



BlackBerry UEM

Architecture et flux de données

12.14

Table des matières

| | |
|--|-----------|
| Architecture et flux de données de BlackBerry UEM..... | 5 |
| Architecture : solution BlackBerry UEM..... | 5 |
| Composants BlackBerry UEM..... | 8 |
| Installation distribuée de BlackBerry UEM..... | 11 |
| Déploiement régional de BlackBerry UEM..... | 15 |
| Activation des terminaux et des applications BlackBerry Dynamics..... | 19 |
| 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..... | 19 |
| Flux de données : activation d'un terminal Android Enterprise Travail et Personnel - Contrôle total à l'aide d'un compte géré Google Play..... | 21 |
| Flux de données : activation d'un terminal Android Enterprise Espace Travail uniquement à l'aide d'un compte géré Google Play..... | 22 |
| Flux de données : activation d'un terminal Android Enterprise Travail et Personnel - Confidentialité des données de l'utilisateur dans un domaine Google..... | 24 |
| Flux de données : activation d'un terminal Android Enterprise Travail et Personnel - Contrôle total dans un domaine Google..... | 25 |
| Flux de données : activation d'un terminal Android Enterprise Espace Travail uniquement dans un domaine Google..... | 27 |
| Flux de données : activation d'un terminal pour utiliser Knox Workspace..... | 29 |
| Flux de données : activation d'un terminal iOS..... | 30 |
| Flux de données : activation d'un terminal macOS..... | 33 |
| Flux de données : activation d'un terminal Windows 10..... | 34 |
| Flux de données : activation d'un terminal BlackBerry 10..... | 36 |
| Flux de données : première activation d'une application BlackBerry Dynamics sur un terminal..... | 37 |
| Flux de données : activation d'une application BlackBerry Dynamics lorsqu'une application est déjà activée sur le terminal..... | 39 |
| Envoi et réception de données professionnelles | 40 |
| Envoi et réception des données professionnelles à l'aide de BlackBerry Infrastructure..... | 41 |
| Flux de données : envoi et réception de données professionnelles depuis une application BlackBerry Dynamics via BlackBerry Dynamics NOC..... | 42 |
| Flux de données : envoi et réception de données professionnelles depuis une application BlackBerry Dynamics via BlackBerry Infrastructure..... | 43 |
| Flux de données : envoi et réception de données professionnelles depuis une application BlackBerry Dynamics à l'aide de BlackBerry Dynamics Direct Connect..... | 43 |
| Flux de données : accès à un serveur d'applications ou de contenu avec BlackBerry Secure Connect Plus..... | 44 |

| | |
|---|----|
| 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..... | 45 |
| Flux de données : envoi d'un e-mail depuis un terminal iOS à l'aide de BlackBerry Secure Gateway... | 46 |
| Flux de données : réception d'un e-mail sur un terminal iOS utilisant BlackBerry Secure Gateway.... | 47 |
| Flux de données : accès à un serveur d'applications ou de contenu à partir d'un terminal BlackBerry 10..... | 47 |
| Flux de données : envoi d'un e-mail depuis un terminal BlackBerry 10..... | 48 |
| Flux de données : réception d'un e-mail sur un terminal BlackBerry 10..... | 48 |
| Flux de données : réception des mises à jour de transmission de données d'entreprise sur un terminal BlackBerry 10..... | 49 |
| Envoi et réception des données professionnelles à l'aide d'un réseau VPN ou d'un réseau Wi-Fi professionnel..... | 51 |
| Flux de données : envoi d'un e-mail depuis un terminal à l'aide d'un VPN ou d'un réseau Wi-Fi professionnel..... | 52 |
| Flux de données : réception d'un e-mail sur un terminal à l'aide d'un VPN ou d'un réseau Wi-Fi professionnel..... | 52 |
| Flux de données : accès à un serveur d'applications ou de contenu avec un VPN ou un réseau Wi-Fi professionnel..... | 53 |

Réception des mises à jour de configuration des terminaux..... 54

| | |
|---|----|
| Flux de données : réception de mises à jour de configuration sur un terminal Android..... | 55 |
| Flux de données : mise à jour du micrologiciel sur les terminaux Samsung Knox..... | 56 |
| Flux de données : réception de mises à jour de configuration sur un terminal iOS..... | 57 |
| Flux de données : réception de mises à jour de configuration sur un terminal macOS..... | 58 |
| Flux de données : réception de mises à jour de configuration sur un terminal Windows 10..... | 58 |
| Flux de données : réception de mises à jour de configuration sur un terminal BlackBerry 10..... | 59 |

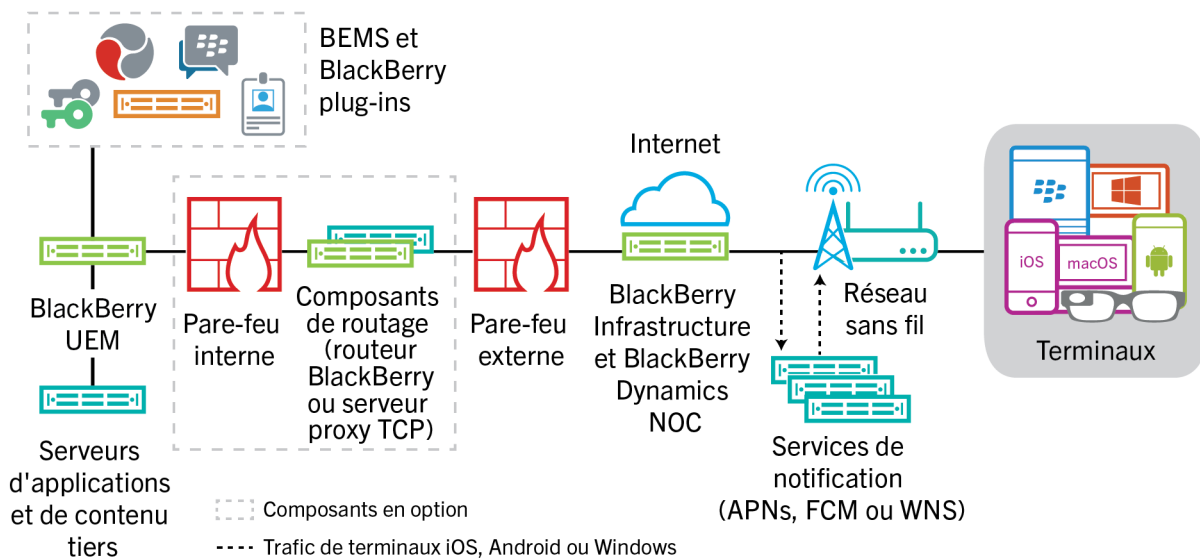
Informations juridiques..... 61

Architecture et flux de données de BlackBerry UEM

BlackBerry UEM est une solution EMM multiplateforme de BlackBerry 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, Windows 10 et BlackBerry 10 pour votre organisation.

L'architecture BlackBerry UEM a été conçue pour vous aider à gérer les terminaux mobiles de votre entreprise 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



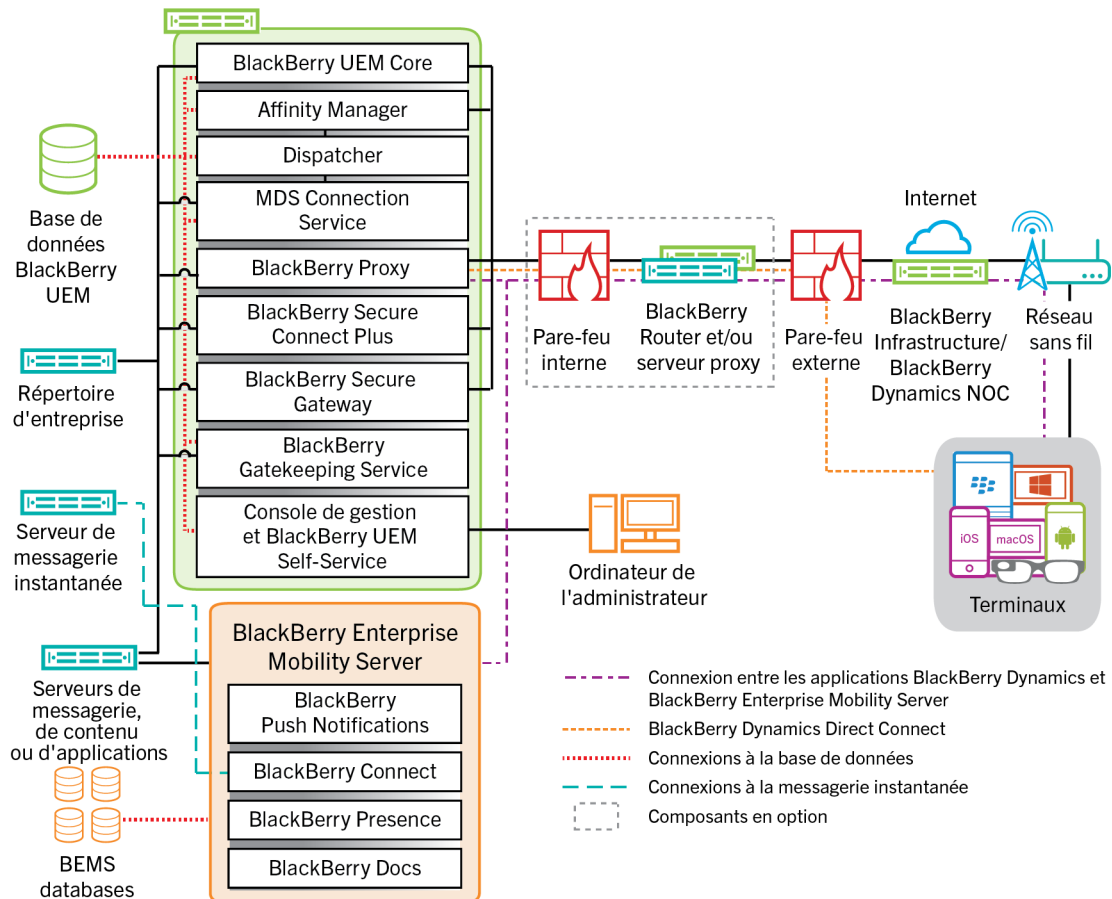
| Composant | Description |
|----------------|---|
| BlackBerry UEM | BlackBerry UEM est une solution unifiée de gestion des points de terminaison qui fournit une gestion multiplateforme complète des terminaux, des applications et du contenu, en offrant une sécurité et une connectivité intégrées. |

| Composant | Description |
|---------------------------|---|
| BlackBerry Infrastructure | <p>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.</p> <p>Pour les organisations utilisant BlackBerry UEM, BlackBerry Infrastructure enregistre les informations utilisateur pour l'activation du terminal, valide les informations de licence pour BlackBerry UEM et fournit un chemin d'accès approuvé entre l'organisation et chacun des utilisateurs en se basant sur une solide authentification cryptographique mutuelle. En raison du cryptage de bout en bout qui protège les données transmises entre le terminal et BlackBerry UEM, BlackBerry UEM maintient une connexion constante à BlackBerry Infrastructure. Par conséquent, 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 BlackBerry 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.</p> |
| BlackBerry Dynamics NOC | BlackBerry Dynamics NOC est un centre d'opérations réseau qui fournit des communications sécurisées entre les applications BlackBerry Dynamics des terminaux et BlackBerry UEM, et BlackBerry Enterprise Mobility Server. |
| Terminaux | BlackBerry UEM prend en charge les terminaux iOS, macOS, Android, Windows 10 et BlackBerry 10. |
| Services de notification | <p>BlackBerry UEM envoie les notifications aux terminaux BlackBerry 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 :</p> <ul style="list-style-type: none"> • 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. |

| Composant | Description |
|---|--|
| Composants de routage | <p>Par défaut, BlackBerry 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 la stratégie de sécurité de votre entreprise empêche les systèmes internes de se connecter directement à Internet, vous pouvez utiliser BlackBerry Router ou un serveur proxy.</p> <p>BlackBerry Router fait office de serveur proxy pour les connexions BlackBerry Infrastructure entre BlackBerry UEM et tous les terminaux. BlackBerry Router peut prendre en charge SOCKS v5 sans aucune authentification.</p> <p>Si votre organisation dispose déjà d'un serveur proxy TCP, ou si elle est contrainte d'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.</p> <p>BlackBerry UEM Core et BlackBerry Proxy prennent en charge l'utilisation d'un serveur proxy HTTP pour se connecter au BlackBerry Dynamics NOC .</p> |
| Serveurs d'applications et de contenu tiers | <p>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.</p> |
| Plug-ins BlackBerry et BEMS | <p>BlackBerry UEM fonctionne avec des produits d'entreprise BlackBerry complémentaires, tels que BlackBerry Enterprise Identity et BlackBerry 2FA pour vous permettre d'étendre les fonctionnalités UEM dans votre organisation.</p> <p>BlackBerry Enterprise Mobility Server fournit différents services permettant d'envoyer des données professionnelles vers et à partir des applications BlackBerry Dynamics.</p> |

Composants BlackBerry UEM

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.



Pour plus d'informations sur les ports utilisés pour les connexions entre les composants, reportez-vous à la section [Configuration des ports du contenu relatif à la planification](#).

| Nom du composant | Description |
|---------------------|--|
| BlackBerry UEM Core | <p>BlackBerry UEM Core est le composant central de l'architecture BlackBerry UEM. Il consiste en de nombreux sous-composants responsables des fonctions suivantes :</p> <ul style="list-style-type: none"> 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. |

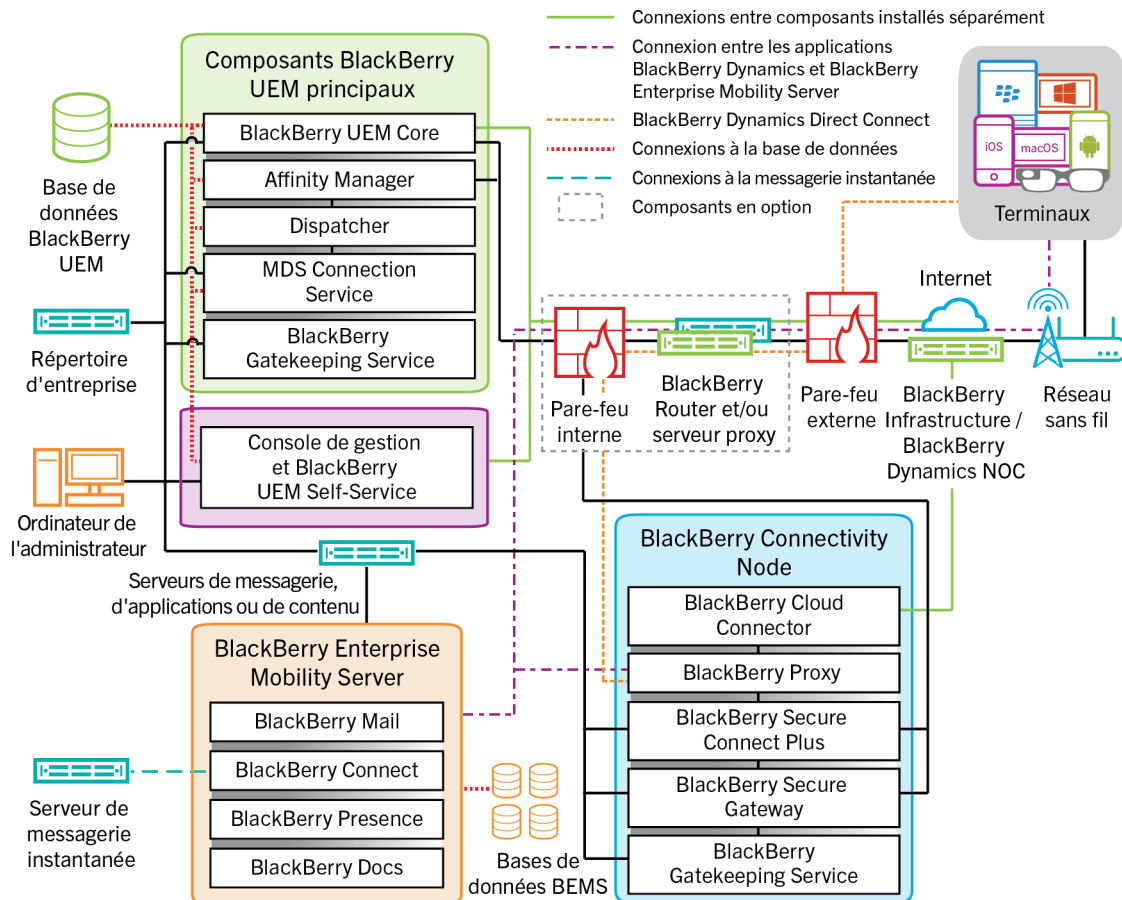
| Nom du composant | Description |
|---|--|
| Base de données BlackBerry UEM | La base de données BlackBerry UEM est une base de données relationnelle qui contient les informations des comptes d'utilisateur et les informations de configuration utilisées par BlackBerry UEM pour gérer les terminaux et les applications BlackBerry Dynamics. |
| BlackBerry MDS Connection Service | BlackBerry MDS Connection Service offre une connexion sécurisée entre les terminaux BlackBerry 10 et le réseau de votre organisation lorsque le terminal n'est pas connecté à votre réseau Wi-Fi professionnel ou via une connexion VPN. |
| BlackBerry Dispatcher | Le terminal BlackBerry Dispatcher procure une connectivité sécurisée utilisant IPPP aux terminaux BlackBerry 10. |
| BlackBerry Affinity Manager | BlackBerry Affinity Manager maintient une connexion SRP active entre les terminaux BlackBerry 10 et BlackBerry Infrastructure lorsque les terminaux n'utilisent pas BlackBerry Secure Connect Plus. |
| BlackBerry Proxy | 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 | 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 BlackBerry 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 BlackBerry UEM. 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 BlackBerry UEM. |
| Console de gestion et BlackBerry UEM Self-Service | <p>La console de gestion et BlackBerry UEM Self-Service fournissent une interface utilisateur basée sur le Web pour l'accès administrateur et utilisateur à BlackBerry UEM.</p> <p>La console de gestion vous permet de gérer les paramètres système, les utilisateurs, les terminaux et les applications.</p> <p>Les utilisateurs peuvent utiliser BlackBerry 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.</p> |
| BlackBerry Enterprise Mobility Server | BEMS consolide plusieurs services permettant d'échanger des données professionnelles avec les applications BlackBerry Dynamics : BlackBerry Push Notifications, BlackBerry Connect, BlackBerry Presence et BlackBerry Docs. |

| Nom du composant | Description |
|--|---|
| Bases de données BlackBerry Enterprise Mobility Server | Les bases de données BEMS stockent les informations relatives aux utilisateurs, aux stratégies et à la configuration. |
| BlackBerry Push Notifications | 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 | 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 | BlackBerry Presence fournit un état de présence en temps réel aux applications BlackBerry Dynamics. |
| BlackBerry Docs | 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. |
| BlackBerry Router et/ou serveurs proxy | <p>Par défaut, BlackBerry UEM se connecte directement à BlackBerry Infrastructure via les ports 3101 et 443. Si la stratégie de sécurité de votre entreprise empêche 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.</p> <p>BlackBerry UEM Core et BlackBerry Proxy prennent en charge un serveur proxy HTTP tiers pour la connexion à BlackBerry Dynamics NOC.</p> |
| BlackBerry Infrastructure et BlackBerry Dynamics NOC | <p>BlackBerry Infrastructure enregistre les informations utilisateur pour l'activation du terminal, valide les informations de licence pour BlackBerry UEM et fournit un chemin d'accès approuvé entre l'organisation et chaque utilisateur en se basant sur une solide authentification cryptographique mutuelle.</p> <p>BlackBerry Dynamics NOC est un NOC distinct qui permet des communications sécurisées entre les applications BlackBerry Dynamics installées sur les terminaux et BlackBerry UEM Core, BlackBerry Proxy et BlackBerry Enterprise Mobility Server.</p> |

Installation distribuée 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 BlackBerry UEM principaux.

Pour plus d'informations sur l'architecture lorsque vous installez BlackBerry UEM sur plusieurs ordinateurs pour une haute disponibilité, consultez le [Guide de planification](#).



Pour plus d'informations sur les ports utilisés pour les connexions entre les composants, reportez-vous à la section [Configuration des ports du contenu relatif à la planification](#).

| Nom du composant | Description |
|--------------------------------------|---|
| Principaux composants BlackBerry UEM | Les principaux composants BlackBerry UEM comprennent BlackBerry UEM Core et tous les composants installés avec lui sur le même serveur. |

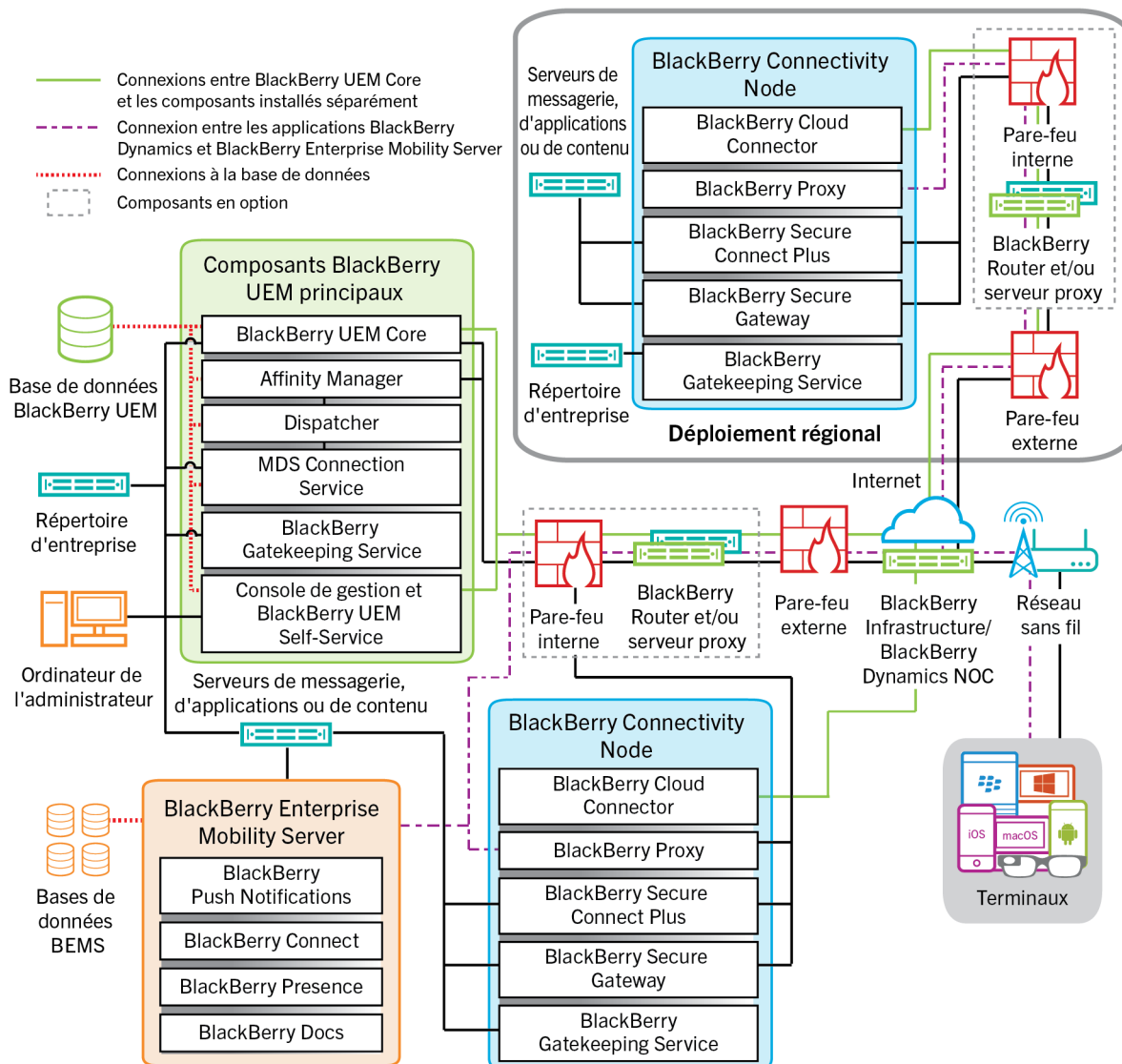
| Nom du composant | Description |
|--|--|
| BlackBerry UEM Core | <p>BlackBerry UEM Core est le composant central de l'architecture BlackBerry UEM. Il consiste en de nombreux sous-composants responsables des fonctions suivantes :</p> <ul style="list-style-type: none"> • Fonctions de journalisation, 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. |
| Base de données BlackBerry UEM | <p>La base de données BlackBerry UEM est une base de données relationnelle qui contient les informations des comptes d'utilisateur et les informations de configuration utilisées par BlackBerry UEM pour gérer les terminaux et les applications BlackBerry Dynamics.</p> |
| BlackBerry MDS Connection Service | <p>BlackBerry MDS Connection Service offre une connexion sécurisée entre les terminaux BlackBerry 10 et le réseau de votre organisation lorsque le terminal n'est pas connecté à votre réseau Wi-Fi professionnel ou via une connexion VPN.</p> |
| BlackBerry Dispatcher | <p>Le terminal BlackBerry Dispatcher procure une connectivité sécurisée utilisant IPPP aux terminaux BlackBerry 10.</p> |
| BlackBerry Affinity Manager | <p>BlackBerry Affinity Manager maintient une connexion SRP active entre les terminaux BlackBerry 10 et BlackBerry Infrastructure lorsque les terminaux n'utilisent pas BlackBerry Secure Connect Plus.</p> |
| BlackBerry Gatekeeping Service (principal) | <p>BlackBerry Gatekeeping Service envoie les commandes à Exchange ActiveSync pour ajouter les terminaux à une liste autorisée lorsque ceux-ci sont activés sur BlackBerry UEM. 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 BlackBerry UEM.</p> |
| Composants de l'interface utilisateur distante | <p>La console de gestion et BlackBerry UEM Self-Service peuvent être installés séparément des autres composants BlackBerry UEM. Si vous les installez séparément, une instance de BlackBerry Management Console Core est également installée.</p> |
| BlackBerry Management Console Core | <p>BlackBerry Management Console Core gère les sous-tâches spécifiques aux activités administratives.</p> |

| Nom du composant | Description |
|---|---|
| Console de gestion et BlackBerry UEM Self-Service | <p>La console de gestion et BlackBerry UEM Self-Service fournissent une interface utilisateur basée sur le Web pour l'accès administrateur et utilisateur à BlackBerry UEM. Elle peut être installée séparément des autres composants BlackBerry UEM.</p> <p>La console de gestion vous permet de gérer les paramètres système, les utilisateurs, les terminaux et les applications.</p> <p>Les utilisateurs peuvent accéder à BlackBerry 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.</p> |
| BlackBerry Connectivity Node | <p>BlackBerry Connectivity Node installe les instances des composants de connectivité des terminaux BlackBerry UEM dans le domaine de votre organisation sur un autre serveur que BlackBerry UEM Core. Chaque instance de BlackBerry Connectivity Node contient les composants suivants :</p> <ul style="list-style-type: none"> • BlackBerry Cloud Connector • BlackBerry Proxy • BlackBerry Secure Connect Plus • BlackBerry Secure Gateway • BlackBerry Gatekeeping Service |
| BlackBerry Cloud Connector | <p>BlackBerry Cloud Connector permet aux composants BlackBerry Connectivity Node de communiquer avec BlackBerry UEM Core. Toute communication entre BlackBerry Cloud Connector et BlackBerry UEM Core transite via BlackBerry Infrastructure.</p> |
| BlackBerry Proxy | <p>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.</p> |
| BlackBerry Secure Connect Plus | <p>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.</p> |
| BlackBerry Secure Gateway | <p>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 BlackBerry UEM.</p> |
| BlackBerry Gatekeeping Service (BlackBerry Connectivity Node) | <p>BlackBerry UEM peut utiliser les instances de BlackBerry Gatekeeping Service installées avec BlackBerry Connectivity Node pour gérer le contrôle d'accès de votre serveur de messagerie. Chaque instance doit être en mesure d'accéder au serveur de contrôle d'accès de votre organisation.</p> <p>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 BlackBerry UEM, vous pouvez désactiver BlackBerry Gatekeeping Service dans chaque instance de BlackBerry Connectivity Node.</p> |

| Nom du composant | Description |
|--|---|
| BlackBerry Enterprise Mobility Server | BEMS consolide plusieurs services permettant d'échanger des données professionnelles avec les applications BlackBerry Dynamics : BlackBerry Push Notifications, BlackBerry Connect, BlackBerry Presence et BlackBerry Docs. |
| Bases de données BlackBerry Enterprise Mobility Server | Les bases de données BEMS stockent les informations relatives aux utilisateurs, aux stratégies et à la configuration. |
| BlackBerry Infrastructure et BlackBerry Dynamics NOC | <p>BlackBerry Infrastructure enregistre les informations utilisateur pour l'activation du terminal, valide les informations de licence pour BlackBerry UEM et fournit un chemin d'accès approuvé entre l'organisation et chaque utilisateur en se basant sur une solide authentification cryptographique mutuelle.</p> <p>BlackBerry Dynamics NOC est un NOC distinct qui permet des communications sécurisées entre les applications BlackBerry Dynamics installées sur les terminaux et BlackBerry UEM Core, BlackBerry Proxy et BlackBerry Enterprise Mobility Server.</p> |

Déploiement régional de BlackBerry UEM

Ce schéma illustre la façon dont les composants BlackBerry UEM se connectent ensemble lorsqu'une ou plusieurs instances de BlackBerry Connectivity Node sont installées à un emplacement distinct. Vous pouvez utiliser des groupes de serveurs pour spécifier l'instance régionale de BlackBerry Connectivity Node à laquelle un terminal doit se connecter.



Pour plus d'informations sur les ports utilisés pour les connexions entre les composants, reportez-vous à la section [Configuration des ports du contenu relatif à la planification](#).

| Nom du composant | Description |
|--------------------------------------|---|
| Principaux composants BlackBerry UEM | Les principaux composants BlackBerry UEM comprennent BlackBerry UEM Core et tous les composants installés avec lui sur le même serveur. |

| Nom du composant | Description |
|---|---|
| BlackBerry UEM Core | <p>BlackBerry UEM Core est le composant central de l'architecture BlackBerry UEM. Il consiste en de nombreux sous-composants responsables des fonctions suivantes :</p> <ul style="list-style-type: none"> • 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. |
| Base de données BlackBerry UEM | <p>La base de données BlackBerry UEM est une base de données relationnelle qui contient les informations des comptes d'utilisateur et les informations de configuration utilisées par BlackBerry UEM pour gérer les terminaux et les applications BlackBerry Dynamics.</p> |
| BlackBerry MDS Connection Service | <p>BlackBerry MDS Connection Service offre une connexion sécurisée entre les terminaux BlackBerry 10 et le réseau de votre organisation lorsque le terminal n'est pas connecté à votre réseau Wi-Fi professionnel ou via une connexion VPN.</p> |
| BlackBerry Dispatcher | <p>Le terminal BlackBerry Dispatcher procure une connectivité sécurisée utilisant IPPP aux terminaux BlackBerry 10.</p> |
| BlackBerry Affinity Manager | <p>BlackBerry Affinity Manager maintient une connexion SRP active entre les terminaux BlackBerry 10 et BlackBerry Infrastructure lorsque les terminaux n'utilisent pas BlackBerry Secure Connect Plus.</p> |
| BlackBerry Gatekeeping Service (principal) | <p>BlackBerry Gatekeeping Service envoie les commandes à Exchange ActiveSync pour ajouter les terminaux à une liste autorisée lorsque ceux-ci sont activés sur BlackBerry UEM. 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 BlackBerry UEM.</p> |
| Console de gestion et BlackBerry UEM Self-Service | <p>La console de gestion et BlackBerry UEM Self-Service fournissent une interface utilisateur basée sur le Web pour l'accès administrateur et utilisateur à BlackBerry UEM. Elle peut être installée séparément des autres composants BlackBerry UEM.</p> <p>La console de gestion vous permet de gérer les paramètres système, les utilisateurs, les terminaux et les applications.</p> <p>Les utilisateurs peuvent accéder à BlackBerry 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.</p> |

| Nom du composant | Description |
|---|--|
| BlackBerry Connectivity Node | <p>BlackBerry Connectivity Node installe les instances des composants de connectivité des terminaux BlackBerry UEM dans le domaine de votre organisation sur un autre serveur que BlackBerry UEM Core. Chaque instance de BlackBerry Connectivity Node contient les composants suivants :</p> <ul style="list-style-type: none"> • BlackBerry Cloud Connector • BlackBerry Proxy • BlackBerry Secure Connect Plus • BlackBerry Secure Gateway • BlackBerry Gatekeeping Service <p>Si vous disposez de déploiements régionaux de BlackBerry Connectivity Node, vous devez configurer la connexion entre BlackBerry UEM Core et le groupe de serveurs contenant l'instance régionale de BlackBerry Connectivity Node.</p> |
| BlackBerry Cloud Connector | <p>BlackBerry Cloud Connector permet aux composants BlackBerry Connectivity Node de communiquer avec BlackBerry UEM Core. Toute communication entre BlackBerry Cloud Connector et BlackBerry UEM Core transite via BlackBerry Infrastructure.</p> |
| BlackBerry Proxy | <p>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.</p> |
| BlackBerry Secure Connect Plus | <p>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.</p> |
| BlackBerry Secure Gateway | <p>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 BlackBerry UEM.</p> |
| BlackBerry Gatekeeping Service (BlackBerry Connectivity Node) | <p>BlackBerry UEM peut utiliser les instances de BlackBerry Gatekeeping Service installées avec BlackBerry Connectivity Node pour gérer le contrôle d'accès de votre serveur de messagerie. Chaque instance doit être en mesure d'accéder au serveur de contrôle d'accès de votre organisation.</p> <p>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 BlackBerry UEM, vous pouvez désactiver BlackBerry Gatekeeping Service dans chaque instance de BlackBerry Connectivity Node.</p> |
| BlackBerry Enterprise Mobility Server | <p>BEMS consolide plusieurs services permettant d'échanger des données professionnelles avec les applications BlackBerry Dynamics, notamment : BlackBerry Push Notifications, BlackBerry Connect, BlackBerry Presence, et BlackBerry Docs.</p> |

| Nom du composant | Description |
|--|---|
| Bases de données BlackBerry Enterprise Mobility Server | Les bases de données BEMS stockent les informations relatives aux utilisateurs, aux stratégies et à la configuration. |
| BlackBerry Infrastructure et BlackBerry Dynamics NOC | <p>BlackBerry Infrastructure enregistre les informations utilisateur pour l'activation du terminal, valide les informations de licence pour BlackBerry UEM et fournit un chemin d'accès approuvé entre l'organisation et chaque utilisateur en se basant sur une solide authentification cryptographique mutuelle.</p> <p>BlackBerry Dynamics NOC est un NOC distinct qui permet des communications sécurisées entre les applications BlackBerry Dynamics installées sur les terminaux et BlackBerry UEM Core, BlackBerry Proxy et BlackBerry Enterprise Mobility Server.</p> |

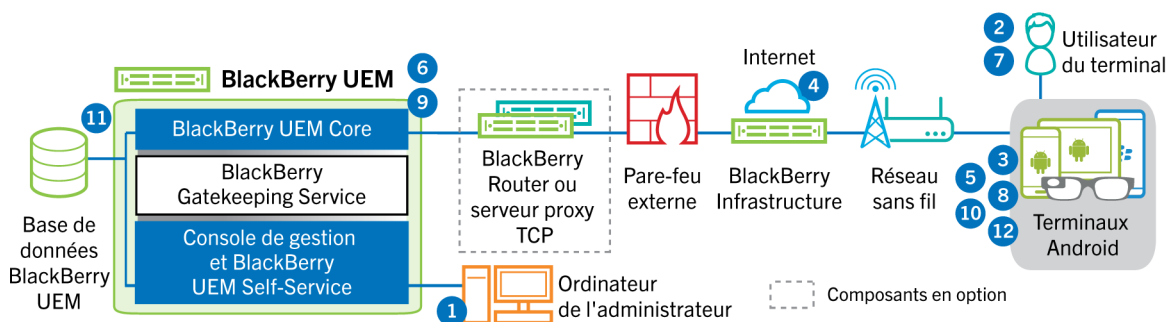
Activation des terminaux et des applications BlackBerry Dynamics

Lorsqu'un utilisateur active un terminal avec BlackBerry UEM, le terminal est associé à BlackBerry UEM pour pouvoir gérer les terminaux et permettre aux utilisateurs d'accéder aux données professionnelles sur leurs terminaux. 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, [reportez-vous à la section « Activation du terminal » dans le contenu relatif à l'administration.](#)

Selon le type de terminal et le type d'activation que vous spécifiez pour celui-ci, le terminal et BlackBerry UEM doivent suivre plusieurs étapes au cours du processus d'activation pour s'authentifier mutuellement, sécuriser un canal de communication et, si nécessaire, créer un espace Travail ou crypter le terminal avant que des données de configuration et des données professionnelles ne puissent être envoyées sur le terminal. Pour obtenir des instructions sur l'activation des terminaux, [reportez-vous à la section « Étapes à suivre pour activer des terminaux » dans le contenu relatif à l'administration.](#)

Les applications BlackBerry Dynamics permettent d'accéder aux ressources professionnelles du terminal. Une fois les applications BlackBerry Dynamics installées sur un terminal, elles doivent également être activées pour leur permettre d'accéder en toute sécurité à vos ressources professionnelles. Pour plus d'informations sur l'activation de BlackBerry Dynamics, [reportez-vous à la section « Générer des clés d'accès, des mots de passe d'activation ou des QR Codes pour les applications BlackBerry Dynamics » dans le contenu relatif à l'administration.](#)

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. Pour plus d'informations, [reportez-vous au contenu relatif à l'administration.](#)

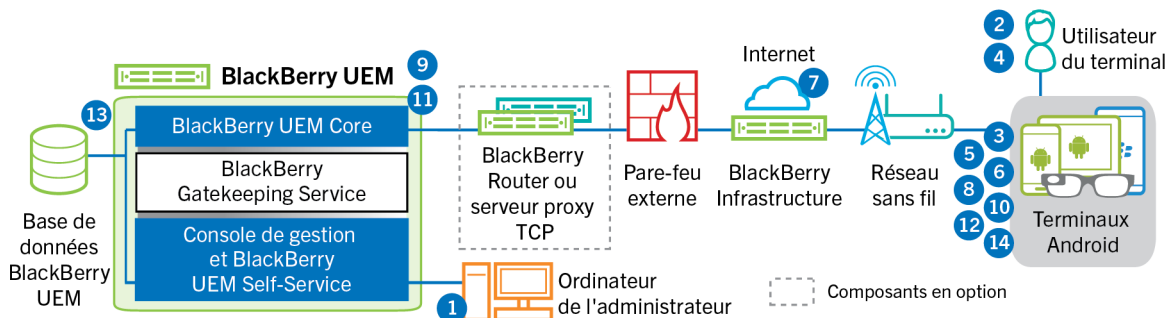
1. Vous effectuez les opérations suivantes :

- 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.
- Assurez-vous que le type d'activation « Travail et Personnel - Confidentialité des données de l'utilisateur » est attribué à l'utilisateur.
- 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 BlackBerry UEM Client et BlackBerry UEM.
 10. 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 géré Google Play



Ce flux de données s'applique lorsque vous autorisez BlackBerry UEM à gérer les comptes Google Play. Pour plus d'informations, reportez-vous au [contenu relatif à l'administration](#).

1. Vous effectuez les opérations suivantes :

- 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
- Assurez-vous que le type d'activation « Travail et Personnel - Contrôle total » est attribué à l'utilisateur.
- 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 :

- Il ouvre l'e-mail d'activation reçu sur son ordinateur ou un autre appareil
- Il appuie sept fois sur l'écran du terminal pour ouvrir un lecteur de QR Codes
- Il connecte le terminal à un réseau Wi-Fi
- Il scanne le QR Code dans l'email d'activation

5. Le terminal effectue les opérations suivantes :

- Il invite l'utilisateur à crypter le terminal et redémarre.
- 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 :

- Il se connecte à BlackBerry Infrastructure
- Il envoie une demande d'informations d'activation à BlackBerry Infrastructure

7. BlackBerry Infrastructure effectue les opérations suivantes :

- Il vérifie que l'utilisateur est valide et enregistré.
- Il récupère l'adresse du serveur BlackBerry UEM pour l'utilisateur
- 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 :

- Il détermine le type d'activation attribué au compte d'utilisateur.
- Il se connecte à Google et crée un utilisateur Google Play géré.
- 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 une 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

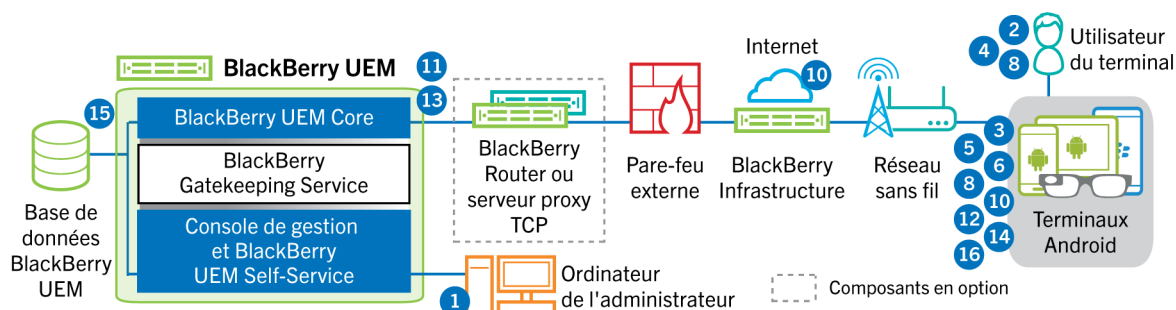
Une session TLS avec authentification mutuelle est établie entre le UEM Client et BlackBerry UEM.

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 géré Google Play



Ce flux de données s'applique lorsque vous autorisez BlackBerry UEM à gérer les comptes Google Play. Pour plus d'informations, reportez-vous au [contenu relatif à l'administration](#).

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 à partir de votre annuaire 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.

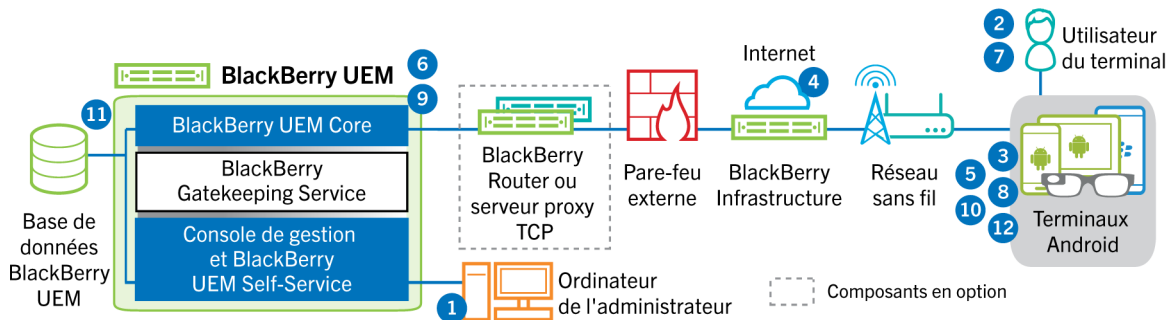
3. Le terminal redémarre et invite l'utilisateur à sélectionner un réseau Wi-Fi et à ajouter un compte.

4. L'utilisateur saisit `afw#blackberry` à la place de son nom d'utilisateur 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 e-mail et son mot de passe d'activation.
7. L'utilisateur saisit son adresse e-mail 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 BlackBerry UEM Client et BlackBerry UEM.
14. 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 G Suite. Pour plus d'informations, reportez-vous au [contenu relatif à l'administration](#).

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 annuaire d'entreprise. Lorsque vous spécifiez l'adresse e-mail, 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.

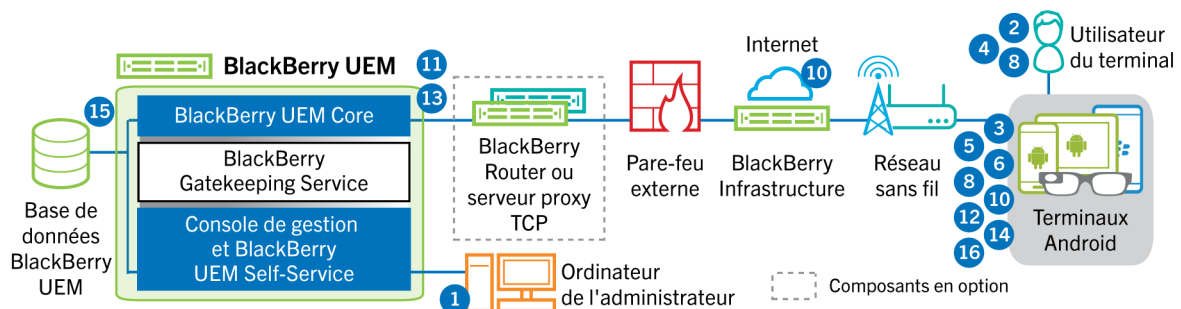
4. BlackBerry Infrastructure effectue les opérations suivantes :

- 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. Il invite l'utilisateur à entrer les informations du compte Google de l'utilisateur.
 - c. Il se connecte au domaine Google géré pour authentifier l'utilisateur.
 - d. Crée le profil professionnel sur le terminal
 - e. 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 BlackBerry UEM Client et BlackBerry UEM.
10. 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 G Suite. Pour plus d'informations, reportez-vous au [contenu relatif à l'administration](#).

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 annuaire d'entreprise. Lorsque vous spécifiez l'adresse e-mail, 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 e-mail et son mot de passe d'activation.
7. L'utilisateur saisit son adresse e-mail 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. Il invite l'utilisateur à entrer les informations du compte Google de l'utilisateur.

- c. Il se connecte au domaine Google pour authentifier l'utilisateur.
- d. 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.

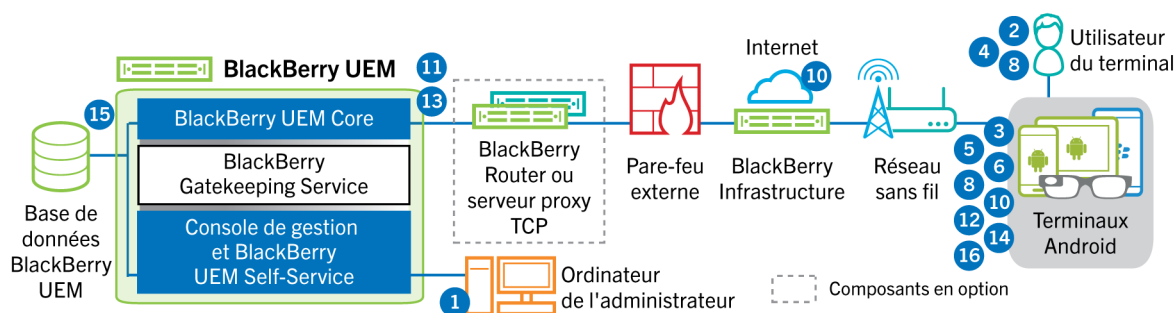
Une session TLS avec authentification mutuelle est établie entre BlackBerry UEM Client et BlackBerry UEM.

14. 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 G Suite. Pour plus d'informations, reportez-vous au [contenu relatif à l'administration](#).

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 annuaire d'entreprise. Lorsque vous spécifiez l'adresse e-mail, 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.

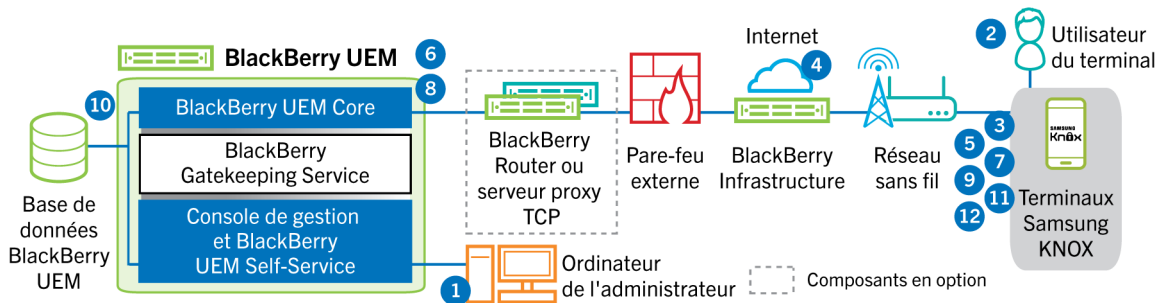
3. Le terminal redémarre et invite l'utilisateur à sélectionner un réseau Wi-Fi et à ajouter un compte.

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 e-mail et son mot de passe d'activation.
7. L'utilisateur saisit son adresse e-mail 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 BlackBerry UEM Client et BlackBerry UEM.
14. 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.

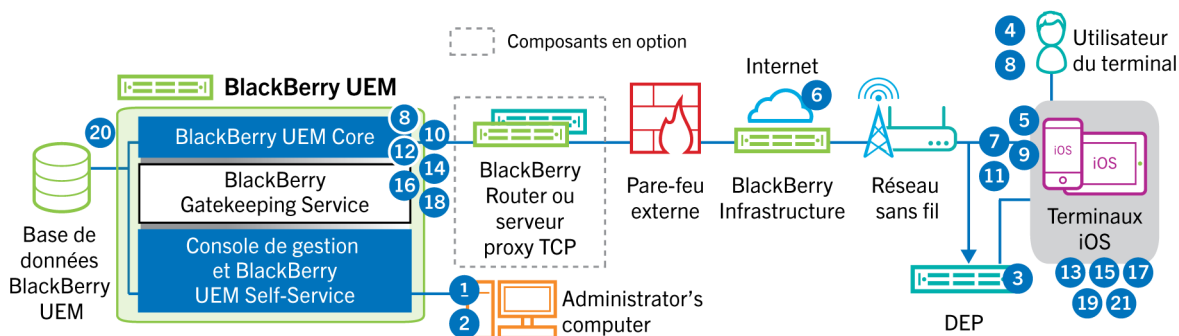
Une session TLS avec authentification mutuelle est établie entre BlackBerry UEM Client et BlackBerry UEM.

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



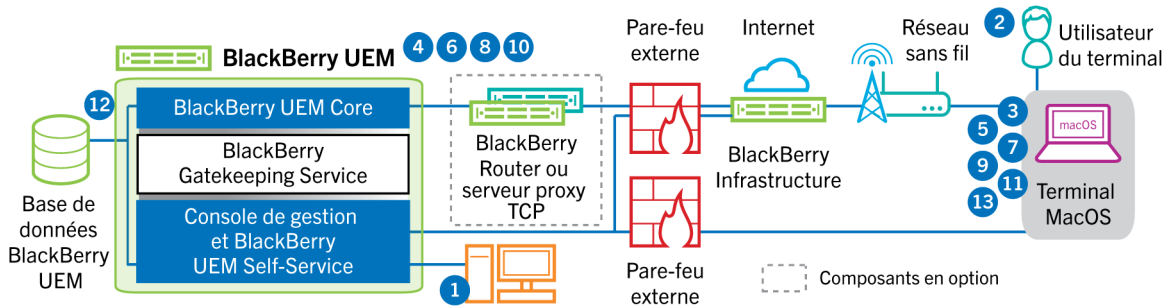
1. Si vous prévoyez d'utiliser le Programme d'inscription des appareils Apple, vous devez effectuer les opérations suivantes :
 - a. Assurez-vous que BlackBerry UEM est configuré pour se synchroniser avec DEP.
 - b. Enregistrez le terminal dans DEP et attribuez-le à un serveur MDM.
 - c. Attribuez une 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 chaîne 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.

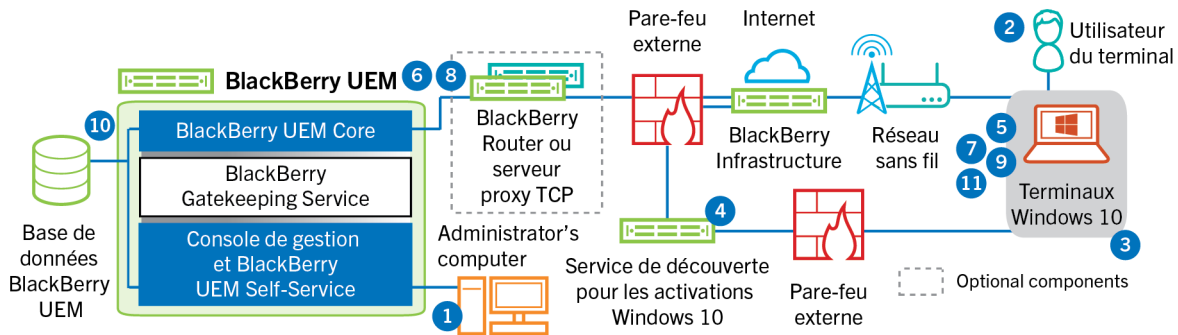
- 15.**Le démon MDM natif envoie à BlackBerry UEM une demande de certificat de l'autorité de certification, d'informations sur les capacités de l'autorité de certification et de certificat émis par le terminal.
- 16.**BlackBerry UEM envoie le certificat de l'autorité de certification, les informations 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 chaîne 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



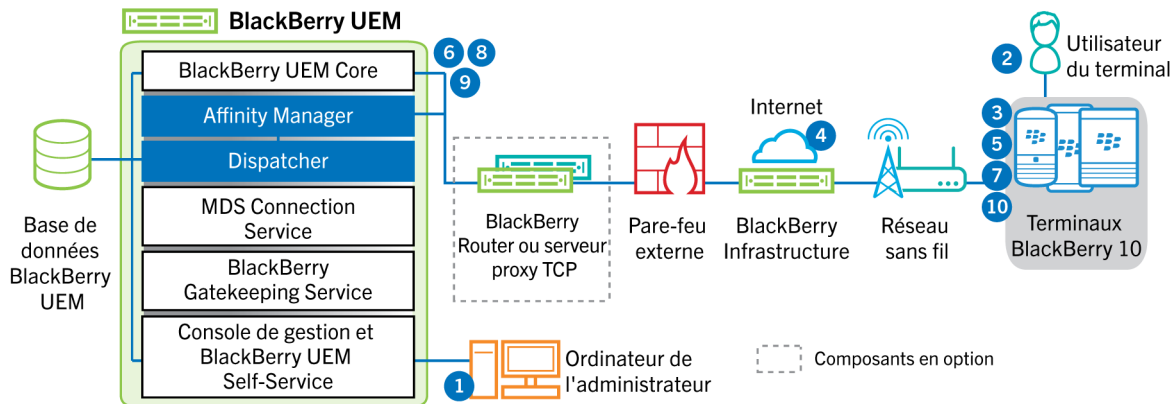
1. Vous effectuez les opérations suivantes :
 - a. Configurez le service de découverte pour simplifier les activations de Windows 10.
 - b. Ajoutez un utilisateur à BlackBerry UEM en tant que compte d'utilisateur local ou à l'aide des informations de compte récupérées depuis votre annuaire d'entreprise.
 - 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 : activation d'un terminal BlackBerry 10



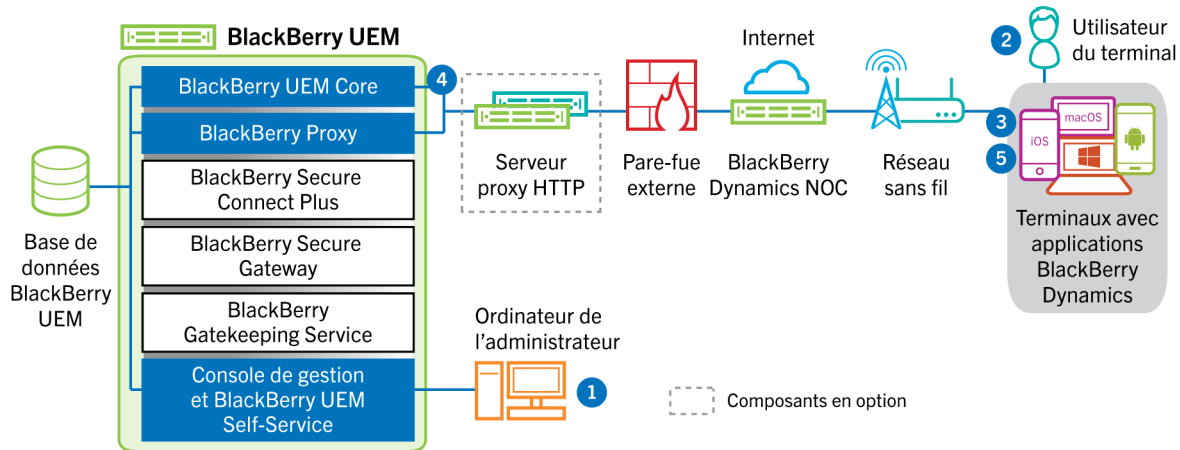
1. Vous effectuez les opérations suivantes :
 - a. Ajoutez un utilisateur à BlackBerry UEM en tant que compte d'utilisateur local ou à l'aide des informations de compte récupérées depuis votre annuaire d'entreprise.
 - b. Attribuer un profil d'activation à l'utilisateur
 - c. Utilisez l'une des options suivantes pour fournir les détails d'activation à l'utilisateur :
 - Générez automatiquement un mot de passe d'activation du terminal et 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.
2. L'utilisateur effectue les opérations suivantes :
 - a. Il saisit le nom d'utilisateur et le mot de passe d'activation sur le terminal
 - b. Pour une activation « Travail et Personnel - Régulé » ou « Espace Travail uniquement », il accepte l'avis d'entreprise qui précise les conditions générales auxquelles l'utilisateur doit souscrire
3. Si l'activation est une activation « Espace Travail uniquement », le terminal supprime toutes les données existantes et redémarre. Pour les autres types d'activation, Enterprise Management Agent effectue les opérations suivantes sur le terminal :
 - 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 Enterprise Management Agent.
5. Le terminal effectue les opérations suivantes :
 - a. Il établit une connexion avec BlackBerry UEM.
 - b. Il génère une clé symétrique partagée utilisée pour protéger le CSR et répondre à BlackBerry UEM en utilisant le mot de passe d'activation et EC-SPEKE.
 - c. Il crée un CSR et un HMAC cryptés comme suit :
 - Il génère une paire de clés pour le certificat
 - Il crée un CSR PKCS#10 qui inclut la clé publique de la paire de clés

- Il crypte le CSR à l'aide de la clé symétrique partagée et d'AES-256 en mode CBC avec remplissage PKCS#5
 - Il calcule un code HMAC du CSR crypté à l'aide de SHA-256 et l'ajoute au CSR
- d. Il envoie le CSR et le HMAC cryptés à BlackBerry UEM.
6. BlackBerry UEM effectue les actions suivantes :
- a. Il vérifie le HMAC du CSR crypté et décrypte le CSR à l'aide de la clé symétrique partagée
 - b. Il récupère le nom d'utilisateur, l'ID de l'espace Travail et le nom de votre organisation depuis la base de données BlackBerry UEM.
 - c. Il conditionne un certificat client à l'aide des informations récupérées et du CSR que le terminal a envoyé
 - d. Il signe le certificat client à l'aide du certificat racine de gestion d'entreprise
 - e. Il crypte le certificat client, le certificat racine de gestion d'entreprise et l'URL de BlackBerry UEM à l'aide de la clé symétrique partagée et d'AES-256 en mode CBC avec remplissage PKCS#5.
 - f. Il calcule un code HMAC du certificat client crypté, le certificat racine de gestion d'entreprise et l'URL de BlackBerry UEM et l'ajoute aux données cryptées.
 - g. Il envoie les données cryptées et le HMAC au terminal
7. Le terminal effectue les opérations suivantes :
- a. Il vérifie le HMAC
 - b. Il décrypte les données qu'il a reçues de BlackBerry UEM.
 - c. Il stocke le certificat client et le certificat racine de gestion d'entreprise dans sa base de stockage de clés
8. BlackBerry UEM effectue les actions suivantes :
- a. BlackBerry UEM Core attribue le nouveau terminal à une instance de BlackBerry UEM du domaine.
 - b. BlackBerry UEM Core notifie l'instance active de BlackBerry Affinity Manager qu'un nouveau terminal a été attribué à l'instance de BlackBerry UEM.
 - c. L'instance active de BlackBerry Affinity Manager avertit BlackBerry Dispatcher sur cette instance de BlackBerry UEM qu'il y a un nouveau terminal.
 - d. BlackBerry UEM Core envoie des informations de configuration, notamment les paramètres de connectivité d'entreprise, au terminal.
9. BlackBerry UEM Core et le terminal génèrent la clé de transport de terminal avec ECMQV et les clés publiques à long terme authentifiées du certificat client et du certificat du serveur pour BlackBerry UEM. Cette clé est utilisée pour crypter les données professionnelles lorsque BlackBerry Secure Connect Plus n'est pas utilisé et pour transmettre des données IPPP.
10. Le terminal envoie un message de confirmation via TLS à BlackBerry UEM pour confirmer qu'il a reçu et appliqué la stratégie informatique et les autres données et qu'il a créé l'espace Travail. Le processus d'activation est terminé.

Les protocoles de courbe elliptique utilisés pendant le processus d'activation utilisent la courbe à 521 bits recommandée par NIST.

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.

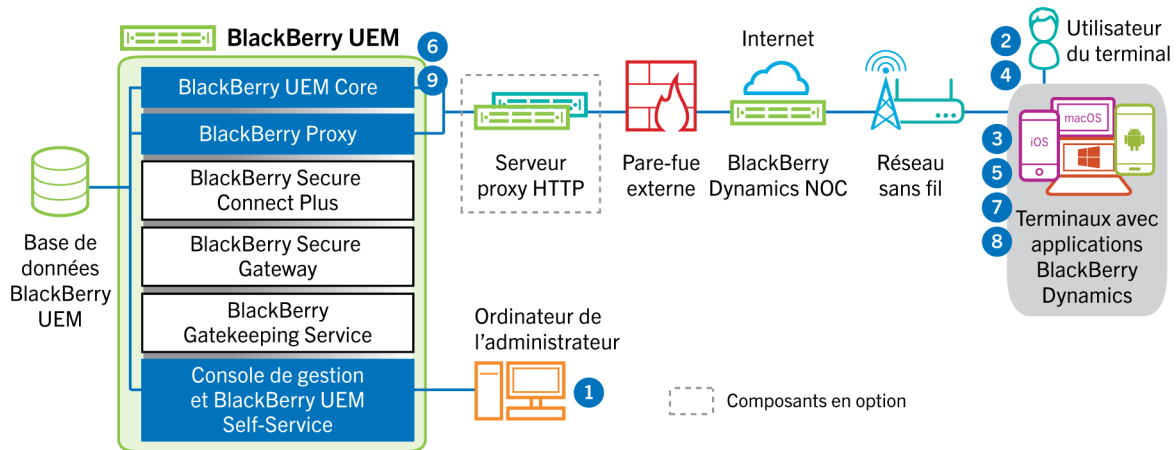


1. Un administrateur effectue les opérations suivantes :
 - a. Attribue une ou plusieurs applications BlackBerry Dynamics à un utilisateur.
 - b. Émet des informations d'identification d'activation (clé d'accès, mot de passe d'activation ou QR Code) et les envoie à l'utilisateur ou demande à l'utilisateur 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 l'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.

Envoi et réception de données professionnelles

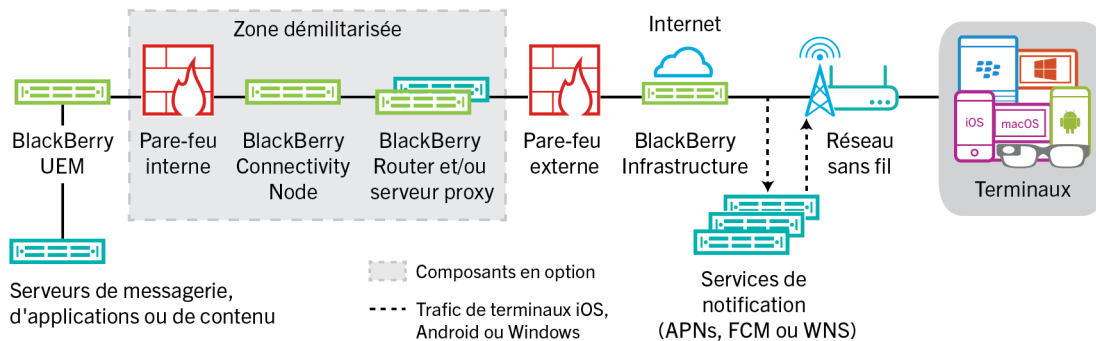
Lorsque les terminaux qui sont activés sur BlackBerry UEM envoient et reçoivent des données professionnelles, ils se connectent aux serveurs de messagerie, d'application ou de contenu de votre entreprise. Par exemple, lorsqu'ils utilisent les applications professionnelles de messagerie ou de calendrier, 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.

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 BlackBerry 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 BlackBerry 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. |
| BlackBerry UEM et BlackBerry Infrastructure ou BlackBerry Dynamics NOC | <p>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 BlackBerry UEM et BlackBerry Infrastructure.</p> <ul style="list-style-type: none">• 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 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 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 BlackBerry 10, 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 BlackBerry 10 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 BlackBerry 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. |

Envoi et réception 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 montre comment les terminaux se connectent à BlackBerry UEM et aux ressources de votre entreprise par le biais de BlackBerry Infrastructure.



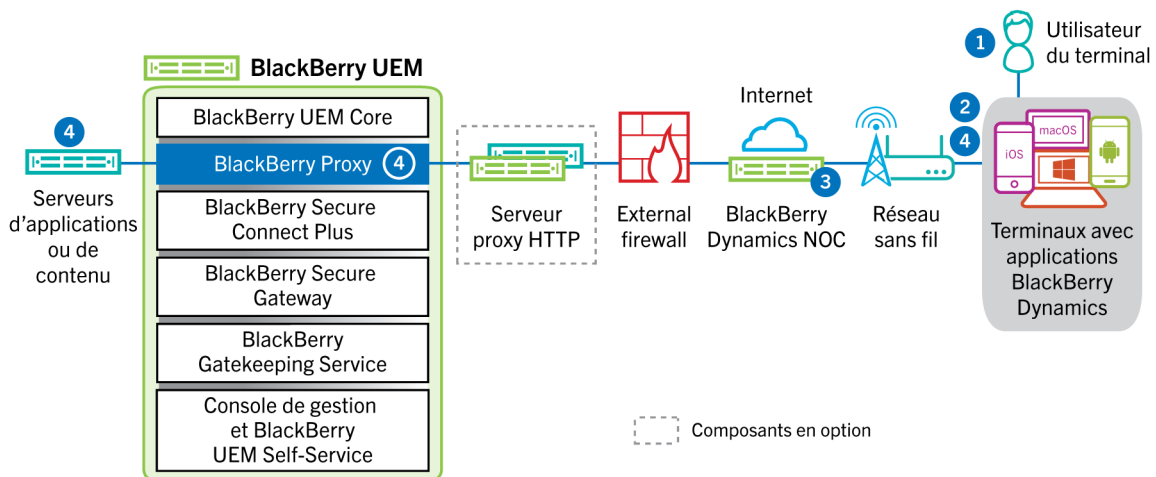
Le tableau suivant décrit les circonstances dans lesquelles les terminaux se connectent à BlackBerry UEM et au réseau de votre entreprise via BlackBerry Infrastructure.

| 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 Réception des mises à jour de configuration des terminaux . |
| Terminals 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, Samsung Knox Workspace et BlackBerry 10. | <p>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.</p> <p>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.</p> <p>Pour les terminaux Android Enterprise et BlackBerry 10, BlackBerry Secure Connect Plus fournit un tunnel sécurisé entre toutes les applications de l'espace de travail et le réseau de votre entreprise.</p> <p>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 professionnelles ou uniquement les applications spécifiées.</p> |
| 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. |
| Terminaux BlackBerry 10 | Les terminaux BlackBerry 10 utilisent ce chemin de communication pour envoyer et recevoir les données professionnelles lorsqu'il s'agit du chemin le plus direct et le plus rentable. |

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.



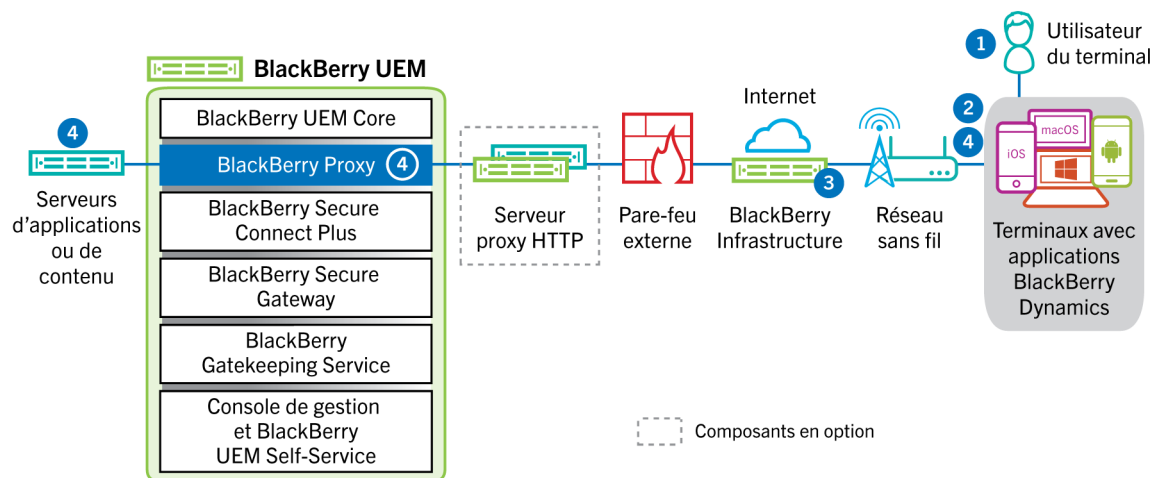
1. L'utilisateur ouvre une application BlackBerry Dynamics pour accéder aux données professionnelles.

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 connaît 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.

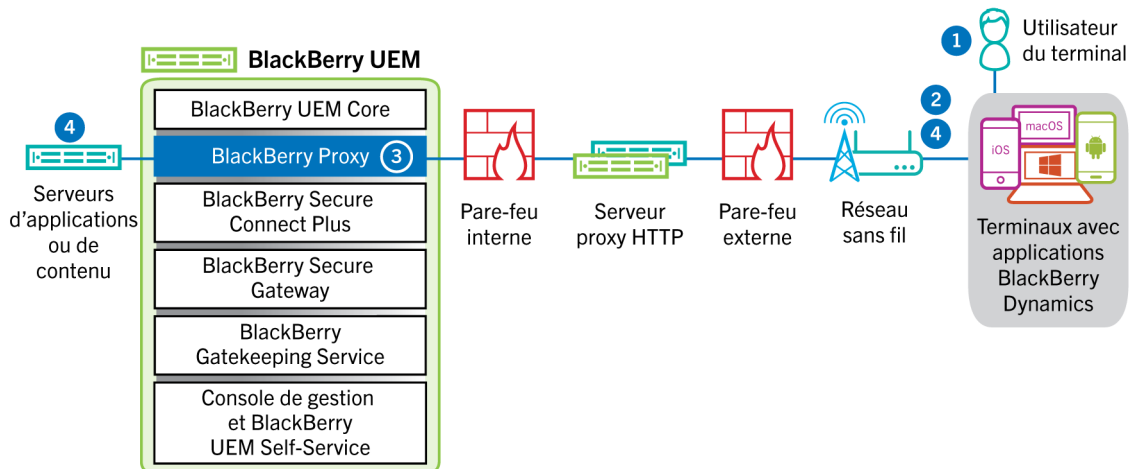
Ce flux de données décrit la façon dont les données sont acheminées lorsqu'une application BlackBerry Dynamics accède à un serveur d'applications ou de contenu de votre organisation par le biais de BlackBerry Infrastructure et BlackBerry UEM.



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](#).

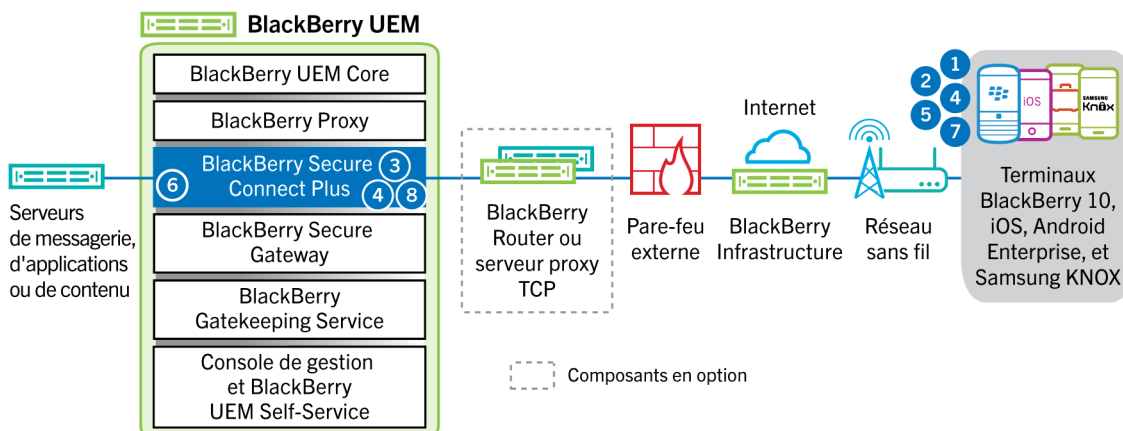


1. L'utilisateur ouvre une application BlackBerry Dynamics pour accéder aux données professionnelles.
2. L'application BlackBerry Dynamics établit une connexion TLS avec BlackBerry Proxy.
3. BlackBerry Proxy s'authentifie auprès de l'application BlackBerry Dynamics. BlackBerry Proxy s'authentifie auprès 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.

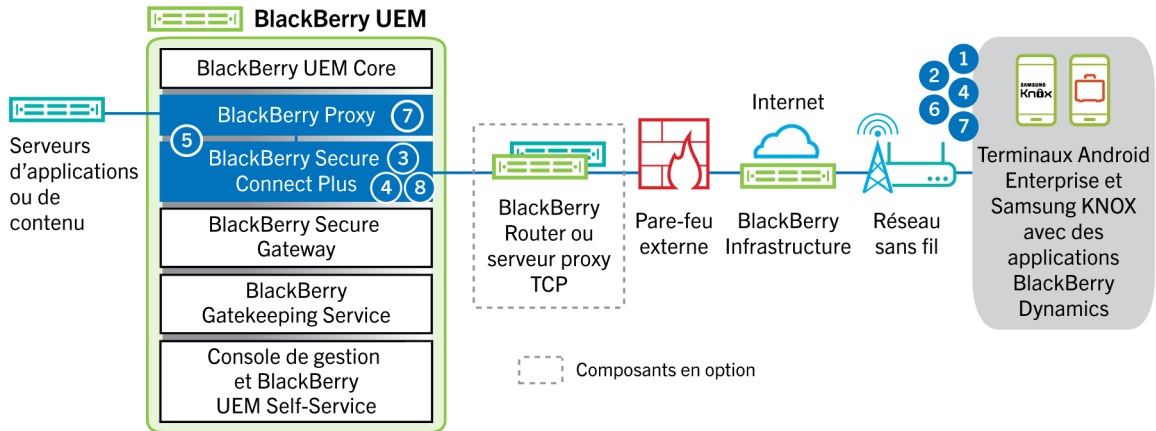
- Pour les terminaux Android Enterprise, toutes les applications de l'espace Travail à l'exception de celles pour lesquelles vous choisissez de limiter l'utilisation de BlackBerry Secure Connect Plus.
 - Pour les terminaux Samsung Knox Workspace, vous devez spécifier si toutes les applications de l'espace 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 spécifiées doivent utiliser BlackBerry Secure Connect Plus.
 - Pour les terminaux BlackBerry 10 et Android Enterprise, toutes les applications de l'espace Travail utilisent 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.

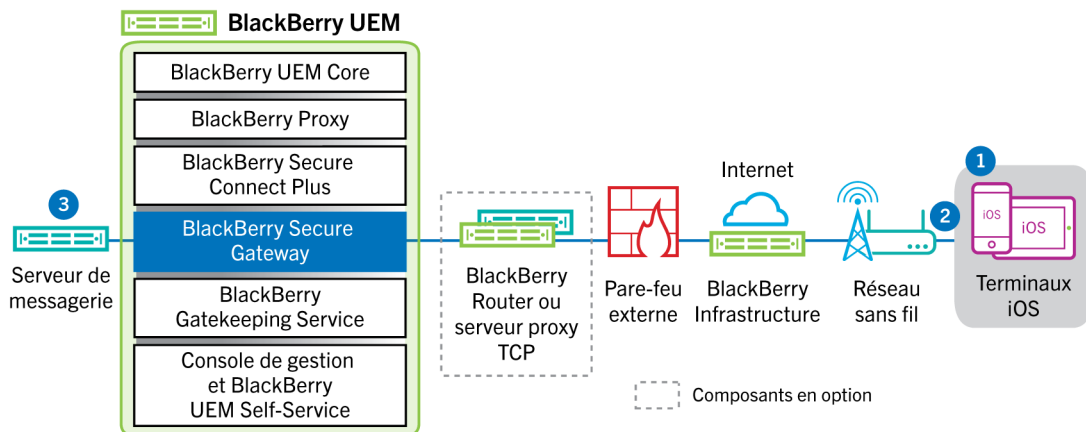
Si vous utilisez BlackBerry Secure Connect Plus avec des applications BlackBerry Dynamics sur un terminal Android Enterprise ou un terminal Samsung Knox Workspace, il est recommandé de configurer BlackBerry UEM dans le but de ne pas envoyer les données de l'application BlackBerry Dynamics à travers BlackBerry 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 : envoi d'un e-mail depuis un terminal iOS à l'aide de BlackBerry Secure Gateway

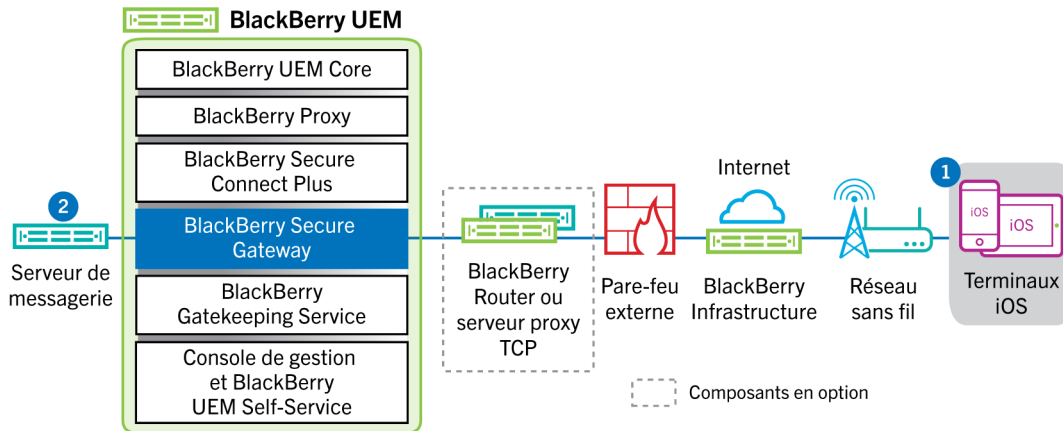
Ce flux de données décrit la façon dont les données de messagerie et de calendrier professionnelles sont acheminées des terminaux iOS vers le serveur Exchange ActiveSync à l'aide de BlackBerry Secure Gateway.



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 boîte 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

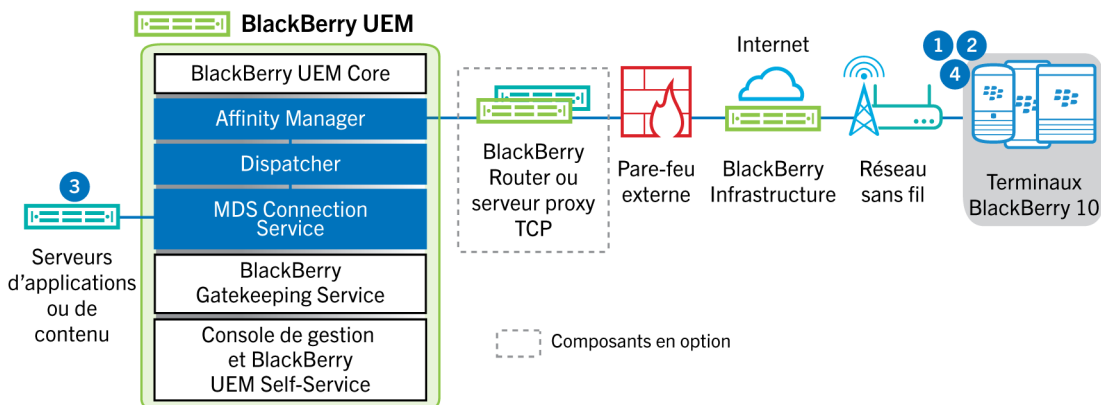
Ce flux de données décrit la façon dont les données de messagerie et de calendrier professionnelles sont acheminées entre les terminaux iOS et le serveur Exchange ActiveSync à l'aide de BlackBerry Secure Gateway.



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.

Flux de données : accès à un serveur d'applications ou de contenu à partir d'un terminal BlackBerry 10

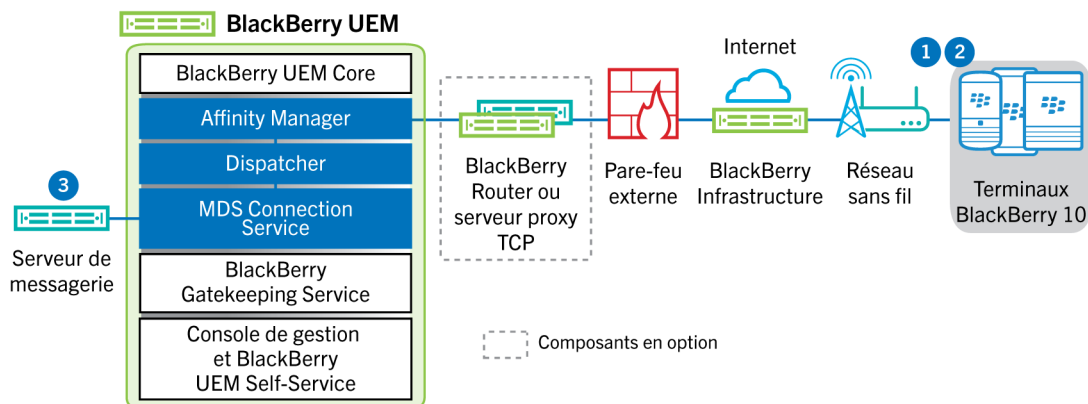
Ce flux de données décrit la façon dont les données sont acheminées lorsqu'une application professionnelle installée sur un terminal BlackBerry 10 accède à un serveur d'applications ou de contenu de votre entreprise alors que BlackBerry Secure Connect Plus est désactivé.



1. L'utilisateur ouvre une application professionnelle pour consulter des données professionnelles. Par exemple, l'utilisateur ouvre le navigateur professionnel pour naviguer sur le réseau intranet ou utilise BlackBerry Work Drives pour accéder à un fichier sur un lecteur réseau.
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 BlackBerry Infrastructure, BlackBerry Affinity Manager, BlackBerry Dispatcher et BlackBerry MDS Connection Service.
3. Le serveur d'applications ou de contenu répond en fournissant les données professionnelles. Les données professionnelles sont acheminées vers le terminal via BlackBerry MDS Connection Service, BlackBerry Dispatcher, BlackBerry Affinity Manager et BlackBerry Infrastructure.
4. L'application reçoit les données et les affiche sur le terminal.

Flux de données : envoi d'un e-mail depuis un terminal BlackBerry 10

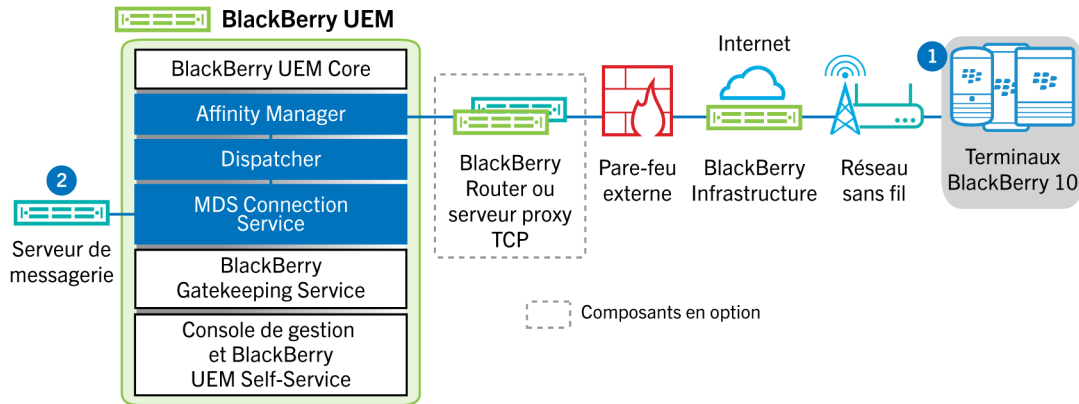
Ce flux de données décrit la façon dont les données de messagerie et de calendrier professionnelles sont acheminées des terminaux BlackBerry Secure Connect Plus vers le serveur BlackBerry 10 lorsque Exchange ActiveSync est désactivé.



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, BlackBerry Affinity Manager, BlackBerry Dispatcher et BlackBerry MDS Connection Service.
3. Le serveur de messagerie met à jour les données de l'organiseur dans la boîte 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 BlackBerry 10

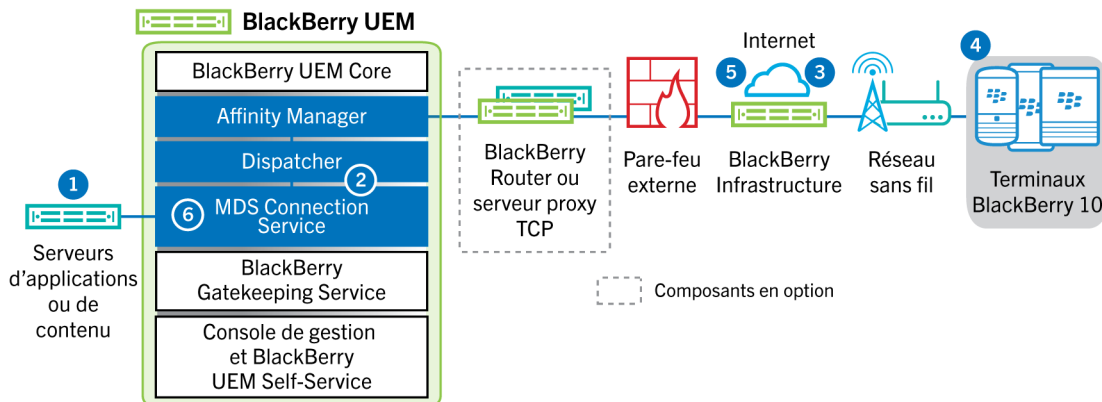
Ce flux de données décrit la façon dont les e-mails professionnels envoyés par le serveur Exchange ActiveSync sont reçus par les terminaux BlackBerry 10 lorsque BlackBerry Secure Connect Plus est désactivé.



1. Le client de messagerie natif du terminal maintient une connexion permanente avec le serveur de messagerie sur un canal crypté et authentifié via BlackBerry Infrastructure, BlackBerry Affinity Manager, BlackBerry Dispatcher et BlackBerry MDS Connection Service, 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 les mises à jour à l'application de messagerie ou à l'application de données de l'organiseur du terminal via BlackBerry MDS Connection Service, BlackBerry Dispatcher, BlackBerry Affinity Manager et BlackBerry Infrastructure en utilisant le protocole Exchange ActiveSync.

Flux de données : réception des mises à jour de transmission de données d'entreprise sur un terminal BlackBerry 10

Ce flux de données décrit la façon dont les données sont acheminées d'un serveur d'applications vers une application appropriée de l'espace Travail d'un terminal BlackBerry 10 lorsque BlackBerry Secure Connect Plus est désactivé.



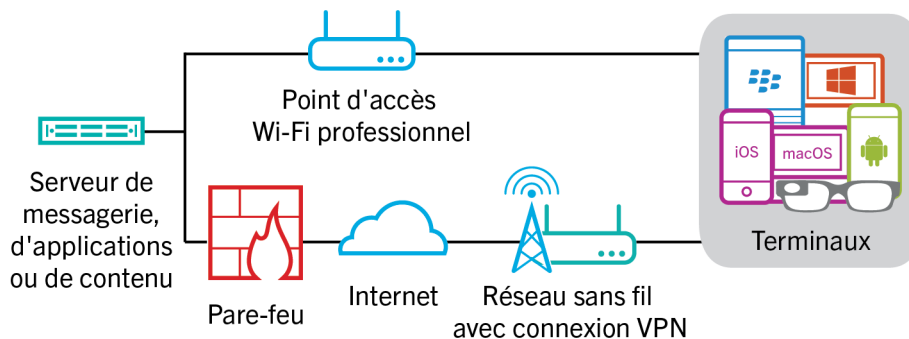
1. Lorsque des nouvelles données ou des mises à jour sont disponibles pour une application professionnelle installée sur un terminal BlackBerry 10, le serveur d'applications ou de contenu transmet les données à BlackBerry MDS Connection Service à l'aide d'une demande HTTP ou HTTPS.
2. BlackBerry MDS Connection Service envoie les données transmises via BlackBerry Dispatcher, BlackBerry Affinity Manager et BlackBerry Infrastructure sur le port 3101 du pare-feu.
3. BlackBerry Infrastructure envoie les données au terminal BlackBerry 10.
4. Le terminal BlackBerry 10 envoie un accusé de réception à BlackBerry Infrastructure. L'application du terminal détecte le contenu entrant et l'affiche dès que l'utilisateur ouvre l'application.

5. BlackBerry Infrastructure envoie un accusé de réception via BlackBerry Affinity Manager et BlackBerry Dispatcher à BlackBerry MDS Connection Service.
6. S'il est configuré en ce sens, BlackBerry MDS Connection Service envoie la confirmation de distribution à l'initiateur Push à l'aide d'une requête HTTP.

Envoi et réception 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 organisation, 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 organisation à l'aide du VPN ou du réseau Wi-Fi professionnel de votre organisation.



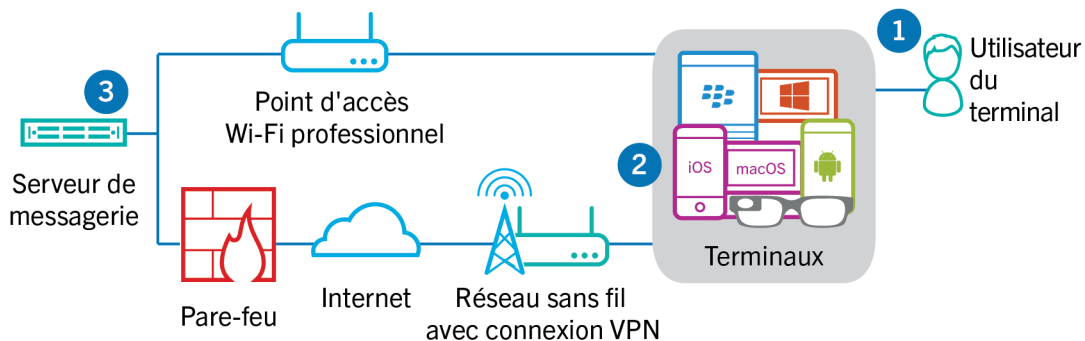
Le tableau suivant indique à quel moment les terminaux utilisent le réseau VPN ou le réseau Wi-Fi professionnel de votre entreprise pour se connecter au réseau de votre entreprise.

| Type de terminal | Description |
|---|---|
| Terminaux Android Enterprise et Knox Workspace | Par défaut, les terminaux Android Enterprise et Knox Workspace utilisent le réseau VPN ou le réseau Wi-Fi professionnel de votre organisation 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. |

| Type de terminal | Description |
|------------------|---|
| BlackBerry 10 | Les terminaux BlackBerry 10 utilisent le réseau VPN ou le réseau Wi-Fi professionnel de votre entreprise pour envoyer et recevoir les données professionnelles lorsqu'il s'agit du chemin le plus direct et le plus rentable. Les terminaux BlackBerry 10 utilisent uniquement les profils VPN et Wi-Fi configurés par vos soins (et non par l'utilisateur) lors de l'accès aux données professionnelles. |

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

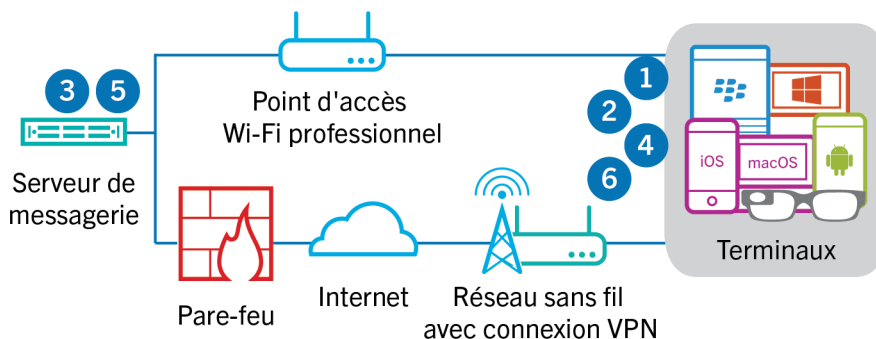
Ce flux de données décrit comment les données professionnelles de messagerie et de calendrier sont acheminées du terminal vers le serveur de messagerie sur le VPN ou réseau Wi-Fi professionnel de votre organisation via Exchange ActiveSync.



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 boîte 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

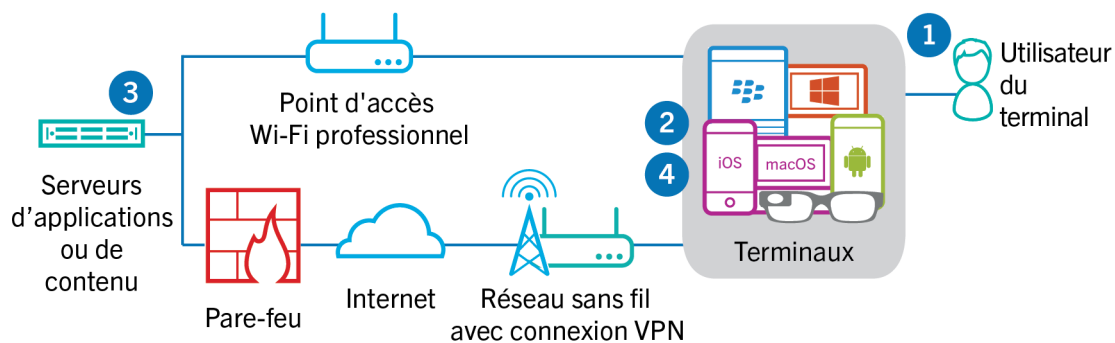
Ce flux de données décrit comment les données professionnelles de messagerie et de calendrier sont acheminées du terminal vers le serveur de messagerie sur le VPN ou réseau Wi-Fi professionnel de votre organisation via Exchange ActiveSync.



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.

Réception des 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.

Lorsqu'une mise à jour de configuration doit être envoyée à un terminal, BlackBerry UEM avertit ce terminal qu'une mise à jour de la configuration est en attente. Les terminaux interrogent en outre régulièrement BlackBerry UEM afin de connaître les actions à exécuter sur le terminal pour éviter qu'une mise à jour de configuration soit manquée au cas où une notification ne serait pas reçue par le terminal.

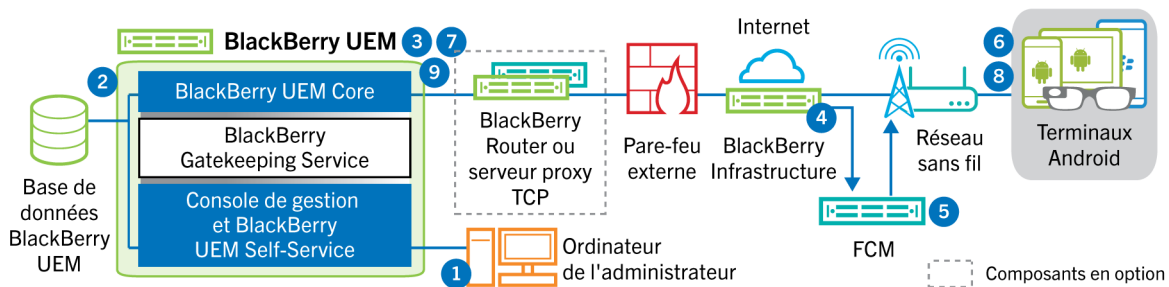
Sur les terminaux Android, BlackBerry UEM Client reçoit et exécute toutes les mises à jour de configuration.

Sur les terminaux iOS, l'application BlackBerry UEM Client affiche l'état de conformité et les informations de configuration du terminal, comme les applications ou stratégies qui lui sont attribuées. Toutefois, le démon MDM natif du terminal reçoit et applique toutes les mises à jour de configuration envoyées au terminal.

Sur les terminaux Windows 10 et macOS, qui ne nécessitent pas BlackBerry UEM Client pour l'activation, le démon MDM natif reçoit et applique toutes les mises à jour de configuration envoyées au terminal.

Sur les terminaux BlackBerry 10, Enterprise Management Agent reçoit et exécute toutes les 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 GCM pour notifier les terminaux Android qu'une mise à jour est en attente.
5. Le service GCM 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 à priorité la plus élevée.

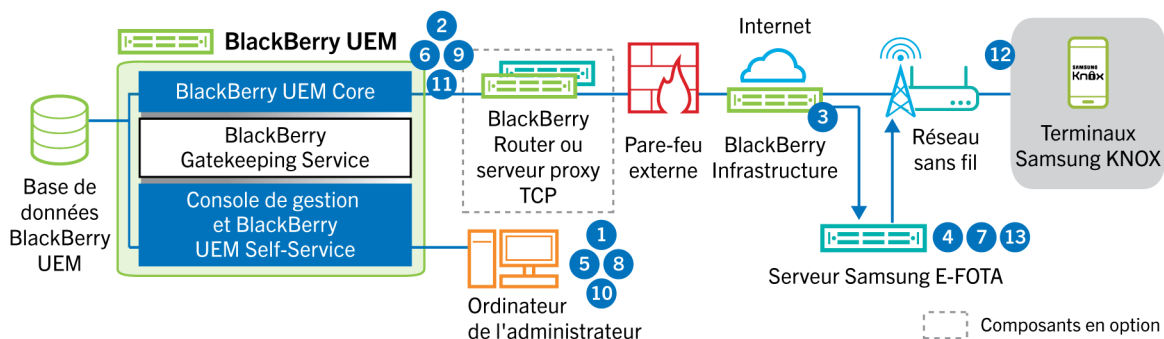
L'ordre de priorité est le suivant : commandes d'administration informatique (telles que Supprimer les données du terminal et Verrouiller le terminal), demandes d'informations sur le terminal, applications installées, etc. BlackBerry UEM Core n'envoie qu'une seule commande à la fois. Si nécessaire, des 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 à priorité 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.

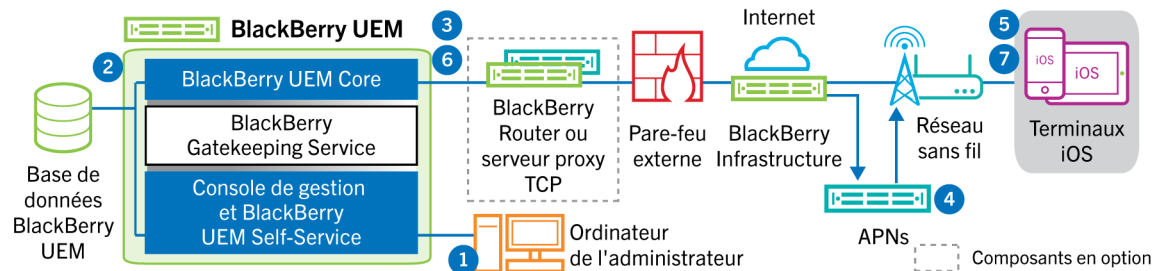
Flux de données : mise à jour du micrologiciel sur les terminaux Samsung Knox

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. Pour plus d'informations, reportez-vous à la section [Contrôle des versions du logiciel qui sont installées sur les terminaux](#) dans le contenu relatif à l'administration.



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.

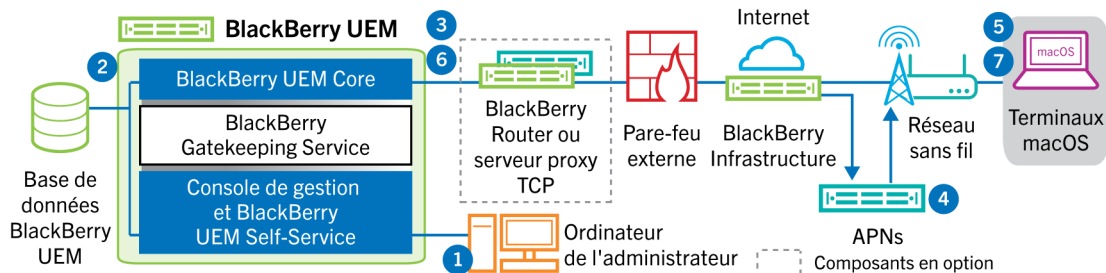
Flux de données : réception de mises à jour de configuration sur un terminal iOS



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.

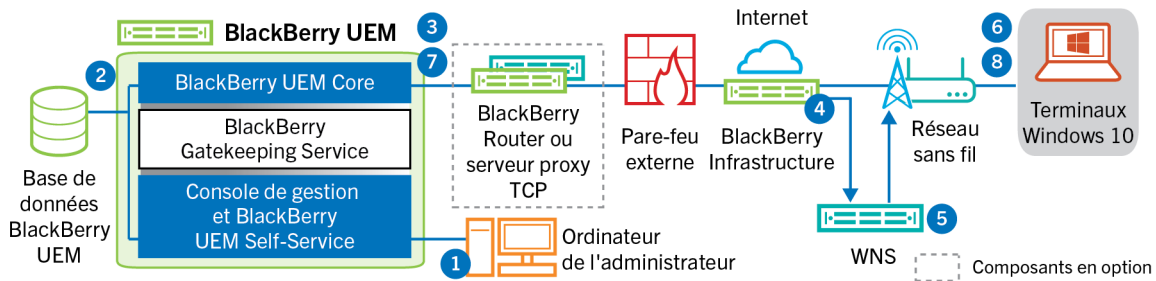
Flux de données : réception de mises à jour de configuration sur un terminal macOS



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.

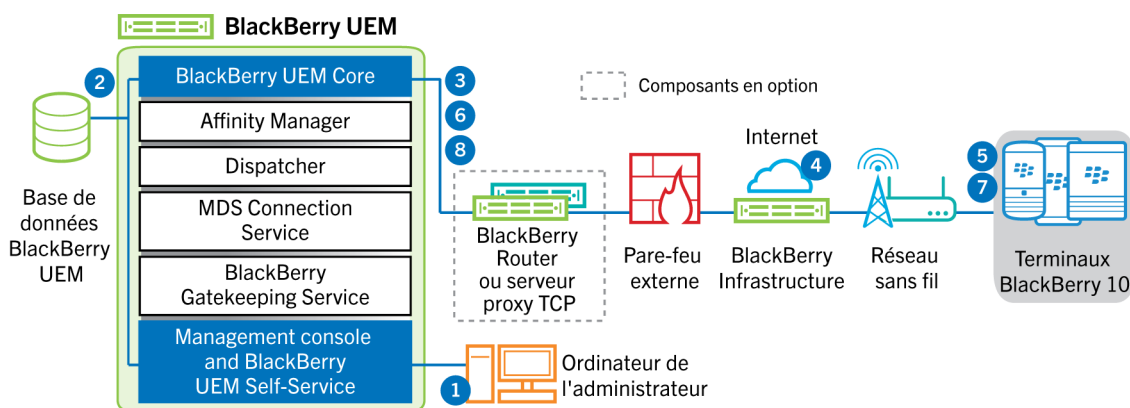
Flux de données : réception de mises à jour de configuration sur un terminal Windows 10



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.

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



1. Sur la console de gestion, une action déclenche la mise à jour de configuration du terminal. 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 notifie BlackBerry Infrastructure qu'une mise à jour est disponible pour un terminal. La notification est transmise par le biais de BlackBerry Router ou du serveur proxy TCP, s'il est installé, et du pare-feu externe, sur le port 3101.
4. BlackBerry Infrastructure notifie l'agent Enterprise Management Agent du terminal qu'une mise à jour est disponible.
5. L'agent Enterprise Management Agent du terminal interroge BlackBerry UEM Core pour connaître les actions et commandes en attente à exécuter sur le terminal. Cette interrogation est transmise via BlackBerry Infrastructure et BlackBerry Router, s'il est installé, jusqu'à BlackBerry UEM Core.
6. 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 à priorité 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.

7. L'agent Enterprise Management Agent du terminal reçoit les mises à jour de configuration et applique la nouvelle configuration ou la mise à jour sur le terminal. Enterprise Management Agent 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.
8. Si d'autres actions ou commandes sont en attente pour le terminal, BlackBerry UEM Core répond, via BlackBerry Infrastructure, en commençant par l'action à priorité 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 6 à 8 sont répétées jusqu'à ce qu'il ne reste aucune action ou commande en attente sur le terminal.

Informations juridiques

©2021 BlackBerry Limited. Les marques commerciales, notamment BLACKBERRY, BBM, BES, EMBLEM Design, ATHOC, CYLANCE et SECUSMART sont des marques commerciales ou des marques déposées de BlackBerry Limited, ses filiales et/ou sociétés affiliées, utilisées sous licence, et les droits exclusifs de ces marques commerciales sont expressément réservés. Toutes les autres marques commerciales appartiennent à leurs propriétaires respectifs.

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 D'UN LOGICIEL, MATÉRIEL, 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 LA GARANTIE LIMITÉE APPLICABLE, L'ACCORD DE LICENCE DU LOGICIEL BLACKBERRY ET/OU 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 L'UTILISATION OU NON-UTILISATION DES LOGICIELS, DU MATÉRIEL, DES SERVICES OU DES PRODUITS ET SERVICES TIERS MENTIONNÉS DANS LES PRÉSENTES, ET NOTAMMENT 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 COÛTS 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, DEMANDE OU ACTION ENTREPRISE PAR VOUS, NOTAMMENT POUR RUPTURE DE CONTRAT, NÉGLIGENCE, FAUTE, RESPONSABILITÉ STRICTE OU TOUT 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 AYANT-DROIT, REPRÉSENTANTS, AGENTS, FOURNISSEURS (NOTAMMENT LES FOURNISSEURS DE SERVICES DE TEMPS DE COMMUNICATION), REVENEURS 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, DISTRIBUTEURS, FOURNISSEURS, SOUS-TRAITANTS INDÉPENDANTS 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 sans fil prend en charge toutes les fonctionnalités. Certains fournisseurs de services sans fil 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 ni garanties expresses ou tacites d'aucune sorte par BlackBerry, et BlackBerry n'engage aucune responsabilité sur les Produits et Services tiers. 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