en-tête de colonne.
3. Cliquez sur **Exporter** et enregistrez le fichier.

Affichage de l'activité téléphonique (appels et SMS/MMS) pour les terminaux Android dotés d'un profil professionnel et les terminaux Samsung KNOX Workspace

Vous pouvez consulter l'activité téléphonique (appels et SMS/MMS) des terminaux Android dotés d'un profil professionnel et des terminaux Samsung KNOX Workspace. BlackBerry UEM consigne l'activité téléphonique des terminaux activés avec les types d'activation « Espace Travail uniquement (Premium) », « Travail et Personnel - Contrôle total (Samsung KNOX) » et « Espace Travail uniquement (Samsung KNOX) ». L'activité téléphonique n'est pas consignée si les terminaux sont activés avec des profils autres que ceux mentionnés.

BlackBerry UEM génère des fichiers journaux .csv distincts pour les appels téléphoniques et les SMS/MMS. Par défaut, ces fichiers journaux sont stockés à l'emplacement suivant : `<lecteur>:\Program Files \BlackBerry\UEM\Logs\<date ou nom de dossier>`. BlackBerry UEM nomme les fichiers journaux *<nom_serveur>_<identifiant_composant>_<version_définition_événement>_<aaaammjj>_<numéro_journal>.<extension_fichier>* (par exemple, ServeurBB01_téléphone_1.0_20160730_0001.csv). Pour plus d'informations sur la recherche de fichiers journaux et la lecture de ceux-ci, reportez-vous à Utilisation des fichiers journaux.

Afficher et enregistrer un rapport de terminal

Vous pouvez générer un rapport permettant d'afficher les informations détaillées sur chaque terminal associé à BlackBerry UEM.

1. Sur la barre de menus, cliquez sur **Utilisateurs > Terminaux gérés**.
2. Recherchez un compte d'utilisateur.
3. Dans les résultats de la recherche, cliquez sur le nom du compte d'utilisateur.
4. Sélectionnez l'onglet Terminal.
5. Cliquez sur **Afficher le rapport de terminal**.
6. Cliquez sur **Exporter** pour enregistrer le rapport dans un fichier de l'ordinateur, si nécessaire.

Exporter les rapports de déploiement des applications

Vous pouvez exporter les rapports de déploiement des applications dans un fichier .html à partir de l'écran Applications de la console de gestion. Le rapport comprend des informations sur les applications déployées par BlackBerry UEM et sur les utilisateurs qui les ont installées sur leurs terminaux. Par exemple, vous trouverez des informations sur tous les utilisateurs dotés d'une application spécifique (ID du terminal, modèle, version du système d'exploitation, etc.).

Vous pouvez choisir les applications que vous souhaitez inclure dans votre rapport. Chacune des applications choisies dispose d'une section distincte répertoriant sa version et les informations relatives à chacun des utilisateurs qui en sont dotés.

Remarque : Pour les terminaux iOS utilisant le type d'activation Confidentialité de l'utilisateur, le rapport répertorie tous les terminaux sur lesquels l'application a été installée. BlackBerry UEM ne précise pas si l'application est toujours installée sur le terminal au moment où le rapport est généré.

Pour une analyse plus approfondie, vous pouvez également ouvrir le fichier .html à l'aide de Microsoft Excel.

Exporter un rapport de déploiement d'applications dans un fichier .html

1. Sur la barre de menus, cliquez sur **Applications > Applications**.
2. Cochez la case située en regard de chacune des applications que vous souhaitez inclure au rapport. Pour sélectionner toutes les applications, cochez la case située en haut de la liste des applications.
3. Cliquez sur  et enregistrez le fichier.

Rapports d'activité et de violation de conformité des applications BlackBerry Dynamics

Lorsque BlackBerry UEM et BlackBerry Dynamics sont intégrés, vous pouvez exporter les données d'activité ou de violation de conformité de l'application BlackBerry Dynamics à partir de la console de gestion. Vous pouvez utiliser ces informations pour prendre des mesures vis-à-vis des activités inappropriées ou suspectes. Les rapports d'activité comprennent les données d'activité de chaque application BlackBerry Dynamics (par exemple, version de l'application, date d'activation et dernier contact avec le serveur). Les rapports de violation de conformité comprennent les données de violation de conformité de chaque application (par exemple, règles de stratégie violées et date de la violation).

Exporter un rapport d'application BlackBerry Dynamics au format .csv

Chaque rapport est limité à 5 000 enregistrements.

1. Dans la barre de menus, cliquez sur **Paramètres > BlackBerry Dynamics > Rapports**.
2. Dans la section **Exporter les données au format .csv**, sélectionnez le type de rapport que vous souhaitez exporter :
   - **Activité de l'application BlackBerry Dynamics**
   - **Violations de conformité de l'application BlackBerry Dynamics**
3. Cliquez sur **Exporter** et enregistrez le fichier.

Contrôle des performances de l'application BlackBerry Work

Vous pouvez contrôler les performances de l'application BlackBerry Work et sélectionner les problèmes à signaler.

Activer la surveillance BlackBerry Work

Pour activer la surveillance BlackBerry Work, vous devez configurer la configuration d'application qui lui est attribuée.

1. Sur la barre de menus, cliquez sur **Applications**.
2. Cliquez sur l'application BlackBerry Work que vous souhaitez surveiller.
3. Sur l'onglet BlackBerry Dynamics, dans le tableau de configuration d'application, cliquez sur le nom de la configuration d'application que vous souhaitez modifier.
4. Sur l'onglet **Rapport de performances**, configurez l'un des éléments suivants :
   - **Activer le rapport de performances** : indiquez si vous voulez surveiller les performances de l'application BlackBerry Work.
   - **Erreur de connexion HTTP** : indiquez si les erreurs de connexion HTTP entre BlackBerry Work et les serveurs d'application spécifiés doivent être signalées.
   - **Temps de réponse HTTP** : indiquez si les réponses HTTP qui prennent plus de temps que le temps indiqué doivent être signalées. Saisissez les adresses de serveur d'applications à surveiller.
   - **Code d'état HTTP** : indiquez si un code d'état HTTP spécifié doit être signalé. Saisissez les adresses de serveur d'applications à surveiller.
   - **Ne pas envoyer de rapports pendant une durée définie (en secondes)** : indiquez le temps d'attente avant l'envoi d'un autre rapport.
5. Cliquez sur **Enregistrer**.

Afficher les notifications d'alerte relative aux performances des terminaux

Avant de commencer :

- Activer la surveillance BlackBerry Work

1. Sur la barre de menus, cliquez sur **Audit et journalisation** > **Performances des terminaux**.
2. Choisissez une catégorie et une plage de dates. Cliquez sur **Submit**.
3. Sous **Filtres**, cliquez sur une catégorie pour la développer.
4. Sélectionnez les filtres que vous souhaitez appliquer et cliquez sur **Envoyer**.
5. Si nécessaire, effectuez l'une des opérations suivantes :

- Pour supprimer un filtre, cliquez sur ✕ en regard du filtre que vous souhaitez supprimer.
- Pour effacer tous les filtres, cliquez sur **Effacer tout.**

6. Pour exporter les résultats dans un fichier .csv, cliquez sur ➔.

Afficher une alerte de performances pour un seul terminal

Au lieu d'afficher une liste d'alertes de performances basée sur la date et le type d'alerte, vous pouvez également afficher toutes les alertes de performances pour un seul terminal au cours des 24 dernières heures. Si des alertes de performances ont été émises pour un terminal, une icône d'avertissement s'affiche sur l'onglet du terminal et un message vous indique le nombre d'alertes détectées sur le terminal.

Avant de commencer :

- Activer la surveillance BlackBerry Work

1. Sur la barre de menus, cliquez sur **Utilisateurs > Terminaux gérés**.
2. Recherchez un compte d'utilisateur.
3. Dans les résultats de la recherche, cliquez sur le nom du compte d'utilisateur.
4. Sélectionnez l'onglet du terminal dont vous souhaitez afficher les alertes. Un terminal avec des alertes de performances ou des violations de conformité est signalé par une icône d'avertissement.
5. Si des alertes de performances ont été émises pour un terminal, cliquez sur **Afficher tout** en regard du message d'alerte de performances pour afficher la liste des alertes de performances concernant ce terminal.

Paramètres de profil

Cette section fournit des descriptions détaillées des options dans les profils qui disposent d'un grand nombre de paramètres pour vous aider à configurer l'e-mail, les connexions réseau et d'autres fonctionnalités.

Pour les profils avec seulement quelques paramètres, reportez-vous au sujet sur la création du profil pour définir des descriptions.

Paramètres de profil de messagerie

Vous pouvez utiliser une variable de paramètre de profil correspondant à un champ de texte pour faire référence à une valeur plutôt que de spécifier la valeur réelle. BlackBerry UEM prend en charge les variables par défaut prédéfinies et les variables personnalisées que vous définissez. Les profils de messagerie sont pris en charge sur les types de terminaux suivants :

- BlackBerry 10
- iOS
- macOS
- Android
- Windows

Dans certains cas, la version minimale du système d'exploitation du terminal requis pour prendre en charge un paramètre correspondant à une version non prise en charge par BlackBerry UEM. Pour en savoir plus sur les versions prises en charge, consultez la Matrice de compatibilité.

Communs : paramètres de profil de messagerie

Commun : paramètre de profil de messagerie	Description
Nom de domaine	Ce paramètre spécifie le nom de domaine du serveur de messagerie.
Adresse électronique	Ce paramètre spécifie l'adresse électronique de l'utilisateur. Si le profil concerne plusieurs utilisateurs, vous pouvez utiliser la variable %UserEmailAddress%.
Nom d'hôte ou adresse IP	Ce paramètre spécifie le nom d'hôte ou l'adresse IP du serveur de messagerie.
Nom d'utilisateur	Ce paramètre spécifie le nom d'utilisateur de l'utilisateur. Si le profil concerne plusieurs utilisateurs, vous pouvez utiliser la variable %UserName%.
Serveurs de contrôle d'accès automatique	Si vous avez configuré des groupes de serveurs pour diriger le trafic BlackBerry Secure Gateway ou BlackBerry Gatekeeping Service vers une connexion régionale spécifique à BlackBerry Infrastructure, ce paramètre spécifie le groupe de serveurs approprié. Pour plus d'informations sur les groupes BlackBerry Connectivity Node et les groupes de serveurs, reportez-vous au contenu relatif à la planification et au contenu relatif à l'installation et à la mise à niveau.

BlackBerry 10 : paramètres de profil de messagerie

BlackBerry 10 : paramètre de profil de messagerie	Description
Nom du compte	Ce paramètre spécifie le nom du compte de messagerie professionnel qui apparait dans BlackBerry Hub et dans les paramètres du terminal. Vous pouvez utiliser une variable telle que %UserEmailAddress%.
Port	Ce paramètre spécifie le port utilisé pour se connecter au serveur de messagerie.
Paramètres de remise	
Type de profil	Ce paramètre spécifie si vous souhaitez que ce profil prenne en charge Exchange ActiveSync ou IBM Notes Traveler. Valeurs possibles : • Exchange ActiveSync • IBM Notes Traveler La valeur par défaut est Exchange ActiveSync.
Serveur SyncML	Ce paramètre indique le FQDN du serveur IBM Notes Traveler qu'un terminal BlackBerry 10 peut utiliser pour synchroniser les données To Do. Ce paramètre est valide uniquement si le paramètre Type de profil est défini sur « IBM Notes Traveler ».
Port SyncML	Ce paramètre indique le port du serveur Notes Traveler qu'un terminal BlackBerry 10 peut utiliser pour synchroniser les données To Do. Ce paramètre est valide uniquement si le paramètre Type de profil est défini sur « IBM Notes Traveler ».
Utiliser SSL pour SyncML	Ce paramètre indique si un terminal BlackBerry 10 doit se connecter au serveur Notes Traveler. Ce paramètre est valide uniquement si le paramètre Type de profil est défini sur « IBM Notes Traveler ».
Push activé	Ce paramètre indique si le serveur de messagerie peut transférer les e-mails au terminal BlackBerry 10.

BlackBerry 10 : paramètre de profil de messagerie	Description
Intervalle entre les synchronisations	Ce paramètre indique la fréquence à laquelle un terminal BlackBerry 10 vérifie la présence de nouveaux e-mails sur le serveur de messagerie. Ce paramètre est valide uniquement si le paramètre Push activé n'est pas sélectionné. Valeurs possibles : • Manuel • 5 minutes • 15 minutes • 30 minutes • 1 heure • 2 heures • 4 heures • 24 heures La valeur par défaut est 15 minutes.
Jours de synchronisation	Ce paramètre spécifie le nombre de jours passés afin de synchroniser les e-mails et données de l'organiseur avec un terminal BlackBerry 10. Valeurs possibles : • 1 jour • 3 jours • 7 jours • 14 jours • 1 mois • Toujours La valeur par défaut est de 1 mois.
Synchronisation manuelle requise lors de l'itinérance	Ce paramètre indique si un utilisateur doit lancer la synchronisation entre un terminal BlackBerry 10 et le serveur de messagerie en cas d'itinérance de l'utilisateur.
Utiliser SSL	Ce paramètre spécifie si un terminal doit utiliser SSL pour se connecter au serveur de messagerie.
Synchronisation du calendrier	Ce paramètre spécifie si un terminal BlackBerry 10 synchronise les entrées de calendrier avec le serveur de messagerie.
Synchronisation des contacts	Ce paramètre spécifie si un terminal BlackBerry 10 synchronise les contacts avec le serveur de messagerie.
Synchronisation des e-mails	Ce paramètre spécifie si un terminal BlackBerry 10 synchronise les e-mails avec le serveur de messagerie.

BlackBerry 10 : paramètre de profil de messagerie	Description
Synchronisation des mémos	Ce paramètre spécifie si un terminal BlackBerry 10 synchronise les données des mémos avec le serveur de messagerie. Ce paramètre est valide uniquement si le paramètre Type de profil est défini sur « Exchange ActiveSync ».
Synchronisation des tâches	Ce paramètre spécifie si un terminal BlackBerry 10 synchronise les données des tâches avec le serveur de messagerie. Ce paramètre est valide uniquement si le paramètre Type de profil est défini sur « Exchange ActiveSync ».
Synchronisation ToDo	Ce paramètre spécifie si un terminal BlackBerry 10 synchronise les données To Do avec Notes Traveler. Ce paramètre est valide uniquement si le paramètre Type de profil est défini sur « IBM Notes Traveler ».
Paramètres de messagerie sécurisée	
Suggérer un codage par défaut pour les messages sortants	Ce paramètre spécifie si un terminal BlackBerry 10 suggère le codage par défaut, (par exemple, texte brut, signer, crypter ou signer et crypter) pour tous les e-mails sortants. Si ce paramètre est défini sur Autoriser, un utilisateur peut choisir si le terminal suggère le codage par défaut ou le codage en fonction de l'historique des messages. Si ce paramètre est défini sur Requis, le terminal suggère le codage par défaut. Si ce paramètre est défini sur Interdire, le terminal suggère le codage en fonction de l'historique des messages. Valeurs possibles : • Autoriser • Requise • Interdire La valeur par défaut est Autoriser. La configuration minimale requise est BlackBerry 10 OS version 10.3.1.
Paramètres S/MIME	

BlackBerry 10 : paramètre de profil de messagerie	Description
Prise en charge S/MIME	Ce paramètre spécifie si S/MIME est activé sur un terminal BlackBerry 10. Si ce paramètre est défini sur Autoriser, un utilisateur peut choisir d'activer ou non la protection S/MIME sur le terminal. Si ce paramètre est défini sur Requis, la protection S/MIME est activée sur le terminal et l'utilisateur ne peut pas la désactiver. Si ce paramètre est défini sur Interdire, la protection S/MIME est désactivée sur le terminal et l'utilisateur ne peut pas l'activer. Pour envoyer des e-mails cryptés, l'utilisateur doit disposer de la clé publique du destinataire sur le terminal ou la carte à puce. Pour envoyer des e-mails avec signature numérique, la clé privée de l'utilisateur doit se trouver sur le terminal ou la carte à puce. Ce paramètre est prioritaire sur les paramètres Messages S/MIME avec signature numérique et Messages S/MIME cryptés. Ce paramètre affecte le paramètre Prise en charge PGP. Si ce paramètre est défini sur Requis, le paramètre Prise en charge PGP doit être défini sur Interdire. Valeurs possibles : • Autoriser • Requise • Interdire La valeur par défaut est Autoriser.
Messages S/MIME avec signature numérique	Ce paramètre spécifie si un terminal BlackBerry 10 envoie des e-mails sortants avec une signature numérique. Si ce paramètre est défini sur Autoriser, l'utilisateur peut choisir de signer numériquement les e-mails sortants. Si ce paramètre est défini sur Requis, l'utilisateur doit signer numériquement les e-mails sortants. Si ce paramètre est défini sur Interdire, l'utilisateur ne peut pas signer numériquement les e-mails sortants. Pour envoyer des e-mails avec signature numérique, la clé privée de l'utilisateur doit se trouver sur le terminal ou la carte à puce. Ce paramètre est valide uniquement si le paramètre Prise en charge S/MIME est défini Autoriser ou Requis. Si le paramètre Prise en charge S/MIME est défini sur Requis et que ce paramètre et le paramètre Messages S/MIME cryptés sont définis sur Interdire, le paramètre Messages S/MIME cryptés et ce paramètre sont ignorés et le paramètre Autoriser est utilisé. Valeurs possibles : • Autoriser • Requise • Interdire La valeur par défaut est Autoriser.

BlackBerry 10 : paramètre de profil de messagerie	Description
Messages S/MIME cryptés	Ce paramètre spécifie si un terminal BlackBerry 10 crypte les e-mails sortants à l'aide du cryptage S/MIME. Si ce paramètre est défini sur Autoriser, l'utilisateur peut choisir de crypter les e-mails sortants. Si ce paramètre est défini sur Requis, l'utilisateur doit crypter les e-mails sortants. Si ce paramètre est défini sur Interdire, l'utilisateur ne peut pas crypter les e-mails sortants. Pour envoyer des e-mails cryptés, l'utilisateur doit disposer de la clé publique du destinataire sur le terminal ou la carte à puce. Ce paramètre est valide uniquement si le paramètre Prise en charge S/MIME est défini Autoriser ou Requis. Si le paramètre Prise en charge S/MIME est défini sur Requis et que ce paramètre et le paramètre Messages S/MIME avec signature numérique sont définis sur Interdire, le paramètre Messages S/MIME avec signature numérique et ce paramètre sont ignorés et le paramètre par défaut Autoriser est utilisé pour les deux paramètres. Valeurs possibles : • Autoriser • Requise • Interdire La valeur par défaut est Autoriser.
Algorithmes de cryptage	Ce paramètre spécifie les algorithmes de cryptage qu'un terminal BlackBerry 10 peut utiliser pour crypter des e-mails protégés par S/MIME. Valeurs possibles : • AES (256 bits) • AES (192 bits) • AES (128 bits) • Triple DES • RC2 La valeur par défaut est une valeur nulle.
Paramètres PGP	

BlackBerry 10 : paramètre de profil de messagerie	Description
Prise en charge PGP	Ce paramètre spécifie si la protection PGP est activée sur un terminal BlackBerry 10. Si ce paramètre est défini sur Autoriser, un utilisateur peut choisir d'activer ou non la protection PGP sur le terminal. Si ce paramètre est défini sur Requis, la protection PGP est activée sur le terminal et l'utilisateur ne peut pas la désactiver. Si ce paramètre est défini sur Interdire, la protection PGP est désactivée sur le terminal et l'utilisateur ne peut pas l'activer. Pour envoyer des e-mails cryptés, l'utilisateur doit disposer de la clé publique du destinataire sur le terminal. Pour envoyer des e-mails avec signature numérique, la clé privée de l'utilisateur doit se trouver sur le terminal. Le paramètre Prise en charge S/MIME affecte ce paramètre. Si le paramètre Prise en charge S/MIME est défini sur Requis ou si le paramètre Prise en charge S/MIME est défini sur Autoriser et le paramètre Messages S/MIME avec signature numérique ou Messages cryptés S/MIME sont définis sur Requis, ce paramètre doit être défini sur Interdire. Valeurs possibles : • Autoriser • Requise • Interdire La valeur par défaut est Autoriser. La configuration minimale requise est BlackBerry 10 OS version 10.3.1.
Adresse Symantec Encryption Management Server	Ce paramètre spécifie le FQDN ou l'adresse IP du serveur Symantec Encryption Management Server de votre entreprise pour demander à un utilisateur de terminal BlackBerry 10 d'inscrire le terminal sur ce serveur afin d'envoyer des PGP. Le paramètre Prise en charge PGP affecte ce paramètre. Le terminal utilise ce paramètre si le paramètre PGP est défini sur Autoriser ou Requis. La configuration minimale requise est BlackBerry 10 OS version 10.3.1.
Méthode d'inscription Symantec Encryption Management Server	Ce paramètre spécifie la méthode qu'un utilisateur de terminal BlackBerry 10 doit utiliser pour inscrire le terminal sur Symantec Encryption Management Server. Si ce paramètre est défini sur Authentification par e-mail, le terminal invite l'utilisateur à saisir son adresse électronique. Si ce paramètre est défini sur Authentification Microsoft Active Directory, le terminal invite l'utilisateur à saisir son nom d'utilisateur de domaine et son mot de passe. Le paramètre Prise en charge PGP affecte ce paramètre. Le terminal utilise ce paramètre si le paramètre PGP est défini sur Autoriser ou Requis. Valeurs possibles : • Authentification par e-mail • Authentification Microsoft Active Directory La valeur par défaut est Authentification par e-mail. La configuration minimale requise est BlackBerry 10 OS version 10.3.1.

BlackBerry 10 : paramètre de profil de messagerie	Description
Profils associés	
Type d'authentification	Ce paramètre spécifie le type d'authentification utilisé par un terminal BlackBerry 10 pour se connecter au serveur de messagerie. Valeurs possibles : • Aucune • SCEP • Informations d'identification de l'utilisateur La valeur par défaut est Aucune.
Profil SCEP associé	Ce paramètre spécifie le profil SCEP associé utilisé par un BlackBerry 10 terminal pour obtenir un certificat client et s'authentifier auprès du serveur de messagerie. Ce paramètre est valide uniquement si le paramètre Type d'authentification est défini sur SCEP.
Profil des informations d'identification de l'utilisateur associé	Ce paramètre spécifie le profil des informations d'identification de l'utilisateur associé utilisé par un BlackBerry 10 terminal pour obtenir un certificat client et s'authentifier auprès du serveur de messagerie. Ce paramètre est valide uniquement si le paramètre Type d'authentification est défini sur Informations d'identification de l'utilisateur. La configuration minimale requise est BlackBerry 10 OS version 10.3.1.
Classification de messages	
Fichier de classification de messages (.json)	Ce paramètre spécifie le fichier de classification de messages à envoyer aux terminaux des utilisateurs. La configuration minimale requise est BlackBerry 10 OS version 10.3.1.

Concepts connexes

Application des e-mails sécurisés à l'aide de la classification de messages

Profil S/MIME et dépendances entre les paramètres des terminaux

Le tableau suivant présente les dépendances entre les paramètres S/MIME que vous pouvez configurer dans BlackBerry UEM et les paramètres S/MIME que les utilisateurs peuvent configurer sur les terminaux BlackBerry 10. Selon leur définition, les options de la liste déroulante Codage des terminaux changent. Les terminaux ignorent la valeur de certains paramètres si un paramètre de priorité plus élevée (paramètre Prise en charge S/MIME, par exemple) est en conflit avec la valeur de ce paramètre.

Paramètre Prise en charge S/MIME	Paramètre Messages S/MIME avec signature numérique	Paramètre Messages S/MIME cryptés	Paramètres S/MIME sur le terminal	Liste déroulante Codage du terminal
Autorisé	Autorisé	Autorisé	L'utilisateur peut activer ou désactiver la protection S/MIME.	• Texte brut • Signer (S/MIME) • Crypter (S/MIME) • Signer et crypter (S/MIME)
	Autorisé	Requise	La protection S/MIME est activée. L'utilisateur ne peut pas la désactiver.	• Crypter (S/MIME) • Signer et crypter (S/MIME)
	Autorisé	Non autorisé	L'utilisateur peut activer ou désactiver la protection S/MIME.	• Texte brut • Signer (S/MIME)
	Requise	Autorisé	La protection S/MIME est activée. L'utilisateur ne peut pas la désactiver.	• Signer (S/MIME) • Signer et crypter (S/MIME)
	Requise	Requise	La protection S/MIME est activée. L'utilisateur ne peut pas la désactiver.	Signer et crypter (S/MIME)
	Requise	Non autorisé	La protection S/MIME est activée. L'utilisateur ne peut pas la désactiver.	Signer (S/MIME)
	Non autorisé	Autorisé	L'utilisateur peut activer ou désactiver la protection S/MIME.	• Texte brut • Crypter (S/MIME)
	Non autorisé	Requise	La protection S/MIME est activée. L'utilisateur ne peut pas la désactiver.	Crypter (S/MIME)
	Non autorisé	Non autorisé	L'utilisateur peut activer ou désactiver la protection S/MIME, mais ne peut pas crypter ou signer les messages, car les profils nécessaires sont définis sur Non autorisé.	Texte brut

Paramètre Prise en charge S/MIME	Paramètre Messages S/MIME avec signature numérique	Paramètre Messages S/MIME cryptés	Paramètres S/MIME sur le terminal	Liste déroulante Codage du terminal
Requise	Autorisé	Autorisé	La protection S/MIME est activée. L'utilisateur ne peut pas la désactiver.	• Signer (S/MIME) • Crypter (S/MIME) • Signer et crypter (S/MIME)
	Autorisé	Requise	La protection S/MIME est activée. L'utilisateur ne peut pas la désactiver.	• Crypter (S/MIME) • Signer et crypter (S/MIME)
	Autorisé	Non autorisé	La protection S/MIME est activée. L'utilisateur ne peut pas la désactiver.	Signer (S/MIME)
	Requise	Autorisé	La protection S/MIME est activée. L'utilisateur ne peut pas la désactiver.	• Signer (S/MIME) • Signer et crypter (S/MIME)
	Requise	Requise	La protection S/MIME est activée. L'utilisateur ne peut pas la désactiver.	Signer et crypter (S/MIME)
	Requise	Non autorisé	La protection S/MIME est activée. L'utilisateur ne peut pas la désactiver.	Signer (S/MIME)
	Non autorisé	Autorisé	La protection S/MIME est activée. L'utilisateur ne peut pas la désactiver.	Crypter (S/MIME)
	Non autorisé	Requise	La protection S/MIME est activée. L'utilisateur ne peut pas la désactiver.	Crypter (S/MIME)
	Non autorisé (Ce paramètre est ignoré)	Non autorisé (Ce paramètre est ignoré)	La protection S/MIME est activée. L'utilisateur ne peut pas la désactiver.	• Signer (S/MIME) • Crypter (S/MIME) • Signer et crypter (S/MIME)
Non autorisé	Tous les paramètres sont ignorés	Tous les paramètres sont ignorés	La protection S/MIME est désactivée. L'utilisateur ne peut pas l'activer.	Texte brut

Profil PGP et dépendances entre les paramètres des terminaux

Le tableau suivant présente les dépendances entre le paramètre Prise en charge PGP que vous pouvez configurer dans PGP et les paramètres BlackBerry UEM que les utilisateurs peuvent configurer sur les terminaux BlackBerry 10. Selon la définition du paramètre Prise en charge PGP, les options de la liste déroulante Codage des terminaux changent. Les terminaux ignorent la valeur de ce paramètre si un paramètre de priorité plus élevée (paramètre Prise en charge S/MIME, par exemple) est en conflit avec la valeur de ce paramètre.

Paramètre Prise en charge PGP	Paramètres PGP du terminal	Liste déroulante Codage du terminal
Autoriser	Les utilisateurs peuvent activer ou désactiver la protection PGP.	• Texte brut • Signer (PGP) • Crypter (PGP) • Signer et crypter (PGP)
Requise	La protection PGP est activée. L'utilisateur ne peut pas la désactiver.	• Signer (PGP) • Crypter (PGP) • Signer et crypter (PGP)
Interdire	La protection PGP est désactivée. L'utilisateur ne peut pas l'activer.	Aucune liste déroulante. Le texte brut est utilisé.

iOS : paramètres de profil de messagerie

iOS : paramètre de profil de messagerie	Description
Paramètres de remise	
Autoriser le déplacement de messages	Ce paramètre spécifie si les utilisateurs peuvent déplacer les e-mails de ce compte vers un autre compte de messagerie présent sur un terminal iOS.
Autoriser la synchronisation des adresses récentes	Ce paramètre spécifie si un utilisateur de terminal iOS peut synchroniser les adresses récemment utilisées sur les terminaux.
Utiliser uniquement dans la messagerie	Ce paramètre spécifie si les applications autres que l'application de messagerie d'un terminal iOS peuvent utiliser ce compte pour envoyer des e-mails.
Activer S/MIME	Ce paramètre spécifie si un utilisateur de terminal iOS peut envoyer des e-mails protégés par S/MIME.
Activer messages S/MIME signés numériquement	Ce paramètre spécifie si un terminal envoie des messages sortants avec une signature numérique. Ce paramètre s'applique uniquement aux terminaux iOS 10.3 et versions ultérieures.

iOS : paramètre de profil de messagerie	Description
Informations d'identification de signature	Ce paramètre spécifie la manière dont les terminaux trouvent les certificats requis pour signer les messages. Ce paramètre est valide uniquement si le paramètre Activer S/MIME est sélectionné. Valeurs possibles : • Certificat partagé • SCEP • Informations d'identification de l'utilisateur Après avoir choisi le type de profil que vous souhaitez utiliser, spécifiez le profil de certificat partagé, profil SCEP ou profil des informations d'identification de l'utilisateur.
Certificat partagé de signature	Ce paramètre spécifie le profil de certificat partagé pour un certificat client utilisé par un terminal iOS afin de signer des e-mails. Ce paramètre est valide uniquement si le paramètre Activer S/MIME est sélectionné.
SCEP de signature	Ce paramètre spécifie le profil SCEP utilisé par les terminaux pour récupérer les certificats requis pour signer les e-mails à l'aide de S/MIME. Ce paramètre est valide uniquement si le paramètre Activer S/MIME est sélectionné.
Informations d'identification de connexion de l'utilisateur	Ce paramètre spécifie le profil des informations d'identification de l'utilisateur utilisé par les terminaux pour obtenir les certificats client requis pour signer les e-mails à l'aide de S/MIME. Ce paramètre est valide uniquement si le paramètre Activer S/MIME est sélectionné.
Activer le cryptage des messages S/MIME	Ce paramètre spécifie si un terminal crypte les e-mails sortants à l'aide du cryptage S/MIME. Ce paramètre s'applique uniquement aux terminaux iOS 10.3 et versions ultérieures.

iOS : paramètre de profil de messagerie	Description
Informations d'identification de cryptage	Ce paramètre spécifie la manière dont les terminaux trouvent les certificats requis pour crypter les messages. Valeurs possibles : • Certificat partagé • SCEP • Informations d'identification de l'utilisateur Après avoir sélectionné le type de profil, sélectionnez le profil de certificat partagé, profil SCEP ou profil des informations d'identification de l'utilisateur que vous souhaitez utiliser. Ce paramètre est valide uniquement si le paramètre Activer S/MIME est sélectionné.
Certificat partagé de cryptage	Ce paramètre spécifie le profil de certificat partagé pour un certificat client utilisé par un terminal iOS afin de crypter des e-mails. Les terminaux choisissent le certificat adapté au destinataire pour crypter les messages à l'aide de S/MIME. Ce paramètre est valide uniquement si le paramètre Activer S/MIME est sélectionné.
SCEP de cryptage	Ce paramètre spécifie le profil SCEP utilisé par les terminaux pour récupérer les certificats requis et crypter les e-mails à l'aide de S/MIME. Ce paramètre s'applique uniquement si le paramètre Activer S/MIME est sélectionné.
Informations d'identification de l'utilisateur de cryptage	Ce paramètre spécifie le profil des informations d'identification de l'utilisateur utilisé par les terminaux pour récupérer les certificats client requis et crypter les e-mails à l'aide de S/MIME. Ce paramètre s'applique uniquement si le paramètre Activer S/MIME est sélectionné.
Crypter les messages	Ce paramètre spécifie si tous les e-mails doivent être cryptés lorsque l'utilisateur les envoie (Obligatoire) ou si l'utilisateur peut choisir les messages à crypter au moment où il les envoie (Autoriser). Ce paramètre s'applique uniquement si le paramètre Activer S/MIME est sélectionné. Valeurs possibles : • Obligatoire • Autoriser La valeur par défaut est Requis. L'exigence minimale est iOS version 8.0 et les terminaux doivent être activés avec les commandes MDM.

iOS : paramètre de profil de messagerie	Description
Jours de synchronisation	Ce paramètre spécifie le nombre de jours passés afin de synchroniser les e-mails et données de l'organiseur avec un terminal iOS. Valeurs possibles : • 1 jour • 3 jours • 7 jours • 14 jours • 1 mois • Toujours La valeur par défaut est 7 jours. **Remarque :** Ce paramètre s'applique uniquement aux applications de messagerie et de l'organiseur par défaut des terminaux iOS avec le type d'activation Contrôles MDM.
Authentification	
Activer BlackBerry Secure Gateway	Ce paramètre spécifie si les terminaux iOS utilisant le type d'activation Contrôles MDM utilisent BlackBerry Secure Gateway pour se connecter au serveur de messagerie.BlackBerry Secure Gateway fournit une connexion sécurisée par le biais de et au serveur de messagerie de votre entreprise via BlackBerry Infrastructure et BlackBerry UEM. Avant d'activer ce service, vérifiez que votre entreprise dispose des licences BlackBerry UEM adéquates. Pour plus d'informations, reportez-vous au contenu relatif aux licences. Si vous avez configuré des groupes de serveurs de manière à rediriger le trafic BlackBerry Secure Gateway vers une connexion locale spécifique à BlackBerry Infrastructure, vous devez associer le profil de messagerie au groupe de serveurs approprié.
Type d'authentification	Ce paramètre spécifie le type d'authentification utilisé par un terminal iOS pour se connecter au serveur de messagerie. Ce paramètre est valide uniquement si le paramètre Activer BlackBerry Secure Gateway n'est pas sélectionné. Valeurs possibles : • Aucune • Certificat partagé • SCEP • Informations d'identification de l'utilisateur La valeur par défaut est Aucune.
Profil de certificat partagé	Ce paramètre spécifie le profil de certificat partagé du certificat client utilisé par un terminal iOS pour se connecter au serveur de messagerie. Ce paramètre est valide uniquement si le paramètre Type d'authentification ou le paramètre Méthode d'authentification est défini sur Certificat partagé.

iOS : paramètre de profil de messagerie	Description
Profil SCEP associé	Ce paramètre spécifie le profil SCEP associé utilisé par un iOS terminal pour inscrire un certificat client et s'authentifier auprès du serveur de messagerie. Ce paramètre est valide uniquement si le paramètre Activer BlackBerry Secure Gateway n'est pas sélectionné et si le paramètre Type d'authentification est défini sur SCEP.
Profil des informations d'identification de l'utilisateur associé	Ce paramètre spécifie le profil des informations d'identification de l'utilisateur associé utilisé par un terminal iOS pour obtenir un certificat client et s'authentifier auprès du serveur de messagerie. Ce paramètre est valide uniquement si le paramètre Activer BlackBerry Secure Gateway n'est pas sélectionné et si le paramètre Type d'authentification est défini sur Informations d'identification de l'utilisateur.
Utiliser des informations d'identification et un certificat	Ce paramètre spécifie si un terminal utilise des informations d'identification et un certificat client obtenus à l'aide du profil SCEP associé pour s'authentifier auprès du serveur de messagerie. Ce paramètre est valide uniquement si le paramètre Activer BlackBerry Secure Gateway n'est pas sélectionné et si le paramètre Type d'authentification est défini sur SCEP.
Utiliser SSL	Ce paramètre spécifie si un terminal doit utiliser SSL pour se connecter au serveur de messagerie.
Accepter tous les certificats SSL	Ce paramètre indique si tous les certificats SSL sont acceptés.
Domaines de messagerie externes	
Liste autorisée des domaines de messagerie externes	Ce paramètre spécifie la liste de domaines vers lesquels un utilisateur peut envoyer des e-mails professionnels et des entrées de calendriers. Par exemple, lorsqu'un utilisateur ajoute un destinataire disposant d'une adresse électronique dans le domaine autorisé à un e-mail ou une entrée de calendrier, aucun message d'avertissement ne s'affiche. Ce paramètre s'applique à l'espace Travail uniquement. Si vous souhaitez indiquer plusieurs noms de domaine, séparez-les par une virgule (,), un point-virgule (;) ou un espace.
Liste restreinte des domaines de messagerie externes	Ce paramètre spécifie la liste de domaines vers lesquels les utilisateurs peuvent envoyer des e-mails professionnels et des entrées de calendriers. Par exemple, si un utilisateur tente d'ajouter un destinataire disposant d'une adresse électronique correspondant au domaine limité à un e-mail ou une invitation de calendrier, l'application Work Connect ne permet pas à l'utilisateur de mener à bien cette opération. Ce paramètre s'applique à l'espace Travail uniquement. Si vous souhaitez indiquer plusieurs noms de domaine, séparez-les par une virgule (,), un point-virgule (;) ou un espace.

iOS : paramètre de profil de messagerie	Description
Autoriser Mail Drop	Ce paramètre spécifie si les utilisateurs peuvent envoyer des fichiers à partir de ce compte avec Mail Drop. L'exigence minimale est iOS version 9.0 et les terminaux doivent être activés avec les commandes MDM.

macOS : paramètres de profil de messagerie

macOS applique les profils aux terminaux ou comptes d'utilisateur. Les profils de messagerie électronique sont appliqués aux comptes d'utilisateur.

macOS : paramètre de profil de messagerie	Description
Chemin d'accès	Ce paramètre spécifie le chemin de réseau du serveur de messagerie.
Port	Ce paramètre spécifie le port utilisé pour se connecter au serveur de messagerie.
Utiliser SSL	Ce paramètre spécifie si un terminal doit utiliser SSL pour se connecter au serveur de messagerie.
Nom d'hôte ou adresse IP externe	Ce paramètre spécifie le nom d'hôte ou l'adresse IP externe du serveur de messagerie.
Utiliser un protocole SSL externe	Ce paramètre spécifie si un terminal doit utiliser SSL pour se connecter au serveur de messagerie externe.
Chemin d'accès externe	Ce paramètre spécifie le chemin de réseau du serveur de messagerie externe.
Port du serveur externe	Ce paramètre spécifie le port utilisé pour se connecter au serveur de messagerie externe.

Android : paramètres de profil de messagerie

Remarque : dans une prochaine version de BlackBerry UEM, les paramètres applicables à BlackBerry Hub + et Divide Productivity seront supprimés du profil de messagerie et seront uniquement disponibles au niveau de la configuration de l'application (paramètres de l'application). Dans la version actuelle, si vous configurez les paramètres de l'application à la fois ici et au niveau de la configuration de l'application, les paramètres définis au niveau de la configuration de l'application sont prioritaires.

Android : paramètre de profil de messagerie	Description
Paramètres de remise	

Android : paramètre de profil de messagerie	Description
Type de profil	Ce paramètre spécifie si vous souhaitez que ce profil prenne en charge Exchange ActiveSync ou IBM Notes Traveler. Valeurs possibles : • Exchange ActiveSync • IBM Notes Traveler La valeur par défaut est Exchange ActiveSync.
Jours de synchronisation	Ce paramètre spécifie le nombre de jours passés afin de synchroniser les e-mails et données de l'organiseur avec un terminal Android. Valeurs possibles : • Illimité • 1 jour • 3 jours • 7 jours • 14 jours • 1 mois La valeur par défaut est de 1 mois. Pour les terminaux Android utilisant Samsung KNOX MDM, si vous définissez la valeur sur Illimité, un seul mois est synchronisé. **Remarque :** Ce paramètre s'applique uniquement aux applications de messagerie et de l'organiseur par défaut des terminaux Android avec le type d'activation Contrôles MDM. Si le type d'activation Travail et Personnel - Confidentialité de l'utilisateur ou Travail et Personnel - Contrôle total est attribué au terminal, ce paramètre n'affecte pas les paramètres de synchronisation des applications de messagerie et de l'organiseur par défaut ou de l'application Work Space Manager.
Type d'authentification	Ce paramètre spécifie le type d'authentification utilisé par un terminal Android pour se connecter au serveur de messagerie. Valeurs possibles : • Aucune • Certificat partagé • SCEP • Informations d'identification de l'utilisateur La valeur par défaut est Aucune.
Profil SCEP associé	Ce paramètre spécifie le profil SCEP associé utilisé par un terminal Android pour obtenir un certificat client et s'authentifier auprès du serveur de messagerie. Ce paramètre est valide uniquement si le paramètre Type d'authentification est défini sur SCEP.

Android : paramètre de profil de messagerie	Description
Utiliser des informations d'identification et un certificat	Ce paramètre spécifie si un terminal utilise des informations d'identification et un certificat client obtenus à l'aide du profil SCEP associé pour s'authentifier auprès du serveur de messagerie. Ce paramètre est valide uniquement si le paramètre Type d'authentification est défini sur SCEP.
Profil de certificat partagé	Ce paramètre spécifie le profil de certificat partagé du certificat client utilisé par un terminal Android pour se connecter au serveur de messagerie. Ce paramètre est valide uniquement si le paramètre Type d'authentification est défini sur Certificat partagé.
Profil des informations d'identification de l'utilisateur associé	Ce paramètre spécifie le profil des informations d'identification de l'utilisateur du certificat client utilisé par un terminal Android pour se connecter au serveur de messagerie. Ce paramètre est valide uniquement si le paramètre Type d'authentification est défini sur Informations d'identification de l'utilisateur.
Utiliser SSL	Ce paramètre spécifie si un terminal doit utiliser SSL pour se connecter au serveur de messagerie.
Accepter tous les certificats SSL	Ce paramètre spécifie si un terminal doit accepter automatiquement les certificats SSL non approuvés du serveur de messagerie. S'il n'est pas sélectionné, les terminaux peuvent se connecter uniquement aux serveurs de messagerie qui utilisent un certificat SSL approuvé.
Taille maximale des pièces jointes aux e-mails	Ce paramètre spécifie la taille maximale autorisée pour les pièces jointes d'e-mail (en Mo). Les valeurs possibles sont 1 à 365. Le paramètre par défaut est 25. Ce paramètre s'applique uniquement aux terminaux Android dotés d'un profil professionnel.
Signature électronique par défaut pour les nouveaux messages	Ce paramètre spécifie une signature d'e-mail qui est automatiquement ajoutée aux nouveaux e-mails. Ce paramètre s'applique uniquement aux terminaux Android dotés d'un profil professionnel.
Activer S/MIME	Ce paramètre spécifie si les terminaux peuvent envoyer des e-mails protégés par S/MIME. Pour les terminaux qui utilisent BlackBerry Productivity Suite, vous devez définir une valeur pour le paramètre Prise en charge S/MIME.

Android : paramètre de profil de messagerie	Description
Signer les messages	Ce paramètre spécifie si les terminaux envoient tous les e-mails sortants avec une signature numérique. Ce paramètre est valide uniquement si le paramètre Activer S/MIME est sélectionné. Pour les terminaux Android dotés d'un profil professionnel, ce paramètre s'applique uniquement aux terminaux qui utilisent Divide Productivity. Pour les terminaux qui utilisent le BlackBerry Productivity Suite, vous devez définir une valeur pour le paramètre Messages S/MIME signés numériquement.
Informations d'identification de signature	Ce paramètre spécifie les identifiants que le terminal utilisera pour signer les e-mails. Ce paramètre est valide uniquement si le paramètre Signer les messages est sélectionné. Valeurs possibles : • Certificat partagé • SCEP • Informations d'identification de l'utilisateur La valeur par défaut est Certificat partagé.
Certificat partagé de signature	Ce paramètre spécifie le profil de certificat partagé pour un certificat client utilisé par un terminal afin de signer des e-mails. Ce paramètre est valide uniquement si le paramètre Identifiants de connexion est défini sur Certificat partagé.
SCEP de signature	Ce paramètre spécifie le profil SCEP pour un certificat client utilisé par un terminal afin de signer des e-mails. Ce paramètre est valide uniquement si le paramètre Identifiants de connexion est défini sur SCEP.
Informations d'identification de connexion de l'utilisateur	Ce paramètre spécifie le profil d'identifiants de connexion pour un certificat client utilisé par un terminal afin de signer des e-mails. Ce paramètre est valide uniquement si le paramètre Identifiants de connexion est défini sur Identifiants de connexion d'utilisateur.
Crypter les messages	Ce paramètre spécifie si les terminaux cryptent les e-mails sortants à l'aide du cryptage S/MIME. Ce paramètre est valide uniquement si le paramètre Activer S/MIME est sélectionné. Pour les terminaux Android dotés d'un profil professionnel, ce paramètre s'applique uniquement aux terminaux qui utilisent Divide Productivity. Pour les terminaux qui utilisent le BlackBerry Productivity Suite, vous devez définir une valeur pour le paramètre Messages S/MIME signés numériquement.

Android : paramètre de profil de messagerie	Description
Informations d'identification de cryptage	Ce paramètre spécifie les identifiants que le terminal utilisera pour crypter les e-mails. Ce paramètre est valide uniquement si le paramètre Crypter les messages est sélectionné. Valeurs possibles : • Certificat partagé • SCEP • Informations d'identification de l'utilisateur La valeur par défaut est Certificat partagé.
Certificat partagé de cryptage	Ce paramètre spécifie le profil de certificat partagé pour un certificat client utilisé par un terminal afin de crypter des e-mails. Ce paramètre est valide uniquement si le paramètre Identifiants de cryptage est défini sur Certificat partagé.
SCEP de cryptage	Ce paramètre spécifie le profil SCEP pour un certificat client utilisé par un terminal afin de crypter des e-mails. Ce paramètre est valide uniquement si le paramètre Identifiants de connexion est défini sur SCEP.
Informations d'identification de l'utilisateur de cryptage	Ce paramètre spécifie le profil d'identifiants de connexion pour un certificat client utilisé par un terminal afin de crypter des e-mails. Ce paramètre est valide uniquement si le paramètre Identifiants de connexion est défini sur Identifiants de connexion d'utilisateur.
Exiger l'authentification par carte à puce pour la messagerie	Ce paramètre spécifie si une carte à puce est requise par les terminaux Samsung KNOX pour s'authentifier auprès du serveur de messagerie.
Autoriser l'utilisateur à modifier les paramètres	Spécifiez si l'utilisateur peut modifier les paramètres de remise. Ce paramètre s'applique uniquement aux terminaux Samsung KNOX.
Domaines de messagerie externes	
Liste autorisée des domaines de messagerie externes	Ce paramètre spécifie la liste de domaines vers lesquels un utilisateur peut envoyer des e-mails professionnels et des entrées de calendriers. Par exemple, lorsqu'un utilisateur ajoute un destinataire disposant d'une adresse électronique dans le domaine autorisé à un e-mail ou une entrée de calendrier, aucun message d'avertissement ne s'affiche. Ce paramètre s'applique à l'espace Travail uniquement. Si vous souhaitez indiquer plusieurs noms de domaine, séparez-les par une virgule (,), un point-virgule (;) ou un espace.

Android : paramètre de profil de messagerie	Description
Liste restreinte des domaines de messagerie externes	Ce paramètre spécifie la liste de domaines vers lesquels les utilisateurs peuvent envoyer des e-mails professionnels et des entrées de calendriers. Par exemple, si un utilisateur tente d'ajouter un destinataire disposant d'une adresse électronique correspondant au domaine limité à un e-mail ou une invitation de calendrier, l'application Messagerie ou Calendrier ne permet pas à l'utilisateur de mener à bien cette opération. Ce paramètre s'applique à l'espace Travail uniquement. Si vous souhaitez indiquer plusieurs noms de domaine, séparez-les par une virgule (,), un point-virgule (;) ou un espace.
BlackBerry Productivity Suite Ces paramètres s'appliquent uniquement aux terminaux Android dotés d'un profil professionnel.	
Effectuer la vérification OCSP	Ce paramètre spécifie si les terminaux peuvent utiliser OCSP pour vérifier l'état de certificats S/MIME.
Autoriser l'acceptation de certificats non approuvés	Ce paramètre spécifie si les utilisateurs peuvent autoriser le terminal à accepter des certificats non approuvés.
Autoriser l'envoi des évènements de télémétrie depuis le profil professionnel	Ce paramètre spécifié si BlackBerry Productivity Suite permet la collecte de données d'utilisation.
Type de sécurité	Ce paramètre spécifie le type de sécurité utilisé par BlackBerry Productivity Suite. Valeurs possibles : • SSL • SSL-Trust All La valeur par défaut est SSL.
Autoriser le partage de données entre les profils professionnel et personnel	Ce paramètre indique si le profil personnel peuvent accéder aux données dans le profil de travail. Sélectionnez ce paramètre, ainsi que le paramètre Autoriser les applications personnelles à accéder aux données professionnelles pour activer les fonctionnalités suivantes : • Une BlackBerry Hub unifiée contenant à la fois les comptes professionnels et personnels. Pour plus d'informations, reportez-vous à Activer un BlackBerry Hub unifié. • Un dictionnaire clavier unifié permettant de partager les mots appris entre les profils professionnel et personnel. Les utilisateurs peuvent décider d'utiliser ou non le dictionnaire clavier unifié pour les prédictions et corrections. .

Android : paramètre de profil de messagerie	Description
Autoriser les applications personnelles à accéder aux données professionnelles	Ce paramètre spécifie si les applications personnelles peuvent accéder aux données professionnelles. Sélectionnez ce paramètre ainsi que le paramètre Autoriser le partage de données entre les profils professionnel et personnel pour activer les fonctionnalités suivantes : • Une BlackBerry Hub unifiée contenant à la fois les comptes professionnels et personnels. Pour plus d'informations, reportez-vous à Activer un BlackBerry Hub unifié. • Un dictionnaire clavier unifié permettant de partager les mots appris entre les profils professionnel et personnel. Les utilisateurs peuvent décider d'utiliser ou non le dictionnaire clavier unifié pour les prédictions et corrections. .
Paramètres S/MIME Ces paramètres s'appliquent uniquement aux terminaux Android dotés d'un profil professionnel.	
Prise en charge S/MIME	Ce paramètre spécifie si un terminal Android qui utilise BlackBerry Productivity Suite peut envoyer des e-mails protégés par S/MIME. Valeurs possibles : • Autoriser • Requise • Interdire La valeur par défaut est Autoriser.
Messages S/MIME avec signature numérique	Ce paramètre spécifie si un terminal Android qui utilise BlackBerry Productivity Suite envoie des e-mails sortants avec une signature numérique. Valeurs possibles : • Autoriser • Requise • Interdire La valeur par défaut est Autoriser.
Messages S/MIME cryptés	Ce paramètre spécifie si un terminal Android qui utilise BlackBerry Productivity Suite crypte les e-mails sortants à l'aide du cryptage S/MIME. Valeurs possibles : • Autoriser • Requise • Interdire La valeur par défaut est Autoriser.

Android : paramètre de profil de messagerie	Description
Algorithmes de cryptage S/MIME	Ce paramètre spécifie les algorithmes de cryptage qu'un terminal Android qui utilise BlackBerry Productivity Suite peut utiliser pour crypter des e-mails protégés par S/MIME. Valeurs possibles : • AES (256 bits) • AES (192 bits) • AES (128 bits) • Triple DES • ARC2

Windows : paramètres de profil de messagerie

Windows : paramètre de profil de messagerie	Description
Paramètres de remise	
Type de profil	Ce paramètre spécifie si vous souhaitez que ce profil prenne en charge Exchange ActiveSync ou IBM Notes Traveler. Valeurs possibles : • Exchange ActiveSync • IBM Notes Traveler La valeur par défaut est Exchange ActiveSync.
Nom du compte	Ce paramètre spécifie le nom du compte de messagerie professionnel qui apparait sur le terminal Windows. Vous pouvez utiliser une variable telle que %UserEmailAddress%.
Intervalle de synchronisation	Ce paramètre spécifie la fréquence à laquelle un terminal Windows télécharge de nouveaux e-mails à partir du serveur de messagerie. Valeurs possibles : • À mesure que les éléments sont reçus • Manuel • 15 minutes • 30 minutes • 60 minutes La valeur par défaut est À mesure que les éléments sont reçus.

Windows : paramètre de profil de messagerie	Description
Jours de synchronisation	Ce paramètre spécifie le nombre de jours passés afin de synchroniser les e-mails et données de l'organiseur avec un terminal Windows. Valeurs possibles : • Toujours • 3 jours • 7 jours • 14 jours • 1 mois La valeur par défaut est 7 jours.
Utiliser SSL	Ce paramètre spécifie si un terminal Windows doit utiliser SSL pour se connecter au serveur de messagerie.
Contenu à synchroniser	
Adresse électronique,	Ce paramètre spécifie si un terminal Windows synchronise les e-mails avec le serveur de messagerie.
Contacts	Ce paramètre spécifie si un terminal Windows synchronise les contacts avec le serveur de messagerie.
Calendrier	Ce paramètre spécifie si un terminal Windows synchronise les entrées de calendrier avec le serveur de messagerie.
Tâche	Ce paramètre spécifie si un terminal Windows synchronise les données des tâches avec le serveur de messagerie. Ce paramètre est valide uniquement si le paramètre Type de profil est défini sur « Exchange ActiveSync ».

Paramètres de profil de messagerie IMAP/POP3

Vous pouvez utiliser une variable de paramètre de profil correspondant à un champ de texte pour faire référence à une valeur plutôt que de spécifier la valeur réelle. BlackBerry UEM prend en charge les variables par défaut prédéfinies et les variables personnalisées que vous définissez. Les profils de messagerie IMAP/POP3 sont pris en charge sur les types de terminaux suivants :

- iOS
- macOS
- Android
- Windows

Dans certains cas, la version minimale du système d'exploitation du terminal requis pour prendre en charge un paramètre correspondant à une version non prise en charge par BlackBerry UEM. Pour en savoir plus sur les versions prises en charge, consultez la Matrice de compatibilité.

Communs : paramètres de profil de messagerie IMAP/POP3

Commun : paramètre de profil de messagerie IMAP/POP3	Description
Type de messagerie	Ce paramètre spécifie le type de serveur de messagerie. Valeurs possibles : • IMAP • POP3 La valeur par défaut est IMAP.
Nom d'affichage	Ce paramètre spécifie le nom d'affichage du compte. Si le profil concerne plusieurs utilisateurs, vous pouvez utiliser la variable %UserDisplayName%.
Adresse e-mail,	Ce paramètre spécifie l'adresse électronique de l'utilisateur. Si le profil concerne plusieurs utilisateurs, vous pouvez utiliser la variable %UserEmailAddress%.
Paramètres du courrier entrant	
Nom d'hôte ou adresse IP	Ce paramètre spécifie le nom d'hôte ou l'adresse IP du serveur de messagerie pour le courrier entrant.
Port	Ce paramètre spécifie le port utilisé pour se connecter au serveur de messagerie pour le courrier entrant.
Nom d'utilisateur	Ce paramètre spécifie le nom d'utilisateur de l'utilisateur. Si le profil concerne plusieurs utilisateurs, vous pouvez utiliser la variable %UserName%.
Utiliser SSL pour les e-mails entrants	Ce paramètre spécifie si un terminal iOS, Android ou Windows Phone doit utiliser SSL pour se connecter au serveur de messagerie et récupérer le courrier reçu.
Paramètres du courrier sortant	
Nom d'hôte ou adresse IP	Ce paramètre spécifie le nom d'hôte ou l'adresse IP du serveur de messagerie pour le courrier sortant.
Port	Ce paramètre spécifie le port utilisé pour se connecter au serveur de messagerie pour le courrier sortant.
Utiliser SSL pour les e-mails sortant	Ce paramètre spécifie si un terminal iOS, Android ou Windows Phone doit utiliser SSL pour se connecter au serveur de messagerie pour envoyer du courrier.
Authentification requise pour les e-mails sortants	Ce paramètre spécifie si un terminal doit s'authentifier auprès du serveur pour envoyer du courrier.

Commun : paramètre de profil de messagerie IMAP/POP3	Description
Utiliser les mêmes informations d'identification que pour les paramètres entrants	Ce paramètre spécifie si un terminal iOS, Android ou Windows Phone utilise les mêmes informations d'identification pour recevoir les e-mails que celles utilisées pour envoyer des e-mails et s'authentifier auprès du serveur de messagerie. Si un terminal n'utilise pas les mêmes informations d'identification pour recevoir les e-mails que celles utilisées pour envoyer des e-mails et s'authentifier auprès du serveur de messagerie, vous pouvez spécifier le nom d'utilisateur et le mot de passe utilisés par un terminal. Ce paramètre est valide uniquement si le paramètre Authentification requise pour les e-mails sortants est sélectionné.

iOS et macOS : paramètres de profil de messagerie IMAP/POP3

macOS applique les profils aux terminaux ou comptes d'utilisateur. Les profils IMAP/POP3 sont appliqués aux comptes d'utilisateur.

iOS : paramètre de profil de messagerie IMAP/ POP3	Description
Préfixe de chemin IMAP	Ce paramètre spécifie le préfixe de chemin IMAP, si nécessaire. Si nécessaire, contactez votre FAI pour plus d'informations. Ce paramètre est valide uniquement si la valeur du paramètre Type de messagerie est définie sur IMAP.
Autoriser le déplacement de messages	Ce paramètre spécifie si les utilisateurs peuvent déplacer les e-mails de ce compte vers un autre compte de messagerie sur un terminal iOS.
Autoriser la synchronisation des adresses récentes	Ce paramètre spécifie si un utilisateur de terminal iOS peut synchroniser les adresses récemment utilisées sur les terminaux.
Utiliser uniquement dans la messagerie	Ce paramètre spécifie si les applications autres que l'application de messagerie d'un terminal iOS peuvent utiliser ce compte pour envoyer des e-mails.
Activer S/MIME	Ce paramètre spécifie si un utilisateur de terminal iOS peut envoyer des e-mails protégés par S/MIME. S/MIME est pris en charge uniquement sur les terminaux qui sont activés avec les commandes MDM.

iOS : paramètre de profil de messagerie IMAP/ POP3	Description
Informations d'identification de signature	Ce paramètre spécifie les identifiants que le terminal utilisera pour signer les e-mails. Ce paramètre est valide uniquement si le paramètre Activer S/MIME est sélectionné. Valeurs possibles : • Certificat partagé • SCEP • Informations d'identification de l'utilisateur La valeur par défaut est Certificat partagé.
Certificat partagé de signature	Ce paramètre spécifie le profil de certificat partagé pour un certificat client utilisé par un terminal afin de signer des e-mails. Ce paramètre est valide uniquement si le paramètre Identifiants de connexion est défini sur Certificat partagé.
SCEP de signature	Ce paramètre spécifie le profil SCEP utilisé par les terminaux pour récupérer les certificats requis pour signer les e-mails à l'aide de S/MIME. Ce paramètre est valide uniquement si le paramètre Identifiants de connexion est défini sur SCEP.
Informations d'identification de connexion de l'utilisateur	Ce paramètre spécifie le profil des informations d'identification de l'utilisateur utilisé par les terminaux pour obtenir les certificats client requis pour signer les e-mails à l'aide de S/MIME. Ce paramètre est valide uniquement si le paramètre Identifiants de connexion est défini sur Identifiants de connexion d'utilisateur.
Informations d'identification de cryptage	Ce paramètre spécifie la manière dont les terminaux trouvent les certificats requis pour crypter les messages. Ce paramètre est valide uniquement si le paramètre Activer S/MIME est sélectionné. Valeurs possibles : • Certificat partagé • SCEP • Informations d'identification de l'utilisateur Après avoir sélectionné le type de profil, sélectionnez le profil de certificat partagé, profil SCEP ou profil des informations d'identification de l'utilisateur que vous souhaitez utiliser.

iOS : paramètre de profil de messagerie IMAP/ POP3	Description
Certificat partagé de cryptage	Ce paramètre spécifie le profil de certificat partagé pour un certificat client utilisé par un terminal afin de crypter des e-mails. Les terminaux choisissent le certificat adapté au destinataire pour crypter les messages à l'aide de S/MIME. Ce paramètre est valide uniquement si le paramètre Identifiants de cryptage est défini sur Certificat partagé.
SCEP de cryptage	Ce paramètre spécifie le profil SCEP utilisé par les terminaux pour récupérer les certificats requis et crypter les e-mails à l'aide de S/MIME. Ce paramètre est valide uniquement si le paramètre Identifiants de cryptage est défini sur SCEP.
Informations d'identification de l'utilisateur de cryptage	Ce paramètre spécifie le profil des informations d'identification de l'utilisateur utilisé par les terminaux pour récupérer les certificats client requis et crypter les e-mails à l'aide de S/MIME. Ce paramètre est valide uniquement si le paramètre Identifiants de cryptage est défini sur Identifiants de connexion d'utilisateur.
Crypter les messages	Ce paramètre spécifie si tous les e-mails doivent être cryptés lorsque l'utilisateur les envoie (Obligatoire), ou si l'utilisateur peut choisir les e-mails à crypter au moment où il les envoie (Autoriser). Ce paramètre s'applique uniquement si le paramètre Activer S/MIME est sélectionné. Valeurs possibles : • Obligatoire • Autoriser La valeur par défaut est Requis. L'exigence minimale est iOS version 8.0 et les terminaux doivent être activés avec les commandes MDM.
Autoriser Mail Drop	Ce paramètre spécifie si les utilisateurs peuvent envoyer des fichiers à partir de ce compte avec Mail Drop. L'exigence minimale est iOS version 9.0 et les terminaux doivent être activés avec les commandes MDM.

Android : paramètres de profil de messagerie IMAP/POP3

Android : paramètre de profil de messagerie IMAP/POP3	Description
Préfixe de chemin IMAP	Ce paramètre spécifie le préfixe de chemin IMAP, si nécessaire. Si nécessaire, contactez votre FAI pour plus d'informations. Ce paramètre est valide uniquement si la valeur du paramètre Type de messagerie est définie sur IMAP.
Supprimer un e-mail du serveur	Ce paramètre spécifie le moment où supprimer un e-mail du serveur de messagerie. Valeurs possibles : • Jamais • En cas de suppression depuis la boite de réception La valeur par défaut est Jamais. Ce paramètre est valide uniquement si la valeur du paramètre Type de messagerie est définie sur POP3.

Windows : paramètres de profil de messagerie IMAP/POP3

Windows : paramètre de profil de messagerie IMAP/POP3	Description
Supprimer un e-mail du serveur	Ce paramètre spécifie comment les e-mails sont traités lorsqu'un utilisateur les supprime. Les e-mails peuvent être supprimés du serveur (suppression physique) ou supprimés de la boîte de réception mais conservés dans le dossier Corbeille (suppression avec récupération possible). Valeurs possibles : • Supprimer définitivement • Supprimer (récupération possible) La valeur par défaut est Supprimer (récupération possible). Ce paramètre est valide uniquement si le paramètre Type de messagerie est défini sur IMAP. Ce paramètre est valide uniquement pour les terminaux Windows 10.
Domaine	Ce paramètre spécifie le nom de domaine du serveur de messagerie.

Windows : paramètre de profil de messagerie IMAP/POP3	Description
Intervalle de synchronisation	Ce paramètre spécifie la fréquence à laquelle un terminal Windows télécharge du nouveau contenu à partir du serveur de messagerie. Valeurs possibles : • Manuel • 15 minutes • 30 minutes • 60 minutes • 2 heures La valeur par défaut est 15 minutes.
Montant de récupération initial	Ce paramètre spécifie le nombre de jours passés afin de synchroniser les e-mails et données de l'organiseur avec un terminal Windows. Valeurs possibles : • Toutes • 7 jours • 14 jours • 30 jours La valeur par défaut est 7 jours.
Utiliser uniquement le réseau cellulaire et non Wi-Fi	Ce paramètre indique si des e-mails sont envoyés et reçus uniquement sur le réseau mobile. Ce paramètre est valide uniquement pour les terminaux Windows 10.

Paramètres du profil Wi-Fi

Vous pouvez utiliser une variable de paramètre de profil correspondant à un champ de texte pour faire référence à une valeur plutôt que de spécifier la valeur réelle. BlackBerry UEM prend en charge les variables par défaut prédéfinies et les variables personnalisées que vous définissez. Les profils Wi-Fi sont pris en charge sur les types de terminaux suivants :

- BlackBerry 10
- iOS
- macOS
- Android
- Windows

Dans certains cas, la version minimale du système d'exploitation du terminal requis pour prendre en charge un paramètre correspondant à une version non prise en charge par BlackBerry UEM. Pour plus d'informations sur les versions de système d'exploitation prises en charge, reportez-vous à la matrice de compatibilité.

Communs : paramètres de profil Wi-Fi

Commun : paramètre de profil Wi-Fi	Description
SSID	Ce paramètre spécifie le nom d'un réseau Wi-Fi et ses points d'accès sans fil. Le SSID est sensible à la casse et doit contenir des caractères alphanumériques. Les valeurs possibles sont limitées à 32 caractères.
Réseau masqué	Ce paramètre spécifie si le réseau Wi-Fi masque le SSID.

BlackBerry 10 : paramètres de profil Wi-Fi

BlackBerry 10 : paramètre de profil Wi-Fi	Description
Type de sécurité	Ce paramètre indique le type de sécurité utilisé par le réseau Wi-Fi. Valeurs possibles : • Aucune • WEP personnel • WPA-Personal • WPA-Enterprise • WPA2-Personal • WPA2-Enterprise La valeur par défaut est Aucune.
Clé WEP	Ce paramètre spécifie la clé WEP du réseau Wi-Fi. La clé WEP doit contenir 10 ou 26 caractères hexadécimaux (0-9, A-F) ou 5 ou 13 caractères alphanumériques (0-9, A-Z). Exemples de valeurs de clés hexadécimales : ABCDEF0123 ou ABCDEF0123456789ABCDEF0123. Exemples de valeurs de clés alphanumériques : abCD5 ou abCDefGHijKL1. Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini sur WEP personnel.
Type de clé pré-partagée	Ce paramètre spécifie le type de clé pré-partagée du réseau Wi-Fi. Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini WPA-Personal ou WPA2-Personal. Valeurs possibles : • ASCII • HEX La valeur par défaut est ASCII.

BlackBerry 10 : paramètre de profil Wi-Fi	Description
Clé pré-partagée	Ce paramètre spécifie la clé pré-partagée du réseau Wi-Fi. Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini WPA-Personal ou WPA2-Personal. Les valeurs possibles sont limitées à 64 caractères.
Protocole d'authentification	Ce paramètre spécifie la méthode EAP utilisée par le réseau Wi-Fi. Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini WPA-Enterprise ou WPA2-Enterprise. Valeurs possibles : • PEAP • TTLS • EAP-FAST • TLS La valeur par défaut est PEAP.
Authentification interne	Ce paramètre spécifie la méthode d'authentification interne utilisée avec un tunnel TLS. Si vous souhaitez utiliser PAP pour l'authentification interne, définissez ce paramètre sur Auto. Ce paramètre est valide uniquement si le paramètre Protocole d'authentification est défini sur PEAP ou TTLS. Valeurs possibles : • Auto • MS-CHAPv2 • GTC La valeur par défaut est Auto.
Méthode de déploiement EAP-FAST	Ce paramètre spécifie la méthode de déploiement pour l'authentification EAP-FAST. Ce paramètre est valide uniquement si le paramètre Protocole d'authentification est défini sur EAP-FAST. Valeurs possibles : • Anonyme • Authentifié La valeur par défaut est Anonyme.
Nom d'utilisateur	Ce paramètre spécifie le nom d'utilisateur utilisé par un terminal BlackBerry 10 pour s'authentifier auprès du réseau Wi-Fi. Si le profil concerne plusieurs utilisateurs, vous pouvez utiliser la variable %UserName%. Ce paramètre est valide uniquement si le paramètre Protocole d'authentification est défini sur PEAP, TTLS, EAP-FAST ou TLS.

BlackBerry 10 : paramètre de profil Wi-Fi	Description
Mot de passe,	Ce paramètre spécifie le mot de passe utilisé par un terminal BlackBerry 10 pour s'authentifier auprès du réseau Wi-Fi. Ce paramètre est valide uniquement si le paramètre Protocole d'authentification est défini sur PEAP, TTLS ou EAP-FAST.
Type de bande	Ce paramètre spécifie la bande de fréquence utilisée par le réseau Wi-Fi. Valeurs possibles : • Dual • 2,4 GHz • 5,0 GHz La valeur par défaut est Dual.
Activer DHCP	Ce paramètre spécifie si le réseau Wi-Fi utilise le DHCP.
Adresse IP	Ce paramètre spécifie l'adresse IP de l'hôte pour le réseau Wi-Fi. Ce paramètre est valide uniquement si le paramètre Activer DHCP n'est pas sélectionné.
Masque de sous-réseau	Ce paramètre spécifie le masque de sous-réseau au format décimal séparé par des points (par exemple, 192.0.2.0). Ce paramètre est valide uniquement si le paramètre Activer DHCP n'est pas sélectionné.
DNS primaire	Ce paramètre spécifie le serveur DNS primaire au format décimal séparé par des points (par exemple, 192.0.2.0). Ce paramètre est valide uniquement si le paramètre Activer DHCP n'est pas sélectionné.
DNS secondaire	Ce paramètre spécifie le serveur DNS secondaire au format décimal séparé par des points (par exemple, 192.0.2.0). Ce paramètre est valide uniquement si le paramètre Activer DHCP n'est pas sélectionné.
Passerelle par défaut	Ce paramètre spécifie la passerelle par défaut au format décimal séparé par des points (par exemple, 192.0.2.0). Ce paramètre est valide uniquement si le paramètre Activer DHCP n'est pas sélectionné.
Suffixe de domaine	Ce paramètre spécifie l'FQDN du suffixe DNS. Ce paramètre est valide uniquement si le paramètre Activer DHCP n'est pas sélectionné.
Activer IPv6	Ce paramètre spécifie si le réseau Wi-Fi prend en charge IPv6.

BlackBerry 10 : paramètre de profil Wi-Fi	Description
Activer le transfert entre points d'accès	Ce paramètre indique si un terminal BlackBerry 10 peut effectuer des transferts de Wi-Fi entre des points d'accès sans fil.
Modifiable par l'utilisateur	Ce paramètre spécifie les paramètres Wi-Fi qu'un utilisateur de terminal BlackBerry 10 peut modifier. Si ce paramètre est défini sur Lecture seule, l'utilisateur ne peut pas modifier les paramètres. Si ce paramètre est défini sur Informations d'identification uniquement, l'utilisateur peut modifier le nom d'utilisateur et le mot de passe. Valeurs possibles : • Lecture seule • Informations d'identification uniquement La valeur par défaut est Lecture seule.
Niveau de sécurité des données	Ce paramètre spécifie le domaine de l'espace Travail où le profil Wi-Fi est stocké lorsque l'espace Travail utilise la protection avancée des données inactives. Ce paramètre est uniquement valide si la règle de stratégie informatique « Appliquer la protection avancée des données inactives » est sélectionnée. Si ce paramètre est défini sur Toujours disponible, le profil est stocké dans le domaine de démarrage et disponible lorsque l'espace Travail est verrouillé. Si ce paramètre est défini sur Disponible après authentification, le profil est stocké dans le domaine opérationnel et disponible lorsque l'espace Travail est déverrouillé une fois jusqu'à ce que le terminal redémarre. Si ce paramètre est défini sur Disponible uniquement lorsque l'espace Travail est déverrouillé, le profil est stocké dans le domaine de verrouillage et peut être utilisé pour les connexionsWi-Fi uniquement lorsque l'espace Travail est déverrouillé. Valeurs possibles : • Toujours disponible • Disponible après authentification • Disponible uniquement lorsque l'espace Travail est déverrouillé La valeur par défaut est Toujours disponible. La configuration minimale requise est BlackBerry 10 OS version 10.3.1.
Imposer TLS 1.2	Ce paramètre indique si les terminaux BlackBerry 10 doivent utiliser TLS 1.2 pour la communication sur le réseau Wi-Fi. Valeurs possibles : • O • I La valeur par défaut est « Off ». La configuration minimale requise est BlackBerry 10 OS version 10.3.3.
Se fier	

BlackBerry 10 : paramètre de profil Wi-Fi	Description
Source du certificat client	Ce paramètre spécifie la manière dont les terminaux BlackBerry 10 obtiennent le certificat client. Quatre options permettent aux terminaux d'obtenir des certificats client : • Si vous choisissez SCEP, vous devez également spécifier le profil SCEP associé que le terminal peut utiliser pour télécharger le certificat client. • Si vous choisissez Informations d'identification de l'utilisateur, vous devez également spécifier le profil des informations d'identification de l'utilisateur associé que le terminal peut utiliser pour télécharger le certificat client. • Si vous choisissez Carte à puce, l'utilisateur doit coupler le terminal avec une carte à puce contenant le certificat client. • Si vous choisissez Autre, l'utilisateur doit manuellement ajouter le certificat client au terminal. Les terminaux exécutant BlackBerry 10 OS version 10.3.1 ou ultérieure prennent en charge la carte à puce. Valeurs possibles : • Carte à puce • SCEP • Informations d'identification de l'utilisateur • Autre La valeur par défaut est Autre.
Profil SCEP associé	Ce paramètre spécifie le profil SCEP associé utilisé par un BlackBerry 10 terminal pour inscrire un certificat client et s'authentifier auprès du réseau Wi-Fi. Ce paramètre est valide uniquement si le paramètre Source du certificat client est défini sur SCEP.
Profil des informations d'identification de l'utilisateur associé	Ce paramètre spécifie le profil des informations d'identification de l'utilisateur associé utilisé par un terminal BlackBerry 10 pour inscrire un certificat client et s'authentifier auprès du réseau Wi-Fi. Ce paramètre est valide uniquement si le paramètre Source du certificat client est défini sur Informations d'identification de l'utilisateur. La configuration minimale pour utiliser un profil des informations d'identification de l'utilisateur est BlackBerry 10 OS version 10.3.1.
Source du certificat approuvé	Ce paramètre spécifie la source du certificat approuvé. Si ce paramètre est défini sur Magasin de certificats approuvé, le terminal BlackBerry 10 peut se connecter à un réseau Wi-Fi utilisant un certificat du magasin de certificats Wi-Fi. Valeurs possibles : • Aucune • Magasin de certificats approuvés La valeur par défaut est Aucune.
Profils associés	

BlackBerry 10 : paramètre de profil Wi-Fi	Description
Utiliser un profil de connectivité d'entreprise avec une connexion BlackBerry Secure Connect Plus pour les données professionnelles	Ce paramètre spécifie si tout le trafic de l'espace Travail est dirigé via BlackBerry Secure Connect Plus, y compris lorsque les terminaux BlackBerry 10 peuvent accéder au réseau Wi-Fi professionnel. Si ce paramètre n'est pas sélectionné, lorsque vous configurez un profil Wi-Fiet l'attribuez aux terminaux BlackBerry 10, les terminaux classent par ordre de priorité le réseau Wi-Fi professionnel au-dessus de BlackBerry Secure Connect Plus pour le trafic de l'espace Travail. Si vous souhaitez utiliser cette fonctionnalité, dans la stratégie informatique attribuée aux utilisateurs de terminaux BlackBerry 10, vérifiez que la règle de stratégie informatique **Forcer le contrôle d'accès au réseau pour les applications professionnelles** n'est pas sélectionnée. Ce paramètre peut avoir une incidence sur l'utilisation des données de votre entreprise et les frais de réseau. Vérifiez qu'il s'agit de la configuration privilégiée par votre entreprise avant d'utiliser cette fonctionnalité. La configuration minimale requise est BlackBerry 10 OS version 10.3.2.
Profil VPN associé	Ce paramètre spécifie le profil VPN associé utilisé par un terminal BlackBerry 10 pour se connecter à un réseau VPN lorsque le terminal est connecté au réseau Wi-Fi.
Profil proxy associé	Ce paramètre spécifie le profil proxy associé utilisé par un terminal BlackBerry 10 pour se connecter à un serveur proxy lorsque le terminal est connecté au réseau Wi-Fi.

iOS et macOS : paramètres de profil Wi-Fi

macOS applique les profils aux terminaux ou comptes d'utilisateur. Vous pouvez configurer un profil Wi-Fi à appliquer à l'un ou à l'autre.

iOS et macOS : paramètre de profil Wi-Fi	Description
Rejoindre automatiquement le réseau	Ce paramètre spécifie si un terminal peut automatiquement rejoindre le réseau Wi-Fi.
Appliquer le profil à	Ce paramètre indique si le profil Wi-Fi est appliqué au compte d'utilisateur ou au terminal. Valeurs possibles : • Utilisateur • Terminal Ce paramètre est valide uniquement pour macOS.
Profil proxy associé	Ce paramètre spécifie le profil proxy associé utilisé par un terminal pour se connecter à un serveur proxy lorsque le terminal est connecté au réseau Wi-Fi.

iOS et macOS : paramètre de profil Wi-Fi	Description
Type de réseau	Ce paramètre spécifie la configuration du réseau Wi-Fi. Les configurations de points d'accès s'appliquent uniquement aux terminaux iOS et macOS. Pour configurer les paramètres Wi-Fi des terminaux BlackBerry, Android et Windows Phone, créez un profil Wi-Fi distinct. Valeurs possibles : • Standard • Point d'accès hérité • Hotspot 2.0 La valeur par défaut est Standard.
Nom de l'opérateur affiché	Ce paramètre spécifie le nom convivial de l'opérateur de points d'accès. Ce paramètre est valide uniquement si le paramètre Type de réseau est défini sur Hotspot 2.0.
Nom de domaine	Ce paramètre spécifie le nom de domaine de l'opérateur de points d'accès. Ce paramètre est valide uniquement si le paramètre Type de réseau est défini sur Hotspot 2.0. Le paramètre SSID n'est pas requis lorsque vous utilisez ce paramètre.
Identifiants d'entreprise des consortiums d'itinérance	Ce paramètre spécifie les identifiants d'entreprise des consortiums d'itinérance et fournisseurs de services agissant en tant que partenaires d'itinérance de l'opérateur de points d'accès. Ce paramètre est valide uniquement si le paramètre Type de réseau est défini sur Hotspot 2.0.
Noms de domaine NAI	Ce paramètre spécifie les noms de domaine de l'identifiant d'accès réseau capables d'authentifier un terminal iOS. Ce paramètre est valide uniquement si le paramètre Type de réseau est défini sur Hotspot 2.0.
MCC/MNC	Ce paramètre spécifie les combinaisons MCC et MNC qui identifient les opérateurs de réseaux mobiles. Chaque valeur doit contenir six chiffres. Ce paramètre est valide uniquement si le paramètre Type de réseau est défini sur Hotspot 2.0.
Autoriser la connexion aux réseaux des partenaires d'itinérance	Ce paramètre spécifie si un terminal peut se connecter aux partenaires d'itinérance pour le point d'accès. Ce paramètre est valide uniquement si le paramètre Type de réseau est défini sur Hotspot 2.0.

iOS et macOS : paramètre de profil Wi-Fi	Description
Type de sécurité	Ce paramètre indique le type de sécurité utilisé par le réseau Wi-Fi. Si le paramètre Type de réseau est défini sur Hotspot 2.0, ce paramètre est défini sur WPA2-Enterprise. Valeurs possibles : • Aucune • WEP personnel • WEP Enterprise • WPA-Personal • WPA-Enterprise • WPA2-Personal • WPA2-Enterprise La valeur par défaut est Aucune.
Clé WEP	Ce paramètre spécifie la clé WEP du réseau Wi-Fi. La clé WEP doit contenir 10 ou 26 caractères hexadécimaux (0-9, A-F) ou 5 ou 13 caractères alphanumériques (0-9, A-Z). Exemples de valeurs de clés hexadécimales : ABCDEF0123 ou ABCDEF0123456789ABCDEF0123. Exemples de valeurs de clés alphanumériques : abCD5 ou abCDefGHijKL1. Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini sur WEP personnel.
Clé pré-partagée	Ce paramètre spécifie la clé pré-partagée du réseau Wi-Fi. Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini WPA-Personal ou WPA2-Personal.
Protocoles	
Protocole d'authentification	Ce paramètre spécifie la méthode EAP prise en charge par le réseau Wi-Fi. Vous pouvez sélectionner plusieurs méthodes EAP. Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini sur WEP Enterprise, WPA-Enterprise ou WPA2-Enterprise. Sélections possibles : • TLS • TTLS • LEAP • PEAP • EAP-FAST • EAP-SIM

iOS et macOS : paramètre de profil Wi-Fi	Description
Authentification interne	Ce paramètre indique la méthode d'authentification interne à utiliser avec TTLS. Ce paramètre est valide uniquement si le paramètre Protocole d'authentification est défini sur TTLS. Valeurs possibles : • Aucune • PAP • CHAP • MS-CHAP • MS-CHAPv2 • EAP La valeur par défaut est MS-CHAPv2.
Utiliser PAC	Ce paramètre spécifie si la méthode EAP-FAST utilise des informations d'accès protégé (PAC). Ce paramètre est valide uniquement si le paramètre Protocole d'authentification est défini sur EAP-FAST.
Déployer PAC	Ce paramètre spécifie si la méthode EAP-FAST permet un déploiement PAC. Ce paramètre est valide uniquement si le paramètre Protocole d'authentification est défini sur EAP-FAST et si le paramètre Utiliser PAC est sélectionné.
Déployer PAC anonymement	Ce paramètre spécifie si la méthode EAP-FAST permet un déploiement PAC anonyme. Ce paramètre est valide uniquement si le paramètre Protocole d'authentification est défini sur Utiliser PAC et si le paramètre Déployer PAC est sélectionné.
Authentification	
Identité externe pour TTLS, PEAP et EAP-FAST	Ce paramètre spécifie l'identité externe d'un utilisateur envoyée en clair. Vous pouvez spécifier un nom d'utilisateur anonyme pour masquer l'identité réelle de l'utilisateur (par exemple, anonyme). Le tunnel crypté est utilisé pour envoyer le nom d'utilisateur réel à des fins d'authentification auprès du réseau Wi-Fi. Si l'identité externe comprend le nom de domaine pour l'acheminement de la demande, il doit correspondre au domaine réel de l'utilisateur (par exemple, anonyme@exemple.com). Ce paramètre est valide uniquement si le paramètre Protocole d'authentification est défini sur TTLS, PEAP ou EAP-FAST.
Utiliser le mot de passe inclus dans le profil Wi-Fi	Ce paramètre spécifie si le profil Wi-Fi inclut le mot de passe à des fins d'authentification. Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini sur WEP Enterprise, WPA-Enterprise ou WPA2-Enterprise.

iOS et macOS : paramètre de profil Wi-Fi	Description
Mot de passe,	Ce paramètre spécifie le mot de passe utilisé par un terminal iOS pour s'authentifier auprès du réseau Wi-Fi. Ce paramètre est valide uniquement si le paramètre Utiliser le mot de passe inclus dans le profil Wi-Fi est sélectionné.
Nom d'utilisateur	Ce paramètre spécifie le nom d'utilisateur utilisé par un terminal iOS pour s'authentifier auprès du réseau Wi-Fi. Si le profil concerne plusieurs utilisateurs, vous pouvez utiliser la variable %UserName%. Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini sur WEP Enterprise, WPA-Enterprise ou WPA2-Enterprise.
Type d'authentification	Ce paramètre spécifie le type d'authentification utilisé par un terminal pour se connecter au réseau Wi-Fi. Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini sur WEP Enterprise, WPA-Enterprise ou WPA2-Enterprise. Valeurs possibles : • Aucune • Certificat partagé • SCEP • Informations d'identification de l'utilisateur La valeur par défaut est Aucune.
Type de liaison de certificat	Ce paramètre spécifie le type de liaison du certificat client associé au profil Wi-Fi. Ce paramètre est valide uniquement si le paramètre Type d'authentification est défini sur Certificat partagé. Valeurs possibles : • Référence unique • Injection de variable La valeur par défaut est Référence unique.
Profil de certificat partagé	Ce paramètre spécifie le profil de certificat partagé avec le certificat client utilisé par un terminal pour s'authentifier auprès du réseau Wi-Fi. Ce paramètre est valide uniquement si le paramètre Type de liaison de certificat est défini sur Référence unique.
Nom du certificat client	Ce paramètre spécifie le nom du certificat client utilisé par un terminal pour s'authentifier auprès du réseau Wi-Fi. Ce paramètre est valide uniquement si le paramètre Type de liaison de certificat est définir sur Injection de variable.

iOS et macOS : paramètre de profil Wi-Fi	Description
Profil SCEP associé	Ce paramètre spécifie le profil SCEP associé utilisé par un terminal pour obtenir un certificat client et s'authentifier auprès du réseau Wi-Fi. Ce paramètre est valide uniquement si le paramètre Type d'authentification est défini sur SCEP.
Profil des informations d'identification de l'utilisateur associé	Ce paramètre spécifie le profil d'informations d'identification de l'utilisateur associé utilisé par un terminal pour obtenir un certificat client et s'authentifier auprès du réseau Wi-Fi. Ce paramètre est valide uniquement si le paramètre Type d'authentification est défini sur Informations d'identification de l'utilisateur.
Se fier	
Noms usuels de certificat attendus par le serveur d'authentification	Ce paramètre spécifie les noms usuels du certificat envoyés par le serveur d'authentification au terminal (par exemple, * .exemple.com). Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini sur WEP Enterprise, WPA-Enterprise ou WPA2-Enterprise.
Type de liaison de certificat	Ce paramètre spécifie le type de liaison des certificats client associés au profil Wi-Fi. Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini sur WEP Enterprise, WPA-Enterprise ou WPA2-Enterprise. Valeurs possibles : • Référence unique • Injection de variable La valeur par défaut est Référence unique.
Profils de certificat d'autorité de certification	Ce paramètre spécifie les profils de certificat d'autorité de certification avec les certificats approuvés utilisés par un terminal pour établir une connexion approuvée au réseau Wi-Fi. Ce paramètre est valide uniquement si le paramètre Type de liaison de certificat est défini sur Référence unique.
Noms de certificats approuvés	Ce paramètre spécifie les noms des certificats approuvés utilisés par un terminal pour établir une connexion approuvée au réseau Wi-Fi. Ce paramètre est valide uniquement si le paramètre Type de liaison de certificat est définir sur Injection de variable.
Faire confiance aux décisions d'utilisateur	Ce paramètre spécifie si un terminal doit inviter l'utilisateur à approuver un serveur lorsque la chaine d'approbation ne peut pas être établie. Si ce paramètre n'est pas sélectionné, seules les connexions aux serveurs approuvés que vous spécifiez sont autorisées. Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini sur WEP Enterprise, WPA-Enterprise ou WPA2-Enterprise.

iOS et macOS : paramètre de profil Wi-Fi	Description
Activer le profil de marquage QoS	Ce paramètre indique si vous pouvez activer les marquages L2 et L3 pour le trafic transitant par le réseau Wi-Fi. Ce paramètre s'applique uniquement aux terminaux exécutant iOS 10 et versions ultérieures.
Utiliser QoS pour les appels FaceTime	Ce paramètre indique si le trafic audio et vidéo des appels FaceTime peut utiliser les marquages L2 et L3. Ce paramètre s'applique uniquement aux terminaux exécutant iOS 10 et versions ultérieures.
Utiliser le marquage L2 uniquement pour le trafic QoS	Ce paramètre indique si le trafic transitant par le réseau Wi-Fi utilise uniquement le marquage L2. Ce paramètre s'applique uniquement aux terminaux exécutant iOS 10 et versions ultérieures.
Appliquer le marquage QoS aux applications sélectionnées	Ce paramètre spécifie les ID d'offre des applications pouvant utiliser les marquages L2 et L3. Ce paramètre s'applique uniquement aux terminaux exécutant iOS 10 et versions ultérieures.

Android : paramètres de profil Wi-Fi

Android : paramètre de profil Wi-Fi	Description
Profil proxy associé	Ce paramètre spécifie le profil proxy associé utilisé par un terminal Android pour se connecter à un serveur proxy lorsque le terminal est connecté au réseau Wi-Fi. Les terminaux Android 8.0 et version ultérieure avec les activations Contrôles MDM ou Confidentialité de l'utilisateur ne prennent pas en charge les profils Wi-Fi avec des paramètres proxy. Si un terminal avec l'un de ces types d'activation est mis à niveau vers Android 8.0, les profils Wi-Fi qui sont associées à un profil proxy seront supprimés du terminal.
BSSID	Ce paramètre spécifie l'adresse MAC du point d'accès sans fil du réseau Wi-Fi.
DNS primaire	Ce paramètre spécifie le serveur DNS primaire au format décimal séparé par des points (par exemple, 192.0.2.0). Ce paramètre s'applique uniquement aux terminaux utilisant Samsung KNOX lorsque l'adresse IP est attribuée de façon statique par le réseau de l'entreprise.
DNS secondaire	Ce paramètre spécifie le serveur DNS secondaire au format décimal séparé par des points (par exemple, 192.0.2.0). Ce paramètre s'applique uniquement aux terminaux utilisant Samsung KNOX lorsque l'adresse IP est attribuée de façon statique par le réseau de l'entreprise.

Android : paramètre de profil Wi-Fi	Description
Type de sécurité	Ce paramètre indique le type de sécurité utilisé par le réseau Wi-Fi. Valeurs possibles : • Aucune • Personnel • Entreprise La valeur par défaut est Aucune.
Type de sécurité personnelle	Ce paramètre indique le type de sécurité personnelle utilisé par le réseau Wi-Fi. Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini sur Personnelle. Valeurs possibles : • Aucune • WEP personnel • WPA-Personal/WPA2-Personal La valeur par défaut est Aucune.
Clé WEP	Ce paramètre spécifie la clé WEP du réseau Wi-Fi. La clé WEP doit contenir 10 ou 26 caractères hexadécimaux (0-9, A-F) ou 5 ou 13 caractères alphanumériques (0-9, A-Z). Exemples de valeurs de clés hexadécimales : ABCDEF0123 ou ABCDEF0123456789ABCDEF0123. Exemples de valeurs de clés alphanumériques : abCD5 ou abCDefGHijKL1. Ce paramètre est valide uniquement si le paramètre Type de sécurité personnelle est défini sur WEP personnel.
Clé pré-partagée	Ce paramètre spécifie la clé pré-partagée du réseau Wi-Fi. Ce paramètre est valide uniquement si le paramètre Type de sécurité personnelle est défini sur WPA-Personal/WPA2-Personal.
Protocole d'authentification	Ce paramètre spécifie la méthode EAP utilisée par le réseau Wi-Fi. Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini sur Entreprise. Valeurs possibles : • TLS • TTLS • PEAP • LEAP La valeur par défaut est TLS. Le protocole LEAP n'est pas pris en charge par les terminaux utilisant Samsung KNOX.

Android : paramètre de profil Wi-Fi	Description
Authentification interne	Ce paramètre indique la méthode d'authentification interne à utiliser avec TTLS. Ce paramètre est valide uniquement si le paramètre Protocole d'authentification est défini sur TTLS. Valeurs possibles : • Aucune • PAP • CHAP • MS-CHAP • MS-CHAPv2 • GTC La valeur par défaut est MS-CHAPv2. Le protocole CHAP n'est pas pris en charge par les terminaux utilisant Samsung KNOX.
Identité Externe pour TTLS	Ce paramètre spécifie l'identité externe d'un utilisateur envoyée en clair. Vous pouvez spécifier un nom d'utilisateur anonyme pour masquer l'identité réelle de l'utilisateur (par exemple, anonyme). Le tunnel crypté est utilisé pour envoyer le nom d'utilisateur réel à des fins d'authentification auprès du réseau Wi-Fi. Si l'identité externe comprend le nom de domaine pour l'acheminement de la demande, il doit correspondre au domaine réel de l'utilisateur (par exemple, anonyme@exemple.com). Ce paramètre est valide uniquement si le paramètre Protocole d'authentification est défini sur TTLS.
Identité Externe pour PEAP	Ce paramètre spécifie l'identité externe d'un utilisateur envoyée en clair. Vous pouvez spécifier un nom d'utilisateur anonyme pour masquer l'identité réelle de l'utilisateur (par exemple, anonyme). Le tunnel crypté est utilisé pour envoyer le nom d'utilisateur réel à des fins d'authentification auprès du réseau Wi-Fi. Si l'identité externe comprend le nom de domaine pour l'acheminement de la demande, il doit correspondre au domaine réel de l'utilisateur (par exemple, anonyme@exemple.com). Ce paramètre est valide uniquement si le paramètre Protocole d'authentification est défini sur PEAP.
Nom d'utilisateur	Ce paramètre spécifie le nom d'utilisateur utilisé par un terminal Android pour s'authentifier auprès du réseau Wi-Fi. Si le profil concerne plusieurs utilisateurs, vous pouvez utiliser la variable %UserName%. Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini sur Entreprise.
Utiliser le mot de passe inclus dans le profil Wi-Fi	Ce paramètre spécifie si le profil Wi-Fi inclut le mot de passe à des fins d'authentification. Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini sur Entreprise.

Android : paramètre de profil Wi-Fi	Description
Mot de passe,	Ce paramètre spécifie le mot de passe utilisé par un terminal Android pour s'authentifier auprès du réseau Wi-Fi. Ce paramètre est valide uniquement si le paramètre Utiliser le mot de passe inclus dans le profil Wi-Fi est sélectionné.
Type d'authentification	Ce paramètre spécifie le type d'authentification utilisé par un terminal Android pour se connecter au réseau Wi-Fi. Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini sur Entreprise. Valeurs possibles : • Aucune • Certificat partagé • SCEP • Informations d'identification de l'utilisateur La valeur par défaut est Aucune.
Type de liaison de certificat	Ce paramètre spécifie le type de liaison du certificat client associé au profil Wi-Fi. Ce paramètre est valide uniquement si le paramètre Type d'authentification est défini sur Certificat partagé. Valeurs possibles : • Référence unique • Injection de variable La valeur par défaut est Référence unique.
Profil de certificat partagé	Ce paramètre spécifie le profil de certificat partagé avec le certificat client utilisé par un terminal Android pour s'authentifier auprès du réseau Wi-Fi. Ce paramètre est valide uniquement si le paramètre Type de liaison de certificat est défini sur Référence unique. Le nom du profil de certificat partagé doit contenir moins de 36 caractères pour les terminaux utilisant un KNOX Workspace.
Profil SCEP associé	Ce paramètre spécifie le profil SCEP associé utilisé par un terminal Android pour obtenir un certificat client et s'authentifier auprès du réseau Wi-Fi. Ce paramètre est valide uniquement si le paramètre Type d'authentification est défini sur SCEP. Le nom du profil SCEP doit contenir moins de 36 caractères pour les terminaux utilisant un KNOX Workspace.

Android : paramètre de profil Wi-Fi	Description
Profil des informations d'identification de l'utilisateur associé	Ce paramètre spécifie le profil d'informations d'identification de l'utilisateur associé utilisé par un terminal Android pour obtenir un certificat client et s'authentifier auprès du réseau Wi-Fi. Ce paramètre est valide uniquement si le paramètre Type d'authentification est défini sur Informations d'identification de l'utilisateur. Le nom du profil d'informations d'identification doit contenir moins de 36 caractères pour les terminaux utilisant un KNOX Workspace.
Nom du certificat client	Ce paramètre spécifie le nom du certificat client utilisé par un terminal Android pour s'authentifier auprès du réseau Wi-Fi. Ce paramètre est valide uniquement si le paramètre Type de liaison de certificat est définir sur Injection de variable.
Noms usuels de certificat attendus par le serveur d'authentification	Ce paramètre spécifie les noms usuels du certificat envoyés par le serveur d'authentification au terminal (par exemple, * .exemple.com). Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini sur Entreprise.
Type de liaison de certificat	Ce paramètre spécifie le type de liaison des certificats client associés au profil Wi-Fi. Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini sur Entreprise. Valeurs possibles : • Référence unique • Injection de variable La valeur par défaut est Référence unique.
Profil du certificat d'autorité de certification	Ce paramètre spécifie le profil de certificat d'autorité de certification avec le certificat client utilisé par un terminal Android pour établir une connexion approuvée au réseau Wi-Fi. Ce paramètre est valide uniquement si le paramètre Type de liaison de certificat est défini sur Référence unique.
Noms de certificats approuvés	Ce paramètre spécifie les noms des certificats approuvés utilisés par un terminal Android pour établir une connexion approuvée au réseau Wi-Fi. Ce paramètre est valide uniquement si le paramètre Type de liaison de certificat est définir sur Injection de variable.

Windows : paramètres de profil Wi-Fi

Windows : paramètre de profil Wi-Fi	Description
Se connecter automatiquement lorsque ce réseau est à portée	Ce paramètre spécifie si les terminaux peuvent se connecter automatiquement au réseau Wi-Fi. Ce paramètre s'applique aux terminaux exécutant Windows Phone 8.1 et versions ultérieures.
Type de sécurité	Ce paramètre indique le type de sécurité utilisé par le réseau Wi-Fi. Valeurs possibles : • Ouvert • WPA-Enterprise • WPA-Personal • WPA2-Enterprise • WPA2-Personal La valeur par défaut est « Ouvert ».
Type de cryptage	Ce paramètre spécifie la méthode de cryptage utilisée par le réseau Wi-Fi. Le paramètre Type de sécurité détermine les types d'authentification pris en charge et la valeur par défaut de ce paramètre. Valeurs possibles : • Aucune • WEP • TKIP • AES
Clé WEP	Ce paramètre spécifie la clé WEP du réseau Wi-Fi. La clé WEP doit contenir 10 ou 26 caractères hexadécimaux (0-9, A-F) ou 5 ou 13 caractères alphanumériques (0-9, A-Z). Exemples de valeurs de clés hexadécimales : ABCDEF0123 ou ABCDEF0123456789ABCDEF0123. Exemples de valeurs de clés alphanumériques : abCD5 ou abCDefGHijKL1. Ce paramètre est valide uniquement si le paramètre « Type de sécurité » est défini sur « Ouvert » et le paramètre « Type de cryptage » sur « WEP ».
Index de clé	Ce paramètre spécifie la position de la clé correspondante stockée sur le point d'accès sans fil. Ce paramètre est valide uniquement si le paramètre « Type de sécurité » est défini sur « Ouvert » et le paramètre « Type de cryptage » sur « WEP ». Les valeurs possibles sont comprises entre 1 et 4. La valeur par défaut est 60.

Windows : paramètre de profil Wi-Fi	Description
Clé pré-partagée	Ce paramètre spécifie la clé pré-partagée du réseau Wi-Fi. Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur WPA-Personal.
Activer l'identification unique	Ce paramètre spécifie si le réseau Wi-Fi prend en charge l'authentification avec identification unique. Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini WPA-Enterprise ou WPA2-Enterprise.
Type d'identification unique	Ce paramètre spécifie le moment où l'authentification avec identification unique intervient. Lorsque ce paramètre est défini sur Exécuter immédiatement avant la connexion d'utilisateur, l'identification unique est exécutée avant que l'utilisateur se connecte à l'instance Active Directory de votre organisation. Lorsque ce paramètre est défini sur Exécuter immédiatement après la connexion d'utilisateur, l'identification unique est exécutée après que l'utilisateur se connecte à l'instance Active Directory de votre organisation. Ce paramètre est valide uniquement si le paramètre Activer VPN à la demande est sélectionné. Valeurs possibles : • Exécuter immédiatement avant la connexion d'utilisateur • Exécuter immédiatement après la connexion d'utilisateur La valeur par défaut est Exécuter immédiatement avant la connexion d'utilisateur.
Délai de connectivité maximum	Ce paramètre spécifie, en secondes, le délai maximum avant que la tentative de connexion avec identification unique échoue. Ce paramètre est valide uniquement si le paramètre Activer VPN à la demande est sélectionné. Les valeurs possibles sont comprises entre 0 et 120 secondes. La valeur par défaut est de 10 secondes.
Autoriser l'affichage de boites de dialogue supplémentaires lors de l'identification unique	Ce paramètre indique si un terminal peut afficher des boites de dialogue au-delà de l'écran de connexion. Par exemple, si un type d'authentification EAP nécessite que l'utilisateur confirme le certificat envoyé par le serveur lors de l'authentification, le terminal peut afficher la boite de dialogue. Ce paramètre est valide uniquement si le paramètre Activer VPN à la demande est sélectionné.
Ce réseau utilise des réseaux LAN virtuels pour l'authentification de l'ordinateur et de l'utilisateur	Ce paramètre spécifie si le réseau VLAN utilisé par un terminal change en fonction des informations de connexion de l'utilisateur Par exemple, si le terminal se trouve sur un réseau VLAN lorsqu'il démarre, puis - selon les autorisations utilisateur - passe sur un autre réseau VLAN après que l'utilisateur se connecte. Ce paramètre est valide uniquement si le paramètre Activer VPN à la demande est sélectionné.

Windows : paramètre de profil Wi-Fi	Description
Valider le certificat du serveur	Ce paramètre spécifie si un terminal doit valider le certificat du serveur qui vérifie l'identité du point d'accès sans fil. Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini WPA-Enterprise ou WPA2-Enterprise.
Ne pas inviter l'utilisateur à autoriser de nouveaux serveurs ou des autorités de certification approuvées	Ce paramètre spécifie si un utilisateur est invité à approuvé le certificat du serveur. Ce paramètre est valide uniquement si le paramètre Valider le certificat du serveur est sélectionné.
Profils de certificat d'autorité de certification	Ce paramètre spécifie le profil de certificat d'autorité de certification fournissant la racine approuvée pour le certificat du serveur utilisé par le point d'accès sans fil. Ce paramètre limite les autorités de certification racine que les terminaux approuvent avec les autorités de certification sélectionnées. Si vous ne sélectionnez aucune autorité de certification racine approuvée, les terminaux approuvent toutes les autorités de certification racine de leur magasin d'autorités de certification racine approuvées. Ce paramètre est valide uniquement si le paramètre Valider le certificat du serveur est sélectionné.
Activer la reconnexion rapide	Ce paramètre spécifie si le réseau Wi-Fi prend en charge la reconnexion rapide à des fins d'authentification PEAP sur plusieurs points d'accès sans fil. Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini WPA-Enterprise ou WPA2-Enterprise.
Appliquer la protection NAP	Ce paramètre spécifie si le réseau Wi-Fi utilise la protection NAP pour contrôler l'intégrité du système sur les terminaux et vérifier si ceux-ci répondent aux exigences d'intégrité avant d'être autorisés à se connecter au réseau. Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini WPA-Enterprise ou WPA2-Enterprise.
Activer le mode FIPS	Ce paramètre spécifie si le réseau Wi-Fi prend en charge la conformité avec la norme FIPS 140-2. Ce paramètre est valide uniquement si le paramètre « Type de passerelle » est défini sur « WPA2-Enterprise » ou « WPA2-Personal » et le « Type d'authentification » sur « AES ». Ce paramètre s'applique aux terminaux exécutant Windows Phone 8.1 et versions ultérieures.
Activer la mise en cache du PMK	Ce paramètre spécifie si un terminal peut mettre en cache le PMK pour activer l'itinérance rapide WPA2. L'itinérance rapide ignore les paramètres 802.1X avec un point d'accès sans fil auprès duquel le terminal s'est précédemment authentifié. Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini sur WPA2-Enterprise.

Windows : paramètre de profil Wi-Fi	Description
Durée de vie du PMK	Ce paramètre spécifie la durée, en minutes, pendant laquelle un terminal peut stocker le PMK dans le cache. Ce paramètre est valide uniquement si le paramètre Activer S/MIME est sélectionné. Les valeurs possibles sont comprises entre 10 et 1440 minutes. La valeur par défaut est 15 minutes.
Nombre d'entrées du cache du PMK	Ce paramètre spécifie le nombre maximum d'entrées du PMK qu'un terminal peut stocker dans le cache. Ce paramètre est valide uniquement si le paramètre Activer S/MIME est sélectionné. Les valeurs possibles sont comprises entre 1 et 255. La valeur par défaut est 128.
Ce réseau utilise la pré-authentification	Ce paramètre spécifie si le point d'accès prend en charge la pré-authentification pour l'itinérance rapide WPA2. La pré-authentification permet aux terminaux de se connecter à un point d'accès sans fil pour utiliser les paramètres 802.1X avec d'autres points d'accès sans fil à portée. La pré-authentification stocke le PMK et les informations qui s'y rapportent dans le cache du PMK. Lorsque le terminal se connecte à un point d'accès sans fil auprès duquel il s'est pré-authentifié, il utilise les informations mises en cache dans le PMK pour réduire le délai d'authentification et de connexion. Ce paramètre est valide uniquement si le paramètre Activer S/MIME est sélectionné.
Tentatives de pré-authentification maximum	Ce paramètre spécifie le nombre maximum de tentatives de pré-authentification autorisées. Ce paramètre est valide uniquement si le paramètre « Ce réseau utilise une pré-authentification » est sélectionné. Les valeurs possibles sont comprises entre 1 et 16. La valeur par défaut est 3.
Type de proxy	Ce paramètre spécifie le type de configuration proxy pour le profil Wi-Fi. Réglages possibles : • Aucun • Configuration PAC • Configuration manuelle • Web Proxy Autodiscovery La valeur par défaut est « Configuration manuelle ». Ce paramètre s'applique uniquement aux terminaux Windows 10 Mobile.

Windows : paramètre de profil Wi-Fi	Description
URL du fichier PAC	Ce paramètre spécifie l'URL du serveur Web qui héberge le fichier PAC et le nom du fichier PAC au format http://<web_server_URL>/<filename>.pac. Ce paramètre est valide uniquement si le paramètre Type de proxy est défini sur Configuration PAC.
Adresse	Ce paramètre spécifie le nom du serveur et le port du proxy du réseau. Utilisez le format hôte:port (par exemple, server01.example.com:123). L'hôte doit être l'un des suivants : • un nom enregistré (ex. : nom de serveur), un nom de domaine complet ou un nom d'étiquette unique (par exemple, serveur01 au lieu de serveur01.exemple.com) • une adresse IPv4 ou IPv6 Ce paramètre est valide uniquement si le paramètre Type de proxy est défini sur Configuration manuelle.
Web Proxy Autodiscovery	Ce paramètre permet d'activer le Web Proxy Autodiscovery Protocol (WPAD) pour la recherche de proxy. Ce paramètre est valide uniquement si le paramètre « Type de proxy » est défini sur « Web Proxy Autodiscovery ». Par défaut, cette case n'est pas cochée.
Désactiver les vérifications de la connectivité Internet	Ce paramètre permet de désactiver les vérifications de la connectivité Internet. Par défaut, cette case n'est pas cochée. Ce paramètre s'applique uniquement aux terminaux Windows 10.
Profil SCEP associé	Ce paramètre spécifie le profil SCEP associé utilisé par un terminal pour obtenir un certificat client et s'authentifier auprès du réseau Wi-Fi. Ce paramètre s'applique uniquement aux terminaux Windows 10.

Paramètres du profil VPN

Vous pouvez utiliser une variable de paramètre de profil correspondant à un champ de texte pour faire référence à une valeur plutôt que de spécifier la valeur réelle. BlackBerry UEM prend en charge les variables par défaut prédéfinies et les variables personnalisées que vous définissez. Les profils VPN sont pris en charge sur les types de terminaux suivants :

- BlackBerry 10
- iOS
- macOS
- Samsung KNOX Workspace
- Windows 10

Dans certains cas, la version minimale du système d'exploitation du terminal requis pour prendre en charge un paramètre correspondant à une version non prise en charge par BlackBerry UEM. Pour plus d'informations sur les versions de système d'exploitation prises en charge, reportez-vous à la matrice de compatibilité.

BlackBerry 10 : paramètres de profil VPN

BlackBerry 10 : paramètre de profil VPN	Description
Activer VPN à la demande	Ce paramètre indique si un VPN à la demande est activé pour ce profil VPN. Si ce paramètre est sélectionné, vous pouvez spécifier les applications utilisant ce profil VPN. Seules les applications spécifiées dans ce profil sont autorisées à utiliser ce profil. Pour utiliser un VPN à la demande, vérifiez que les applications spécifiées sont développées pour utiliser un VPN à la demande, que les applications sont attribuées aux utilisateurs de terminaux BlackBerry 10 et que ce profil VPN est attribué aux utilisateurs de terminaux. La configuration minimale requise est BlackBerry 10 OS version 10.3.3.
Adresse du serveur	Ce paramètre spécifie le FQDN ou l'adresse IP d'un serveur VPN.
Type de passerelle	Ce paramètre indique le type de client VPN que le client VPN d'un terminal BlackBerry 10 émule. Valeurs possibles : • Check Point VPN-1 • Cisco VPN 3000 Series Concentrator • Cisco Secure PIX Firewall • Cisco IOS Easy VPN • Cisco ASA Series • Cisco AnyConnect • Juniper SRX Series (VPN IPsec) • Juniper MAG Series ou Juniper SA Series (VPN SSL) • Serveur Microsoft VPN IKEv2 • Serveur générique VPN IKEv2 • Serveur VPN IKEv2 conforme NIAP La valeur par défaut est Check Point VPN-1.
Type d'authentification	Ce paramètre spécifie le type d'authentification de la passerelle VPN. Le paramètre Type de passerelle détermine les types d'authentification pris en charge et la valeur par défaut de ce paramètre. Valeurs possibles : • PSK • PKI • XAUTH-PSK • XAUTH-PKI • EAP-TLS • EAP-MS-CHAPv2

BlackBerry 10 : paramètre de profil VPN	Description
Clé pré-partagée ou mot de passe de groupe	Ce paramètre spécifie la clé pré-partagée ou le mot de passe de groupe pour la passerelle VPN. Ce paramètre est valide uniquement si le paramètre Type d'authentification est défini sur PSK ou XAUTH-PSK.
Nom d'utilisateur	Ce paramètre spécifie le nom d'utilisateur utilisé par un terminal BlackBerry 10 pour s'authentifier auprès de la passerelle VPN. Si le profil concerne plusieurs utilisateurs, vous pouvez utiliser la variable %UserName%. Ce paramètre est valide uniquement si le paramètre Type de passerelle est défini sur Cisco AnyConnect ou si le paramètre Type d'authentification est défini sur XAUTH-PSK ou XAUTH-PKI.
Jeton physique	Ce paramètre spécifie si un utilisateur doit utiliser un jeton physique pour s'authentifier auprès de la passerelle VPN. Ce paramètre est valide uniquement si le paramètre Type d'authentification est défini sur XAUTH-PSK ou XAUTH-PKI.
Mot de passe,	Ce paramètre spécifie le mot de passe utilisé par un BlackBerry 10 pour s'authentifier auprès de la passerelle VPN. Ce paramètre est valide uniquement si le paramètre Type de passerelle est défini sur Cisco AnyConnect ou si le paramètre Type d'authentification est défini sur XAUTH-PSK ou XAUTH-PKI et que le paramètre Jeton physique n'est pas sélectionné.
Identité EAP	Ce paramètre spécifie l'identité EPA utilisée par un terminal BlackBerry 10 pour s'authentifier auprès de la passerelle VPN. Ce paramètre est valide uniquement si le paramètre Type d'authentification est défini sur EAP-TLS.
ID de passerelle EAP-TLS	Ce paramètre n'est valide que si le Type de passerelle est défini sur Serveur VPN IKEv2 conforme NIAP et si le Type d'authentification est défini sur EAP-TLS. La configuration minimale requise est BlackBerry 10 OS version 10.3.3.
Identité MS-CHAPv2 EAP	Ce paramètre spécifie l'identité MS-CHAPv2 EAP utilisée par un terminal BlackBerry 10 pour s'authentifier auprès de la passerelle VPN. Ce paramètre est valide uniquement si le paramètre Type d'authentification est défini sur EAP-MS-CHAPv2.
Nom d'utilisateur MS-CHAPv2	Ce paramètre spécifie l'identité MS-CHAPv2 utilisée par un terminal BlackBerry 10 pour s'authentifier auprès de la passerelle VPN. Ce paramètre est valide uniquement si le paramètre Type d'authentification est défini sur EAP-MS-CHAPv2.

BlackBerry 10 : paramètre de profil VPN	Description
Mot de passe MS-CHAPv2	Ce paramètre spécifie le mot de passe MS-CHAPv2 utilisé par un terminal BlackBerry 10 pour s'authentifier auprès de la passerelle VPN. Ce paramètre est valide uniquement si le paramètre Type d'authentification est défini sur EAP-MS-CHAPv2.
Type d'ID d'authentification	Ce paramètre spécifie le type d'ID d'authentification de la passerelle VPN. Ce paramètre est valide uniquement si le paramètre Type de passerelle est défini sur Juniper MAG Series ou Juniper SA Series (VPN SSL), serveur VPN IKEv2 Microsoft, serveur VPN générique IKEv2 ou serveur VPN IKEv2 conforme NIAP. Le paramètre Type de passerelle détermine les types d'ID d'authentification pris en charge et la valeur par défaut de ce paramètre. Valeurs possibles : • IPv4 • Nom de domaine complet • Adresse e-mail, • Nom distinctif du certificat d'identité • Nom général du certificat d'identité • ID de clé
ID d'authentification ou nom de groupe	Ce paramètre spécifie l'ID d'authentification ou le nom de groupe pour la passerelle VPN. Ce paramètre est valide uniquement si le paramètre Type de passerelle est défini sur Juniper MAG Series ou Juniper SA Series (VPN SSL), serveur VPN IKEv2 Microsoft ou serveur VPN générique IKEv2 ou si le paramètre Type d'authentification est défini sur PSK ou XAUTH-PSK.
Type d'authentification de passerelle	Ce paramètre spécifie le type d'authentification de la passerelle VPN. Ce paramètre est valide uniquement si le paramètre Type de passerelle est défini sur Juniper MAG Series ou Juniper SA Series (VPN SSL), serveur VPN IKEv2 Microsoft ou serveur VPN générique IKEv2. Valeurs possibles : • Aucune • PSK • PKI La valeur par défaut est Aucune.
Activer la vérification OCSP/CRL sur les certificats à partir du VPN	Ce paramètre active la vérification de la révocation de certificat pour les certificats utilisés pendant l'authentification. Ce paramètre n'est valide que si le Type de passerelle est défini sur Serveur VPN IKEv2 conforme NIAP et si le Type d'authentification est défini sur PKI ou EAP-TLS. La configuration minimale requise est BlackBerry 10 OS version 10.3.3.

BlackBerry 10 : paramètre de profil VPN	Description
Clé pré-partagée de passerelle	Ce paramètre spécifie la clé pré-partagée de la passerelle VPN. Ce paramètre est valide uniquement si le paramètre Type d'authentification de passerelle est défini sur PSK.
Type d'ID d'authentification de passerelle	Ce paramètre spécifie l'ID d'authentification de la passerelle VPN. Ce paramètre est valide uniquement si le paramètre Type de passerelle est défini sur Juniper MAG Series ou Juniper SA Series (VPN SSL), serveur VPN IKEv2 Microsoft ou serveur VPN générique IKEv2. Valeurs possibles : • IPv4 • Nom de domaine complet • Adresse e-mail, • Nom distinctif du certificat d'identité • Nom général du certificat d'identité • ID de clé La valeur par défaut est IPv4.
ID d'authentification de passerelle	Ce paramètre spécifie l'ID d'authentification de la passerelle VPN. Ce paramètre est valide uniquement si le paramètre Type d'ID d'authentification de passerelle est défini sur Nom de domaine complet ou Adresse électronique.
Envoyer l'ID de demande de passerelle supplémentaire dans le message 1 du protocole IKEv2	La valeur par défaut est Désactivé. Ce paramètre est valide uniquement si le paramètre Type de passerelle est défini sur Serveur VPN IKEv2 conforme NIAP. La configuration minimale requise est BlackBerry 10 OS version 10.3.3.
Type d'ID de passerelle demandé	Ce paramètre spécifie le type d'ID de passerelle du VPN. Ce paramètre n'est valide que si le Type de passerelle est défini sur Serveur VPN IKEv2 conforme NIAP et si le paramètre « Envoyez l'ID de passerelle demandé dans le message 1 du protocole IKEv2 est sélectionné. Valeurs possibles : • IPv4 • Nom de domaine complet • Adresse e-mail, • Nom distinctif du certificat d'identité • Nom général du certificat d'identité • ID de clé La valeur par défaut est IPv4. La configuration minimale requise est BlackBerry 10 OS version 10.3.3.

BlackBerry 10 : paramètre de profil VPN	Description
ID de passerelle demandé	Ce paramètre requiert un ID de passerelle spécifique dans le premier message IKE au cours de la connexion, si le serveur VPN prend en charge plusieurs identifiants. Peut être différent de celui de l'ID de la passerelle utilisé pour l'authentification. Ce paramètre n'est valide que si le Type de passerelle est défini sur Serveur VPN IKEv2 conforme NIAP et si le paramètre « Envoyez l'ID de passerelle demandé dans le message 1 du protocole IKEv2 est sélectionné. La configuration minimale requise est BlackBerry 10 OS version 10.3.3.
Nom d'utilisateur secondaire	Ce paramètre spécifie le nom de l'utilisateur utilisé par un terminal BlackBerry 10 à des fins d'authentification secondaire auprès de la passerelle VPN. Si le profil concerne plusieurs utilisateurs, vous pouvez utiliser la variable %UserName%. Ce paramètre est valide uniquement si le paramètre Type de passerelle est défini sur Cisco AnyConnect. La configuration minimale requise est BlackBerry 10 OS version 10.3.1.
Mot de passe secondaire	Ce paramètre spécifie le mot de passe utilisé par un terminal BlackBerry 10 à des fins d'authentification secondaire auprès de la passerelle VPN. Ce paramètre est valide uniquement si le paramètre Type de passerelle est défini sur Cisco AnyConnect. La configuration minimale requise est BlackBerry 10 OS version 10.3.1.
Nom de groupe	Ce paramètre spécifie le nom de groupe pour la passerelle VPN. Ce paramètre est valide uniquement si le paramètre Type de passerelle est défini sur Cisco AnyConnect. La configuration minimale requise est BlackBerry 10 OS version 10.3.1.
Activer le traitement automatique du certificat client	Ce paramètre spécifie si un certificat client est automatiquement sélectionné lorsqu'une connexion VPN est établie. Ce paramètre est valide uniquement si le paramètre Type de passerelle est défini sur Cisco AnyConnect. La configuration minimale requise est BlackBerry 10 OS version 10.3.1.
Activer l'authentification IPsec	Ce paramètre spécifie si la passerelle VPN utilise l'authentification IPsec. Ce paramètre est valide uniquement si le paramètre Type de passerelle est défini sur Cisco AnyConnect. La configuration minimale requise est BlackBerry 10 OS version 10.3.1.

BlackBerry 10 : paramètre de profil VPN	Description
Type d'authentification IPsec	Ce paramètre spécifie le type d'authentification d'une connexion VPN IPsec. Ce paramètre est valide uniquement si le paramètre Activer l'authentification IPsec est sélectionné. Valeurs possibles : • EAP-MS-CHAPv2 • EAP-MD5 • EAP-GTC • EAP-AnyConnect • IKE- RSA La valeur par défaut est EAP-MS-CHAPv2. La configuration minimale requise est BlackBerry 10 OS version 10.3.1.
ID d'authentification EAP	Ce paramètre spécifie l'identité EPA utilisée par un terminal BlackBerry 10 pour s'authentifier auprès de la passerelle VPN. Ce paramètre est valide uniquement si le paramètre Type d'authentification IPSec est défini sur EAP MSCHAPv2, EAP MD5 ou EAP GTC.
Exclure les sous-réseaux	Ce paramètre spécifie si vous souhaitez empêcher des sous-réseaux spécifiques d'utiliser la connexion VPN. Ce paramètre est valide uniquement si le paramètre Type de passerelle est défini sur Cisco AnyConnect. La configuration minimale requise est BlackBerry 10 OS version 10.3.1.
Sous-réseaux exclus	Ce paramètre spécifie les sous-réseaux et masques de sous-réseau qui ne sont pas envoyés via la connexion VPN. Ce paramètre est valide uniquement si le paramètre Exclure des sous-réseaux est sélectionné.
Fichier de configuration Cisco AnyConnect (.xml)	Ce paramètre spécifie l'emplacement du fichier de configuration Cisco AnyConnect envoyé aux terminaux BlackBerry 10. Ce paramètre est valide uniquement si le paramètre Type de passerelle est défini sur Cisco AnyConnect. La configuration minimale requise est BlackBerry 10 OS version 10.3.1.
Autoriser les applications personnelles sur les réseaux professionnels	Ce paramètre spécifie si les applications personnelles d'un terminal BlackBerry 10 peuvent utiliser la connexion VPN. Ce paramètre est valide uniquement si le paramètre Autoriser les applications personnelles à utiliser les réseaux professionnels est sélectionné. La configuration minimale requise est BlackBerry 10 OS version 10.3.1.

BlackBerry 10 : paramètre de profil VPN	Description
Action de certificats non approuvés	Ce paramètre spécifie si un terminal BlackBerry 10 accepte des certificats non approuvés. Si ce paramètre est défini sur Autoriser, le terminal accepte automatiquement les certificats non approuvés. Si cette option est définie sur Invite, l'utilisateur peut choisir d'accepter les certificats non approuvés. Si ce paramètre est défini sur Interdire, le terminal n'accepte pas les certificats non approuvés. Le paramètre Type de passerelle détermine les actions de certificats non approuvés prises en charge et la valeur par défaut de ce paramètre. Valeurs possibles : • Autoriser • Invite • Interdire La configuration minimale requise est BlackBerry 10 OS version 10.3.2.
Source du certificat client	Ce paramètre spécifie la manière dont les terminaux BlackBerry 10 obtiennent le certificat client. Quatre options permettent aux terminaux d'obtenir des certificats client : • Si vous choisissez Carte à puce, l'utilisateur doit coupler le terminal avec une carte à puce contenant le certificat client. • Si vous choisissez SCEP, vous devez également spécifier le profil SCEP associé que le terminal peut utiliser pour télécharger le certificat client. • Si vous choisissez Identifiants de l'utilisateur, vous devez également spécifier le profil des identifiants de l'utilisateur associé que le terminal peut utiliser pour télécharger le certificat client. • Si vous choisissez Autre, l'utilisateur doit manuellement ajouter le certificat client au terminal. Les terminaux exécutant BlackBerry 10 OS version 10.3.1 ou ultérieure prennent en charge la carte à puce. Ce paramètre est valide uniquement si le paramètre Type d'authentification est défini sur PKI ou XAUTH-PKI. Valeurs possibles : • Carte à puce • SCEP • Informations d'identification de l'utilisateur • Autre La valeur par défaut est Autre.
Profil SCEP associé	Ce paramètre spécifie le profil SCEP associé utilisé par un terminal BlackBerry 10 pour obtenir un certificat client et s'authentifier auprès du VPN. Ce paramètre est valide uniquement si le paramètre Source du certificat client est défini sur SCEP.

BlackBerry 10 : paramètre de profil VPN	Description
Profil des informations d'identification de l'utilisateur associé	Ce paramètre spécifie le profil des informations d'identification de l'utilisateur associé utilisé par un terminal BlackBerry 10 pour obtenir un certificat client et s'authentifier auprès du VPN. Ce paramètre est valide uniquement si le paramètre Source du certificat client est défini sur Informations d'identification de l'utilisateur. La configuration minimale pour utiliser un profil des informations d'identification de l'utilisateur est BlackBerry 10 OS version 10.3.1.
Durée de vie IKE	Ce paramètre spécifie la durée de vie de la connexion IKE (en secondes). Si vous définissez une valeur non prise en charge ou une valeur nulle, la valeur par défaut du terminal BlackBerry 10 est utilisée. Les valeurs possibles sont comprises entre 1 et 2 147 483 647.
Seuil IKE	Ce paramètre indique le pourcentage de la durée de vie IKE auquel le client VPN va initier un nouvel échange de clés. Valeurs possibles : 0 à 100 % La valeur par défaut est 90. Ce paramètre est valide uniquement si le paramètre Type de passerelle est défini sur Serveur VPN IKEv2 conforme NIAP. La configuration minimale requise est BlackBerry 10 OS version 10.3.3.
Durée de vie IPsec	Ce paramètre spécifie la durée de vie de la connexion IPsec (en secondes). Si vous définissez une valeur non prise en charge ou une valeur nulle, la valeur par défaut du terminal BlackBerry 10 est utilisée. Les valeurs possibles sont comprises entre 1 et 2 147 483 647.
Seuil IPsec	Ce paramètre indique le pourcentage du seuil IPsec auquel le client VPN va initier un nouvel échange de clés. Valeurs possibles : 0 à 100 % La valeur par défaut est 90. Ce paramètre est valide uniquement si le paramètre Type de passerelle est défini sur Serveur VPN IKEv2 conforme NIAP. La configuration minimale requise est BlackBerry 10 OS version 10.3.3.
Autoriser les extensions VPN	Ce paramètre vous permet d'activer ou de désactiver les extensions. Ce paramètre est valide uniquement si le paramètre Type de passerelle est défini sur Serveur VPN IKEv2 conforme NIAP. La configuration minimale requise est BlackBerry 10 OS version 10.3.3.

BlackBerry 10 : paramètre de profil VPN	Description
Liste des extensions VPN	Ce paramètre vous permet d'entrer une liste d'extensions qui sont utilisées pour générer des charges utiles d'ID de fournisseur et effectuer la validation de certificat supplémentaire. Ce paramètre n'est valide que si le Type de passerelle est défini sur Serveur VPN IKEv2 conforme NIAP et si le paramètre Autoriser les extensions VPN est sélectionné. La configuration minimale requise est BlackBerry 10 OS version 10.3.3.
Exiger l'extension d'ID du fournisseur	Ce paramètre indique que l'administrateur souhaite utiliser l'une des extensions dans la liste d'extensions pour générer une charge utile d'ID fournisseur au cours de la connexion. Ce paramètre n'est valide que si le Type de passerelle est défini sur Serveur VPN IKEv2 conforme NIAP et si le paramètre Autoriser les extensions VPN est sélectionné. La configuration minimale requise est BlackBerry 10 OS version 10.3.3.
Exiger l'extension de validation de certificat	Ce paramètre indique que l'administrateur souhaite utiliser l'une des extensions pour effectuer la validation de certificat supplémentaire. Ce paramètre n'est valide que si le Type de passerelle est défini sur Serveur VPN IKEv2 conforme NIAP et si le paramètre Autoriser les extensions VPN est sélectionné. La configuration minimale requise est BlackBerry 10 OS version 10.3.3.
Activer la reprise de la session	Ce paramètre active les paramètres de reprise de session IKEv2. Si le serveur VPN prend en charge cette fonctionnalité, le client VPN suspend et reprend une session au lieu de se déconnecter et de se reconnecter complètement, chaque fois que la connexion automatique VPN est activée. Ce paramètre est valide uniquement si le paramètre Type de passerelle est défini sur Serveur VPN IKEv2 conforme NIAP. La configuration minimale requise est BlackBerry 10 OS version 10.3.3.
Seuil de ticket	Ce paramètre spécifie à quel pourcentage du seuil de ticket la reprise de la session se produira. Valeurs possibles : 0 à 100 % La valeur par défaut est 90. Ce paramètre n'est valide que si le Type de passerelle est défini sur Serveur VPN IKEv2 conforme NIAP et si le paramètre Activer la reprise de la session est sélectionné. La configuration minimale requise est BlackBerry 10 OS version 10.3.3.

BlackBerry 10 : paramètre de profil VPN	Description
Activer les charges utiles de certificat au format hachage et URL pendant l'IKE	Ce paramètre indique si le client VPN annonce au serveur VPN qu'il prend en charge l'utilisation de IKEv2 pour l'échange de certificats à l'aide des URL et récupère les certificats, si disponible, à partir d'une URL HTTP. Ce paramètre est valide uniquement si le paramètre Type de passerelle est défini sur Serveur VPN IKEv2 conforme NIAP. La configuration minimale requise est BlackBerry 10 OS version 10.3.3.
Activer l'application stricte d'algorithmes approuvés	Ce paramètre indique si l'utilisation d'algorithmes approuvés par le NIAP est strictement appliquée. Ce paramètre est valide uniquement si le paramètre Type de passerelle est défini sur Serveur VPN IKEv2 conforme NIAP. La configuration minimale requise est BlackBerry 10 OS version 10.3.3.
Tunnellisation fractionnée	Ce paramètre spécifie si un terminal BlackBerry 10 peut utiliser la tunnellisation fractionnée pour contourner la passerelle VPN (sous réserve de prise en charge par la passerelle VPN). Ce paramètre n'est pas valide si le paramètre Type de passerelle est défini sur Serveur VPN IKEv2 conforme NIAP.
Désactiver la bannière	Ce paramètre spécifie si un terminal BlackBerry 10 bloque la bannière VPN. Ce paramètre n'est pas valide si le paramètre Type de passerelle est défini sur Serveur VPN IKEv2 conforme NIAP.
Source du certificat approuvé	Ce paramètre spécifie la source du certificat approuvé. Si ce paramètre est défini sur Magasin de certificats approuvé, un terminal BlackBerry 10 peut se connecter à un VPN à l'aide d'un certificat du magasin de certificats. Ce paramètre est valide uniquement si le paramètre Type d'authentification est défini sur PKI ou XAUTH-PKI. Valeurs possibles : • Aucune • Magasin de certificats approuvés La valeur par défaut est Aucune.
Déterminer automatiquement la configuration IP	Ce paramètre spécifie si un terminal BlackBerry 10 détermine automatiquement la configuration IP de la passerelle VPN.
Adresse IP privée	Ce paramètre spécifie l'adresse IP privée de la passerelle VPN. Ce paramètre est valide uniquement si le paramètre Déterminer automatiquement l'IP n'est pas sélectionné.

BlackBerry 10 : paramètre de profil VPN	Description
Masque IP privé	Ce paramètre spécifie le masque d'adresse IP privée de la passerelle VPN. Ce paramètre est valide uniquement si le paramètre Déterminer automatiquement l'IP n'est pas sélectionné.
Sous-réseau	Ce paramètre spécifie le sous-réseau de la passerelle VPN. Ce paramètre est valide uniquement si le paramètre Déterminer automatiquement l'IP n'est pas sélectionné.
Masque de sous-réseau	Ce paramètre spécifie le masque de sous-réseau de la passerelle VPN. Ce paramètre est valide uniquement si le paramètre Déterminer automatiquement l'IP n'est pas sélectionné.
Déterminer automatiquement la configuration DNS	Ce paramètre spécifie si un terminal BlackBerry 10 détermine automatiquement la configuration DNS de la passerelle VPN.
DNS primaire	Ce paramètre spécifie le serveur DNS primaire au format décimal séparé par des points (par exemple, 192.0.2.0). Ce paramètre est valide uniquement si le paramètre Déterminer automatiquement le DNS n'est pas sélectionné.
DNS secondaire	Ce paramètre spécifie le serveur DNS secondaire au format décimal séparé par des points (par exemple, 192.0.2.0). Ce paramètre est valide uniquement si le paramètre Déterminer automatiquement le DNS n'est pas sélectionné.
Suffixe de domaine	Ce paramètre spécifie l'FQDN du suffixe DNS. Ce paramètre est valide uniquement si le paramètre Déterminer automatiquement le DNS n'est pas sélectionné.
Perfect Forward Secrecy (confidentialité totale des transferts)	Ce paramètre spécifie si la passerelle VPN prend en charge PFS. Si ce paramètre est sélectionné, le paramètre Groupe DH IPsec doit être défini sur 0.
Sélection manuelle des algorithmes	Ce paramètre spécifie si vous devez définir les algorithmes cryptographiques de la passerelle VPN.

BlackBerry 10 : paramètre de profil VPN	Description
Groupe DH IKE	Ce paramètre spécifie le groupe DH utilisé par un terminal BlackBerry 10 pour générer les clés. Ce paramètre est valide uniquement si le paramètre Sélection manuelle des algorithmes est sélectionné. Valeurs possibles : • 1 à 26, sauf 3, 4 et 6 • Personnalisé 1 à Personnalisé 5 La valeur par défaut est 1.
Fournisseur DH IKE personnalisé	Ce paramètre spécifie le nom du fournisseur pour DH IKE personnalisé. Ce paramètre est uniquement valide que si le paramètre Groupe DH IKE est défini sur une des valeurs personnalisées.
Activer MOBIKE	Ce paramètre spécifie si la passerelle VPN prend en charge MOBIKE. Ce paramètre est valide uniquement si le paramètre Type de passerelle est défini sur Serveur VPN IKEv2 Microsoft ou Serveur VPN générique IKEv2, le paramètre Type d'authentification sur PKI et le paramètre Groupe DH IKE sur une des valeurs personnalisées. La configuration minimale requise est BlackBerry 10 OS version 10.3.1.
Cryptage IKE	Ce paramètre spécifie l'algorithme utilisé par un terminal BlackBerry 10 pour générer une clé secrète partagée. Ce paramètre est valide uniquement si le paramètre Sélection manuelle des algorithmes est sélectionné. Valeurs possibles : • Aucune • DES (clé 56 bits) • Triple DES (clé 168 bits) • AES (clé 128 bits) • AES (clé 192 bits) • AES (clé 256 bits) La valeur par défaut est Aucune.

BlackBerry 10 : paramètre de profil VPN	Description
Hachage IKE	Ce paramètre spécifie la fonction de hachage utilisée par un terminal BlackBerry 10 avec IKE. Ce paramètre est valide uniquement si le paramètre Sélection manuelle des algorithmes est sélectionné. Valeurs possibles : • Aucune • MD5 • AES-XCBC • SHA-1 • SHA-256 • SHA-384 • SHA-512 La valeur par défaut est Aucune.
PRF IKE	Ce paramètre spécifie la fonction PRF utilisée par un terminal BlackBerry 10 avec IKE. Ce paramètre est valide uniquement si le paramètre Sélection manuelle des algorithmes est sélectionné. Valeurs possibles : • Aucune • HMAC • HMAC-MD5 • AES-XCBC • HMAC-SHA-1 • HMAC-SHA-256 • HMAC-SHA-384 • HMAC-SHA-512 La valeur par défaut est Aucune.
Groupe DH IPsec	Ce paramètre spécifie le groupe DH utilisé par un terminal BlackBerry 10 avec IPsec. Ce paramètre est valide uniquement si le paramètre Sélection manuelle des algorithmes est sélectionné. Les valeurs possibles sont comprises entre 0 et 26, sauf 3, 4 et 6. La valeur par défaut est 0.

BlackBerry 10 : paramètre de profil VPN	Description
Cryptage IPsec	Ce paramètre spécifie l'algorithme utilisé par un terminal BlackBerry 10 avec IPsec. Ce paramètre est valide uniquement si le paramètre Sélection manuelle des algorithmes est sélectionné. Valeurs possibles : • Aucune • DES (clé 56 bits) • Triple DES (clé 168 bits) • AES (clé 128 bits) • AES (clé 192 bits) • AES (clé 256 bits) La valeur par défaut est Aucune.
Hachage IPsec	Ce paramètre spécifie la fonction de hachage utilisée par un terminal BlackBerry 10 avec IPsec. Ce paramètre est valide uniquement si le paramètre Sélection manuelle des algorithmes est sélectionné. Valeurs possibles : • Aucune • MD5 • AES-XCBC • SHA-1 • SHA-256 • SHA-384 • SHA-512 La valeur par défaut est Aucune.
NAT keepalive	Ce paramètre spécifie la fréquence à laquelle un terminal envoie un paquet NAT keepalive. Si vous définissez une valeur non prise en charge ou une valeur nulle, la valeur par défaut du terminal BlackBerry 10 est utilisée. Les valeurs possibles sont comprises entre 1 et 2 147 483 647.
Fréquence DPD	Ce paramètre spécifie la fréquence DPD, en secondes. Un terminal BlackBerry 10prend en charge un minimum de 10 secondes. Si vous définissez une valeur non prise en charge ou une valeur nulle, la valeur par défaut du terminal est utilisée. Les valeurs possibles sont comprises entre 1 et 2 147 483 647.

BlackBerry 10 : paramètre de profil VPN	Description
Modifiable par l'utilisateur	Ce paramètre spécifie les paramètres VPN qu'un utilisateur de terminal BlackBerry 10 peut modifier. Si ce paramètre est défini sur Lecture seule, l'utilisateur ne peut pas modifier les paramètres. Si ce paramètre est défini sur Informations d'identification uniquement, l'utilisateur peut modifier le nom d'utilisateur et le mot de passe. Valeurs possibles : • Lecture seule • Informations d'identification uniquement La valeur par défaut est Lecture seule.
Afficher les informations VPN sur le terminal	Ce paramètre spécifie si les informations VPN s'affichent sur un terminal BlackBerry 10. Si ce paramètre est défini sur Visibles, la plupart des informations du profil VPN s'affichent sur le terminal. Si ce paramètre est défini sur Invisibles, seul le nom du profil s'affiche sur le terminal. Si ce paramètre est défini sur Informations d'identification uniquement, les champs relatifs au nom du profil et aux informations d'identification s'affichent sur le terminal. Valeurs possibles : • Visibles • Invisibles • Informations d'identification uniquement La valeur par défaut est Visibles.
Niveau de sécurité des données	Ce paramètre spécifie le domaine de l'espace Travail où le profil VPN est stocké lorsque l'espace Travail utilise la protection avancée des données inactives. Ce paramètre est uniquement valide si la règle de stratégie informatique « Appliquer la protection avancée des données inactives » est sélectionnée. Si ce paramètre est défini sur Toujours disponible, le profil est stocké dans le domaine de démarrage et disponible lorsque l'espace Travail est verrouillé. Si ce paramètre est défini sur Disponible après authentification, le profil est stocké dans le domaine opérationnel et disponible lorsque l'espace Travail est déverrouillé une fois jusqu'à ce que le terminal redémarre. Si ce paramètre est défini sur Disponible uniquement lorsque l'espace Travail est déverrouillé, le profil est stocké dans le domaine de verrouillage et peut être utilisé pour les connexions VPN uniquement lorsque l'espace Travail est déverrouillé. Valeurs possibles : • Toujours disponible • Disponible après authentification • Disponible uniquement lorsque l'espace Travail est déverrouillé La valeur par défaut est Toujours disponible. La configuration minimale requise est BlackBerry 10 OS version 10.3.1.
Profil proxy associé	Ce paramètre spécifie le profil proxy associé utilisé par un terminal BlackBerry 10 pour se connecter à un serveur proxy lorsque le terminal est connecté au VPN.

iOS et macOS : paramètres de profil VPN

macOS applique les profils aux terminaux ou comptes d'utilisateur. Vous pouvez configurer un profil VPN à appliquer à l'un ou à l'autre.

iOS et macOS : paramètre de profil VPN	Description
Appliquer le profil à	Ce paramètre indique si le profil VPN est appliqué au compte d'utilisateur ou au terminal. Valeurs possibles : • Utilisateur • Terminal Ce paramètre est valide uniquement pour les terminaux macOS.
Type de connexion	Ce paramètre spécifie le type de connexion utilisé par un terminal pour une passerelle VPN. Certains types de connexion requièrent également que les utilisateurs installent l'application VPN sur le terminal. Valeurs possibles : • L2TP • PPTP • IPsec • Cisco AnyConnect • Juniper • Pulse Secure • F5 • SonicWALL Mobile Connect • Aruba VIA • Check Point Mobile • OpenVPN • Personnalisée • IKEv2 La valeur par défaut est L2TP. Certaines valeurs ne sont pas valides pour les terminaux macOS.
ID d'offre VPN	Ce paramètre spécifie l'ID d'offre de l'application VPN pour un VPN SSL personnalisé. L'ID d'offre est au format DNS inversé (par exemple, com.exemple.VPNapp). Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur Personnalisée.
Serveur,	Ce paramètre spécifie le FQDN ou l'adresse IP d'un serveur VPN.
Nom d'utilisateur	Ce paramètre spécifie le nom d'utilisateur utilisé par un terminal pour s'authentifier auprès de la passerelle VPN. Si le profil concerne plusieurs utilisateurs, vous pouvez utiliser la variable %UserName%.

iOS et macOS : paramètre de profil VPN	Description
Valeurs et clés personnalisées	Ce paramètre spécifie les clés et les valeurs associées du VPN SSL personnalisé. Les informations de configuration sont spécifiques à l'application VPN du fournisseur. Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur Personnalisée.
Groupe de connexion ou domaine	Ce paramètre spécifie le groupe de connexion ou le domaine utilisé par la passerelle VPN pour authentifier un terminal iOS. Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur SonicWALL Mobile Connect.
Domaine	Ce paramètre spécifie le nom de domaine d'authentification utilisé par la passerelle VPN pour authentifier un terminal iOS. Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur Juniper ou Pulse Secure.
Rôle	Ce paramètre spécifie le nom du rôle d'utilisateur utilisé par la passerelle VPN pour vérifier les ressources réseau auxquelles un terminal iOS peut accéder. Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur Juniper ou Pulse Secure.
Type d'authentification	Ce paramètre spécifie le type d'authentification de la passerelle VPN. Le paramètre Type de connexion détermine les types d'authentification pris en charge et la valeur par défaut de ce paramètre. Valeurs possibles : • Mot de passe, • RSA SecurID • Secret partagé/Nom de groupe • Certificat partagé • SCEP • Informations d'identification de l'utilisateur
Mot de passe,	Ce paramètre spécifie le mot de passe utilisé par un terminal pour s'authentifier auprès de la passerelle VPN. Ce paramètre est valide uniquement si le paramètre Type d'authentification est défini sur Mot de passe.
Nom de groupe	Ce paramètre spécifie le nom de groupe pour la passerelle VPN. Ce paramètre est valide uniquement dans les conditions suivantes : • Le paramètre Type de connexion est défini sur Cisco AnyConnect. • Le paramètre Type de connexion est défini sur IPsec et le paramètre Type d'authentification est défini sur Secret partagé/Nom de groupe.

iOS et macOS : paramètre de profil VPN	Description
Secret partagé	Ce paramètre spécifie le secret partagé à utiliser pour l'authentification VPN. Ce paramètre est valide uniquement dans les conditions suivantes : • Le paramètre Type de connexion est défini sur L2TP. • Le paramètre Type de connexion est défini sur IPsec et le paramètre Type d'authentification est défini sur Secret partagé/Nom de groupe. • Le paramètre Type de connexion est défini sur IKEv2 et le paramètre Méthode d'authentification est défini sur Secret partagé.
Profil de certificat partagé	Ce paramètre spécifie le profil de certificat partagé avec le certificat client utilisé par un terminal pour s'authentifier auprès de la passerelle VPN. Ce paramètre est valide uniquement si le paramètre Type d'authentification ou le paramètre Méthode d'authentification est défini sur Certificat partagé.
Profil SCEP associé	Ce paramètre spécifie le profil SCEP associé utilisé par un terminal iOS pour obtenir un certificat client et s'authentifier auprès du VPN. Ce paramètre est valide uniquement si le paramètre Type d'authentification ou le paramètre Méthode d'authentification est défini sur SCEP.
Profil des informations d'identification de l'utilisateur associé	Ce paramètre spécifie le profil d'informations d'identification de l'utilisateur associé utilisé par un terminal pour obtenir un certificat client et s'authentifier auprès du VPN. Ce paramètre est valide uniquement si le paramètre Type d'authentification ou le paramètre Méthode d'authentification est défini sur Identifiants de l'utilisateur.
Niveau de cryptage	Ce paramètre spécifie le niveau de cryptage des données pour la connexion VPN. Si ce paramètre est défini sur Automatique, tous les niveaux de cryptage sont autorisés. Si ce paramètre est défini sur Maximum, seul le cryptage maximum est autorisé. Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur PPTP. Valeurs possibles : • Aucune • Automatique • Maximum La valeur par défaut est Aucune.
Acheminer le trafic réseau via VPN	Ce paramètre spécifie si vous souhaitez acheminer le trafic réseau via une connexion VPN. Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur L2TP ou PPTP.

iOS et macOS : paramètre de profil VPN	Description
Utiliser une authentification hybride	Ce paramètre spécifie si vous souhaitez utiliser un certificat côté serveur pour l'authentification. Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur IPsec et le paramètre Type d'authentification sur Secret partagé/Nom de groupe.
Demander un mot de passe	Ce paramètre spécifie si un terminal invite l'utilisateur à saisir un mot de passe. Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur IPsec et le paramètre Type d'authentification sur Secret partagé/Nom de groupe.
Demander un code PIN à l'utilisateur	Ce paramètre spécifie si le terminal invite l'utilisateur à saisir un code PIN. Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur IPsec et le paramètre Type d'authentification sur Certificat partagé, SCEP ou Informations d'identification de l'utilisateur.
Adresse distante	Ce paramètre spécifie l'adresse IP ou le nom d'hôte du serveur VPN. Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur IKEv2.
ID local	Ce paramètre spécifie l'identité du client IKEv2 dans l'un des formats suivants : FQDN, UserFQDN, Adresse et ASN1DN. Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur IKEv2.
ID distant	Ce paramètre spécifie l'identifiant distant du client IKEv2 à l'aide de l'un des formats suivants : FQDN, FQDN de l'utilisateur, Adresse ou ASN1DN. Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur IKEv2.
Méthode d'authentification	Ce paramètre spécifie la méthode d'authentification du VPN. Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur IKEv2. Valeurs possibles : • Secret partagé • Certificat partagé • SCEP • Informations d'identification de l'utilisateur

iOS et macOS : paramètre de profil VPN	Description
Activer VPN à la demande	Ce paramètre spécifie si un terminal peut automatiquement établir une connexion VPN lorsqu'il accède à certains domaines. Pour les terminaux iOS, ce paramètre s'applique aux applications professionnelles. Ce paramètre est valide uniquement dans les conditions suivantes : • Le paramètre Type de connexion est défini sur IPsec, Cisco AnyConnect, Juniper, Pulse Secure, F5, SonicWALL Mobile Connect, Aruba VIA, Check Point Mobile, OpenVPN ou Personnalisée et le paramètre Type d'authentification sur Certificat partagé, SCEP ou Identifiants de l'utilisateur. • Le paramètre Type de connexion est défini sur IKEv2 et le paramètre Méthode d'authentification est défini sur Certificat partagé.
Domaine ou noms d'hôte pouvant utiliser un VPN à la demande	Ce paramètre spécifie les domaines et actions associées pour utiliser un VPN à la demande. Ce paramètre est valide uniquement si le paramètre Activer VPN à la demande est sélectionné. Valeurs possibles pour Action à la demande : • Toujours établir • Établir si nécessaire • Ne jamais établir
Règles de VPN à la demande pour iOS 7.0 ou version ultérieure	Ce paramètre spécifie les exigences de connexion pour utiliser un VPN à la demande. Vous devez utiliser une ou plusieurs clés de l'exemple de format de charge utile. Ce paramètre remplace le paramètre Domaine ou noms d'hôte pouvant utiliser un VPN à la demande. Ce paramètre est valide uniquement si le paramètre Activer VPN à la demande est sélectionné.
Activer l'authentification étendue	Ce paramètre spécifie si le VPN prend en charge xAuth. Ce paramètre est valide uniquement si le paramètre « Type de connexion » est défini sur « IKEv2 » ou « IKEv2 Always On ».
Version TLS minimale	Ce paramètre spécifie la version TLS minimale utilisée par les terminaux exécutant iOS 11 et version ultérieure pour l'authentification EAP-TLS. Ce paramètre est valide uniquement si le paramètre Activer xAuth est sélectionné et que le type d'authentification est « Certificat ». Valeurs possibles : • 1.0 • 1.1 • 1.2 Le paramètre par défaut est « 1.0 ».

iOS et macOS : paramètre de profil VPN	Description
Version TLS maximale	Ce paramètre spécifie la version TLS maximale utilisée par les terminaux exécutant iOS 11 et version ultérieure pour l'authentification EAP-TLS. Ce paramètre est valide uniquement si le paramètre Activer xAuth est sélectionné et que le type d'authentification est « Certificat ». Valeurs possibles : • 1.0 • 1.1 • 1.2 Le paramètre par défaut est « 1.2 ».
Intervalle keepalive	Ce paramètre spécifie la fréquence à laquelle un terminal envoie un paquet keepalive. Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur IKEv2. Valeurs possibles : • Désactivée • 30 minutes • 10 minutes • 1 minute Le paramètre par défaut est 10 minutes.
Désactiver MOBIKE	Ce paramètre indique si le MOBIKE est désactivé. Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur IKEv2. La configuration minimale pour les terminaux iOS est iOS 9.
Désactiver la redirection IKEv2	Ce paramètre spécifie si la redirection IKEv2 est désactivée. Si ce paramètre n'est pas coché, la connexion IKEv2 est redirigée si une demande de redirection est reçue à partir du serveur. Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur IKEv2. La configuration minimale pour les terminaux iOS est iOS 9.
Activer Perfect Forward Secrecy (confidentialité totale des transferts)	Ce paramètre spécifie si la passerelle VPN prend en charge le PFS. Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur IKEv2. La configuration minimale pour les terminaux iOS est iOS 9.

iOS et macOS : paramètre de profil VPN	Description
Activer NAT keepalive	Ce paramètre spécifie si la passerelle VPN prend en charge les paquets keepalive NAT. Les paquets keepalive sont utilisés pour maintenir les mappages NAT pour les connexions IKEv2. Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur IKEv2. La configuration minimale pour les terminaux iOS est iOS 9.
Intervalle NAT keepalive	Ce paramètre spécifie la fréquence à laquelle un terminal envoie un paquet NAT keepalive (en secondes). Ce paramètre n'est valide que si le paramètre Type de connexion est défini sur IKEv2 et si le paramètre Activer le keepalive NAT est sélectionné. La valeur minimale, également valeur par défaut, est de 20. La configuration minimale pour les terminaux iOS est iOS 9.
Utiliser les sous-réseaux internes IPv4 et IPv6 IKEv2	Ce paramètre indique si le VPN peut utiliser l'attribut de configuration IKEv2 INTERNAL_IP4_SUBNET et INTERNAL_IP6_SUBNET. Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur IKEv2. La configuration minimale pour les terminaux iOS est iOS 9.
Nom commun du certificat de serveur	Ce paramètre spécifie le nom usuel du certificat envoyé par le serveur IKE au terminal. Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur IKEv2.
Nom commun de l'émetteur du certificat de serveur	Ce paramètre spécifie le nom usuel de l'émetteur du certificat dans le certificat envoyé par le serveur IKE au terminal. Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur IKEv2.
Appliquer les paramètres d'association de sécurité enfant	Ce paramètre spécifie s'il faut appliquer les paramètres d'association de sécurité enfant. Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur IKEv2.
Appliquer les paramètres d'association de sécurité IKE	Ce paramètre spécifie s'il faut appliquer les paramètres d'association de sécurité IKE. Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur IKEv2.

iOS et macOS : paramètre de profil VPN	Description
Groupe DH	Ce paramètre spécifie le groupe DH utilisé par un terminal pour générer les clés. Ce paramètre n'est valide que si le paramètre "Appliquer les paramètres de sécurité d'association enfant" ou "Appliquer les paramètres d'association de sécurité IKE" est sélectionné. Valeurs possibles : • 0 • 1 • 2 • 5 • 14 • 15 • 16 • 17 • 18 Le paramètre par défaut est 2.
Algorithme de cryptage	Ce paramètre spécifie l'algorithme de cryptage IKE. Ce paramètre n'est valide que si le paramètre "Appliquer les paramètres de sécurité d'association enfant" ou "Appliquer les paramètres d'association de sécurité IKE" est sélectionné. Valeurs possibles : • DES • 3DES • AES 128 • AES 256 Le paramètre par défaut est 3DES.
Algorithme d'intégrité	Ce paramètre spécifie l'algorithme d'intégrité IKE. Ce paramètre n'est valide que si le paramètre "Appliquer les paramètres de sécurité d'association enfant" ou "Appliquer les paramètres d'association de sécurité IKE" est sélectionné. Valeurs possibles : • SHA1 96 • SHA1 160 • SHA1 256 • SHA2 384 • SHA2 512 La valeur par défaut est SHA1-96.

iOS et macOS : paramètre de profil VPN	Description
Intervalle de renouvellement de clés	Ce paramètre spécifie la durée de vie de la connexion IKE. Ce paramètre n'est valide que si le paramètre "Appliquer les paramètres de sécurité d'association enfant" ou "Appliquer les paramètres d'association de sécurité IKE" est sélectionné. Les valeurs possibles sont comprises entre 10 et 1440 minutes. La valeur par défaut est 1440.
Activer un VPN par application	Ce paramètre spécifie si la passerelle VPN prend en charge un VPN par application. Cette fonction permet de diminuer la charge d'un VPN d'entreprise. Par exemple, vous pouvez activer un trafic professionnel spécifique sur le VPN, comme l'accès aux serveurs d'applications ou aux pages Web derrière un pare-feu. Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur Cisco AnyConnect, Juniper, Pulse Secure, F5, SonicWALL Mobile Connect, Aruba VIA, Check Point Mobile, OpenVPN, Personnalisée ou IKEv2.
Autoriser la connexion automatique des applications	Ce paramètre spécifie si les applications associées au VPN par application peuvent établir automatiquement la connexion VPN. Ce paramètre est valide uniquement si le paramètre Activer VPN par application est sélectionné.
Domaines Safari	Ce paramètre spécifie les domaines pouvant établir la connexion VPN dans Safari. Ce paramètre est valide uniquement si le paramètre Activer VPN par application est sélectionné.
Tunnellisation du trafic	Ce paramètre indique si le VPN achemine le trafic vers la couche d'application ou la couche IP. Ce paramètre est valide uniquement si le paramètre Activer VPN par application est sélectionné. Valeurs possibles : • Couche d'application • Couche IP La valeur par défaut est Couche d'application.
Profil proxy associé	Ce paramètre spécifie le profil proxy associé utilisé par un terminal iOS pour se connecter à un serveur proxy lorsque le terminal est connecté à la passerelle VPN.

Android : paramètres de profil VPN

Les paramètres de profil VPN suivants sont uniquement pris en charge sur les terminaux Samsung KNOX Workspace.

Pour plus d'informations sur les paramètres de profil VPN pris en charge par les terminaux Samsung KNOX Workspace, reportez-vous à la section Samsung KNOX Paramètres JSON d'un VPN.

Android : paramètre de profil VPN	Description
Adresse du serveur	Ce paramètre spécifie le FQDN ou l'adresse IP d'un serveur VPN.
Type de VPN	Ce paramètre spécifie si un terminal utilise le protocole IPsec ou SSL pour se connecter au serveur VPN. Valeurs possibles : • IPsec • SSL La valeur par défaut est IPsec. L'application VPN Juniper prend uniquement en charge SSL.
Authentification de l'utilisateur requise	Ce paramètre spécifie si un utilisateur de terminal doit fournir un nom d'utilisateur et un mot de passe pour se connecter au serveur VPN.
Nom d'utilisateur	Ce paramètre spécifie le nom d'utilisateur utilisé par un terminal pour s'authentifier auprès de la passerelle VPN. Si le profil concerne plusieurs utilisateurs, vous pouvez utiliser la variable %UserName%. Ce paramètre est valide uniquement si le paramètre Authentification de l'utilisateur requise est sélectionné.
Mot de passe,	Ce paramètre spécifie le mot de passe utilisé par un terminal pour s'authentifier auprès de la passerelle VPN. Ce paramètre est valide uniquement si le paramètre Authentification de l'utilisateur requise est sélectionné.
Type de tunnellisation fractionnée	Ce paramètre spécifie si un terminal peut utiliser la tunnellisation fractionnée pour contourner la passerelle VPN (sous réserve de prise en charge par la passerelle VPN). Valeurs possibles : • Désactivée • Manuel • Auto Si le paramètre Type de VPN est défini sur IPsec, ce paramètre doit être défini sur Désactivé. La valeur par défaut est Désactivé.
Itinéraires de transfert	Ce paramètre spécifie le(s) cheminement(s) contournant la passerelle VPN. Vous pouvez spécifier une ou plusieurs adresses IP. Ce paramètre est valide uniquement si le paramètre Type de VPN est défini sur SSL et le paramètre Type de tunnellisation fractionnée sur Manuel.

Android : paramètre de profil VPN	Description
DPD	Ce paramètre indique si le protocole DPD est activé. Ce paramètre est valide uniquement si le paramètre Type de VPN est défini sur IPsec.
Version IKE	Ce paramètre spécifie la version du protocole IKE à utiliser avec la connexion VPN. Valeurs possibles : • IKEv1 • IKEv2 La valeur par défaut est IKEv1. Ce paramètre est valide uniquement si le paramètre Type de VPN est défini sur IPsec.
Type d'authentification IPsec	Ce paramètre spécifie le type d'authentification d'une connexion VPN IPsec. Le paramètre Version IKE détermine les types d'authentification IPsec pris en charge et la valeur par défaut de ce paramètre. Valeurs possibles : • Certificat • Clé pré-partagée • EAP MD5 • EAP MSCHAPv2 • Hybride RSA • Authentification CAC Ce paramètre est valide uniquement si le paramètre Type de VPN est défini sur IPsec.
Type d'ID de groupe IPsec	Ce paramètre spécifie le type d'ID de groupe IPsec de la connexion VPN. Le paramètre Type d'authentification IPsec détermine les types d'ID de groupe IPsec pris en charge et la valeur par défaut de ce paramètre. Valeurs possibles : • Par défaut • Adresse IPv4 • Nom de domaine complet • FQDN de l'utilisateur • ID de clé IKE Si le paramètre Type d'authentification IPsec correspond à Certificat, ce paramètre est automatiquement défini sur Par défaut. Ce paramètre est valide uniquement si le paramètre Type de VPN est défini sur IPsec.

Android : paramètre de profil VPN	Description
ID de groupe IPsec	Ce paramètre spécifie l'ID de groupe IPsec de la connexion VPN. Ce paramètre est valide uniquement si le paramètre Type de VPN est défini sur IPsec.
Mode d'échange de clé de la phase 1 IKE	Ce paramètre spécifie le mode d'échange de la connexion VPN. Valeurs possibles : • Mode principal • Mode agressif La valeur par défaut est Mode principal. Ce paramètre est valide uniquement si le paramètre Type de VPN est défini sur IPsec.
Durée de vie IKE	Ce paramètre spécifie la durée de vie de la connexion IKE (en secondes). Si vous définissez une valeur non prise en charge ou une valeur nulle, la valeur par défaut du terminal est utilisée. Ce paramètre est valide uniquement si le paramètre Type de VPN est défini sur IPsec.
Algorithme de cryptage IKE	Ce paramètre spécifie l'algorithme de cryptage utilisé pour la connexion IKE. Ce paramètre est valide uniquement si le paramètre Type de VPN est défini sur IPsec.
Algorithme d'intégrité IKE	Ce paramètre indique l'algorithme d'intégrité utilisé pour la connexion IKE. Ce paramètre est valide uniquement si le paramètre « Type de VPN » est défini sur « IPsec » et le paramètre « Version IKE » sur « IKEv2 ».
Groupe DH IPsec	Ce paramètre spécifie le groupe DH utilisé par un terminal pour générer les clés. Les valeurs possibles sont 0, 1, 2, 5 et comprises entre 14 et 26. La valeur par défaut est 0. Ce paramètre est valide uniquement si le paramètre Type de VPN est défini sur IPsec.
Paramètre IPsec	Ce réglage définit le paramètre IPsec utilisé pour la connexion VPN. Ce paramètre est valide uniquement si le paramètre Type de VPN est défini sur IPsec.
Perfect Forward Secrecy (confidentialité totale des transferts)	Ce paramètre spécifie si la passerelle VPN prend en charge PFS. Ce paramètre est valide uniquement si le paramètre Type de VPN est défini sur IPsec.

Android : paramètre de profil VPN	Description
Activer MOBIKE	Ce paramètre spécifie si la passerelle VPN prend en charge MOBIKE. Ce paramètre est valide uniquement si le paramètre Type de VPN est défini sur IPsec.
Durée de vie IPsec	Ce paramètre spécifie la durée de vie de la connexion IPsec (en secondes). Si vous définissez une valeur non prise en charge ou une valeur nulle, la valeur par défaut du terminal est utilisée. Ce paramètre est valide uniquement si le paramètre Type de VPN est défini sur IPsec.
Algorithme de cryptage IPsec	Ce paramètre spécifie l'algorithme de cryptage IPsec utilisé pour la connexion VPN. Ce paramètre est valide uniquement si le paramètre Type de VPN est défini sur IPsec.
Algorithme d'intégrité IPsec	Ce paramètre indique l'algorithme d'intégrité IPsec utilisé pour la connexion VPN. Ce paramètre est valide uniquement si le paramètre « Type de sécurité » est défini sur « Ouvert » et le paramètre « Type de cryptage » sur « WEP ».
Type d'authentification	Ce paramètre spécifie le type d'authentification de la passerelle VPN. Valeurs possibles : • Aucune • Authentification basée sur certificat • Authentification CAC La valeur par défaut est Aucune. Ce paramètre est valide uniquement si le paramètre Type de VPN est défini sur SSL.
Algorithme SSL	Ce paramètre spécifie l'algorithme de cryptage requis pour une connexion VPN SSL. Ce paramètre est valide uniquement si le paramètre « Type de VPN » est défini sur « SSL ».
Ajouter des informations UID/PID	Ce paramètre spécifie si les informations UID et PID sont ajoutées aux paquets envoyés au client VPN. Ce paramètre doit être sélectionné pour l'application VPN Cisco AnyConnect.

Android : paramètre de profil VPN	Description
Chainage de prise en charge	Ce paramètre spécifie comment le chainage VPN est pris en charge. Valeurs possibles : • Chainage de prise en charge • Tunnel extérieur • Tunnel intérieur La valeur par défaut est « Chainage de prise en charge ».
Type de saisie de la chaine fournisseur	Ce paramètre spécifie les paires clé-valeur ou la chaine JSON du VPN. Les informations de configuration sont spécifiques à l'application VPN du fournisseur. Valeurs possibles : • Paires clé-valeur du fournisseur • Valeur JSON du fournisseur La valeur par défaut est Paires valeur-clé du fournisseur.
Paires valeur-clé du fournisseur	Ce paramètre spécifie les clés et les valeurs associées du VPN. Les informations de configuration sont spécifiques à l'application VPN du fournisseur. Ce paramètre est uniquement valide si le paramètre Type de saisie de la chaine fournisseur est défini sur Paires valeur-clé du fournisseur.
Valeur JSON du fournisseur	Ce paramètre spécifie les informations de configuration propres à l'application VPN du fournisseur au format .json. Ce paramètre est uniquement valide si le paramètre Type de saisie de la chaine fournisseur est défini sur Valeur JSON du fournisseur.
ID du progiciel client VPN	Ce paramètre spécifie l'ID de package de l'application VPN.
Essayer automatiquement de se reconnecter après une erreur	Ce paramètre spécifie si la connexion VPN doit être automatiquement redémarrée après que la connexion ait été perdue.
Activer le mode FIPS	Ce paramètre spécifie si le protocole FIPS est activé. L'activation du mode FIPS veille à ce que seuls les algorithmes cryptographiques soient utilisés pour la connexion VPN.
Connectivité d'entreprise pour les terminaux Android comprenant un espace Travail	Ce paramètre indique si les terminaux Samsung KNOX Workspace utilisent une connexion VPN pour toutes les applications dans l'espace Travail ou seulement pour les applications spécifiées. • « VPN à l'échelle du conteneur » utilise une connexion VPN pour toutes les applications dans l'espace Travail sur le terminal. • « VPN par application » utilise une connexion VPN uniquement pour les applications spécifiées.

Android : paramètre de profil VPN	Description
Applications autorisées à utiliser la connexion VPN	Ce paramètre indique les applications dans l'espace Travail qui peuvent utiliser une connexion VPN. Vous pouvez sélectionner les applications dans la liste des applications disponibles ou spécifier l'ID de package d'application. Ce paramètre est valide uniquement si le paramètre « Connectivité d'entreprise pour les terminaux Android comprenant un espace Travail » est défini sur « VPN par application ».
Profil proxy associé	Ce paramètre spécifie le profil proxy associé utilisé par un terminal pour se connecter à un serveur proxy lorsque le terminal est connecté au VPN.

Référence connexe

iOS et macOS : paramètres de profil VPN
Windows 10 : paramètres de profil VPN

Windows 10 : paramètres de profil VPN

Windows : paramètre de profil VPN	Description
Type de connexion	Ce paramètre spécifie le type de connexion utilisé par un terminal Windows 10 pour un VPN. Valeurs possibles : • Microsoft • Junos Pulse • SonicWALL Mobile Connect • F5 • Check Point Mobile • Définition de la connexion manuelle La valeur par défaut est Microsoft.
Serveur,	Ce paramètre spécifie l'adresse IP publique ou routable ou le nom DNS pour le VPN. Ce paramètre peut pointer vers l'IP externe d'un VPN, ou une adresse IP virtuelle pour un parc de serveurs. Ce paramètre est valide uniquement si le Type de connexion est défini sur Microsoft.
Liste d'URL de serveur	Ce paramètre spécifie une liste séparée par des virgules des serveurs au format URL, nom d'hôte ou format IP. Ce paramètre est valide uniquement si le paramètre Type de connexion n'est pas défini sur Microsoft.

Windows : paramètre de profil VPN	Description
Type de stratégie de routage	Ce paramètre spécifie le type de stratégie de routage. Ce paramètre est valide uniquement si le Type de connexion est défini sur Microsoft. Valeurs possibles : • Tunnel fractionné • Appliquer le tunnel La valeur par défaut est Forcer le tunnel.
Type de protocole natif	Ce paramètre spécifie le type de stratégie de routage utilisé par le VPN. Ce paramètre est valide uniquement si le Type de connexion est défini sur Microsoft. Valeurs possibles : • L2TP • PPTP • IKEv2 • Automatique La valeur par défaut est Automatique.
Authentification	Ce paramètre indique la méthode d'authentification utilisée pour le VPN natif. Le paramètre Type de protocole natif détermine les méthodes d'authentification prises en charge et la valeur par défaut de ce paramètre. • Si vous sélectionnez L2TP ou PPTP, les valeurs possibles sont MS-CHAPv2 et EAP. La valeur par défaut est MS-CHAPv2. • Si vous sélectionnez IKEv2, les valeurs possibles sont Méthode utilisateur et Méthode machine. La valeur par défaut est Mode Utilisateur. • Si vous sélectionnez Automatique, la seule valeur possible est EAP. Valeurs possibles : • EAP • MS-CHAPv2 • Méthode utilisateur • Méthode machine
Configuration EAP	Ce paramètre spécifie le code XML de la configuration EAP. Pour plus d'informations sur la génération du code XML de la configuration EAP, visitezhttps://docs.microsoft.com/en-us/windows/client-management/mdm/eap-configuration Ce paramètre est valide uniquement si le paramètre Authentification est défini sur EAP.

Windows : paramètre de profil VPN	Description
Méthode utilisateur	Ce paramètre indique le type d'authentification de méthode utilisateur à utiliser. Ce paramètre est valide uniquement si le paramètre Authentification est défini sur Méthode utilisateur. Valeurs possibles : • EAP
Méthode machine	Ce paramètre indique le type d'authentification de méthode machine à utiliser. Ce paramètre est valide uniquement si le paramètre Authentification est défini sur Méthode machine. Valeur possible : • Certificat
Configuration personnalisée	Ce paramètre indique le blob XML en code HTML pour une configuration de plug-in SSL-VPN spécifique, avec les informations d'authentification envoyées au terminal pour la prise en charge des plug-ins SSL-VPN. Ce paramètre est valide uniquement si le paramètre Type de connexion n'est pas défini sur Microsoft.
Nom de la famille de package de plug-ins	Ce paramètre spécifie le nom de famille de package du VPN SSL personnalisé. Ce paramètre est valide uniquement si le Type de connexion est défini sur Définition de la connexion manuelle.
Clé pré-partagée L2TP	Ce paramètre spécifie la clé pré-partagée utilisée pour une connexion L2TP.
Liste d'applications de déclenchement	Ce paramètre spécifie une liste d'applications qui démarrent la connexion VPN.
Liste d'applications de déclenchement > ID d'application	Ce paramètre identifie une application pour un VPN par application. Valeurs possibles : • Nom de la famille de package. Pour trouver le nom de famille de package, installez l'application et exécutez la commande Windows PowerShell, `Get-AppxPackage`. Pour plus d'informations, visitez http://technet.microsoft.com/en-us/library/hh856044.aspx . • Emplacement d'installation de l'application. Par exemple, C:\Windows\System\notepad.exe .
Liste des itinéraires	Ce paramètre spécifie une liste des itinéraires que le VPN peut emprunter. Si le VPN utilise la tunnellisation fractionnée, une liste des itinéraires est requise.
Adresse du sous-réseau	Ce paramètre spécifie l'adresse IP du préfixe de destination au format d'adresse IPv4 ou IPv6.
Préfixe de sous-réseau	Ce paramètre spécifie le préfixe de sous-réseau du préfixe de destination.

Windows : paramètre de profil VPN	Description
Exclusion	Ce paramètre indique si le routage qui est ajouté doit pointer vers l'interface VPN via la passerelle ou l'interface physique. Si vous cochez la case, le trafic est dirigé vers l'interface physique. Si vous ne la cochez pas, le trafic est dirigé vers le VPN.
Liste des noms de domaines	Ce paramètre spécifie les règles NRPT pour le VPN.
Nom de domaine	Ce paramètre spécifie le nom complet ou le suffixe du domaine.
Serveurs DNS	Ce paramètre spécifie la liste des adresses IP des serveurs DNS en les séparant par des virgules.
Serveur Web proxy	Ce paramètre spécifie l'adresse IP du serveur Web proxy.
Déclencheur de VPN	Ce paramètre indique si cette règle de nom de domaine déclenche le VPN.
Permanent	Ce paramètre indique si la règle de nom de domaine est appliquée lorsque le VPN n'est pas connecté.
Liste des filtres de trafic	Ce paramètre spécifie les règles autorisant le trafic via le VPN.
Liste des filtres de trafic > ID d'application	Ce paramètre identifie une application pour un filtre de trafic basé sur l'application. Valeurs possibles : • Nom de la famille de package. Pour trouver le nom de famille de package, installez l'application et exécutez la commande Windows PowerShell, `Get-AppxPackage`. Pour plus d'informations, visitez http://technet.microsoft.com/en-us/library/hh856044.aspx . • Emplacement d'installation de l'application. Par exemple, `C:\Windows\System\notepad.exe` . • Tapez « SYSTEM » pour que les pilotes du noyau puissent envoyer le trafic par le biais du VPN (par exemple, PING ou SMB).
Protocole	Ce paramètre spécifie le protocole utilisé par le VPN. Valeurs possibles : • Toutes • TCP • UDP La valeur par défaut est Tout.
Plages de ports locaux	Ce paramètre spécifie la liste des plages de ports locaux autorisées en les séparant par des virgules. Par exemple, 100-120, 200, 300-320.
Plages de ports distants	Ce paramètre spécifie la liste des plages de ports distants autorisées en les séparant par des virgules. Par exemple, 100-120, 200, 300-320.

Windows : paramètre de profil VPN	Description
Plages d'adresses locales	Ce paramètre spécifie la liste des plages d'adresses IP locales autorisées en les séparant par des virgules.
Plages d'adresses distantes	Ce paramètre spécifie la liste des plages d'adresses IP distantes autorisées en les séparant par des virgules.
Type de stratégie de routage	Ce paramètre spécifie la stratégie de routage utilisée par le filtre de trafic. Si vous le définissez sur Forcer le tunnel, tout le trafic passe par le VPN. Si vous le définissez sur Tunnel partagé, le trafic peut passer par le VPN ou Internet. Valeurs possibles : • Tunnel fractionné • Appliquer le tunnel Le paramètre par défaut est Appliquer le tunnel.
Mémoriser les informations d'identification	Ce paramètre spécifie si les identifiants doivent être mis en cache lorsque cela est possible.
Toujours activer	Ce paramètre spécifie si les terminaux se connectent automatiquement au VPN lors de l'authentification et restent connectés jusqu'à ce que l'utilisateur déconnecte manuellement le VPN.
Verrouiller	Ce paramètre spécifie si cette connexion VPN doit être utilisée lorsque le terminal se connecte à un réseau. Lorsque ce paramètre est activé, les points suivants s'appliquent : • Le terminal reste connecté au VPN. Il ne peut pas être déconnecté. • Le terminal doit être connecté à ce VPN pour disposer d'une connexion réseau. • Le terminal ne peut pas se connecter à, ou modifier, d'autres profils VPN.
Suffixe DNS	Ce paramètre spécifie un ou plusieurs suffixes DNS séparés par des virgules. Le premier suffixe DNS de la liste est également utilisé en tant que connexion principale pour le VPN. La liste est ajoutée à SuffixSearchList.
Détection de réseau sécurisé	Ce paramètre spécifie une chaine séparée par des virgules pour identifier le réseau sécurisé. Le VPN ne se connecte pas automatiquement lorsque les utilisateurs sont sur le réseau sans fil de leur entreprise.
Propriétés de la sécurité IP	

Windows : paramètre de profil VPN	Description
Constantes de transformation de l'authentification	Valeurs possibles : • MD596 • SHA196 • SHA256128 • GCMAES128 • GCMAE192 • GCMAES256 Le paramètre par défaut est MD596.
Constantes de transformation du chiffrement	Valeurs possibles : • DES • DES3 • AES 128 • AES 192 • AES256 • GCMAES128 • GCMAES192 • GCMAES256 Le paramètre par défaut est « DES ».
Méthode de cryptage	Valeurs possibles : • DES • DES3 • AES 128 • AES 192 • AES256 Le paramètre par défaut est « DES ».
Méthode de vérification de l'intégrité	Valeurs possibles : • MD5 • SHA196 • SHA256 • SHA384 Le paramètre par défaut est MD5.

Windows : paramètre de profil VPN	Description
Groupe Diffie-Hellman	Valeurs possibles : • Groupe 1 • Groupe 2 • Groupe 14 • ECP256 • ECP384 • Groupe 24 Le paramètre par défaut est Group1.
Groupe PFS	Valeurs possibles : • PFS1 • PFS2 • PFS2048 • ECP256 • ECP384 • PFSMM • PFS24 La valeur par défaut est « PFS1 ».
Type de proxy	Ce paramètre spécifie le type de configuration proxy pour le VPN. Valeurs possibles : • Aucun • Configuration PAC • Configuration manuelle La valeur par défaut est Aucune.
URL du fichier PAC	Ce paramètre spécifie l'URL du serveur Web qui héberge le fichier PAC, y compris le nom du fichier PAC. Par exemple, http://www.example.com/PACfile.pac. Ce paramètre est valide uniquement si le paramètre Type de proxy est défini sur Configuration PAC.
Adresse	Ce paramètre spécifie le FQDN ou l'adresse IP du serveur proxy. Ce paramètre est valide uniquement si le paramètre Type de proxy est défini sur Configuration manuelle.
Profil SCEP associé	Ce paramètre spécifie le profil SCEP associé utilisé par un terminal pour obtenir un certificat client et s'authentifier auprès du VPN.

Paramètres du profil SCEP

Vous pouvez utiliser une variable de paramètre de profil correspondant à un champ de texte pour faire référence à une valeur plutôt que de spécifier la valeur réelle. BlackBerry UEM prend en charge les variables par défaut

prédéfinies et les variables personnalisées que vous définissez. Les profils SCEP sont pris en charge sur les types de terminaux suivants :

- BlackBerry 10
- iOS
- macOS
- Android
- Windows 10

Dans certains cas, la version minimale du système d'exploitation du terminal requis pour prendre en charge un paramètre correspondant à une version non prise en charge par BlackBerry UEM. Pour plus d'informations sur les versions de système d'exploitation prises en charge, reportez-vous à la matrice de compatibilité.

Communs : paramètres de profil SCEP

Commun : paramètre de profil SCEP	Description
Connexion à l'autorité de certification	Ce paramètre spécifie si l'autorité de certification correspond à Entrust, à OpenTrust ou à une autre autorité de certification. Si vous avez configuré une ou plusieurs connexions au logiciel Entrust ou OpenTrust de votre entreprise, vous pouvez en sélectionner une dans la liste déroulante. Sélectionnez Générique si vous utilisez une autre autorité de certification. Si vous sélectionnez une connexion Entrust ou OpenTrust, vous devez ensuite sélectionner le profil PKI qui convient et spécifier les valeurs nécessaires. Les profils disponibles varient en fonction de ce que l'administrateur Entrust ou OpenTrust a configuré dans le logiciel PKI. La valeur par défaut est Générique.
URL	Ce paramètre spécifie l'URL du service SCEP. L'URL doit inclure le protocole, le FQDN, le numéro de port et le chemin SCEP (chemin CGI défini dans la spécification SCEP). Vous devez définir la valeur de ce paramètre pour bien activer un terminal. Les URL HTTPS SCEP sont prises en charge par les terminaux iOS et BlackBerry 10 OS version 10.3.0 ou ultérieure.
Nom de l'instance	Ce paramètre spécifie le nom de l'instance CA. La valeur peut correspondre à n'importe quelle chaine comprise par le service SCEP. Par exemple, il peut s'agir d'un nom de domaine comme exemple.org. Si une autorité de certification dispose de plusieurs certificats d'autorité de certification, ce champ permet de distinguer le certificat requis.

Commun : paramètre de profil SCEP	Description
Type de challenge SCEP	Ce paramètre spécifie si le mot de passe de vérification SCEP est généré de manière dynamique ou fourni en tant que mot de passe statique. Si ce paramètre est défini sur Statique, chaque terminal utilise le même mot de passe de vérification. Si ce paramètre est défini sur Dynamique, chaque terminal reçoit un mot de passe de vérification unique. Valeurs possibles : • Statique • Dynamique La valeur par défaut est Dynamique. Pour les terminaux Windows, seuls les mots de passe Statiques sont pris en charge.
URL de génération d'un mot de passe de vérification	Ce paramètre spécifie l'URL utilisée par les terminaux pour obtenir un mot de passe généré de manière dynamique à partir du service SCEP. L'URL doit inclure le protocole, le FQDN, le numéro de port et le chemin SCEP (chemin CGI défini dans la spécification SCEP). Si vous utilisez un mot de passe de vérification dynamique, vous devez définir une valeur pour correctement activer les terminaux BlackBerry 10. Ce paramètre est valide uniquement si le paramètre Type de challenge SCEP est défini sur Dynamique.
Type d'authentification	Ce paramètre spécifie le type d'authentification utilisé par les terminaux pour se connecter au service SCEP et obtenir un mot de passe de vérification. Ce paramètre est valide uniquement si le paramètre Type de challenge SCEP est défini sur Dynamique. Valeurs possibles : • De base • NTLM La valeur par défaut est De base.
Domaine	Ce paramètre spécifie le domaine utilisé pour l'authentification NTLM lorsque les terminaux se connectent au service SCEP afin d'obtenir un mot de passe de vérification. Ce paramètre est valide uniquement si le paramètre Type d'authentification est défini sur NTLM.
Nom d'utilisateur	Ce paramètre spécifie le nom d'utilisateur requis pour obtenir un mot de passe de vérification à partir du service SCEP. Ce paramètre est valide uniquement si le paramètre Type de challenge SCEP est défini sur Dynamique.

Commun : paramètre de profil SCEP	Description
Mot de passe,	Ce paramètre spécifie le mot de passe requis pour obtenir le mot de passe de vérification à partir du service SCEP. Ce paramètre est valide uniquement si le paramètre Type de challenge SCEP est défini sur Dynamique.
Mot de passe de vérification	Ce paramètre spécifie le mot de passe de vérification utilisé par un terminal pour inscrire le certificat. Si vous utilisez un mot de passe de vérification statique, vous devez définir la valeur de ce paramètre pour bien activer les terminaux BlackBerry 10. Ce paramètre est valide uniquement si le paramètre Type de challenge SCEP est défini sur Statique.

BlackBerry 10 : paramètres de profil SCEP

BlackBerry 10 : paramètre de profil SCEP	Description
Utiliser un objet par défaut de terminal et un autre nom d'objet	Ce paramètre spécifie si un terminal BlackBerry 10 génère l'objet et l'autre nom d'objet d'une demande de certificat. Si ce paramètre n'est pas sélectionné, vous devez spécifier l'objet et l'autre nom d'objet ainsi que la valeur.
Objet	Ce paramètre spécifie l'objet du certificat, si requis pour la configuration SCEP de votre entreprise. Saisissez l'objet au format « /CN=<*common_name*>/O=<*domain_name*> » Si le profil concerne plusieurs utilisateurs, vous pouvez utiliser une variable (%UserDistinguishedName%, par exemple). Ce paramètre est valide uniquement si le paramètre Utiliser un objet par défaut de terminal et un autre nom d'objet n'est pas sélectionné. La configuration minimale requise est BlackBerry 10 OS version 10.3.1.
SAN	Ce paramètre spécifie le type d'autre nom d'objet et la valeur d'un certificat. Ce paramètre est valide uniquement si le paramètre Utiliser un objet par défaut de terminal et un autre nom d'objet n'est pas sélectionné. La configuration minimale requise est BlackBerry 10 OS version 10.3.1.
Type SAN	Ce paramètre spécifie le type d'autre nom d'objet du certificat, si nécessaire. Valeurs possibles : • Nom RFC 822 • URI • Nom principal NT • Nom DNS La valeur par défaut est Nom RFC 822.

BlackBerry 10 : paramètre de profil SCEP	Description
Valeur SAN	Ce paramètre spécifie l'autre représentation de l'objet de certificat. La valeur doit correspondre à une adresse électronique, le nom DNS du serveur CA, l'URL complète du serveur ou le nom principal. Le paramètre Type SAN détermine le type de valeur que vous spécifiez. Si cette option est définie sur «Nom RFC822», la valeur doit correspondre à une adresse électronique valide. Si cette option est définie sur « URI », la valeur doit correspondre à une URL valide incluant le protocole et le FQDN ou l'adresse IP. Si cette option est définie sur Nom principal, la valeur doit correspondre à un nom principal valide. Si cette option est définie sur «Nom DNS», la valeur doit correspondre à un FQDN valide.
Algorithme de clé	Ce paramètre spécifie l'algorithme utilisé par un terminal BlackBerry 10 pour générer la paire de clés client. Vous devez sélectionner un algorithme pris en charge par votre autorité de certification. Valeurs possibles : • Aucune • RSA • ECC La valeur par défaut est RSA.
Puissance RSA	Ce paramètre spécifie la force BlackBerry 10 utilisée par un terminal RSA pour générer la paire de clés client. Vous devez saisir une force de clé prise en charge par votre autorité de certification. Ce paramètre est valide uniquement si le paramètre Algorithme de clé est défini sur RSA. Valeurs possibles : • 1024 • 2048 • 4096 • 8192 • 16384 La valeur par défaut est 1 024.

BlackBerry 10 : paramètre de profil SCEP	Description
Puissance ECC	Ce paramètre spécifie la courbe elliptique utilisée par un terminal BlackBerry 10 pour générer la paire de clés client. La courbe elliptique définit la force de la paire de clés client. Vous devez sélectionner une courbe elliptique prise en charge par votre autorité de certification. Ce paramètre est valide uniquement si le paramètre Algorithme de clé est défini sur ECC. Valeurs possibles : • sect163k1 • sect283k1 • secp192r1 • secp256r1 • secp384r1 • secp521r1 La valeur par défaut est secp521r1.
Algorithme de cryptage	Ce paramètre spécifie l'algorithme de cryptage utilisé par un terminal BlackBerry 10 pour la demande d'inscription de certificat. Valeurs possibles : • Aucune • Triple DES • AES (128 bits) • AES (196 bits) • AES (256 bits) La valeur par défaut est Triple DES.
Fonction de hachage	Ce paramètre spécifie la fonction de hachage utilisée par un terminal BlackBerry 10 pour la demande d'inscription de certificat. Valeurs possibles : • Aucune • SHA-1 • SHA-224 • SHA-256 • SHA-384 • SHA-512 La valeur par défaut est SHA-1.
Empreinte de certificat	Ce paramètre spécifie le hachage codé au format hexadécimal du certificat racine de l'autorité de certification. Vous pouvez utiliser les algorithmes suivants pour spécifier l'empreinte : MD5, SHA-1, SHA-224, SHA-256, SHA-384 et SHA-512. Vous devez définir la valeur de ce paramètre pour bien activer un terminal BlackBerry 10.

BlackBerry 10 : paramètre de profil SCEP	Description
Renouvellement automatique	Ce paramètre spécifie le nombre de jours avant renouvellement automatique d'un certificat qui arrive à expiration. Les valeurs possibles sont comprises entre 1 et 999 999 999 jours. La valeur par défaut est 30.
Utilisation de la clé	Ce paramètre spécifie les opérations cryptographiques pouvant être effectuées à l'aide de la clé publique contenue dans le certificat. Sélections possibles : • Signature numérique • Non-répudiation • Cryptage de clé • Cryptage de données • Accord de la clé • Signature du certificat clé • Signature CRL • Crypter uniquement • Décrypter uniquement Les sélections par défaut sont Signature numérique, Cryptage de clé et Accord de la clé. La configuration minimale requise est BlackBerry 10 OS version 10.3.1.
Utilisation étendue de la clé	Ce paramètre spécifie l'objectif de la clé contenue dans le certificat. Sélections possibles : • Authentification du serveur • Authentification du client • Signature de code • Protection des e-mails • Horodatage • Signature OCSP • Client Secure Shell • Serveur Secure Shell La sélection par défaut est Authentification du client. La configuration minimale requise est BlackBerry 10 OS version 10.3.1.

iOS : paramètres de profil SCEP

iOS : paramètre de profil SCEP	Description
Utiliser BlackBerry UEM comme proxy pour les demandes SCEP	Ce paramètre spécifie si toutes les demandes SCEP des terminaux sont envoyées via BlackBerry UEM. Si l'autorité de certification se situe derrière votre pare-feu, ce paramètre vous permet d'inscrire des certificats client pour les terminaux sans exposer l'autorité de certification en dehors du pare-feu.
Objet	Ce paramètre spécifie l'objet du certificat, si requis pour la configuration SCEP de votre entreprise. Saisissez l'objet au format « /CN=<*common_name*>/O=<*domain_name*> » Si le profil concerne plusieurs utilisateurs, vous pouvez utiliser une variable (%UserDistinguishedName%, par exemple).
Nouvelles tentatives	Ce paramètre spécifie le nombre de nouvelles tentatives de connexion au service SCEP si la tentative de connexion échoue. Les valeurs possibles sont comprises entre 1 et 999. La valeur par défaut est 3.
Délai de nouvelle tentative	Ce paramètre spécifie le délai d'attente, en secondes, avant une nouvelle tentative de connexion au service SCEP. Les valeurs possibles sont comprises entre 1 et 999. La valeur par défaut est de 10 secondes.
Taille de la clé	Ce paramètre spécifie la taille de la clé du certificat. Valeurs possibles : • 1024 • 2048 La valeur par défaut est 1 024.
Empreinte	Ce paramètre spécifie l'empreinte d'inscription d'un certificat SCEP. Si votre autorité de certification utilise HTTP plutôt que HTTPS, les terminaux utilisent l'empreinte pour confirmer l'identité de l'autorité de certification lors du processus d'inscription. L'empreinte digitale ne peut pas contenir d'espace.
Type SAN	Ce paramètre spécifie le type d'autre nom d'objet du certificat, si nécessaire. Valeurs possibles : • Aucune • Nom RFC822 • Nom DNS • Uniform Resource Identifier (Identificateur de ressources uniformes) La valeur par défaut est Aucune.

iOS : paramètre de profil SCEP	Description
Valeur SAN	Ce paramètre spécifie l'autre représentation de l'objet du certificat. La valeur doit correspondre à une adresse électronique, le nom DNS du serveur CA ou l'URL complète du serveur. Le paramètre Type SAN détermine le type de valeur que vous spécifiez. Si cette option est définie sur «Nom RFC822», la valeur doit correspondre à une adresse électronique valide. Si cette option est définie sur « URI », la valeur doit correspondre à une URL valide incluant le protocole et le FQDN ou l'adresse IP. Si cette option est définie sur Nom principal, la valeur doit correspondre à un nom principal valide. Si cette option est définie sur «Nom DNS», la valeur doit correspondre à un FQDN valide.
Nom principal NT	Ce paramètre spécifie le Nom principal NT pour la génération du certificat. Ce paramètre est valide uniquement si le paramètre Type SAN est défini sur un autre paramètre que Aucun.
Expiration du profil	Indiquez le nombre de jours qui doit s'écouler après l'émission d'un certificat, avant que le terminal ne demande un nouveau certificat à l'autorité de certification. Si le certificat sur le terminal a été émis avant la mise à niveau vers BlackBerry UEM version 12.8, la première demande de renouvèlement intervient au bout du nombre de jours spécifié qui suit la mise à niveau UEM. La valeur doit être inférieure à la période de validité du certificat définie par l'autorité de certification. La valeur par défaut est de 1 825 jours.

macOS : paramètres de profil SCEP

macOS applique les profils aux terminaux ou comptes d'utilisateur. Vous pouvez configurer un profil SCEP à appliquer à l'un ou à l'autre.

macOS : paramètre de profil SCEP	Description
Utiliser BlackBerry UEM comme proxy pour les demandes SCEP	Ce paramètre spécifie si toutes les demandes SCEP des terminaux sont envoyées via BlackBerry UEM. Si l'autorité de certification se situe derrière votre pare-feu, ce paramètre vous permet d'inscrire des certificats client pour les terminaux sans exposer l'autorité de certification en dehors du pare-feu.
Appliquer le profil à	Ce paramètre indique si le profil SCEP est appliqué au compte d'utilisateur ou au terminal. Valeurs possibles : • Utilisateur • Terminal
Objet	Ce paramètre spécifie l'objet du certificat, si requis pour la configuration SCEP de votre entreprise. Saisissez l'objet au format « /CN=<*common_name*>/O=<*domain_name*> » Si le profil concerne plusieurs utilisateurs, vous pouvez utiliser une variable (%UserDistinguishedName%, par exemple).

macOS : paramètre de profil SCEP	Description
Nouvelles tentatives	Ce paramètre spécifie le nombre de nouvelles tentatives de connexion au service SCEP si la tentative de connexion échoue. Les valeurs possibles sont comprises entre 1 et 999. La valeur par défaut est 3.
Délai de nouvelle tentative	Ce paramètre spécifie le délai d'attente, en secondes, avant une nouvelle tentative de connexion au service SCEP. Les valeurs possibles sont comprises entre 1 et 999. La valeur par défaut est de 10 secondes.
Taille de la clé	Ce paramètre spécifie la taille de la clé du certificat. Valeurs possibles : • 1024 • 2048 La valeur par défaut est 1 024.
Empreinte	Ce paramètre spécifie l'empreinte d'inscription d'un certificat SCEP. Si votre autorité de certification utilise HTTP plutôt que HTTPS, les terminaux utilisent l'empreinte pour confirmer l'identité de l'autorité de certification lors du processus d'inscription. L'empreinte digitale ne peut pas contenir d'espace.
Type SAN	Ce paramètre spécifie le type d'autre nom d'objet du certificat, si nécessaire. Valeurs possibles : • Aucune • Nom RFC822 • Nom DNS • Uniform Resource Identifier (Identificateur de ressources uniformes) La valeur par défaut est Aucune.
Valeur SAN	Ce paramètre spécifie l'autre représentation de l'objet du certificat. La valeur doit correspondre à une adresse électronique, le nom DNS du serveur CA ou l'URL complète du serveur. Le paramètre Type SAN détermine le type de valeur que vous spécifiez. Si cette option est définie sur «Nom RFC822», la valeur doit correspondre à une adresse électronique valide. Si cette option est définie sur URI, la valeur doit correspondre à une URL valide incluant le protocole et le FQDN ou l'adresse IP. Si cette option est définie sur Nom principal, la valeur doit correspondre à un nom principal valide. Si cette option est définie sur Nom DN, la valeur doit correspondre à un FQDN valide.
Nom principal NT	Ce paramètre spécifie le Nom principal NT pour la génération du certificat. Ce paramètre est valide uniquement si le paramètre Type SAN est défini sur un autre paramètre que Aucun.

Android : paramètres de profil SCEP

Pour obtenir un exemple de profil SCEP pour les terminaux Android, rendez-vous sur http://support.blackberry.com/kb/ et lisez l'article KB38248.

Android : paramètre de profil SCEP	Description
Utiliser BlackBerry UEM comme proxy pour les demandes SCEP	Ce paramètre spécifie si toutes les demandes SCEP des terminaux sont envoyées via BlackBerry UEM. Si l'autorité de certification se situe derrière votre pare-feu, ce paramètre vous permet d'inscrire des certificats client pour les terminaux sans exposer l'autorité de certification en dehors du pare-feu.
Algorithme de cryptage	Ce paramètre spécifie l'algorithme de cryptage utilisé par un terminal Android pour la demande d'inscription de certificat. Valeurs possibles : • Aucune • Triple DES • AES (128 bits) • AES (196 bits) • AES (256 bits) La valeur par défaut est Triple DES.
Fonction de hachage	Ce paramètre spécifie la fonction de hachage utilisée par un terminal Android pour la demande d'inscription de certificat. Valeurs possibles : • Aucune • SHA-1 • SHA-224 • SHA-256 • SHA-384 • SHA-512 La valeur par défaut est SHA-1.
Empreinte de certificat	Ce paramètre spécifie le hachage codé au format hexadécimal du certificat racine de l'autorité de certification. Vous pouvez utiliser les algorithmes suivants pour spécifier l'empreinte : SHA-1, SHA-224, SHA-256, SHA-384 et SHA-512. Vous devez définir la valeur de ce paramètre pour activer les terminaux utilisant les profils professionnels Android ou Samsung KNOX.
Renouvellement automatique	Ce paramètre spécifie le nombre de jours avant renouvellement automatique d'un certificat qui arrive à expiration. Les valeurs possibles sont 1 à 365. La valeur par défaut est 30.
Profils professionnels Android et Samsung KNOX	

Android : paramètre de profil SCEP	Description
Objet	Ce paramètre spécifie l'objet du certificat, si requis pour la configuration SCEP de votre entreprise. Saisissez l'objet au format « /CN=<*common_name*>/O=<*domain_name*> » Si le profil concerne plusieurs utilisateurs, vous pouvez utiliser une variable (%UserDistinguishedName%, par exemple).
Type SAN	Ce paramètre spécifie le type d'autre nom d'objet du certificat, si nécessaire. Valeurs possibles : • Nom RFC 822 • Uniform Resource Identifier (Identificateur de ressources uniformes) • Nom principal NT • Nom DNS La valeur par défaut est Nom RFC 822.
Valeur SAN	Ce paramètre spécifie l'autre représentation de l'objet de certificat. La valeur doit correspondre à une adresse électronique, le nom DNS du serveur CA, l'URL complète du serveur ou le nom principal. Le paramètre Type SAN détermine le type de valeur que vous spécifiez. Si cette option est définie sur «Nom RFC822», la valeur doit correspondre à une adresse électronique valide. Si cette option est définie sur « URI », la valeur doit correspondre à une URL valide incluant le protocole et le FQDN ou l'adresse IP. Si cette option est définie sur Nom principal, la valeur doit correspondre à un nom principal valide. Si cette option est définie sur «Nom DNS», la valeur doit correspondre à un FQDN valide.
Algorithme de clé	Ce paramètre spécifie l'algorithme utilisé par les terminaux dotés d'un profil professionnel Android ou Samsung KNOX pour générer la paire de clés client. Vous devez sélectionner un algorithme pris en charge par votre autorité de certification. Valeurs possibles : • Aucune • RSA • ECC La valeur par défaut est RSA.

Android : paramètre de profil SCEP	Description
Puissance RSA	Ce paramètre spécifie la puissance RSA utilisée par les terminaux dotés d'un profil professionnel Android ou Samsung KNOX pour générer la paire de clés client. Vous devez saisir une force de clé prise en charge par votre autorité de certification. Ce paramètre est valide uniquement si le paramètre Algorithme de clé est défini sur RSA. Valeurs possibles : • 1024 • 2048 • 4096 • 8192 • 16384 La valeur par défaut est 1 024.
Utilisation de la clé	Ce paramètre spécifie les opérations cryptographiques pouvant être effectuées à l'aide de la clé publique contenue dans le certificat. Sélections possibles : • Signature numérique • Non-répudiation • Cryptage de clé • Cryptage de données • Accord de la clé • Signature du certificat clé • Signature CRL • Crypter uniquement • Décrypter uniquement Les sélections par défaut sont Signature numérique, Cryptage de clé et Accord de la clé.
Utilisation étendue de la clé	Ce paramètre spécifie l'objectif de la clé contenue dans le certificat. Sélections possibles : • Authentification du serveur • Authentification du client • Signature de code • Protection des e-mails • Horodatage • Signature OCSP • Client Secure Shell • Serveur Secure Shell La sélection par défaut est Authentification du client.

Windows 10 : paramètres de profil SCEP

Windows 10 : paramètre de profil SCEP	Description
Objet	Ce paramètre spécifie l'objet du certificat, si requis pour la configuration SCEP de votre entreprise. Saisissez l'objet au format « /CN=<*common_name*>/O=<*domain_name*> » Si le profil concerne plusieurs utilisateurs, vous pouvez utiliser une variable (%UserDistinguishedName%, par exemple).
Type SAN	Ce paramètre spécifie le type d'autre nom d'objet du certificat, si nécessaire. Valeurs possibles : • Aucune • Nom RFC 822 • Nom DNS • Uniform Resource Identifier (Identificateur de ressources uniformes) La valeur par défaut est Aucune.
Valeur SAN	Ce paramètre spécifie l'autre représentation de l'objet du certificat. La valeur doit correspondre à une adresse électronique, le nom DNS du serveur CA ou l'URL complète du serveur. La valeur appropriée pour ce paramètre dépend de la valeur sélectionnée pour le paramètre Type SAN.
Nouvelles tentatives	Ce paramètre spécifie le nombre de nouvelles tentatives de connexion au service SCEP si la tentative de connexion échoue. Les valeurs possibles sont comprises entre 1 et 999. La valeur par défaut est 3.
Délai de nouvelle tentative	Ce paramètre spécifie le délai d'attente, en secondes, avant une nouvelle tentative de connexion au service SCEP. Les valeurs possibles sont comprises entre 1 et 999. La valeur par défaut est de 10 secondes.
Taille de la clé	Ce paramètre spécifie la taille de la clé du certificat. Valeurs possibles : • 1024 • 2048 • 4096 • 8192 • 16384 La valeur par défaut est 1 024.

Windows 10 : paramètre de profil SCEP	Description
Utilisation de la clé	Ce paramètre spécifie les opérations cryptographiques pouvant être effectuées à l'aide de la clé publique contenue dans le certificat. • Signature numérique • Non-répudiation • Cryptage de clé • Cryptage de données • Accord de la clé • Signature du certificat clé • Signature CRL • Crypter uniquement Les sélections par défaut sont Signature numérique, Cryptage de clé et Accord de la clé.
Utilisation étendue de la clé	Ce paramètre spécifie l'objectif de la clé contenue dans le certificat. • Authentification du serveur • Authentification du client • Signature de code • Protection des e-mails • Horodatage • Signature OCSP • Client Secure Shell • Serveur Secure Shell La sélection par défaut est Authentification du client.
Fonction de hachage	Ce paramètre spécifie la fonction de hachage utilisée par un terminal Windows 10 pour la demande d'inscription de certificat. Valeurs possibles : • SHA-1 • SHA-224 • SHA-256 • SHA-384 • SHA-512 La valeur par défaut est SHA-1.
Empreinte de certificat	Ce paramètre spécifie le hachage codé au format hexadécimal du certificat racine de l'autorité de certification. Vous pouvez utiliser les algorithmes suivants pour spécifier l'empreinte : SHA-1, SHA-224, SHA-256, SHA-384 et SHA-512.
Renouvellement automatique	Ce paramètre spécifie le nombre de jours avant renouvellement automatique d'un certificat qui arrive à expiration. Les valeurs possibles sont 1 à 365. La valeur par défaut est 30.

Paramètres des profils de conformité

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

- BlackBerry 10
- iOS
- macOS
- Android
- Windows

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.

Communs : paramètre de profil de conformité	Description
Action d'application	Ce paramètre spécifie l'action prise par BlackBerry UEM sur les terminaux non conformes. Valeurs possibles : • Invite à la conformité • Ne pas faire confiance : sur les terminaux iOS, macOS, Android et Windows, cette option empêche l'utilisateur d'accéder aux ressources et applications professionnelles. Les données et les applications ne sont pas supprimées du terminal. **Remarque :** Untrust n'est pas pris en charge pour les applications BlackBerry Dynamics. **Remarque :** Sur les terminaux iOS, 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. • Mettre en quarantaine : sur les terminaux BlackBerry 10, cette option empêche l'utilisateur d'accéder aux ressources et applications professionnelles. Les données et les applications ne sont pas supprimées du terminal. • Supprimer uniquement les données professionnelles • Supprimer toutes les données • Supprimer du serveur : sur les terminaux BlackBerry 10, iOS, Android et Windows, un terminal peut être désactivé de BlackBerry UEM s'il enfreint la règle « Non joignable ». • Aucun : permet d'identifier une violation de conformité mais aucune action n'est mise en œuvre. Le paramètre par défaut est « Invite à la conformité ». Sur les terminaux activés via « Travail et Personnel - Confidentialité de l'utilisateur », il vous est impossible de supprimer toutes les données d'un terminal d'utilisateur. Si vous sélectionnez « Supprimer toutes les données », BlackBerry UEM exécute la même action qu'avec « Supprimer uniquement les données professionnelles ». Pour les terminaux Samsung KNOX Workspace qui n'ont qu'un espace Travail, si vous sélectionnez « Supprimer uniquement des données professionnelles », « Supprimer toutes les données » ou « Supprimer du serveur », toutes les données seront supprimées du terminal. Les actions d'application de la règle « Une application interdite est installée » ne concernent pas les terminaux iOS 9.3.2 sous supervision et versions ultérieures. L'installation d'applications interdites est impossible.

Communs : paramètre de profil de conformité	Description
Méthode d'invite	Les valeurs possibles sont : • Les deux • Notification par e-mail • Notification de terminal Le paramètre par défaut est « Les deux ». Ce paramètre est uniquement valide si le paramètre « Action d'application » est défini sur « Invite à la conformité ». Les notifications du terminal ne sont pas prises en charge sur les terminaux Windows 10.
Nombre d'invites	Nombre de fois où l'utilisateur est invité à se remettre en conformité. La valeur par défaut est 3. Ce paramètre est uniquement valide si le paramètre « Action d'application » est défini sur « Invite à la conformité ».
Intervalle entre les invites	Délai entre les invites, en minutes, heures ou jours. Le paramètre par défaut est 4 jours. Ce paramètre est uniquement valide si le paramètre « Action d'application » est défini sur « Invite à la conformité ».
Action à l'expiration de l'intervalle entre les invites	Ce paramètre détermine l'action à prendre lorsque l'utilisateur a reçu le nombre total d'invites défini dans Nombre d'invites, et que le terminal n'est toujours pas conforme. Valeurs possibles : • Aucun • Ne pas faire confiance : sur les terminaux iOS, macOS, Android et Windows, cette option empêche l'utilisateur d'accéder aux ressources et applications professionnelles. Les données et les applications ne sont pas supprimées du terminal. **Remarque :** L'action Ne pas faire confiance n'est pas prise en charge pour les applications BlackBerry Dynamics. Utilisation d'une autre mesure d'application. • Mettre en quarantaine : sur les terminaux BlackBerry 10, cette option empêche l'utilisateur d'accéder aux ressources et applications professionnelles. Les données et les applications ne sont pas supprimées du terminal. • Supprimer uniquement les données professionnelles • Supprimer toutes les données Le paramètre par défaut est « Ne pas faire confiance ». Ce paramètre est uniquement valide si le paramètre « Action d'application » est défini sur « Invite à la conformité ».

Communs : paramètre de profil de conformité	Description
Action d'application pour les applications BlackBerry Dynamics	Ce paramètre définit comment traiter les applications BlackBerry Dynamics lorsqu'un terminal n'est pas conforme. Valeurs possibles : • Ne pas autoriser l'exécution d'applications BlackBerry Dynamics • Supprimer les données d'applications BlackBerry Dynamics La valeur par défaut est Ne pas autoriser l'exécution d'applications BlackBerry Dynamics.

BlackBerry 10 : paramètres de profil de conformité

Voir, Communs : paramètres de profil de conformité pour la description des actions possibles si vous sélectionnez une règle de conformité.

BlackBerry 10 : paramètre de profil de conformité	Description
Alerte d'intégrité	Ce paramètre crée une règle de conformité si un utilisateur malveillant a réussi à obtenir un accès racine ou des privilèges accrus sur un terminal BlackBerry 10.
Une version limitée du logiciel est installée	Ce paramètre crée une règle de conformité pour empêcher les terminaux d'utiliser une version non autorisée du logiciel, comme spécifié dans un profil d'exigences SR. Pour plus d'informations, reportez-vous à Créer un profil de configuration logicielle minimale requise du terminal pour les terminaux BlackBerry 10. Cette règle ne s'applique pas aux terminaux utilisant le type d'activation Travail et Personnel - Entreprise.
Une version limitée du SE est installée	Ce paramètre crée une règle de conformité pour veiller à ce qu'une version limitée du système d'exploitation ne soit pas installée sur les terminaux, comme spécifié dans ce paramètre. Vous pouvez spécifier les versions interdites du système d'exploitation.
Modèle de terminal interdit détecté	Ce paramètre crée une règle de conformité pour interdire les modèles de terminaux spécifiés. Valeurs possibles : • Autoriser les modèles de terminaux sélectionnés • Ne pas autoriser les modèles de terminaux sélectionnés Vous pouvez sélectionner les modèles de terminaux autorisés ou interdits.
Terminal non joignable	Ce paramètre crée une règle de conformité pour veiller à ce que les terminaux ne restent pas déconnectés de BlackBerry UEM au-delà du laps de temps spécifié.

BlackBerry 10 : paramètre de profil de conformité	Description
Heure du dernier contact	Ce paramètre spécifie la durée (en nombre de jours) pendant laquelle un terminal peut rester déconnecté de BlackBerry UEM. Ce paramètre s'applique uniquement si le paramètre Terminal non joignable est sélectionné.

iOS : paramètres de profil de conformité

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

iOS : paramètre de 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 iOS. Un terminal est cracké lorsqu'un utilisateur ou un utilisateur malveillant contourne différentes restrictions pour modifier le système d'exploitation d'un terminal.
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 iOS, un message d'avertissement et un lien sont affichés sur l'onglet Terminaux gérés. Lorsque vous cliquez sur le lien, la liste des applications qui mettent le terminal hors conformité est affichée. Ce paramètre ne s'applique pas aux terminaux activés avec le type d'activation Confidentialité de l'utilisateur.
Une application requise n'est pas installée	Ce paramètre crée une règle de conformité pour veiller à ce que les applications requises soient installées sur les terminaux. Lorsque vous sélectionnez ce paramètre et qu'une application requise n'est pas installée sur un terminal iOS, un message d'avertissement et un lien sont affichés sur l'onglet Terminaux gérés. Lorsque vous cliquez sur le lien, la liste des applications qui mettent le terminal hors conformité est affichée.
Une version limitée du SE est installée	Ce paramètre crée une règle de conformité pour veiller à ce qu'une version limitée du système d'exploitation ne soit pas installée sur les terminaux, comme spécifié dans ce paramètre. Vous pouvez sélectionner les versions limitées du système d'exploitation.

iOS : paramètre de profil de conformité	Description
Modèle de terminal interdit détecté	Ce paramètre crée une règle de conformité pour interdire les modèles de terminaux spécifiés. Valeurs possibles : • Autoriser les modèles de terminaux sélectionnés • Ne pas autoriser les modèles de terminaux sélectionnés Vous pouvez sélectionner les modèles de terminaux autorisés ou interdits.
Terminal non joignable	Ce paramètre crée une règle de conformité pour veiller à ce que les terminaux ne restent pas déconnectés de BlackBerry UEM au-delà du laps de temps spécifié.
Heure du dernier contact	Ce paramètre spécifie la durée (en nombre de jours) pendant laquelle un terminal peut rester déconnecté de BlackBerry UEM. Ce paramètre s'applique uniquement si le paramètre Terminal non joignable est sélectionné.
Vérification de la version de la bibliothèque BlackBerry Dynamics	Ce paramètre crée une règle de conformité qui vous permet de sélectionner les versions de la bibliothèque BlackBerry Dynamics ne pouvant pas être activées. Vous pouvez sélectionner les versions bloquées de la bibliothèque.
Vérification de la connectivité BlackBerry Dynamics	Ce paramètre crée une règle de conformité pour veiller à ce que les applications BlackBerry Dynamics ne restent pas déconnectés de BlackBerry UEM au-delà du laps de temps spécifié. L'action d'application concerne les applications BlackBerry Dynamics.
Baser l'intervalle de connectivité sur des applications de délégation de l'authentification	Ce paramètre spécifie que la vérification de la connectivité repose sur la connexion d'une application de délégation de l'authentification à BlackBerry UEM. Ce paramètre est uniquement valide si le paramètre Vérification de la connectivité est sélectionné.

iOS : paramètre de profil de conformité	Description
Heure du dernier contact	Ce paramètre spécifie le nombre de jours à l'issue duquel le terminal devra se connecter à BlackBerry UEM. Valeurs possibles : • 8 heures • 16 heures • 1 jour • 2 jours • 3 jours • 7 jours • 14 jours • 30 jours • 60 jours • 90 jours • 180 jours • 365 jours La valeur par défaut est 2 jours. Ce paramètre est uniquement valide si le paramètre Vérification de la connectivité est sélectionné.

iOS : paramètre de profil de conformité	Description
Une application interdite est installée	Ce paramètre crée une règle de conformité pour empêcher les utilisateurs d'installer certaines applications. Pour interdire des applications, effectuez l'une des tâches suivantes : • Sélectionnez une application dans la liste des applications interdites. Pour plus d'informations, reportez-vous à Ajouter une application à la liste des applications limitées. Effectuez l'une des opérations suivantes : • Pour sélectionner des applications à l'aide de leur nom, cliquez sur l'option Sélectionner les applications depuis la liste des applications. • Pour sélectionner des applications en utilisant l'ID du package d'applications, cliquez sur l'option Spécifier l'ID du package d'applications. Vous ne devez pas utiliser l'ID du package pour ajouter des applications publiques. Ajoutez les applications publiques à la liste d'applications restreintes, puis utilisez l'option Sélectionner des applications dans la liste des applications pour sélectionner ces applications. • Sélectionnez une application intégrée (terminaux iOS 9.3.2 sous supervision et versions ultérieures uniquement) Pour supprimer une application de la liste, cliquez sur ✕. Lorsque vous sélectionnez ce paramètre et qu'une application interdite est installée sur un terminal iOS, un message d'avertissement et un lien sont affichés sur l'onglet Terminaux gérés. Lorsque vous cliquez sur le lien, la liste des applications qui mettent le terminal hors conformité est affichée. Les actions d'application de cette règle ne concernent pas les terminaux iOS 9.3.2 sous supervision et versions ultérieures. L'installation d'applications interdites est impossible.
Afficher les applications autorisées sur le terminal uniquement	Ce paramètre crée une règle de conformité répertoriant les applications qui peuvent être installées sur les terminaux des utilisateurs. Toutes les autres applications sont interdites. Pour autoriser des applications spécifiques, effectuez l'une des tâches suivantes : • Sélectionnez une application dans la liste des applications interdites. Pour plus d'informations, reportez-vous à Ajouter une application à la liste des applications limitées. • Sélectionnez une application intégrée (terminaux iOS 9.3.2 sous supervision et versions ultérieures uniquement) Par défaut, certaines applications sont incluses dans la liste autorisée. Pour supprimer une application de la liste, cliquez sur ✕. Ce paramètre s'applique uniquement aux terminaux supervisés exécutant iOS 9.3.2 ou version ultérieure.

macOS : paramètres de profil de conformité

Voir, Communs : paramètres de profil de conformité pour la description des actions possibles si vous sélectionnez une règle de conformité.

macOS : paramètre de profil de conformité	Description
Une version limitée du SE est installée	Ce paramètre crée une règle de conformité pour veiller à ce qu'une version limitée du système d'exploitation ne soit pas installée sur les terminaux, comme spécifié dans ce paramètre. Vous pouvez sélectionner les versions limitées du système d'exploitation.
Modèle de terminal interdit détecté	Ce paramètre crée une règle de conformité pour interdire les modèles de terminaux spécifiés. Valeurs possibles : • Autoriser les modèles de terminaux sélectionnés • Ne pas autoriser les modèles de terminaux sélectionnés Vous pouvez sélectionner les modèles de terminaux autorisés ou interdits.
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 BlackBerry UEM au-delà du laps de temps spécifié. L'action d'application concerne les applications BlackBerry Dynamics.
Baser l'intervalle de connectivité sur des applications de délégation de l'authentification	Ce paramètre spécifie que la vérification de la connectivité repose sur la connexion d'une application de délégation de l'authentification à BlackBerry UEM. Ce paramètre est uniquement valide si le paramètre Vérification de la connectivité est sélectionné.

macOS : paramètre de profil de conformité	Description
Heure du dernier contact	Ce paramètre spécifie le nombre de jours à l'issue duquel le terminal devra se connecter à BlackBerry UEM. Valeurs possibles : • 8 heures • 16 heures • 1 jour • 2 jours • 3 jours • 7 jours • 14 jours • 30 jours • 60 jours • 90 jours • 180 jours • 365 jours La valeur par défaut est 2 jours. Ce paramètre est uniquement valide si le paramètre Vérification de la connectivité est sélectionné.

Android : paramètres de profil de conformité

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

Android : paramètre de profil de conformité	Description
Système d'exploitation flashé	Ce paramètre crée une règle de conformité qui empêche de flasher les terminaux. Un terminal est flashé lorsqu'un utilisateur ou un utilisateur malveillant accède au niveau racine du système d'exploitation Android.
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'onglet Terminaux gérés. Lorsque vous cliquez sur le lien, la liste des applications qui mettent le terminal hors conformité est affichée. Pour les terminaux Android dotés d'un profil professionnel 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.

Android : paramètre de 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. Lorsque vous sélectionnez ce paramètre et qu'une application requise n'est pas installée sur un terminal Android, un message d'avertissement et un lien sont affichés sur l'onglet Terminaux gérés. Lorsque vous cliquez sur le lien, la liste des applications qui mettent le terminal hors conformité est affichée. Pour les terminaux Android dotés d'un profil professionnel, les mesures 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.
Une version limitée du SE est installée	Ce paramètre crée une règle de conformité pour veiller à ce qu'une version limitée du système d'exploitation ne soit pas installée sur les terminaux, comme spécifié dans ce paramètre. Vous pouvez sélectionner les versions limitées du système d'exploitation.
Modèle de terminal interdit détecté	Ce paramètre crée une règle de conformité pour interdire les modèles de terminaux spécifiés. Valeurs possibles : • Autoriser les modèles de terminaux sélectionnés • Ne pas autoriser les modèles de terminaux sélectionnés Vous pouvez sélectionner les modèles de terminaux autorisés ou interdits.
Terminal non joignable	Ce paramètre crée une règle de conformité pour veiller à ce que les terminaux ne restent pas déconnectés de BlackBerry UEM au-delà du laps de temps spécifié. Le terminal vérifie la conformité avec cette règle et peut supprimer les données professionnelles, supprimer toutes les données ou se désactiver de BlackBerry UEM s'il n'est pas conforme.
Heure du dernier contact	Ce paramètre spécifie la durée (en nombre de jours) pendant laquelle un terminal peut rester déconnecté de BlackBerry UEM. Ce paramètre s'applique uniquement si le paramètre Terminal non joignable est sélectionné.
Niveau requis du correctif de sécurité manquant	Ce paramètre crée une règle de conformité pour veiller à ce que les terminaux disposent des correctifs de sécurité spécifiés. Vous pouvez spécifier les modèles de terminaux et les dates des correctifs de sécurité. Les terminaux exécutant un correctif de sécurité de date équivalente ou ultérieure aux dates de correctif de sécurité spécifiées sont considérés comme conformes. Ce paramètre s'applique uniquement aux terminaux exécutant Android 6.0 et versions ultérieures et aux terminaux PRIV exécutant Android 5.1.1 et versions ultérieures.

Android : paramètre de profil de conformité	Description
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 BlackBerry UEM au-delà du laps de temps spécifié. L'action d'application concerne les applications BlackBerry Dynamics.
Baser l'intervalle de connectivité sur des applications de délégation de l'authentification	Ce paramètre spécifie que la vérification de la connectivité repose sur la connexion d'une application de délégation de l'authentification à BlackBerry UEM. Ce paramètre est uniquement valide si le paramètre Vérification de la connectivité est sélectionné.
Heure du dernier contact	Ce paramètre spécifie le nombre de jours à l'issue duquel le terminal devra se connecter à BlackBerry UEM. Valeurs possibles : • 8 heures • 16 heures • 1 jour • 2 jours • 3 jours • 7 jours • 14 jours • 30 jours • 60 jours • 90 jours • 180 jours • 365 jours La valeur par défaut est 2 jours.

Android : paramètre de profil de conformité	Description
Une application interdite est installée	Ce paramètre crée une règle de conformité pour vérifier qu'aucune application interdite n'est installée sur les terminaux. Pour plus d'informations sur les applications interdites, reportez-vous à Ajouter une application à la liste des applications limitées. Pour les terminaux Android dotés d'un profil professionnel, 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. 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'onglet Terminaux gérés. Lorsque vous cliquez sur le lien, la liste des applications qui mettent le terminal hors conformité est affichée.
Le mot de passe ne répond pas aux critères de complexité	Ce paramètre crée une règle de conformité pour faire en sorte que l'utilisateur définisse des mots de passe pour le terminal ou l'espace de travail répondant aux exigences de complexité définies dans la stratégie informatique qui leur a été attribuée.
Appliquer les mesures de conformité dans l'espace personnel	Pour les terminaux Samsung KNOX, vous pouvez sélectionner ce paramètre pour empêcher les utilisateurs d'installer une application interdite dans les espaces Personnel et Travail.

Windows : paramètres de profil de conformité

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

Windows : paramètre de 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. Seuls les terminaux exécutant Windows Phone 8.0 permettent de suivre les dispositions des applications internes. Lorsque vous sélectionnez ce paramètre et qu'une application requise n'est pas installée sur un terminal Windows Phone, un message d'avertissement et un lien sont affichés sur l'onglet Terminaux gérés. Lorsque vous cliquez sur le lien, la liste des applications qui mettent le terminal hors conformité est affichée.

Windows : paramètre de profil de conformité	Description
Une version limitée du SE est installée	Ce paramètre crée une règle de conformité pour veiller à ce qu'une version limitée du système d'exploitation ne soit pas installée sur les terminaux, comme spécifié dans ce paramètre. Vous pouvez sélectionner les versions limitées du système d'exploitation.
Modèle de terminal interdit détecté	Ce paramètre crée une règle de conformité pour interdire les modèles de terminaux spécifiés. Valeurs possibles : • Autoriser les modèles de terminaux sélectionnés • Ne pas autoriser les modèles de terminaux sélectionnés Vous pouvez sélectionner les modèles de terminaux autorisés ou interdits.
Terminal non joignable	Ce paramètre crée une règle de conformité pour veiller à ce que les terminaux ne restent pas déconnectés de BlackBerry UEM au-delà du laps de temps spécifié.
Vérification de la version de la bibliothèque BlackBerry Dynamics	Ce paramètre crée une règle de conformité qui vous permet de sélectionner les versions de la bibliothèque BlackBerry Dynamics ne pouvant 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 BlackBerry UEM au-delà du laps de temps spécifié. L'action d'application 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.
État du pare-feu	Ce paramètre crée une règle de conformité pour veiller à ce qu'un pare-feu soit activé sur les terminaux.
État de cryptage	Ce paramètre crée une règle de conformité pour veiller à ce que le cryptage soit activé sur les terminaux.
État des mises à jour Windows	Ce paramètre crée une règle de conformité pour veiller à ce que les terminaux autorisent BlackBerry UEM à installer les mises à jour de Windows OS ou avertissent les utilisateurs lorsque des mises à jour obligatoires sont disponibles.
Une application interdite est installée	Ce paramètre crée une règle de conformité pour vérifier qu'aucune application interdite n'est installée sur les terminaux. Pour plus d'informations sur les applications interdites, reportez-vous à Ajouter une application à la liste des applications limitées. Ce paramètre s'applique aux terminaux exécutant Windows Phone 8.1 et versions ultérieures.

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

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

Paramètres de profil BlackBerry Dynamics

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

- iOS
- Android
- macOS
- Windows

Paramètre de profil BlackBerry Dynamics	Description
Configuration	
Demander l'utilisation de la gestion des terminaux pour utiliser les applications BlackBerry Dynamics	Ce paramètre détermine si un terminal doit être activé avec MDM pour utiliser les applications BlackBerry Dynamics.

Paramètre de profil BlackBerry Dynamics	Description
Autoriser UEM Client à s'inscrire dans BlackBerry Dynamics	Si un terminal utilise BlackBerry UEM Client, ce paramètre indique si BlackBerry Dynamics gère l'activation des applications BlackBerry Dynamics et si les applications BlackBerry Dynamics peuvent être utilisées sur le terminal. Si cette option n'est pas sélectionnée, les applications BlackBerry Dynamics peuvent être supprimées du terminal, car celui-ci n'est pas activé pour BlackBerry Dynamics. Si vous n'avez pas l'intention d'utiliser BlackBerry Dynamics dans votre environnement, ne sélectionnez pas cette option.
Mot de passe	
Expiration du mot de passe	Ce paramètre détermine si le mot de passe d'une application BlackBerry Dynamics expire. Si oui, il détermine aussi la durée de validité du mot de passe avant expiration.
Ne pas autoriser les mots de passe précédents	Ce paramètre détermine si de précédents mots de passe peuvent être utilisés. Si oui, il détermine aussi le nombre maximum de mots de passe précédents qu'il est impossible d'utiliser pour une application BlackBerry Dynamics.
Longueur minimale du mot de passe	Ce paramètre détermine la longueur minimale du mot de passe d'une application BlackBerry Dynamics.
Occurrences autorisées d'un caractère	Ce paramètre détermine le nombre d'occurrences d'un même caractère dans le mot de passe d'une application BlackBerry Dynamics.
Demander à la fois des lettres et des chiffres	Ce paramètre détermine si le mot de passe d'une application BlackBerry Dynamics doit contenir des lettres et des chiffres.
Demander à la fois des majuscules et des minuscules	Ce paramètre détermine si le mot de passe d'une application BlackBerry Dynamics doit contenir des lettres majuscules et minuscules.
Demander des caractères spéciaux	Ce paramètre détermine si le mot de passe d'une application BlackBerry Dynamics doit contenir au moins un caractère spécial.
Ne pas autoriser les séquences de plus de deux chiffres	Ce paramètre détermine si le mot de passe d'une application BlackBerry Dynamics peut contenir plus de deux chiffres qui se suivent (par exemple 1, 2, 3).
Ne pas autoriser plus d'une modification du mot de passe par jour	Ce paramètre détermine si le mot de passe d'une application BlackBerry Dynamics peut être modifié plusieurs fois toutes les 24 heures.
Ne pas autoriser les informations personnelles	Ce paramètre détermine si les informations personnelles suivantes peuvent être utilisées dans le mot de passe d'une application BlackBerry Dynamics : • Nom et prénom de l'utilisateur (à l'exception de ses initiales), comme stipulé dans Active Directory. • Segment d'une adresse électronique précédant le signe @.

Paramètre de profil BlackBerry Dynamics	Description
Autoriser la biométrie	Ce paramètre détermine si les applications BlackBerry Dynamics peuvent être déverrouillées à l'aide d'une entrée biométrique lorsqu'elles sont déjà ouvertes dans le sélecteur d'application des terminaux iOS. Vous pouvez autoriser les options suivantes : • Aucun • Autoriser Touch ID • Autoriser Face ID • Autoriser Touch ID et Face ID
Activer Touch ID et Face ID à partir d'un démarrage à froid	Ce paramètre détermine si les applications BlackBerry Dynamics peuvent être déverrouillées à l'aide de la méthode d'entrée biométrique sélectionnée lorsqu'elles sont ouvertes pour la première fois après un redémarrage du terminal.
Demander que le mot de passe soit de nouveau saisi pour désactiver Touch ID et Face ID	Ce paramètre spécifie la durée après laquelle les utilisateurs doivent saisir un mot de passe pour déverrouiller une application BlackBerry Dynamics et réactiver Touch ID, Face ID, ou les deux.
Autoriser l'authentification Android p empreinte digitale	Ce paramètre indique si BlackBerry Dynamics les applications peuvent être débloquées en utilisant Android l'authentification par empreintes digitales.
Ne pas demander de mot de passe	Ce paramètre précise si un utilisateur peut accéder à une application BlackBerry Dynamics sans saisir de mot de passe. Les choix sont les suivants : • iOS • macOS • Android • Windows
Liste de mots de passe bloqués	
Fichier de mots de passe bloqués (.txt)	Ce paramètre spécifie une liste de mots de passe interdits. Vous pouvez télécharger la liste de mots de passe interdits précédemment chargée. Les mots de passe de la liste doivent répondre aux critères suivants : chaque mot de passe doit être séparé par un retour à la ligne, seuls les caractères UTF-8 sont pris en charge, et les mots de passe doivent comporter 14 caractères maximum.
Écran de verrouillage	
Demander un mot de passe au démarrage des applications BlackBerry Dynamics	Ce paramètre détermine si un mot de passe est requis chaque fois qu'une application BlackBerry Dynamics est lancée. **Remarque :** Si vous utilisez la délégation d'authentification, ne sélectionnez pas cette option.

Paramètre de profil BlackBerry Dynamics	Description
Demander un mot de passe après une période d'inactivité	Ce paramètre détermine la période d'inactivité à l'issue de laquelle un mot de passe est requis.
Prendre des mesures après divers échecs de saisie du mot de passe	Ce paramètre détermine si le nombre de saisies d'un mot de passe incorrect est limité. Si vous sélectionnez cette règle, spécifiez le nombre de tentatives de saisie de mot de passe possibles et l'action qui s'ensuit lorsque la limite est atteinte. Choisissez l'une des actions suivantes : • Bloquer l'utilisateur • Effacer les données
Portables	
Autoriser les appareils portables	Ce paramètre détermine si les applications BlackBerry Dynamics peuvent être utilisées sur un appareil portable. Si vous sélectionnez cette règle, spécifiez le laps de temps à l'issue duquel l'appareil portable sera déconnecté et s'il peut se reconnecter automatiquement.
Délégation d'authentification d'application	
	Vous pouvez sélectionner jusqu'à trois applications qui serviront de délégué d'authentification pour d'autres applications afin d'éviter que les utilisateurs aient à créer un mot de passe pour chaque application BlackBerry Dynamics qu'ils installent. Une fois qu'un délégué d'authentification est configuré, chaque fois qu'un utilisateur ouvre une application BlackBerry Dynamics, le terminal affiche l'écran de mot de passe du délégué d'authentification au lieu de l'application qu'il essaie d'ouvrir. Une fois le mot de passe du délégué d'authentification saisi, l'utilisateur peut ouvrir l'application BlackBerry Dynamics. N'importe quelle application peut être choisie comme délégué d'authentification, mais nous vous conseillons de choisir l'application la plus couramment utilisée comme délégué d'authentification principal.
Lutte contre les fuites de données	
Ne pas autoriser la copie de données d'applications non BlackBerry Dynamics dans des applications BlackBerry Dynamics	Ce paramètre détermine si les utilisateurs peuvent copier des données d'applications non BlackBerry Dynamics dans des applications BlackBerry Dynamics.
Ne pas autoriser la dictée Android	Ce paramètre détermine si les utilisateurs de terminaux Android peuvent utiliser la dictée vocale avec les applications BlackBerry Dynamics.

Paramètre de profil BlackBerry Dynamics	Description
Ne pas autoriser les captures d'écran sur les terminaux Android	Ce paramètre détermine si les utilisateurs de terminaux Android peuvent effectuer des captures d'écran dans les applications BlackBerry Dynamics.
Ne pas autoriser l'enregistrement et le partage d'écran sur les terminaux iOS	Ce paramètre détermine si les utilisateurs de terminaux iOS peuvent partager et enregistrer des écrans dans les applications BlackBerry Dynamics. Ce paramètre s'applique aux terminaux exécutant iOS 11 et version ultérieure.
Ne pas autoriser la dictée iOS	Ce paramètre détermine si les utilisateurs de terminaux iOS peuvent utiliser la dictée vocale avec les applications BlackBerry Dynamics.
Ne pas autoriser les claviers personnalisés sur les terminaux iOS	Ce paramètre détermine si les utilisateurs de terminaux iOS peuvent utiliser des claviers personnalisés avec les applications BlackBerry Dynamics.
Activer le mode FIPS	Ce paramètre détermine si la norme américaine FIPS (Federal Information Processing) 140-2 s'applique.
Certificats	
Activer le magasin de certificats du terminal	Ce paramètre détermine si les applications BlackBerry Dynamics peuvent obtenir des certificats du magasin de certificats du terminal.
Journalisation détaillée	
Autoriser la journalisation détaillée pour les applications BlackBerry Dynamics	Ce paramètre indique si les fichiers journaux peuvent être générés et chargés à partir des applications BlackBerry Dynamics.
Empêcher les utilisateurs d'activer la journalisation détaillée dans les applications BlackBerry Dynamics	Ce paramètre indique si les utilisateurs peuvent activer la génération et le partage des fichiers journaux détaillés provenant des applications BlackBerry Dynamics.
Accord	

Paramètre de profil BlackBerry Dynamics	Description
Activer un message d'acceptation pour les applications BlackBerry Dynamics	Ce paramètre détermine si un message d'acceptation doit s'afficher pour les applications BlackBerry Dynamics. Si la délégation d'authentification est activée, le message s'affiche uniquement dans l'application d'authentification. Si vous sélectionnez cette règle, procédez comme suit : • Spécifiez si le message doit s'afficher chaque fois que l'application est déverrouillée. Si ce n'est pas le cas, le message s'affichera uniquement la première fois que l'utilisateur ouvrira l'application. • Dans le champ **Message**, entrez le message à afficher. **Remarque :** Sur les terminaux Android, seuls les 4 000 premiers caractères sont affichés.

BlackBerry Dynamics : paramètres de profil de connectivité

Les profils de connectivité BlackBerry Dynamics sont pris en charge sur les types de terminaux suivants :

- iOS
- Android
- macOS
- Windows

Paramètre de profil de connectivité BlackBerry Dynamics	Description
Importer le profil de connectivité BlackBerry Dynamics	Cliquez sur l'icône pour importer des paramètres de connectivité depuis un fichier .csv. Lorsque vous importez un fichier .csv, il remplace le contenu du profil de connectivité. Cela facilite le processus si vous devez modifier manuellement des valeurs ou si plusieurs URL ou serveurs requièrent des modifications.
Exporter le profil de connectivité BlackBerry Dynamics	Cliquez sur pour exporter des paramètres de connectivité vers un fichier .csv.
Infrastructure	
Acheminer tout le trafic	Spécifiez si toutes les données d'application BlackBerry Dynamics sont acheminées via BlackBerry Proxy. Pour plus d'informations, reportez-vous à Acheminement de toutes les données d'une application BlackBerry Dynamics via BlackBerry Proxy.
Domaine	Spécifiez les domaines Internet auxquels vous souhaitez autoriser l'accès, au format *.domaine. Par exemple, `blackberry.com` permet d'accéder à n'importe quel serveur du domaine blackberry.com. Les applications BlackBerry Dynamics sont autorisées à se connecter à tous les serveurs des domaines répertoriés dans ce tableau via le pare-feu de votre entreprise.

Paramètre de profil de connectivité BlackBerry Dynamics	Description
Clusters BlackBerry Proxy principal et secondaire	Spécifiez le nom de domaine complet, le port et la priorité des clusters BlackBerry Proxy à utiliser pour accéder au domaine.
Domaines par défaut	
Domaine	Spécifiez les domaines autorisés par défaut (par exemple, qa.blackberry.com). Les applications BlackBerry Dynamics peuvent essayer de se connecter à un nom d'hôte incomplets tel que " portail " au lieu d'utiliser un nom de domaine complet tel que » portail.ventes.xyzcorp.com ». Les domaines répertoriés dans cette liste seront ajoutés aux noms d'hôtes incomplets pour construire les noms de domaine samedi.
Serveurs supplémentaires	
Serveur	Spécifiez le nom de domaine complet des autres serveurs auxquels les applications BlackBerry Dynamics peuvent se connecter. Plutôt que d'utiliser la liste Domaines autorisés, ajoutez les serveurs à cette liste si vous souhaitez que les applications BlackBerry Dynamics se connectent uniquement à certains serveurs, et non à tous les serveurs d'un domaine.
Plages d'adresses IP	
Plage	Spécifiez une plage d'adresses IP auxquelles les applications BlackBerry Dynamics peuvent accéder. Les plages d'adresses doivent être entrées avec une adresse à limites inférieure et supérieure (par exemple, 192.168.2.0-192.168.2.255) ou en notation IPv4 CIDR (par exemple, 192.168.2.0/24). Par exemple : • Adresses distinctes : Exemple : //.192.168.2.0/2,255 • Sous-réseau entier : Exemple : //.192.168.2.0/24
Serveurs d'applications	Si vous disposez d'une application BlackBerry Dynamics prise en charge par un serveur d'applications ou par un serveur Web, vous pouvez spécifier le nom de ce serveur et la priorité des clusters BlackBerry Proxy utilisés pour communiquer avec elle. Pour plus d'informations, reportez-vous à Ajouter un serveur d'applications à un profil de connectivité BlackBerry Dynamics.

Paramètres de profil de connectivité d'entreprise

Les profils de connectivité d'entreprise sont pris en charge sur les types de terminaux suivants :

- BlackBerry 10

- iOS
- Android

Communs : paramètres de profil de connectivité d'entreprise

Communs : paramètre de profil de conformité	Description
Groupe de serveurs BlackBerry Secure Connect Plus	Ce paramètre spécifie le groupe de serveurs utilisé par BlackBerry Secure Connect Plus pour diriger le trafic vers un chemin régional spécifique. Ce paramètre est valide uniquement si vous avez installé une ou plusieurs instances de BlackBerry Connectivity Node et configuré des groupes de serveurs.

BlackBerry 10 : paramètres de profil de connectivité d'entreprise

Paramètre	Description
Connectivité d'entreprise	La connectivité d'entreprise est toujours activée pour les terminaux BlackBerry 10. Vous ne pouvez pas modifier ce paramètre.
Profil de proxy	Ce paramètre indique le profil proxy associé si vous souhaitez acheminer le trafic du tunnel sécurisé des terminaux au réseau professionnel via un serveur proxy.
Enable BlackBerry Secure Connect Plus	Ce paramètre indique si les applications professionnelles utilisent BlackBerry Secure Connect Plus pour l'envoi de données professionnelles entre les terminaux et votre réseau.

iOS : paramètres de profil de connectivité d'entreprise

Paramètre	Description
Enable BlackBerry Secure Connect Plus	Ce paramètre indique si les applications professionnelles utilisent BlackBerry Secure Connect Plus pour l'envoi de données professionnelles entre les terminaux et votre réseau.
Activer VPN à la demande	Ce paramètre indique si une application professionnelle peut lancer automatiquement une connexion VPN à l'aide de BlackBerry Secure Connect Plus lorsqu'elle accède à des ressources professionnelles. Sélectionnez ce paramètre pour spécifier des règles pour les connexions BlackBerry Secure Connect Plus.
Règles de VPN à la demande pour iOS 9 ou version ultérieure	Ce paramètre spécifie les exigences de connexion pour le VPN à la demande à l'aide de BlackBerry Secure Connect Plus. Vous devez utiliser une ou plusieurs clés de l'exemple de format de charge utile. Ce paramètre est valide uniquement si le paramètre Activer VPN à la demande est sélectionné.

Paramètre	Description
Activer un VPN par application	Sélectionnez ce paramètre pour autoriser uniquement certaines applications à utiliser BlackBerry Secure Connect Plus. **Remarque :** Si vous sélectionnez cette option, les utilisateurs doivent activer manuellement la connexion VPN sur leur terminal pour pouvoir utiliser BlackBerry Secure Connect Plus. Tant que la connexion VPN est activée, le terminal utilise BlackBerry Secure Connect Plus pour se connecter au réseau d'entreprise. L'utilisateur doit désactiver la connexion VPN pour utiliser une autre connexion, telle que le réseau Wi-Fi de l'entreprise. Indiquez aux utilisateurs à quel moment il est approprié d'activer et de désactiver la connexion VPN (par exemple, vous pouvez leur demander d'activer la connexion VPN lorsqu'ils sont hors de portée du réseau Wi-Fi de l'entreprise).
Domaines Safari	Cliquez sur + pour spécifier les domaines autorisés à lancer une connexion VPN dans Safari.
Autoriser la connexion automatique des applications	Spécifiez si les applications peuvent lancer la connexion VPN automatiquement.
Profil de proxy	Ce paramètre indique le profil proxy associé si vous souhaitez acheminer le trafic du tunnel sécurisé des terminaux au réseau professionnel via un serveur proxy. Le profil de proxy doit utiliser une configuration manuelle avec une adresse IP. La Configuration PAC n'est pas prise en charge. Pour plus d'informations, reportez-vous à Création de profils proxy pour les terminaux.

Android : paramètres de profil de connectivité d'entreprise

Paramètre	Description
Enable BlackBerry Secure Connect Plus	Ce paramètre indique si les applications professionnelles utilisent BlackBerry Secure Connect Plus pour l'envoi de données professionnelles entre les terminaux et votre réseau.
Connectivité d'entreprise pour les terminaux Android comprenant un espace Travail	Ce paramètre indique si le profil professionnel Android et les terminaux Samsung KNOX Workspace utilisent BlackBerry Secure Connect Plus pour toutes les applications dans l'espace Travail ou seulement pour les applications spécifiées. • « VPN à l'échelle du conteneur » utilise une connexion VPN pour toutes les applications dans l'espace Travail sur le terminal. • « VPN par application » utilise une connexion VPN uniquement pour les applications spécifiées.

Paramètre	Description
Applications non autorisées à utiliser BlackBerry Secure Connect Plus	Ce paramètre indique les applications de l'espace Travail sur les terminaux Android dotés d'un profil professionnel qui ne sont pas autorisés à utiliser BlackBerry Secure Connect Plus. Cliquez sur + et saisissez un ID de package d'application. Si nécessaire, répétez l'opération pour restreindre d'autres applications. Par défaut, Google Play et les services sous-jacents (com.android.providers.media, com.android.vending, com.google.android.gms et com.google.android.apps.gcs) sont restreints car Google Play ne prend en charge aucun proxy. Il est recommandé de maintenir ces restrictions. Si vous supprimez l'une de ces restrictions, vous devez contacter l'assistance Google Play pour obtenir la configuration de pare-feu requise afin d'autoriser les connexions à Google Play à l'aide de BlackBerry Secure Connect Plus. Si la stratégie informatique « Forcer les applications professionnelles à utiliser VPN uniquement » est appliquée au terminal, ce paramètre est ignoré et il n'est interdit à aucune application professionnelle, y compris BlackBerry UEM Client et Google Play, d'utiliser BlackBerry Secure Connect Plus. Dans ce cas, vous devez ouvrir les ports dans le pare-feu pour permettre à BlackBerry UEM Client de communiquer avec BlackBerry Infrastructure via BlackBerry UEM. Pour plus d'informations sur l'ouverture de ports dans le pare-feu lorsque les applications professionnelles utilisent BlackBerry Secure Connect Plus, rendez-vous sur http://support.blackberry.com/kb et consultez l'article KB 48330. Si votre entreprise utilise des applications BlackBerry Dynamics, nous vous recommandons d'empêcher celles-ci d'utiliser BlackBerry Secure Connect Plus. Si vous ne le faites pas, vous devrez ouvrir des ports supplémentaires sur le pare-feu de votre entreprise pour permettre aux applications d'envoyer des données à BlackBerry Dynamics NOC, et l'activité réseau depuis les applications pourra être retardée car les données seront acheminées à la fois vers BlackBerry Infrastructure et vers BlackBerry Dynamics NOC. Ce paramètre est valide uniquement si le paramètre « Connectivité d'entreprise pour les terminaux Android comprenant un espace Travail » est défini sur « VPN à l'échelle du conteneur ».
Applications autorisées à utiliser la connectivité d'entreprise	Ce paramètre indique les applications de l'espace Travail sur le profil professionnel Android et les terminaux Samsung KNOX Workspace qui sont autorisés à utiliser BlackBerry Secure Connect Plus. Vous pouvez sélectionner les applications dans la liste des applications disponibles ou spécifier l'ID de package d'application. Ce paramètre est valide uniquement si le paramètre « Connectivité d'entreprise pour les terminaux Android comprenant un espace Travail » est défini sur « VPN par application ».
Profil de proxy	Si vous souhaitez acheminer le trafic du tunnel sécurisé depuis les terminaux Samsung KNOX Workspace version 2.5 et ultérieure jusqu'au réseau professionnel via un serveur proxy, sélectionnez le profil de proxy adéquat. Ce paramètre ne s'applique ni aux terminaux Android dotés d'un profil professionnel, ni aux terminaux exécutant Samsung KNOX Workspace version 2.4 ou antérieure.

Paramètres du profil Enterprise Management Agent

Les profils Enterprise Management Agent sont pris en charge sur les types de terminaux suivants :

- BlackBerry 10
- iOS
- Android
- Windows

BlackBerry 10 : paramètres de profil Enterprise Management Agent

Paramètre	Description
Intervalle d'interrogation de Enterprise Management Web Service	Indiquez la fréquence (en secondes) à laquelle le service Enterprise Management Web Service du terminal demande des mises à jour de configuration. Valeurs possibles : • 3600 à 86400 La valeur par défaut est 3600.
Intervalle d'interrogation rapide	Indiquez la fréquence (en secondes) à laquelle le terminal demande des mises à jour de configuration lorsque la notification Push n'est pas disponible pour l'interrogation rapide (BPDS n'est pas enregistré). • Minimum : 900 La valeur par défaut est 900.
Intervalle d'interrogation lent	Indiquez la fréquence (en secondes) à laquelle le terminal demande des mises à jour de configuration lorsque la notification Push est disponible pour l'interrogation lente (BPDS est enregistré). • Minimum : 900 La valeur par défaut est 900.
Autoriser la collection d'applications personnelles	Ce paramètre spécifie si BlackBerry UEM doit recevoir une liste des applications personnelles installées sur les terminaux de l'utilisateur. Ce paramètre n'est pas pris en charge sur les terminaux ayant des activations de type Travail et Personnel - Entreprise.

Paramètre	Description
Fichier de configuration (.json)	Ce paramètre vous permet de spécifier un fichier de configuration pour définir quelles suites de codes de la bibliothèque SSL sont prises en charge par le terminal. Spécifiez un fichier de configuration que si vous voulez supprimer la prise en charge d'une suite de codes qui a une vulnérabilité de sécurité et que les ressources de votre organisation ne nécessitent pas cette suite de codes pour la communication. La spécification d'un fichier de configuration n'affecte pas la communication du terminal avec BlackBerry UEM mais peut avoir un impact sur la communication avec d'autres serveurs de votre organisation, en fonction des exigences de ces serveurs. Le fichier de configuration doit être au format .json. **Exemple :** `{"tls": {"tls_protocols": ["TLSv1"], "tls_ciphersuites": [49200, 49196, 49192, 49188, 49172, 49162, 163, 159, 107, 106, 57, 56, 136, 135, 49202, 49198, 49194, 49190, 49167, 49157, 157, 61, 53, 132, 141, 49199, 49195, 49191, 49187, 49171, 49161, 162, 158, 103, 64, 51, 50, 154, 153, 69, 68, 49201, 49197, 49193, 49189, 49166, 49156, 156, 60, 47, 150, 65, 140, 49169, 49159, 49164, 49154, 5, 4, 138, 49170, 49160, 22, 19, 49165, 49155, 10, 139, 21, 18, 9, 20, 17, 8, 6, 3], "tls_curves": ["secp256r1", "secp521r1", "brainpoolP512r1", "brainpoolP384r1", "secp384r1", "brainpoolP256r1", "secp256k1", "sect571r1", "sect571k1", "sect409k1", "sect409r1", "sect283k1", "sect283r1", "secp224k1", "secp224r1", "secp192k1", "secp192r1", "secp160k1", "secp160r1", "secp160r2", "sect239k1", "sect233k1", "sect233r1", "sect193r1", "sect193r2", "sect163k1", "sect163r1", "sect163r2"], "tls_sigalgs": ["ECDSA+SHA512", "DSA+SHA512", "RSA+SHA512", "ECDSA +SHA384", "DSA+SHA384", "RSA+SHA384", "ECDSA+SHA256", "DSA +SHA256", "RSA+SHA256", "ECDSA+SHA224", "DSA+SHA224", "RSA+SHA224", "ECDSA+SHA1", "DSA+SHA1", "RSA+SHA1"], "tls_dh_min_key_bits":768, "tls_suiteb_mode": "SUITEB_OFF"}, "vpn": {"vpn_encr": ["aes128", "aes256", "aes128_icv16_gcm", "aes256_icv16_gcm", "3des", "aes192"], "vpn_dh": ["dh2", "dh5", "dh7", "dh8", "dh9", "dh10", "dh11", "dh12", "dh13", "dh14", "dh15", "dh16", "dh17", "dh18", "dh19", "dh20", "dh21", "dh22", "dh23", "dh24", "dh25", "dh26"], "vpn_integ": ["sha1", "sha384", "sha512", "aes", "sha256"], "vpn_prf": ["sha1", "sha384", "sha512", "aes", "hmac", "sha256"]}}`

iOS : paramètres de profil Enterprise Management Agent

Paramètre	Description
Fréquence d'interrogation de Enterprise Management Agent	Indiquez la fréquence (en secondes) à laquelle le terminal interroge les commandes du serveur de Enterprise Management Agent. Valeurs possibles : • 900 to 86400 La valeur par défaut est 3600.
Autoriser la collection d'applications personnelles	Ce paramètre spécifie si BlackBerry UEM reçoit la liste des applications installées dans l'espace personnel de l'utilisateur. Ce paramètre n'est pas pris en charge sur les terminaux qui sont activés avec .

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. Valeurs possibles : • De 3600 à 86400 secondes La valeur par défaut est 3600.
Seuil de niveau de batterie	Indiquez le pourcentage de changement du niveau de la batterie (de 5 à 100) requis que le terminal ne renvoie les informations à BlackBerry UEM. Valeurs possibles : • 5 à 100 % La valeur par défaut est 20.
Seuil d'espace libre RAM	Indiquez le changement nécessaire de la quantité de mémoire libre en mégaoctets avant que le terminal ne renvoie des informations à BlackBerry UEM. Par défaut, le terminal n'envoie pas ces informations à BlackBerry UEM.
Seuil de stockage interne	Indiquez le changement nécessaire de la quantité d'espace de stockage libre interne en mégaoctets avant que le terminal ne renvoie des informations à BlackBerry UEM. La valeur par défaut est 250.
Seuil de la carte mémoire	Indiquez le changement de la quantité d'espace libre externe requis en mégaoctets avant que le terminal ne renvoie des informations à BlackBerry UEM . La valeur par défaut est 500.

Paramètre	Description
Fréquence d'interrogation de Enterprise Management Agent	Indiquez la fréquence (en secondes) à laquelle le terminal interroge les commandes du serveur de Enterprise Management Agent. Valeurs possibles : • Minimum : 900 La valeur par défaut est 900.
Autoriser la collection d'applications personnelles	Ce paramètre spécifie si BlackBerry UEM reçoit la liste des applications installées dans l'espace personnel de l'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.
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.

Paramètre	Description
Interrogation de tous les utilisateurs lors de la première connexion	Indiquez si le terminal doit lancer une session de gestion lors de la première connexion de tous les utilisateurs.
Autoriser la collection d'applications personnelles	Ce paramètre spécifie si BlackBerry UEM reçoit la liste des applications installées dans l'espace personnel de l'utilisateur.

Paramètres des profils de protection des données Windows

Les profils de protection des données Windows sont pris en charge sur les types de terminaux suivants :

- Windows 10

Windows 10 : Windows paramètres de profil de protection des données

Windows 10 : Windows paramètre de profil de protection des données	Description
Paramètres de protection des données Windows	Ce paramètre indique si la protection des données Windows est activée et son degré d'application. Lorsque ce paramètre est défini sur « Désactivé », les données ne sont pas cryptées et la journalisation des audits est désactivée. Lorsque ce paramètre est défini sur « Silencieux », les données sont cryptées et toute tentative de partage de données protégées est consignée. Lorsque ce paramètre est défini sur « Remplacer », les données sont cryptées, l'utilisateur reçoit une invite lorsqu'il tente de partager des données protégées, et toute tentative de partage de données protégées est consignée. Lorsque ce paramètre est défini sur « Bloquer », les données sont cryptées, les utilisateurs ne peuvent pas partager des données protégées, et toute tentative de partage de données protégées est consignée. Valeurs possibles : • O • Silencieux • Remplacer • Bloquer La valeur par défaut est « Off ».
Noms de domaines d'entreprise protégés	Ce paramètre spécifie les noms des domaines du réseau professionnel que votre entreprise utilise pour les identités de ses utilisateurs. Vous pouvez séparer plusieurs domaines avec des barres verticales (|). Le premier domaine est utilisé comme une chaine pour marquer les fichiers protégés par des applications qui utilisent WIP. Par exemple : `exemple.com|exemple.net`.

Windows 10 : Windows paramètre de profil de protection des données	Description
Fichier de certificat de récupération de données (.der, .cer)	Ce paramètre spécifie le fichier de certificat de récupération de données. Le fichier que vous spécifiez doit être un certificat codé PEM ou DER, avec une extension de fichier.der ou .cer. Vous utilisez le fichier de certificat de récupération de données pour récupérer des fichiers qui étaient protégés localement sur un terminal. Par exemple, si votre entreprise souhaite récupérer des données protégées par WIP depuis un terminal. Pour plus d'informations sur la création d'un certificat de récupération des données, consultez la documentation relative à la protection des données MicrosoftWindows.
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. Lorsque 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. Par défaut, cette option n'est pas sélectionnée.
Serveurs proxy internes d'entreprise	Ce paramètre spécifie les serveurs proxy internes qui sont utilisés lors de la connexion à des emplacements de réseaux professionnels. Ces serveurs proxy sont utilisés uniquement lors de la connexion à des domaines répertoriés dans les paramètres des ressources Enterprise Cloud.
Ressources d'entreprise dans le cloud	Ce paramètre spécifie la liste des domaines de ressources d'entreprise hébergés dans le cloud qui doivent être protégés. Les données de ces ressources sont considérées comme des données d'entreprise et sont donc protégées.
Domaine de ressources dans le cloud	Ce paramètre spécifie le nom du domaine.

Windows 10 : Windows paramètre de profil de protection des données	Description
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. Par exemple, `exemple.com`, `exemple.net`.
Code de charge utile d'application de bureau	Spécifiez les clés et les valeurs des applications de bureau qui sont utilisées pour configurer les restrictions de lancement d'application sur les terminaux Windows 10. Vous devez utiliser les clés définies par Microsoft pour le type 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>` Pour plus d'informations sur l'utilisation d'AppLocker, reportez-vous à https://technet.microsoft.com/en-us/itpro/windows/keep-secure/administer-applocker.

Windows 10 : Windows paramètre de profil de protection des données	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>`
	
	Pour plus d'informations sur l'utilisation d'AppLocker, reportez-vous à https://technet.microsoft.com/en-us/itpro/windows/keep-secure/administer-applocker.

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

Paramètres du profil de protection des applications Microsoft Intune

Les profils de protection des applications Microsoft Intune sont pris en charge sur les types de terminaux suivants :

- iOS
- Android

Commun : paramètres du profil de protection des applications Microsoft Intune

Paramètres du profil de protection des applications Intune	Description
Interopérabilité	
Activer l'interopérabilité entre les applications Intune et Dynamics	Ce paramètre détermine si les applications BlackBerry Dynamics peuvent interagir avec les applications gérées Intune, notamment les applications Microsoft Office 365 sur le terminal. Pour permettre l'interopérabilité entre les applications BlackBerry Dynamics et les applications gérées Intune, BlackBerry Enterprise BRIDGE doit être installé sur les terminaux des utilisateurs. Pour plus d'informations, consultez le Guide d'administration de BlackBerry Enterprise BRIDGE.
Réadressage des données	
Autoriser l'application à transférer des données vers d'autres applications	Ce paramètre spécifie les applications auxquelles les applications gérées par Intune peuvent envoyer des données. Valeurs possibles : • Applications gérées par une stratégie : cette option permet de transférer des données uniquement vers d'autres applications gérées par Intune. • Toutes les applications • Aucun

Paramètres du profil de protection des applications Intune	Description
Interopérabilité	
Autoriser une application à recevoir des données d'autres applications	Ce paramètre spécifie les applications à partir desquelles les applications gérées par une stratégie de protection des applications peuvent recevoir des données. Valeurs possibles : • Applications gérées par une stratégie : cette option permet de transférer des données uniquement à partir d'autres applications gérées par Intune. • Toutes les applications • Aucun
Interdire « Enregistrer sous »	Ce paramètre spécifie si l'option « Enregistrer sous » est activée pour les applications. Si vous sélectionnez ce paramètre, vous pouvez autoriser l'utilisation de l'option Enregistrer sous pour enregistrer uniquement des données professionnelles à un ou plusieurs des emplacements suivants : • Stockage local • OneDrive for Business • SharePoint
Limiter les opérations couper, copier et coller avec d'autres applications	Ce paramètre spécifie comment les opérations couper, copier et coller peuvent être utilisées avec l'application. Valeurs possibles : • Bloqué : cette option empêche les opérations couper, copier et coller entre cette application et d'autres applications. • Applications gérées par une stratégie : cette option autorise les opérations couper, copier et coller entre l'application et d'autres applications gérées par Intune. • Applications gérées par une stratégie avec l'option coller : cette option permet de coller des données de n'importe quelle application, mais les données coupées ou copiées à partir d'une application gérée par une stratégie peuvent être collées uniquement dans d'autres applications gérées par Intune. • N'importe quelle application : cette option autorise les opérations couper, copier et coller entre toutes les applications sur le terminal.
Limiter le contenu Web affiché dans le navigateur géré	Ce paramètre indique si les liens Web dans les applications doivent être ouverts dans un navigateur géré par Intune.
Désactiver la synchronisation des contacts	Ce paramètre spécifie si l'application peut enregistrer des contacts dans l'application native Contacts du terminal.
Désactiver l'impression	Ce paramètre spécifie si l'application peut imprimer des données.

Paramètres du profil de protection des applications Intune	Description
Interopérabilité	
Accès	
Les informations d'identification de l'entreprise sont requises pour l'accès	Ce paramètre indique si les utilisateurs doivent utiliser les informations d'identification de leur entreprise pour accéder à l'application. Si vous sélectionnez cette règle, elle est prioritaire sur les exigences de code PIN ou d'empreintes digitales.
Bloquer l'exécution des applications gérées sur des terminaux débridés ou flashés	Ce paramètre spécifie si les applications peuvent être exécutées sur des terminaux débridés ou flashés.
Délai d'expiration de la revérification des conditions d'accès	Ce paramètre spécifie, en nombre de minutes, à quelle fréquence les conditions d'accès à l'application sont revérifiées lorsque l'application est ouverte.
Période de grâce hors connexion	Ce paramètre spécifie, en nombre de minutes, à quelle fréquence les conditions d'accès à l'application sont revérifiées lorsque le terminal est hors ligne.
Intervalle hors connexion avant l'effacement des données de l'application	Ce paramètre spécifie, en nombre de jours, combien de temps un terminal peut rester hors ligne avant que les données de l'application soient effacées du terminal.
Code PIN requis pour l'accès	Ce paramètre indique si les utilisateurs doivent saisir un code PIN pour accéder à l'application. Si vous sélectionnez cette option, l'utilisateur est invité à fournir un code PIN à la première exécution de l'application. Si l'option « Les informations d'identification de l'entreprise sont requises pour l'accès » est sélectionnée, elle est prioritaire sur cette règle.
Nombre de tentatives avant la réinitialisation du code PIN	Ce paramètre spécifie le nombre de tentatives de saisie du code PIN autorisé avant la réinitialisation du code PIN.
Autoriser un code PIN simple	Ce paramètre spécifie si les utilisateurs peuvent utiliser des séquences de code PIN simples, comme 1234 ou 1111.
Longueur du code PIN	Ce paramètre spécifie le nombre minimum de chiffres du code PIN.
Autoriser les empreintes digitales au lieu du code PIN	Ce paramètre spécifie si les utilisateurs peuvent utiliser les empreintes digitales au lieu d'un code PIN pour accéder à l'application. Ce paramètre est pris en charge par iOS versions 8.0 et ultérieures et Android versions 6.0 et ultérieures.

Paramètres du profil de protection des applications Intune	Description
Interopérabilité	
Désactiver le code PIN de l'application lorsque le code PIN du terminal est géré	Ce paramètre permet de définir si une invite de l'application demande à saisir le code PIN lorsque le terminal doit disposer d'un mot de passe. Si ce paramètre est sélectionné, le code PIN de l'application n'est pas demandé sur les terminaux Android si la stratégie informatique UEM du terminal nécessite un mot de passe. Pour désactiver le code PIN de l'application sur les terminaux iOS, le code PIN du terminal doit être requis par Intune.

iOS : paramètres du profil de protection des applications Microsoft Intune

Paramètres du profil de protection des applications Intune	Description
Chiffrer les données de l'application	Ce paramètre spécifie quand les données de l'application sont chiffrées. Valeurs possibles : • Lorsque le terminal est verrouillé : cette option permet de chiffrer toutes les données de l'application quand le terminal est verrouillé. • Lorsque le terminal est verrouillé et que les fichiers sont ouverts : cette option permet de chiffrer les données de l'application quand le terminal est verrouillé. Les données des fichiers ouverts ne sont pas chiffrées • Après le redémarrage du terminal : cette option permet de chiffrer les données de l'application quand le terminal est redémarré jusqu'au premier déverrouillage du terminal. • Utiliser les paramètres du terminal : cette option permet de chiffrer les données de l'application selon les paramètres par défaut du terminal. Cette option nécessite la configuration d'un mot de passe pour le terminal.
Interdire les sauvegardes iTunes et iCloud	Ce paramètre indique si les données de l'application peuvent être sauvegardées sur iTunes ou iCloud.
Identifiants des packages d'applications	Ce paramètre spécifie l'identifiant du package d'applications appliqué par ce profil. Vous pouvez saisir l'ID de package ou le choisir dans la liste des applications gérées Intune disponibles.
Requiert une version minimale du système d'exploitation iOS	Sélectionnez cette option pour spécifier une version minimale de iOS pour utiliser cette application. Si la version de iOS installée sur le terminal ne répond pas à cette exigence, l'utilisateur ne peut pas utiliser l'application. Vous pouvez spécifier un seul point décimal (par exemple, 10.3).
Requiert une version minimale du système d'exploitation iOS (avertissement seulement)	Sélectionnez cette option pour spécifier une version minimale recommandée de iOS pour utiliser cette application. Si la version de iOS installée sur le terminal ne répond pas à cette exigence, l'utilisateur reçoit une notification qui peut être ignorée. Vous pouvez spécifier un seul point décimal (par exemple, 10.3).

Paramètres du profil de protection des applications Intune	Description
Requiert une version minimale de l'application	Sélectionnez cette option pour spécifier une version minimale de l'application pour pouvoir l'utiliser. Si la version de l'application installée sur le terminal ne répond pas à cette exigence, l'utilisateur ne peut pas utiliser cette application. Vous pouvez spécifier un seul point décimal (par exemple, 4.2). Étant donné que différentes applications ont généralement des systèmes de gestion des versions distincts, si vous souhaitez spécifier une version minimale d'une application, vous devez créer un profil distinct pour chaque application.
Requiert une version minimale de l'application (avertissement seulement)	Sélectionnez cette option pour spécifier une version minimale recommandée de l'application pour pouvoir l'utiliser. Si la version de l'application installée sur le terminal ne répond pas à cette exigence, l'utilisateur reçoit une notification qui peut être ignorée. Vous pouvez spécifier un seul point décimal (par exemple, 4.2). Parce que les différentes applications ont généralement des systèmes de gestion des versions distinctes, si vous voulez spécifier un minimum version app, vous devez créer un profil distinct pour chaque application.

Android : paramètres du profil de protection des applications Microsoft Intune

Paramètres du profil de protection des applications Intune	Description
Chiffrer les données de l'application	Ce paramètre spécifie si les données de l'application sont chiffrées ou non. Si vous sélectionnez cette règle, les données de l'application sont chiffrées de façon synchronisée durant les tâches de saisie et de production de fichiers.
Interdire les sauvegardes Android	Ce paramètre indique si les données de l'application peuvent être sauvegardées ou non sur le service de sauvegarde Android.
Bloquer la capture d'écran et l'assistant Android	Ce paramètre indique si les fonctionnalités de capture d'écran et d'analyse de l'application de l'assistant Android sont autorisées ou non lors de l'utilisation d'une application protégée. Ce paramètre est pris en charge par Android 6.0 et versions ultérieures.
Identifiants des packages d'applications	Ce paramètre spécifie l'identifiant du package d'applications appliqué par ce profil. Vous pouvez saisir l'ID de package ou le choisir dans la liste des applications gérées Intune disponibles.
Requiert une version minimale de Android	Sélectionnez cette option pour spécifier une version minimale de Android pour utiliser cette application. Si la version de Android installée sur le terminal ne répond pas à cette exigence, l'utilisateur ne peut pas utiliser l'application. Vous pouvez indiquer jusqu'à quatre identifiants de version. Séparez les identifiants par des points (par exemple, 10.3 ou 10.3.14.2).

Paramètres du profil de protection des applications Intune	Description
Version Android minimale requise (avertissement uniquement)	Sélectionnez cette option pour spécifier une version minimale recommandée de Android pour utiliser cette application. Si la version de Android installée sur le terminal ne répond pas à cette exigence, l'utilisateur reçoit une notification qui peut être ignorée. Vous pouvez indiquer jusqu'à quatre identifiants de version. Séparez les identifiants par des points (par exemple, 10.3 ou 10.3.14.2).
Version du correctif Android minimale requise (avertissement uniquement)	Sélectionnez ce paramètre pour spécifier une version minimale du correctif Android pour utiliser cette application. Si la version du correctif Android installée sur le terminal ne répond pas à cette exigence, l'utilisateur ne peut pas utiliser l'application. Spécifiez la version en utilisant le format de date AAAA-MM-JJ.
Version du correctif Android minimale requise (avertissement uniquement)	Sélectionnez ce paramètre pour spécifier une version minimale recommandée du correctif Android pour utiliser cette application. Si la version du correctif Android installée sur le terminal ne répond pas à cette exigence, l'utilisateur reçoit une notification qui peut être ignorée. Spécifiez la version en utilisant le format de date AAAA-MM-JJ.
Version app nécessitent un minimum	Sélectionnez cette option pour spécifier une version minimale de l'application pour pouvoir l'utiliser. Si la version de l'application installée sur le terminal ne répond pas à cette exigence, l'utilisateur ne peut pas utiliser cette application. Vous pouvez indiquer jusqu'à quatre identifiants de version. Séparez les identifiants par des points (par exemple, 10.3 ou 10.3.14.2). Parce que les différentes applications ont généralement des systèmes de gestion des versions distinctes, si vous voulez spécifier un minimum version app, vous devez créer un profil distinct pour chaque application.
Version app nécessitent un minimum (Avertissement uniquement)	Sélectionnez cette option pour spécifier une version minimale recommandée de l'application pour pouvoir l'utiliser. Si la version de l'application installée sur le terminal ne répond pas à cette exigence, l'utilisateur reçoit une notification qui peut être ignorée. Vous pouvez indiquer jusqu'à quatre identifiants de version. Séparez les identifiants par des points (par exemple, 10.3 ou 10.3.14.2). Parce que les différentes applications ont généralement des systèmes de gestion des versions distinctes, si vous voulez spécifier un minimum version app, vous devez créer un profil distinct pour chaque application.

Feuille de référence des stratégies

Pour en savoir plus sur les stratégies informatiques, téléchargez la Fiche de référence des stratégies à l'adresse help.blackberry.com/detectLang/blackberry-uem/current/policy-reference-spreadsheet-zip/

Glossaire

AES	Advanced Encryption Standard (méthode de cryptage avancé)
AET	Jeton d'inscription d'application
APNs	Apple Push Notification service (Service Apple Push Notification)
BES5	BlackBerry Enterprise Server 5
BES10	BlackBerry Enterprise Service 10
BES12	BlackBerry Enterprise Service 12
Instance de BES12	Le terme « instance de BES12 » désigne tous les composants BES12 installés sur un ordinateur, à l'exception de BlackBerry Router, qui est un composant facultatif installé séparément. Une instance de BES12 est parfois appelée « unité d'échelle ».
Protocole inter-processus BlackBerry	Le protocole inter-processus BlackBerry est un protocole propriétaire qui génère la clé de session que les composants de BlackBerry Enterprise Solution tels que BlackBerry Enterprise Server et BlackBerry Mobile Voice System peuvent utiliser pour communiquer mutuellement de façon hautement sécurisée. Le protocole inter-processus BlackBerry génère la clé de session en fonction du mot de passe de communication.
BlackBerry UEM domain	A BlackBerry UEM domain consists of a BlackBerry UEM database and a BlackBerry Control database and any BlackBerry UEM instances that connect to them.
BlackBerry UEM instance	A BlackBerry UEM instance refers to one installation of the BlackBerry UEM Core and all associated BlackBerry UEM components that communicate with it. The components can be installed on the same server or multiple servers. There can be more than one BlackBerry UEM instance in a BlackBerry UEM domain.
CA	certification authority (autorité de certification)
certificat	Un certificat est un document numérique qui lie l'identité et la clé publique d'un sujet de certificat. À chaque certificat correspond une clé privée stockée séparément. Une autorité de certification signe le

	certificat pour attester de son authenticité et de sa fiabilité.
CRL	Certificate Revocation List (liste de révocation des certificats)
DEP	Programme d'inscription des appareils
DNS	Domain Name System (système DNS)
DPD	Dead Peer Detection
EAP	Extensible Authentication Protocol (protocole d'authentification extensible)
EAP-FAST	Extensible Authentication Protocol Flexible Authentication via Secure Tunneling
EAP-MS-CHAP	Extensible Authentication Protocol Microsoft® Challenge Handshake Authentication Protocol (protocole d'authentification extensible - protocole d'authentification par challenge Microsoft®)
EAP-TLS	Extensible Authentication Protocol Transport Layer Security (protocole d'authentification extensible - sécurité de la couche de transport)
EDP	Enterprise Data Protection (protection des données d'entreprise)
EMM	Enterprise Mobility Management (Gestion de la mobilité d'entreprise)
FQDN	Fully Qualified Domain Name (nom de domaine complet)
GTC	Generic Token Card
HMAC	Code d'authentification du message fragmenté
HTTP	Hypertext Transfer Protocol (protocole de transfert hypertexte)
HTTPS	Hypertext Transfer Protocol over Secure Sockets Layer
ICCID	Integrated Circuit Card Identifier (identifiant de carte de circuit intégré)
IKE	Internet Key Exchange (protocole IKE)
IMAP	Internet Message Access Protocol (protocole de messagerie IMAP)

IMEI	International Mobile Equipment Identity (identification internationale d'équipement mobile)
IP	Internet Protocol (protocole Internet)
IPsec	Internet Protocol Security (sécurité du protocole Internet)
Stratégie informatique	Une stratégie informatique est composée de diverses règles qui contrôlent les fonctions de sécurité et le comportement des terminaux.
LAN	Local Area Network (réseau local)
LDAP	Lightweight Directory Access Protocol (protocole LDAP)
MD5	Message-Digest Algorithm, version 5
MDM	Mobile device management (gestion des terminaux mobiles)
MS-CHAP	Microsoft Challenge Handshake Authentication Protocol (protocole d'authentification par challenge de Microsoft)
NAT	Network Address Translation (traduction d'adresses de réseau)
NTLM	NT LAN Manager
OCSP	Online Certificate Status Protocol
OID	identifiant d'objet
PAC	Proxy Auto-Configuration (configuration automatique de proxy)
PFS	Perfect Forward Secrecy (confidentialité totale des transferts)
PKI	Public Key Infrastructure (infrastructure de clé publique)
PMK	Pairwise Master Key (clé maîtresse du cryptage par paires)
POP	Post Office Protocol (protocole de réception des e-mails)
PRF	Famille de fonctions pseudo-aléatoires
PSK	Pre-Shared Key (clé prépartagée)

SCEP	Simple Certificate Enrollment Protocol (service d'inscription de périphériques réseau)
SHA	Secure Hash Algorithm (algorithme SHA)
SIM	Subscriber Identity Module (module d'identification de l'abonné)
S/MIME	Secure Multipurpose Internet Mail Extensions
SNMP	Simple Network Management Protocol (protocole SNMP)
Espace	Un espace est une zone distincte du terminal qui permet de compartimenter et de gérer différents types de données, d'applications et de connexions réseau. Différents espaces peuvent avoir différentes règles pour le stockage de données, les autorisations d'application et le routage réseau. Les espaces étaient auparavant appelés périmètres.
SSL	Secure Sockets Layer (protocole SSL)
Terminaux iOS supervisés	Les terminaux supervisés sont configurés pour permettre un plus grand contrôle des fonctionnalités des terminaux iOS. Pour activer la supervision des terminaux iOS appartenant à votre organisation, vous pouvez utiliser Apple Configurator ou Apple Device Enrollment Program.
TCP	Transmission Control Protocol (protocole de contrôle de transmissions)
TGT	TGT (Ticket-Granting Ticket) est un ticket de service que le client d'un service Kerberos envoie au TGS pour demander le ticket de service du service Kerberos.
TLS	Transport Layer Security (sécurité de la couche de transport)
UEM	Unified Endpoint Manager
USB	Universal Serial Bus (bus série universel)
VPN	Virtual Private Network (réseau privé virtuel)
xAuth	Authentification étendue

Informations juridiques

cette documentation n'implique pas l'endossement par BlackBerry de tiers et de Services ou de la tierce partie en quelque sorte.

SAUF DANS LA MESURE EXPRESSÉMENT INTERDITE PAR LA LOI APPLICABLE DANS VOTRE JURIDICTION, TOUTES LES CONDITIONS, ENDOSSEMENTS, GARANTIES, REPRÉSENTATIONS OU GARANTIES DE TOUTE SORTE, EXPRESSE OU IMPLICITEMENT, Y COMPRIS, SANS LIMITATION, LES CONDITIONS, AVENANTS, GARANTIES, REPRÉSENTATIONS OU GARANTIES DE DURABILITÉ, D'ADÉQUATION À UN USAGE PARTICULIER OU L'UTILISATION, VALEUR MARCHANDE, LA QUALITÉ MARCHANDE, QUALITÉ DE NON-CONTREFACON, SATISFAISANTE, OU TITRE OU DÉCOULANT D'UNE LOI OU UNE COUTUME OU UNE CONDUITE HABITUELLE OU L'USAGE DE COMMERCE, OU LIÉS À LA DOCUMENTATION OU SON UTILISATION, OU LA PERFORMANCE OU L'INEXÉCUTION DE TOUT LOGICIEL, MATÉRIEL, SERVICE, OU TOUT TIERS PRODUITS ET SERVICES MENTIONNÉS AUX PRÉSENTES, SONT ICI EXCLUES. VOUS POUVEZ AVOIR AUSSI D'AUTRES DROITS QUI VARIENT SELON L'ÉTAT OU LA PROVINCE. CERTAINES JURIDICTIONS N'AUTORISENT PAS L'EXCLUSION OU LA LIMITATION DES GARANTIES IMPLICITES ET CONDITIONS. IMPLICITES DANS LA MESURE PERMISE PAR LA LOI, LES GARANTIES OU CONDITIONS RELATIVES À LA DOCUMENTATION DANS LA MESURE OÙ ILS NE PEUVENT ÊTRE EXCLUES COMME ENSEMBLE DEHORS AU-DESSUS, MAIS PEUVENT ÊTRE LIMITÉES, SONT LIMITÉES À QUATRE-VINGT-DIX 90 JOURS À PARTIR DE LA DATE QUE VOUS AVEZ ACQUIS TOUT D'ABORD LA DOCUMENTATION OU LA ORDRE DU JOUR QUI FAIT L'OBJET DE LA RÉCLAMATION.

DANS LA MESURE MAXIMALE PERMISE PAR LA LOI APPLICABLE DANS VOTRE JURIDICTION, EN AUCUN CAS BLACKBERRY SERA RESPONSABLE POUR TOUT TYPE DE DOMMAGES LIÉS À CETTE DOCUMENTATION OU SON UTILISATION, OU LA PERFORMANCE OU L'INEXÉCUTION DE TOUT LOGICIEL, MATÉRIEL, SERVICE, OU TOUT TIERS PRODUITS ET SERVICES MENTIONNÉS AUX PRÉSENTES Y COMPRIS SANS LIMITATION LES DOMMAGES SUIVANTS : DOMMAGE DIRECT, CONSÉCUTIF, EXEMPLAIRE, FORTUIT, INDIRECT, SPÉCIAL, PUNITIF OU AGGRAVÉE, DOMMAGES-INTÉRÊTS POUR PERTE DE PROFITS OU DE REVENUS, ÉCHEC DE RÉALISER TOUT PRÉVU DES ÉCONOMIES, INTERRUPTION D'ACTIVITÉ, PERTES D'INFORMATIONS COMMERCIALES, PERTE D'OPPORTUNITÉ COMMERCIALE, DE CORRUPTION OU DE PERTE DE DONNÉES, PANNES POUR TRANSMETTRE OU RECEVOIR N'IMPORTE QUEL DA TA, PROBLÈMES LIÉS À TOUTES LES APPLICATIONS UTILISANT EN CONJONCTION AVEC BLACKBERRY PRODUITS OU SERVICES, DURÉE D'INDISPONIBILITÉ DES COÛTS, PERTE D'USAGE DU BLACKBERRY, PRODUITS, SERVICES OU TOUTE PARTIE DE CELLE-CI OU DE TOUT SERVICE DE TEMPS D'ANTENNE, COÛT DE MARCHANDISES DE REMPLACEMENT, LES COÛTS DE COUVERTURE, INSTALLATIONS OU SERVICES, COÛT DU CAPITAL OU AUTRES PERTES PÉCUNIAIRES SEMBLABLES, SI CES DOMMAGES ONT ÉTÉ PRÉVUES OU IMPRÉVUES, ET MÊME SI LE BLACKBERRY A ÉTÉ AVISÉ DE LA DEMAND Y DE TELS DOMMAGES.

DANS LA MESURE MAXIMALE PERMISE PAR LA LOI APPLICABLE DANS VOTRE JURIDICTION, BLACKBERRY N'AURA AUCUNE AUTRE OBLIGATION, OBLIGATION OU RESPONSABILITÉ QUE CE SOIT EN CONTRAT, UN TORT, OU AUTREMENT VOUS Y COMPRIS TOUTE RESPONSABILITÉ POUR NÉGLIGENCE OU STRICT RESPONSABILITÉ CIVILE.

LES LIMITATIONS ET EXCLUSIONS CI-DESSUS SERONT APPLIQUENT : (A) INDÉPENDAMMENT DE LA NATURE DE LA CAUSE D'ACTION, DEMANDE OU ACTION PAR VOUS, Y COMPRIS MAIS NON LIMITÉ À B PORTÉE DE CONTRAT, NÉGLIGENCE, RESPONSABILITÉ DÉLICTUELLE, RESPONSABILITÉ STRICTE OU TOUTE AUTRE THÉORIE JURIDIQUE ET DOIVENT SURVIVRE À UNE INEXÉCUTION FONDAMENTALE OU BRE DOULEURS OU L'ÉCHEC DE L'OBJECTIF ESSENTIEL DU PRÉSENT ACCORD OU DE TOUTE MESURE CORRECTIVE QU'IL CONTIENT ; ET (B) À BLACKBERRY ET SES SOCIÉTÉS AFFILIÉES, LEURS SUCCESSEURS, LES AYANTS DROIT, LES AGENTS, LES FOURNISSEURS (Y COMPRIS LES TEMPS D'ANTENNE SERVICE P ROVIDERS), DISTRIBUTEURS DE BLACKBERRY (Y COMPRIS LES FOURNISSEURS DE SERVICES DE TEMPS D'ANTENNE) AGRÉÉS ET LEURS DIRECTEURS RESPECTIFS, EMPL OYEES ET LES ENTREPRENEURS INDÉPENDANTS.

OUTRE LES LIMITATIONS ET EXCLUSIONS VISÉES CI-DESSUS, EN AUCUN CAS, N'IMPORTE QUEL DIRIGEANT, EMPLOYÉ, AGENT, DISTRIBUTEUR, FOURNISSEUR, ENTREPRENEUR INDÉPENDANT DE BLACKBERRY OU TOUT AFFILIÉ DE BLACKBERRY A TOUTE RESPONSABILITÉ DÉCOULANT D'OU LIÉS À LA DOCUMENTATION.

Avant de souscrire pour, installant ou utilisant des produits tiers et les Services, il est de votre responsabilité de vous assurer que votre fournisseur de service de temps d'antenne a accepté de prend en charge toutes leurs fonctionnalités. Certains fournisseurs de services de temps d'antenne ne pourraient pas offrir fonctionnalité de

navigation Internet avec un abonnement à le BlackBerry® Interne t Service. Vérifiez auprès de votre fournisseur de services pour la disponibilité, des arrangements, des plans de service et des caractéristiques de l'itinérance. Installation ou l'utilisation des Services et produits tiers avec les produits et les services de BlackBerry peut exiger un ou plusieurs brevets, marque, droit d'auteur, ou d'autres licences afin d'éviter la contrefaçon ou violation des droits de tiers. Vous êtes seul responsable de déterminer s'il faut utiliser des produits tiers, et Services, si les licences de tiers sont tenus de le faire. Si vous êtes responsable de l'acquisition. Vous ne devriez pas installer ou utiliser les Services et produits tiers jusqu'à ce que toutes les autorisations nécessaires ont été acquis. Tous les produits de tiers et les Services qui sont fournis avec les produits et les services de BlackBerry sont fournis à titre utilitaire à vous et sont fournis « Tel quel » avec aucune conditions implicites ou explicites, endossements, garanties, représentations ou garantie d'aucune genre de BlackBerry et BlackBerry n'assume aucune responsabilité quelle qu'elle soit, en relation avec celui-ci. Votre utilisation des Services et des produits de tiers est régie par et sous réserve de vous acceptant les conditions de licen séparé SSE et autres accords applicables s'y rapportant avec les tierces parties, sauf dans la mesure expressément couverte par une licence ou d'autre accord avec BlackBerry.

Les conditions d'utilisation de tout produit BlackBerry ou service figurent dans une licence distincte ou de toute autre entente avec BlackBerry applicables s'y rapportant. RIEN DANS LA PRÉSENTE DOCUMENTATION VISE À REMPLACER TOUTE ENTENTE ÉCRITE EXPRESSE OU GARANTIES FOURNIES PAR BLACKBERRY POUR UNE PARTIE DE N'IMPORTE QUEL BLACKBERRY PRODUIT OU SERVICE AUTRE QUE DE CETTE DOCUMENTATION.

BlackBerry Enterprise Software intègre certains logiciels de tierce partie. La licence et les informations de copyright associées à ce logiciel est disponible àhttp://Worldwide.BlackBerry.com/legal/thirdpartysoftware.jsp.

BlackBerry Limited 2200, Avenue University est Waterloo, Ontario Canada N2K 0 a 7 BlackBerry UK Limited 200 Bath Road Slough, Berkshire SL1 3XE United Kingdom publié au Canada