BlackBerry UEM Cloud

Architecture et flux de données

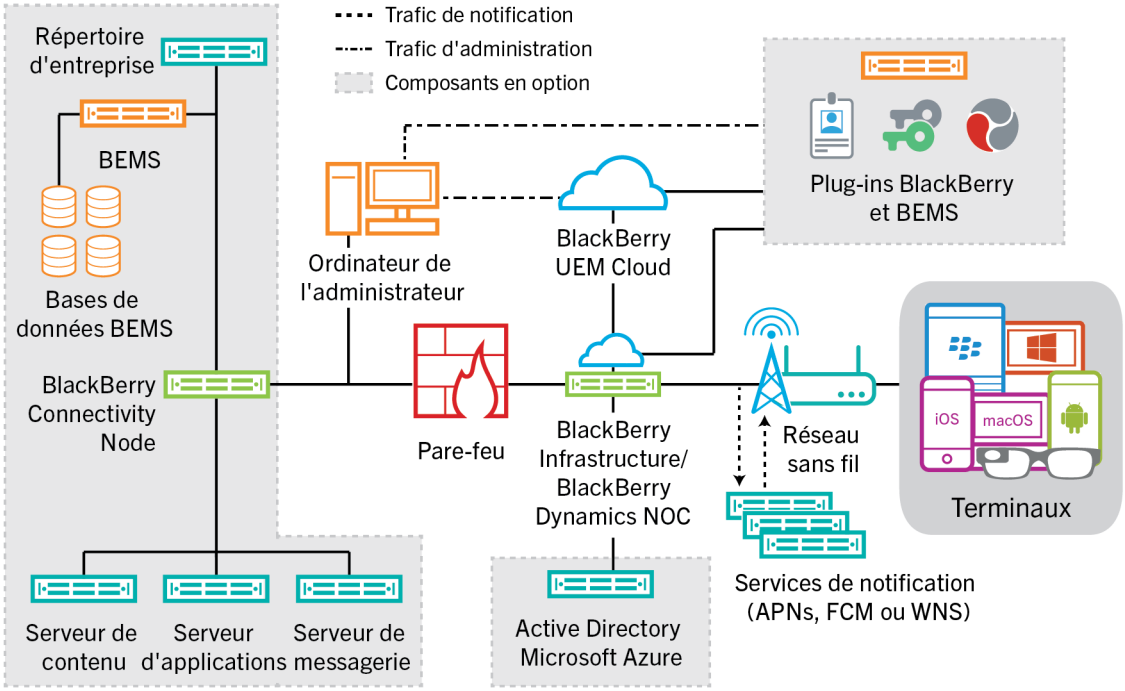
Table des matières

Architecture et flux de données de BlackBerry UEM Cloud

BlackBerry UEM Cloud est une solution de gestion de points de terminaison unifiée de BlackBerry. BlackBerry UEM Cloud vous permet de gérer des terminaux iOS, macOS, Android, Windows 10 et BlackBerry 10 à l'aide d'une simple interface Web et de protéger vos informations commerciales sur des terminaux BYOD, COPE et COBO.

L'architecture BlackBerry UEM Cloud 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 Cloud



Composant	Description
BlackBerry UEM Cloud	BlackBerry UEM Cloud est un service qui vous permet de gérer les terminaux utilisés dans l'environnement de votre entreprise.

Composant	Description
BlackBerry Infrastructure et BlackBerry Dynamics NOC	BlackBerry Infrastructure enregistre les informations utilisateur requises pour activer le terminal et valide les informations de licence de BlackBerry UEM Cloud. Si vous activez BlackBerry Secure Connect Plus ou BlackBerry Secure Gateway, les données en transit qui utilisent ces services passent par BlackBerry Infrastructure. BlackBerry Dynamics NOC est un NOC distinct qui permet des communications sécurisées entre les applications BlackBerry Dynamics installées sur les terminaux, et BlackBerry Proxy installé derrière le pare-feu lors de l'installation de BlackBerry Connectivity Node.
Terminaux	BlackBerry UEM Cloud prend en charge les terminaux iOS, macOS, Android, Windows 10 et BlackBerry 10.
Services de notification	BlackBerry UEM Cloud 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 : • APNs est un service fourni par Apple pour envoyer des notifications aux terminaux iOS et macOS. • Le service GCM fourni par Google envoie les notifications aux terminaux Android. • Le service WNS fourni par Microsoft envoie les notifications aux terminaux Windows 10.

Composant	Description
BlackBerry Connectivity Node	BlackBerry Connectivity Node est un composant facultatif que vous installez à l'intérieur du pare-feu de votre entreprise. Il comprend cinq composants qui améliorent le fonctionnement de BlackBerry UEM Cloud : • Le BlackBerry Cloud Connector connecte BlackBerry UEM Cloud à votre annuaire d'entreprise derrière le pare-feu pour permettre la synchronisation des attributs de base, une fonction de recherche et des services d'authentification des utilisateurs. Si vous n'installez pas BlackBerry Connectivity Node et que votre annuaire d'entreprise est derrière le pare-feu, vous devez créer des comptes utilisateur locaux dans BlackBerry UEM Cloud plutôt que d'utiliser les comptes utilisateur dans votre annuaire d'entreprise. BlackBerry Cloud Connector n'est pas nécessaire pour que BlackBerry UEM Cloud se connecte à Microsoft Azure Active Directory. • BlackBerry Proxy maintient une connexion sécurisée entre votre entreprise et BlackBerry Dynamics NOC, qui permet aux applications BlackBerry Dynamics de communiquer en toute sécurité avec les ressources de votre entreprise derrière le pare-feu. Il prend également en charge BlackBerry Dynamics Direct Connect, qui permet aux données d'application de contourner BlackBerry Dynamics NOC. • BlackBerry Gatekeeping Service envoie les commandes à Exchange ActiveSync pour ajouter les terminaux à une liste autorisée lorsque ceux-ci sont activés sur BlackBerry UEM Cloud. Les terminaux non gérés qui tentent de se connecter au serveur de messagerie d'une entreprise peuvent être examinés, vérifiés et bloqués ou autorisés par un administrateur via la console de gestion de BlackBerry UEM. • BlackBerry Secure Connect Plus fournit un tunnel IP sécurisé entre les applications professionnelles sur les terminaux et le réseau de votre organisation. Un tunnel prenant en charge les données IPv4 standard (TCP et UDP) est établi pour chaque terminal par l'intermédiaire de BlackBerry Infrastructure. • BlackBerry Secure Gateway fournit une connexion sécurisée avec le serveur de messagerie de votre entreprise par le biais de BlackBerry Infrastructure et BlackBerry UEM Cloud pour les terminaux iOS. BlackBerry Connectivity Node utilise le port 3101 pour communiquer avec BlackBerry UEM Cloud.

Composant	Description
BlackBerry Enterprise Mobility Server	Si vous avez installé BlackBerry Connectivity Node, vous pouvez également installer un BEMS sur site. BEMS consolide plusieurs services permettant d'échanger des données professionnelles avec les applications BlackBerry Dynamics : • BlackBerry Connect fournit une messagerie instantanée sécurisée, une recherche dans l'annuaire d'entreprise et des informations de présence des utilisateurs aux terminaux iOS et Android. • BlackBerry Presence fournit un état de présence en temps réel aux applications BlackBerry Dynamics. • BlackBerry Docs permet aux utilisateurs d'applications BlackBerry Dynamics d'accéder aux documents, de les synchroniser et de les partager à l'aide leur serveur de fichiers professionnel, de SharePoint, de Box et des systèmes de gestion de contenu prenant en charge CMIS. Aucun logiciel VPN, aucune reconfiguration du pare-feu et aucune duplication des magasins de données ne sont nécessaires.
Bases de données BlackBerry Enterprise Mobility Server	Les bases de données BEMS stockent les informations relatives aux utilisateurs, aux applications, aux stratégies et à la configuration.
Répertoire d'entreprise	BlackBerry UEM Cloud prend en charge la connectivité avec Microsoft Active Directory ou l'annuaire d'entreprise LDAP de votre organisation derrière le pare-feu à l'aide de BlackBerry Connectivity Node.
Microsoft Azure Active Directory	Microsoft Azure Active Directory est un service de gestion de répertoire reposant sur le Cloud. Si votre organisation utilise Azure Active Directory, vous pouvez vous y connecter à la place, ou en plus, d'un répertoire d'entreprise derrière le pare-feu.
Serveurs de contenu, d'applications et de messagerie	Lorsque vous activez BlackBerry Secure Connect Plus ou lorsque des utilisateurs disposent d'applications BlackBerry Dynamics, les terminaux peuvent se connecter aux serveurs de votre entreprise sans que vous deviez ouvrir une connexion directe entre le serveur et Internet. Les données professionnelles en transit entre vos serveurs et terminaux sont envoyées via BlackBerry Secure Connect Plus et BlackBerry Infrastructure. Les données d'applications BlackBerry Dynamics sont envoyées par BlackBerry Proxy et BlackBerry Dynamics NOC. BlackBerry Secure Gateway fournit une connexion sécurisée via BlackBerry Infrastructure et BlackBerry Connectivity Node entre le serveur de messagerie de votre entreprise et les terminaux iOS.
Plug-ins BlackBerry et BEMS	La version Cloud de BlackBerry Enterprise Mobility Server fournit BlackBerry Push Notifications, qui 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. Si Microsoft Exchange se situe derrière le pare-feu de votre entreprise, vous devez ouvrir un port pour que BEMS puisse communiquer avec Microsoft Exchange. BlackBerry UEM Cloud fonctionne avec des produits d'entreprise BlackBerry complémentaires, tels que BlackBerry Enterprise Identity, BlackBerry 2FA et BlackBerry Workspaces, pour vous permettre d'étendre les fonctionnalités UEM de votre entreprise.

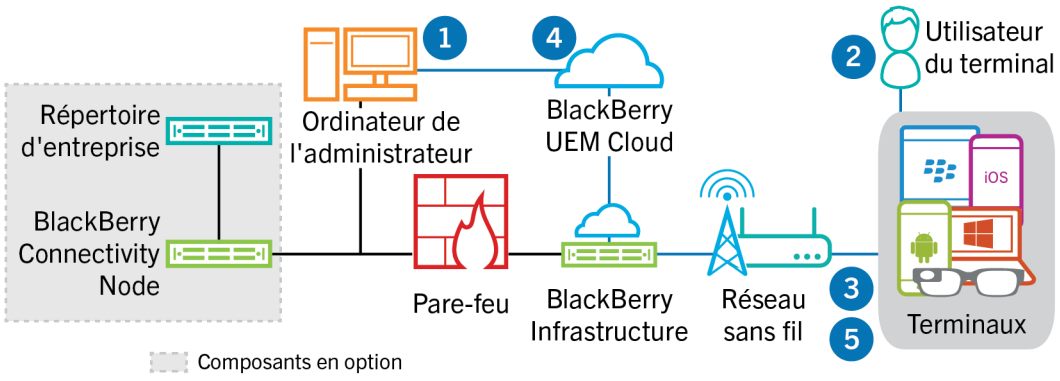
Activation des terminaux et des applications BlackBerry Dynamics

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 iOS, Android, Windows 10 ou BlackBerry 10

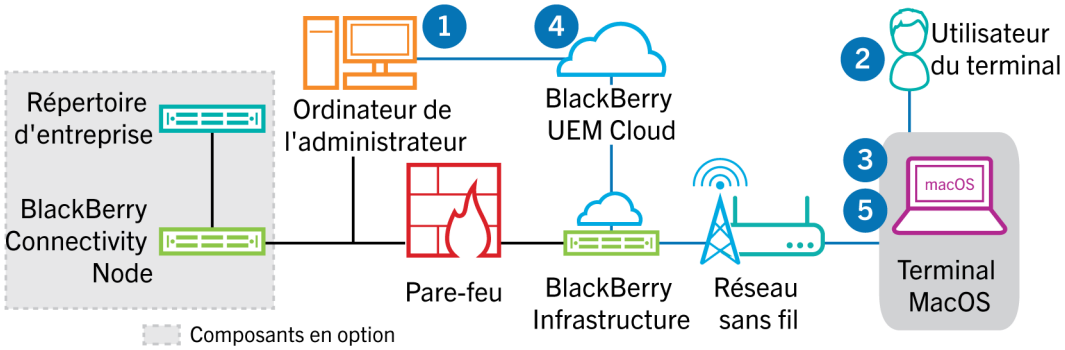


1. Vous effectuez les opérations suivantes :
   a. Ajoutez un utilisateur à BlackBerry UEM Cloud en tant que compte d'utilisateur local ou, si vous avez installé BlackBerry Connectivity Node, à l'aide des informations de compte récupérées à partir de votre répertoire d'entreprise.
   b. Attribuez un profil d'activation à l'utilisateur.
   c. Selon le type de terminal et les préférences de votre entreprise, utilisez l'une des options suivantes pour communiquer les détails de l'activation à l'utilisateur :
      - Générez automatiquement un mot de passe d'activation du terminal et éventuellement un code QR, 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 communiquez l'adresse de BlackBerry UEM Self-Service à l'utilisateur afin qu'il puisse définir son propre password d'activation et afficher un code QR.

2. L'utilisateur effectue les opérations suivantes :
   a. S'il active un terminal iOS ou Android, télécharger et installer BlackBerry UEM Client.
   b. Saisir son nom d'utilisateur et mot de passe d'activation ou lire le code QR sur son terminal.
3. Le terminal envoie une demande d'activation à BlackBerry UEM.
4. BlackBerry UEM Cloud vérifie les informations d'identification d'activation de l'utilisateur et envoie les détails de l'activation au terminal, y compris les informations sur la configuration du terminal.
5. Le terminal reçoit les détails d'activation à partir de BlackBerry UEM Cloud et termine la configuration. Le terminal envoie ensuite une confirmation à BlackBerry UEM Cloud indiquant que l'activation est réussie.

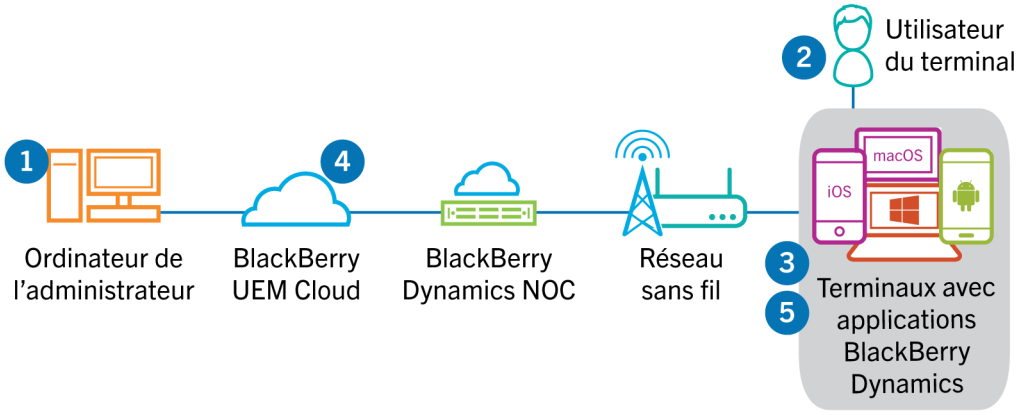
Flux de données : activation d'un terminal macOS



1. Vous effectuez les opérations suivantes :
   a. Ajoutez l'utilisateur à BlackBerry UEM Cloud en tant que compte d'utilisateur local ou, si vous avez installé BlackBerry Connectivity Node, à l'aide des informations de compte récupérées à partir de votre répertoire d'entreprise.
   b. Attribuez un profil d'activation à l'utilisateur.
   c. Vous devez vous assurer que l'utilisateur dispose 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 Cloud.
4. BlackBerry UEM Cloud vérifie les informations d'identification d'activation et envoie les détails de l'activation au terminal, y compris les informations sur la configuration du terminal.
5. Le terminal reçoit les détails d'activation à partir de BlackBerry UEM Cloud et termine la configuration. Le terminal envoie ensuite une confirmation à BlackBerry UEM Cloud indiquant que l'activation est réussie.

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.

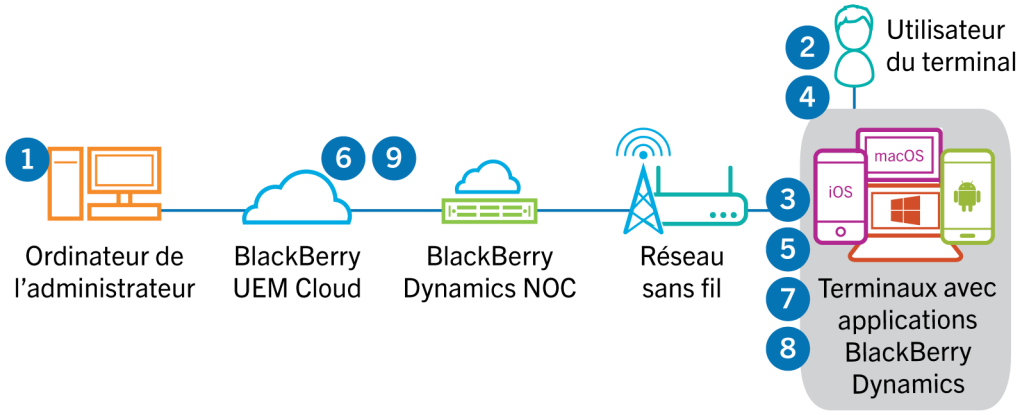


1. Un administrateur effectue les opérations suivantes :
   a. Attribue une ou plusieurs applications BlackBerry Dynamics à un utilisateur.
   b. Émet des informations d'identification d'activation (clé d'accès, mot de passe d'activation ou QR Code) et les envoie à l'utilisateur ou demande à l'utilisateur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



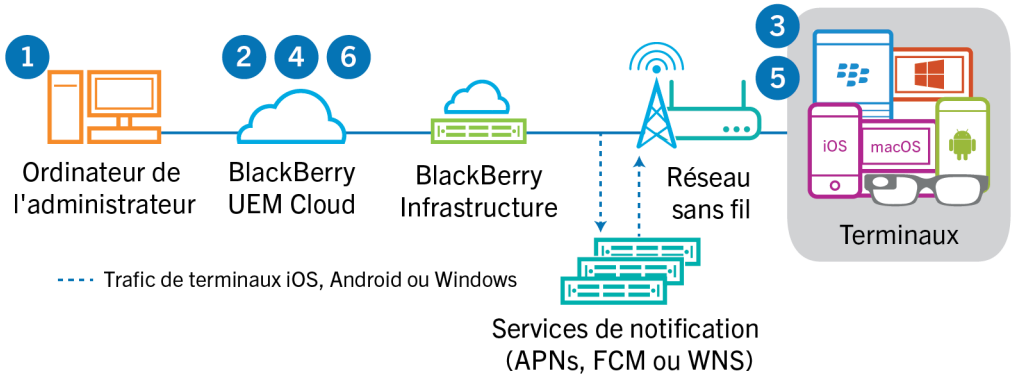
1. Un administrateur attribue une ou plusieurs applications BlackBerry Dynamics à un utilisateur.
2. L'utilisateur installe l'application sur le terminal.
3. L'application effectue les opérations suivantes :
   a. Interroge BlackBerry Dynamics NOC et identifie une autre application qui est activée sur 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.

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

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 Cloud avertit ce terminal qu'une mise à jour de la configuration est en attente. Les terminaux interrogent en outre régulièrement BlackBerry UEM Cloud afin de connaitre 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.



1. Vous utilisez la console de gestion pour envoyer des commandes au terminal (comme verrouiller le terminal ou supprimer les données professionnelles) ou vous effectuez des tâches de gestion sur le terminal (comme mettre à jour les stratégies informatiques, les profils et les paramètres d'applications ou encore les attributions), et déclenchez une mise à jour de configuration du terminal.
2. BlackBerry UEM Cloud attribue la mise à jour et identifie les objets devant être partagés avec le terminal, puis effectue l'une des actions suivantes :
   - Pour les terminaux Android, BlackBerry UEM Cloud notifie BlackBerry UEM Client sur le terminal qu'une mise à jour est en attente à l'aide de GCM. Le service GCM envoie une notification au terminal pour contacter BlackBerry UEM Cloud.
   - Pour les terminaux iOS et OS X, BlackBerry UEM Cloud notifie le démon MDM sur le terminal qu'une mise à jour est en attente à l'aide de l'APNs. L'APNs envoie une notification au terminal pour contacter BlackBerry UEM Cloud.
   - Pour les terminaux BlackBerry UEM Cloud, Windows 10 notifie le démon MDM sur le terminal qu'une mise à jour est en attente à l'aide du service WNS. Le service WNS envoie une notification au terminal pour contacter BlackBerry UEM Cloud.
   - Pour les terminaux BlackBerry 10, BlackBerry UEM Cloud notifie Enterprise Management Agent sur le terminal qu'une mise à jour est en attente.
3. Le terminal contacte BlackBerry UEM Cloud pour toute demande d'actions en attente devant être effectuée sur le terminal.
4. BlackBerry UEM Cloud répond par l'action à priorité la plus élevée.

   L'ordre de priorité est le suivant : commandes d'administration informatique (telles que Verrouiller le terminal), demandes d'informations sur le terminal, applications installées, etc. BlackBerry UEM Cloud envoie une seule commande à la fois. Si nécessaire, des informations supplémentaires sont incluses dans la réponse.
5. Le terminal effectue les opérations suivantes :

   a. Le terminal examine la réponse de BlackBerry UEM Cloud
   b. Planifie la commande à traiter et attend l'exécution de celle-ci
   c. Envoie une réponse à BlackBerry UEM Cloud 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.
6. Si d'autres actions ou commandes sont en attente pour le terminal, BlackBerry UEM Cloud répond en commençant par l'action à priorité la plus élevée.

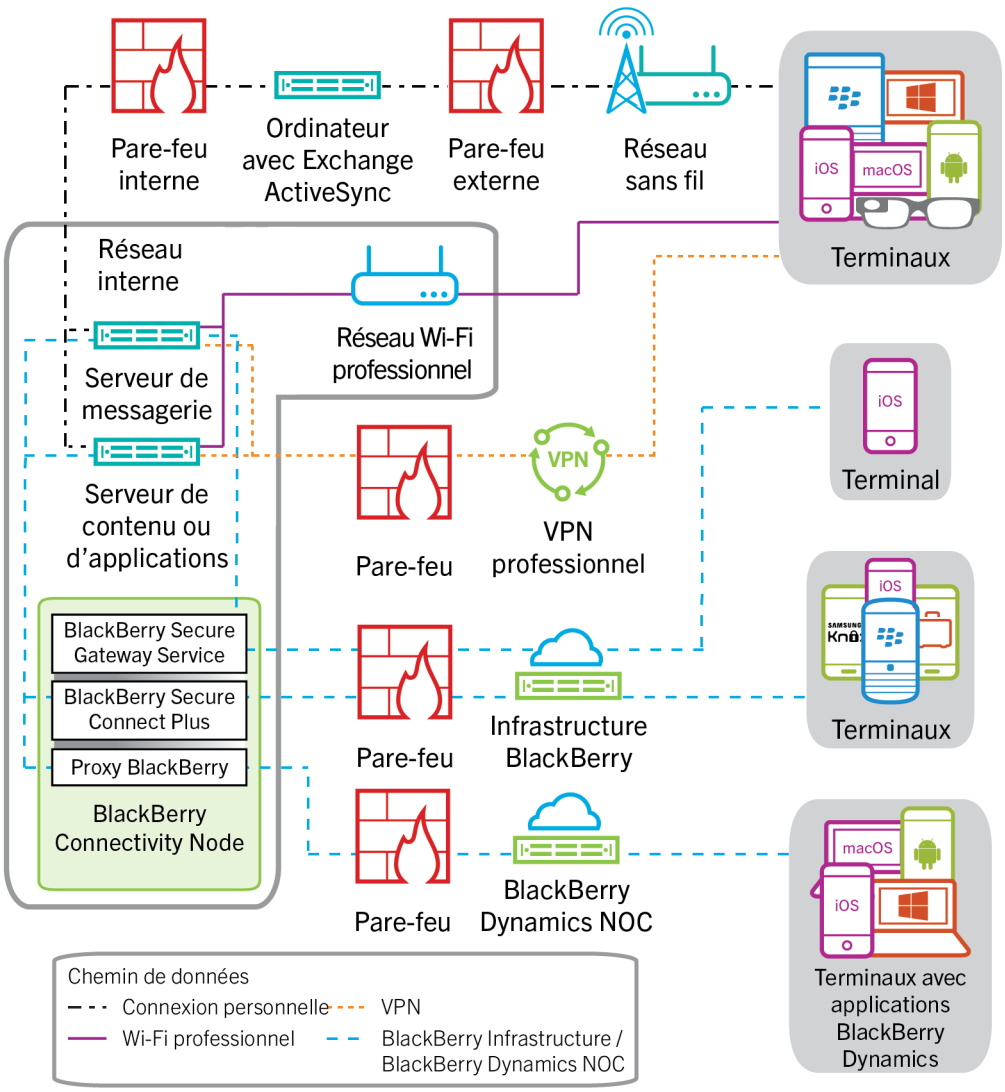
   Les étapes 4 à 6 sont répétées jusqu'à ce qu'il ne reste aucune action ou commande en attente et BlackBerry UEM Cloud répond avec une commande d'inactivité.

Envoi et réception de données professionnelles

Lorsque les utilisateurs envoient et reçoivent des données professionnelles sur un terminal, les données peuvent circuler entre le terminal et vos ressources à l'aide des connexions suivantes :

- Les terminaux peuvent utiliser une connexion directe via un réseau sans fil du terminal au serveur de messagerie, d'applications ou de contenu (par exemple un serveur Exchange ActiveSync, qui est placé dans une zone démilitarisée (DMZ) ou exposé au réseau public).
- Les terminaux peuvent utiliser une connexion directe via le VPN ou le réseau Wi-Fi professionnel de votre entreprise au serveur de messagerie, d'applications ou de contenu. Le profil VPN ou Wi-Fi du terminal peut être configuré par vous ou par les utilisateurs.
- En installant BlackBerry Connectivity Node, BlackBerry Secure Connect Plus peut établir un tunnel IP sécurisé entre les applications via BlackBerry Infrastructure sur les terminaux BlackBerry 10, iOS, Android Enterprise et Samsung Knox Workspace et le réseau de votre organisation.
- En installant BlackBerry Connectivity Node, BlackBerry Proxy peut fournir une connexion sécurisée entre les applications BlackBerry Dynamics installées sur les terminaux et le réseau de votre entreprise.
- En installant BlackBerry Connectivity Node, BlackBerry Secure Gateway peut fournir une connexion sécurisée par le biais de BlackBerry Infrastructure et BlackBerry UEM au serveur de messagerie de votre entreprise pour les terminaux iOS.

Ce diagramme illustre les chemins de données possibles.

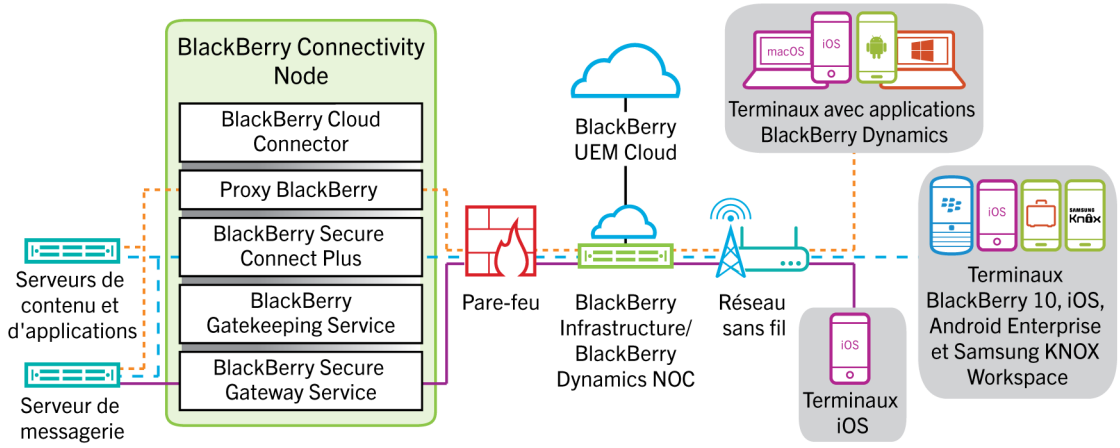

Pare-feu interne
Ordinateur avec Exchange ActiveSync
Pare-feu externe
Réseau sans fil
iOS
macOS
Terminaux
Réseau interne
Réseau Wi-Fi professionnel
Serveur de messagerie
Serveur de contenu ou d'applications
iOS
Terminal
VPN
Pare-feu
VPN professionnel
BlackBerry Secure Gateway Service
BlackBerry Secure Connect Plus
Proxy BlackBerry
BlackBerry Connectivity Node
iOS
Terminaux
Pare-feu
Infrastructure BlackBerry
Pare-feu
BlackBerry Dynamics NOC
macOS
iOS
Terminaux avec applications BlackBerry Dynamics
Chemin de données
Connexion personnelle
VPN
Wi-Fi professionnel
BlackBerry Infrastructure / BlackBerry Dynamics NOC

Envoi et réception de données professionnelles à l'aide de BlackBerry UEM Cloud et de BlackBerry Infrastructure

Si vous installez BlackBerry Connectivity Node, les terminaux peuvent se connecter aux ressources de votre entreprise via BlackBerry UEM Cloud et BlackBerry Infrastructure ou BlackBerry Dynamics NOC à l'aide des services suivants :

Service	Description
BlackBerry Secure Connect Plus	BlackBerry Secure Connect Plus est un composant BlackBerry Infrastructure qui fournit un tunnel IP sécurisé entre les applications et votre réseau d'entreprise. Pour les terminaux BlackBerry 10 et Android Enterprise, BlackBerry Secure Connect Plus fournit un tunnel sécurisé entre toutes les applications de l'espace de travail et le réseau de votre entreprise. Pour les terminaux Samsung Knox Workspace, BlackBerry Secure Connect Plus peut fournir un tunnel sécurisé entre le réseau de votre entreprise et toutes les applications professionnelles ou uniquement les applications spécifiées. 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.
BlackBerry Proxy	BlackBerry Proxy offre une connexion sécurisée entre les applications BlackBerry Dynamics installées sur les terminaux et les ressources de votre entreprise derrière le pare-feu. Il prend également en charge BlackBerry Dynamics Direct Connect, qui permet aux données d'application de contourner BlackBerry Dynamics NOC.
BlackBerry Secure Gateway	BlackBerry Secure Gateway fournit une connexion sécurisée avec le serveur de messagerie de votre entreprise par le biais de BlackBerry Infrastructure et BlackBerry UEM pour les terminaux iOS.

Le schéma suivant montre comment les terminaux peuvent se connecter aux ressources de votre organisation par le biais de BlackBerry Infrastructure et BlackBerry UEM Cloud.

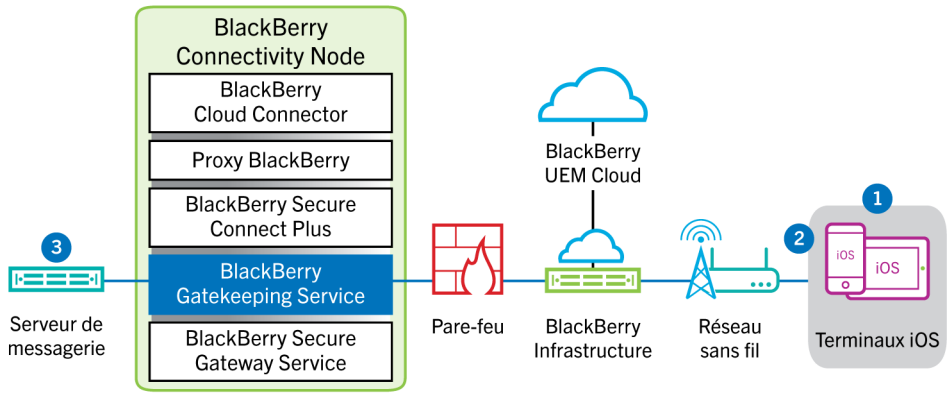


Pour en savoir plus sur l'activation de BlackBerry Secure Connect Plus, reportez-vous à la section « Activation et configuration de BlackBerry Secure Connect Plus » dans le contenu relatif à l'administration.

Pour plus d'informations sur l'activation de BlackBerry Secure Gateway, reportez-vous à la section « Protéger les données de la messagerie électronique à l'aide de BlackBerry Secure Gateway » dans le contenu relatif à l'administration.

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

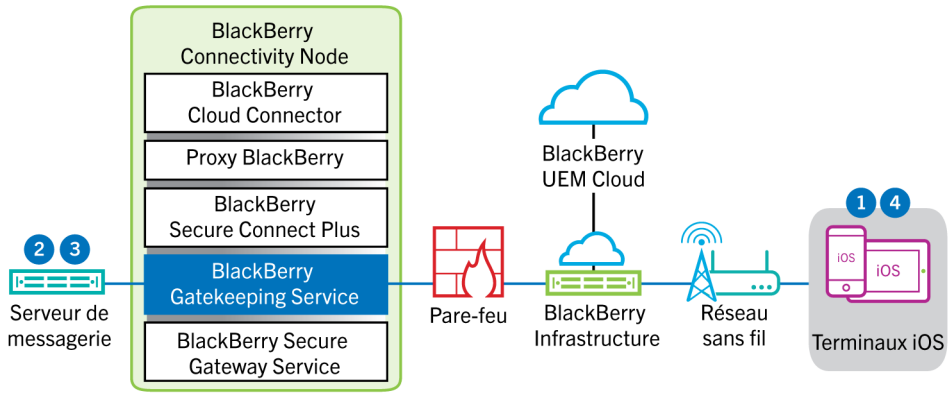
Ce flux de données décrit la façon dont les données de messagerie et de calendrier professionnelles sont acheminées des terminaux iOS vers le serveur Exchange ActiveSync à l'aide de BlackBerry Secure Gateway.



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

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

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

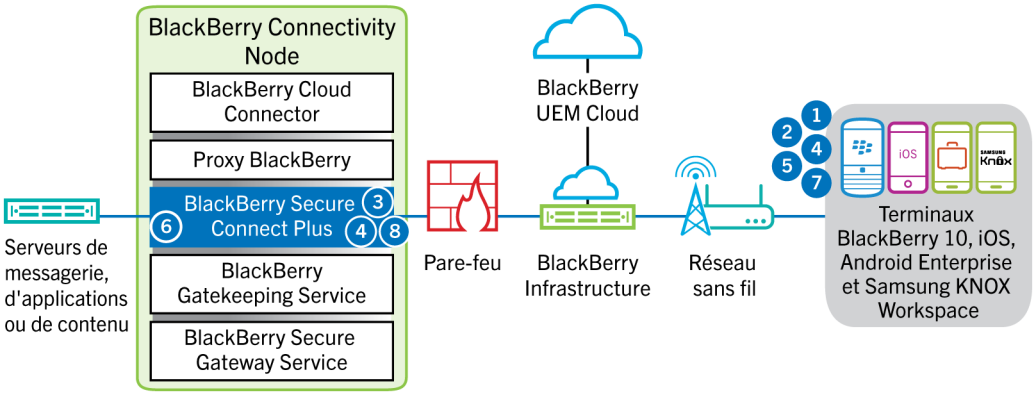


1. Le terminal adresse une demande HTTPS au serveur de messagerie pour que celui-ci l'avertisse en cas de modification des éléments dans les dossiers qui sont configurés pour se synchroniser. La demande est acheminée vers le serveur de messagerie via le canal crypté et authentifié établi entre BlackBerry Infrastructure et BlackBerry Secure Gateway.

2. En l'absence d'éléments nouveaux ou modifiés au cours de cet intervalle, le serveur de messagerie envoie un message « HTTP 200 OK » au terminal. Le terminal émet une nouvelle demande et le processus recommence.
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 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.
4. Lorsque la synchronisation est terminée, le terminal émet une autre demande pour recommencer le processus.

Flux de données : envoi et réception de données professionnelles à l'aide de 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.



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 BlackBerry 10, Android Enterprise et Samsung Knox Workspace, toutes les applications professionnelles peuvent utiliser BlackBerry Secure Connect Plus.
   - Sur les terminaux iOS, vous devez spécifier si toutes les applications ou uniquement les applications spécifiées peuvent utiliser BlackBerry Secure Connect Plus.
2. Le terminal détermine qu'un tunnel IP sécurisé est la méthode la plus directe et la plus rentable pour se connecter au serveur d'applications ou de contenu afin de récupérer les données et il envoie une demande via un tunnel TLS, via le port 443, à BlackBerry Infrastructure pour accéder à un tunnel sécurisé sur 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.

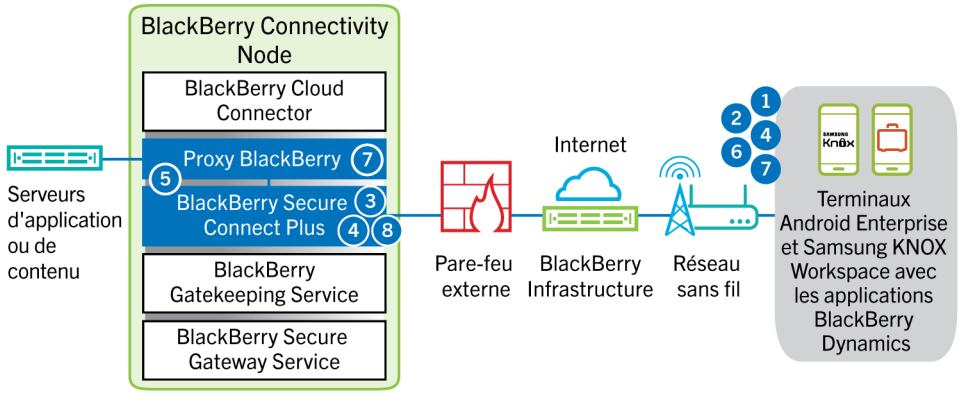
   Pour les terminaux iOS, si vous configurez un VPN par application pour BlackBerry Secure Connect Plus, le tunnel est désactivé lorsqu'aucune des applications configurées n'est en cours d'utilisation.

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.

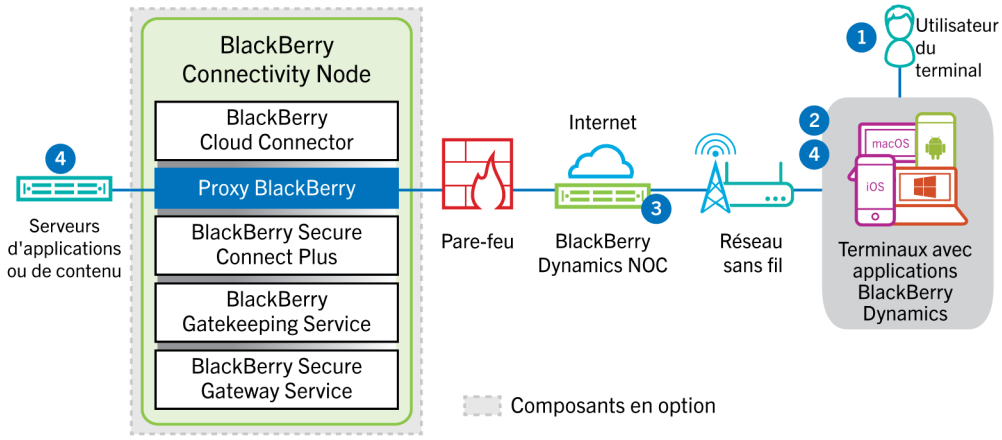
Si vous utilisez BlackBerry Secure Connect Plus avec des applications BlackBerry Dynamics sur un terminal Android Enterprise ou un terminal Samsung Knox Workspace, il est recommandé de configurer BlackBerry UEM dans le but de ne pas envoyer les données de l'application BlackBerry Dynamics à travers BlackBerry 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 et réception de données professionnelles depuis une application BlackBerry Dynamics

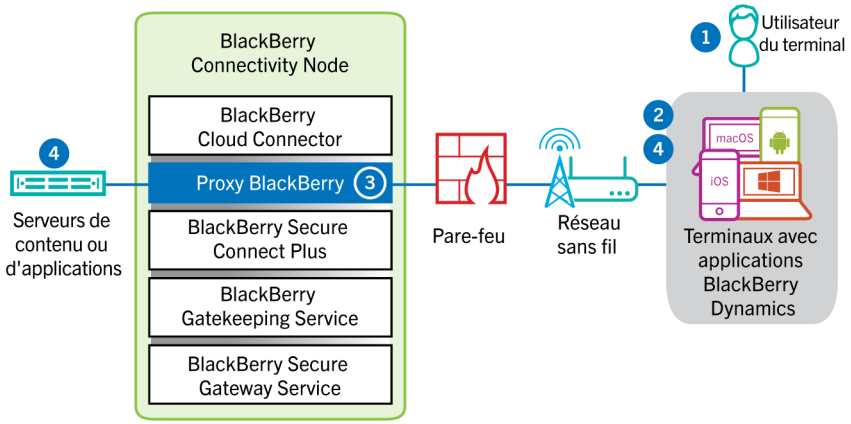
Ce flux de données décrit la façon dont les données sont acheminées lorsqu'une application BlackBerry Dynamics accède à un serveur d'applications ou de contenu de votre entreprise.



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 effectue l'une des opérations suivantes :
   a. Il communique avec BlackBerry Proxy via une connexion sécurisée pré-établie afin d'établir une connexion de bout en bout sur le port 443 entre l'application BlackBerry Dynamics et BlackBerry Proxy qui achemine les données professionnelles. Les données professionnelles sont cryptées avec une clé de session que BlackBerry Dynamics NOC ne connait pas.
   b. Si BlackBerry Connectivity Node n'est pas configuré, il communique directement avec vos serveurs d'applications ou de contenu via un port que vous avez ouvert dans le pare-feu de votre entreprise.
4. Si BlackBerry Connectivity Node est configuré, une fois que la connexion sécurisée de bout en bout est établie entre BlackBerry Dynamics NOC et BlackBerry Proxy, 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 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 Proxy.

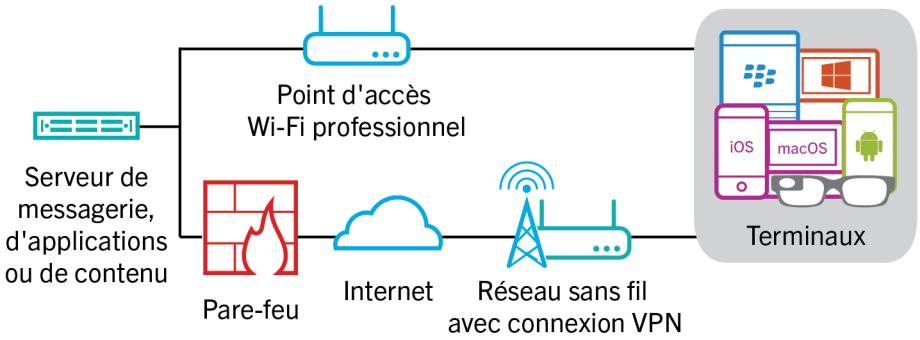


1. L'utilisateur ouvre une application BlackBerry Dynamics pour accéder aux données professionnelles.
2. L'application BlackBerry Dynamics établit une connexion TLS avec BlackBerry Proxy sur le port 17533.
3. BlackBerry Proxy s'authentifie auprès de l'application BlackBerry Dynamics. BlackBerry Proxy 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.

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.



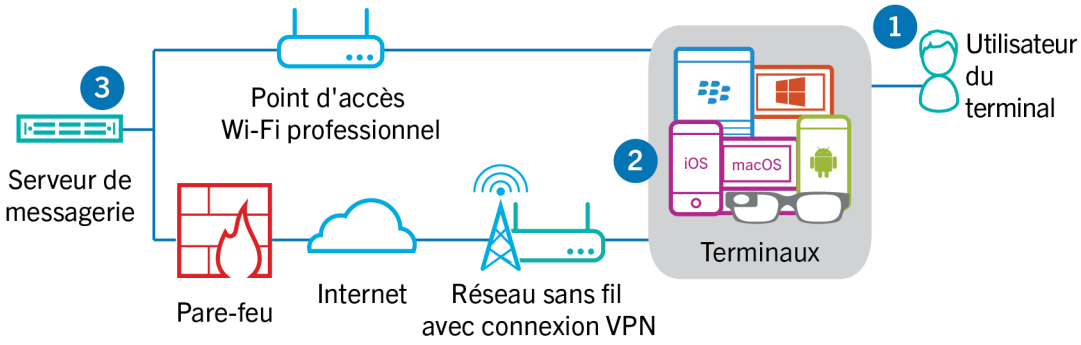
Le tableau suivant indique à quel moment les terminaux utilisent le réseau VPN ou le réseau Wi-Fi professionnel de votre entreprise pour se connecter au réseau de votre entreprise.

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

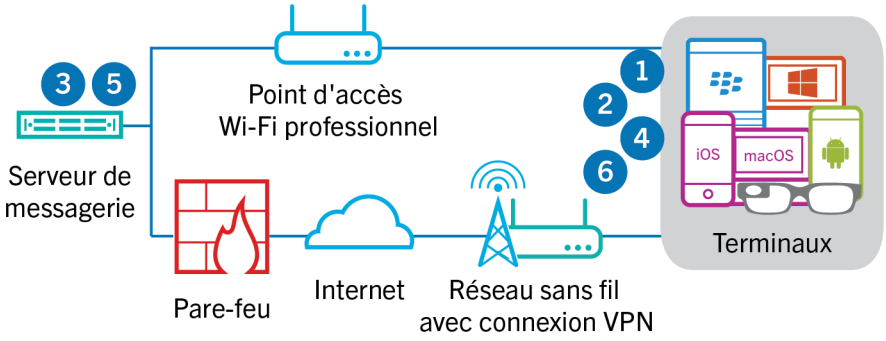
Ce flux de données décrit comment les données professionnelles de messagerie et de calendrier sont acheminées du terminal vers le serveur de messagerie sur le VPN ou réseau Wi-Fi professionnel de votre organisation via Exchange ActiveSync.



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 boite aux lettres de l'utilisateur ou transmet l'élément de messagerie au destinataire et envoie une confirmation au terminal.

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

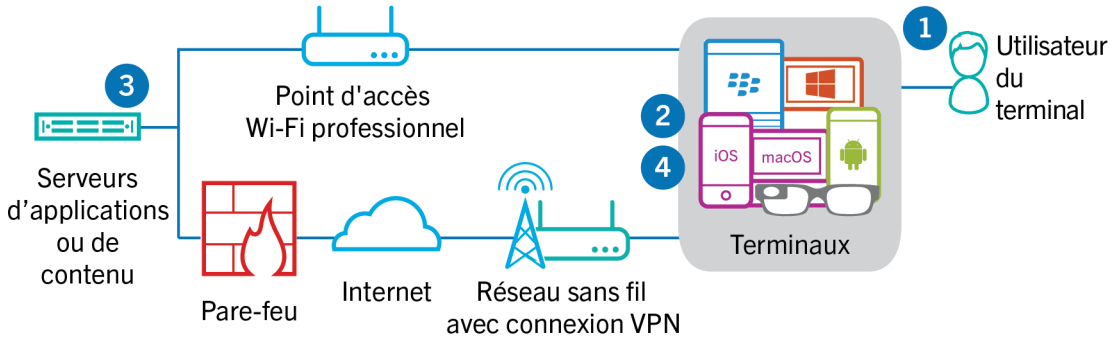
Ce flux de données décrit comment les données professionnelles de messagerie et de calendrier sont acheminées du terminal vers le serveur de messagerie sur le VPN ou réseau Wi-Fi professionnel de votre organisation via Exchange ActiveSync.



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

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

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



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

Informations juridiques

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

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

SAUF DANS LA MESURE SPÉCIFIQUEMENT INTERDITE PAR LES LOIS EN VIGUEUR DANS VOTRE JURIDICTION, TOUTES LES CONDITIONS, GARANTIES OU REPRÉSENTATIONS DE TOUTE NATURE, EXPRESSES OU TACITES, NOTAMMENT (SANS LIMITATIONS) LES CONDITIONS, GARANTIES OU REPRÉSENTATIONS DE DURABILITÉ, D'ADÉQUATION À UNE UTILISATION OU À UN BUT PARTICULIER, DE COMMERCIALISATION, DE QUALITÉ MARCHANDE, DE NON-INFRACTION, DE SATISFACTION DE LA QUALITÉ OU DE TITRE, OU RÉSULTANT D'UNE LOI, D'UNE COUTUME, D'UNE PRATIQUE OU D'UN USAGE COMMERCIAL, OU EN RELATION AVEC LA DOCUMENTATION OU SON UTILISATION, OU LA PERFORMANCE OU NON-PERFORMANCE 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 COUTS D'INDISPONIBILITÉ, LA PERTE D'UTILISATION DES PRODUITS OU SERVICES BLACKBERRY EN TOUT OU EN PARTIE, OU DE TOUT

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

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

LES LIMITATIONS, EXCLUSIONS ET CLAUSES DE NON-RESPONSABILITÉ CONTENUES DANS LES PRÉSENTES S'APPLIQUENT : (A) INDÉPENDAMMENT DE LA NATURE DE LA CAUSE D'ACTION, 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), REVENDEURS AGRÉÉS BLACKBERRY (NOTAMMENT LES FOURNISSEURS DE SERVICES) ET LEURS DIRECTEURS, EMPLOYÉS ET SOUS-TRAITANTS RESPECTIFS.

OUTRE LES LIMITATIONS ET EXCLUSIONS SUSMENTIONNÉES, EN AUCUN CAS, LES DIRECTEURS, EMPLOYÉS, AGENTS, 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