BlackBerry UEM

Présentation et architecture

12.20

Contents

Qu'est-ce que BlackBerry UEM ?

BlackBerry UEM est une solution EMM multiplateforme qui fournit une gestion étendue des terminaux, des applications et du contenu, avec une sécurité et une connectivité intégrées, et vous aide à gérer les terminaux iOS, macOS, Android et Windows pour votre organisation.

Vous pouvez installer UEM dans un environnement sur site pour un contrôle maximal de vos serveurs, de vos données et de vos terminaux, ou vous pouvez utiliser UEM Cloud, qui offre une solution facile d'emploi, économique et sécurisée. Comme BlackBerry héberge UEM Cloud sur Internet, vous n'avez besoin que d'un navigateur Web pris en charge pour accéder au service.

UEM sur site et UEM Cloud offrent une sécurité de bout en bout et le contrôle dont votre organisation a besoin pour gérer tous les points de terminaison et les modèles de propriété.

Les avantages de UEM comprennent :

Fonctionnalité	Avantage
Faible cout total de propriété	UEM sur site réduit la complexité, optimise les ressources mises en commun, garantit une disponibilité maximale et vous aide à atteindre le plus bas cout total de propriété pour une solution sur site. UEM Cloud réduit le cout de propriété en supprimant la nécessité d'installer, de gérer et de mettre à jour les services.
Interface Web unique	Vous pouvez gérer les terminaux iOS, macOS, Android et Windows, outre des services supplémentaires, à partir d'une même console de gestion.
Modèles de propriété flexibles	Utilisez un ensemble de stratégies et de profils personnalisables pour gérer les terminaux BYOD, COPE et COBO et protéger vos informations commerciales.
Rapports sur les utilisateurs et les terminaux	Gérez vos parcs de terminaux à l'aide de rapports, de tableaux de bords, de filtres dynamiques et de fonctions de recherche complets.
Configuration et inscription simples de l'utilisateur	Permet aux utilisateurs d'activer leurs propres terminaux sur UEM avec BlackBerry UEM Self-Service.
Sécurité mobile de pointe	S'appuie sur BlackBerry Infrastructure pour garantir la sécurité des données sur tous les terminaux.
Haute disponibilité	Configurez la haute disponibilité sur site afin de minimiser les interruptions de service pour les utilisateurs de terminaux ou appuyez-vous sur BlackBerry pour maintenir UEM Cloud et optimiser le temps de disponibilité pour vous.
Services supplémentaires disponibles	Vous pouvez activer des services tels que BlackBerry Workspaces, BlackBerry Enterprise Identity, BlackBerry 2FA, BBM Enterprise et UEM Notifications pour ajouter de la valeur à votre déploiement UEM.

Principales fonctionnalités de BlackBerry UEM

Fonctionnalité	Description
Gestion de terminaux multiplateforme	Vous pouvez gérer des terminaux iOS, macOS, Android et Windows.
Une seule interface utilisateur intuitive	Vous pouvez afficher tous les terminaux au même emplacement et accéder à toutes les tâches de gestion à partir d'une seule et unique interface utilisateur Web. Vous pouvez partager des tâches avec différents administrateurs qui peuvent accéder simultanément aux consoles de gestion. Vous pouvez alterner entre la vue par défaut et les vues avancées pour afficher les options d'affichage des informations et du filtrage de la liste d'utilisateurs.
Expérience approuvée et sécurisée	Les commandes des terminaux vous permettent de gérer avec précision la façon dont les terminaux se connectent à votre réseau, ainsi que de choisir les fonctionnalités à activer et les applications disponibles. Que les terminaux appartiennent à votre organisation ou à vos utilisateurs, vous pouvez protéger les données de votre organisation.
Séparer les besoins professionnels et personnels	Vous pouvez gérer des terminaux à l'aide des technologies Samsung Knox, Android Enterprise et Android Management conçues pour séparer et sécuriser les informations personnelles et professionnelles stockées sur des terminaux. Si un terminal est perdu ou compromis, vous pouvez supprimer l'intégralité des informations qui y sont stockées ou uniquement les informations professionnelles.
Sécuriser la connectivité IP	Vous pouvez utiliser BlackBerry Secure Connect Plus pour établir un tunnel IP sécurisé entre les applications de l'espace Travail sur les terminaux iOS et Android qui utilisent un profil professionnel et le réseau de votre organisation. Ce tunnel permet aux utilisateurs d'accéder à des ressources professionnelles derrière le pare-feu de l'entreprise tout en assurant la sécurité des données à l'aide des protocoles IPv4 standard (TCP et UDP) et du chiffrement de bout en bout.
Libre-service utilisateur simple	BlackBerry UEM Self-Service réduit les demandes d'assistance et les couts informatiques de votre entreprise, tout en offrant aux utilisateurs la possibilité de gérer leurs terminaux opportunément. Avec UEM Self-Service, les utilisateurs peuvent activer un terminal ou changer de terminal, changer le mot de passe de leur terminal à distance, supprimer des données de leur terminal ou verrouiller un terminal perdu ou volé.
Intégration à d'autres services BlackBerry	Vous pouvez intégrer UEM à BlackBerry Workspaces, BlackBerry Enterprise Identity et BlackBerry 2FA afin d'ajouter de la valeur à l'instance UEM de votre organisation.
Gestion performante des applications	UEM est une plateforme de gestion complète compatible avec tous les terminaux. Vous pouvez déployer des applications à partir des principales boutiques d'applications, notamment App Store et Google Play.

Fonctionnalité	Description
Administration basée sur des rôles	Vous pouvez partager des tâches avec différents administrateurs qui peuvent accéder simultanément aux consoles de gestion. Vous pouvez utiliser des rôles pour définir les actions qu'un administrateur peut effectuer, ce qui vous permet de réduire les risques de sécurité, de répartir les responsabilités liées aux tâches et d'accroitre l'efficacité. Vous pouvez utiliser des rôles prédéfinis ou créer vos propres rôles personnalisés.
Intégration de l'annuaire d'entreprise	Vous pouvez utiliser l'authentification utilisateur locale intégrée pour accéder à la console de gestion et à la console en libre-service, ou vous pouvez intégrer UEM aux répertoires Microsoft Active Directory, LDAP ou Entra ID que vous utilisez dans l'environnement de votre organisation. UEM prend en charge les connexions à différents répertoires. Vous pouvez créer des comptes d'utilisateur dans UEM à l'aide des données d'utilisateur du répertoire et lier des groupes de répertoires d'entreprise à UEM pour organiser les utilisateurs dans UEM comme ils le sont dans votre répertoire d'entreprise. Vous pouvez également activer l'intégration pour des groupes spécifiques de votre répertoire d'entreprise afin de créer automatiquement des utilisateurs de UEM. Si vous activez l'intégration, vous pouvez également configurer la suppression afin de supprimer des données ou comptes d'utilisateur lorsque des utilisateurs sont supprimés des groupes de votre répertoire d'entreprise.
Migration	Vous pouvez migrer des utilisateurs, des terminaux, des groupes et d'autres données depuis une base de données UEM source sur site vers une nouvelle instance de UEM Cloud sur site.
Intégration de Cisco ISE	Cisco Identity Services Engine (ISE) est un logiciel de gestion de réseau qui permet à une entreprise de contrôler l'accès au réseau professionnel des terminaux (par exemple, autorisant ou refusant les connexions Wi-Fi ou VPN). Vous pouvez créer une connexion entre Cisco ISE et UEM sur site de sorte que Cisco ISE puisse récupérer les données sur les terminaux qui sont activés sur UEM. Cisco ISE contrôle les données des terminaux pour déterminer si les terminaux sont conformes aux politiques d'accès de votre entreprise.

Fonctionnalité	Description
Déploiement régional	Vous pouvez configurer des connexions régionales pour les fonctionnalités de connectivité d'entreprise en déployant une ou plusieurs instances de BlackBerry Connectivity Node dans une région dédiée. Ce processus est connu sous le nom de groupe de serveurs. Chaque instance de BlackBerry Connectivity Node comprend BlackBerry Secure Connect Plus, BlackBerry Gatekeeping Service, BlackBerry Secure Gateway, BlackBerry Proxy et BlackBerry Cloud Connector. Vous pouvez associer les profils de connectivité d'entreprise et de messagerie à un groupe de serveurs pour permettre aux utilisateurs qui se voient attribuer ces profils d'utiliser une connexion régionale spécifique à BlackBerry Infrastructure lorsqu'ils utilisent des composants BlackBerry Connectivity Node. Le déploiement de plusieurs instances de BlackBerry Connectivity Node dans un groupe de serveurs permet aussi une haute disponibilité et un équilibrage de la charge.
Appareils portables	Vous pouvez activer et gérer certains terminaux portables Android dans UEM. Par exemple, vous pouvez gérer Vuzix M300 Smart Glasses. Les lunettes intelligentes offrent aux utilisateurs un accès mains libres aux informations visuelles telles que les notifications, les instructions pas-à-pas, les images et les vidéos, et permettent aux utilisateurs d'émettre des commandes vocales, de scanner des codes à barres et d'utiliser la navigation GPS. Voici des exemples de fonctions de gestion prises en charge par UEM : activation d'un terminal à l'aide d'un code QR, stratégies informatiques, profils Wi-Fi et VPN, gestion des applications et services de localisation.
Intégration de Microsoft Intune	Pour les terminaux iOS et Android, si vous souhaitez protéger les données des applications Microsoft 365 à l'aide des fonctionnalités MAM de Microsoft Intune, vous pouvez utiliser Intune pour protéger les données des applications tout en utilisant UEM pour gérer les terminaux. Intune offre des fonctions de sécurité qui protègent les données au sein des applications. Par exemple, Intune peut exiger que les données contenues dans les applications soient cryptées et empêcher le copier-coller, l'impression et l'utilisation de la commande Enregistrer sous. En connectant UEM à Intune, vous pouvez gérer les stratégies de protection de l'application Intune à partir de la console de gestion UEM.

Principales fonctionnalités pour tous les types de terminaux

Fonctionnalité	Description
Activer des terminaux	Lorsqu'un utilisateur active un terminal, il l'associe à UEM et à l'environnement de votre organisation afin d'avoir accès aux données professionnelles sur ce terminal. Les utilisateurs peuvent activer leurs terminaux à l'aide d'un code QR ou de leur adresse e-mail et d'un mot de passe d'activation. Vous pouvez autoriser les utilisateurs à activer les terminaux eux-mêmes ou activer les terminaux pour eux avant de les distribuer. Tous les types de terminaux peuvent être activés à l'aide du réseau sans fil.
Gérer les terminaux	Vous pouvez afficher tous les terminaux et accéder à toutes les tâches de gestion à partir d'une seule et même console Web. Vous pouvez gérer plusieurs terminaux pour chaque compte d'utilisateur et afficher l'inventaire des terminaux de votre organisation. Vous pouvez exécuter les actions suivantes si elles sont prises en charge par le terminal : • Verrouillez le terminal, modifiez le mot de passe du terminal ou de l'espace Travail ou supprimez des informations du terminal. • Connectez le terminal à l'environnement de messagerie de votre organisation de manière sécurisée, en utilisant Microsoft Exchange ActiveSync pour la prise en charge de la messagerie et du calendrier. • Déterminez de quelle façon le terminal peut se connecter au réseau de votre organisation, paramètres Wi-Fi et VPN compris. • Configurez une authentification unique pour le terminal afin qu'il s'authentifie automatiquement auprès des domaines et des services Web du réseau de votre organisation. • Déterminez les fonctionnalités du terminal (par exemple, configurer les règles de niveau de sécurité du mot de passe ou désactiver des fonctions telles que l'appareil photo). • Gérez la disponibilité des applications sur le terminal, en spécifiant notamment les versions des applications et le caractère obligatoire ou facultatif de ces dernières. • Recherchez les applications à attribuer aux terminaux dans les boutiques d'applications. • Installez des certificats sur le terminal et, éventuellement, configurez le protocole SCEP pour permettre l'inscription automatique des certificats. • Renforcez la sécurité de la messagerie via S/MIME ou PGP.
Gérer des groupes d'utilisateurs, d'applications et de terminaux	Les groupes simplifient la gestion des utilisateurs, des applications et des terminaux. Vous pouvez utiliser des groupes pour appliquer les mêmes paramètres de configuration à des comptes d'utilisateur ou à des terminaux similaires. Vous pouvez attribuer différents groupes d'applications à différents groupes d'utilisateurs, et un utilisateur peut être membre de plusieurs groupes.
Désigner les terminaux autorisés à accéder à Microsoft Exchange ActiveSync	Vous pouvez utiliser le contrôle d'accès pour vous assurer que seuls les terminaux gérés par UEM ont accès à la messagerie professionnelle et aux autres informations du terminal. Ce contrôle permet également de faire respecter la stratégie de sécurité de votre organisation.

Fonctionnalité	Description
Déterminer la manière dont les applications se connectent aux ressources de votre organisation	Vous pouvez utiliser un profil de connectivité d'entreprise pour déterminer la manière dont les applications des terminaux se connectent aux ressources de votre organisation. Lorsque vous activez la connectivité d'entreprise, vous n'êtes pas tenu d'ouvrir plusieurs ports d'accès à Internet dans le pare-feu de votre organisation pour gérer les terminaux et les applications tierces telles que le serveur de messagerie, l'autorité de certification ainsi que d'autres serveurs Web ou serveurs de contenu. La connectivité d'entreprise dirige tout le trafic qui passe par BlackBerry Infrastructure vers UEM par le biais du port 3101.
Gérer les applications professionnelles	Sur tous les terminaux gérés, les applications professionnelles sont des applications que votre organisation met à la disposition de ses utilisateurs. Vous pouvez rechercher les applications à attribuer aux terminaux dans les boutiques d'applications. Vous pouvez désigner des applications obligatoires et vérifier si une application professionnelle est installée sur un terminal. Les applications professionnelles peuvent également être des applications propriétaires développées par votre organisation ou par des développeurs tiers pour le compte de votre organisation.
Appliquer les exigences de votre organisation en matière de terminaux	Vous pouvez utiliser un profil de conformité pour répondre plus facilement aux exigences de sécurité de votre organisation. Vous pouvez par exemple empêcher que les terminaux crackés, flashés ou présentant une alerte d'intégrité n'accèdent aux données professionnelles ou exiger que certaines applications soient installées sur les terminaux. Vous pouvez envoyer une notification aux utilisateurs leur demandant de se conformer aux exigences de votre organisation ou vous pouvez limiter l'accès des utilisateurs aux ressources et applications de votre organisation, supprimer les données professionnelles ou supprimer toutes les données du terminal.
Envoyer un e-mail aux utilisateurs	Vous pouvez envoyer un e-mail à plusieurs utilisateurs directement depuis la console de gestion.
Créer ou importer un grand nombre de comptes d'utilisateur à l'aide d'un fichier .csv	Vous pouvez importer un fichier .csv dans UEM pour créer ou importer simultanément un grand nombre de comptes d'utilisateur. En fonction de vos besoins, vous pouvez également spécifier dans le fichier .csv des paramètres d'appartenance à un groupe et d'activation pour les comptes d'utilisateur.
Afficher des rapports sur les informations relatives aux utilisateurs et aux terminaux	Le tableau de bord des rapports présente un aperçu de votre environnement UEM. Par exemple, vous pouvez afficher le nombre de terminaux de votre organisation en les classant par fournisseur de services. Vous pouvez afficher des informations détaillées sur les utilisateurs et sur les terminaux, exporter ces informations dans un fichier .csv et accéder aux comptes d'utilisateur depuis le tableau de bord.

Fonctionnalité	Description
Haute disponibilité et récupération après incident	Répartis dans le monde entier, les centres de données BlackBerry sont conçus pour fournir une haute disponibilité et assurer la récupération après incident. Les centres de données BlackBerry fournissent un accès physique sécurisé aux bâtiments, une surveillance et des redondances matérielles afin de protéger les données de votre organisation des catastrophes naturelles. Les centres de données BlackBerry disposent de plans de récupération après incident afin de faire face aux interruptions de service. Ces plans sont conçus pour avoir un impact minimal sur les utilisateurs des terminaux et assurer la continuité du service. Les données et applications sont sauvegardées quasiment en temps réel pour éviter la perte de données.
Authentification basée sur certificat	Vous pouvez envoyer des certificats aux terminaux à l'aide de profils de certificat. Ces profils permettent de limiter l'accès à Microsoft Exchange ActiveSync, ainsi qu'aux connexions Wi-Fi et VPN aux terminaux qui utilisent l'authentification basée sur certificat.
Gérer les licences pour des fonctionnalités et commandes de terminal spécifiques	Vous pouvez gérer les licences et afficher des informations détaillées sur chaque type de licence, comme l'utilisation et l'expiration. Les types de licences utilisées par votre organisation déterminent les terminaux et fonctionnalités que vous pouvez gérer. Avant de pouvoir activer les terminaux, vous devez activer les licences. Des licences d'essai gratuites sont disponibles pour vous permettre d'essayer le service.

Principales fonctionnalités de chaque type de terminal

Terminaux iOS

Fonctionnalité	Description
Activation des terminaux	Vous pouvez utiliser Apple Configurator 2 pour préparer les terminaux à l'activation avec UEM. Les utilisateurs peuvent activer les terminaux préparés sans utiliser BlackBerry UEM Client.
Filtrer le contenu Web	Vous pouvez utiliser les profils de filtre de contenu Web pour limiter les sites Web qu'un utilisateur peut afficher sur un terminal. Vous pouvez activer le filtrage automatique en autorisant ou en limitant l'accès au Web, ou n'autoriser l'accès qu'à certains sites Web.
Associer des comptes Apple VPP à un domaine UEM	Le Programme d'achat en volume (Volume Purchase Program - VPP) vous permet d'acheter et de distribuer des applications iOS en bloc. Vous pouvez associer des comptes Apple VPP à un domaine UEM afin de pouvoir distribuer les licences achetées pour les applications iOS associées aux comptes VPP.

Fonctionnalité	Description
Apple Programme d'inscription des appareils	Vous pouvez configurer UEM pour qu'il utilise le programme d'inscription des appareils Apple (DEP) afin de vous permettre de synchroniser UEM avec le programme d'inscription des appareils. Après avoir configuré UEM, vous pouvez utiliser la console de gestion afin de gérer l'activation des terminaux iOS que votre organisation a achetés pour le DEP. Vous pouvez utiliser plusieurs comptes DEP. Vous pouvez lier plusieurs comptes DEP Apple dans un domaine UEM.
Prise en charge des solutions PKI d'application	UEM prend en charge les solutions PKI basées sur les applications, telles que Purebred, capables d'inscrire des certificats pour les applications BlackBerry Dynamics. Vous pouvez maintenant installer l'application PKI sur les terminaux et autoriser les dernières versions des applications BlackBerry Dynamics, telles que BlackBerry Work et BlackBerry Access, à utiliser des certificats inscrits par l'intermédiaire de l'application PKI.
Profils de la charge utile personnalisée	Vous pouvez utiliser des profils de charge utile personnalisée pour contrôler les fonctions sur les terminaux iOS qui ne sont pas contrôlés par les règles ou profils UEM existants. Vous pouvez créer des profils de configuration Apple à l'aide d'Apple Configurator et les ajouter aux profils de charge utile UEM personnalisée. Vous pouvez affecter les profils de charge utile personnalisée aux utilisateurs, aux groupes d'utilisateurs et aux groupes de terminaux.
BlackBerry Secure Gateway	BlackBerry Secure Gateway autorise les terminaux iOS avec le type d'activation Contrôles MDM à se connecter à votre serveur de messagerie professionnelle via BlackBerry Infrastructure et UEM. Si vous utilisez BlackBerry Secure Gateway, vous n'avez pas à exposer votre serveur de messagerie à l'extérieur du pare-feu pour autoriser les utilisateurs de ces terminaux à recevoir des e-mails professionnels lorsqu'ils ne sont pas connectés au réseau VPN ou au réseau Wi-Fi professionnel de votre organisation.
Intégration avec BlackBerry Dynamics	Vous pouvez utiliser le profil BlackBerry Dynamics pour permettre à des terminaux iOS et BlackBerry Dynamics d'accéder à des applications de productivité BlackBerry Work telles que BlackBerry Access et BlackBerry Connect. Vous pouvez attribuer le profil BlackBerry Dynamics à des comptes d'utilisateur, groupes d'utilisateurs ou groupes de terminaux. Plusieurs terminaux peuvent accéder aux mêmes applications. Le profil vous permet d'activer BlackBerry Dynamics pour les utilisateurs qui ne sont pas encore activés pour BlackBerry Dynamics.
VPN par application	Pour les terminaux iOS, 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 affectez l'application ou le groupe d'applications à un utilisateur, à un groupe d'utilisateurs ou à un groupe de terminaux.

Fonctionnalité	Description
Verrouillage de l'activation Apple	La fonctionnalité de verrouillage de l'activation nécessite l'identifiant et le mot de passe Apple de l'utilisateur pour que celui-ci puisse désactiver l'option Localiser mon iPhone, effacer le terminal ou réactiver et utiliser le terminal. Vous pouvez contourner le verrouillage de l'activation pour céder un terminal COPE ou COBO à un autre utilisateur.
Listes des applications personnelles	Vous pouvez afficher la liste des applications installées dans l'espace Personnel de l'utilisateur sur les terminaux iOS de votre environnement. Vous pouvez afficher la liste des applications personnelles installées sur le terminal d'un utilisateur sur la page des détails utilisateur ou afficher la liste de toutes les applications personnelles installées dans l'espace personnel des utilisateurs sur la page des applications personnelles de la console de gestion.
Exécuter le mode de verrouillage des applications	Sur les terminaux iOS supervisés à l'aide de Apple Configurator 2, vous pouvez utiliser un profil du mode de verrouillage des applications afin de contraindre le terminal à n'exécuter qu'une seule application. Par exemple, vous pouvez limiter l'accès à une seule application pour les formations ou les démonstrations en points de vente.
Mode Perdu sur les terminaux iOS supervisés	Le mode Perdu vous permet de verrouiller un terminal, de définir un message que vous voulez afficher et d'afficher l'emplacement actuel du terminal perdu. Vous pouvez activer le mode Perdu sur les terminaux iOS supervisés.
Prise en charge IBM Notes Traveler	Les terminaux iOS peuvent se connecter à IBM Notes Traveler via BlackBerry Secure Gateway.
Prise en charge Face ID	UEM prend en charge Face ID pour l'authentification de terminaux et l'ouverture d'applications BlackBerry Dynamics.
Gestion de terminaux partagés	Vous pouvez autoriser plusieurs utilisateurs à partager un terminal iOS. 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 et, une fois terminé, il peut l'archiver pour le rendre disponible pour l'utilisateur suivant. Les terminaux partagés restent gérés par 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
iPad	Les terminaux iPad peuvent être partagés entre plusieurs utilisateurs. Lorsque les utilisateurs se connectent avec un identifiant Apple géré, leurs données sont chargées et ils peuvent accéder à leurs propres comptes de messagerie, aux fichiers, à la bibliothèque de photos iCloud, aux données d'application, etc.

Terminaux Android

Fonctionnalité	Description
Gérer les terminaux Android Enterprise et Android Management	Vous pouvez activer les terminaux Android afin d'utiliser Android Enterprise ou Android Management, qui est une fonctionnalité développée par Google et offrant une sécurité supplémentaire aux organisations souhaitant gérer et autoriser des applications et des données sur les terminaux Android. Les terminaux peuvent être activés pour n'avoir qu'un profil professionnel ou pour avoir à la fois des profils professionnel et personnel. Vous pouvez avoir un contrôle total sur les deux profils et avoir la possibilité d'effacer l'intégralité du terminal, ou autoriser la confidentialité de l'utilisateur pour le profil personnel et avoir la possibilité de supprimer seulement les données professionnelles du terminal. Les terminaux Samsung offrent des options d'administrateur supplémentaires, notamment un ensemble amélioré de règles de stratégie informatique, lorsqu'ils sont activés avec Android Enterprise.
Activations Travail et Personnel – Contrôle total pour les terminaux Android Enterprise et Android Management	Ce type d'activation vous permet de gérer intégralement le terminal. Il crée un profil professionnel sur l'appareil qui sépare les données professionnelles et personnelles, mais permet à votre entreprise de maintenir un contrôle total sur l'appareil et d'effacer toutes les données de l'appareil. Toutes les données des profils professionnels et personnels sont protégées à l'aide du chiffrement et d'une méthode d'authentification de type mot de passe.
Gérer les terminaux avec Knox MDM et Knox Workspace	UEM peut également gérer les terminaux Samsung avec Samsung Knox MDM et Samsung Knox Workspace. Knox Workspace fournit un conteneur protégé par mot de passe et crypté situé sur un terminal Samsung incluant vos applications et données professionnelles. Il sépare les applications et les données personnelles d'un utilisateur des applications et des données de votre organisation et protège les applications et les données professionnelles à l'aide des fonctionnalités de gestion et de sécurité améliorées développées par Samsung. Lorsqu'un terminal est activé, UEM détermine automatiquement s'il prend en charge Knox. Outre les fonctionnalités de gestion standard de Android, UEM propose les fonctionnalités suivantes pour les terminaux qui prennent en charge Knox : • Ensemble développé de règles de stratégie informatique • Gestion avancée des applications, avec installation et désinstallation silencieuses des applications, désinstallation silencieuse des applications limitées et interdiction d'installer les applications limitées • Mode de verrouillage des applications Pour en savoir plus sur les terminaux pris en charge, consultez la matrice de compatibilité.

Fonctionnalité	Description
Intégration avec BlackBerry Dynamics	Vous pouvez utiliser le profil BlackBerry Dynamics pour permettre à des terminaux Android et BlackBerry Dynamics d'accéder à des applications de productivité BlackBerry Work telles que BlackBerry Access et BlackBerry Connect. Vous pouvez attribuer le profil BlackBerry Dynamics à des comptes d'utilisateur, groupes d'utilisateurs ou groupes de terminaux. Plusieurs terminaux peuvent accéder aux mêmes applications. Le profil vous permet d'activer BlackBerry Dynamics pour les utilisateurs qui ne sont pas encore activés pour BlackBerry Dynamics.
VPN par application	Vous pouvez activer un VPN par application pour les terminaux Android qui utilisent un profil professionnel afin de restreindre l'utilisation de BlackBerry Secure Connect Plus aux applications spécifiques de l'espace Travail que vous ajoutez à une liste des applications autorisées.
Inscription sans intervention	UEM prend en charge les terminaux ayant été activés pour une inscription sans intervention. L'inscription sans intervention offre une méthode de déploiement fluide pour les terminaux d'entreprise Android, rendant le déploiement à grande échelle rapide, facile et sûr. L'inscription sans intervention simplifie la configuration des terminaux en ligne par les administrateurs informatiques et la mise à disposition de la gestion appliquée lorsque les employés reçoivent leurs terminaux. Pour plus d'informations de Google, reportez-vous à la section Inscription sans intervention et à la présentation de l'inscription sans intervention. Vous pouvez démarrer avec l'inscription sans intervention en seulement quelques étapes : achetez des terminaux, attribuez-les aux utilisateurs, configurez les stratégies pour votre entreprise et déployez les terminaux aux utilisateurs. Vous devez collaborer avec votre revendeur ou votre opérateur pour obtenir l'accès au portail sans intervention et obtenir des terminaux configurés dans le portail.
Prise en charge des solutions PKI d'application	UEM prend en charge les solutions PKI basées sur les applications, telles que Purebred, capables d'inscrire des certificats pour les applications BlackBerry Dynamics. Vous pouvez maintenant installer l'application PKI sur les terminaux et autoriser les dernières versions des applications BlackBerry Dynamics, telles que BlackBerry Work et BlackBerry Access, à utiliser des certificats inscrits par l'intermédiaire de l'application PKI.
SafetyNet et Play Integrity	Lorsque les administrateurs utilisent l'attestation Android SafetyNet ou Google Play Integrity, UEM envoie des défis pour tester l'authenticité et l'intégrité des terminaux Android qui ont été activés avec le type d'activation Android Enterprise, Samsung Knox et Contrôles MDM dans l'environnement de votre organisation.
Application de correctifs de sécurité pour les applications BlackBerry Dynamics	Vous pouvez appliquer des correctifs de sécurité aux applications BlackBerry Dynamics. Si le niveau de correctif de sécurité n'est pas atteint, vous pouvez choisir de supprimer les données de l'application BlackBerry Dynamics, de ne pas autoriser les applications BlackBerry Dynamics à s'exécuter sur le terminal ou de n'effectuer aucune action sur le terminal.
Informations d'identification dérivées intelligentes	Utilisez les informations d'identification dérivées intelligentes Entrust IdentityGuard pour la signature, le cryptage et l'authentification pour les applications BlackBerry Dynamics et les applications de l'espace Travail des terminaux Android Enterprise et Samsung Knox Workspace.

Fonctionnalité	Description
Protection contre la réinitialisation définie en usine pour les terminaux Android Enterprise	Vous pouvez configurer un profil de protection contre la réinitialisation définie en usine pour les terminaux Android Enterprise de votre organisation qui ont été activés en utilisant le type d'activation Espace Travail uniquement. Ce profil vous permet de spécifier un compte d'utilisateur qui peut être utilisé pour déverrouiller un terminal après sa réinitialisation aux paramètres d'usine ou de supprimer la nécessité de vous connecter après la réinitialisation du terminal aux paramètres d'usine.

Terminaux Windows

Fonctionnalité	Description
Prise en charge des terminaux Windows 10	Vous pouvez gérer des terminaux Windows, y compris les terminaux Windows 10 Mobile et les tablettes et ordinateurs Windows 10.
Prise en charge d'un proxy par les terminaux Windows 10	Vous pouvez configurer un VPN et des connexions Wi-Fi professionnelles pour des terminaux Windows 10 et configurer un serveur proxy dans le cadre du profil Wi-Fi destiné aux terminaux Windows 10 Mobile.
VPN par application	Pour les terminaux 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.
Protection des informations Windows pour les terminaux Windows 10	Vous pouvez configurer des profils de protection des données Windows pour séparer les données personnelles des données professionnelles sur les terminaux, empêcher les utilisateurs de partager des données professionnelles en dehors des applications professionnelles protégées ou avec des personnes extérieures à votre organisation et auditer les pratiques de partage de données inappropriées. Vous pouvez spécifier quelles applications sont protégées et lesquelles sont approuvées pour créer et accéder aux fichiers professionnels.
Autoriser les fournisseurs d'antivirus	Dans le profil de conformité, dans la règle État de l'antivirus pour les terminaux Windows, vous pouvez choisir d'autoriser le logiciel antivirus de n'importe quel fournisseur, ou autoriser uniquement ceux que vous avez ajoutés à la liste des fournisseurs d'antivirus autorisés. La règle est appliquée si un appareil possède un logiciel antivirus activé à partir d'un fournisseur non autorisé.
Jonction à Entra ID	UEM prend en charge la jonction à Entra ID, qui permet un processus d'inscription MDM simplifié pour les terminaux Windows 10. Les utilisateurs peuvent inscrire leurs terminaux avec UEM à l'aide de leurs nom d'utilisateur et mot de passe Entra ID . La jonction à Entra ID est également nécessaire pour prendre en charge Windows AutoPilot, qui permet aux terminaux Windows 10 d'être activés automatiquement avec UEM lors de la première expérience de configuration de Windows 10.

Terminaux macOS

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

Fonctionnalités prises en charge par type de terminal

Cette référence rapide compare les fonctions prises en charge par les terminaux iOS, macOS, Android et Windows 10 dans 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	iOS	macOS	Android	Windows 10
Activation sans fil	√	√	√	√
Activation sans fil à l'aide d'un code QR	√		√	
Application client requise pour l'activation	√ [1]		√	
Personnalisation du contrat des conditions d'utilisation pour l'activation	√	√	√	√
Limitation des activations par modèle de terminal	√	√	√	
Afficher et exporter le rapport de terminal (par exemple, les détails du matériel)	√	√	√	√

Fonctionnalité	iOS	macOS	Android	Windows 10
Limiter les terminaux non supervisés	√[2]	√[2]		

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

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

Fonctionnalités de sécurité

Fonctionnalité	iOS	macOS	Android	Windows 10
Séparation des données professionnelles et personnelles	√ [1]		√ [2]	√
Confidentialité de l'utilisateur pour les données personnelles	√ [1]		√ [2]	
Cryptage des données professionnelles inactives	√ [1]		√ [2]	√
Envoyer des commandes informatiques aux terminaux	√	√	√	√
Contrôler les 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	√	√	√	√
Application du cryptage de la carte multimédia			√ [3]	
Application du cryptage de stockage interne			√	√

[1] Requiert des applications BlackBerry Dynamics.

[2] Requiert l'application Samsung Knox Workspace, Android Enterprise, Android Management ou BlackBerry Dynamics.

[3]Pour les terminaux Samsung Knox uniquement.

Envoi de certificats aux terminaux

Fonctionnalité	iOS	macOS	Android	Windows 10
Profils de certificat d'autorité de certification	√	√	√	√
Profils SCEP	√	√	√	√
Profils des certificats partagés	√	√	√	
Profils d'informations d'identification de l'utilisateur	√	√	√	

Gestion des connexions professionnelles pour les terminaux

Fonctionnalité	iOS	macOS	Android	Windows 10
Profils BlackBerry 2FA	√		√	
Profils de connectivité BlackBerry Dynamics	√	√	√	√
Profils CalDAV	√	√		
Profils CardDAV	√	√		
Connectivité d'entreprise				
BlackBerry Secure Connect Plus	√		√ [1]	
Profils de messagerie Exchange ActiveSync	√	√	√ [2]	√
BlackBerry Secure Gateway	√			
Profils de messagerie IMAP/POP3	√	√	√	√
Profils proxy	√	√	√	√
Profils d'identification unique	√			
Profils VPN	√	√	√ [3]	√
Profils Wi-Fi	√	√	√	√

[1] Uniquement pour les terminaux Android Enterprise et Knox Workspace.

[2] Uniquement pour les terminaux Motorola prenant en charge les API EDM, les terminaux Android Enterprise et les terminaux Knox.

[3]Pour les terminaux Knox Workspace uniquement.

Gestion des normes de votre entreprise en matière de terminaux

Fonctionnalité	iOS	macOS	Android	Windows 10
Profils d'activation	√	√	√	√
Profils du mode de verrouillage des applications	√ [1]		√ [1]	√ [1]
Profils BlackBerry Dynamics	√	√	√	√
Profils de conformité	√		√	
Profils des terminaux	√		√	
Profils Enterprise Management Agent	√		√	√
Profils de service de localisation	√		√	√

[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.

Protection des terminaux perdus ou volés

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

[1] Uniquement pour les terminaux Android Enterprise.

[2] Pour les terminaux Motorola qui prennent en charge l'API EDM, les informations présentes 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	iOS	macOS	Android	Windows 10
Désactiver la synchronisation automatique en itinérance	√		√ [1]	
Désactiver les données en itinérance	√[2]		√ [3]	√

[1] Pour les terminaux Knox uniquement.

[2] Vous pouvez configurer les paramètres d'itinérance des données dans un profil d'utilisation du réseau.

[3] Pour les terminaux Android Enterprise et Knox uniquement.

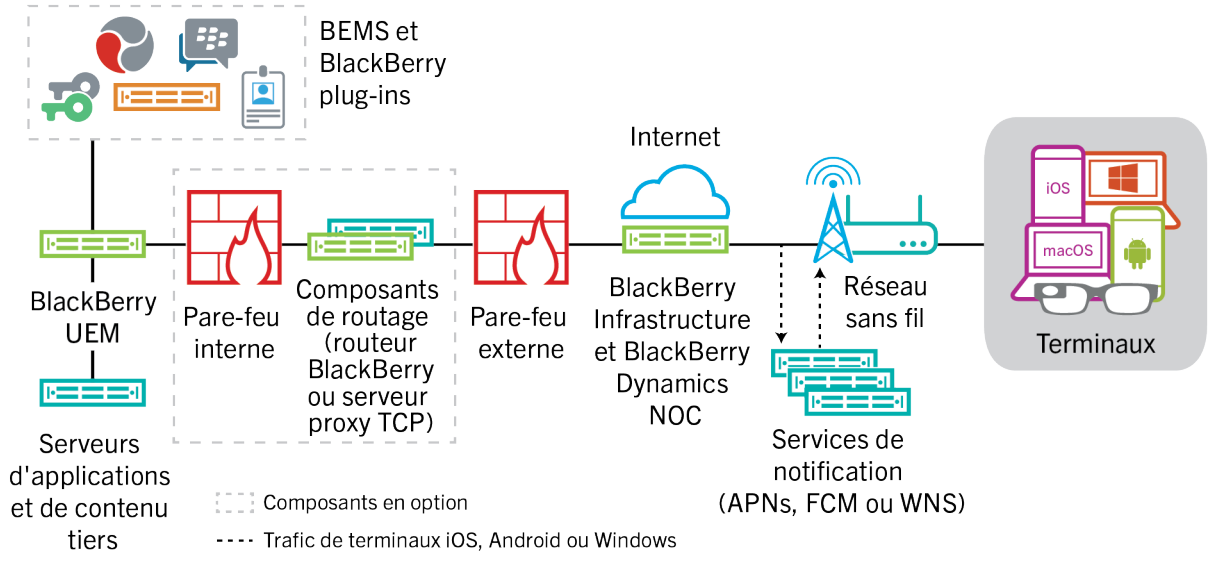
Gestion des applications

Fonctionnalité	iOS	macOS	Android	Windows 10
Distribuer les applications publiques à partir de la boutique (App Store, Google Play, Windows Store, BlackBerry World)	√		√	√
Gérer le catalogue d'applications professionnelles	√		√	√
Catalogue d'applications professionnelles de la marque	√			
Limiter les applications	√		√	
Distribuer les applications internes	√		√	√
Ajouter des raccourcis d'application aux terminaux	√	√	√	

Architecture BlackBerry UEM

L'architecture BlackBerry UEM est conçue pour vous aider à gérer les terminaux mobiles de votre organisation et fournir une liaison sécurisée pour l'acheminement des données entre les serveurs de messagerie et de contenu de votre organisation et les terminaux des utilisateurs.

Architecture : solution BlackBerry UEM

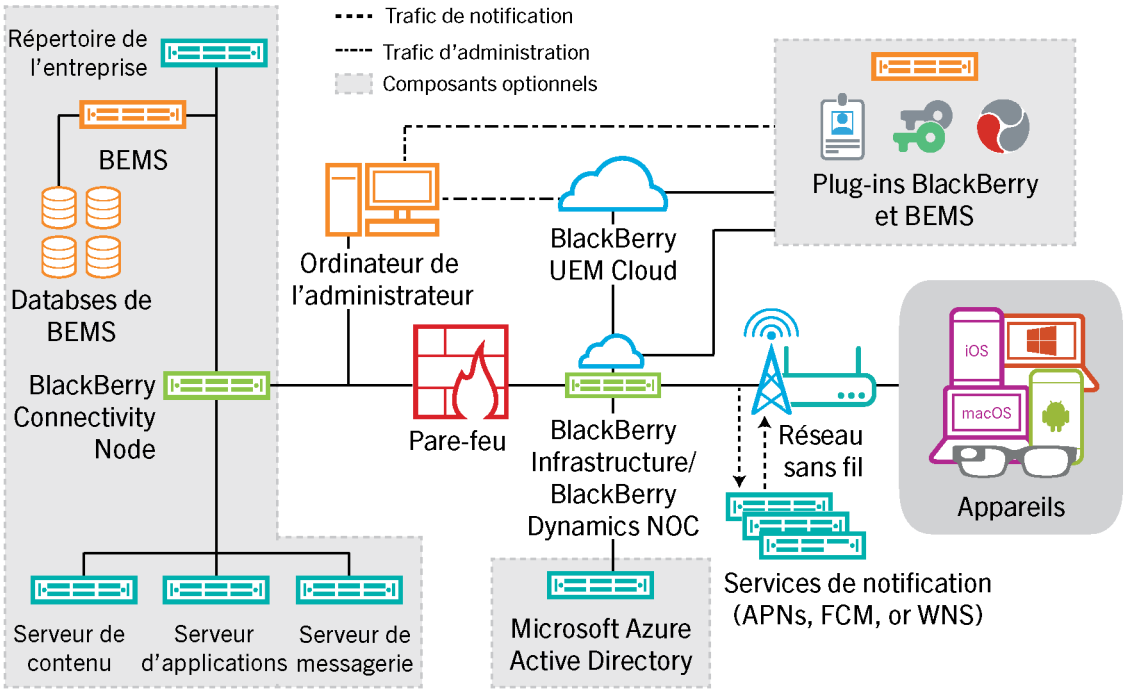


Composant	Description
BlackBerry UEM	BlackBerry UEM est une solution unifiée de gestion des points de terminaison qui fournit une gestion multiplateforme complète des terminaux, des applications et du contenu, en offrant une sécurité et une connectivité intégrées.
BlackBerry Infrastructure	BlackBerry Infrastructure est un réseau de données privées global réparti sur plusieurs régions, qui permet d'utiliser et de sécuriser des données en transit entre des milliers d'organisations et des millions d'utilisateurs à travers le monde. Il est conçu pour gérer efficacement le transport de données entre les services BlackBerry et les terminaux des utilisateurs finaux. Pour les organisations utilisant UEM, BlackBerry Infrastructure enregistre les informations utilisateur pour l'activation du terminal, valide les informations de licence et fournit un chemin d'accès approuvé entre l'organisation et chacun des utilisateurs en se basant sur une solide authentification cryptographique mutuelle. UEM maintient une connexion permanente à BlackBerry Infrastructure, de sorte qu'une seule connexion sortante vers une adresse IP approuvée suffit aux organisations pour envoyer des données aux utilisateurs. Toutes les données qui transitent entre BlackBerry Infrastructure et UEM sont authentifiées et cryptées afin de fournir à votre organisation un canal de communication sécurisé pour les terminaux situés à l'extérieur du pare-feu.

Composant	Description
BlackBerry Dynamics NOC	BlackBerry Dynamics NOC est un centre d'opérations réseau qui fournit des communications sécurisées entre les applications BlackBerry Dynamics sur les terminaux, UEM et BlackBerry Enterprise Mobility Server.
Terminaux	BlackBerry UEM prend en charge les terminaux iOS, macOS, Android et Windows.
Services de notification	UEM envoie les notifications aux terminaux UEM afin d'informer des mises à jour et de signaler certaines informations pour l'inventaire des terminaux de votre organisation. Ces notifications sont envoyées à BlackBerry Infrastructure, où elles sont transférées aux terminaux via le service de notification approprié : • APNs est un service fourni par Apple pour envoyer des notifications aux terminaux iOS et macOS. • Le service GCM fourni par Google envoie les notifications aux terminaux Android. • Les services de notification Push de Windows, fournis par Microsoft, envoient des notifications aux terminaux Windows.
Composants de routage	Par défaut, UEM établit une connexion directe avec BlackBerry Infrastructure sur les ports 3101 et 443, et vous n'avez pas besoin d'installer d'autres composants de routage. Toutefois, si les normes de sécurité de votre organisation empêchent les systèmes internes de se connecter directement à Internet, vous pouvez utiliser BlackBerry Router ou un serveur proxy. BlackBerry Router fait office de serveur proxy pour les connexions BlackBerry Infrastructure entre UEM et tous les terminaux. BlackBerry Router peut prendre en charge SOCKS v5 sans aucune authentification. Si votre organisation dispose déjà d'un serveur proxy TCP ou doit en utiliser un pour répondre à certaines exigences de mise en réseau, vous pouvez utiliser un serveur proxy TCP plutôt que BlackBerry Router. Le serveur proxy TCP peut prendre en charge SOCKS v5 sans aucune authentification. BlackBerry UEM Core et BlackBerry Proxy prennent en charge l'utilisation d'un serveur proxy HTTP pour se connecter au NOC BlackBerry Dynamics.
Serveurs d'applications et de contenu tiers	Serveurs de contenu et d'applications supplémentaires dans l'environnement de votre entreprise, comme l'annuaire d'entreprise, le serveur de messagerie, les autorités de certification, etc.
Plug-ins BlackBerry et BEMS	UEM fonctionne avec des produits d'entreprise BlackBerry complémentaires, tels que BlackBerry Enterprise Identity, BlackBerry 2FA et BlackBerry Workspaces, pour vous permettre d'étendre les fonctionnalités UEM de votre organisation. Pour plus d'informations, reportez-vous à Produits et services complémentaires. BlackBerry Enterprise Mobility Server fournit des services permettant d'envoyer des données professionnelles vers et depuis des applications BlackBerry Dynamics. Pour plus d'informations, reportez-vous à la documentation de BlackBerry Enterprise Mobility Server.

Architecture : solution BlackBerry UEM Cloud

L'architecture BlackBerry UEM Cloud a été conçue pour vous aider à gérer les terminaux mobiles de votre organisation et fournir une liaison sécurisée pour l'acheminement des données entre les serveurs de messagerie et de contenu de votre organisation et les terminaux des utilisateurs.



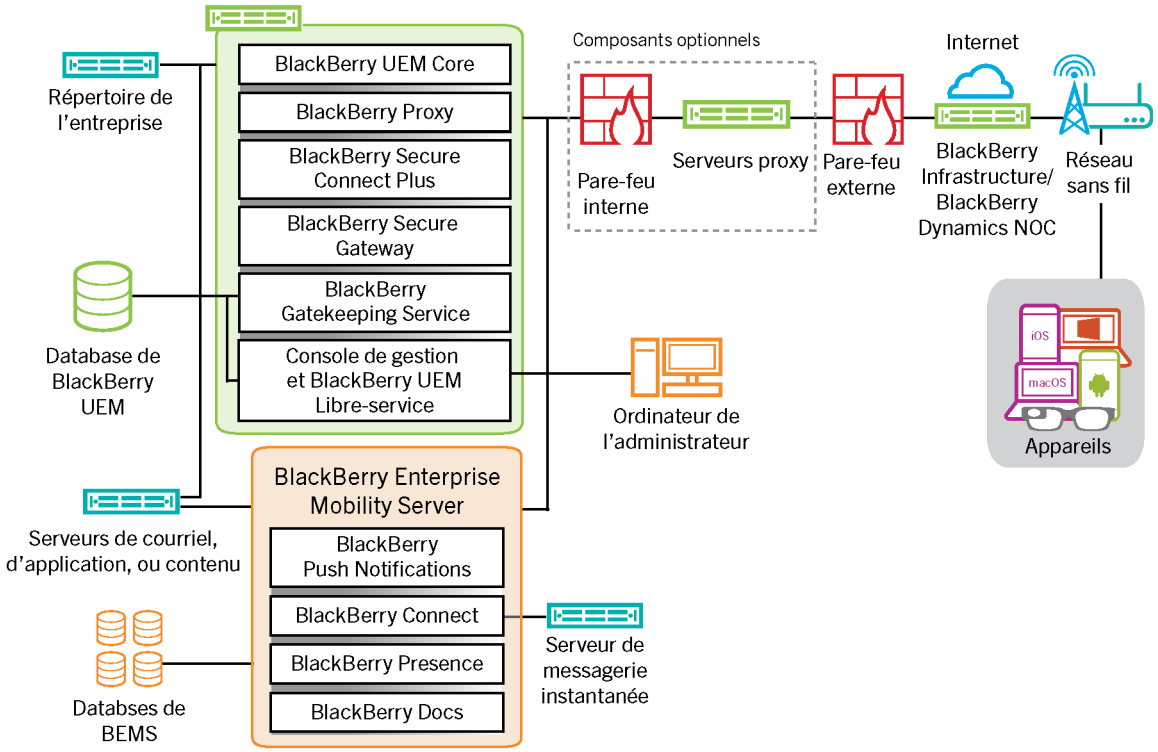
Composant	Description
BlackBerry UEM Cloud	BlackBerry UEM Cloud est un service qui vous permet de gérer les terminaux utilisés dans l'environnement de votre entreprise.
BlackBerry Infrastructure et BlackBerry Dynamics NOC	BlackBerry Infrastructure enregistre les informations utilisateur requises pour activer le terminal et valide les informations de licence. Si vous activez BlackBerry Secure Connect Plus ou BlackBerry Secure Gateway, les données en transit qui utilisent ces services passent par BlackBerry Infrastructure. BlackBerry Dynamics NOC est un NOC distinct qui permet des communications sécurisées entre les applications BlackBerry Dynamics installées sur les terminaux et BlackBerry Proxy installé derrière le pare-feu lors de l'installation de BlackBerry Connectivity Node.
Terminaux	BlackBerry UEM Cloud prend en charge les terminaux iOS, macOS, Android et Windows.

Composant	Description
Services de notification	UEM Cloud envoie les notifications aux terminaux UEM afin d'informer des mises à jour et de signaler certaines informations pour l'inventaire des terminaux de votre organisation. Ces notifications sont envoyées à BlackBerry Infrastructure, où elles sont transférées aux terminaux via le service de notification approprié : • APNs est un service fourni par Apple pour envoyer des notifications aux terminaux iOS et macOS. • Le service GCM fourni par Google envoie les notifications aux terminaux Android. • Le service WNS fourni par Microsoft envoie les notifications aux terminaux Windows 10.
BlackBerry Connectivity Node	BlackBerry Connectivity Node est un composant facultatif que vous installez à l'intérieur du pare-feu de votre entreprise. Il comprend les composants suivants qui améliorent le fonctionnement de UEM Cloud : • Le BlackBerry Cloud Connector connecte UEM Cloud à votre annuaire d'entreprise derrière le pare-feu pour permettre la synchronisation des attributs de base, une fonction de recherche et des services d'authentification des utilisateurs. Si vous n'installez pas BlackBerry Connectivity Node et que votre annuaire d'entreprise est derrière le pare-feu, vous devez créer des comptes utilisateur locaux dans UEM Cloud plutôt que d'utiliser les comptes utilisateur dans votre annuaire d'entreprise. Le BlackBerry Cloud Connector n'est pas nécessaire pour UEM Cloud afin de se connecter à Microsoft Entra ID. • BlackBerry Proxy maintient une connexion sécurisée entre votre organisation et BlackBerry Dynamics NOC, qui permet aux applications BlackBerry Dynamics de communiquer en toute sécurité avec les ressources de votre organisation derrière le pare-feu. Il prend également en charge BlackBerry Dynamics Direct Connect, qui permet aux données d'application de contourner BlackBerry Dynamics NOC. • BlackBerry Gatekeeping Service envoie les commandes à Exchange ActiveSync pour ajouter les terminaux à une liste autorisée lorsque ceux-ci sont activés sur UEM Cloud. Les terminaux non gérés qui tentent de se connecter au serveur de messagerie d'une entreprise peuvent être examinés, vérifiés et bloqués ou autorisés par un administrateur via la console de gestion de UEM. • BlackBerry Secure Connect Plus fournit un tunnel IP sécurisé entre les applications professionnelles sur les terminaux et le réseau de votre organisation. Un tunnel prenant en charge les données IPv4 standard (TCP et UDP) est établi pour chaque terminal par l'intermédiaire de BlackBerry Infrastructure. • BlackBerry Secure Gateway fournit une connexion sécurisée au serveur de messagerie de votre organisation via BlackBerry Infrastructure et UEM Cloud pour les terminaux iOS.
Répertoire d'entreprise	UEM Cloud prend en charge la connectivité avec Microsoft Active Directory ou l'annuaire d'entreprise LDAP de votre organisation derrière le pare-feu à l'aide de BlackBerry Connectivity Node.
Microsoft Entra ID (anciennement Azure AD)	Microsoft Entra ID est un service de gestion d'annuaire reposant sur le Cloud. Si votre organisation utilise Entra ID, vous pouvez vous y connecter à la place ou en plus d'un répertoire d'entreprise derrière le pare-feu.

Composant	Description
Serveurs de contenu, d'applications et de messagerie	Lorsque vous activez BlackBerry Secure Connect Plus ou lorsque des utilisateurs disposent d'applications BlackBerry Dynamics, les terminaux peuvent se connecter aux serveurs de votre entreprise sans que vous deviez ouvrir une connexion directe entre le serveur et Internet. Les données professionnelles en transit entre vos serveurs et terminaux sont envoyées via BlackBerry Secure Connect Plus et BlackBerry Infrastructure. Les données d'applications BlackBerry Dynamics sont envoyées par BlackBerry Proxy et BlackBerry Dynamics NOC. BlackBerry Secure Gateway fournit une connexion sécurisée via BlackBerry Infrastructure et BlackBerry Connectivity Node entre le serveur de messagerie de votre organisation et les terminaux iOS.
Plug-ins BlackBerry et BEMS	UEM fonctionne avec des produits d'entreprise BlackBerry complémentaires, tels que BlackBerry Enterprise Identity, BlackBerry 2FA et BlackBerry Workspaces, pour vous permettre d'étendre les fonctionnalités UEM de votre organisation. Pour plus d'informations, reportez-vous à Produits et services complémentaires. BlackBerry Enterprise Mobility Server fournit des services permettant d'envoyer des données professionnelles vers et depuis des applications BlackBerry Dynamics. Pour plus d'informations, reportez-vous à la documentation de BlackBerry Enterprise Mobility Server.

Composants BlackBerry UEM sur site

Ce schéma illustre la façon dont les composants BlackBerry UEM se connectent lorsque tous les composants sont installés dans la configuration la plus simple du produit.



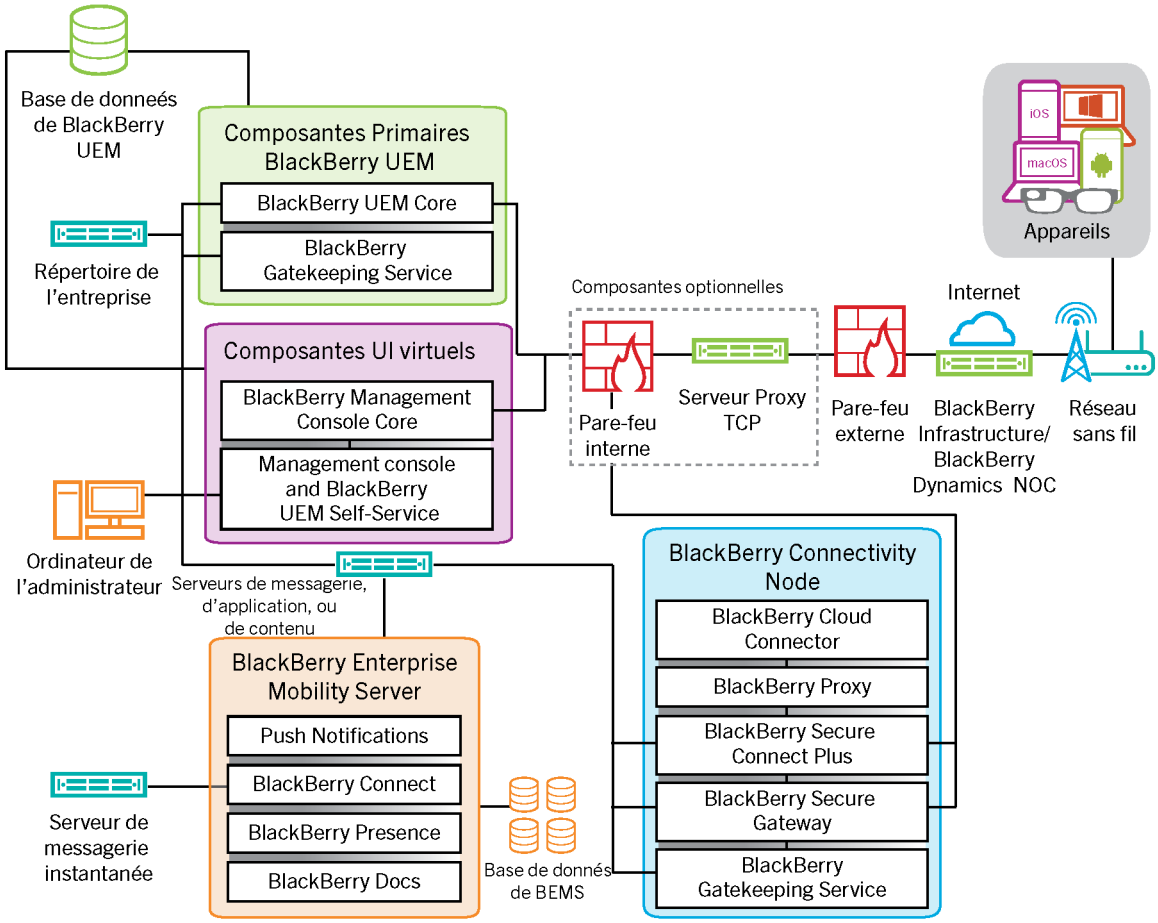
Nom du composant	Description
BlackBerry UEM Core	BlackBerry UEM Core est le composant central de l'architecture UEM. Il consiste en de nombreux sous-composants responsables des fonctions suivantes : • Fonctions de journalisation, de surveillance, de génération de rapports et de gestion • Services d'authentification et d'autorisation • Planification et envoi de commandes, de stratégies informatiques et de profils aux terminaux • Envoi de données relatives aux utilisateurs, aux stratégies et à la configuration aux applications BlackBerry Dynamics
BlackBerry Proxy	BlackBerry Proxy maintient une connexion sécurisée entre votre organisation et BlackBerry Dynamics NOC. Il prend également en charge BlackBerry Dynamics Direct Connect, qui permet aux données d'application de contourner BlackBerry Dynamics NOC.

Nom du composant	Description
BlackBerry Secure Connect Plus	BlackBerry Secure Connect Plus fournit un tunnel IP sécurisé entre les applications professionnelles sur les terminaux et le réseau de votre organisation. Un tunnel prenant en charge les données IPv4 standard (TCP et UDP) est établi pour chaque terminal par l'intermédiaire de BlackBerry Infrastructure.
BlackBerry Secure Gateway	Pour les terminaux iOS, BlackBerry Secure Gateway fournit une connexion sécurisée avec le serveur de messagerie de votre organisation par le biais de BlackBerry Infrastructure et UEM.
BlackBerry Gatekeeping Service	BlackBerry Gatekeeping Service envoie les commandes à Exchange ActiveSync pour ajouter les terminaux à une liste autorisée lorsque ceux-ci sont activés sur UEM. Les terminaux non gérés qui tentent de se connecter au serveur de messagerie d'une organisation peuvent être examinés, vérifiés et bloqués ou autorisés par un administrateur via la console de gestion.
Console de gestion et BlackBerry UEM Self-Service	La console de gestion et BlackBerry UEM Self-Service fournissent une interface utilisateur basée sur le Web pour l'accès administrateur et utilisateur à UEM. La console de gestion vous permet de gérer les paramètres système, les utilisateurs, les terminaux et les applications. Les utilisateurs peuvent utiliser UEM Self-Service pour définir un mot de passe d'activation et envoyer des commandes aux terminaux, par exemple pour définir un mot de passe, verrouiller le terminal et supprimer les données de leurs terminaux.
Base de données BlackBerry UEM	La base de données UEM est une base de données relationnelle qui contient les informations des comptes d'utilisateur et les informations de configuration utilisées par UEM pour gérer les terminaux et les applications BlackBerry Dynamics.
BlackBerry Enterprise Mobility Server	BEMS regroupe différents services qui permettent d'échanger les données professionnelles avec les applications BlackBerry Dynamics, y compris : • BlackBerry Push Notifications : accepte les demandes d'inscription push des terminaux iOS et Android, puis communique avec Microsoft Exchange pour contrôler les modifications du compte de messagerie professionnelle de l'utilisateur. • BlackBerry Connect : fournit une messagerie instantanée sécurisée, une recherche dans le répertoire d'entreprise et des informations de présence des utilisateurs aux terminaux iOS et Android. • BlackBerry Presence : fournit un état de présence en temps réel aux applications BlackBerry Dynamics. • BlackBerry Docs : permet aux utilisateurs d'applications BlackBerry Dynamics d'accéder aux documents, de les synchroniser et de les partager à l'aide leur serveur de fichiers professionnel, de SharePoint, de Box et des systèmes de gestion de contenu prenant en charge CMIS. Aucun logiciel VPN, aucune reconfiguration du pare-feu et aucune duplication des magasins de données ne sont nécessaires. Les bases de données BEMS stockent les informations relatives aux utilisateurs, aux stratégies et à la configuration.

Nom du composant	Description
BlackBerry Router et/ou serveurs proxy	Par défaut, UEM se connecte directement à BlackBerry Infrastructure via les ports 3101 et 443. Si les normes de sécurité de votre organisation empêchent les systèmes internes de se connecter directement à Internet, vous pouvez installer BlackBerry Router ou un serveur proxy TCP tiers prenant en charge SOCKS v5 sans authentification. UEM Core et BlackBerry Proxy prennent en charge un serveur proxy HTTP tiers pour la connexion à BlackBerry Dynamics NOC.
BlackBerry Infrastructure et BlackBerry Dynamics NOC	BlackBerry Infrastructure enregistre les informations utilisateur pour l'activation du terminal, valide les informations de licence et fournit un chemin d'accès approuvé entre l'entreprise et chaque utilisateur en se basant sur une solide authentification cryptographique mutuelle. BlackBerry Dynamics NOC est un NOC distinct qui permet des communications sécurisées entre les applications BlackBerry Dynamics installées sur les terminaux et UEM Core, BlackBerry Proxy et BEMS.

Installation distribuée sur site de BlackBerry UEM

Ce schéma illustre la façon dont les composants BlackBerry UEM se connectent ensemble lorsque BlackBerry Connectivity Node et l'interface utilisateur sont tous deux installés séparément des composants UEM principaux.



Nom du composant	Description
Principaux composants UEM	Les principaux composants UEM comprennent BlackBerry UEM Core et tous les composants installés avec lui sur le même serveur.
BlackBerry UEM Core	UEM Core est le composant central de l'architecture UEM. Il consiste en de nombreux sous-composants responsables des fonctions suivantes : • Fonctions de journalisation, de surveillance, de génération de rapports et de gestion • Services d'authentification et d'autorisation • Planification et envoi de commandes, de stratégies informatiques et de profils aux terminaux • Envoi de données relatives aux utilisateurs, aux stratégies et à la configuration aux applications BlackBerry Dynamics installées sur les terminaux.

Nom du composant	Description
Base de données BlackBerry UEM	La base de données UEM est une base de données relationnelle qui contient les informations des comptes d'utilisateur et les informations de configuration utilisées par UEM pour gérer les terminaux et les applications BlackBerry Dynamics.
BlackBerry Gatekeeping Service (principal)	BlackBerry Gatekeeping Service envoie les commandes à Exchange ActiveSync pour ajouter les terminaux à une liste autorisée lorsque ceux-ci sont activés sur UEM. Les terminaux non gérés qui tentent de se connecter au serveur de messagerie d'une organisation peuvent être examinés, vérifiés et bloqués ou autorisés via la console de gestion.
Composants de l'interface utilisateur distante	La console de gestion et BlackBerry UEM Self-Service peuvent être installés séparément des autres composants UEM. Si vous les installez séparément, une instance de BlackBerry Management Console Core est également installée.
BlackBerry Management Console Core	Si l'instance est installée, le système BlackBerry Management Console Core traite uniquement les demandes d'interface utilisateur de la console de gestion et de UEM Self-Service. Cela garantit la réactivité de ces interfaces même lorsque la charge sur UEM Core est élevée.
Console de gestion et BlackBerry UEM Self-Service	La console de gestion et UEM Self-Service fournissent une interface utilisateur basée sur le Web pour l'accès administrateur et utilisateur à UEM. Elle peut être installée séparément des autres composants. La console de gestion vous permet de gérer les paramètres système, les utilisateurs, les terminaux et les applications. Les utilisateurs peuvent accéder à UEM Self-Service pour définir un mot de passe d'activation et envoyer des commandes à des terminaux, par exemple pour définir un mot de passe, verrouiller le terminal et supprimer les données de leurs terminaux.

Nom du composant	Description
BlackBerry Connectivity Node	BlackBerry Connectivity Node installe les instances des composants de connectivité des terminaux UEM dans le domaine de votre organisation sur un serveur autre que UEM Core. Chaque instance de BlackBerry Connectivity Node contient les composants suivants : • BlackBerry Cloud Connector : permet aux composants BlackBerry Connectivity Node de communiquer avec UEM Core. Toutes les communications entre BlackBerry Cloud Connector et UEM Core transitent via BlackBerry Infrastructure. • BlackBerry Proxy : maintient la connexion sécurisée entre votre organisation et BlackBerry Dynamics NOC. Il prend également en charge BlackBerry Dynamics Direct Connect, qui permet aux données d'application de contourner BlackBerry Dynamics NOC. • BlackBerry Secure Connect Plus : fournit un tunnel IP sécurisé entre les applications professionnelles sur les terminaux et le réseau de votre organisation. Un tunnel prenant en charge les données IPv4 standard (TCP et UDP) est établi pour chaque terminal par l'intermédiaire de BlackBerry Infrastructure. • BlackBerry Secure Gateway : fournit une connexion sécurisée avec le serveur de messagerie de votre organisation par le biais de BlackBerry Infrastructure et UEM pour les terminaux iOS. • BlackBerry Gatekeeping Service: gère le contrôle d'accès pour votre serveur de messagerie. Si vous souhaitez que les données de contrôle d'accès soient uniquement gérées par l'instance de BlackBerry Gatekeeping Service installée avec les composants principaux de UEM, vous pouvez désactiver BlackBerry Gatekeeping Service sur chaque instance de BlackBerry Connectivity Node.
BlackBerry Enterprise Mobility Server	BEMS regroupe différents services qui permettent d'échanger les données professionnelles avec les applications BlackBerry Dynamics, y compris : • BlackBerry Push Notifications : accepte les demandes d'inscription push des terminaux iOS et Android, puis communique avec Microsoft Exchange pour contrôler les modifications du compte de messagerie professionnelle de l'utilisateur. • BlackBerry Connect : fournit une messagerie instantanée sécurisée, une recherche dans le répertoire d'entreprise et des informations de présence des utilisateurs aux terminaux iOS et Android. • BlackBerry Presence : fournit un état de présence en temps réel aux applications BlackBerry Dynamics. • BlackBerry Docs : permet aux utilisateurs d'applications BlackBerry Dynamics d'accéder aux documents, de les synchroniser et de les partager à l'aide leur serveur de fichiers professionnel, de SharePoint, de Box et des systèmes de gestion de contenu prenant en charge CMIS. Aucun logiciel VPN, aucune reconfiguration du pare-feu et aucune duplication des magasins de données ne sont nécessaires. Les bases de données BEMS stockent les informations relatives aux utilisateurs, aux stratégies et à la configuration.

Nom du composant	Description
BlackBerry Infrastructure et BlackBerry Dynamics NOC	BlackBerry Infrastructure enregistre les informations utilisateur pour l'activation du terminal, valide les informations de licence et fournit un chemin d'accès approuvé entre l'entreprise et chaque utilisateur en se basant sur une solide authentification cryptographique mutuelle. BlackBerry Dynamics NOC est un NOC distinct qui permet des communications sécurisées entre les applications BlackBerry Dynamics installées sur les terminaux et UEM Core, BlackBerry Proxy et BEMS.

Produits et services complémentaires

Cette section fournit des informations sur les nombreux produits et services complémentaires pouvant être utilisés avec BlackBerry UEM.

Applications d'entreprise et BlackBerry Dynamics

Applications d'entreprise BlackBerry

BlackBerry propose plusieurs applications d'entreprise que les administrateurs peuvent transmettre aux terminaux ou que les utilisateurs peuvent installer pour accéder aux données professionnelles et renforcer leur productivité.

Composant	Description
BlackBerry UEM Client	BlackBerry UEM Client permet à UEM de gérer les terminaux iOS et Android. Les utilisateurs ont besoin de UEM Client pour activer des terminaux iOS ou Android pour gérer des terminaux mobiles avec UEM. Les utilisateurs peuvent télécharger la dernière version du UEM Client à partir du App Store ou du Google Play. Une fois que les utilisateurs ont activé leurs terminaux, UEM Client leur permet d'effectuer les opérations suivantes : • Vérifier si leurs terminaux sont conformes aux normes de l'organisation • Afficher les profils qui leur ont été attribués • Afficher les règles de stratégie informatique qui leur ont été attribuées • Accéder aux applications professionnelles • Créer des clés d'accès pour des applications BlackBerry Dynamics • Pré-authentifier avec BlackBerry 2FA • Code OTP d'accès à un logiciel • Récupérer et envoyer par e-mail les fichiers journaux du terminal • Désactiver leurs terminaux Pour plus d'informations, consultez la documentation relative à UEM Client.
BBM Enterprise	BBM Enterprise ajoute une couche supplémentaire de cryptage de bout en bout pour les messages BBM envoyés entre les utilisateurs BBM Enterprise de votre organisation et d'autres utilisateurs BBM à l'intérieur ou à l'extérieur de votre organisation. BBM Enterprise est disponible pour les terminaux iOS, Android, Windows et macOS. BBM Enterprise utilise une bibliothèque cryptographique validée FIPS 140-2. C'est votre organisation qui possède les clés de cryptage et personne d'autre, même BlackBerry ne peut pas y accéder. Pour la plupart des terminaux, vous pouvez utiliser UEM pour affecter BBM Enterprise aux utilisateurs. Une fois que vous avez autorisé les utilisateurs à utiliser BBM Enterprise, ils peuvent télécharger l'application à partir de la boutique d'applications appropriée. Pour plus d'informations, consultez la documentation relative à BBM Enterprise.

Applications BlackBerry Dynamics

Les applications de productivité BlackBerry Dynamics permettent aux utilisateurs d'accéder aux données professionnelles et aux outils de productivité.

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. Pour plus d'informations, consultez la documentation relative à BlackBerry Work.
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. Pour plus d'informations, consultez la documentation relative à BlackBerry Access.
BlackBerry Connect	BlackBerry Connect permet la communication et la collaboration avec la messagerie instantanée sécurisée, les recherches dans le répertoire d'entreprise et la présence des utilisateurs à l'aide d'une interface facile à utiliser sur le terminal de l'utilisateur. Pour plus d'informations, consultez la documentation relative à BlackBerry Connect.
BlackBerry Tasks	BlackBerry Tasks permet aux utilisateurs de créer, modifier et gérer les tâches synchronisées avec Microsoft Exchange. Pour plus d'informations, consultez la documentation relative à BlackBerry Tasks.
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. Pour plus d'informations, consultez la documentation relative à BlackBerry Notes.
BlackBerry BRIDGE	BlackBerry BRIDGE est une application Microsoft Intune qui est activée pour BlackBerry Dynamics. Elle vous permet d'afficher, de modifier et d'enregistrer des documents en utilisant des applications Microsoft gérées par Intune, telles que Microsoft Word, Microsoft PowerPoint et Microsoft Excel dans BlackBerry Dynamics sur des terminaux iOS et Android. Pour plus d'informations, consultez la documentation relative à BlackBerry Bridge.

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.

Votre organisation peut également développer des applications BlackBerry Dynamics personnalisées à l'aide du BlackBerry Dynamics SDK. Pour plus d'informations, consultez la documentation relative à BlackBerry Dynamics SDK.

Avantages de BlackBerry Enterprise Identity

BlackBerry Enterprise Identity facilite l'accès des utilisateurs aux applications cloud à partir de n'importe quel terminal, y compris iOS, Android et les plateformes informatiques traditionnelles. Cette fonctionnalité est étroitement intégrée à BlackBerry UEM et associe une solution EMM de pointe à des capacités d'autorisation et de contrôle de tous vos services cloud.

BlackBerry Enterprise Identity fournit une identification unique (SSO) à des services cloud tels que Microsoft 365, Google Workspace, BlackBerry Workspaces et de nombreux autres. L'identification unique évite aux utilisateurs d'effectuer de nombreuses connexions ou de retenir de nombreux mots de passe. Les administrateurs peuvent également ajouter des services personnalisés à Enterprise Identity pour offrir aux utilisateurs un accès aux applications internes.

Les administrateurs utilisent la console de gestion UEM pour ajouter des services, gérer des utilisateurs et ajouter des administrateurs supplémentaires. L'intégration à UEM facilite la gestion des utilisateurs et des autorisations d'accès aux applications et services cloud depuis leurs terminaux. Les services cloud et les binaires d'applications mobiles peuvent être groupés, puis simplement attribués à des utilisateurs et à des groupes.

Pour plus d'informations, consultez la documentation relative à BlackBerry Enterprise Identity.

Avantages de BlackBerry 2FA

BlackBerry 2FA offre aux utilisateurs une authentification à deux facteurs pour accéder aux ressources de votre entreprise. Vous pouvez ainsi utiliser des terminaux iOS et Android comme second facteur d'authentification via une invite de confirmation simple lorsque des utilisateurs tentent de se connecter aux ressources de votre organisation.

Pour les utilisateurs qui ne disposent pas d'un terminal mobile ou dont la connectivité du terminal mobile est insuffisante pour prendre en charge le temps réel BlackBerry 2FA, vous pouvez émettre des jetons OTP basés sur des normes. Le premier facteur d'authentification est le mot de passe du répertoire de l'utilisateur et le second facteur est le code dynamique qui apparaît sur l'écran du jeton.

Vous gérez BlackBerry 2FA depuis la console de gestion UEM. BlackBerry 2FA est également intégré à BlackBerry Enterprise Identity. Vous pouvez utiliser BlackBerry 2FA pour fournir un second facteur d'authentification pour les ressources dont vous gérez l'accès avec Enterprise Identity.

Pour plus d'informations, consultez la documentation relative à BlackBerry 2FA.

Avantages de BlackBerry Workspaces

BlackBerry Workspaces est une plate-forme de gestion des fichiers d'entreprise qui permet aux utilisateurs d'accéder, de synchroniser, de modifier et de partager des fichiers et des dossiers en toute sécurité sur divers terminaux. BlackBerry Workspaces limite le risque de perte ou de vol des données en intégrant la sécurité de gestion des droits numériques à tous les fichiers pour que le contenu demeure sécurisé et sous votre contrôle, même après avoir été téléchargé et partagé avec d'autres utilisateurs. Avec un magasin de fichiers sécurisé et la capacité de transférer des données tout en conservant le contrôle, les employés et le personnel informatique sont assurés de la sécurité des données et des documents partagés.

Les utilisateurs peuvent accéder à BlackBerry Workspaces à partir d'un navigateur Web et depuis les applications installées sur des ordinateurs Windows et macOS ainsi que sur des terminaux iOS et Android. Le contenu est synchronisé sur tous les terminaux de l'utilisateur lorsqu'ils sont en ligne, permettant aux utilisateurs de gérer, d'afficher, de créer, de modifier et d'annoter les fichiers depuis n'importe quel appareil. Vous pouvez utiliser le

plug-in Workspaces pour BlackBerry UEM afin d'intégrer les fonctionnalités de gestion Workspaces à la console de gestion UEM.

Si votre organisation met également en œuvre BlackBerry Enterprise Identity, vous pouvez utiliser Enterprise Identity pour gérer le droit des utilisateurs à utiliser Workspaces.

Pour plus d'informations, consultez la documentation relative à BlackBerry Workspaces.

Avantages de BlackBerry UEM Notifications

BlackBerry UEM Notifications tire parti du système de communication de crise en réseau BlackBerry AtHoc pour permettre aux administrateurs d'envoyer des messages et des notifications critiques aux utilisateurs et aux groupes à partir de la console de gestion UEM.

Dans la mesure où UEM Notifications permet aux administrateurs de gérer les terminaux et les notifications au sein de la console de gestion UEM, ces derniers n'ont pas besoin de gérer et de synchroniser les informations de contact de l'utilisateur réparties sur plusieurs systèmes ou de résoudre des problèmes d'accès dans des systèmes externes. UEM Notifications utilise les informations de contact à l'aide de la synchronisation Microsoft Active Directory. UEM Notifications propose également des options de livraison flexibles, notamment les appels de conversion de texte par synthèse vocale, les SMS et les e-mails afin que les utilisateurs reçoivent des alertes via leur canal préféré, ce qui augmente la probabilité d'action et de conformité.

Les administrateurs peuvent suivre et gérer les notifications envoyées, y compris l'état détaillé des messages par mode de livraison. UEM Notifications utilise les services de livraison agréés FedRAMP et fournit un rapport complet de tous les messages envoyés et de leurs états.

BlackBerry UEM Notifications est disponible pour une utilisation avec BlackBerry UEM sur site uniquement.

Pour plus d'informations, consultez la documentation relative aux notifications UEM.

SDK d'entreprise BlackBerry

BlackBerry offre plusieurs options SDK pour aider votre organisation à personnaliser et étendre votre solution BlackBerry.

SDK	Description
BlackBerry Dynamics SDK	BlackBerry Dynamics SDK offre un ensemble d'outils puissant permettant aux développeurs de se concentrer sur la création d'applications de productivité utiles plutôt que d'avoir à apprendre comment sécuriser, déployer et gérer ces applications. Les développeurs peuvent utiliser le BlackBerry Dynamics SDK afin de développer des applications pour toutes les plateformes principales qui exploitent des services précieux, y compris les communications sécurisées, l'échange de données entre applications, la présence, les applications push, la recherche de répertoire, l'authentification unique et la gestion des identités et des accès. Pour plus d'informations, consultez la documentation relative à BlackBerry Dynamics SDK.

SDK	Description
BlackBerry Web Services	BlackBerry Web Services est un ensemble de services Web REST et SOAP que les développeurs peuvent utiliser pour créer des applications afin de gérer le domaine UEM, les comptes d'utilisateurs et tous les terminaux compatibles de votre organisation. Vous pouvez utiliser BlackBerry Web Services pour automatiser de nombreuses tâches généralement effectuées par les administrateurs à l'aide de la console de gestion. Par exemple, vous pouvez créer une application qui automatise le processus de création de comptes d'utilisateurs, ajoute des utilisateurs à plusieurs groupes et gère les terminaux des utilisateurs. Pour plus d'informations, consultez la documentation relative à BlackBerry Web Services.
BlackBerry Workspaces Android SDK	Les développeurs peuvent utiliser le SDK BlackBerry Workspaces Android pour développer des applications permettant aux utilisateurs de travailler avec des fichiers protégés par BlackBerry Workspaces. Pour plus d'informations, consultez la documentation relative à BlackBerry Workspaces Android SDK.

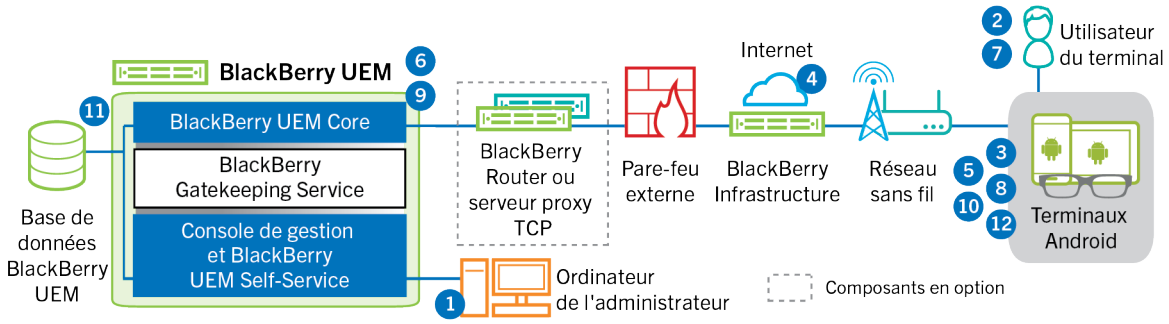
Pour plus d'informations sur l'obtention et l'utilisation de tous les outils de développement disponibles sur BlackBerry, consultez le site des développeurs de BlackBerry.

Flux de données : activation des terminaux et des applications BlackBerry Dynamics

Lorsqu'un utilisateur active un terminal avec BlackBerry UEM, le terminal est associé à UEM pour pouvoir gérer les terminaux et permettre aux utilisateurs d'accéder aux données professionnelles sur leurs terminaux. Les types d'activation de terminaux 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. Pour plus d'informations sur les types d'activation et sur la manière d'activer des terminaux, reportez-vous au contenu relatif à l'administration de l' activation des terminaux.

Cette section fournit des flux de données qui détaillent la façon dont les données transitent dans l'environnement UEM de votre organisation lorsque vous activez un terminal ou une application BlackBerry Dynamics.

Flux de données : activation d'un terminal Android Enterprise Travail et Personnel - Confidentialité des données de l'utilisateur à l'aide d'un compte Google Play géré



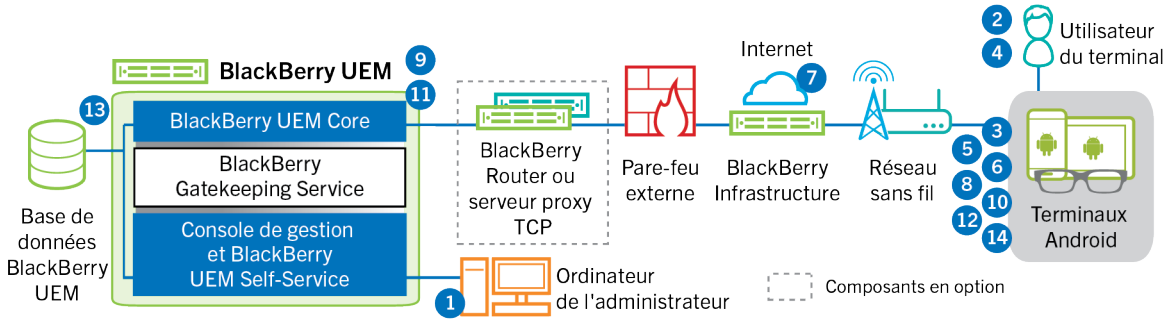
Ce flux de données s'applique lorsque vous autorisez BlackBerry UEM à gérer les comptes Google Play.

1. Vous effectuez les opérations suivantes :
   a. Ajoutez un utilisateur à BlackBerry UEM en tant que compte d'utilisateur local ou à l'aide des informations de compte récupérées depuis votre répertoire d'entreprise.
   b. Assurez-vous que le type d'activation « Travail et Personnel - Confidentialité des données de l'utilisateur » est attribué à l'utilisateur.
   c. Utilisez l'une des options suivantes pour fournir les détails d'activation à l'utilisateur :
      - Générez automatiquement un mot de passe d'activation du terminal et, de manière facultative, un QR Code, puis envoyez un e-mail contenant les instructions d'activation à l'utilisateur
      - Définissez un mot de passe d'activation du terminal et communiquez le nom d'utilisateur et le mot de passe à l'utilisateur directement ou par e-mail.
      - Ne définissez aucun mot de passe d'activation pour le terminal et ne communiquez pas l'adresse de BlackBerry UEM Self-Service à l'utilisateur afin qu'il puisse définir son propre mot de passe d'activation et afficher un QR Code.
2. L'utilisateur télécharge BlackBerry UEM Client à partir de Google Play et l'installe sur le terminal. Au terme de l'installation, l'utilisateur ouvre BlackBerry UEM Client, puis saisit son adresse électronique et le mot de passe d'activation ou lit le QR Code.
3. Depuis le terminal, BlackBerry UEM Client exécute les actions suivantes :

   a. Il se connecte à BlackBerry Infrastructure.
   b. Il envoie une demande d'informations d'activation à BlackBerry Infrastructure.
4. BlackBerry Infrastructure effectue les opérations suivantes :
   a. Il vérifie que l'utilisateur est valide et enregistré.
   b. Il récupère l'adresse BlackBerry UEM de l'utilisateur.
   c. Il envoie l'adresse à BlackBerry UEM Client.
5. BlackBerry UEM Client établit une connexion avec BlackBerry UEM via un appel HTTP CONNECT sur le port 443 et envoie une demande d'activation à BlackBerry UEM. La demande d'activation comprend le nom d'utilisateur, le mot de passe, le système d'exploitation du terminal et un identifiant de terminal unique.
6. BlackBerry UEM effectue les actions suivantes :
   a. Il détermine le type d'activation attribué au compte d'utilisateur.
   b. Il se connecte à Google et crée un utilisateur Google Play géré.
   c. Il crée une instance de terminal.
   d. Il associe l'instance du terminal au compte d'utilisateur spécifié.
   e. Il ajoute l'ID de la session d'inscription à une session HTTP
   f. Il envoie les informations du compte géré Google Play de l'utilisateur et un message d'authentification réussie au terminal.
7. Si le terminal n'est pas crypté, l'utilisateur est invité à effectuer cette action.
8. BlackBerry UEM Client effectue les opérations suivantes :
   a. Il se connecte à Google pour vérifier l'utilisateur.
   b. Crée le profil professionnel sur le terminal
   c. Il crée un CSR (requête de signature de certificat) à l'aide des informations reçues de BlackBerry UEM et envoie une demande de certificat client à BlackBerry UEM via HTTPS.
9. BlackBerry UEM effectue les actions suivantes :
   a. Il valide la demande de certificat client en la comparant à l'ID de session d'inscription dans la session HTTP.
   b. Il signe la demande de certificat client avec le certificat racine.
   c. Il renvoie le certificat client signé et le certificat racine à BlackBerry UEM Client

   Une session TLS avec authentification mutuelle est établie entre le BlackBerry UEM Client et BlackBerry UEM.
10. Le BlackBerry UEM Client demande toutes les informations de configuration et envoie les informations relatives au terminal et au logiciel à BlackBerry UEM.
11. BlackBerry UEM stocke les informations relatives au terminal dans la base de données et envoie les informations de configuration demandées au terminal.
12. Le terminal envoie un accusé de réception à BlackBerry UEM pour lui confirmer qu'il a reçu et appliqué les informations de configuration. Le processus d'activation est terminé.

Flux de données : activation d'un terminal Android Enterprise Travail et Personnel - Contrôle total à l'aide d'un compte Google Play géré



Ce flux de données s'applique lorsque vous autorisez BlackBerry UEM à gérer les comptes Google Play.

1. Vous effectuez les opérations suivantes :
   a. Ajouter un utilisateur à BlackBerry UEM en tant que compte d'utilisateur local ou à l'aide des informations de compte récupérées depuis votre répertoire d'entreprise
   b. Assurez-vous que le type d'activation « Travail et Personnel - Contrôle total » est attribué à l'utilisateur.
   c. Autorisez les QR Codes d'activation pour inclure le mot de passe d'activation et l'emplacement de téléchargement de BlackBerry UEM Client.
2. L'utilisateur réinitialise les paramètres par défaut de son terminal.
3. Le terminal redémarre et affiche un écran de bienvenue ou de démarrage.
4. L'utilisateur effectue les opérations suivantes :
   a. Il ouvre l'e-mail d'activation reçu sur son ordinateur ou un autre appareil
   b. Il appuie sept fois sur l'écran du terminal pour ouvrir un lecteur de QR Codes
   c. Il connecte le terminal à un réseau Wi-Fi.
   d. Il scanne le QR Code dans l'email d'activation
5. Le terminal effectue les opérations suivantes :
   a. Il invite l'utilisateur à crypter le terminal et redémarre.
   b. Il télécharge le UEM Client à partir de l'emplacement de téléchargement spécifié par le QR Code et l'installe
6. UEM Client effectue les opérations suivantes :
   a. Il se connecte à BlackBerry Infrastructure.
   b. Il envoie une demande d'informations d'activation à BlackBerry Infrastructure.
7. BlackBerry Infrastructure effectue les opérations suivantes :
   a. Il vérifie que l'utilisateur est valide et enregistré.
   b. Il récupère l'adresse du serveur BlackBerry UEM pour l'utilisateur.
   c. Il envoie l'adresse du serveur à UEM Client.
8. UEM Client établit une connexion avec BlackBerry UEM via un appel HTTP CONNECT sur le port 443 et envoie une demande d'activation à BlackBerry UEM. La demande d'activation comprend le nom d'utilisateur, le mot de passe, le système d'exploitation du terminal et un identifiant de terminal unique.
9. BlackBerry UEM effectue les actions suivantes :
   a. Il détermine le type d'activation attribué au compte d'utilisateur.
   b. Il se connecte à Google et crée un utilisateur Google Play géré.
   c. Il crée une instance de terminal.
   d. Il associe l'instance du terminal au compte d'utilisateur spécifié.

e. Il ajoute l'ID de la session d'inscription à une session HTTP
f. Il envoie les informations du compte géré Google Play de l'utilisateur et un message d'authentification réussie au terminal.

10. UEM Client effectue les opérations suivantes :

a. Il se connecte à Google pour vérifier l'utilisateur.
b. Crée le profil professionnel sur le terminal
c. Il crée un CSR (requête de signature de certificat) à l'aide des informations reçues de BlackBerry UEM et envoie une demande de certificat client à BlackBerry UEM via HTTPS.

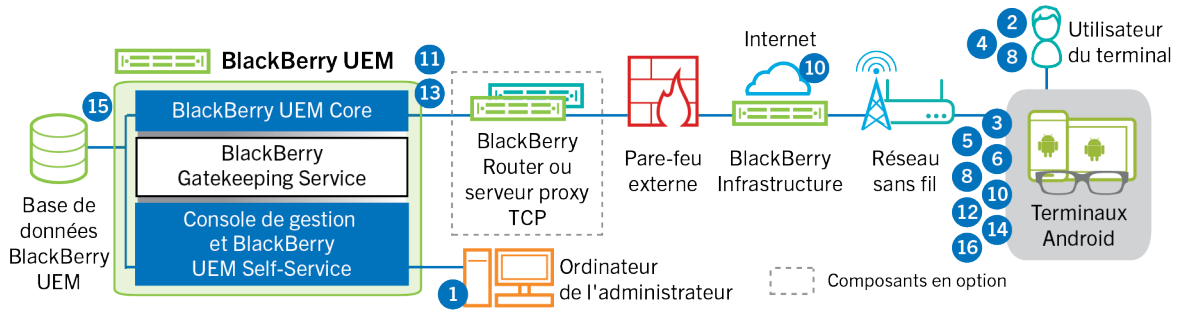
11. BlackBerry UEM effectue les actions suivantes :

a. Il valide la demande de certificat client en la comparant à l'ID de session d'inscription dans la session HTTP.
b. Il signe la demande de certificat client avec le certificat racine.
c. Il renvoie le certificat client signé et le certificat racine à UEM Client

Une session TLS avec authentification mutuelle est établie entre le UEM Client et BlackBerry UEM.

12. Le UEM Client demande toutes les informations de configuration et envoie les informations relatives au terminal et au logiciel à BlackBerry UEM.
13. BlackBerry UEM stocke les informations relatives au terminal dans la base de données et envoie les informations de configuration demandées au terminal.
14. Le terminal envoie un accusé de réception à BlackBerry UEM pour lui confirmer qu'il a reçu et appliqué les informations de configuration. Le processus d'activation est terminé.

Flux de données : activation d'un terminal Android Enterprise Espace Travail uniquement à l'aide d'un compte Google Play géré



Ce flux de données s'applique lorsque vous autorisez BlackBerry UEM à gérer les comptes Google Play.

1. Vous effectuez les opérations suivantes :

a. Ajoutez un utilisateur à BlackBerry UEM en tant que compte d'utilisateur local ou à l'aide des informations de compte récupérées depuis votre répertoire d'entreprise.
b. Assurez-vous que le type d'activation « Espace Travail uniquement » est attribué à l'utilisateur.
c. Définissez le mot de passe d'activation de l'utilisateur.

2. L'utilisateur réinitialise les paramètres par défaut de son terminal.
3. Le terminal redémarre et invite l'utilisateur à sélectionner un réseau Wi-Fi et à ajouter un compte.
4. L'utilisateur saisit ses informations d'identification Google.
5. Le terminal effectue les opérations suivantes :

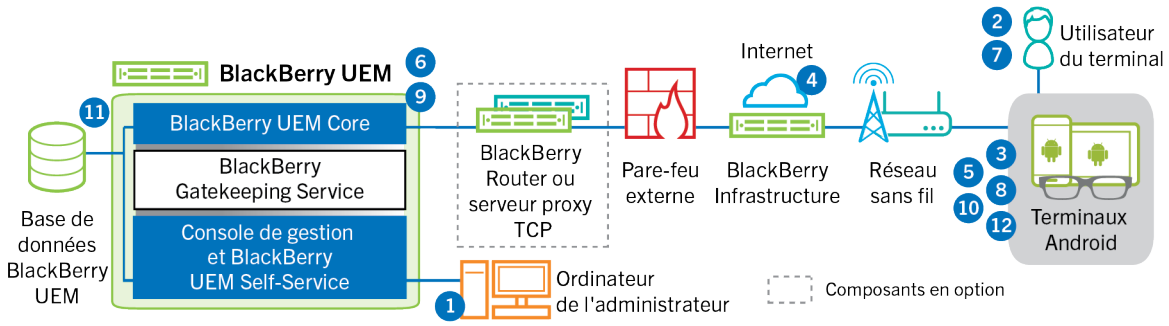
a. Si le terminal n'est pas crypté, l'utilisateur est invité à le crypter, puis le terminal redémarre.

b. Il télécharge BlackBerry UEM Client depuis Google Play et l'installe.

6. L'instance de BlackBerry UEM Client exécutée sur le terminal invite l'utilisateur à saisir son adresse électronique et son mot de passe d'activation.
7. L'utilisateur saisit son adresse électronique et son mot de passe d'activation ou lit le QR Code.
8. BlackBerry UEM Client effectue les opérations suivantes :
   a. Il se connecte à BlackBerry Infrastructure.
   b. Il envoie une demande d'informations d'activation à BlackBerry Infrastructure.
9. BlackBerry Infrastructure effectue les opérations suivantes :
   a. Il vérifie que l'utilisateur est valide et enregistré.
   b. Il récupère l'adresse du serveur BlackBerry UEM pour l'utilisateur.
   c. Il envoie l'adresse du serveur à BlackBerry UEM Client.
10. BlackBerry UEM Client établit une connexion avec BlackBerry UEM via un appel HTTP CONNECT sur le port 443 et envoie une demande d'activation à BlackBerry UEM. La demande d'activation comprend le nom d'utilisateur, le mot de passe, le système d'exploitation du terminal et un identifiant de terminal unique.
11. BlackBerry UEM effectue les actions suivantes :
   a. Il détermine le type d'activation attribué au compte d'utilisateur.
   b. Il se connecte à Google et crée un utilisateur Google Play géré.
   c. Il crée une instance de terminal.
   d. Il associe l'instance du terminal au compte d'utilisateur spécifié.
   e. Il ajoute l'ID de la session d'inscription à une session HTTP
   f. Il envoie les informations du compte géré Google Play de l'utilisateur et un message d'authentification réussie au terminal.
12. BlackBerry UEM Client effectue les opérations suivantes :
   a. Il se connecte à Google pour vérifier l'utilisateur.
   b. Il crée un CSR (requête de signature de certificat) à l'aide des informations reçues de BlackBerry UEM et envoie une demande de certificat client à BlackBerry UEM via HTTPS.
13. BlackBerry UEM effectue les actions suivantes :
   a. Il valide la demande de certificat client en la comparant à l'ID de session d'inscription dans la session HTTP.
   b. Il signe la demande de certificat client avec le certificat racine.
   c. Il renvoie le certificat client signé et le certificat racine à BlackBerry UEM Client

   Une session TLS avec authentification mutuelle est établie entre le BlackBerry UEM Client et BlackBerry UEM.
14. Le BlackBerry UEM Client demande toutes les informations de configuration et envoie les informations relatives au terminal et au logiciel à BlackBerry UEM.
15. BlackBerry UEM stocke les informations relatives au terminal dans la base de données et envoie les informations de configuration demandées au terminal.
16. Le terminal envoie un accusé de réception à BlackBerry UEM pour lui confirmer qu'il a reçu et appliqué les informations de configuration. Le processus d'activation est terminé.

Flux de données : activation d'un terminal Android Enterprise Travail et Personnel - Confidentialité des données de l'utilisateur dans un domaine Google



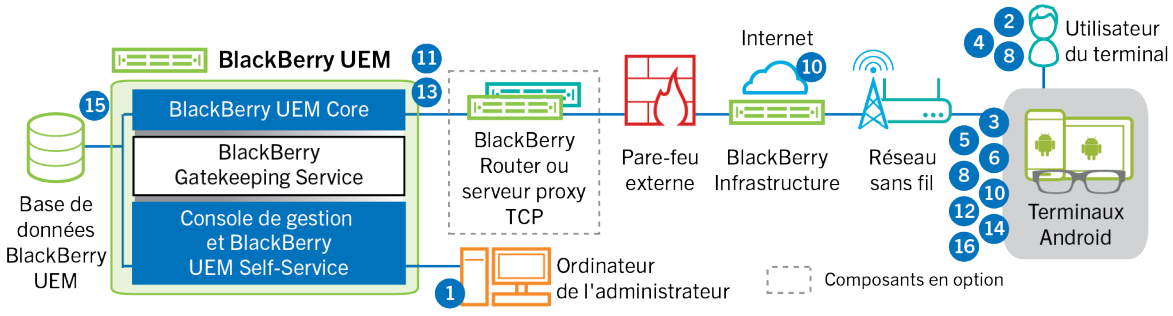
Ce flux de données s'applique lorsque BlackBerry UEM est connecté à un domaine Google Cloud ou Google Workspace.

1. Vous effectuez les opérations suivantes :
   a. Vérifiez que l'utilisateur dispose d'un compte Google associé à son adresse électronique professionnelle. Vous pouvez également configurer BlackBerry UEM pour créer le compte Google de l'utilisateur pendant le processus d'activation. Lorsque BlackBerry UEM crée le compte pour l'utilisateur dans Google, l'utilisateur reçoit un e-mail du domaine Google avec le mot de passe de son compte Google.
   b. Ajoutez un utilisateur à BlackBerry UEM en tant que compte d'utilisateur local ou à l'aide des informations de compte récupérées depuis votre répertoire d'entreprise. Lorsque vous spécifiez l'adresse électronique, utilisez celle associée au compte Google de cet utilisateur.
   c. Assurez-vous que le type d'activation « Travail et Personnel - Confidentialité des données de l'utilisateur » est attribué à l'utilisateur.
   d. Utilisez l'une des options suivantes pour fournir les détails d'activation à l'utilisateur :
      - Générez automatiquement un mot de passe d'activation du terminal et, de manière facultative, un QR Code, puis envoyez un e-mail contenant les instructions d'activation à l'utilisateur
      - Définissez un mot de passe d'activation du terminal et communiquez le nom d'utilisateur et le mot de passe à l'utilisateur directement ou par e-mail.
      - Ne définissez aucun mot de passe d'activation pour le terminal et ne communiquez pas l'adresse de BlackBerry UEM Self-Service à l'utilisateur afin qu'il puisse définir son propre mot de passe d'activation et afficher un QR Code.
2. L'utilisateur télécharge BlackBerry UEM Client à partir de Google Play et l'installe sur le terminal. Au terme de l'installation, l'utilisateur ouvre BlackBerry UEM Client, puis saisit son adresse électronique et le mot de passe d'activation ou lit le QR Code.
3. Depuis le terminal, BlackBerry UEM Client exécute les actions suivantes :
   a. Il se connecte à BlackBerry Infrastructure.
   b. Il envoie une demande d'informations d'activation à BlackBerry Infrastructure.
4. BlackBerry Infrastructure effectue les opérations suivantes :
   a. Il vérifie que l'utilisateur est valide et enregistré.
   b. Il récupère l'adresse BlackBerry UEM de l'utilisateur.
   c. Il envoie l'adresse à BlackBerry UEM Client.

5. BlackBerry UEM Client établit une connexion avec BlackBerry UEM via un appel HTTP CONNECT sur le port 443 et envoie une demande d'activation à BlackBerry UEM. La demande d'activation comprend le nom d'utilisateur, le mot de passe, le système d'exploitation du terminal et un identifiant de terminal unique.
6. BlackBerry UEM effectue les actions suivantes :
   a. Il détermine le type d'activation attribué au compte d'utilisateur.
   b. Il se connecte au domaine Google géré pour vérifier les informations de l'utilisateur. Si l'utilisateur n'existe pas, en fonction de votre configuration, BlackBerry UEM peut créer l'utilisateur dans le domaine Google.
   c. Il crée une instance de terminal.
   d. Il associe l'instance du terminal au compte d'utilisateur spécifié.
   e. Il ajoute l'ID de la session d'inscription à une session HTTP
   f. Il envoie un message d'authentification réussie au terminal
7. Si le terminal n'est pas crypté, l'utilisateur est invité à effectuer cette action.
8. BlackBerry UEM Client effectue les opérations suivantes :
   a. Crée le profil professionnel sur le terminal
   b. Invite l'utilisateur à entrer les informations du compte Google de l'utilisateur
   c. Se connecte au domaine Google géré pour authentifier l'utilisateur
   d. Crée le profil professionnel sur le terminal
   e. Crée un CSR (requête de signature de certificat) à l'aide des informations reçues de BlackBerry UEM et envoie une demande de certificat client à BlackBerry UEM via HTTPS.
9. BlackBerry UEM effectue les actions suivantes :
   a. Il valide la demande de certificat client en la comparant à l'ID de session d'inscription dans la session HTTP.
   b. Il signe la demande de certificat client avec le certificat racine.
   c. Il renvoie le certificat client signé et le certificat racine à BlackBerry UEM Client

   Une session TLS avec authentification mutuelle est établie entre le BlackBerry UEM Client et BlackBerry UEM.
10. Le BlackBerry UEM Client demande toutes les informations de configuration et envoie les informations relatives au terminal et au logiciel à BlackBerry UEM.
11. BlackBerry UEM stocke les informations relatives au terminal et envoie les informations de configuration demandées au terminal.
12. Le terminal envoie un accusé de réception à BlackBerry UEM pour lui confirmer qu'il a reçu et appliqué les informations de configuration. Le processus d'activation est terminé.

Flux de données : activation d'un terminal Android Enterprise Travail et Personnel - Contrôle total dans un domaine Google



Ce flux de données s'applique lorsque BlackBerry UEM est connecté à un domaine Google Cloud ou Google Workspace.

1. Vous effectuez les opérations suivantes :
   a. Vérifiez que l'utilisateur dispose d'un compte Google associé à son adresse électronique professionnelle. Vous pouvez également configurer BlackBerry UEM pour créer le compte Google de l'utilisateur pendant le processus d'activation. Lorsque BlackBerry UEM crée le compte pour l'utilisateur dans Google, l'utilisateur reçoit un e-mail du domaine Google avec le mot de passe de son compte Google.
   b. Vérifiez que le paramètre « Appliquer la stratégie EMM » est activé pour le domaine Google. Ce paramètre indique que les terminaux activés sont gérés par un fournisseur de modules EMM, tels que BlackBerry UEM.
   c. Ajoutez un utilisateur à BlackBerry UEM en tant que compte d'utilisateur local ou à l'aide des informations de compte récupérées depuis votre répertoire d'entreprise. Lorsque vous spécifiez l'adresse électronique, utilisez celle associée au compte Google de cet utilisateur.
   d. Assurez-vous que le type d'activation « Travail et Personnel - Contrôle total » est attribué à l'utilisateur.
   e. Définissez le mot de passe d'activation de l'utilisateur.
2. L'utilisateur réinitialise les paramètres par défaut de son terminal.
3. Le terminal redémarre et invite l'utilisateur à sélectionner un réseau Wi-Fi et à ajouter un compte.
4. L'utilisateur saisit son adresse e-mail professionnelle et son mot de passe.
5. Le terminal communique avec le domaine Google pour vérifier que l'utilisateur est un utilisateur professionnel et s'assurer que le paramètre Appliquer la stratégie EMM est activé. Après avoir effectué les validations nécessaires, le terminal effectue les opérations suivantes :
   a. Si le terminal n'est pas crypté, l'utilisateur est invité à le crypter, puis le terminal redémarre.
   b. Il télécharge BlackBerry UEM Client depuis Google Play et l'installe.
6. L'instance de BlackBerry UEM Client exécutée sur le terminal invite l'utilisateur à saisir son adresse électronique et son mot de passe d'activation.
7. L'utilisateur saisit son adresse électronique et son mot de passe d'activation ou lit le QR Code.
8. Depuis le terminal, BlackBerry UEM Client exécute les actions suivantes :
   a. Il se connecte à BlackBerry Infrastructure.
   b. Il envoie une demande d'informations d'activation à BlackBerry Infrastructure.
9. BlackBerry Infrastructure effectue les opérations suivantes :
   a. Il vérifie que l'utilisateur est valide et enregistré.
   b. Il récupère l'adresse du serveur BlackBerry UEM pour l'utilisateur.
   c. Il envoie l'adresse du serveur à BlackBerry UEM Client.
10. BlackBerry UEM Client établit une connexion avec BlackBerry UEM via un appel HTTP CONNECT sur le port 443 et envoie une demande d'activation à BlackBerry UEM. La demande d'activation comprend le nom d'utilisateur, le mot de passe, le système d'exploitation du terminal et un identifiant de terminal unique.
11. BlackBerry UEM effectue les actions suivantes :
   a. Il détermine le type d'activation attribué au compte d'utilisateur.
   b. Il se connecte au domaine Google pour vérifier les informations de l'utilisateur. Si l'utilisateur n'existe pas, en fonction de votre configuration, BlackBerry UEM peut créer l'utilisateur dans le domaine Google
   c. Il crée une instance de terminal.
   d. Il associe l'instance du terminal au compte d'utilisateur spécifié.
   e. Il ajoute l'ID de la session d'inscription à une session HTTP
   f. Il envoie un message d'authentification réussie au terminal
12. BlackBerry UEM Client effectue les opérations suivantes :
   a. Crée le profil professionnel sur le terminal
   b. Invite l'utilisateur à entrer les informations du compte Google de l'utilisateur

c. Se connecte au domaine Google pour authentifier l'utilisateur
d. Crée un CSR (requête de signature de certificat) à l'aide des informations reçues de BlackBerry UEM et envoie une demande de certificat client à BlackBerry UEM via HTTPS

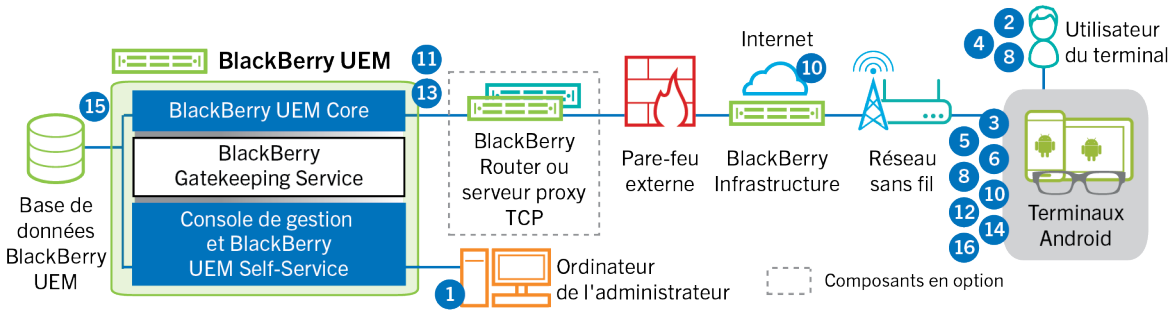
13. BlackBerry UEM effectue les actions suivantes :

a. Il valide la demande de certificat client en la comparant à l'ID de session d'inscription dans la session HTTP.
b. Il signe la demande de certificat client avec le certificat racine.
c. Il renvoie le certificat client signé et le certificat racine à BlackBerry UEM Client

Une session TLS avec authentification mutuelle est établie entre le BlackBerry UEM Client et BlackBerry UEM.

14. Le BlackBerry UEM Client demande toutes les informations de configuration et envoie les informations relatives au terminal et au logiciel à BlackBerry UEM.
15. BlackBerry UEM stocke les informations relatives au terminal et envoie les informations de configuration demandées au terminal.
16. Le terminal envoie un accusé de réception à BlackBerry UEM pour lui confirmer qu'il a reçu et appliqué les informations de configuration. Le processus d'activation est terminé.

Flux de données : activation d'un terminal Android Enterprise Espace Travail uniquement dans un domaine Google



Ce flux de données s'applique lorsque BlackBerry UEM est connecté à un domaine Google Cloud ou Google Workspace.

1. Vous effectuez les opérations suivantes :

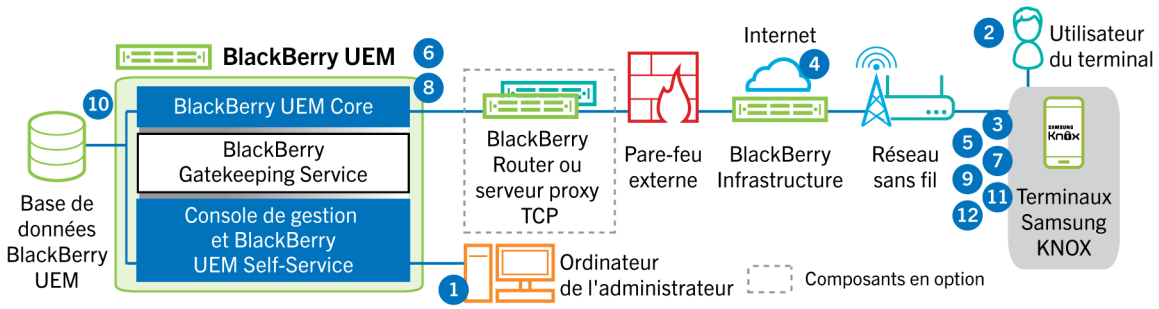
a. Vérifiez que l'utilisateur dispose d'un compte Google associé à son adresse électronique professionnelle. Vous pouvez également configurer BlackBerry UEM pour créer le compte Google de l'utilisateur pendant le processus d'activation. Lorsque BlackBerry UEM crée le compte pour l'utilisateur dans Google, l'utilisateur reçoit un e-mail du domaine Google avec le mot de passe de son compte Google.
b. Vérifiez que le paramètre « Appliquer la stratégie EMM » est activé pour le domaine Google. Ce paramètre indique que les terminaux activés sont gérés par un fournisseur de modules EMM, tels que BlackBerry UEM.
c. Ajoutez un utilisateur à BlackBerry UEM en tant que compte d'utilisateur local ou à l'aide des informations de compte récupérées depuis votre répertoire d'entreprise. Lorsque vous spécifiez l'adresse électronique, utilisez celle associée au compte Google de cet utilisateur.
d. Assurez-vous que le type d'activation « Espace Travail uniquement » est attribué à l'utilisateur.
e. Définissez le mot de passe d'activation de l'utilisateur.

2. L'utilisateur réinitialise les paramètres par défaut de son terminal.
3. Le terminal redémarre et invite l'utilisateur à sélectionner un réseau Wi-Fi et à ajouter un compte.
4. L'utilisateur saisit son adresse e-mail professionnelle et son mot de passe.

5. Le terminal communique avec le domaine Google pour vérifier que l'utilisateur est un utilisateur professionnel et s'assurer que le paramètre Appliquer la stratégie EMM est activé. Après avoir effectué les validations nécessaires, le terminal effectue les opérations suivantes :
   a. Si le terminal n'est pas crypté, l'utilisateur est invité à le crypter, puis le terminal redémarre.
   b. Il télécharge BlackBerry UEM Client depuis Google Play et l'installe
6. L'instance de BlackBerry UEM Client exécutée sur le terminal invite l'utilisateur à saisir son adresse électronique et son mot de passe d'activation.
7. L'utilisateur saisit son adresse électronique et son mot de passe d'activation ou lit le QR Code.
8. Depuis le terminal, BlackBerry UEM Client exécute les actions suivantes :
   a. Il se connecte à BlackBerry Infrastructure.
   b. Il envoie une demande d'informations d'activation à BlackBerry Infrastructure.
9. BlackBerry Infrastructure effectue les opérations suivantes :
   a. Il vérifie que l'utilisateur est valide et enregistré.
   b. Il récupère l'adresse du serveur BlackBerry UEM pour l'utilisateur.
   c. Il envoie l'adresse du serveur à BlackBerry UEM Client.
10. BlackBerry UEM Client établit une connexion avec BlackBerry UEM via un appel HTTP CONNECT sur le port 443 et envoie une demande d'activation à BlackBerry UEM. La demande d'activation comprend le nom d'utilisateur, le mot de passe, le système d'exploitation du terminal et un identifiant de terminal unique.
11. BlackBerry UEM effectue les actions suivantes :
   a. Il détermine le type d'activation attribué au compte d'utilisateur.
   b. Il se connecte au domaine Google pour vérifier les informations de l'utilisateur. Si l'utilisateur n'existe pas, en fonction de votre configuration, BlackBerry UEM peut créer l'utilisateur dans le domaine Google.
   c. Il crée une instance de terminal.
   d. Il associe l'instance du terminal au compte d'utilisateur spécifié.
   e. Il ajoute l'ID de la session d'inscription à une session HTTP
   f. Il envoie un message d'authentification réussie au terminal
12. BlackBerry UEM Client effectue les opérations suivantes :
   a. Il invite l'utilisateur à entrer les informations du compte Google de l'utilisateur.
   b. Il se connecte au domaine Google pour authentifier l'utilisateur.
   c. Il crée un CSR (requête de signature de certificat) à l'aide des informations reçues de BlackBerry UEM et envoie une demande de certificat client à BlackBerry UEM via HTTPS.
13. BlackBerry UEM effectue les actions suivantes :
   a. Il valide la demande de certificat client en la comparant à l'ID de session d'inscription dans la session HTTP.
   b. Il signe la demande de certificat client avec le certificat racine.
   c. Il renvoie le certificat client signé et le certificat racine à BlackBerry UEM Client

   Une session TLS avec authentification mutuelle est établie entre le BlackBerry UEM Client et BlackBerry UEM.
14. Le BlackBerry UEM Client demande toutes les informations de configuration et envoie les informations relatives au terminal et au logiciel à BlackBerry UEM.
15. BlackBerry UEM stocke les informations relatives au terminal et envoie les informations de configuration demandées au terminal.
16. Le terminal envoie un accusé de réception à BlackBerry UEM pour lui confirmer qu'il a reçu et appliqué les informations de configuration. Le processus d'activation est terminé.

Flux de données : activation d'un terminal pour utiliser Knox Workspace



1. Vous effectuez les opérations suivantes :
   a. Ajoutez un utilisateur à BlackBerry UEM en tant que compte d'utilisateur local ou à l'aide des informations de compte récupérées depuis votre annuaire d'entreprise.
   b. Assurez-vous que le type d'activation Travail et Personnel - Contrôle total (Samsung Knox), Travail et Personnel - Confidentialité des données de l'utilisateur (Samsung Knox) ou Espace Travail uniquement - (Samsung Knox) est attribué à l'utilisateur.
   c. Utilisez l'une des options suivantes pour fournir les détails d'activation à l'utilisateur :
      - Générez automatiquement un mot de passe d'activation du terminal et, de manière facultative, un QR Code, puis envoyez un e-mail contenant les instructions d'activation à l'utilisateur.
      - Définissez un mot de passe d'activation du terminal et communiquez le nom d'utilisateur et le mot de passe à l'utilisateur directement ou par e-mail.
      - Ne définissez aucun mot de passe d'activation pour le terminal et ne communiquez pas l'adresse de BlackBerry UEM Self-Service à l'utilisateur afin qu'il puisse définir son propre mot de passe d'activation et afficher un QR Code.
2. L'utilisateur télécharge et installe BlackBerry UEM Client sur le terminal. Au terme de l'installation, l'utilisateur ouvre BlackBerry UEM Client, puis saisit l'adresse e-mail et le mot de passe d'activation ou lit le QR Code.
3. BlackBerry UEM Client effectue les opérations suivantes :
   a. Il se connecte à BlackBerry Infrastructure.
   b. Il envoie une demande d'informations d'activation à BlackBerry Infrastructure.
4. BlackBerry Infrastructure effectue les opérations suivantes :
   a. Il vérifie que l'utilisateur est valide et enregistré.
   b. Il récupère l'adresse BlackBerry UEM de l'utilisateur.
   c. Il envoie l'adresse à BlackBerry UEM Client.
5. BlackBerry UEM Client établit une connexion avec BlackBerry UEM via un appel HTTP CONNECT sur le port 443 et envoie une demande d'activation à BlackBerry UEM. La demande d'activation comprend le nom d'utilisateur, le mot de passe, le système d'exploitation du terminal et un identifiant de terminal unique.
6. BlackBerry UEM effectue les opérations suivantes :
   a. Il vérifie que les informations d'identification sont valides.
   b. Il crée une instance de terminal.
   c. Il associe l'instance de terminal au compte d'utilisateur spécifié dans la base de données BlackBerry UEM.
   d. Il ajoute l'ID de la session d'inscription à une session HTTP
   e. Il envoie un message d'authentification réussie au terminal
7. BlackBerry UEM Client crée un CSR à l'aide des informations reçues de BlackBerry UEM et envoie une demande de certificat client à BlackBerry UEM via HTTPS.

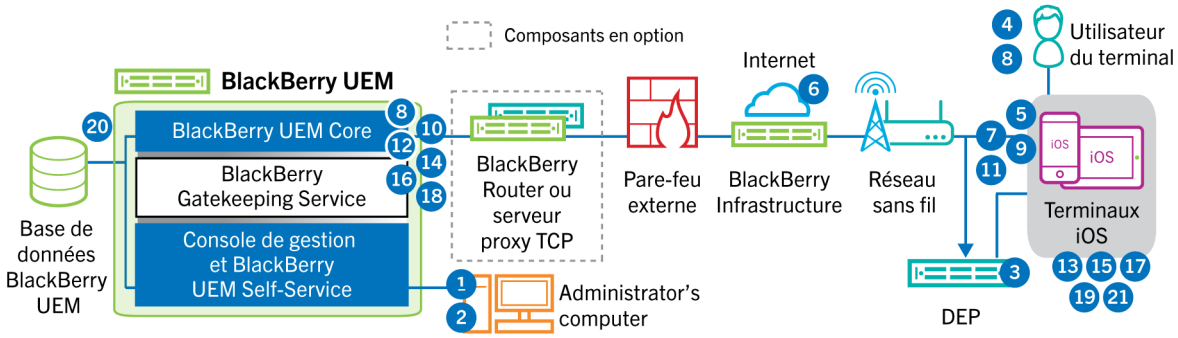
8. BlackBerry UEM effectue les actions suivantes :
   a. Il valide la demande de certificat client en la comparant à l'ID de session d'inscription dans la session HTTP.
   b. Il signe la demande de certificat client avec le certificat racine.
   c. Il renvoie le certificat client signé et le certificat racine à BlackBerry UEM Client.

   Une session TLS avec authentification mutuelle est établie entre BlackBerry UEM Client et BlackBerry UEM.
9. BlackBerry UEM Client demande toutes les informations de configuration et envoie les informations relatives au terminal et au logiciel à BlackBerry UEM.
10. BlackBerry UEM stocke les informations relatives au terminal dans la base de données et envoie les informations de configuration demandées au terminal.
11. BlackBerry UEM Client détermine si le terminal utilise Knox Workspace et exécute une version prise en charge. Si le terminal utilise Knox Workspace, il se connecte à l'infrastructure Samsung et active la licence de gestion Knox. Une fois celle-ci activée, BlackBerry UEM Client applique les règles de stratégie informatique Knox MDM et Knox Workspace.
12. Le terminal envoie un accusé de réception à BlackBerry UEM pour lui confirmer qu'il a reçu et appliqué les informations de configuration. Le processus d'activation est terminé.

Au terme de l'activation, l'utilisateur est invité à créer un mot de passe d'espace Travail pour Knox Workspace. Les données de Knox Workspace sont protégées à l'aide du cryptage et d'une méthode d'authentification, comme un mot de passe, un PIN, un motif ou une empreinte digitale.

Remarque : Si le terminal est activé avec le type d'activation Espace Travail uniquement - (Samsung Knox), le Personal Space est supprimé lorsque Knox Workspace est configuré.

Flux de données : activation d'un terminal iOS



1. Si vous prévoyez d'utiliser le Programme d'inscription des appareils Apple, vous devez effectuer les opérations suivantes :
   a. Assurez-vous que BlackBerry UEM est configuré pour se synchroniser avec DEP.
   b. Enregistrez le terminal dans DEP et attribuez-le à un serveur MDM.
   c. Attribuez une configuration d'inscription au terminal.
2. Vous effectuez les opérations suivantes :
   a. Ajoutez un utilisateur à BlackBerry UEM en tant que compte d'utilisateur local ou à l'aide des informations de compte récupérées depuis votre annuaire d'entreprise.
   b. Attribuer un profil d'activation à l'utilisateur
   c. Utilisez l'une des options suivantes pour fournir les détails d'activation à l'utilisateur :

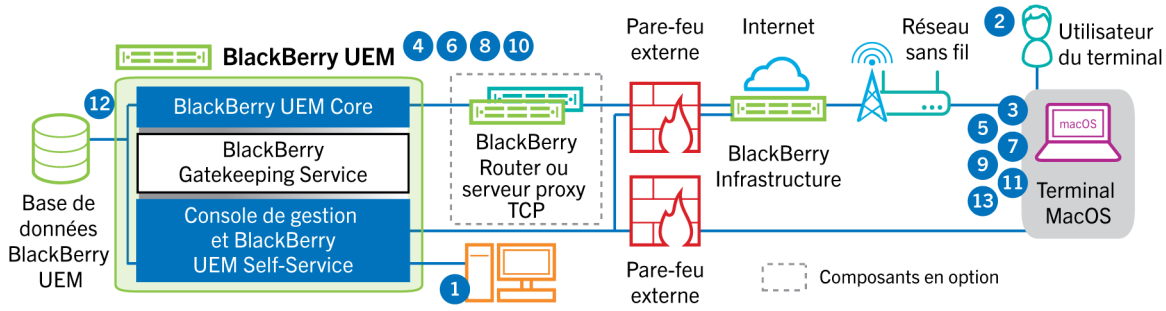
- Générez automatiquement un mot de passe d'activation du terminal et, de manière facultative, un QR Code, puis envoyez un e-mail contenant les instructions d'activation à l'utilisateur.
- Définissez un mot de passe d'activation du terminal et communiquez le nom d'utilisateur et le mot de passe à l'utilisateur directement ou par e-mail.
- Ne définissez aucun mot de passe d'activation pour le terminal et ne communiquez pas l'adresse de BlackBerry UEM Self-Service à l'utilisateur afin qu'il puisse définir son propre mot de passe d'activation et afficher un QR Code.

3. Si le terminal est enregistré dans Apple DEP, le terminal communique avec le service Web Apple DEP lors de sa configuration initiale. Si vous avez configuré le terminal pour installer l'application BlackBerry UEM Client, le terminal la télécharge et l'installe automatiquement.
4. Si le terminal n'est pas enregistré dans Apple DEP ou si vous n'avez pas configuré le terminal pour installer BlackBerry UEM Client, l'utilisateur télécharge et installe manuellement BlackBerry UEM Client sur le terminal. Au terme de l'installation, l'utilisateur ouvre BlackBerry UEM Client, puis saisit l'adresse e-mail et le mot de passe d'activation ou lit le QR Code.
5. BlackBerry UEM Client effectue les opérations suivantes :
   a. Il se connecte à BlackBerry Infrastructure.
   b. Il envoie une demande d'informations d'activation à BlackBerry Infrastructure.
6. BlackBerry Infrastructure effectue les opérations suivantes :
   a. Il vérifie que l'utilisateur est valide et enregistré.
   b. Il récupère l'adresse BlackBerry UEM de l'utilisateur.
   c. Il envoie l'adresse à BlackBerry UEM Client.
7. BlackBerry UEM Client établit une connexion avec BlackBerry UEM via un appel HTTP CONNECT sur le port 443 et envoie une demande d'activation à BlackBerry UEM. La demande d'activation comprend le nom d'utilisateur, le mot de passe, le système d'exploitation du terminal et un identifiant de terminal unique.
8. BlackBerry UEM effectue les opérations suivantes :
   a. Il vérifie que les informations d'identification sont valides.
   b. Il crée une instance de terminal.
   c. Il associe l'instance de terminal au compte d'utilisateur spécifié dans la base de données BlackBerry UEM.
   d. Il ajoute l'ID de la session d'inscription à une session HTTP
   e. Il envoie un message d'authentification réussie au terminal
9. BlackBerry UEM Client crée un CSR (requête de signature de certificat) à l'aide des informations reçues de BlackBerry UEM et envoie une demande de certificat client via HTTPS.
10. BlackBerry UEM effectue les actions suivantes :
    a. Il valide la demande de certificat client en la comparant à l'ID de session d'inscription dans la session HTTP.
    b. Il signe la demande de certificat client avec le certificat racine.
    c. Il renvoie le certificat client signé et le certificat racine à BlackBerry UEM Client.

    Une session TLS avec authentification mutuelle est établie entre BlackBerry UEM Client et BlackBerry UEM.
11. BlackBerry UEM Client affiche un message pour informer l'utilisateur qu'un certificat doit être installé afin de poursuivre l'activation. L'utilisateur clique sur OK et est redirigé vers le lien d'activation du démon MDM natif. BlackBerry UEM Client se connecte à BlackBerry UEM.
12. BlackBerry UEM fournit le profil MDM au terminal. Ce profil contient l'URL d'activation MDM et la demande. Le profil MDM est encapsulé en tant que message PKCS#7 signé et comprend la chaine de certificat complète du signataire, ce qui permet au terminal de valider le profil. Le processus d'inscription est alors déclenché.
13. Le démon MDM natif du terminal envoie le profil du terminal, qui comprend l'ID du client, la langue et la version du système d'exploitation, à BlackBerry UEM.
14. BlackBerry UEM vérifie que la demande est signée par une autorité de certification et répond au démon MDM natif en lui envoyant une notification d'authentification réussie.

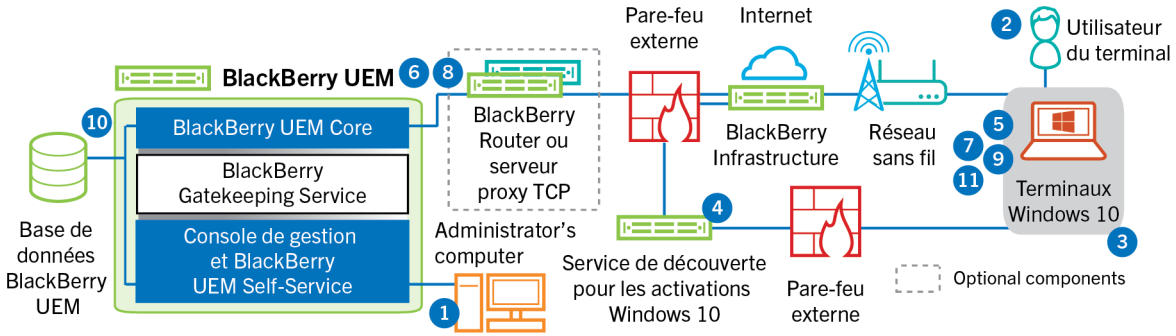
15. Le démon MDM natif envoie à BlackBerry UEM une demande de certificat de l'autorité de certification, d'informations sur les capacités de l'autorité de certification et de certificat émis par le terminal.
16. BlackBerry UEM envoie le certificat de l'autorité de certification, les informations sur les capacités de l'autorité de certification et le certificat émis par le terminal au démon MDM natif.
17. Le démon MDM natif installe le profil MDM sur le terminal. BlackBerry UEM Client informe BlackBerry UEM que l'installation du profil et du certificat MDM s'est bien déroulée et interroge régulièrement BlackBerry UEM jusqu'à ce qu'il confirme que l'activation MDM est terminée.
18. BlackBerry UEM confirme que l'activation MDM est terminée.
19. BlackBerry UEM Client demande toutes les informations de configuration et envoie les informations relatives au terminal et au logiciel à BlackBerry UEM.
20. BlackBerry UEM stocke les informations relatives au terminal dans la base de données et envoie les informations de configuration au terminal.
21. Le terminal envoie un accusé de réception à BlackBerry UEM pour lui confirmer qu'il a reçu et appliqué les mises à jour de configuration. Le processus d'activation est terminé.

Flux de données : activation d'un terminal macOS



1. Vous devez vous assurer que l'utilisateur dispose d'un compte d'utilisateur BlackBerry UEM et des informations de connexion à BlackBerry UEM Self-Service, notamment :
   - Adresse Web de BlackBerry UEM Self-Service
   - Nom d'utilisateur et mot de passe
   - Nom de domaine
2. L'utilisateur se connecte à BlackBerry UEM Self-Service sur son terminal macOS et active le terminal.
3. Le terminal envoie une demande d'activation à BlackBerry UEM sur le port 443.
4. BlackBerry UEM fournit le profil MDM au terminal. Ce profil contient l'URL d'activation MDM et la demande. Le profil MDM est encapsulé en tant que message PKCS#7 signé et comprend la chaine de certificat complète du signataire, ce qui permet au terminal de valider le profil. Le processus d'inscription est alors déclenché.
5. Le démon MDM natif du terminal envoie le profil du terminal, qui comprend l'ID du client, la langue et la version du système d'exploitation, à BlackBerry UEM.
6. BlackBerry UEM vérifie que la demande est signée par une autorité de certification et répond au démon MDM natif en lui envoyant une notification d'authentification réussie.
7. Le démon MDM natif envoie à BlackBerry UEM une demande de certificat de l'autorité de certification, d'informations sur les capacités de l'autorité de certification et de certificat émis par le terminal.
8. BlackBerry UEM envoie le certificat de l'autorité de certification, les informations sur les capacités de l'autorité de certification et le certificat émis par le terminal au démon MDM natif.
9. Le démon MDM natif installe le profil MDM sur le terminal.
10. BlackBerry UEM confirme que l'activation MDM est terminée.
11. Le terminal demande toutes les informations de configuration.
12. BlackBerry UEM stocke les informations relatives au terminal dans la base de données et envoie les informations de configuration au terminal.
13. Le terminal envoie un accusé de réception à BlackBerry UEM pour lui confirmer qu'il a reçu et appliqué les informations de configuration. Le processus d'activation est terminé.

Flux de données : activation d'un terminal Windows 10



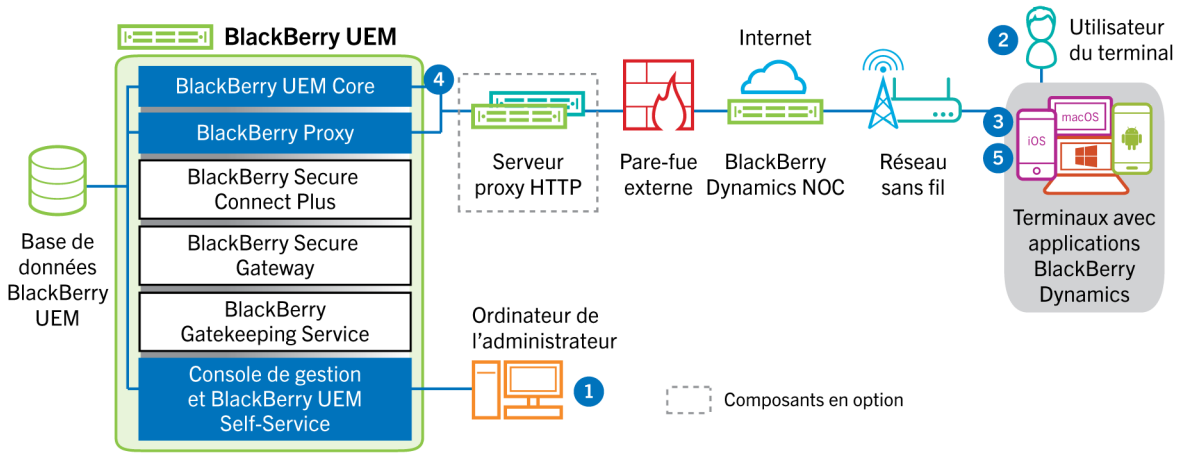
1. Vous effectuez les opérations suivantes :
   a. Configurez le service de découverte pour simplifier les activations de Windows 10.
   b. Ajoutez un utilisateur à BlackBerry UEM en tant que compte d'utilisateur local ou à l'aide des informations de compte récupérées depuis votre annuaire d'entreprise.
   c. Utilisez l'une des options suivantes pour fournir les détails d'activation à l'utilisateur :
      - Générez automatiquement le mot de passe d'activation du terminal et envoyez un e-mail d'instructions d'activation à l'utilisateur.
      - Définissez un mot de passe d'activation du terminal et sélectionnez l'option d'envoi des informations d'activation à l'adresse électronique de l'utilisateur.
      - Ne définissez aucun mot de passe d'activation pour le terminal et ne communiquez pas l'adresse de BlackBerry UEM Self-Service à l'utilisateur afin qu'il puisse définir son propre mot de passe d'activation et afficher son adresse de serveur.
   d. Fournissez à l'utilisateur un certificat d'autorité de certification généré par BlackBerry UEM à installer sur le terminal.
2. L'utilisateur effectue les actions suivantes sur son terminal :
   a. Il vérifie que le terminal dispose d'une connectivité Internet sur le port 443.
   b. Il ouvre et installe le certificat.
   c. Il accède à Paramètres > Comptes > Accès professionnel et appuie sur Se connecter.
   d. Lorsqu'il y est invité, il saisit son adresse électronique et le mot de passe d'activation qu'il a reçu dans son e-mail d'activation.
3. Le terminal établit une connexion au service de découverte que vous avez configuré pour simplifier les activations de Windows 10 dans votre organisation.
4. Le service de découverte vérifie la validité de l'ID SRP du serveur BlackBerry UEM et redirige le terminal vers BlackBerry UEM.
5. Le terminal envoie une demande d'activation à BlackBerry UEM sur le port 443. La demande d'activation comprend le nom d'utilisateur, le mot de passe, le système d'exploitation du terminal et un identifiant de terminal unique.
6. BlackBerry UEM effectue les opérations suivantes :
   a. Il vérifie que les informations d'identification sont valides.
   b. Il crée une instance de terminal.
   c. Il associe l'instance de terminal au compte d'utilisateur spécifié dans la base de données BlackBerry UEM.
   d. Il ajoute l'ID de la session d'inscription à une session HTTP
   e. Il envoie un message d'authentification réussie au terminal
7. Le terminal crée un CSR et l'envoie à BlackBerry UEM via HTTPS. Le CSR contient le nom d'utilisateur et le mot de passe d'activation.

8. BlackBerry UEM valide le nom d'utilisateur, le mot de passe et le CSR, puis renvoie le certificat client et le certificat d'autorité de certification au terminal.

   Toute communication entre le terminal et BlackBerry UEM est désormais mutuellement authentifiée de bout en bout à l'aide de ces certificats.
9. Le terminal demande toutes les informations de configuration.
10. BlackBerry UEM stocke les informations relatives au terminal dans la base de données et envoie les informations de configuration au terminal.
11. Le terminal envoie un accusé de réception à BlackBerry UEM pour lui confirmer qu'il a reçu et appliqué les informations de configuration. Le processus d'activation est terminé.

Flux de données : première activation d'une application BlackBerry Dynamics sur un terminal

Ce flux de données décrit la façon dont les données sont acheminées lorsqu'une application BlackBerry Dynamics est activée sur un terminal et qu'aucune autre application BlackBerry Dynamics ni BlackBerry UEM Client ne sont activés.



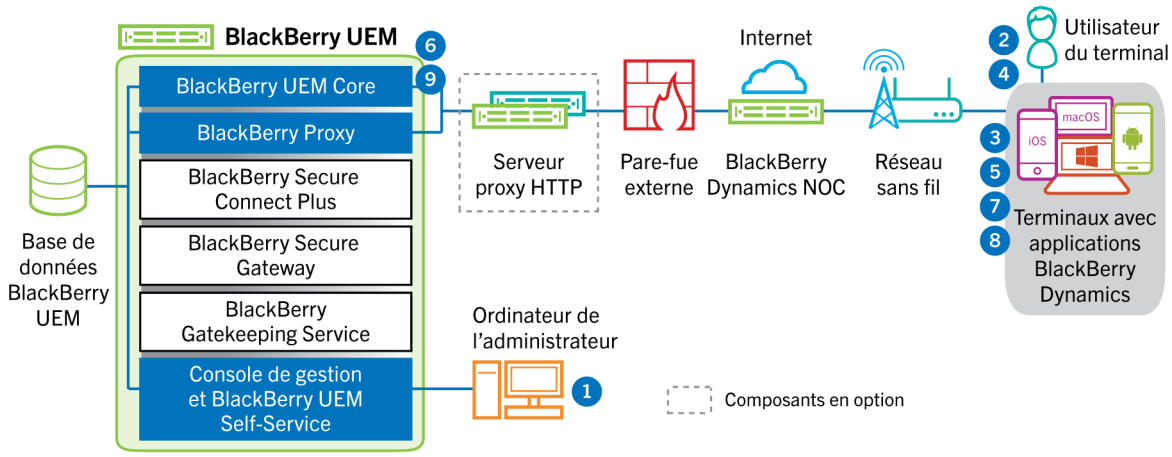
1. Un administrateur effectue les opérations suivantes :
   a. Attribue une ou plusieurs applications BlackBerry Dynamics à un utilisateur.
   b. Émet des informations d'identification d'activation (clé d'accès, mot de passe d'activation ou QR Code) ou utilise un fournisseur d'identité tiers et les envoie à l'utilisateur ou demande à l'utilisateur de générer des informations d'identification à partir de BlackBerry UEM Self-Service.
2. L'utilisateur effectue les opérations suivantes :
   a. Installe l'application sur le terminal.
   b. Obtient et saisit les informations d'identification d'activation fournies.
3. L'application BlackBerry Dynamics effectue les opérations suivantes :
   a. Se connecte à BlackBerry Dynamics NOC et termine l'activation.
   b. Obtient l'adresse BlackBerry UEM à l'aide de l'une des méthodes suivantes :
      - Si l'utilisateur a saisi manuellement les informations d'identification, l'application récupère l'adresse de l'BlackBerry Infrastructure.
      - Si l'utilisateur a scanné un QR Code, l'application reçoit l'adresse via ce QR Code.
   c. Se connecte à BlackBerry UEM via BlackBerry Infrastructure et établit une session chiffrée de bout en bout avec BlackBerry UEM à l'aide du protocole EC-SPEKE.

      Cette session ne peut être déchiffrée que par l'instance BlackBerry UEM qui a émis les informations d'identification d'activation.
   d. Envoie la demande d'activation via la session sécurisée.
4. BlackBerry UEM vérifie la demande d'activation et envoie une réponse d'activation chiffrée à l'application. La réponse d'activation inclut les données requises par l'application pour communiquer avec BlackBerry UEM, notamment un certificat client, une clé de session principale, une liste d'instances BlackBerry Proxy et des autorités de certification approuvées.
5. L'application invite l'utilisateur à définir un mot de passe pour l'application et à l'enregistrer en tant que délégué d'activation facile avec BlackBerry Dynamics NOC pour permettre à l'application BlackBerry

Dynamics suivante d'être activée sur le terminal sans que l'utilisateur n'ait besoin d'obtenir manuellement de nouvelles informations d'identification.

Flux de données : activation d'une application BlackBerry Dynamics lorsqu'une application est déjà activée sur le terminal

Ce flux de données décrit la façon dont les données sont acheminées lorsqu'une application BlackBerry Dynamics est activée sur un terminal et BlackBerry UEM Client ou qu'une autre application BlackBerry Dynamics est déjà activée et agit comme un délégué d'activation facile.



1. Un administrateur attribue une ou plusieurs applications BlackBerry Dynamics à un utilisateur.
2. L'utilisateur installe l'application sur le terminal.
3. L'application effectue les opérations suivantes :
   a. Interroge BlackBerry Dynamics NOC et identifie une autre application qui est activée sur le terminal.
   b. Demande les informations d'identification d'activation à partir de l'application précédemment activée.
4. L'utilisateur approuve la demande d'activation émise par l'application précédemment activée sur le terminal.
5. L'application précédemment activée envoie les informations d'identification à BlackBerry UEM.
6. BlackBerry UEM envoie la demande d'informations d'identification et l'URL de BlackBerry UEM à l'application existante.
7. L'application précédemment activée renvoie les informations d'identification et l'URL à la nouvelle application.
8. La nouvelle application effectue les opérations suivantes :
   a. S'active avec BlackBerry Dynamics NOC.
   b. Se connecte à BlackBerry UEM via BlackBerry Infrastructure et établit une session chiffrée de bout en bout avec BlackBerry UEM à l'aide du protocole EC-SPEKE.

      Cette session ne peut être déchiffrée que par l'instance BlackBerry UEM qui a émis les informations d'identification d'activation.
   c. Envoie la demande d'activation via la session sécurisée.
9. BlackBerry UEM vérifie la demande d'activation et envoie une réponse d'activation chiffrée à l'application. La réponse d'activation inclut les données requises par l'application pour communiquer avec BlackBerry UEM, notamment un certificat client, une clé de session principale, une liste d'instances BlackBerry Proxy et des autorités de certification approuvées.

Flux de données : envoi et réception de données professionnelles

Lorsque les terminaux qui sont activés sur BlackBerry UEM envoient et reçoivent des données professionnelles, ils se connectent aux serveurs de messagerie, d'application ou de contenu de votre entreprise. Par exemple, lorsqu'ils utilisent les applications professionnelles de messagerie ou de calendrier, les terminaux se connectent au serveur de messagerie de votre entreprise. Lorsqu'ils utilisent le navigateur professionnel pour accéder à l'intranet, les terminaux se connectent au serveur Web de votre organisation, et ainsi de suite.

Cette section fournit des flux de données qui détaillent la façon dont les données professionnelles transitent dans l'environnement UEM de votre entreprise.

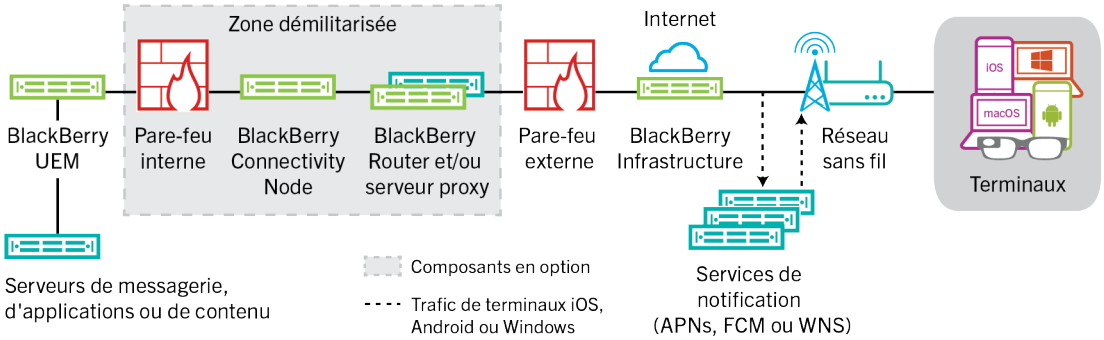
Selon le type de terminal, le type d'activation, les types de licences et les paramètres de configuration, un terminal peut établir des connexions avec les serveurs de votre entreprise en suivant les chemins d'accès suivants :

Chemin de données	Description
Réseau Wi-Fi professionnel	Vous pouvez utiliser UEM pour configurer des profils Wi-Fi pour les terminaux, de sorte que ces derniers puissent se connecter aux ressources de votre entreprise à l'aide de votre réseau Wi-Fi professionnel.
VPN	Vous pouvez utiliser UEM pour configurer les profils VPN pour les terminaux ou les utilisateurs peuvent configurer des profils VPN sur leur terminal afin que ce dernier puisse se connecter aux ressources de votre entreprise via un réseau VPN.

Chemin de données	Description
UEM et BlackBerry Infrastructure ou NOC BlackBerry Dynamics	Selon le terminal, l'activation, le type de licence et la présence ou non d'applications BlackBerry Dynamics, les terminaux peuvent être en mesure d'utiliser la connectivité d'entreprise pour communiquer avec les ressources de votre entreprise via UEM et BlackBerry Infrastructure. • Concernant les terminaux iOS, s'ils disposent d'une licence appropriée, vous pouvez activer BlackBerry Secure Gateway pour leur permettre de se connecter à votre serveur de messagerie par le biais de BlackBerry Infrastructure et de UEM. Si vous utilisez BlackBerry Secure Gateway, vous n'avez pas à exposer votre serveur de messagerie à l'extérieur du pare-feu pour autoriser les utilisateurs de terminaux iOS à se connecter à Microsoft Exchange lorsqu'ils ne sont pas connectés au réseau VPN ou au réseau Wi-Fi professionnel de votre entreprise. • Concernant les terminaux iOS, Android Enterprise et Samsung Knox Workspace, s'ils disposent d'une licence appropriée, vous pouvez utiliser la connectivité d'entreprise en activant BlackBerry Secure Connect Plus. Lorsque les terminaux utilisent BlackBerry Secure Connect Plus, les données professionnelles sont acheminées par un tunnel IP sécurisé établi entre les applications installées sur les terminaux et le réseau de votre entreprise par le biais de BlackBerry Infrastructure. • Les applications BlackBerry Dynamics installées sur les terminaux communiquent avec BlackBerry Proxy. Selon votre configuration, les données peuvent circuler via BlackBerry Dynamics NOC ou BlackBerry Infrastructure, ou les contourner à l'aide de BlackBerry Dynamics Direct Connect. • Les terminaux peuvent utiliser la connectivité d'entreprise pour toutes les données professionnelles. La connectivité d'entreprise crypte et authentifie toutes les données professionnelles et les envoie via UEM et BlackBerry Infrastructure. La connectivité d'entreprise limite le nombre de ports à ouvrir sur le pare-feu externe de votre organisation à un port unique, 3101.

Envoyer et recevoir des données professionnelles à l'aide de BlackBerry Infrastructure

Les terminaux se connectent à BlackBerry UEM via BlackBerry Infrastructure pour obtenir des mises à jour de la configuration et envoyer et recevoir des données professionnelles à l'aide de la connectivité d'entreprise ou de BlackBerry Secure Gateway. Le schéma suivant illustre comment les terminaux se connectent à BlackBerry UEM et aux ressources de votre entreprise par le biais de BlackBerry Infrastructure.



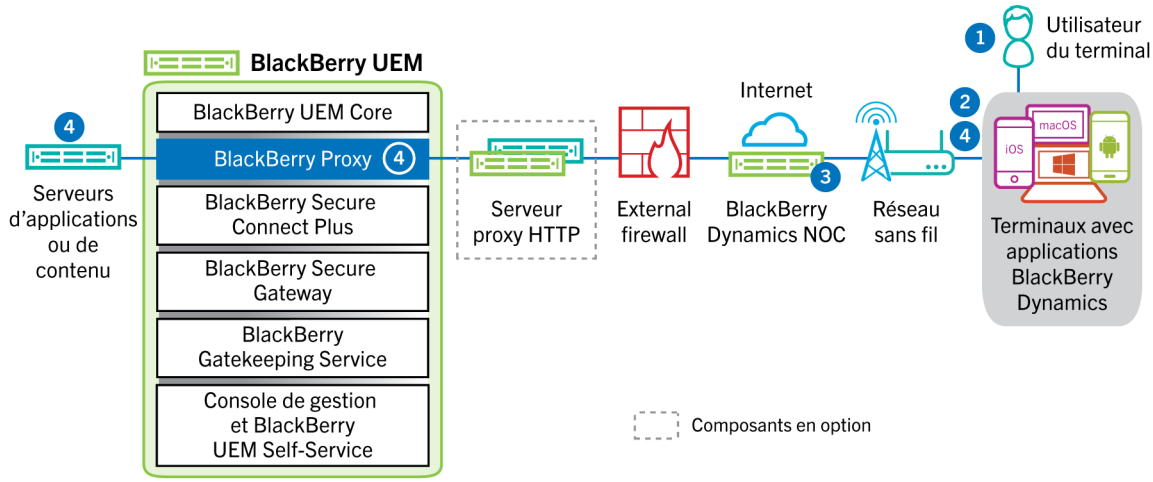
Le tableau suivant décrit les circonstances dans lesquelles les terminaux se connectent à BlackBerry UEM et au réseau de votre entreprise via BlackBerry Infrastructure.

Type de terminal	Description
Tous les terminaux	Tous les terminaux utilisent ce chemin de communication pour envoyer et recevoir les données de configuration telles que les mises à jour de commandes, de stratégies et de profils, ainsi que pour envoyer les informations relatives aux terminaux et les rapports d'activité. Pour plus d'informations, reportez-vous à Flux de données : réception de mises à jour de configuration des terminaux.
Terminaux iOS	Vous pouvez activer BlackBerry Secure Gateway pour autoriser les terminaux iOS à se connecter à votre serveur de messagerie professionnelle par le biais de BlackBerry Infrastructure et de BlackBerry UEM. Si vous utilisez BlackBerry Secure Gateway, vous n'avez pas à exposer votre serveur de messagerie à l'extérieur du pare-feu pour autoriser les utilisateurs à recevoir des e-mails professionnels lorsqu'ils ne sont pas connectés au réseau VPN ou au réseau Wi-Fi professionnel de votre entreprise.

Type de terminal	Description
Terminaux iOS, Android Enterprise et Samsung Knox Workspace.	Les terminaux ayant un profil de connectivité d'entreprise configuré pour utiliser BlackBerry Secure Connect Plus peuvent utiliser un tunnel IP sécurisé via BlackBerry Infrastructure pour transférer des données entre les applications et le réseau de votre entreprise. Pour les terminaux iOS, BlackBerry Secure Connect Plus peut fournir un tunnel sécurisé entre le réseau de votre entreprise et toutes les applications ou uniquement les applications spécifiées. Pour les terminaux Android Enterprise, BlackBerry Secure Connect Plus fournit un tunnel sécurisé entre toutes les applications de l'espace de travail et le réseau de votre entreprise. Pour les terminaux Samsung Knox Workspace, BlackBerry Secure Connect Plus peut fournir un tunnel sécurisé entre le réseau de votre entreprise et toutes les applications ou uniquement les applications spécifiées.
Terminaux iOS et Android dotés d'applications BlackBerry Dynamics	Pour les applications BlackBerry Dynamics, la connectivité d'entreprise n'utilise pas BlackBerry Infrastructure. Les données en transit entre les applications BlackBerry Dynamics et BlackBerry Proxy peuvent circuler via BlackBerry Dynamics NOC ou contourner NOC via BlackBerry Dynamics Direct Connect.

Flux de données : envoi et réception de données professionnelles depuis une application BlackBerry Dynamics via BlackBerry Dynamics NOC

Ce flux de données décrit la façon dont les données sont acheminées lorsqu'une application BlackBerry Dynamics accède à un serveur d'applications ou de contenu de votre organisation par le biais de BlackBerry Dynamics NOC et BlackBerry UEM.



1. L'utilisateur ouvre une application BlackBerry Dynamics pour accéder aux données professionnelles.
2. L'application BlackBerry Dynamics se connecte à BlackBerry Dynamics NOC. La connexion est authentifiée avec la clé principale du lien qui a été créée lors de l'activation de l'application.
3. BlackBerry Dynamics NOC communique avec BlackBerry Proxy via une connexion sécurisée préétablie afin d'établir une connexion de bout en bout entre l'application BlackBerry Dynamics et l'instance de BlackBerry

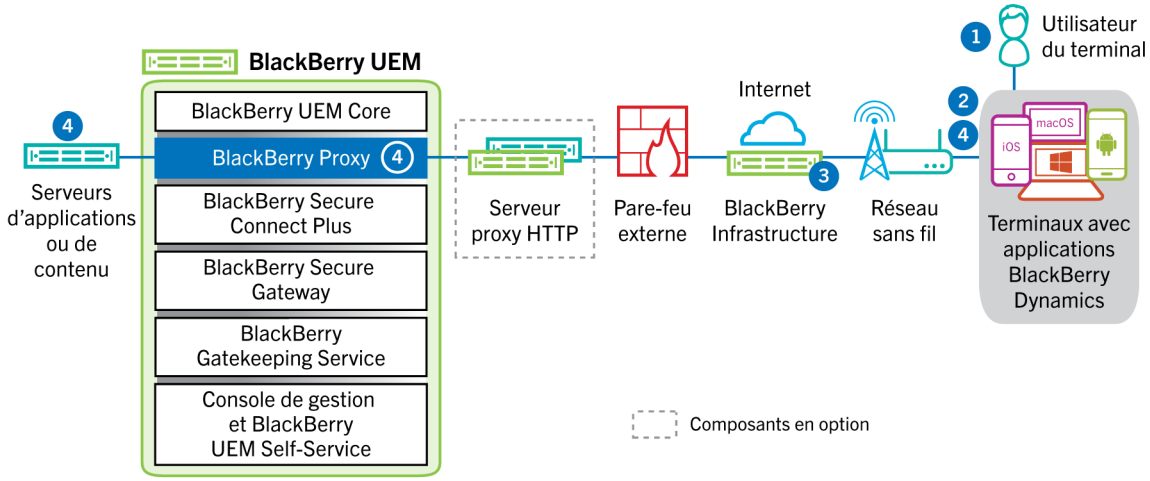
Proxy qui achemine les données professionnelles. Les données professionnelles sont cryptées avec une clé de session que BlackBerry Dynamics NOC ne connait pas.

4. Lorsque la connexion sécurisée de bout en bout est établie, les données professionnelles peuvent être acheminées derrière le pare-feu entre le terminal et les serveurs d'applications ou de contenu via BlackBerry Proxy.

Flux de données : envoi et réception de données professionnelles depuis une application BlackBerry Dynamics via BlackBerry Infrastructure

En fonction de la configuration de votre serveur, les données professionnelles des applications développées avec BlackBerry Dynamics SDK 7.0 et versions ultérieures peuvent se déplacer via BlackBerry Infrastructure plutôt que dans BlackBerry Dynamics NOC. Si vous disposez d'une nouvelle installation de BlackBerry UEM version 12.12, BlackBerry UEM utilise BlackBerry Infrastructure par défaut. Si vous avez effectué une mise à niveau à partir d'une version précédente de BlackBerry UEM, vous devez contacter l'assistance technique BlackBerry si vous souhaitez activer cette fonction.

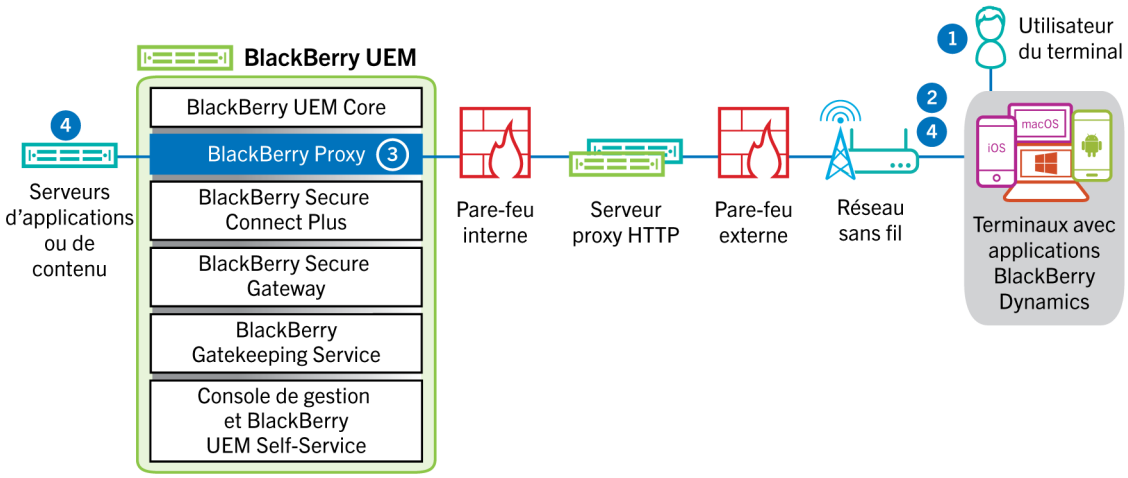
Ce flux de données décrit la façon dont les données sont acheminées lorsqu'une application BlackBerry Dynamics accède à un serveur d'applications ou de contenu de votre organisation par le biais de BlackBerry Infrastructure et BlackBerry UEM.



1. L'utilisateur ouvre une application BlackBerry Dynamics pour accéder aux données professionnelles.
2. L'application BlackBerry Dynamics se connecte à BlackBerry Infrastructure.
3. BlackBerry Infrastructure communique avec BlackBerry Proxy via une connexion TLS préétablie.
4. L'application BlackBerry Dynamics établit une connexion TLS avec BlackBerry Proxy et les données professionnelles sont échangées via une connexion sécurisée de bout en bout.

Flux de données : envoi et réception de données professionnelles depuis une application BlackBerry Dynamics à l'aide de BlackBerry Dynamics Direct Connect

Ce flux de données décrit la façon dont les données sont acheminées lorsqu'une application BlackBerry Dynamics accède à un serveur d'applications ou de contenus de votre organisation par le biais de BlackBerry Dynamics Direct Connect et BlackBerry UEM. Pour plus d'informations sur Direct Connect, reportez-vous à la section Configuration de Direct Connect avec BlackBerry UEM.

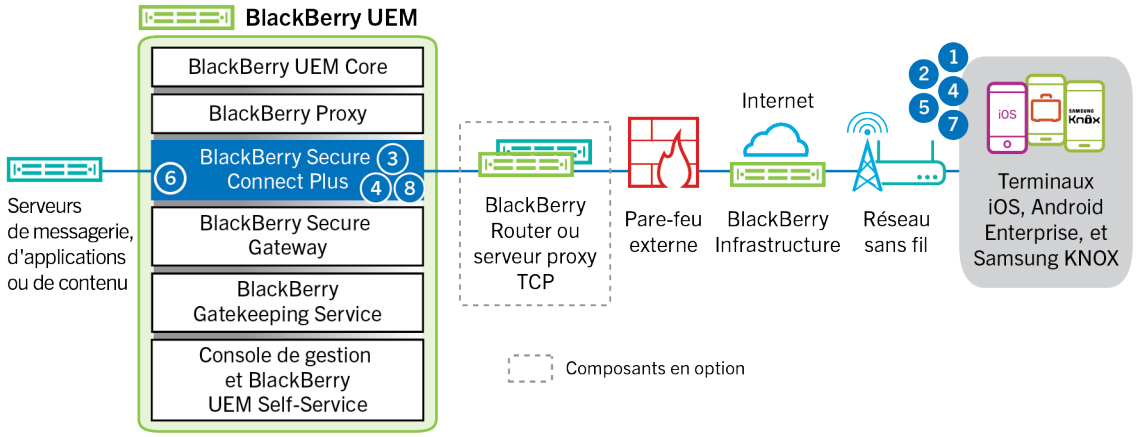


1. L'utilisateur ouvre une application BlackBerry Dynamics pour accéder aux données professionnelles.
2. L'application BlackBerry Dynamics établit une connexion TLS avec BlackBerry Proxy.
3. BlackBerry Proxy s'authentifie auprès de l'application BlackBerry Dynamics. BlackBerry Proxy s'authentifie auprès de l'application à l'aide de son certificat de serveur. BlackBerry Proxy valide l'application à l'aide d'un code MAC doté d'une clé de session que seuls BlackBerry Proxy et l'application connaissent.
4. Lorsque la connexion sécurisée de bout en bout est établie, les données professionnelles peuvent être acheminées derrière le pare-feu entre le terminal et les serveurs d'applications ou de contenu via BlackBerry Proxy.

Flux de données : accès à un serveur d'applications ou de contenu avec BlackBerry Secure Connect Plus

Ce flux de données décrit comment les données sont acheminées lorsqu'une application installée sur un terminal configuré pour utiliser BlackBerry Secure Connect Plus accède à un serveur d'applications ou de contenu de votre entreprise.

Ce flux de données ne s'applique pas aux applications BlackBerry Dynamics dans l'espace Travail sur des terminaux Android Enterprise ou Samsung Knox Workspace. Pour plus d'informations, reportez-vous à, Flux de données : envoi et réception de données professionnelles depuis une application BlackBerry Dynamics sur un terminal Android à l'aide de BlackBerry Secure Connect Plus



1. L'utilisateur ouvre une application pour accéder aux données professionnelles d'un serveur de contenu ou d'applications derrière le pare-feu de votre entreprise.

- Pour les terminaux Android Enterprise, toutes les applications de l'espace Travail à l'exception de celles pour lesquelles vous choisissez de limiter l'utilisation de BlackBerry Secure Connect Plus.
- Pour les terminaux Samsung Knox Workspace, vous devez spécifier si toutes les applications de l'espace Travail ou uniquement les applications professionnelles spécifiées doivent utiliser BlackBerry Secure Connect Plus.
- Pour les terminaux iOS, vous devez spécifier si toutes les applications ou uniquement les applications spécifiés doivent utiliser BlackBerry Secure Connect Plus.

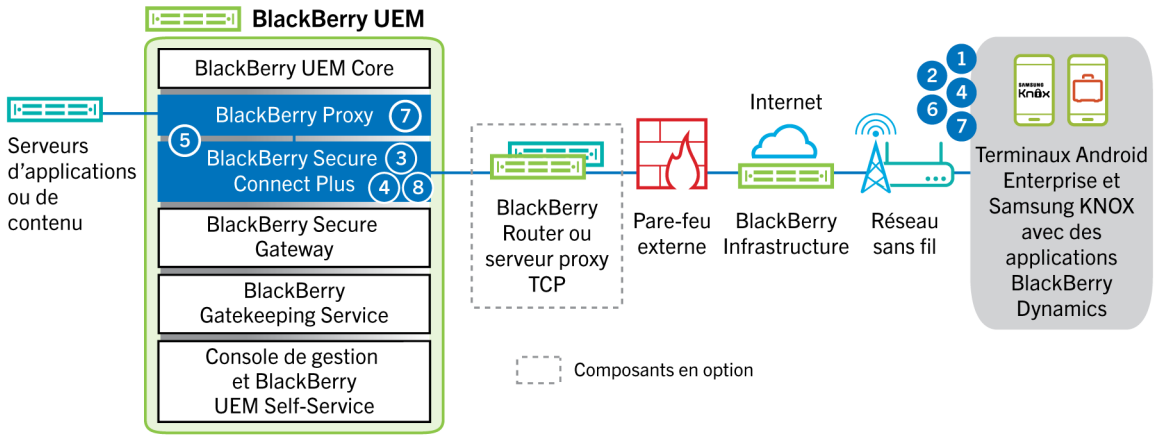
2. Le terminal envoie une requête à BlackBerry Infrastructure via un tunnel TLS, sur le port 443, pour demander un tunnel sécurisé vers le réseau professionnel. Le signal est crypté par défaut à l'aide de bibliothèques Certicom certifiées FIPS-140. Le tunnel de signalisation est crypté de bout en bout.
3. BlackBerry Secure Connect Plus reçoit la requête de BlackBerry Infrastructure via le port 3101.
4. Le terminal et BlackBerry Secure Connect Plus négocient les paramètres du tunnel et établissent un tunnel sécurisé pour le terminal via BlackBerry Infrastructure. Le tunnel est authentifié et crypté de bout en bout avec DTLS.
5. L'application utilise le tunnel pour se connecter au serveur d'applications ou de contenu à l'aide de protocoles IPv4 standard (TCP et UDP).
6. BlackBerry Secure Connect Plus transfère les données IP vers et depuis le réseau de votre entreprise. BlackBerry Secure Connect Plus crypte et décrypte le trafic en utilisant les bibliothèques Certicom certifiées FIPS-140.
7. L'application reçoit les données et les affiche sur le terminal.
8. Tant que le tunnel est ouvert, les applications prises en charge peuvent l'utiliser pour accéder aux ressources du réseau. Lorsque le tunnel n'est plus la meilleure méthode disponible pour se connecter au réseau de votre entreprise, BlackBerry Secure Connect Plus l'arrête.

Flux de données : envoi et réception de données professionnelles depuis une application BlackBerry Dynamics sur un terminal Android à l'aide de BlackBerry Secure Connect Plus

Ce flux de données décrit comment les données sont acheminées lorsqu'une application BlackBerry Dynamics sur un terminal Android Enterprise ou Samsung Knox Workspace utilise BlackBerry Secure Connect Plus.

Si vous utilisez BlackBerry Secure Connect Plus avec des applications BlackBerry Dynamics sur un terminal Android Enterprise, il est recommandé de restreindre les applications BlackBerry Dynamics qui utilisent BlackBerry Secure Connect Plus afin d'éviter une latence du réseau. Vous ne pouvez pas restreindre des applications spécifiques sur les terminaux Samsung Knox Workspace.

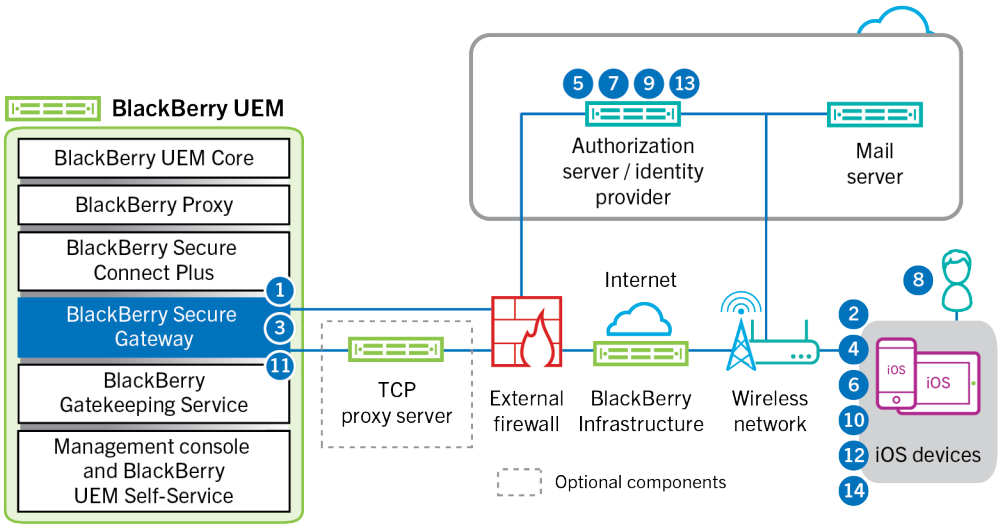
Si vous utilisez BlackBerry Secure Connect Plus avec des applications BlackBerry Dynamics sur un terminal Android Enterprise ou un terminal Samsung Knox Workspace, il est recommandé de configurer BlackBerry UEM dans le but de ne pas envoyer les données de l'application BlackBerry Dynamics à travers BlackBerry Dynamics NOC afin de réduire la latence du réseau.



1. L'utilisateur ouvre une application BlackBerry Dynamics pour accéder aux données professionnelles.
2. Le terminal envoie une requête à BlackBerry Infrastructure via un tunnel TLS, sur le port 443 pour demander un tunnel sécurisé vers le réseau professionnel. Le signal est crypté par défaut à l'aide de bibliothèques Certicom certifiées FIPS-140. Le tunnel de signalisation est crypté de bout en bout.
3. BlackBerry Secure Connect Plus reçoit la requête de BlackBerry Infrastructure via le port 3101.
4. Le terminal et BlackBerry Secure Connect Plus négocient les paramètres du tunnel et établissent un tunnel sécurisé pour le terminal via BlackBerry Infrastructure. Le tunnel est authentifié et crypté de bout en bout avec DTLS (Datagram Transport Layer Security, sécurité de la couche de transport en mode datagramme).
5. BlackBerry Secure Connect Plus établit une connexion avec BlackBerry Proxy.
6. L'application BlackBerry Dynamics se connecte à BlackBerry Proxy à l'aide du tunnel BlackBerry Secure Connect Plus.
7. BlackBerry Proxy s'authentifie auprès de l'application BlackBerry Dynamics à l'aide de son certificat de serveur. BlackBerry Proxy valide l'application à l'aide d'un code MAC doté d'une clé de session que seuls BlackBerry Proxy et l'application connaissent.
8. Lorsque la connexion sécurisée est établie entre BlackBerry Proxy et l'application, les données professionnelles peuvent circuler entre le terminal et les serveurs d'applications ou de contenu derrière le pare-feu en utilisant le tunnel BlackBerry Secure Connect Plus vers BlackBerry Proxy. BlackBerry Secure Connect Plus crypte et décrypte le trafic en utilisant les bibliothèques Certicom certifiées FIPS-140.

Flux de données: authentification auprès du serveur de messagerie à partir d'un terminal iOS lors de l'utilisation de BlackBerry Secure Gateway

Ce flux de données décrit comment les terminaux iOS s'authentifient auprès de votre serveur de messagerie via BlackBerry Secure Gateway à l'aide de l'authentification moderne Microsoft.



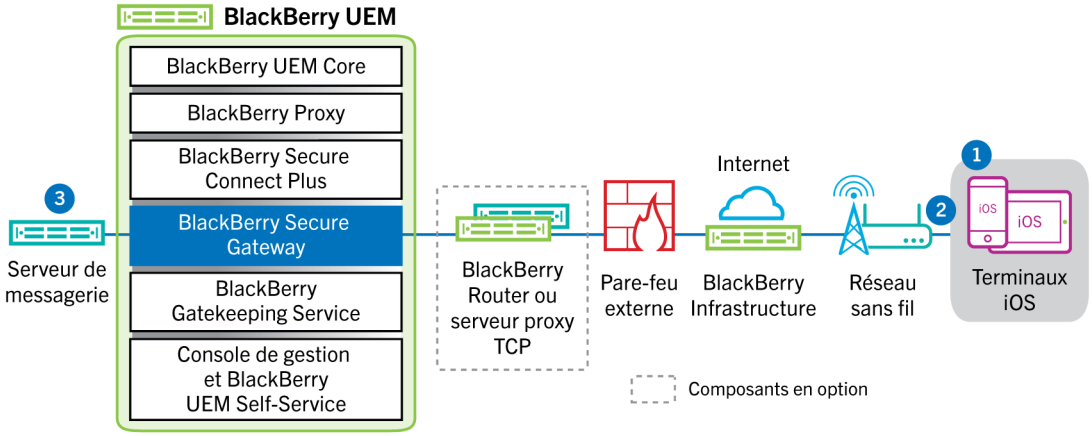
Les étapes suivantes décrivent le flux de données standard. Certains détails peuvent varier en fonction de la configuration de votre locataire Entra. Pour plus d'informations sur la façon dont le fournisseur d'identité Microsoft gère les demandes d'autorisation, reportez-vous à la documentation Microsoft.

1. BlackBerry Secure Gateway récupère et met en cache les documents de découverte provenant du serveur d'autorisation/fournisseur d'identité spécifié dans les paramètres de configuration BlackBerry Secure Gateway. BlackBerry Secure Gateway récupère à la fois le document de découverte sans version pour les terminaux iOS version 13 et le document de détection v2.0 pour les terminaux iOS version 14.6 et ultérieure.
2. Le terminal établit une connexion sécurisée avec BlackBerry Secure Gateway via BlackBerry Infrastructure.
3. Le système BlackBerry Secure Gateway établit une connexion TLS avec le serveur d'autorisation/fournisseur d'identité spécifié dans les paramètres de configuration BlackBerry Secure Gateway.
4. Le terminal envoie une demande de code d'autorisation via BlackBerry Secure Gateway au serveur d'autorisation/fournisseur d'identité.
5. Le serveur d'autorisation/fournisseur d'identité renvoie une réponse redirigée HTTP 302 au terminal.
6. L'appareil envoie une demande d'autorisation à l'URL spécifiée par la réponse redirigée. La demande n'est pas transmise par BlackBerry Secure Gateway.
7. Le serveur d'autorisation/fournisseur d'identité envoie une demande d'authentification de l'utilisateur au terminal. Le type de demande (par exemple, une page de connexion ou une invite de l'application Microsoft Authenticator) et le flux de messages pour l'authentification de l'utilisateur dépendent de la configuration de votre locataire Entra.
8. L'utilisateur fournit les informations d'identification demandées au serveur d'autorisation/fournisseur d'identité.
9. Une fois l'authentification de l'utilisateur terminée, le serveur d'autorisation/fournisseur d'identité envoie un code d'autorisation au terminal.
10. Le terminal demande le document de découverte du serveur d'autorisation/fournisseur d'identité auprès de BlackBerry Secure Gateway.
11. BlackBerry Secure Gateway envoie le document de découverte au terminal.
12. Le terminal envoie une demande de jeton d'accès au serveur d'autorisation/fournisseur d'identité via BlackBerry Secure Gateway.
13. Le serveur d'autorisation/fournisseur d'identité envoie le jeton d'accès au terminal.
14. Lorsqu'il envoie ou reçoit un e-mail, le terminal présente le jeton d'accès pour établir une connexion sécurisée avec le serveur de messagerie.

    Lorsque le jeton d'accès expire, le terminal envoie une demande de nouveau jeton au serveur d'autorisation/fournisseur d'identité via BlackBerry Secure Gateway.

Flux de données : envoi d'un e-mail depuis un terminal iOS à l'aide de BlackBerry Secure Gateway

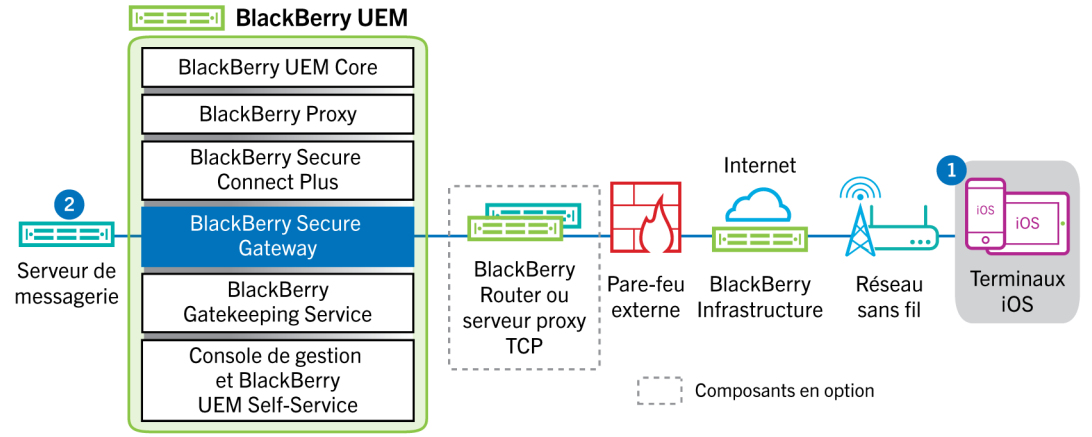
Ce flux de données décrit la façon dont les données de messagerie et de calendrier professionnelles sont acheminées des terminaux iOS vers le serveur Exchange ActiveSync à l'aide de BlackBerry Secure Gateway.



1. Un utilisateur crée un e-mail ou met à jour un élément de l'organiseur dans l'espace Travail.
2. Le terminal envoie l'élément nouveau ou modifié au serveur de messagerie via BlackBerry Infrastructure et BlackBerry Secure Gateway.
3. Le serveur de messagerie met à jour les données de l'organiseur dans la boite aux lettres de l'utilisateur ou transmet l'élément de messagerie au destinataire et envoie une confirmation au terminal.

Flux de données : réception d'un e-mail sur un terminal iOS utilisant BlackBerry Secure Gateway

Ce flux de données décrit la façon dont les données de messagerie et de calendrier professionnelles sont acheminées entre les terminaux iOS et le serveur Exchange ActiveSync à l'aide de BlackBerry Secure Gateway.

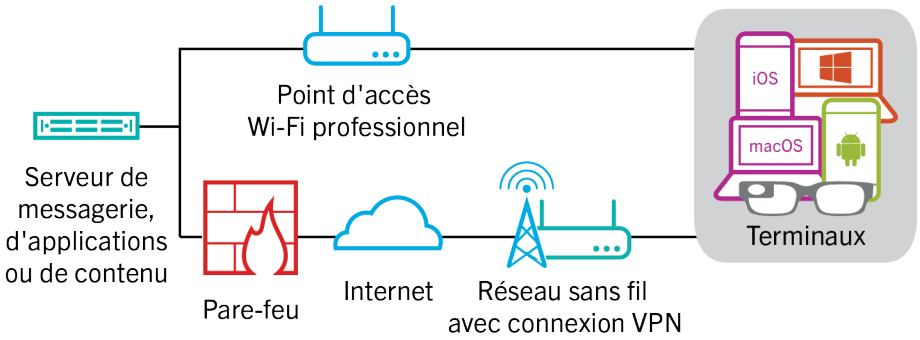


1. Le client de messagerie natif du terminal iOS maintient une connexion permanente avec le serveur de messagerie sur un canal crypté et authentifié entre BlackBerry Infrastructure et BlackBerry Secure Gateway, et détecte les changements qui interviennent dans les dossiers configurés pour la synchronisation sur le serveur de messagerie.
2. En présence d'éléments nouveaux ou modifiés destinés au terminal, comme un nouvel e-mail ou une entrée de calendrier mise à jour, le serveur de messagerie envoie ces mises à jour à l'application de messagerie ou à l'application de données de l'organiseur du terminal via le canal sécurisé établi entre BlackBerry Secure Gateway et BlackBerry Infrastructure en utilisant le protocole Exchange ActiveSync.

Envoyer et recevoir des données professionnelles à l'aide d'un réseau VPN ou d'un réseau Wi-Fi professionnel

Les terminaux pour lesquels des profils VPN ou Wi-Fi ont été configurés (par vous-même ou par les utilisateurs) peuvent accéder aux ressources de votre entreprise à l'aide du VPN ou du réseau Wi-Fi professionnel de votre entreprise. Pour utiliser le VPN de votre entreprise, les utilisateurs possédant un terminal Android avec le type d'activation Contrôles MDM ou Samsung Knox Workspace doivent configurer manuellement un profil VPN sur leur terminal.

Ce schéma illustre comment les données sont acheminées lorsqu'un terminal se connecte aux ressources de votre entreprise à l'aide du VPN ou du réseau Wi-Fi professionnel de votre entreprise.

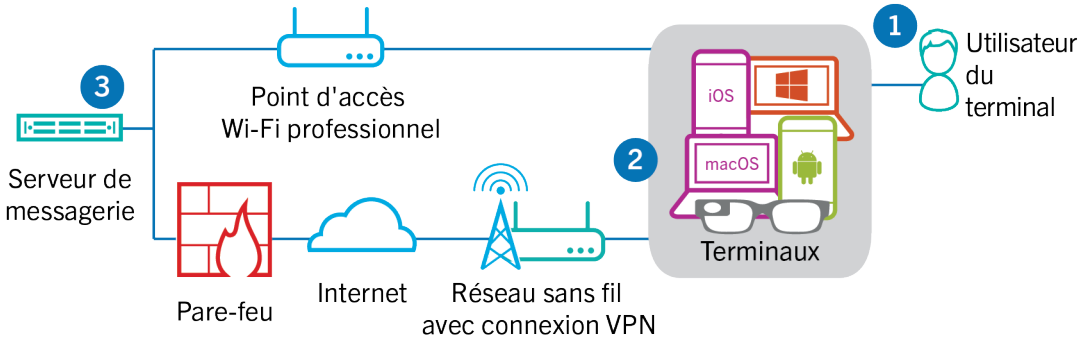


Le tableau suivant indique à quel moment les terminaux utilisent le réseau VPN ou le réseau Wi-Fi professionnel de votre entreprise pour se connecter au réseau de votre entreprise.

Type de terminal	Description
Terminaux Android Enterprise et terminaux Knox Workspace	Par défaut, les terminaux Android Enterprise et Knox Workspace utilisent le réseau VPN ou le réseau Wi-Fi professionnel de votre entreprise pour envoyer et recevoir des données professionnelles uniquement lorsque BlackBerry Secure Connect Plus est désactivé.
Terminaux Windows et macOS, et terminaux Android utilisant le type d'activation Contrôles MDM	Les terminaux Windows et macOS, ainsi que les terminaux Android utilisant le type d'activation Contrôles MDM utilisent le réseau VPN ou le réseau Wi-Fi professionnel de votre entreprise pour envoyer et recevoir les données professionnelles. Pour utiliser le VPN de votre organisation, les utilisateurs de terminaux Android doivent manuellement configurer un profil VPN sur leurs terminaux.
iOS	Les terminaux iOS utilisent le réseau VPN ou le réseau Wi-Fi professionnel de votre entreprise pour envoyer et recevoir les données Exchange ActiveSync lorsque BlackBerry Secure Gateway est désactivé. Toutes les autres données professionnelles utilisent le réseau VPN ou le réseau Wi-Fi professionnel de votre entreprise.

Flux de données : envoi d'un e-mail depuis un terminal à l'aide d'un VPN ou d'un réseau Wi-Fi professionnel

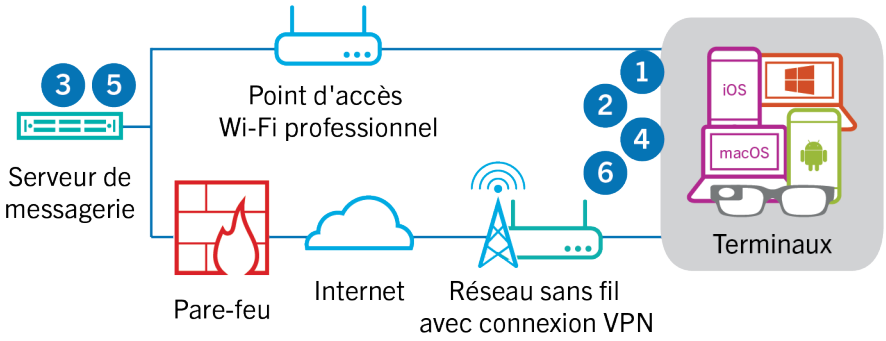
Ce flux de données décrit comment les données professionnelles de messagerie et de calendrier sont acheminées du terminal vers le serveur de messagerie sur le VPN ou réseau Wi-Fi professionnel de votre organisation via Exchange ActiveSync.



1. Un utilisateur crée un e-mail ou met à jour un élément de l'organiseur dans l'espace Travail.
2. Le terminal envoie l'élément nouveau ou modifié au serveur de messagerie sur le VPN ou le réseau Wi-Fi professionnel de votre organisation.
3. Le serveur de messagerie met à jour les données de l'organiseur dans la boite aux lettres de l'utilisateur ou transmet l'élément de messagerie au destinataire et envoie une confirmation au terminal.

Flux de données : réception d'un e-mail sur un terminal à l'aide d'un VPN ou d'un réseau Wi-Fi professionnel

Ce flux de données décrit comment les données professionnelles de messagerie et de calendrier sont acheminées du terminal vers le serveur de messagerie sur le VPN ou réseau Wi-Fi professionnel de votre organisation via Exchange ActiveSync.

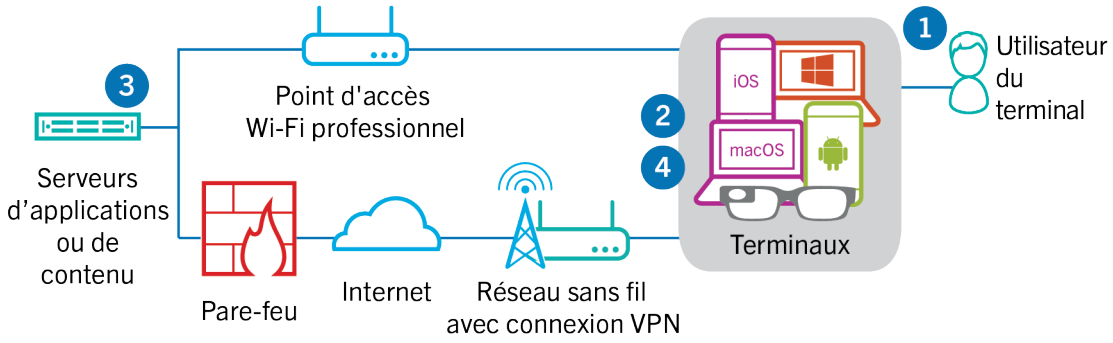


1. Le terminal adresse une demande HTTPS au serveur de messagerie pour que celui-ci le notifie en cas de modification des éléments dans les dossiers qui sont configurés pour se synchroniser. La demande est acheminée vers le serveur de messagerie via le VPN ou le réseau Wi-Fi professionnel de votre organisation.
2. Le terminal se met en veille.
3. En présence d'éléments nouveaux ou modifiés destinés au terminal, comme un nouvel e-mail ou une entrée de calendrier mise à jour, le serveur de messagerie envoie les mises à jour au terminal. Les éléments nouveaux ou modifiés sont acheminés vers l'application de messagerie ou de données de l'organiseur du terminal via le VPN ou le réseau Wi-Fi professionnel de votre organisation.
4. Lorsque la synchronisation est terminée, le terminal émet une autre demande pour recommencer le processus.

5. En l'absence d'éléments nouveaux ou modifiés au cours de cet intervalle, le serveur de messagerie ou d'applications envoie un message au terminal en utilisant le protocole Exchange ActiveSync.
6. Le terminal émet une nouvelle demande et le processus recommence.

Flux de données : accès à un serveur d'applications ou de contenu avec un VPN ou un réseau Wi-Fi professionnel

Ce flux de données décrit comment les données sont acheminées entre un serveur d'applications ou de contenu de votre organisation et une application installée sur un terminal à l'aide de la connexion VPN ou d'un réseau Wi-Fi professionnel.



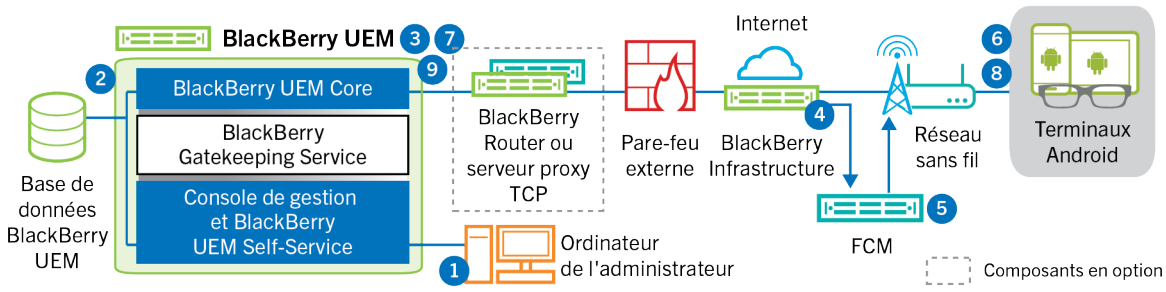
1. L'utilisateur ouvre une application professionnelle pour consulter des données professionnelles. Par exemple, il ouvre le navigateur professionnel pour naviguer sur l'intranet ou il utilise une application développée en interne pour accéder aux données clients de l'entreprise.
2. L'application se connecte au serveur d'applications ou de contenu pour récupérer les données. La demande est acheminée vers le serveur d'applications ou de contenu via le VPN ou le réseau Wi-Fi professionnel de votre organisation.
3. Le serveur d'applications ou de contenu répond en fournissant les données professionnelles. Les données professionnelles sont acheminées vers l'application de l'espace Travail du terminal via le VPN ou le réseau Wi-Fi professionnel de votre organisation.
4. L'application reçoit les données et les affiche sur le terminal.

Flux de données : réception de mises à jour de configuration des terminaux

Lorsque vous utilisez la console de gestion pour envoyer des commandes au terminal (pour le verrouiller ou pour supprimer ses données professionnelles, par exemple), ou lorsque vous effectuez d'autres tâches de gestion sur le terminal (pour mettre à jour les stratégies, les profils et les paramètres d'applications ou encore pour les attributions), vous déclenchez une mise à jour de configuration du terminal.

Cette section fournit des flux de données qui détaillent la façon dont les données transitent dans l'environnement UEM de votre organisation lorsque les terminaux reçoivent des mises à jour de configuration.

Flux de données : réception de mises à jour de configuration sur un terminal Android



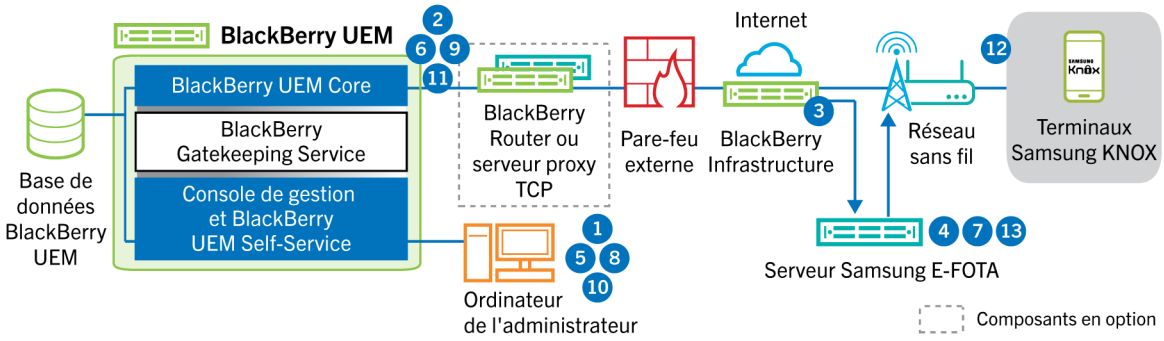
1. Sur la console de gestion, une action déclenche la mise à jour de configuration d'un terminal Android.
2. Les mises à jour sont appliquées dans BlackBerry UEM, et les objets qui doivent être partagés avec le terminal sont identifiés.
3. BlackBerry UEM Core contacte BlackBerry Infrastructure, par le biais de BlackBerry Router ou du serveur proxy TCP, s'il est installé, ainsi que le pare-feu externe sur le port 3101.
4. BlackBerry Infrastructure utilise le service FCM pour notifier les terminaux Android qu'une mise à jour est en attente.
5. Le service FCM envoie une notification à BlackBerry UEM Client sur le terminal Android pour contacter BlackBerry UEM Core.
6. BlackBerry UEM Client contacte BlackBerry UEM Core, sur le port 3101 du pare-feu externe, pour demander toutes les actions et commandes en attente à exécuter sur le terminal.
7. BlackBerry UEM Core répond, par le biais de BlackBerry Infrastructure et BlackBerry Router ou du serveur proxy TCP, s'il est installé, en commençant par l'action dont la priorité est la plus élevée.

   L'ordre de priorité est le suivant : commandes d'administration informatique (telles que Supprimer les données du terminal et Verrouiller le terminal), demandes d'informations sur le terminal, applications installées, etc. BlackBerry UEM Core n'envoie qu'une seule commande à la fois. Si nécessaire, des informations supplémentaires sont incluses dans la réponse.
8. BlackBerry UEM Client examine la réponse, planifie la commande à traiter et attend l'exécution de celle-ci. BlackBerry UEM Client envoie une réponse à BlackBerry UEM Core, via BlackBerry Infrastructure, pour mettre à jour l'état de la commande. L'état indique si la commande a bien été exécutée et affiche un message d'erreur en cas d'échec.
9. Si d'autres actions ou commandes sont en attente pour le terminal, BlackBerry UEM Core répond, via BlackBerry Infrastructure, en commençant par l'action dont la priorité est la plus élevée. Si aucune action ou commande n'est en attente pour le terminal, BlackBerry UEM Core répond avec une commande d'inactivité.

   Les étapes 7 à 9 sont répétées jusqu'à ce qu'il ne reste aucune action ou commande en attente sur le terminal.

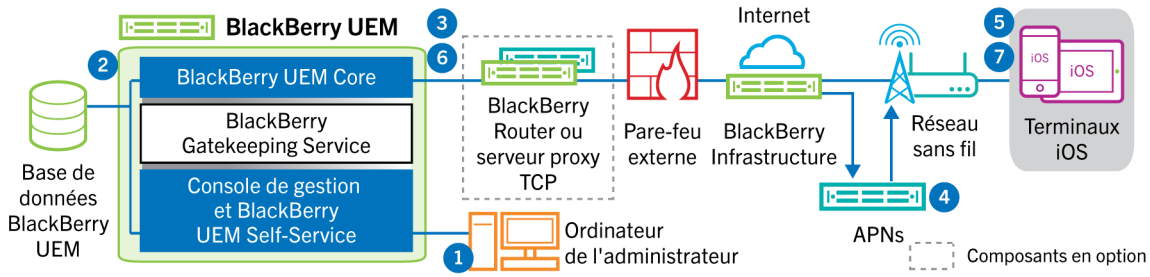
Flux de données : mise à jour du micrologiciel sur les terminaux Samsung Knox

Ce flux de données décrit comment les données sont transmises lorsque vous utilisez le micrologiciel Samsung Enterprise Firmware Over the Air pour contrôler le moment où les mises à jour du micrologiciel de Samsung sont mises en œuvre sur les terminaux.



1. Un administrateur ajoute un ID client Samsung E-FOTA et une clé de licence à BlackBerry UEM.
2. BlackBerry UEM Core envoie les données de la licence à BlackBerry Infrastructure via une connexion TLS.
3. BlackBerry Infrastructure établit une connexion TLS avec les serveurs E-FOTA Samsung et fournit l'ID client et la clé de licence.
4. Le serveur E-FOTA vérifie les informations et renvoie les informations de licence via BlackBerry Infrastructure à BlackBerry UEM Core.
5. Un administrateur crée un profil de configuration logicielle minimale requise pour le terminal et spécifie un modèle de terminal Samsung, une langue et un fournisseur de services mobiles pour une nouvelle règle relative au micrologiciel de terminal Samsung.
6. BlackBerry UEM Core se connecte au serveur E-FOTA via BlackBerry Infrastructure au moyen d'une connexion TLS et envoie les critères spécifiés au serveur E-FOTA.
7. Le serveur E-FOTA vérifie les critères et renvoie les informations du micrologiciel via BlackBerry Infrastructure à BlackBerry UEM Core.
8. L'administrateur enregistre le nouveau profil d'exigences SR du terminal.
9. BlackBerry UEM Core se connecte au serveur E-FOTA via BlackBerry Infrastructure au moyen d'une connexion TLS et envoie le profil au Cloud Samsung.
10. L'administrateur attribue le profil d'exigences SR du terminal à un ou plusieurs utilisateurs.
11. BlackBerry UEM envoie le profil à BlackBerry UEM Client sur le terminal Samsung de l'utilisateur.
12. Le terminal Samsung s'enregistre auprès du serveur E-FOTA.
13. Si une mise à jour du micrologiciel est disponible et répond aux paramètres spécifiés dans le profil d'exigences SR du terminal, le serveur E-FOTA envoie la mise à jour au terminal.

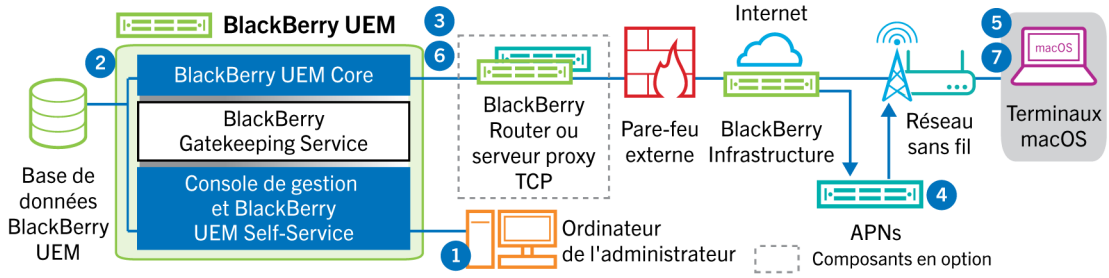
Flux de données : réception de mises à jour de configuration sur un terminal iOS



1. Sur la console de gestion, une action déclenche la mise à jour de configuration d'un terminal iOS. Par exemple, vous pouvez mettre à jour la stratégie informatique ou attribuer un nouveau profil ou une nouvelle application au compte d'utilisateur.
2. Les mises à jour sont appliquées dans BlackBerry UEM et les objets qui doivent être partagés avec le terminal sont identifiés.
3. BlackBerry UEM Core effectue les opérations suivantes :
   a. Il contacte BlackBerry Infrastructure, par le biais de BlackBerry Router ou du serveur proxy TCP, s'il est installé, ainsi que le pare-feu externe sur le port 3101.
   b. Il envoie une demande au service APNs via BlackBerry Infrastructure pour notifier le terminal qu'une mise à jour est en attente.
4. Le service APNs envoie une notification au démon MDM natif du terminal iOS pour contacter BlackBerry UEM Core.
5. Lorsque le démon MDM natif du terminal iOS reçoit la notification, il contacte BlackBerry UEM Core, sur le port 3101 du pare-feu externe, en passant par BlackBerry Router ou par le serveur proxy TCP, s'il est installé, afin de récupérer les actions en attente.
6. BlackBerry UEM Core répond en commençant par l'action à priorité la plus élevée. Les actions concernant le terminal (telles que Supprimer les données du terminal et Verrouiller le terminal) sont prioritaires. BlackBerry UEM Core n'envoie qu'une seule commande à la fois. Si nécessaire, des informations supplémentaires sont incluses dans la réponse. Si aucune action ou commande n'est en attente pour le terminal, BlackBerry UEM Core lui répond avec une commande d'inactivité.
7. Le démon MDM natif du terminal iOS effectue les opérations suivantes :
   a. Il examine la réponse de BlackBerry UEM Core, planifie la commande à traiter et attend l'exécution de celle-ci.
   b. Il envoie une réponse à BlackBerry UEM Core pour mettre à jour l'état de la commande. L'état indique si la commande a bien été exécutée et affiche un message d'erreur en cas d'échec.

   Les étapes 6 et 7 sont répétées jusqu'à ce qu'il ne reste aucune action ou commande en attente sur le terminal.

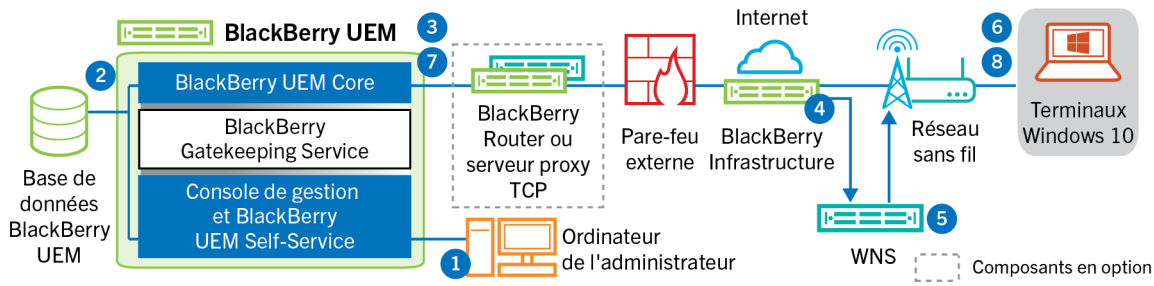
Flux de données : réception de mises à jour de configuration sur un terminal macOS



1. Sur la console de gestion, une action déclenche la mise à jour de configuration d'un terminal macOS. Par exemple, vous pouvez mettre à jour la stratégie informatique ou attribuer un nouveau profil ou une nouvelle application au compte d'utilisateur.
2. Les mises à jour sont appliquées dans BlackBerry UEM et les objets qui doivent être partagés avec le terminal sont identifiés.
3. BlackBerry UEM Core effectue les opérations suivantes :
   a. Il contacte BlackBerry Infrastructure, par le biais de BlackBerry Router ou du serveur proxy TCP, s'il est installé, ainsi que le pare-feu externe sur le port 3101.
   b. Il envoie une demande au service APNs via BlackBerry Infrastructure pour notifier le terminal qu'une mise à jour est en attente.
4. Le service APNs envoie une notification au terminal pour contacter BlackBerry UEM Core.
5. Lorsque le terminal reçoit la notification, il contacte BlackBerry UEM Core, sur le port 3101 du pare-feu externe, en passant par BlackBerry Router ou par le serveur proxy TCP, s'il est installé, afin de récupérer les actions en attente.
6. Lorsqu'une mise à jour est en attente pour le terminal, BlackBerry UEM Core répond en commençant par l'action à priorité la plus élevée. Les actions concernant le terminal (telles que Supprimer les données du terminal et Verrouiller le terminal) sont prioritaires. Si nécessaire, des informations supplémentaires sont incluses dans la réponse. Si aucune action ou commande n'est en attente pour le terminal, BlackBerry UEM Core lui répond avec un message vide.
7. Le terminal effectue les opérations suivantes :
   a. Il examine la réponse de BlackBerry UEM Core, planifie la commande à traiter et attend l'exécution de celle-ci.
   b. Il envoie une réponse à BlackBerry UEM Core pour mettre à jour l'état de la commande. L'état indique si la commande a bien été exécutée et affiche un message d'erreur en cas d'échec.

   Les étapes 6 et 7 sont répétées jusqu'à ce qu'il ne reste aucune action ou commande en attente sur le terminal.

Flux de données : réception de mises à jour de configuration sur un terminal Windows 10



1. Sur la console de gestion, une action déclenche la mise à jour de configuration d'un terminal Windows 10. Par exemple, vous pouvez mettre à jour la stratégie informatique ou attribuer un nouveau profil ou une nouvelle application au compte d'utilisateur.
2. Les mises à jour sont appliquées dans BlackBerry UEM et les objets qui doivent être partagés avec le terminal sont identifiés.
3. BlackBerry UEM Core contacte BlackBerry Infrastructure, par le biais de BlackBerry Router ou du serveur proxy TCP, s'il est installé, ainsi que le pare-feu externe sur le port 3101.
4. BlackBerry Infrastructure utilise le service WNS pour notifier le terminal qu'une mise à jour est en attente.
5. Le service WNS envoie une notification au terminal pour contacter BlackBerry UEM Core.
6. Lorsque le terminal reçoit la notification, il contacte BlackBerry UEM Core, sur le port 3101 du pare-feu externe, en passant par BlackBerry Router ou par le serveur proxy TCP, s'il est installé, afin de récupérer les actions en attente.
7. Lorsqu'une mise à jour est en attente pour le terminal, BlackBerry UEM Core répond en commençant par l'action à priorité la plus élevée. Les actions concernant le terminal (telles que Supprimer les données du terminal et Verrouiller le terminal) sont prioritaires. Si nécessaire, des informations supplémentaires sont incluses dans la réponse. Si aucune action ou commande n'est en attente pour le terminal, BlackBerry UEM Core lui répond avec un message vide.
8. Le terminal examine la réponse, planifie la commande à traiter et attend l'exécution de celle-ci. Le terminal envoie une réponse à BlackBerry UEM Core pour mettre à jour le statut de la commande. L'état indique si la commande a bien été exécutée et affiche un message d'erreur en cas d'échec.

   Les étapes 7 et 8 sont répétées jusqu'à ce qu'il ne reste aucune action ou commande en attente sur le terminal.

Informations juridiques

Cette documentation, y compris la documentation incluse pour référence telle que celle fournie ou mise à disposition sur le site Web BlackBerry, est fournie ou mise à disposition « EN L'ÉTAT » et « TELLE QUELLE », sans condition ni garantie en tout genre de la part de BlackBerry Limited et de ses filiales (« BlackBerry »), et BlackBerry décline toute responsabilité en cas d'erreur ou d'oubli typographique, technique ou autre inexactitude contenue dans ce document. Pour des raisons de protection des informations confidentielles et/ou des secrets commerciaux de BlackBerry, cette documentation peut décrire certains aspects de la technologie BlackBerry en termes généraux. BlackBerry se réserve le droit de modifier périodiquement les informations contenues dans cette documentation. Cependant, BlackBerry ne s'engage en aucune manière à vous communiquer les modifications, mises à jour, améliorations ou autres ajouts apportés à cette documentation.

La présente documentation peut contenir des références à des sources d'informations, du matériel ou des logiciels, des produits ou des services tiers, y compris des composants et du contenu tel que du contenu protégé par copyright et/ou des sites Web tiers (ci-après dénommés collectivement « Produits et Services tiers »). BlackBerry ne contrôle pas et décline toute responsabilité concernant les Produits et Services tiers, y compris, sans s'y limiter, le contenu, la précision, le respect du code de la propriété intellectuelle, la compatibilité, les performances, la fiabilité, la légalité, l'éthique, les liens ou tout autre aspect desdits Produits et Services tiers. La présence d'une référence aux Produits et Services tiers dans cette documentation ne suppose aucunement que BlackBerry se porte garant des Produits et Services tiers ou de la tierce partie concernée.

SAUF DANS LA MESURE SPÉCIFIQUEMENT INTERDITE PAR LES LOIS EN VIGUEUR DANS VOTRE JURIDICTION, TOUTES LES CONDITIONS, GARANTIES OU REPRÉSENTATIONS DE TOUTE NATURE, EXPRESSES OU TACITES, NOTAMMENT (SANS LIMITATIONS) LES CONDITIONS, GARANTIES OU REPRÉSENTATIONS DE DURABILITÉ, D'ADÉQUATION À UNE UTILISATION OU À UN BUT PARTICULIER, DE COMMERCIALISATION, DE QUALITÉ MARCHANDE, DE NON-INFRACTION, DE SATISFACTION DE LA QUALITÉ OU DE TITRE, OU RÉSULTANT D'UNE LOI, D'UNE COUTUME, D'UNE PRATIQUE OU D'UN USAGE COMMERCIAL, OU EN RELATION AVEC LA DOCUMENTATION OU SON UTILISATION, OU LA PERFORMANCE OU NON-PERFORMANCE DES LOGICIELS, DU MATÉRIEL, DES SERVICE OU DES PRODUITS ET SERVICES TIERS CITÉS, SONT EXCLUES. VOUS POUVEZ JOUIR D'AUTRES DROITS QUI VARIENT SELON L'ÉTAT OU LA PROVINCE. CERTAINES JURIDICTIONS N'AUTORISENT PAS L'EXCLUSION OU LA LIMITATION DES GARANTIES ET CONDITIONS IMPLICITES. DANS LA MESURE AUTORISÉE PAR LES LOIS, TOUTE GARANTIE OU CONDITION IMPLICITE RELATIVE À LA DOCUMENTATION, DANS LA MESURE OÙ ELLES NE PEUVENT PAS ÊTRE EXCLUES EN VERTU DES CLAUSES PRÉCÉDENTES, MAIS PEUVENT ÊTRE LIMITÉES, SONT PAR LES PRÉSENTES LIMITÉES À QUATRE-VINGT-DIX (90) JOURS À COMPTER DE LA DATE DE LA PREMIÈRE ACQUISITION DE LA DOCUMENTATION OU DE L'ARTICLE QUI FAIT L'OBJET D'UNE RÉCLAMATION.

DANS LA MESURE MAXIMALE PERMISE PAR LES LOIS EN VIGUEUR DANS VOTRE JURIDICTION, EN AUCUN CAS BLACKBERRY N'EST RESPONSABLE DES DOMMAGES LIÉS À LA PRÉSENTE DOCUMENTATION OU À SON UTILISATION, OU À LA PERFORMANCE OU NON-PERFORMANCE DES LOGICIELS, DU MATÉRIEL, DES SERVICES OU DES PRODUITS ET SERVICES TIERS MENTIONNÉS DANS LES PRÉSENTES, ET NOTAMMENT, SANS S'Y LIMITER, DES DOMMAGES DIRECTS, EXEMPLAIRES, ACCIDENTELS, INDIRECTS, SPÉCIAUX, PUNITIFS OU AGGRAVÉS, DES DOMMAGES LIÉS À UNE PERTE DE PROFITS OU DE REVENUS, UN MANQUE À GAGNER, UNE INTERRUPTION D'ACTIVITÉ, UNE PERTE D'INFORMATIONS COMMERCIALES, UNE PERTE D'OPPORTUNITÉS COMMERCIALES, LA CORRUPTION OU LA PERTE DE DONNÉES, LE NON-ENVOI OU LA NON-RÉCEPTION DE DONNÉES, DES PROBLÈMES LIÉS À DES APPLICATIONS UTILISÉES AVEC DES PRODUITS OU SERVICES BLACKBERRY, DES COUTS D'INDISPONIBILITÉ, LA PERTE D'UTILISATION DES PRODUITS OU SERVICES BLACKBERRY EN TOUT OU EN PARTIE, OU DE TOUT SERVICE DE COMMUNICATION, DU COUT DE BIENS DE

SUBSTITUTION, DES FRAIS DE GARANTIE, DES ÉQUIPEMENTS OU SERVICES, DES COUTS DE CAPITAL, OU AUTRES PERTES FINANCIÈRES SIMILAIRES, PRÉVISIBLES OU NON, MÊME SI BLACKBERRY A ÉTÉ INFORMÉ DE LA POSSIBILITÉ DE TELS DOMMAGES.

DANS LA MESURE MAXIMALE PERMISE PAR LES LOIS APPLICABLES DANS VOTRE JURIDICTION, BLACKBERRY N'EST NULLEMENT TENU PAR DES OBLIGATIONS, DEVOIRS OU RESPONSABILITÉS, CONTRACTUELS, DÉLICTUELS OU AUTRES, PAS MÊME PAR UNE RESPONSABILITÉ EN CAS DE NÉGLIGENCE OU RESPONSABILITÉ STRICTE ET NE VOUS EST REDEVABLE EN RIEN.

LES LIMITATIONS, EXCLUSIONS ET CLAUSES DE NON-RESPONSABILITÉ CONTENUES DANS LES PRÉSENTES S'APPLIQUENT : (A) INDÉPENDAMMENT DE LA NATURE DE LA CAUSE D'ACTION, DE DEMANDE OU D'ACTION ENTREPRISE PAR VOUS, NOTAMMENT, SANS S'Y LIMITER, POUR RUPTURE DE CONTRAT, NÉGLIGENCE, FAUTE, RESPONSABILITÉ STRICTE OU TOUTE AUTRE THÉORIE LÉGALE, ET RESTENT APPLICABLES EN CAS DE RUPTURES SUBSTANTIELLES OU DE MANQUEMENT AU BUT ESSENTIEL DU PRÉSENT CONTRAT OU DE TOUT RECOURS ENVISAGEABLE PAR LES PRÉSENTES ; ET (B) À BLACKBERRY ET À SES FILIALES, LEURS AYANTS DROIT, REPRÉSENTANTS, AGENTS, FOURNISSEURS (NOTAMMENT LES FOURNISSEURS DE SERVICES), REVENDEURS AGRÉÉS BLACKBERRY (NOTAMMENT LES FOURNISSEURS DE SERVICES) ET LEURS DIRECTEURS, EMPLOYÉS ET SOUS-TRAITANTS RESPECTIFS.

OUTRE LES LIMITATIONS ET EXCLUSIONS SUSMENTIONNÉES, EN AUCUN CAS, LES DIRECTEURS, EMPLOYÉS, AGENTS, REVENDEURS, FOURNISSEURS, SOUS-TRAITANTS DE BLACKBERRY OU DE SES FILIALES N'ONT UNE RESPONSABILITÉ CONSÉCUTIVE OU RELATIVE À LA PRÉSENTE DOCUMENTATION.

Avant de vous abonner, d'installer ou d'utiliser des Produits et Services tiers, il est de votre responsabilité de vérifier que votre fournisseur de services prend en charge toutes les fonctionnalités. Certains fournisseurs de services peuvent ne pas proposer de fonctionnalités de navigation Internet avec un abonnement à BlackBerry® Internet Service. Vérifiez auprès de votre fournisseur de services la disponibilité, les accords d'itinérance, les plans de service et les fonctionnalités. L'installation ou l'utilisation de Produits et Services tiers avec des produits et services BlackBerry peuvent nécessiter un ou plusieurs brevets, marques commerciales, licences de copyright ou autres licences à des fins de protection des droits d'autrui. Vous êtes seul responsable de votre décision d'utiliser ou non les Produits et Services tiers et si cela nécessite l'obtention de licences tierces. Si de telles licences sont requises, vous êtes seul responsable de leur acquisition. Vous ne devez pas installer ou utiliser de Produits et Services tiers avant d'avoir acquis la totalité des licences nécessaires. Les Produits et Services tiers fournis avec les produits et services BlackBerry vous sont fournis à toutes fins utiles « EN L'ÉTAT » sans conditions, garanties ou représentations expresses ou tacites d'aucune sorte par BlackBerry, et BlackBerry n'engage aucune responsabilité sur les Produits et Services tiers à cet égard. L'utilisation que vous faites des Produits et Services tiers est régie par et dépendante de votre acceptation des termes des licences et autres accords distincts applicables à cet égard avec d'autres parties, sauf dans la limite couverte expressément par une licence ou autre accord conclu avec BlackBerry.

Les conditions d'utilisation de tout produit ou service BlackBerry sont stipulées dans une licence ou autre accord distinct conclu avec BlackBerry à cet égard. LE CONTENU DE CETTE DOCUMENTATION N'EST PAS DESTINÉ À REMPLACER LES ACCORDS OU GARANTIES EXPRÈS ET ÉCRITS FOURNIS PAR BLACKBERRY POUR UNE PARTIE DES PRODUITS OU SERVICES BLACKBERRY AUTRES QUE CETTE DOCUMENTATION.

BlackBerry Enterprise Software incorpore des éléments logiciels tiers. La licence et les informations de copyright associées à ce logiciel sont disponibles à l'adresse http://worldwide.blackberry.com/legal/thirdpartysoftware.jsp.

BlackBerry Limited
2200 University Avenue Est
Waterloo, Ontario
Canada N2K 0A7

BlackBerry UK Limited
Ground Floor, The Pearce Building, West Street,

Maidenhead, Berkshire SL6 1RL
Royaume-Uni

Publié au Canada