BlackBerry UEM

Configuration

12.17

Table des matières

Configurer BlackBerry UEM pour la première fois

Le tableau suivant récapitule les tâches de configuration initiales décrites dans ce guide. Utilisez ce tableau pour déterminer les tâches de configuration requises. Une fois les tâches appropriées terminées, vous êtes prêt à configurer les administrateurs, à créer et gérer des utilisateurs et des groupes, à configurer les contrôles des terminaux et à activer les terminaux.

Tâche	Description
Remplacer les certificats par défaut par des certificats approuvés	Vous pouvez remplacer les certificats autosignés par défaut utilisés par BlackBerry UEM pour authentifier la communication entre divers composants UEM et avec les terminaux.
Configurer BlackBerry UEM pour envoyer les données via un serveur proxy	Vous pouvez configurer BlackBerry UEM pour envoyer les données via un serveur proxy TCP avant d'atteindre BlackBerry Infrastructure. Vous pouvez également configurer BlackBerry UEM pour envoyer les données via un proxy HTTP avant d'atteindre BlackBerry Dynamics NOC.
Configurer des connexions via des serveurs proxy internes	Si votre entreprise utilise un serveur proxy pour établir la connexion entre les serveurs de votre réseau, vous devrez peut-être configurer les paramètres proxy côté serveur pour permettre à BlackBerry UEM Core de communiquer avec les instances à distance de la console de gestion.
Connecter BlackBerry UEM à des répertoires d'entreprise	Vous pouvez connecter BlackBerry UEM à un ou plusieurs répertoires d'entreprise, comme Microsoft Active Directory ou un répertoire LDAP, pour permettre à BlackBerry UEM d'accéder aux données des utilisateurs et de créer des comptes d'utilisateur.
Connecter BlackBerry UEM à un serveur SMTP	Si vous souhaitez que BlackBerry UEM envoie des e-mails d'activation et d'autres notifications aux utilisateurs, vous devez spécifier les paramètres de serveur SMTP que BlackBerry UEM peut utiliser.
Configurer la mise en miroir des bases de données	Pour maintenir le niveau de service de la base de données et l'intégrité des données en cas de problèmes au niveau de la base de données de BlackBerry UEM, vous pouvez installer et configurer une base de données de basculement qui fera office de sauvegarde de la base de données principale.
Connecter BlackBerry UEM à Microsoft Azure	Si vous souhaitez utiliser BlackBerry UEM pour déployer des applications iOS et Android gérées par Microsoft Intune ou si vous souhaitez gérer des applications Windows 10 dans BlackBerry UEM, connectez BlackBerry UEM à Microsoft Azure.
Obtenir et enregistrer un certificat APNs	Si vous souhaitez gérer et envoyer des données aux terminaux iOS ou macOS, vous devez vous procurer un fichier CSR signé auprès de BlackBerry, l'utiliser pour obtenir un certificat APNs auprès de Apple et enregistrer le certificat APNs auprès du domaine BlackBerry UEM.
Configurer BlackBerry UEM pour le programme d'inscription Apple	Si vous voulez utiliser la console de gestion de BlackBerry UEM pour gérer les terminaux iOS que votre entreprise a achetés auprès de Apple pour DEP, vous devez configurer cette fonctionnalité.

Tâche	Description
Configurer BlackBerry UEM pour la prise en charge des terminaux Android Enterprise	Pour prendre en charge des terminaux Android Enterprise, vous devez configurer votre domaine G Suite ou Google Cloud pour la prise en charge de fournisseurs de gestion de terminaux mobiles tiers et configurer BlackBerry UEM pour communiquer avec votre domaine G Suite ou Google Cloud.
Configurer votre réseau pour simplifier les activations Windows 10	Vous pouvez simplifier le processus d'activation des terminaux Windows 10 en modifiant la configuration de votre réseau de sorte que les utilisateurs n'aient pas besoin de saisir une adresse de serveur.
Migration d'utilisateurs, de terminaux, de groupes et d'autres données depuis un serveur source	Vous pouvez utiliser la console de gestion pour migrer les utilisateurs, les terminaux, les groupes et autres données depuis un BlackBerry UEM ou Good Control source sur site (autonome).
Configurer les paramètres BlackBerry Dynamics	Vous pouvez configurer les paramètres qui sont spécifiques aux applications BlackBerry Proxy et BlackBerry Dynamics.
Intégrer BlackBerry UEM avec Cisco ISE	Vous pouvez créer une connexion entre Cisco ISE et BlackBerry UEM de sorte que Cisco ISE puisse récupérer des données de terminaux de BlackBerry UEM et appliquer des stratégies de contrôle d'accès au réseau.

Droits d'administrateur requis pour configurer BlackBerry UEM

Pour effectuer les tâches de configuration décrites dans ce guide, connectez-vous à la console de gestion à l'aide du compte administrateur que vous avez créé lors de l'installation de BlackBerry UEM. Si vous souhaitez que plusieurs personnes soient habilitées à effectuer des tâches de configuration, vous pouvez créer d'autres comptes d'administrateur. Pour en savoir plus sur la création de comptes d'administrateur, consultez le contenu relatif à l'administration.

Si vous créez d'autres comptes d'administrateur pour configurer BlackBerry UEM, vous devez attribuer le rôle d'administrateur de sécurité aux comptes. Par défaut le rôle d'administrateur de sécurité possède les autorisations nécessaires pour effectuer n'importe quelle tâche de configuration.

Obtention et activation des licences

Pour activer les terminaux, vous devez obtenir les licences nécessaires. Vous devez obtenir les licences avant de suivre les instructions de configuration de ce guide, et avant d'ajouter les comptes d'utilisateur.

Pour plus d'informations sur les options de licences et les fonctionnalités et produits pris en charge par les différents types de licence, consultez le contenu relatif aux licences.

Modification des certificats BlackBerry UEM

Lorsque vous installez BlackBerry UEM, l'application d'installation génère plusieurs certificats autosignés qui sont utilisés pour authentifier les communications entre composants UEM et avec les terminaux. Vous pouvez modifier les certificats si la stratégie de sécurité de votre organisation exige que les certificats soient signés par l'autorité de certification de l'organisation, ou si vous voulez utiliser des certificats émis par une autorité de certification déjà approuvée par les terminaux et les navigateurs.

Remarque : Si des problèmes se produisent lorsque vous modifiez un certificat, la communication entre les composants UEM et entre UEM et les terminaux risque d'être perturbée. Si vous choisissez de modifier les certificats, planifiez et testez les modifications avec soin.

Vous pouvez modifier les certificats suivants :

Certificat	Description
Certificat SSL pour consoles	Un certificat SSL que la console de gestion BlackBerry UEM et BlackBerry UEM Self-Service utilisent pour l'authentification des navigateurs. Si vous configurez la haute disponibilité, le certificat doit avoir le nom du domaine BlackBerry UEM. Vous trouverez le nom du domaine BlackBerry UEM dans la console de gestion, sous Paramètres > Infrastructure > Instances.
Certificats SSL pour BlackBerry Web Services	Un certificat SSL que BlackBerry Web Services utilise pour l'authentification des applications qui utilisent les API BlackBerry Web Services pour gérer BlackBerry UEM. Si vous configurez la haute disponibilité, le certificat doit avoir le nom du domaine BlackBerry UEM. Vous trouverez le nom du domaine BlackBerry UEM dans la console de gestion, sous Paramètres > Infrastructure > Instances.
Certificat de signature de profil Apple	Un certificat que BlackBerry UEM utilise pour signer le profil MDM que les utilisateurs doivent accepter lorsqu'ils activent des terminaux iOS. Si vous utilisez un certificat signé par une autorité de certification, vérifiez qu'un certificat racine pour l'autorité de certification est installé sur les terminaux iOS des utilisateurs avant l'activation.
Certificat SSL pour les applications BlackBerry Dynamics	Certificat SSL utilisé par BlackBerry Dynamics Launcher pour établir un canal de communication sécurisé avec BlackBerry UEM. Les applications BlackBerry Dynamics qui incluent le système intégré BlackBerry Dynamics Launcher peuvent présenter le certificat à BlackBerry UEM pour l'authentification auprès du serveur.
Certificat pour les serveurs BlackBerry Dynamics	Un certificat SSL qui permet d'authentifier les connexions entre BlackBerry UEM et BlackBerry Proxy.

Certificat	Description
Certificat destiné à la gestion des applications	Certificat SSL utilisé pour l'authentification entre BlackBerry UEM et les applications BlackBerry Dynamics . L'autorité de certification racine pour ce certificat est stockée dans la liste des certificats de confiance sur le terminal. Lorsque le serveur s'authentifie auprès du terminal, il présente ce certificat au terminal pour validation. Si vous modifiez ce certificat et que la modification prend effet avant que BlackBerry UEM ne pousse le certificat vers toutes les applications BlackBerry Dynamics, toute application qui n'aura pas reçu le certificat devra être réactivée.
Certificat pour Direct Connect	Certificat SSL utilisé pour l'authentification entre un serveur BlackBerry Proxy configuré pour des applications BlackBerry Dynamics Direct Connect et BlackBerry Dynamics sur les terminaux de l'utilisateur final. Lorsque vous mettez à jour ce certificat, la nouvelle version est toujours envoyée aux terminaux via une connexion non-BlackBerry Dynamics Direct Connect. Tous les terminaux ou conteneurs qui ne sont pas en ligne au moment de la modification recevront la mise à jour lorsqu'ils seront de nouveau en ligne. La mise à jour de ce certificat doit être effectuée simultanément sur le serveur BlackBerry UEM et sur toutes les appliances réseau applicables. Pour plus d'informations sur Direct Connect, reportez-vous à la section Configuration de Direct Connect avec BlackBerry UEM

Considérations pour la modification des certificats BlackBerry Dynamics

Si vous voulez modifier des certificats SSL BlackBerry Dynamics, gardez les considérations suivantes à l'esprit. Si des problèmes se produisent lorsque vous modifiez un certificat, la communication entre les composants BlackBerry UEM et entre les applications BlackBerry UEM et BlackBerry Dynamics risque d'être perturbée. Planifiez et testez les modifications du certificat avec soin.

Ajouter de nouveaux certificats à n'importe quel équipement périphérique

Si vous avez ajouté des certificats BlackBerry Dynamics à un équipement périphérique sur votre réseau, ajoutez le nouveau certificat à l'équipement périphérique avant de l'ajouter à BlackBerry UEM

Mettre à jour des applications BlackBerry Dynamics

Si vous remplacez le certificat BlackBerry Dynamics destiné à la gestion des applications ou Direct Connect, assurez-vous que les utilisateurs des applications BlackBerry Dynamics disposent des versions les plus récentes avant de remplacer le certificat.

Les applications BlackBerry Dynamics développées par votre entreprise doivent être conçues avec la version 3.2 ou ultérieure de BlackBerry Dynamics SDK. Les applications plus anciennes ne peuvent pas recevoir le nouveau certificat depuis BlackBerry UEM.

Les applications BlackBerry Dynamics doivent être ouvertes pour recevoir un certificat

Les utilisateurs doivent ouvrir une application BlackBerry Dynamics pour recevoir un certificat de BlackBerry UEM. Si vous remplacez le certificat BlackBerry Dynamics destiné à la gestion des applications ou Direct Connect et que la modification prend effet avant que BlackBerry UEM ne pousse le certificat vers toutes les applications BlackBerry Dynamics, toute application qui n'aura pas reçu le certificat devra être réactivée. Les applications ne reçoivent pas de certificats lorsqu'elles sont suspendues sur les terminaux iOS ou lorsque les terminaux Android sont en mode Doze.

Assurer l'accès à BlackBerry Connectivity Node

Si toutes les instances de BlackBerry Proxy sont inaccessibles par BlackBerry UEM lorsque les certificats BlackBerry Dynamics sont remplacés, les applications BlackBerry Dynamics ne seront pas en mesure de se connecter à ces instances une fois le certificat remplacé.

Programmer la modification des certificats avec soin

Si vous remplacez le certificat des serveurs BlackBerry Dynamics, choisissez une période de faible activité pour redémarrer les serveurs.

Laissez suffisamment de temps aux nouveaux certificats pour qu'ils se propagent aux applications BlackBerry ProxyBlackBerry Dynamics. Si vous remplacez uniquement le certificat pour les serveurs BlackBerry Dynamics, patientez au moins 10 minutes avant que le serveur redémarre.

Si vous remplacez le certificat BlackBerry Dynamics destiné à la gestion des applications ou Direct Connect, il est recommandé que le délai jusqu'à la date d'entrée en vigueur soit plus long que celui défini dans le paramètre de vérification Heure de la dernière prise de contact dans le profil de conformité.

Si vous remplacez le certificat BlackBerry Dynamics destiné à la gestion des applications et Direct Connect, définissez des délais d'entrée en vigueur espacés d'au moins 30 minutes. Si vous avez un grand nombre d'utilisateurs et d'applications BlackBerry Dynamics, vous devez patienter plus de 30 minutes entre chaque certificat.

Modification d'un certificat BlackBerry UEM

Avant de commencer :

- Obtenez un certificat signé par une autorité de certification approuvée. Le format du certificat doit être compatible avec la base de stockage de clés (.pfx, .pkcs12).
- Si vous remplacez le certificat BlackBerry Dynamics destiné à la gestion des applications ou Direct Connect, assurez-vous que les utilisateurs des applications BlackBerry Dynamics disposent des versions les plus récentes.

1. Sur la barre de menus, cliquez sur **Paramètres > Infrastructure > Certificats de serveur**.
2. Dans la section relative au certificat que vous souhaitez remplacer, cliquez sur **Afficher les détails**.
3. Cliquez sur **Remplacer le certificat**.
4. Accédez au fichier de certificat et sélectionnez-le.
5. Saisissez un mot de passe de chiffrement pour le certificat.
6. Si vous remplacez le certificat pour les serveurs BlackBerry Dynamics, spécifiez si vous voulez que BlackBerry UEM redémarre pour prendre en compte la modification.

   Il est recommandé de choisir une période de faible activité pour redémarrer les serveurs.

7. Si vous remplacez le certificat BlackBerry Dynamics destiné à la gestion des applications ou Direct Connect, précisez la date effective du changement de certificat.

   Il est recommandé que la date effective soit ultérieure à la date indiquée dans le paramètre de vérification Heure de la dernière prise de contact dans le profil de conformité. Si vous modifiez plus d'un certificat, il est recommandé de définir des délais d'entrée en vigueur espacés d'au moins 30 minutes. Notez qu'il n'y a pas d'invite pour la date effective lorsque le nouveau certificat est émis par la même autorité de certification que le certificat précédent. Pour en savoir plus, rendez-vous sur le site Web support.blackberry.com/community pour consulter l'article 74167.
8. Cliquez sur **Remplacer**.

À la fin :

- Si vous avez remplacé l'un des certificats sur l'onglet **Certificats de serveur**, redémarrez le service BlackBerry UEM Core sur tous les serveurs. Il est recommandé de choisir une période de faible activité pour redémarrer les serveurs.
- Pour les certificats sur l'onglet Certificats BlackBerry Dynamics, vous pouvez cliquer sur **Rétablir les valeurs par défaut** pour revenir à l'utilisation d'un certificat autosigné.
- Sur l'onglet Certificats BlackBerry Dynamics, vous pouvez décocher les cases **Approuver l'autorité de certification BlackBerry UEM** et **Approuver l'autorité de certification BlackBerry Dynamics** si vous n'avez plus besoin d'approuver les certificats autosignés. Vous pouvez décocher les cases **Approuver l'autorité de certification BlackBerry Dynamics** uniquement si vous avez remplacé tous les certificats sur l'onglet Certificats BlackBerry Dynamics.
- Si les applications BlackBerry Dynamics cessent de communiquer après avoir modifié les certificats, vérifiez si elles sont à jour, puis demandez aux utilisateurs de les réactiver.

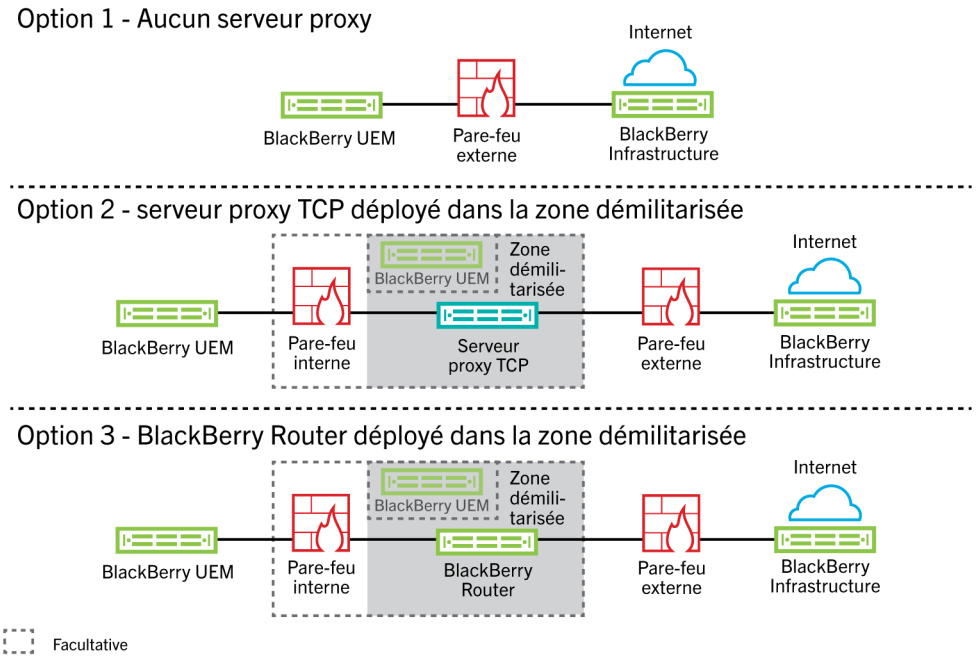
Configuration de BlackBerry UEM pour envoyer des données via un serveur proxy

Vous pouvez configurer BlackBerry UEM pour envoyer les données via un serveur proxy TCP avant d'atteindre BlackBerry Infrastructure.

Par défaut, BlackBerry UEM se connecte directement à BlackBerry Infrastructure à l'aide du port 3101. Si la stratégie de sécurité de votre organisation empêche les systèmes internes de se connecter directement à Internet, vous pouvez installer un serveur proxy TCP. Le serveur proxy TCP fait office d'intermédiaire entre BlackBerry UEM et BlackBerry Infrastructure.

Vous pouvez installer un serveur proxy en dehors du pare-feu de votre organisation dans une zone démilitarisée. L'installation d'un serveur proxy TCP dans une zone démilitarisée offre un niveau de sécurité plus élevé pour BlackBerry UEM. Seul le serveur proxy se connecte à BlackBerry UEM en dehors du pare-feu. Toutes les connexions vers BlackBerry Infrastructure entre BlackBerry UEM et des terminaux passent par le serveur proxy.

Ce schéma illustre les options suivantes d'envoi des données via un serveur proxy vers BlackBerry Infrastructure : aucun serveur proxy, un serveur proxy TCP déployé dans une zone démilitarisée et BlackBerry Router déployé dans une zone démilitarisée.



Envoi de données via un serveur proxy TCP vers BlackBerry Infrastructure

Vous pouvez configurer un serveur proxy TCP transparent pour le service BlackBerry UEM Core. Ce service requiert une connexion sortante et différents ports peuvent être configurés pour eux. Vous ne pouvez pas installer ou configurer plusieurs serveurs proxy TCP transparents pour chaque service.

Vous pouvez configurer plusieurs serveurs proxy TCP configurés avec SOCKS v5 (sans authentification) pour la connexion à BlackBerry UEM. Plusieurs serveurs proxy TCP configurés avec SOCKS v5 (sans authentification) peuvent fournir une assistance lorsqu'un serveur proxy actif ne fonctionne pas correctement.

Vous ne pouvez configurer qu'un seul port d'écoute pour toutes les instances de service SOCKS v5. Si vous configurez plusieurs serveurs proxy TCP avec SOCKS v5, chaque serveur doit partager le même port d'écoute proxy.

Comparaison des proxys TCP

Proxy	Description
Proxy TCP transparent	• Intercepte la communication normale au niveau de la couche réseau sans qu'aucune configuration particulière ne soit nécessaire de la part du client • Ne nécessite aucune configuration du navigateur client • Généralement situé entre le client et Internet • Exécute certaines fonctions de passerelle ou de routeur • Souvent utilisé pour appliquer une stratégie d'utilisation acceptable • Couramment utilisé par les FAI de certains pays pour économiser de la bande passante en amont et améliorer les temps de réponse des clients grâce à la mise en cache
Proxy SOCKS v5	• Protocole Internet permettant de gérer le trafic Internet via un serveur proxy • Peut être géré avec pratiquement n'importe quelle application TCP/UDP, comme les navigateurs et clients FTP prenant en charge SOCKS • Peut être une bonne solution pour l'anonymat et la sécurité Internet • Achemine les paquets réseau entre un client et un serveur via un serveur proxy • Peut fournir une authentification grâce à laquelle seuls les utilisateurs autorisés peuvent accéder à un serveur • Redirige les connexions TCP vers une adresse IP arbitraire • Peut rendre anonyme les protocoles UDP et TCP comme HTTP

Configurer BlackBerry UEM pour utiliser un serveur proxy TCP transparent

Avant de commencer : Installer un serveur proxy TCP transparent compatible dans le domaine BlackBerry UEM.

1. Sur la barre de menus, cliquez sur **Paramètres > Infrastructure > BlackBerry Router et proxy**.
2. Sélectionnez l'option **Serveur proxy**.
3. Effectuez l'une des tâches suivantes :

Tâche	Étapes
Acheminer les données TCP via un serveur proxy TCP.	Dans les champs **BlackBerry UEM Core, BlackBerry Secure Gateway Service**, saisissez le FQDN ou l'adresse IP et le numéro de port du serveur proxy. Chaque champ requiert une seule valeur.
Acheminer le trafic BlackBerry Secure Connect Plus via un serveur proxy TCP	Dans les champs **BlackBerry Secure Connect Plus**, saisissez le FQDN ou l'adresse IP et le numéro de port du serveur proxy. Chaque champ requiert une seule valeur.

4. Cliquez sur **Enregistrer**.

Activer SOCKS v5 sur un serveur proxy TCP

Avant de commencer : Installez un serveur proxy TCP compatible avec SOCKS v5 (sans authentification) dans le domaine BlackBerry UEM.

1. Sur la barre de menus, cliquez sur **Paramètres > Infrastructure > BlackBerry Router et proxy**.
2. Sélectionnez l'option **Serveur proxy**.
3. Cochez la case **Activer SOCKS v5**.
4. Cliquez sur +.
5. Dans le champ **Adresse du serveur**, saisissez l'adresse IP ou le nom d'hôte du serveur proxy SOCKS v5.
6. Cliquez sur **Ajouter**.
7. Répétez les étapes 1 et 6 pour chaque serveur proxy SOCKS v5 que vous souhaitez configurer.
8. Dans le champ **Port**, saisissez le numéro de port.
9. Cliquez sur **Enregistrer**.

Configuration de connexions par le biais de serveurs proxy internes

Si votre entreprise utilise un serveur proxy pour établir la connexion entre les serveurs de votre réseau, vous devrez peut-être configurer les paramètres proxy côté serveur pour permettre à BlackBerry UEM Core de communiquer avec la console de gestion BlackBerry UEM (si elle est installée sur un ordinateur distinct). Vous devrez également configurer les paramètres proxy côté serveur pour permettre à BlackBerry UEM de communiquer avec d'autres services internes, tels que les autorités de certification et les serveurs hébergeant des applications Push qui envoient les données.

Les paramètres proxy côté serveur ne s'appliquent pas aux connexions sortantes. Pour plus d'informations sur la configuration de BlackBerry UEM de manière à utiliser un serveur proxy TCP, reportez-vous à la section Configuration de BlackBerry UEM pour envoyer des données via un serveur proxy.

Configurer les paramètres proxy côté serveur

Avant de commencer : Assurez-vous de disposer de l'URL du fichier PAC ou du nom d'hôte et du numéro de port et de tout autre paramètre nécessaire pour vous connecter au serveur proxy.

1. Sur la barre de menus, cliquez sur **Paramètres > Infrastructure > Proxy côté serveur**.
2. Si la plupart des serveurs ou tous les serveurs qui composent votre installation BlackBerry UEM doivent se connecter à un serveur proxy, exécutez les actions suivantes pour définir les paramètres globaux de proxy côté serveur :
   a) Sous **Paramètres globaux de proxy côté serveur**, dans la liste **Type**, sélectionnez **Configuration PAC** ou **Configuration manuelle**
   b) Spécifiez les paramètres requis par le serveur proxy et cliquez sur **Enregistrer**.
3. Si un ou plusieurs serveurs nécessitent des paramètres de proxy différents des paramètres globaux, effectuez les actions suivantes pour définir les paramètres de proxy du serveur :
   a) Sous le nom du serveur, dans la liste **Type**, sélectionnez **Aucun**, **Configuration PAC** ou **Configuration manuelle**.
   b) Si vous avez sélectionné **Configuration PAC** ou **Configuration manuelle**, spécifiez les paramètres requis par le serveur proxy.
   c) Cliquez sur **Enregistrer**.

Connexion à vos annuaires d'entreprise

Vous pouvez connecter BlackBerry UEM à l'annuaire de votre entreprise pour lui permettre d'accéder à la liste des utilisateurs de votre entreprise. Vous pouvez connecter BlackBerry UEM à plusieurs répertoires et ceux-ci peuvent être une combinaison Microsoft Active Directory et LDAP.

Une fois votre répertoire d'entreprise connecté, vous pouvez bénéficier des fonctionnalités suivantes :

- Vous pouvez créer des comptes d'utilisateur dans BlackBerry UEM en utilisant les données d'utilisateur de l'annuaire, et BlackBerry UEM peut authentifier les administrateurs pour la console de gestion et les utilisateurs pour BlackBerry UEM Self-Service.
- Vous pouvez lier les groupes d'annuaires d'entreprise à des groupes BlackBerry UEM pour organiser les utilisateurs de BlackBerry UEM tels qu'ils sont organisés dans votre annuaire d'entreprise. Reportez-vous à la section Activer les groupes liés par annuaire.
- Vous pouvez activer l'intégration pour des groupes spécifiques de votre annuaire d'entreprise afin de créer automatiquement des utilisateurs de BlackBerry UEM. Si vous activez l'intégration, vous pouvez également configurer la suppression afin de supprimer des données ou comptes d'utilisateur lorsque des utilisateurs sont supprimés des groupes de votre répertoire d'entreprise. Reportez-vous à la section Activer l'intégration.

Si vous ne connectez pas BlackBerry UEM à un répertoire d'entreprise, vous pouvez manuellement créer des comptes utilisateur locaux et authentifier les administrateurs à l'aide de l'authentification par défaut.

Pour connecter BlackBerry UEM à votre annuaire d'entreprise, effectuez les opérations suivantes :

Étape	Action
1	Créez une connexion à une instance Microsoft Active Directory ou à un annuaire LDAP. Si votre environnement inclut une forêt de ressources, consultez la section Configuration de l'authentification Microsoft Active Directory dans un environnement qui inclut des boîtes aux lettres Exchange liées.
2	Si vous le souhaitez, activez les groupes liés par répertoire.
3	Si vous le souhaitez, activez l'intégration.
4	Si vous le souhaitez, ajoutez un calendrier de synchronisation.

Configuration de l'authentification Microsoft Active Directory dans un environnement qui inclut des boîtes aux lettres Exchange liées

Dans un modèle de forêt de ressources, le serveur Microsoft Exchange est situé dans une forêt (la forêt de ressources) et les comptes utilisateur individuels sont situés dans des forêts de comptes. Si l'environnement de votre organisation inclut une forêt de ressources dédiée à l'exécution de Microsoft Exchange, vous pouvez configurer l'authentification Microsoft Active Directory pour les comptes d'utilisateurs situés dans des forêts de compte approuvées.

S'il existe une forêt de ressources Exchange dans l'environnement de votre organisation, vous devez configurer BlackBerry UEM pour qu'il se connecte à cette forêt de ressources. Vous devez créer une boîte aux lettres dans la forêt de ressources pour chaque compte d'utilisateur, puis associer ces boîtes aux lettres aux comptes d'utilisateur. Lorsque vous associez les boites aux lettres de la forêt de ressources à des comptes d'utilisateur des forêts de comptes, les comptes d'utilisateur obtiennent l'accès complet aux boites aux lettres et les comptes d'utilisateur sont connectés au serveur Microsoft Exchange. BlackBerry UEM utilise les boîtes aux lettres pour rechercher les comptes d'utilisateur dans les domaines individuels.

Afin d'authentifier les utilisateurs qui se connectent à BlackBerry UEM, BlackBerry UEM doit lire les informations utilisateur qui sont stockées sur les serveurs de catalogue global qui font partie de la forêt de ressources. Vous devez créer un compte Microsoft Active Directory pour BlackBerry UEM qui est situé dans un domaine Windows faisant partie de la forêt de ressources. Lorsque vous créez la connexion au répertoire, vous indiquez le domaine Windows, le nom d'utilisateur et le mot de passe du compte Microsoft Active Directory et, si nécessaire, les noms des serveurs de catalogue global que BlackBerry UEM peut utiliser.

Pour plus d'informations, rendez-vous sur technet.microsoft.com pour consulter l'article *Gérer les boites aux lettres liées*.

Se connecter à une instance de Microsoft Active Directory

Avant de commencer : Créez un compte Microsoft Active Directory utilisable par BlackBerry UEM. Le compte doit être conforme aux exigences suivantes :

- Il doit se trouver dans un domaine Windows qui fait partie de la forêt Microsoft Exchange.
- Il doit avoir l'autorisation d'accéder au conteneur d'utilisateurs et de lire les objets utilisateur stockés sur les serveurs de catalogue global de la forêt Microsoft Exchange.
- Le mot de passe doit être configuré pour ne pas expirer et ne doit pas être modifié lors de la connexion suivante.
- Si vous avez configuré l'authentification unique, la délégation contrainte doit être configurée pour le compte.
- Le serveur UEM doit également être joint au domaine Active Directory.

1. Sur la barre de menus, cliquez sur **Paramètres > Intégration externe > Répertoire d'entreprise**.
2. Cliquez sur **Ajouter une connexion Microsoft Active Directory**.
3. Dans le champ **Nom de la connexion au répertoire**, saisissez le nom de la connexion au répertoire.
4. Dans le champ **Nom d'utilisateur**, saisissez le nom d'utilisateur du compte Microsoft Active Directory.
5. Dans le champ **Domaine**, saisissez le nom du domaine Windows qui fait partie de la forêt Microsoft Exchange au format DNS (par exemple : exemple.com).
6. Dans le champ **Mot de passe**, saisissez le mot de passe du compte.
7. Dans la liste déroulante **Sélection du centre de distribution clé Kerberos**, effectuez l'une des opérations suivantes :
   - Pour autoriser BlackBerry UEM à détecter automatiquement les centres de distribution clés (KDC), cliquez sur **Automatique**.
   - Pour spécifier la liste de KDC à utiliser pour l'authentification de BlackBerry UEM, cliquez sur **Manuel**. Dans le champ **Noms des serveurs**, saisissez le nom du contrôleur de domaine KDC au format DNS (par exemple, kdc01.exemple.com). Si vous le souhaitez, ajoutez le numéro de port utilisé par le contrôleur de domaine (par exemple kdc01.exemple.com:88). Cliquez sur + pour spécifier des contrôleurs de domaine KDC supplémentaires que BlackBerry UEM doit utiliser.
8. Dans la liste déroulante **Sélection du catalogue global**, effectuez l'une des opérations suivantes :
   - Si vous souhaitez que BlackBerry UEM détecte automatiquement les serveurs de catalogue global, cliquez sur **Automatique**.

- Pour spécifier la liste de serveurs de catalogue global que BlackBerry UEM doit utiliser, cliquez sur **Manuel**. Dans le champ **Noms des serveurs**, saisissez le nom DNS du serveur de catalogue global auquel vous souhaitez que BlackBerry UEM accède (par exemple : catalogueglobal01.exemple.com). Si vous le souhaitez, ajoutez le numéro de port utilisé par le serveur de catalogue global (par exemple, globalcatalog01.com:3268). Cliquez sur + pour spécifier d'autres serveurs.

9. Cliquez sur **Continuer**.
10. Dans le champ **Base de recherche du catalogue global**, effectuez l'une des opérations suivantes :
    - Pour permettre à BlackBerry UEM d'effectuer des recherches dans tout le catalogue global, laissez le champ vide.
    - Pour désigner les comptes d'utilisateur que BlackBerry UEM peut authentifier, saisissez le nom distinctif du conteneur d'utilisateurs (par exemple, OU=sales,DC=example,DC=com).
11. Si vous voulez activer la prise en charge de groupes globaux, dans la liste déroulante **Prise en charge des groupes globaux**, cliquez sur **Oui**.

    Si vous voulez utiliser des groupes globaux pour l' intégration, vous devez sélectionner **Oui**. Pour configurer un domaine de groupe global, dans la section **Liste des domaines de groupes globaux**, cliquez sur +. Dans le champ **Domaine**, sélectionnez le domaine à ajouter. La sélection par défaut pour le champ **Spécifier le nom d'utilisateur et le mot de passe ?** est Non. Si vous conservez cette sélection par défaut, le nom d'utilisateur et le mot de passe pour la connexion de la forêt sont utilisés. Si vous sélectionnez Oui, vous devez fournir des informations d'identification valides pour un compte Microsoft Active Directory dans le domaine que vous avez sélectionné. Dans le champ **Sélection KDC**, vous pouvez sélectionner Automatique pour permettre à BlackBerry UEM de découvrir automatiquement les centres de distribution clés ou Manuel pour spécifier la liste de KDC que BlackBerry UEM peut utiliser pour l'authentification. Cliquez sur **Ajouter**.
12. Si votre environnement comprend une forêt de ressources Microsoft Exchange et si vous voulez activer la prise en charge de boites aux lettres Microsoft Exchange liées, dans la liste déroulante **Prise en charge des boites aux lettres Microsoft Exchange liées**, cliquez sur **Oui**.

    Pour configurer le compte Microsoft Active Directory de chacune des forêts auxquelles vous souhaitez que BlackBerry UEM ait accès, dans la section **Liste des forêts de comptes**, cliquez sur +. Spécifiez le nom du domaine de l'utilisateur (l'utilisateur peut appartenir à n'importe quel domaine de la forêt de comptes) et le nom d'utilisateur et le mot de passe. Si nécessaire, spécifiez les KDC dans lesquels BlackBerry UEM doit effectuer la recherche. Si nécessaire, spécifiez les serveurs de catalogue global auxquels BlackBerry UEM doit accéder. Cliquez sur **Ajouter**.
13. Pour activer l'authentification unique, cochez la case **Activer l'authentification unique Windows**. Pour en savoir plus sur l'identification unique, reportez-vous au contenu relatif à l'administration. L'identification unique est prise en charge uniquement dans un environnement sur site.
14. Pour synchroniser plus d'informations sur les utilisateurs à partir du répertoire de votre entreprise, cochez la case **Synchroniser les informations complémentaires sur l'utilisateur**. Les informations supplémentaires comprennent le nom de l'entreprise et le téléphone du bureau.
15. Cliquez sur **Enregistrer**.
16. Cliquez sur **Fermer**.

À la fin : Si vous souhaitez ajouter un calendrier de synchronisation du répertoire, reportez-vous à Ajouter un calendrier de synchronisation.

Se connecter à un annuaire LDAP

Avant de commencer :

- pour BlackBerry UEM, créez un compte LDAP situé dans l'annuaire LDAP qui convient. Le compte doit être conforme aux exigences suivantes :

    - Le compte doit avoir l'autorisation de lire tous les utilisateurs de l'annuaire.
    - Le mot de passe du compte n'expire jamais et il n'est pas nécessaire que l'utilisateur modifie le mot de passe lors de la connexion suivante.
- Si la connexion LDAP est chiffrée SSL, vérifiez que vous disposez du certificat de serveur correspondant à la connexion LDAP et que le serveur LDAP prend en charge TLS 1.2. Si SSL est activé, la connexion LDAP à BlackBerry UEM doit utiliser TLS 1.2.
- Vérifiez les valeurs d'attribut LDAP qu'utilise votre organisation (les étapes ci-dessous donnent des exemples de valeurs d'attribut typiques). Vous devez spécifier les valeurs d'attribut LDAP à partir de l'étape 11.

1. Sur la barre de menus, cliquez sur **Paramètres > Intégration externe > Annuaire d'entreprise**.
2. Cliquez sur **Ajouter une connexion LDAP**.
3. Dans le champ **Nom de connexion du répertoire**, saisissez le nom de la connexion à l'annuaire.
4. Dans la liste déroulante **Détection du serveur LDAP**, effectuez l'une des opérations suivantes :
    - Pour détecter automatiquement le serveur LDAP, cliquez sur **Automatique**. Dans le champ **Nom de domaine DNS**, saisissez le nom de domaine du serveur qui héberge le répertoire d'entreprise.
    - Pour spécifier une liste de serveurs LDAP, cliquez sur **Sélectionner un serveur dans la liste ci-dessous**. Dans le champ **Serveur LDAP**, saisissez le nom du serveur LDAP. Pour spécifier plusieurs serveurs LDAP, cliquez sur +.
5. Dans la liste déroulante **Activer SSL**, effectuez l'une des opérations suivantes :
    - Si la connexion LDAP est cryptée SSL, cliquez sur **Oui**. En regard du champ **Certificat SSL du serveur LDAP**, cliquez sur **Parcourir** et sélectionnez le certificat du serveur LDAP.
    - Si la connexion LDAP n'est pas cryptée SSL, cliquez sur **Non**.
6. Dans le champ **Port LDAP**, saisissez le numéro de port TCP pour la communication. Les valeurs par défaut sont 636 si SSL est activé ou 389 si SSL est désactivé.
7. Dans la liste déroulante **Autorisation requise**, effectuez l'une des opérations suivantes :
    - Si une autorisation est requise pour la connexion, cliquez sur **Oui**. Dans le champ **Connexion**, saisissez le DN de l'utilisateur autorisé à se connecter au LDAP (par exemple, an=admin,o=Org1). Dans le champ **Mot de passe**, saisissez le mot de passe.
    - Si aucune autorisation n'est requise pour la connexion, cliquez sur **Non**.
8. Dans le champ **Base de recherche d'utilisateurs**, saisissez la valeur à utiliser en tant que DN de base pour les recherches d'informations d'utilisateur.
9. Dans le champ **Filtre de recherche d'utilisateurs LDAP**, saisissez le filtre de recherche LDAP requis pour trouver des objets utilisateur dans le serveur d'annuaires de votre organisation. Par exemple, pour un IBM Domino Directory, saisissez `(objectClass=Person)`.

    Remarque : si vous souhaitez exclure les comptes d'utilisateur désactivés des résultats de la recherche, saisissez `(&(objectclass=user)(logindisabled=false))`.
10. Dans la liste déroulante **Étendue de la recherche d'utilisateurs LDAP**, effectuez l'une des opérations suivantes :
    - Pour rechercher tous les objets qui suivent l'objet de base, cliquez sur **Tous les niveaux**. Il s'agit du paramètre par défaut.
    - Pour rechercher les objets situés un niveau après le DN de base, cliquez sur **Un seul niveau**.
11. Dans le champ **Identifiant unique**, saisissez le nom de l'attribut qui identifie de manière unique chaque utilisateur du répertoire LDAP de votre organisation (cet attribut doit être une chaine immuable et globalement unique). Par exemple, `dominoUNID`IBM Domino dans LDAP 7 et ultérieures.
12. Dans le champ **Prénom**, saisissez l'attribut du prénom de chaque utilisateur (par exemple, `givenName`).
13. Dans le champ **Nom**, saisissez l'attribut du nom de chaque utilisateur (par exemple, `sn`).

14. Dans le champ **Attribut de connexion**, saisissez l'attribut de connexion à utiliser pour l'authentification (par exemple, `uid`).
15. Dans le champ **Adresse électronique**, saisissez l'attribut de messagerie de chaque utilisateur (par exemple, `mail`). Si vous ne définissez rien, la valeur par défaut sera utilisée.
16. Dans le champ **Nom d'affichage**, saisissez l'attribut du nom d'affichage de chaque utilisateur (par exemple, `displayName`). Si vous ne définissez rien, la valeur par défaut sera utilisée.
17. Dans le champ **Nom du compte du profil de messagerie**, saisissez l'attribut du nom du compte du profil de messagerie de chaque utilisateur (par exemple, `mail`).
18. Dans le champ **Nom de l'utilisateur principal**, saisissez le nom principal de l'utilisateur pour SCEP (par exemple, `mail`).
19. Pour activer des groupes liés par répertoire pour la connexion au répertoire, cochez la case **Activer les groupes liés par répertoire**.

    Spécifiez les informations suivantes :

    - Dans le champ **Base de recherche de groupes**, saisissez la valeur à utiliser en tant que DN de base pour les recherches d'informations de groupe.
    - Dans le champ **Filtre de recherche de groupes LDAP**, saisissez le filtre de recherche LDAP requis pour trouver des objets de groupe dans le répertoire de votre organisation. Par exemple, pour un IBM Domino Directory, saisissez `(objectClass=dominoGroup)`.
    - Dans le champ **Identifiant unique du groupe**, saisissez l'attribut de l'identifiant unique de chaque groupe. Cet attribut doit être immuable et globalement unique (par exemple, saisissez `cn`).
    - Dans le champ **Nom d'affichage du groupe**, saisissez l'attribut du nom d'affichage de chaque groupe (par exemple, saisissez `cn`).
    - Dans le champ **Attribut d'adhésion au groupe**, saisissez le nom de l'attribut d'adhésion au groupe. Les valeurs d'attribut doivent être au format DN (par exemple, `CN=jsmith,CN=Users,DC=example,DC=com`).
    - Dans le champ **Nom du groupe test**, saisissez un nom de groupe existant pour valider les attributs de groupe spécifiés.
20. Cliquez sur **Enregistrer**.
21. Cliquez sur **Fermer**.

À la fin : Si vous souhaitez ajouter un calendrier de synchronisation du répertoire, reportez-vous à Ajouter un calendrier de synchronisation.

Activer les groupes liés par annuaire

Avant de commencer : vérifiez qu'aucune synchronisation du répertoire d'entreprise n'est en cours. Vous ne pouvez pas enregistrer les modifications que vous apportez à la connexion au répertoire d'entreprise tant que la synchronisation n'est pas terminée.

1. Sur la barre de menus, cliquez sur **Paramètres > Intégration externe > Répertoire d'entreprise**.
2. Cliquez sur le nom du répertoire d'entreprise que vous souhaitez modifier.
3. Dans l'onglet **Paramètres de synchronisation**, cochez la case **Activer les groupes liés par répertoire**.
4. Pour forcer la synchronisation des groupes de répertoires d'entreprise, cochez la case **Forcer la synchronisation**.

   Si cette case est cochée, lorsqu'un groupe est supprimé de votre répertoire d'entreprise, les liaisons vers ce groupe sont supprimées des groupes liés par répertoire et des groupes de répertoires d'intégration. Si tous les groupes de répertoires d'entreprise associés à un groupe lié par répertoire sont supprimés, celui-ci est converti en groupe local. Si cette case n'est pas cochée et qu'aucun répertoire d'entreprise n'est trouvé, le processus de synchronisation est annulé.

5. Dans le champ **Limite de synchronisation**, saisissez le nombre maximal de modifications de votre choix pour chaque synchronisation.

   Le paramètre par défaut est cinq. Si le nombre de modifications à synchroniser dépasse la limite de synchronisation, vous pouvez empêcher l'exécution du processus de synchronisation. Les modifications sont calculées en ajoutant ce qui suit : utilisateurs à ajouter aux groupes, utilisateurs à supprimer des groupes, utilisateurs à intégrer, utilisateurs à supprimer.
6. Dans le champ **Niveau d'imbrication maximal des groupes de répertoire**, saisissez le nombre de niveaux imbriqués à synchroniser pour les groupes de répertoires d'entreprise.
7. Cliquez sur **Enregistrer**.

À la fin : Créez des groupes liés par répertoire. Pour plus d'informations, reportez-vous au contenu relatif à l'administration.

Activer l'intégration

L'intégration vous permet d'ajouter automatiquement des comptes d'utilisateur à BlackBerry UEM en fonction de l'appartenance des utilisateurs à un groupe de répertoires d'entreprise universel ou global. Les comptes d'utilisateur sont ajoutés à BlackBerry UEM lors du processus de synchronisation.

Vous pouvez en outre choisir d'envoyer automatiquement aux utilisateurs intégrés un e-mail et des mots de passe d'activation ou des clés d'accès pour les applications BlackBerry Dynamics.

Suppression

Si vous activez l'intégration, vous pouvez aussi choisir de configurer la suppression. Lorsqu'un utilisateur est désactivé dans Microsoft Active Directory ou supprimé de tous les groupes de répertoires d'entreprise des groupes de répertoires d'intégration, BlackBerry UEM peut automatiquement supprimer l'utilisateur de l'une des façons suivantes :

- Supprimer les données professionnelles ou toutes les données à partir des terminaux des utilisateurs
- Supprimer le compte d'utilisateur de BlackBerry UEM

Vous pouvez utiliser la protection contre la suppression pour retarder la suppression des données des terminaux ou des comptes d'utilisateur pour éviter toute suppression inattendue en raison de la latence de la réplication du répertoire. Par défaut, la protection contre la suppression retarde les actions de suppression de deux heures après le prochain cycle de synchronisation.

Remarque : Les paramètres de suppression s'appliquent également aux utilisateurs de répertoires existants dans BlackBerry UEM. Il est recommandé de cliquer sur l'icône d'aperçu pour générer le rapport de synchronisation de l'annuaire et vérifier les modifications.

Synchronisation

Lorsque vous avez activé la suppression, lors de la prochaine synchronisation, les règles de suppression sont appliquées à tous les utilisateurs que vous avez ajoutés manuellement dans la console de gestion avant l'activation de la suppression qui ne sont pas membres d'un groupe associé à un répertoire d'intégration.

Lorsque vous avez activé l'intégration, vous pouvez ajouter manuellement des utilisateurs à BlackBerry UEM, même s'ils appartiennent déjà à un groupe associé à un répertoire. Si la suppression est activée, les utilisateurs que vous ajoutez manuellement à BlackBerry UEM verront les règles de suppression appliquées à leurs terminaux lors de la prochaine synchronisation s'ils ne sont pas membres d'un groupe de synchronisation d'intégration au moment de la synchronisation.

Activer et configurer l'intégration et la suppression

Vous pouvez intégrer automatiquement les utilisateurs qui sont membres de groupes universels et globaux. L'intégration n'est pas prise en charge pour les groupes locaux de domaines.

Avant de commencer :

- vérifiez qu'aucune synchronisation du répertoire d'entreprise n'est en cours. Vous ne pouvez pas enregistrer les modifications que vous apportez à la connexion au répertoire d'entreprise tant que la synchronisation n'est pas terminée.
- Pour intégrer des membres de groupes globaux, vous devez activer la prise en charge des groupes globaux dans vos paramètres de connexion Microsoft Active Directory.

1. Sur la barre de menus, cliquez sur **Paramètres > Intégration externe > Annuaire d'entreprise**.
2. Cliquez sur le nom du répertoire d'entreprise que vous souhaitez modifier.
3. Dans l'onglet **Paramètres de synchronisation**, cochez la case **Activer les groupes liés par répertoire**.
4. Cochez la case **Activer l'intégration**.
5. Exécutez les opérations suivantes pour chaque groupe que vous souhaitez configurer pour l'intégration avec une option d'activation des terminaux :
   a) Cliquez sur +.
   b) Saisissez le nom du groupe de répertoires d'entreprise. Cliquez sur 🔍.
   c) Sélectionnez le groupe. Cliquez sur **Ajouter**.
   d) Si vous le souhaitez, sélectionnez **Relier les groupes imbriqués**.
   e) Dans la section **Activation des terminaux**, indiquez si vous souhaitez que les utilisateurs intégrés reçoivent un mot de passe d'activation généré automatiquement ou non. Si vous sélectionnez l'option de mot de passe généré automatiquement, configurez la période d'activation et sélectionnez un modèle d'e-mail d'activation.
6. Pour intégrer des utilisateurs à BlackBerry Dynamics, cochez la case **Intégrer uniquement les utilisateurs disposant d'applications à BlackBerry Dynamics**.
7. Exécutez les opérations suivantes pour chaque groupe que vous souhaitez intégrer à l'activation pour les applications BlackBerry Dynamics uniquement :
   a) Cliquez sur +.
   b) Saisissez le nom du groupe de répertoires d'entreprise. Cliquez sur 🔍.
   c) Sélectionnez le groupe. Cliquez sur **Ajouter**.
   d) Si vous le souhaitez, sélectionnez **Relier les groupes imbriqués**.
   e) Sélectionnez le nombre de clés d'accès à générer par utilisateur ajouté, l'expiration des clés d'accès et le modèle d'e-mail.
8. Pour supprimer les données d'un terminal lorsqu'un utilisateur est supprimé, cochez la case **Supprimer les données du terminal lorsque l'utilisateur est supprimé de tous les groupes de répertoires d'intégration**. Sélectionnez l'une des options suivantes :
   - Supprimer uniquement les données professionnelles
   - Supprimer toutes les données du terminal
   - Supprimer toutes les données professionnelles du terminal/Supprimer uniquement les données professionnelles individuelles
9. Pour supprimer un compte d'utilisateur de BlackBerry UEM lorsqu'un utilisateur est supprimé de tous les groupes d'intégration, sélectionnez **Supprimer l'utilisateur lorsqu'il est supprimé de tous les groupes de répertoires d'intégration**. La première fois qu'un cycle de synchronisation se produit après la suppression d'un compte d'utilisateur de tous les groupes de répertoires d'intégration, le compte d'utilisateur est supprimé de BlackBerry UEM.

10. Pour empêcher la suppression inattendue de comptes d'utilisateur ou de données de terminaux de BlackBerry UEM, sélectionnez **Protection contre la suppression**.

    La protection contre la suppression signifie que les utilisateurs ne seront pas supprimés de BlackBerry UEM avant l'expiration d'un délai de deux heures après le cycle de synchronisation suivant.
11. Pour forcer la synchronisation des groupes de répertoires d'entreprise, cochez la case **Forcer la synchronisation**.

    Si cette case est cochée, lorsqu'un groupe est supprimé de votre répertoire d'entreprise, les liaisons vers ce groupe sont supprimées des groupes liés par répertoire et des groupes de répertoires d'intégration. Si cette case n'est pas cochée et qu'aucun répertoire d'entreprise n'est trouvé, le processus de synchronisation est annulé.
12. Dans le champ **Limite de synchronisation**, saisissez le nombre maximal de modifications de votre choix pour chaque processus de synchronisation (cinq par défaut).

    Si le nombre de modifications à synchroniser dépasse la limite de synchronisation, vous pouvez empêcher l'exécution du processus de synchronisation. Les modifications sont calculées en ajoutant ce qui suit : utilisateurs à ajouter aux groupes, utilisateurs à supprimer des groupes, utilisateurs à intégrer, utilisateurs à supprimer.
13. Dans le champ **Niveau d'imbrication maximal des groupes d'annuaires**, saisissez le nombre de niveaux imbriqués à synchroniser pour les groupes de répertoires d'entreprise.
14. Cliquez sur **Enregistrer**.

Synchroniser une connexion à un répertoire d'entreprise

Avant de commencer : Prévisualiser un rapport de synchronisation

1. Sur la barre de menus, cliquez sur **Paramètres > Intégration externe > Répertoire d'entreprise**.
2. Dans la colonne **Synchronisation**, cliquez sur .

À la fin : Afficher un rapport de synchronisation

Prévisualiser un rapport de synchronisation

Prévisualiser un rapport de synchronisation vous permet de vérifier que les mises à jour planifiées répondent à vos attentes avant la synchronisation.

1. Sur la barre de menus, cliquez sur **Paramètres > Intégration externe > Répertoire d'entreprise**.
2. Dans la colonne **Aperçu**, cliquez sur .
3. Cliquez sur **Afficher un aperçu maintenant**.
4. Une fois le traitement du rapport terminé, cliquez sur la date de la colonne **Dernier rapport**.
5. Pour afficher les rapports de synchronisation générés précédemment, cliquez sur le menu déroulant.

Afficher un rapport de synchronisation

1. Sur la barre de menus, cliquez sur **Paramètres > Intégration externe > Annuaire d'entreprise**.
2. Dans la colonne **Dernier rapport**, cliquez sur la date.
3. Pour afficher les rapports de synchronisation générés précédemment, cliquez sur le menu déroulant.
4. Pour exporter un rapport au format .csv, cliquez sur .

Ajouter un calendrier de synchronisation

Vous pouvez ajouter un calendrier de synchronisation pour synchroniser automatiquement BlackBerry UEM avec le répertoire d'entreprise de votre entreprise. Il existe trois types de calendriers de synchronisation :

- Intervalle : permet de spécifier la durée entre chaque synchronisation, la période et les jours où elle se produit.
- Une fois par jour : Permet de spécifier l'heure à laquelle la synchronisation démarre et les jours où elle se produit.
- Aucune récurrence : Permet de spécifier l'heure et le jour d'une synchronisation unique.

L'écran Répertoire d'entreprise vous permet de synchroniser manuellement BlackBerry UEM avec votre répertoire d'entreprise à tout moment.

1. Sur la barre de menus, cliquez sur **Paramètres > Intégration externe > Répertoire d'entreprise**.
2. Cliquez sur le nom du répertoire d'entreprise que vous souhaitez modifier.
3. Dans l'onglet **Calendrier de synchronisation**, cliquez sur +.
4. Pour réduire la quantité d'informations synchronisées, dans la liste déroulante **Type de synchronisation**, choisissez une des options suivantes :
   - **Tous les groupes et utilisateurs** : Il s'agit du paramètre par défaut. Si vous choisissez cette option, les utilisateurs seront intégrés, supprimés et liés aux groupes reliés au répertoire approprié au cours de la synchronisation, les utilisateurs qui ne sont pas intégrés ou supprimés mais dont les groupes reliés au répertoire ont été modifiés, et les utilisateurs dont les attributs ont été modifiés seront synchronisés.
   - **Groupes d'intégration** : si vous choisissez cette option, les utilisateurs seront intégrés, supprimés et liés aux groupes reliés au répertoire approprié au cours de la synchronisation, et les utilisateurs dont les attributs ont été modifiés seront synchronisés. Les utilisateurs qui ne sont pas intégrés ou supprimés mais dont les groupes reliés au répertoire ont été modifiés ne sont pas synchronisés.
   - **Groupes associés à un répertoire** : si vous choisissez cette option les utilisateurs ne pourront pas être intégrés et supprimés lors de la synchronisation. Les utilisateurs dont les groupes reliés au répertoire ont été modifiés seront liés de manière appropriée. Les utilisateurs dont les attributs ont été modifiés seront synchronisés.
   - **Attributs de l'utilisateur** : si vous choisissez cette option les utilisateurs ne pourront pas être intégrés et supprimés lors de la synchronisation. Les utilisateurs dont les groupes reliés au répertoire ont été modifiés ne sont pas synchronisés. Les utilisateurs dont les attributs ont été modifiés seront synchronisés.
5. Dans la liste déroulante **Récurrence**, sélectionnez l'une des options suivantes :

Option	Étapes
Intervalle	**a.** Dans le champ **Intervalle**, saisissez la durée, en minutes, entre les synchronisations. **b.** Spécifiez la période de synchronisation. **c.** Sélectionnez les jours de la semaine lors desquels vous souhaitez que les synchronisations interviennent.
Une fois par jour	**a.** Spécifiez l'heure à laquelle vous souhaitez que la synchronisation commence. **b.** Sélectionnez les jours de la semaine lors desquels vous souhaitez que les synchronisations interviennent.
Aucune récurrence	**a.** Spécifiez l'heure à laquelle vous souhaitez que la synchronisation commence. **b.** Sélectionnez le jour où vous souhaitez que la synchronisation intervienne.

6. Cliquez sur **Ajouter**.

Suppression d'une connexion à un répertoire d'entreprise

Si vous supprimez une connexion à un répertoire d'entreprise, tous les utilisateurs ajoutés à BlackBerry UEM à partir de ce répertoire d'entreprise seront convertis en utilisateurs locaux. Une fois les utilisateurs convertis en utilisateurs locaux, ils ne peuvent plus être reconvertis en utilisateurs associés à un répertoire, même si vous ajoutez à nouveau la connexion au répertoire d'entreprise ultérieurement. Les utilisateurs continueront à fonctionner en tant qu'utilisateurs locaux mais UEM ne pourra pas synchroniser les mises à jour à partir du répertoire d'entreprise, telles que les modifications apportées au nom, à l'adresse e-mail et à d'autres attributs.

1. Sur la barre de menus, cliquez sur **Paramètres > Intégration externe > Annuaire d'entreprise**.
2. Cliquez sur **X** en regard du nom du répertoire d'entreprise que vous souhaitez supprimer.
3. Cliquez sur **Supprimer**.

Se connecter à un serveur SMTP pour envoyer des notifications par e-mail

Pour permettre à BlackBerry UEM d'envoyer des notifications par e-mail, vous devez connecter BlackBerry UEM à un serveur SMTP.

BlackBerry UEM utilise les notifications par e-mail pour envoyer les instructions d'activation aux utilisateurs. Vous pouvez également configurer BlackBerry UEM pour qu'il envoie les mots de passe de BlackBerry UEM Self-Service et les avertissements de conformité des terminaux, et vous pouvez envoyer des e-mails individuels.

Si vous ne connectez pas BlackBerry UEM à un serveur SMTP, BlackBerry UEM ne peut pas envoyer les mots de passe, les messages d'activation ou les e-mails. Vous pouvez toujours configurer BlackBerry UEM pour envoyer les avertissements de conformité directement aux terminaux.

Pour plus d'informations sur les messages d'activation, les avertissements de conformité des terminaux et l'envoi d'e-mails individuels, consultez le contenu relatif à l'administration.

Se connecter à un serveur SMTP pour envoyer des notifications par e-mail

1. Sur la barre de menus, cliquez sur **Paramètres > Intégration externe > Serveur SMTP**.
2. Cliquez sur ✎.
3. Dans le champ **Nom d'affichage de l'expéditeur**, saisissez un nom à utiliser pour les notifications BlackBerry UEM par e-mail. Par exemple, `donotreply` ou `BUEM Admin`.
4. Dans le champ **Adresse de l'expéditeur**, saisissez l'adresse électronique que vous souhaitez que BlackBerry UEM utilise pour envoyer les notifications par e-mail.
5. Dans le champ **Serveur SMTP**, saisissez le nom de domaine complet du serveur SMTP. Par exemple, `mail.exemple.com`.
6. Dans le champ **Port de serveur SMTP**, saisissez le numéro de port du serveur SMTP. Le numéro de port par défaut est 25.
7. Dans le menu déroulant **Type de cryptage pris en charge**, sélectionnez le type de cryptage que vous souhaitez appliquer aux e-mails.
8. Si le serveur SMTP requiert une authentification, saisissez l'identifiant de connexion du serveur SMTP dans le champ **Nom d'utilisateur**. Dans le champ **Mot de passe**, saisissez le mot de passe du serveur SMTP.
9. Si nécessaire, importez un certificat CA SMTP :
   a) Copiez le fichier de certificat SSL du serveur SMTP de votre organisation sur l'ordinateur que vous utilisez.
   b) Cliquez sur **Parcourir**.
   c) Accédez au fichier de certificat SSL et cliquez sur **Charger**.
10. Cliquez sur **Enregistrer**.

À la fin : Cliquez sur **Test de connexion** si vous souhaitez tester la connexion avec le serveur SMTP et envoyer un e-mail test. BlackBerry UEM envoie le message à l'adresse électronique que vous avez indiquée dans le champ **Adresse de l'expéditeur**.

Configuration de la mise en miroir des bases de données

Vous pouvez utiliser la mise en miroir pour configurer une base de données BlackBerry UEM haute disponibilité. La mise en miroir de bases de données est une fonctionnalité Microsoft SQL Server qui vous permet de maintenir le niveau de service de la base de données et l'intégrité des données en cas de problèmes au niveau de la base de données BlackBerry UEM. Pour plus d'informations sur l'utilisation de la mise en miroir des bases de données, consultez le contenu relatif à la planification.

Remarque : Dans la mesure où Microsoft envisage de supprimer la fonctionnalité de mise en miroir des bases de données dans les futures versions de Microsoft SQL Server, il vous est recommandé d'utiliser la fonctionnalité AlwaysOn pour garantir la haute disponibilité des bases de données. Pour utiliser AlwaysOn, une procédure de configuration doit être suivie avant d'installer BlackBerry UEM. Pour plus d'informations sur l'utilisation de la fonctionnalité AlwaysOn, consultez le contenu relatif à la planification.

Étapes à suivre pour configurer la mise en miroir de bases de données

Pour configurer la mise en miroir de bases de données, procédez comme suit :

Étape	Action
1	Passez en revue les exigences du contenu relatif à la planification et vérifiez que le domaine BlackBerry UEM répond aux conditions préalables.
2	Créez la base de données miroir, démarrez une session de mise en miroir et configurez un serveur témoin.
3	Configurez chaque instance de BlackBerry UEM pour qu'elle se connecte à la base de données miroir.

Conditions préalables : Configuration de la mise en miroir des bases de données

- Configurez le serveur principal et le serveur miroir de manière à ce qu'ils soient accessibles depuis des ordinateurs distants.
- Configurez le serveur principal et le serveur miroir de manière à ce qu'ils disposent des mêmes autorisations.
- Configurez un serveur témoin que vous utiliserez pour analyser le serveur principal.
- Configurez l'agent Microsoft SQL Server pour qu'il utilise un compte d'utilisateur de domaine doté des mêmes autorisations administratives locales que le compte Windows qui exécute les services BlackBerry UEM.
- Vérifiez que le compte d'utilisateur de domaine dispose des autorisations suffisantes pour accéder au serveur principal et au serveur miroir.
- Vérifiez que le serveur DNS est en cours d'exécution.
- Sur chaque ordinateur qui héberge une instance de base de données de BlackBerry UEM, dans le client natif SQL Server 2012, désactivez l'option Canaux nommés. Si vous choisissez de ne pas désactiver l'option Canaux nommés, rendez-vous sur le site https://support.blackberry.com/community et consultez l'article 34373.

- Pour connaitre les autres conditions préalables qui s'appliquent à la version de Microsoft SQL Server utilisée par votre entreprise, rendez-vous sur la page Web technet.microsoft.com/sqlserver et consultez l'article Mise en miroir de bases de données : SQL Server 2012 ou Mise en miroir de bases de données : SQL Server 2014.
- Si la base de données miroir utilise l'instance par défaut, les composants BlackBerry UEM peuvent uniquement se connecter à la base de données miroir via le port par défaut 1433, et non via un port statique personnalisé. Cela est dû à une limitation imposée par Microsoft SQL Server 2005 et versions ultérieures. Pour plus d'informations sur ce problème, reportez-vous à l'article SQL 2005 : pilote JDBC et mise en miroir de bases de données).

Créer et configurer la base de données miroir

Avant de commencer : Pour préserver l'intégrité de la base de données pendant la création et la configuration de la base de données miroir, arrêtez les services BlackBerry UEM sur tous les ordinateurs qui hébergent une instance de BlackBerry UEM.

1. Dans Microsoft SQL Server Management Studio, accédez à la base de données principale.
2. Définissez la propriété **Modèle de récupération** sur **Complet**.
3. Dans l'éditeur de requête, exécutez la requête **-- ALTER DATABASE** *<BUEM_db>* **SET TRUSTWORTHY ON**, où *<BUEM_db>* correspond au nom de la base de données principale.
4. Sauvegardez la base de données principale. Définissez l'option **Type de sauvegarde** sur **Complète**.
5. Copiez les fichiers de sauvegarde sur le serveur miroir.
6. Sur le serveur miroir, restaurez la base de données pour créer la base de données miroir. Lorsque vous restaurez la base de données, sélectionnez l'option **AUCUNE RÉCUPÉRATION**.
7. Vérifiez que le nom de la base de données miroir correspond à celui de la base de données principale.
8. Sur le serveur principal, dans Microsoft SQL Server Management Studio, cliquez avec le bouton droit sur la base de données principale et sélectionnez la tâche **Miroir**. Sur la page **Mise en miroir**, cliquez sur **Configurer la sécurité** pour exécuter l'assistant de configuration de la sécurité de la mise en miroir de bases de données.
9. Lancez le processus de mise en miroir. Pour plus d'informations, reportez-vous à Configuration de la mise en miroir de bases de données – SQL Server 2012 ou Configuration de la mise en miroir de bases de données – SQL Server 2014.
10. Pour activer le basculement automatique, ajoutez un témoin à la session de mise en miroir. Pour plus d'informations, reportez-vous à Témoin de mise en miroir de bases de données – SQL Server 2012 ou Témoin de mise en miroir de bases de données – SQL Server 2014.

À la fin :

- Pour vérifier que le basculement fonctionne correctement, basculez manuellement le service vers la base de données miroir et revenez à la base de données principale.
- Redémarrez les services BlackBerry UEM sur tous les ordinateurs qui hébergent une instance de BlackBerry UEM.
- Connecter BlackBerry UEM à la base de données miroir.

Connecter BlackBerry UEM à la base de données miroir

Vous devez répéter cette tâche sur chaque ordinateur qui héberge une instance BlackBerry UEM.

Avant de commencer :

- Créer et configurer la base de données miroir.
- Vérifiez que le serveur miroir est en cours d'exécution.

- Vous pouvez effectuer cette tâche à l'aide de l'outil de configuration BlackBerry UEM, ou vous pouvez mettre à jour le fichier de propriétés de la base de données en suivant les instructions ci-dessous. Si vous souhaitez utiliser l'outil de configuration BlackBerry UEM, rendez-vous sur le site support.blackberry.com/community pour consulter l'article KB36443. Dans la section « Mise à jour des propriétés de la base de données BlackBerry UEM », suivez les instructions pour activer la mise en miroir SQL et fournir le FQDN du serveur miroir.

1. Sur l'ordinateur qui héberge l'instance de BlackBerry UEM, accédez à *<drive>*:\Program Files\BlackBerry\UEM\common-settings.
2. Dans un éditeur de texte, ouvrez **DB.properties**.
3. Dans la section **paramètres facultatifs à utiliser pour le basculement**, après **configuration.database.ng.failover.server=**, saisissez le FQDN du serveur miroir (par exemple, `configuration.database.ng.failover.server=mirror_server.domain.net`).
4. Si nécessaire, effectuez l'une des opérations suivantes :
   - Si vous avez spécifié une instance nommée pour la base de données principale lors de l'installation, et que la base de données miroir utilise l'instance par défaut, supprimez la valeur située après **configuration.database.ng.failover.instance=**.
   - Si la base de données principale utilise une instance par défaut et que la base de données miroir utilise une instance nommée, après **configuration.database.ng.failover.instance=**, saisissez l'instance nommée.
5. Enregistrez et fermez **DB.properties**.

À la fin :

- Redémarrez les services BlackBerry UEM.
- Vous devez répéter cette tâche sur tous les ordinateurs qui hébergent une instance de BlackBerry UEM.
- Vérifiez que tous les ordinateurs qui hébergent une instance de BlackBerry UEM peuvent se connecter au serveur miroir à l'aide du pseudo du serveur.

Configuration d'une nouvelle base de données miroir

Si vous créez et configurez une nouvelle base de données miroir après un changement de rôle (c'est-à-dire si les composants BlackBerry UEM ont été basculés vers la base de données miroir actuelle et que la base de données miroir actuelle est devenue la base de données principale), répétez les tâches de la section Connecter BlackBerry UEM à la base de données miroir sur tous les ordinateurs qui hébergent une instance de BlackBerry UEM.

Connexion de BlackBerry UEM à Microsoft Azure

Microsoft Azure est le service informatique en nuage Microsoft de déploiement et de gestion des applications et des services. Vous devez connecter BlackBerry UEM à Azure si vous souhaitez utiliser BlackBerry UEM pour déployer des applications iOS et Android gérées par Microsoft Intune, si vous souhaitez utiliser l'accès conditionnel Azure Active Directory, ou si vous souhaitez gérer les applications Windows 10 dans BlackBerry UEM.

BlackBerry UEM prend en charge la configuration d'une seule entité Azure. Pour connecter BlackBerry UEM à Azure, effectuez les actions suivantes :

Étape	Action
1	Créer un compte Microsoft Azure.
2	Synchroniser Microsoft Active Directory avec Microsoft Azure.
3	Créer un point de terminaison d'entreprise dans Azure.
4	Configurer BlackBerry UEM pour une synchronisation de avec Microsoft Intune et Windows Store for Business.
5	(Facultatif) Configurer l'accès conditionnel Azure Active Directory.

Créer un compte Microsoft Azure

Pour déployer des applications protégées par Microsoft Intune sur des terminaux iOS et Android ou gérer des applications Windows 10 dans BlackBerry UEM, vous devez posséder un compte Microsoft Azure et authentifier BlackBerry UEM avec Azure.

Effectuez cette tâche si votre organisation n'a pas de compte Microsoft Azure.

Remarque : Pour vous assurer que vous disposez des licences et des autorisations de compte correctes pour Microsoft Intune, rendez-vous sur le site Web support.blackberry.com/community pour consulter l'article 50341.

1. Accédez à https://azure.microsoft.com/fr-fr/ et cliquez sur **Compte gratuit**, puis suivez les instructions pour créer le compte.

   Vous devez fournir des informations de carte de crédit pour créer le compte.
2. Connectez-vous au portail de gestion Azure à l'adresse https://portal.azure.com et connectez-vous avec le nom d'utilisateur et le mot de passe que vous avez créés lorsque vous vous êtes connecté.

À la fin : Synchroniser Microsoft Active Directory avec Microsoft Azure.

Synchroniser Microsoft Active Directory avec Microsoft Azure

Pour autoriser les utilisateurs de Windows 10 à installer des applications en ligne ou à envoyer des applications protégées par Microsoft Intune à des terminaux iOS et Android, les utilisateurs doivent exister dans Microsoft Azure Active Directory. Vous devez synchroniser les utilisateurs et les groupes entre vos instances de Active Directory et de Azure Active Directory sur site à l'aide de Microsoft Azure Active Directory Connect. Pour plus d'informations, accédez à https://docs.microsoft.com/fr-fr/azure/active-directory/connect/active-directory-aadconnect.

1. Téléchargez Azure AD Connect depuis le Centre de téléchargement Microsoft.
2. Installez le logiciel Azure AD Connect.
3. Configurez Azure AD Connect pour connecter votre instance de Active Directory sur site avec Azure Active Directory.

À la fin : Créer un point de terminaison d'entreprise dans Azure

Créer un point de terminaison d'entreprise dans Azure

Pour que BlackBerry UEM ait accès à Microsoft Azure, vous devez créer un point de terminaison d'entreprise dans Azure. Le point de terminaison d'entreprise permet à BlackBerry UEM de s'authentifier avec Microsoft Azure. Pour plus d'informations, reportez-vous à https://docs.microsoft.com/en-us/azure/active-directory/active-directory-app-registration.

Si vous connectez BlackBerry UEM en même temps à Microsoft Intune et Windows Store pour Business, utilisez une autre application d'entreprise pour chaque objet en raison des différences dans les autorisations et les changements futurs possibles.

Remarque :

Les déploiements cloud nationaux Microsoft (ou tout déploiement nécessitant une URL de connexion autre que login.microsoftonline.com) nécessitent des étapes supplémentaires pour connecter UEM à Intune. Pour plus d'informations, rendez-vous sur support.blackberry.com/community pour lire l'article KB75773.

Avant de commencer :

-
- Assurez-vous d'être en possession de l'URL de réponse. Pour des instructions sur l'obtention de l'URL de réponse en vue d'une authentification moderne, reportez-vous à la section Configurer BlackBerry UEM pour la synchronisation avec Microsoft Intune.

1. Connectez-vous au portail Azure.
2. Accédez à **Microsoft Azure > Azure Active Directory > Inscriptions des applications**.
3. Cliquez sur **Nouvelle inscription**.
4. Dans le champ **Nom**, saisissez un nom pour l'application.
5. Sélectionnez les types de compte qui peuvent utiliser l'application ou accéder à l'API.
6. Dans la section **Rediriger l'URI**, sélectionnez **Client mobile/Bureau** dans la liste déroulante, puis saisissez une URL valide. Le format de l'URL est https://<*FQDN_du_serveur_BlackBerry_UEM*>:<*port*>/admin/intuneauth
7. Cliquez sur **S'inscrire**.
8. Copiez l'**ID d'application** de votre application et collez-le dans un fichier texte.

   Il s'agit de l'**ID client** requis dans BlackBerry UEM.
9. Si vous créez l'application pour utiliser Microsoft Intune, cliquez sur **Autorisations API** dans la section **Gérer**. Procédez comme suit :

a) Cliquez sur **Ajouter une autorisation**.
b) Cliquez sur **Microsoft Graph**.
c) Sélectionnez **Autorisations déléguées**.
d) Faites défiler la liste des autorisations vers le bas, puis, sous **Autorisations déléguées**, définissez les autorisations suivantes pour Microsoft Intune :

- Lire et écrire les applications Microsoft Intune (**DeviceManagementApps > DeviceManagementApps.ReadWrite.All**)
- Lire tous les groupes (**Groupe > Group.Read.All**)
- Lire tous les profils de base des utilisateurs (**Utilisateur > User.ReadBasic.All**)

e) Cliquez sur **Ajouter des autorisations**.
f) Sous **Accorder le consentement**, cliquez sur **Accorder le consentement de l'administrateur**.

Remarque : Vous devez être administrateur général pour octroyer des autorisations.

g) Lorsque vous y êtes invité, cliquez sur **Oui** pour octroyer des autorisations pour tous les comptes dans l'annuaire actuel.

Vous pouvez utiliser les autorisations par défaut si vous créez l'application pour vous connecter à Windows Store Entreprise.

10. Cliquez sur **Certificats et secrets** dans la section **Gérer**. Procédez comme suit :

a) Sous **Secrets de client**, cliquez sur **Nouveau secret de client**.
b) Saisissez la description du secret du client.
c) Sélectionnez une durée pour le secret du client.
d) Cliquez sur **Ajouter**.
e) Copiez la valeur du nouveau secret du client.

Il s'agit de la **Clé client** qui est requise dans BlackBerry UEM.

Avertissement : Si vous ne copiez pas la valeur de votre clé à ce moment, vous devrez créer une nouvelle clé, car la valeur ne s'affiche pas après avoir quitté cet écran.

À la fin : Configurer BlackBerry UEM pour une synchronisation avec Microsoft Intune
ou Configurer BlackBerry UEM pour une synchronisation avec Windows Store Entreprise.

Configuration de l'accès conditionnel Azure Active Directory

Si vous avez configuré l'accès conditionnel Azure AD pour votre entreprise, vous pouvez configurer un locataire BlackBerry UEM en tant que partenaire de conformité afin que les terminaux iOS et Android gérés par UEM puissent se connecter à vos applications basées sur le cloud telles que Office 365. Vous ne pouvez configurer qu'un locataire UEM pour chaque locataire Azure.

Vous pouvez configurer des connexions pour plusieurs locataires Azure. Si vous créez plusieurs connexions,

Remarque : La prise en charge de l'accès conditionnel Azure AD est actuellement limitée dans les situations suivantes :

- BlackBerry UEM Client ne prend pas en charge les stratégies d'accès conditionnel Azure AD lorsque l'option Toutes les applications cloud est sélectionnée sous Applications cloud ou Actions. À la place, vous devez sélectionner les applications spécifiques que vous souhaitez inclure dans la stratégie. Pour en savoir plus, rendez-vous sur support.blackberry.com/community pour consulter l'article 90010.
- BlackBerry Work ne prend pas en charge la fonction de conformité d'accès conditionnel Azure AD. Pour en savoir plus, rendez-vous sur support.blackberry.com/community pour consulter l'article 89668.

Pour pouvoir utiliser cette fonction, les utilisateurs doivent répondre aux exigences suivantes :

- Les utilisateurs doivent exister dans Azure AD,
- Si vous synchronisez votre Active Directory sur site avec Azure AD, l'UPN Active Directory sur site des utilisateurs doit correspondre à leur UPN Azure AD. Si ces valeurs ne correspondent pas à votre environnement, rendez-vous sur support.blackberry.com/community pour consulter l'article 88208.
- Les utilisateurs doivent être ajoutés à UEM via la synchronisation avec Active Directory.
- Les utilisateurs doivent avoir installé l'application Authenticator Microsoft et le BlackBerry UEM Client .

Si vous configurez l'accès conditionnel Azure AD, UEM avertit Azure AD lorsqu'un terminal n'est pas conforme et que des conditions sont appliquées dans les situations suivantes :

- Si le paramètre Action d'application pour les terminaux est défini sur une valeur autre que Surveiller et consigner, UEM avertit Azure AD une fois que toutes les invites utilisateur ont expiré.
- Si le paramètre Action d'application pour les applications BlackBerry Dynamics est défini sur une valeur autre que Surveiller et consigner, UEM avertit Azure AD dès qu'une violation de conformité est détectée.

Pour plus d'informations sur les profils de conformité, reportez-vous au contenu relatif à l'administration UEM.

Pour plus d'informations sur l'accès conditionnel Azure AD, reportez-vous à la documentation Microsoft.

Configurer BlackBerry UEM en tant que partenaire de conformité dans Azure

Avant de commencer : Vous devez disposer de la licence Microsoft Intune appropriée pour utiliser cette fonction. Pour en savoir plus, rendez-vous sur support.blackberry.com et consultez les articles KB91041 et KB50341. Pour plus d'informations sur les licences, consultez les détails de Microsoft. Le compte d'administrateur que vous utilisez pour effectuer les étapes suivantes doit disposer d'une licence Intune.

Dans le centre d'administration Endpoint Manager de Microsoft, sous **Administration des locataires > Connecteurs et jetons > Gestion de la conformité des partenaires**, ajoutez **BlackBerry UEM** en tant que partenaire de conformité pour les terminaux iOS et Android, puis attribuez-le aux utilisateurs et aux groupes.

Si vous prenez en charge les terminaux iOS et Android, vous devez ajouter BlackBerry UEM en tant que partenaire de conformité pour chaque plateforme. Pour plus d'informations, consultez la documentation Microsoft.

Configurer l'accès conditionnel Azure Active Directory

1. Dans la console de gestion BlackBerry UEM, cliquez sur **Paramètres > Intégration externe > Accès conditionnel Azure Active Directory**.
2. Dans le tableau, cliquez sur +.
3. Saisissez un nom pour la configuration.
4. Dans la liste déroulante **Cloud Azure**, sélectionnez **Global**.
5. Saisissez votre **ID de locataire Azure**.

   Vous pouvez saisir le nom du locataire qui est au format FQDN, ou l'ID de locataire unique qui est au format GUID.
6. Dans le remplacement de mappage de terminal, sélectionnez **UPN** ou **E-mail**.

   UPN est sélectionné par défaut. Si UPN est utilisé, vous devez vérifier que le locataire Azure AD et tous les répertoires mappés partagent la même valeur UPN pour les utilisateurs avant d'enregistrer la connexion. Une fois la connexion enregistrée, le remplacement de mappage de terminal ne peut pas être modifié.
7. Dans la liste **Répertoires d'entreprise disponibles**, sélectionnez une ou plusieurs instances de répertoire et cliquez sur →.
8. Cliquez sur **Enregistrer**.
9. Sélectionnez le compte administrateur que vous souhaitez utiliser pour vous connecter à votre locataire Azure.

Le compte administrateur doit pouvoir accorder des autorisations à l'application pour accéder aux ressources de votre entreprise. comme l'administrateur général, l'administrateur d'application cloud ou l'administrateur d'application.

10. Acceptez la demande d'autorisation de Microsoft.

Configurer le profil de connectivité BlackBerry Dynamics pour prendre en charge la fonctionnalité Azure Accès conditionnel

Dans la console de gestion BlackBerry UEM, modifiez chaque profil de connectivité BlackBerry Dynamics.

1. Sous Serveurs d'applications, cliquez sur Ajouter.
2. Sélectionnez **Feature-Azure Conditional Access** dans la liste des applications.
3. Cliquez sur + pour ajouter un nouveau serveur d'applications.
4. Si vous utilisez BlackBerry UEM dans un environnement sur site, spécifiez les paramètres de serveur suivants.

Élément	Description
Serveur	gdas-<SRP_ID>.<region_code>.bbsecure.com
Port	443
Itinéraires	Direct

Si votre environnement comprend BlackBerry UEM Cloud et BEMS cloud, et que vous avez configuré les notifications par e-mail ou BEMS-Docs pour créer un locataire BEMS, la priorité, le numéro de port et l'URL de BEMS cloud sont automatiquement ajoutés à la section de charge utile du serveur d'applications.

Attribuer l'application Fonctionnalité Accès conditionnel Azure à des utilisateurs

Vous pouvez attribuer l'application à des utilisateurs ou à des groupes.

Effectuez l'une des opérations suivantes :

Tâche	Étapes
Attribuer l'application à un utilisateur	**a.** Sur la barre de menus, cliquez sur **Utilisateurs > Terminaux gérés**. **b.** Dans les résultats de la recherche, cliquez sur le nom d'un compte d'utilisateur. **c.** Dans la section **Applications**, cliquez sur **+**. **d.** Recherchez et sélectionnez l'application Fonctionnalité Accès conditionnel Azure. **e.** Cliquez sur **Suivant**. **f.** Vous pouvez également renseigner les champs **Disposition**, **VPN de pré-application** et **Configuration de l'application**. **g.** Cliquez sur **Attribuer**.

Tâche	Étapes
Attribuer l'application à un groupe	a. Sur la barre de menus, cliquez sur **Groupes**. b. Dans l'onglet **Groupes d'utilisateurs**, cliquez sur le nom d'un groupe. c. Dans la section **Applications attribuées**, cliquez sur **+**. d. Recherchez et sélectionnez l'application Fonctionnalité Accès conditionnel Azure. e. Cliquez sur **Suivant**. f. Vous pouvez également renseigner les champs **Disposition**, **VPN de pré-application** et **Configuration de l'application**. g. Cliquez sur **Attribuer**.

Configurer un profil BlackBerry Dynamics

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Stratégie > BlackBerry Dynamics**.
3. Cliquez sur **+**.
4. Saisissez le nom et la description du profil.
5. Sélectionnez le paramètre **Autoriser UEM Client à s'inscrire dans BlackBerry Dynamics**.
6. Configurez les valeurs qui conviennent pour les autres paramètres de profil. Pour plus d'informations sur chaque paramètre de profil, reportez-vous à la section Paramètres de profil BlackBerry Dynamics.
7. Cliquez sur **Ajouter**.

À la fin :

- L' application Microsoft Authenticator doit être installée sur les terminaux des utilisateurs. Vous pouvez télécharger l'application depuis l'App Store appropriée et l'ajouter à UEM. Pour plus de détails, consultez les informations pour iOS et les informations pour Android. Vous pouvez ensuite attribuer l'application à des utilisateurs ou à des groupes. Vous pouvez également demander aux utilisateurs d'installer l'application depuis leur App Store.
- Une fois l'accès conditionnel Active Directory configuré, les utilisateurs activant des terminaux sont invités à s'inscrire à l'accès conditionnel Active Directory lors de l'activation. Les utilisateurs disposant de terminaux activés sont invités à s'inscrire à l'accès conditionnel Active Directory la prochaine fois qu'ils ouvrent le UEM Client.

Supprimer les terminaux Azure Active Directory de l'accès conditionnel

Lorsque vous désactivez un terminal à partir de BlackBerry UEM, le terminal reste inscrit à l'accès conditionnel Azure AD. Azure reconnaît que le terminal n'est plus géré, ce qui, selon vos paramètres d'accès conditionnel, peut le mettre hors conformité.

Les utilisateurs peuvent supprimer leurs terminaux d'Azure en supprimant leur compte Azure AD dans les paramètres de compte de l'application Authenticator Microsoft ou vous pouvez supprimer le terminal de Azure.

1. Sur le portail Azure, dans Azure AD, sélectionnez l'utilisateur pour lequel vous souhaitez supprimer le terminal.
2. Affichez la page **Terminaux** de l'utilisateur.
3. Sélectionnez le groupe et cliquez sur **Supprimer**.

Activer l'accès à BlackBerry Web Services sur BlackBerry Infrastructure

Si votre organisation utilise un client de service Web qui ne bénéficie pas du pare-feu de l'organisation et a besoin d'accéder aux API BlackBerry Web Services (REST ou SOAP hérité), il peut se connecter aux API en toute sécurité sur BlackBerry Infrastructure. Pour plus d'informations sur l'activation de cet accès dans les applications clientes, les développeurs peuvent consulter la section Mise en route du document de référence de l'API REST BlackBerry Web Services.

Les clients de services Web ne peuvent utiliser le système BlackBerry Infrastructure pour accéder aux API BlackBerry Web Services que si vous activez cet accès dans la console de gestion. Par défaut, cet accès n'est pas activé.

1. Dans la barre de menus, cliquez sur **Paramètres > Paramètres généraux > Accès aux services Web BlackBerry**.
2. Cliquez sur **Activer**.
3. Cliquez sur **Enregistrer**.

Obtention d'un certificat APNs pour gérer les terminaux iOS et macOS

APNs (Apple Push Notification Service) est le service de notification Push d'Apple. Pour permettre à BlackBerry UEM de gérer des terminaux iOS ou macOS, vous devez vous procurer un certificat APNs et l'enregistrer. Si vous configurez plusieurs domaines BlackBerry UEM, chaque domaine requiert un certificat APNs.

Vous pouvez vous procurer et enregistrer le certificat APNs à l'aide de l'assistant de première connexion ou de la section Intégration externe de la console d'administration.

Remarque : Chaque certificat APNs est valable un an. La console de gestion affiche la date d'expiration. Vous devez renouveler le certificat APNs avant la date d'expiration en utilisant le même ID Apple que celui utilisé pour obtenir le certificat. Vous pouvez noter l'ID Apple dans la console de gestion. Vous pouvez également créer une notification d'évènement par e-mail pour vous rappeler de renouveler le certificat 30 jours avant son expiration. Si le certificat expire, les terminaux ne reçoivent pas de données de BlackBerry UEM. Si vous enregistrez un nouveau certificat APNs, les utilisateurs de terminaux doivent réactiver leurs terminaux pour recevoir des données.

Pour plus d'informations, rendez-vous sur https://developer.apple.com et consultez la section *Problèmes rencontrés lors de l'envoi de notifications Push* de l'article TN2265.

Il est recommandé d'accéder à la console d'administration et au portail Apple Push Certificates Portal à l'aide du navigateur Google Chrome ou Safari. Ces navigateurs offrent une prise en charge optimale pour la demande et l'enregistrement d'un certificat APNs.

Pour obtenir et enregistrer un certificat APNs, procédez comme suit :

Étape	Action
1	Procurez-vous un fichier CSR signé auprès de BlackBerry.
2	Utilisez le fichier CSR signé pour demander un certificat APNs à Apple.
3	Enregistrez le certificat APNs.

Obtenir un fichier CSR signé auprès de BlackBerry

Avant de pouvoir obtenir un certificat APNs, vous devez vous procurer un fichier CSR signé auprès de BlackBerry.

1. Sur la barre de menus, cliquez sur **Paramètres > Intégration externe > Apple Push Notification**.
2. Si vous n'avez pas encore de certificat APNs, dans la section **Étape 1 sur 3 - Télécharger le certificat CSR signé de BlackBerry**, cliquez sur **Télécharger le certificat**.

   Si vous souhaitez renouveler le certificat APNs actuel, cliquez plutôt sur **Renouveler le certificat**.
3. Cliquez sur **Enregistrer** pour enregistrer le fichier CSR signé (.scsr) sur votre ordinateur.

À la fin : Demander un certificat APNs auprès d'Apple.

Demander un certificat APNs auprès d'Apple

Avant de commencer : Obtenir un fichier CSR signé auprès de BlackBerry.

1. Sur la barre de menus, cliquez sur **Paramètres > Intégration externe > Notification push Apple**.
2. Dans la section **Étape 2 sur 3 - Obtenir un certificat APNs auprès d'Apple**, cliquez sur **Apple Push Certificate Portal**. Vous êtes dirigé vers le portail Apple Push Certificates Portal.
3. Connectez-vous au portail Apple Push Certificates Portal en utilisant un ID Apple valide.
4. Suivez les instructions pour charger le fichier CSR signé (.scsr). Notez que si l'erreur suivante s'affiche : « Vous avez chargé un type de fichier non valide. Les extensions de fichier prises en charge sont .txt, .rtf, .plist, .b64. », vous pouvez renommer le fichier .scr au format .txt, puis charger à nouveau le fichier CSR.
5. Téléchargez et enregistrez le certificat APNs (.pem) sur votre ordinateur.
6. (Facultatif) Cliquez sur pour afficher une fenêtre **Remarque**.
7. Dans la fenêtre **Remarque**, saisissez l'ID Apple que vous avez utilisé pour demander le certificat APNs.

   Vous devez utiliser le même ID Apple pour renouveler le certificat.
8. Cliquez n'importe où en dehors de la fenêtre **Remarque** pour la fermer.

À la fin : Enregistrer le certificat APNs.

Enregistrer le certificat APNs

Avant de commencer : Demander un certificat APNs auprès d'Apple.

1. Sur la barre de menus, cliquez sur **Paramètres > Intégration externe > Apple Push Notification**.
2. Dans la section **Étape 3 sur 3 : inscrire le certificat APNs**, cliquez sur **Parcourir**. Accédez au certificat APNs (.pem) et sélectionnez-le.
3. Cliquez sur **Envoyer**.

À la fin : Pour tester la connexion entre BlackBerry UEM et le serveur APNs, cliquez sur **Tester le certificat APNs**.

Renouveler le certificat APNs

Le certificat APNs est valable un an. Vous devez renouveler le certificat APNs chaque année avant qu'il n'expire. Le certificat doit être renouvelé en utilisant le même ID Apple que celui utilisé pour obtenir le certificat APNs d'origine.

Vous pouvez créer une notification d'évènement par e-mail pour vous rappeler de renouveler le certificat 30 jours avant son expiration.

Avant de commencer : Obtenir un fichier CSR signé auprès de BlackBerry.

1. Sur la barre de menus, cliquez sur **Paramètres > Intégration externe > Notification push Apple**.
2. Cliquez sur **Renouveler le certificat**.
3. Dans la section **Étape 1 sur 3 - Télécharger le certificat CSR signé de BlackBerry**, cliquez sur **Télécharger le certificat**.
4. Cliquez sur **Enregistrer** pour enregistrer le fichier CSR signé (.scsr) sur votre ordinateur.
5. Dans la section **Étape 2 sur 3 - Obtenir un certificat APNs auprès d'Apple**, cliquez sur **Apple Push Certificate Portal**. Vous êtes dirigé vers le portail Apple Push Certificates Portal.

6. Connectez-vous au portail Apple Push Certificates Portal en utilisant l'ID Apple utilisé pour obtenir le certificat APNs d'origine.
7. Suivez les instructions pour renouveler le certificat APNs (.pem). Vous devrez alors télécharger le nouveau fichier CSR signé. Notez que si l'erreur suivante s'affiche : « Vous avez chargé un type de fichier non valide. Les extensions de fichier prises en charge sont .txt, .rtf, .plist, .b64. », vous pouvez renommer le fichier .scr au format .txt, puis charger à nouveau le fichier CSR.
8. Téléchargez et enregistrez le certificat APNs renouvelé sur votre ordinateur.
9. Dans la section **Étape 3 sur 3 - Inscrire le certificat APNs**, cliquez sur **Parcourir**. Accédez au certificat APNs renouvelé et sélectionnez-le.
10. Cliquez sur **Submit**.

À la fin : Pour tester la connexion entre BlackBerry UEM et le serveur APNs, cliquez sur **Tester le certificat APNs**.

Dépannage de l'APNs

Cette section vous aide à dépanner les problèmes de l'APNs.

Le certificat APNs ne correspond pas au fichier CSR. Fournissez le fichier APNs (.pem) qui convient ou envoyez un nouveau fichier CSR.

Description

Lors de la tentative d'enregistrement du certificat APNs, vous pouvez recevoir un message d'erreur si vous n'avez pas envoyé le fichier .scsr signé le plus récent de BlackBerry au portail Apple Push Certificates Portal.

Solution possible

Si vous avez téléchargé plusieurs fichiers CSR depuis BlackBerry, seul le dernier fichier téléchargé est valide. Si vous savez quel fichier CSR est le plus récent, revenez au portail Apple Push Certificates Portal pour le charger. Si vous l'ignorez, procurez-vous un nouveau fichier CSR auprès de BlackBerry, puis revenez au portail Apple Push Certificates Portal et chargez-le.

Je reçois le message « Le système a rencontré une erreur » lorsque j'essaye d'obtenir un CSR signé.

Description

Lorsque vous essayez d'obtenir un CSR signé, vous recevez l'erreur suivante : « Le système a rencontré une erreur. Réessayez. »

Solution possible

Rendez-vous sur support.blackberry.com pour consulter l'article 37266.

Je ne peux pas activer des terminaux iOS ou macOS

Cause possible

Si vous n'êtes pas en mesure d'activer les terminaux iOS ou macOS, cela signifie peut-être que le certificat APNs n'est pas correctement installé.

Solution possible

Effectuez une ou plusieurs des opérations suivantes :

- Sur la barre de menus de la console d'administration, cliquez sur **Paramètres > Intégration externe > Apple Push Notification**. Vérifiez que l'état du certificat APNs est Installé. Si l'état n'est pas correct, essayez à nouveau d'enregistrer le certificat APNs.
- Cliquez sur **Tester le certificat APNs** pour tester la connexion entre BlackBerry UEM et le serveur APNs.
- Si nécessaire, procurez-vous un nouveau fichier CSR signé auprès de BlackBerry ainsi qu'un nouveau certificat APNs.

Configuration de BlackBerry UEM pour le programme d'inscription des appareils (DEP)

Vous devez configurer BlackBerry UEM pour qu'il utilise le programme d'inscription des appareils (DPE) Apple avant de pouvoir synchroniser BlackBerry UEM avec le programme d'inscription des appareils. Après avoir configuré BlackBerry UEM, vous pouvez utiliser la console de gestion BlackBerry UEM pour gérer l'activation des terminaux iOS que votre organisation a achetés pour le programme d'inscription des appareils.

Vous pouvez utiliser un compte Apple Business Manager pour synchroniser BlackBerry UEM avec le DEP. Apple Business Manager est un portail Web où vous pouvez inscrire et gérer des terminaux iOS dans le DEP, et gérer des comptes d'achat en volume Apple. Si votre organisation utilise DEP ou VPP, vous pouvez effectuer une mise à niveau vers Apple Business Manager.

Lorsque vous configurez BlackBerry UEM pour le programme d'inscription des appareils Apple, vous devez effectuer les actions suivantes :

Étape	Action
1	Créer un compte du programme d'inscription des appareils.
2	Télécharger une clé publique.
3	Générer un jeton de serveur.
4	Enregistrer le jeton de serveur avec BlackBerry UEM.
5	Ajouter la première configuration d'inscription.

Créer un compte du programme d'inscription des appareils

1. Sur la barre de menus, cliquez sur **Paramètres > Intégration externe > Programme d'inscription des appareils Apple**.
2. Cliquez sur +.
3. Dans le champ **Nom**, saisissez un nom pour le compte.
4. À l'étape **1 sur 4 : Créer un compte du programme d'inscription des appareils Apple**, cliquez sur **Créer un compte du programme d'inscription des appareils Apple**.
5. Remplissez les champs et suivez les instructions à l'écran pour créer votre compte.

À la fin : Télécharger une clé publique.

Télécharger une clé publique

Avant de commencer : Créer un compte du programme d'inscription des appareils.

1. Sur la barre de menus, cliquez sur **Paramètres > Intégration externe > Programme d'inscription des appareils Apple**.
2. Cliquez sur +.
3. À l'étape **2 sur 4 : télécharger une clé publique**, cliquez sur **Télécharger une clé publique**.
4. Cliquez sur **Enregistrer**.

À la fin : Générer un jeton de serveur.

Générer un jeton de serveur

Avant de commencer : Télécharger une clé publique.

1. Sur la barre de menus, cliquez sur **Paramètres > Intégration externe > Programme d'inscription des appareils Apple**.
2. Cliquez sur +.
3. À l'étape **3 sur 4 : générer le jeton de serveur à partir du compte du programme d'inscription des appareils Apple**, cliquez sur **Ouvrir le portail du Programme d'inscription des appareils Apple**.
4. Connectez-vous à votre compte du programme d'inscription des appareils.
5. Suivez les instructions à l'écran pour générer un jeton de serveur.

À la fin : Enregistrer le jeton de serveur avec BlackBerry UEM.

Enregistrer le jeton de serveur avec BlackBerry UEM

BlackBerry UEM utilise un jeton de serveur pour l'authentification lorsqu'il communique avec le programme d'inscription des appareils Apple.

Avant de commencer : Générer un jeton de serveur.

1. Sur la barre de menus, cliquez sur **Paramètres > Intégration externe > Programme d'inscription des appareils Apple**.
2. Cliquez sur +.
3. À l'étape **4 sur 4 : enregistrer le jeton de serveur avec BlackBerry UEM**, cliquez sur **Parcourir**.
4. Sélectionnez le fichier du jeton de serveur **.p7m**.
5. Cliquez sur **Ouvrir**.
6. Cliquez sur **Suivant**.

À la fin : Ajouter la première configuration d'inscription.

Ajouter la première configuration d'inscription

Avant de commencer : Enregistrer le jeton de serveur avec BlackBerry UEM avant d'ajouter votre première configuration d'inscription.

Après avoir enregistré un jeton de serveur, BlackBerry UEM affiche automatiquement la fenêtre dans laquelle vous ajoutez votre première configuration d'inscription.

1. Saisissez un nom pour la configuration.
2. Effectuez l'une des tâches suivantes :
   - Si vous souhaitez que BlackBerry UEM attribue automatiquement la configuration d'inscription aux appareils lorsque vous les enregistrez dans le programme d'inscription des appareils d'Apple, cochez la case Attribuer automatiquement cette configuration à tous les nouveaux appareils.
   - Si vous souhaitez utiliser la console BlackBerry UEM pour attribuer manuellement la configuration d'inscription aux appareils concernés, ne cochez pas la case Attribuer automatiquement cette configuration à tous les nouveaux appareils.
3. Vous avez la possibilité de saisir un nom de service et le numéro de téléphone de l'assistance qui s'afficheront sur les terminaux au cours de la configuration.
4. Dans la section **Configuration de l'appareil**, cochez les cases suivantes :
   - Autoriser le couplage : cette option permet aux utilisateurs de coupler le terminal à un ordinateur.
   - Obligatoire : cette option permet aux utilisateurs d'activer les terminaux avec le nom d'utilisateur et le mot de passe du répertoire de leur entreprise.
   - Autoriser la suppression du profil MDM : cette option permet aux utilisateurs de désactiver les terminaux.
   - Veuillez patienter pendant la configuration du terminal : si elle est sélectionnée, cette option empêche les utilisateurs d'annuler la configuration des appareils tant que l'activation avec BlackBerry UEM n'est pas terminée.
5. Dans la section **Ignorer pendant la configuration**, sélectionnez les éléments que vous ne souhaitez pas inclure dans la configuration des appareils :
   - Mot de passe : avec cette option, les utilisateurs ne sont pas invités à créer un mot de passe pour le terminal.
   - Services de localisation : cette option permet de désactiver les services de localisation sur le terminal.
   - Restaurer : cette option empêche les utilisateurs de restaurer les données à partir d'un fichier de sauvegarde.
   - Déplacer depuis Android : cette option vous empêche de restaurer les données à partir d'un terminal Android.
   - ID Apple : si elle est sélectionnée, cette option empêche les utilisateurs de se connecter avec leur identifiant Apple et iCloud.
   - Conditions générales : si elle est sélectionnée, cette option permet de masquer les conditions générales de iOS
   - Siri : cette option permet de désactiver Siri sur les terminaux.
   - Diagnostics : cette option bloque l'envoi automatique des informations de diagnostic au terminal pendant la configuration.
   - Biométrique : cette option empêche les utilisateurs de configurer Touch ID.
   - Paiement : cette option empêche les utilisateurs de configurer Apple Pay.
   - Zoom : cette option empêche les utilisateurs de configurer le zoom.
   - Configuration de l'icône de l'écran d'accueil : si cette option est sélectionnée, les utilisateurs ne peuvent pas régler le clic de l'icône de l'écran d'accueil
   - Screen Time : si cette option est sélectionnée, l'option de configuration de l'application Screen Time est ignorée lors de l'inscription DEP
   - Mise à jour du logiciel : si cette option est sélectionnée, les utilisateurs ne voient pas l'écran de mise à jour obligatoire du logiciel sur l'appareil
   - IMessage et Face Time - si cette option est sélectionnée, les utilisateurs ne voient pas l'écran iMessage et Face Time sur l'appareil
   - Ton d'affichage : si cette option est sélectionnée, l'écran Ton d'affichage ne s'affiche pas sur le terminal

- Confidentialité : si cette option est sélectionnée, l'écran Confidentialité ne s'affiche pas sur le terminal
- Intégration : si cette option est sélectionnée, les utilisateurs ne voient pas l'écran Intégration sur le terminal
- Migration Watch : si cette option est sélectionnée, les utilisateurs ne voient pas l'écran Migration Watch sur le terminal
- Configuration SIM : si cette option est sélectionnée, l'écran permettant de configurer un forfait cellulaire ne s'affiche pas sur le terminal
- Migration terminal à terminal : si cette option est sélectionnée, l'écran Migration terminal à terminal ne s'affiche pas sur le terminal

6. Cliquez sur **Enregistrer**.

   Si le message « Une erreur est survenue. Impossible de déchiffrer le fichier de jeton du serveur » s'affiche, rendez-vous sur la page Web support.blackberry.com/community et consultez l'article 37282.
7. Si vous avez sélectionné Attribuer automatiquement de nouveaux appareils à cette configuration, cliquez sur **Oui**.

À la fin : Activez les terminaux iOS. Pour plus d'informations sur l'activation des terminaux inscrits dans DEP, consultez le contenu relatif à l'administration.

Mettre à jour le jeton de serveur

Le jeton de serveur est valide pendant un an. Vous devez renouveler le jeton chaque année avant qu'il n'expire. Pour afficher l'état actuel du jeton, reportez-vous à la Date d'expiration dans la fenêtre du programme d'inscription des appareils Apple.

Avant de commencer : Si la clé publique a changé, téléchargez une nouvelle clé publique.

1. Sur la barre de menus, cliquez sur **Paramètres > Intégration externe > Programme d'inscription des appareils Apple**.
2. Cliquez sur le nom d'un compte DEP.
3. Dans la section **Date d'expiration**, cliquez sur **Mettre à jour le jeton de serveur**.
4. À **l'étape 1 sur 2 : Générer le jeton de serveur à partir du compte du programme d'inscription des appareils Apple**, cliquez sur **Ouvrir le portail DEP Apple**.
5. Connectez-vous à votre compte du programme d'inscription des appareils.
6. Suivez les instructions à l'écran pour générer un jeton de serveur.
7. À l'étape **2 sur 2 : Enregistrer le jeton de serveur avec BlackBerry UEM**, cliquez sur **Parcourir**.
8. Sélectionnez le fichier du jeton de serveur **.p7m**.
9. Cliquez sur **Ouvrir**.
10. Cliquez sur **Enregistrer**.

Supprimer une connexion DEP

ATTENTION : si vous supprimez toutes les connexions DEP, vous ne pouvez pas activer de nouveaux terminaux iOS dans le programme d'inscription des appareils Apple. Si vous avez attribué des configurations d'inscription à des terminaux et que celles-ci n'ont pas été appliquées, BlackBerry UEM supprime les configurations d'inscription attribuées aux terminaux. La suppression de la connexion n'affecte pas les terminaux actifs sur BlackBerry UEM.

Si votre entreprise ne déploie plus de terminaux iOS qui utilisent le programme d'inscription des appareils, vous pouvez supprimer les connexions BlackBerry UEM au programme d'inscription des appareils.

1. Sur la barre de menus, cliquez sur **Paramètres > Intégration externe > Programme d'inscription des appareils Apple**.
2. Cliquez sur le nom d'un compte DEP.
3. Cliquez sur **Supprimer la connexion au programme d'inscription des appareils**.
4. Cliquez sur **Supprimer**.
5. Cliquez sur **OK**.

Configuration de BlackBerry UEM pour la prise en charge des terminaux Android Enterprise

Les terminaux Android Enterprise offrent une sécurité supplémentaire aux entreprises qui souhaitent gérer des terminaux Android. Pour plus d'informations sur les terminaux Android Enterprise, rendez-vous sur le site Web https://support.google.com/work/android/.

Pour obtenir des instructions détaillées sur la configuration de BlackBerry UEM pour la prise en charge des terminaux Android Enterprise, rendez-vous sur le site Web support.blackberry.com/community et consultez l'article 37748.

Il existe deux façons de configurer BlackBerry UEM pour prendre en charge des terminaux Android Enterprise :

1. Connectez BlackBerry UEM à un domaine Google Cloud ou G Suite.

   Remarque : Vous ne pouvez connecter qu'un domaine BlackBerry UEM à un domaine Google.
2. Autoriser BlackBerry UEM à gérer les terminaux Android Enterprise qui ont des comptes gérés Google Play. Vous n'avez pas besoin d'avoir un domaine Google pour utiliser cette option. Pour plus d'informations, reportez-vous à https://support.google.com/googleplay/work/.

Le tableau suivant récapitule les différentes options de configuration des terminaux Android Enterprise :

Méthode de configuration de BlackBerry UEM pour prendre en charge les terminaux Android Enterprise	Quand choisir cette méthode	Type de compte d'utilisateur	Services Google pris en charge
Connecter BlackBerry UEM à votre domaine G Suite	Vous disposez d'un domaine G Suite dans votre entreprise	Comptes G Suite (pour les entreprises)	Prend en charge tous les services G Suite tels que Gmail, Google Calendar et Drive. Prend en charge la gestion d'applications via Google Play.
Connecter BlackBerry UEM à votre domaine Google Cloud	Vous disposez d'un domaine Google Cloud dans votre entreprise	Comptes Google Cloud, également appelés comptes Google gérés (pour les entreprises)	Semblables à G Suite mais sans l'accès aux produits payants tels que Gmail, Google Calendar et Drive. Prend en charge la gestion d'applications via Google Play.

Méthode de configuration de BlackBerry UEM pour prendre en charge les terminaux Android Enterprise	Quand choisir cette méthode	Type de compte d'utilisateur	Services Google pris en charge
Autoriser BlackBerry UEM à gérer les terminaux Android Enterprise comme des comptes gérés Google Play.	Vous ne disposez pas de domaine Google dans votre entreprise ou Vous disposez d'un domaine Google déjà connecté à un domaine BlackBerry UEM et vous souhaitez utiliser les terminaux Android Enterprise sur un deuxième domaine BlackBerry UEM	Les terminaux Android Enterprise qui ont des comptes gérés Google Play	Prend en charge la gestion d'applications via Google Play. Les services Google ne sont pas pris en charge.

Pour plus d'informations sur la configuration de la prise en charge de BlackBerry UEM et de Chrome OS, reportez-vous à la section Extension de la gestion des terminaux Chrome OS à BlackBerry UEM.

Configurer BlackBerry UEM pour la prise en charge des terminaux Android Enterprise

Vous ne pouvez connecter qu'un seul domaine BlackBerry UEM à votre domaine Google. Avant de connecter un autre domaine BlackBerry UEM, vous devez supprimer la connexion existante. Reportez-vous à la section Supprimer la connexion à votre domaine Google.

1. Sur la barre de menus, cliquez sur **Paramètres > Intégration externe > Android Enterprise**.
2. Effectuez l'une des tâches suivantes :

Tâche	Étapes
Utiliser des terminaux Android Enterprise dotés de comptes Google Play gérés	a. Sélectionnez **Autoriser BlackBerry UEM à gérer les comptes Google Play**. b. Cliquez sur **Suivant**. c. Dans la fenêtre **Bring Android to Work**, connectez-vous à l'aide d'un compte Google. Vous pouvez utiliser un compte Google ou Gmail. Le compte que vous utilisez devient le compte d'administrateur pour le service **Bring Android to Work**. d. Cliquez sur **Mise en route**. e. Saisissez le nom de votre entreprise Cliquez sur **Confirmer**. f. Cliquez sur **Terminer l'enregistrement**. Vous accédez à la console de gestion BlackBerry UEM.

Tâche	Étapes
Utiliser un domaine Google	a. Sélectionnez **Connecter BlackBerry UEM à votre domaine Google existant**. Notez que vous ne pouvez pas partager de domaines Google entre plusieurs domaines BlackBerry UEM. Cette option prend en charge Android Enterprise et Chrome OS Enterprise. b. Cliquez sur **Suivant**. c. Renseignez les champs pour créer un compte de service et cliquez sur **Suivant**. Pour obtenir des instructions détaillées, rendez-vous sur support.blackberry.com/community pour consulter l'article 37748.

3. Spécifiez comment les configurations de l'application doivent être envoyées à un terminal. Toutes les informations que vous avez ajoutées à la configuration de l'application peuvent être fournies à l'aide de BlackBerry Infrastructure ou à l'aide de l'infrastructure Google. Effectuez l'une des opérations suivantes :
   - Sélectionnez **Envoyer la configuration de l'application à l'aide d'UEM Client** pour envoyer les configurations d'applications via BlackBerry Infrastructure.
   - Sélectionnez **Envoyer la configuration de l'application à l'aide de Google Play** pour envoyer les détails de configuration de l'application à l'aide de l'infrastructure Google.
4. Lorsque vous y êtes invité, cliquez sur **Accepter** pour accepter l'ensemble d'autorisations pour certaines ou l'ensemble des applications suivantes :
   - Google Chrome
   - BlackBerry Connectivity
   - Services BlackBerry Hub +
   - BlackBerry Hub
   - Calendrier BlackBerry
   - Contacts par BlackBerry
   - Notes par BlackBerry
   - Tâches par BlackBerry
5. Cliquez sur **Terminé**.

À la fin : Effectuez les étapes pour activer les terminaux Android Enterprise. Pour plus d'informations sur l'activation de terminal, consultez « Activation du terminal » dans le contenu relatif à l'administration.

Supprimer la connexion à votre domaine Google

Vous ne pouvez connecter qu'un domaine BlackBerry UEM à votre domaine Google Cloud ou G Suite. Avant de connecter un autre domaine BlackBerry UEM, vous devez supprimer la connexion existante.

Supprimez la connexion à votre domaine Google avant d'effectuer l'une des tâches suivantes :

- Désaffecter un domaine BlackBerry UEM
- Connecter une autre instance de BlackBerry UEM à votre domaine Google Cloud ou G Suite

Si vous ne supprimez pas la connexion à votre domaine Google, vous ne pourrez peut-être plus connecter votre domaine Google Cloud ou G Suite à une nouvelle instance de BlackBerry UEM. Si vous supprimez la connexion dans BlackBerry UEM, tous les terminaux activés avec un type d'activation Android Enterprise seront désactivés.

1. Dans la barre de menus, cliquez sur **Paramètres > Intégration externe**.
2. Cliquez sur **Connexion au domaine Google**.
3. Cliquez sur **Supprimer la connexion**.
4. Cliquez sur **Supprimer**.

Supprimer la connexion de domaine Google à l'aide de votre compte Google

Si vous avez configuré BlackBerry UEM pour prendre en charge les terminaux Android Enterprise, vous pouvez supprimer la connexion dans Google.

1. À l'aide du compte Google que vous avez utilisé pour configurer les terminaux Android Enterprise, connectez-vous à https://play.google.com/work.
2. Cliquez sur **Paramètres d'administration**.
3. Dans la section **Informations d'organisation**, cliquez sur .
4. Cliquez sur **Supprimer l'entreprise**.
5. Cliquez sur **Supprimer**.
6. Dans la console BlackBerry UEM, cliquez sur **Paramètres > Intégration externe** dans la barre de menus.
7. Cliquez sur **Connexion au domaine Google**.
8. Cliquez sur **Tester la connexion**.
9. Cliquez sur **Supprimer la connexion**.
10. Cliquez sur **Supprimer**.

Modifier ou tester la connexion au domaine Google

Vous pouvez modifier la connexion au domaine Google dans BlackBerry UEM pour modifier le type de domaine Google que vous utilisez pour gérer les appareils Android Enterprise ou pour tester la connexion au domaine Google. Lorsque vous modifiez ou testez la connexion, les terminaux déjà activés ne sont pas affectés.

1. Dans la barre de menus, cliquez sur **Paramètres > Intégration externe**.
2. Cliquez sur **Connexion au domaine Google**.
3. Cliquez sur .
4. Effectuez l'une des tâches suivantes :
   - Cliquez sur **Tester la connexion** pour voir l'état actuel de la connexion.
   - Sélectionnez le type de domaine à utiliser pour gérer les appareils Android Enterprise et cliquez sur **Enregistrer**.

Extension de la gestion des terminaux Chrome OS à BlackBerry UEM

La prise en charge de Chrome OS BlackBerry UEM requiert un domaine géré Google. L'inscription et certaines tâches de gestion des terminaux Chrome OS s'effectuent toujours via la console de domaines gérés Google. L'intégration de Chrome OS à BlackBerry UEM étend la gestion de certaines fonctionnalités de gestion de Chrome OS à UEM.

Dans la console d'administration Google, les utilisateurs et les terminaux sont organisés en unités organisationnelles, qui sont une représentation hiérarchique des groupes d'utilisateurs, de terminaux et de paramètres. BlackBerry UEM synchronise ces unités organisationnelles à partir de la console d'administration Google en groupes d'unités organisationnelles UEM. Pour plus d'informations sur les unités organisationnelles, reportez-vous aux informations de Google.

À l'issue de la synchronisation entre Google et BlackBerry UEM, UEM s'enregistre auprès du domaine Google pour recevoir des notifications de modifications apportées aux unités organisationnelles, aux utilisateurs ou aux terminaux. Par exemple, si un terminal est inscrit, si le nom d'un utilisateur change ou si une unité organisationnelle est déplacée, UEM est immédiatement averti et met à jour la base de données en conséquence.

Si l'environnement UEM de votre entreprise est déjà configuré pour Android Enterprise, vous pouvez ajouter une autre connexion à utiliser pour gérer vos terminaux Chrome OS.

Pour en savoir plus, rendez-vous sur le site support.blackberry.com et consultez l'article 98789.

Remarque : Votre domaine géré Google doit inclure « Mise à niveau de Chrome Enterprise ».

Configuration de la gestion des terminaux Chrome OS lorsque vous avez déjà configuré BlackBerry UEM pour utiliser Android Enterprise

Si vous utilisez déjà Android Enterprise, il vous suffit d'effectuer les étapes suivantes pour préparer la gestion des terminaux Chrome OS dans BlackBerry UEM :

- Assurez-vous que le domaine Google de votre organisation est doté de Chrome OS Enterprise activé
- Assurez-vous que l'API de stratégie Chrome est activée dans le domaine Google de votre organisation. Pour plus d'informations, reportez-vous à la section Créer un compte de service pour permettre à BlackBerry UEM de s'authentifier auprès de votre domaine Google Cloud ou Google Workspace par Google
- Assurez-vous que toutes les étendues sont ajoutées. Pour plus d'informations, reportez-vous à la section Activer des API supplémentaires pour permettre à BlackBerry UEM de synchroniser les données de Chrome OS
- Activez la gestion Chrome OS dans la console BlackBerry UEM, reportez-vous à la section Synchroniser BlackBerry UEM avec la console d'administration Google

Créer un compte de service que BlackBerry UEM utilise pour vous authentifier auprès de votre domaine Google Cloud ou Google Workspace par Google

Effectuez ces étapes uniquement si BlackBerry UEM n'est pas déjà connecté à un domaine Google géré existant.

1. Connectez-vous à la console Google Developers à l'aide du compte Google que vous souhaitez utiliser pour gérer votre projet.

2. Cliquez sur **Créer un projet**.
3. Saisissez un nom pour le projet.
4. Cliquez sur **Créer**.
5. Une fois votre projet créé, cliquez dessus et dans le volet de gauche, développez **IAM & Admin**, puis cliquez sur **Comptes de service**.
6. Cliquez sur **Créer un compte de service**.
7. Saisissez un nom pour le compte de service, puis cliquez sur **Créer et continuer**.
8. Dans la liste **Rôle**, sélectionnez **De base > Éditeur**.
9. Cliquez sur **Continuer**.
10. Cliquez sur **Terminé**.
11. Sélectionnez votre compte de service.
12. Cliquez sur l'onglet **Clés**.
13. Cliquez sur **Ajouter une clé > Créer une nouvelle clé > P12 > Créer**.
14. Copiez le mot de passe de la clé privée, car vous l'utiliserez plus tard.
15. Vous serez peut-être invité à télécharger le certificat, ou il sera automatiquement téléchargé. Recherchez-le et enregistrez-le dans un dossier connu.
16. Cliquez sur **Fermer**.
17. Cliquez sur ☰ > **Comptes de service**.
18. Dans la colonne **Actions**, cliquez sur > ⋮ **Gérer les détails**.
19. Copiez l'**ID client unique** et l'**adresse électronique** associés au compte de service. Copiez-les dans le même fichier texte que vous avez utilisé pour stocker le mot de passe de la clé privée que vous utiliserez ultérieurement au cours de la procédure.
20. Cliquez sur ☰ > **API et services > API et services activés**.
21. Cliquez sur **Activer les API et les services**.
22. Recherchez et sélectionnez **Admin SDK API**.
23. Cliquez sur **Activer**.
24. Recherchez et sélectionnez **Google Play EMM API**.
25. Cliquez sur **Activer**.
26. Recherchez et sélectionnez **Chrome Policy API**.
27. Cliquez sur **Activer**.

Activer des API supplémentaires pour permettre à BlackBerry UEM de synchroniser des données de Chrome OS

Vous devez utiliser la console d'administration Google de votre organisation pour activer des API supplémentaires qui permettront à UEM de synchroniser des données Chrome OS.

1. Connectez-vous à la console d'administration Google à l'aide du compte d'administrateur de votre domaine Google.
2. Accédez à **Accueil > Terminaux > Mobile et points de terminaison > Paramètres > Intégrations tierces**.
3. Cliquez sur **Android EMM** et assurez-vous que l'option **Activer la gestion mobile Android tierce** est sélectionnée.
4. Cliquez sur **Ajouter des fournisseurs EMM > Générer un jeton**.

5. Copiez le jeton. Collez-le dans le même fichier texte que celui dans lequel vous avez collé le mot de passe de la clé privée.
6. Fermez la fenêtre Jeton et cliquez sur **Enregistrer**.
7. Cliquez sur **Enregistrer malgré tout**.
8. Cliquez sur **Sécurité > contrôle des accès et des données > Commandes d'API**.
9. Sous **Délégation à l'échelle du domaine**, cliquez sur **GÉRER LA DÉLÉGATION À L'ÉCHELLE DU DOMAINE**.
10. Cliquez sur **Ajouter nouveau** (près des clients API).
11. Dans le champ **ID client**, collez l'ID client unique du compte de service Google que vous avez enregistré précédemment, puis saisissez les adresses suivantes dans le champ Étendues OAuth, dans une liste séparée par des virgules :
    - https://www.googleapis.com/auth/admin.directory.user
    - https://www.googleapis.com/auth/admin.directory.customer
    - https://www.googleapis.com/auth/admin.directory.device.chromeos
    - https://www.googleapis.com/auth/admin.directory.device.mobile
    - https://www.googleapis.com/auth/admin.directory.orgunit
    - https://www.googleapis.com/auth/admin.directory.user
    - https://www.googleapis.com/auth/chrome.management.policy
    - https://www.googleapis.com/auth/admin.reports.audit.readonly
12. Cliquez sur **Autoriser**.
    Remarque : le fait d'autoriser cet API pour le compte de service permet à UEM d'accéder à l'annuaire de l'utilisateur pour votre domaine Google Cloud ou Google Workspace par Google.

Intégrer BlackBerry UEM à votre domaine Google Cloud ou Google Workspace par Google pour utiliser les terminaux Chrome OS

1. Connectez-vous à la console de gestion UEM à l'aide d'un compte d'administrateur de sécurité.
2. Sur la barre de menus, cliquez sur **Paramètres > Intégration externe > Android Enterprise**.
3. Sélectionnez **Connecter BlackBerry UEM à votre domaine Google existant**. Notez que vous ne pouvez pas partager de domaines Google entre plusieurs domaines BlackBerry UEM. Cette option prend en charge Android Enterprise et Chrome OS Enterprise.
4. Dans la section Mode d'envoi des configurations d'application, sélectionnez **Envoyer la configuration d'application à l'aide de Google Play**.
5. Cliquez sur **Suivant**.
6. Dans le champ **Mot de passe de clé privée**, collez le mot de passe de la clé privée que vous avez copié depuis la console Google Developers.
7. À côté du champ **Fichier de certificat P12**, cliquez sur **Parcourir**.
8. Accédez au fichier de certificat reçu à partir de la console Google Developers, puis cliquez sur **Ouvrir**.
9. Dans le champ **Adresse e-mail du compte de service**, collez l'adresse électronique du compte de service Google que vous avez copiée à partir de la console Google Developers.
10. Dans le champ **Adresse électronique pour l'administrateur de domaine Google**, saisissez l'adresse électronique du compte d'administrateur utilisé pour gérer le domaine Google Cloud ou Google Workspace par Google.
11. Dans le champ **Jeton**, collez le jeton que vous avez généré dans le domaine Google.
12. Dans la section **Sélectionnez le type de domaine utilisé pour la gestion des terminaux Android avec profil professionnel**, indiquez si vous disposez d'un domaine Google Cloud ou Google Workspace par Google.

13. Si vous sélectionnez un domaine Google Cloud, choisissez l'une des options suivantes :

- **Ne pas autoriser BlackBerry UEM à créer des utilisateurs dans le domaine** : si vous choisissez cette option, vous devez créer des utilisateurs dans votre domaine Google Cloud et créer des utilisateurs locaux avec les mêmes adresses électroniques dans UEM.
- **Autoriser BlackBerry UEM à créer des utilisateurs dans le domaine** : si vous choisissez cette option, sélectionnez l'une des options suivantes :
  - **Ne pas autoriser BlackBerry UEM à supprimer des utilisateurs dans le domaine Google**
  - **Autoriser BlackBerry UEM à supprimer des utilisateurs dans le domaine Google**

14. Cliquez sur **Suivant** et choisissez les applications que vous souhaitez ajouter à UEM.

15. Cliquez sur **Suivant**.

16. Cliquez sur **Suivant**.

Synchroniser BlackBerry UEM avec la console d'administration Google

Après avoir synchronisée BlackBerry UEM avec votre domaine Google, vous pouvez effectuer certaines actions de gestion sur les terminaux Chrome OS de votre organisation, telles que l'activation, la désactivation et l'annulation de la gestion.

1. Connectez-vous à la console de gestion UEM à l'aide d'un compte d'administrateur de sécurité.
2. Sur la barre de menus, cliquez sur **Paramètres > Intégration externe > Android Enterprise**.
3. Dans la section Gestion de Chrome OS, cliquez sur **Activer**. Ce bouton effectue une synchronisation initiale des données en 10 minutes et planifie également des synchronisations régulières.
   Remarque : une fois la synchronisation terminée, vous pouvez utiliser les boutons **Synchroniser les unités organisationnelles, Synchroniser les utilisateurs** et **Synchroniser les terminaux** pour effectuer des synchronisations non planifiées.

Simplification des activations Windows 10

Vous pouvez utiliser une application Web Java de BlackBerry comme service de détection afin de simplifier le processus d'activation pour les utilisateurs dotés de terminaux Windows 10. Si vous utilisez le service de détection, les utilisateurs n'auront plus besoin de saisir l'adresse du serveur lors du processus d'activation. Si vous choisissez de ne pas déployer cette application Web, les utilisateurs pourront toujours activer leurs terminaux Windows 10 en saisissant l'adresse du serveur lorsqu'ils sont invités à le faire.

Vous pouvez utiliser différents systèmes d'exploitation et outils d'application Web pour déployer une application Web de détection. Cette rubrique décrit les étapes avancées. Consultez la page Déployer un service de détection pour simplifier les activations Windows 10 pour connaitre les étapes à suivre avec les outils et les systèmes d'exploitation courants.

Pour déployer une application Web de détection, procédez comme suit :

Étape	Action
1	Créez un enregistrement hôte A statique au DNS pour le serveur d'applications Java. L'enregistrement doit indiquer `enterpriseenrollment.<email_domain>`, où <*email_domain*> correspond aux adresses électroniques de vos utilisateurs.
2	Si vous souhaitez autoriser les utilisateurs à activer des terminaux en dehors du réseau de votre organisation, configurez l'hôte du service de détection pour écouter le port 443.
3	Créez et installez un certificat pour sécuriser les connexions TLS entre les terminaux Windows 10 et le service de détection.
4	Connectez-vous à *my*Account pour télécharger l'outil de détection automatique de proxy. Exécutez le fichier pour extraire un fichier .war, puis déployez-le à la racine de votre serveur d'applications Java.
5	Mettez à jour le fichier wdp.properties de l'application Web de détection pour inclure les ID SRP de votre entreprise.

Intégration de UEM avec la jonction à Azure Active Directory

Vous pouvez intégrer BlackBerry UEM avec la jonction à Azure Active Directory pour simplifier le processus d'inscription pour les appareils Windows 10. Une fois la configuration terminée, les utilisateurs peuvent inscrire leurs terminaux avec UEM, à l'aide de leur nom d'utilisateur et de leur mot de passe Azure Active Directory. La jonction à Azure Active Directory est également nécessaire pour la prise en charge de Windows Autopilot, qui permet aux terminaux Windows 10 d'être activés automatiquement avec UEM lors de la configuration initiale de Windows 10.

Pour intégrer la jonction à Azure Active Directory avec UEM, procédez comme suit :

Étape	Description
1	Utilisez la valeur de la variable par défaut %ClientlessActivationURL% dans UEM pour déterminer les URL suivantes afin d'intégrer UEM avec la jonction à Azure Active Directory. Par exemple, dans l'écran d'information sur l'utilisateur d'un utilisateur qui utilise le modèle d'e-mail d'activation par défaut, vous pouvez cliquer sur **Afficher l'e-mail d'activation** pour trouver la valeur de %ClientlessActivationURL% dans le champ Nom du serveur Windows 10. 1. Déterminez l'URL des conditions d'utilisation de MDM. L'URL utilise la structure suivante : *%ClientlessActivationURL%*/azure/termsofuse Par exemple, si la variable %ClientlessActivationURL% correspond à `https://enrol.example.net/S123456789/win/mdm`, utilisez `https://enrol.example.net/S123456789/win/mdm/azure/termsofuse`. 2. Déterminez l'URL de détection de MDM. L'URL utilise la structure suivante : *%ClientlessActivationURL%*/azure/discovery Par exemple, si la variable %ClientlessActivationURL% correspond à `https://enrol.example.net/S123456789/win/mdm`, utilisez `https://enrol.example.net/S123456789/win/mdm/azure/discovery`. 3. Déterminez l'URI de l'ID de l'application en utilisant seulement le nom d'hôte de la variable par défaut %ClientlessActivationURL%. Par exemple, si la variable %ClientlessActivationURL% correspond à `https://enrol.example.net/S123456789/win/mdm`, utilisez `https://enrol.example.net`.
2	Intégrer UEM avec la jonction à Azure Active Directory.

Intégrer UEM avec la jonction à Azure Active Directory

Avant de commencer : Déterminez l'URL des conditions d'utilisation de MDM, l'URL de découverte MDM et l'URI de l'ID de l'application. Pour plus d'informations, reportez-vous à Intégration de UEM avec la jonction à Azure Active Directory.

1. Connectez-vous au portail de gestion Microsoft Azure à l'adresse https://portal.azure.com.
2. Accédez à **Mobilité (MDM et MAM)**.
3. Cliquez sur **Ajouter une application**.
4. Cliquez sur **Application MDM sur site**. Saisissez un nom convivial (par exemple, `BlackBerry UEM`).
5. Cliquez sur **Ajouter**.
6. Cliquez sur l'application que vous avez ajoutée à l'étape précédente pour configurer ses paramètres.
7. Spécifiez la portée de l'utilisateur, **Tout** ou **Partie**. Le cas échéant, sélectionnez les groupes.
8. Dans le champ **URL des conditions d'utilisation de MDM**, spécifiez l'URL.
9. Dans le champ **URL de détection de MDM**, spécifiez l'URL.
10. Cliquez sur **Enregistrer**.
11. Cliquez sur **Paramètres de l'application MDM sur site > Propriétés**.
12. Dans le champ **URI de l'ID de l'application**, spécifiez l'URL.
13. Cliquez sur **Enregistrer**.

Configuration de Windows Autopilot dans Microsoft Azure

Pour la prise en charge de l'activation de l'appareil Windows Autopilot, procédez comme suit :

Étape	Description
1	Intégrer UEM avec la jonction à Azure Active Directory.
2	Créer un profil de déploiement Windows Autopilot dans Azure et attribuez-le à des groupes d'utilisateurs dans Azure.
3	Importer des terminaux Windows Autopilot dans Azure.

Créer un profil de déploiement Windows Autopilot dans Azure

Vous devez attribuer un profil de déploiement Windows Autopilot aux groupes d'utilisateurs appropriés dans Azure pour permettre aux utilisateurs d'activer leur terminal à l'aide de Windows Autopilot.

1. Connectez-vous au portail de gestion Microsoft Azure à l'adresse https://portal.azure.com.
2. Naviguez jusqu'à **Inscription de l'appareil > Inscription Windows > Profils de déploiement Windows Autopilot**.
3. Créez un profil de déploiement Windows Autopilot.
4. Saisissez le nom et la description du profil.
5. Configurez les paramètres de configuration initiale.
6. Attribuez le profil aux groupes d'utilisateurs appropriés.
7. Cliquez sur **Enregistrer**.

Importer des terminaux Windows Autopilot dans Azure

Procédez comme suit pour importer chaque terminal Windows 10 qui pourra être activé avec Windows Autopilot.

1. Mettez le terminal Windows 10 sous tension pour charger la configuration prête à l'emploi.
2. Connectez-vous à un réseau Wi-Fi avec une connexion Internet.
3. Sur le clavier, appuyez sur **CTRL + MAJ + F3** ou **CTRL + Fn + MAJ + F3**. Le terminal redémarre et passe en mode audit.
4. Exécutez **Windows PowerShell** en tant qu'administrateur.
5. Exécutez `Save-script -Name Get-WindowsAutoPilotInfo -Path C:\Windows\Temp` pour inspecter le script Windows PowerShell.
6. Exécutez `Install-script -Name Get-WindowsAutoPilotInfo` pour installer le script.
7. Exécutez `get-WindowsAutoPilotInfo.ps1 -OutputFile C:\Windows\Temp\MyComputer.csv` pour enregistrer les informations du terminal dans un fichier .csv.
8. Pour importer un fichier .csv dans Microsoft Azure, procédez comme suit :
   a) Dans le portail Azure, accédez à **Inscription de l'appareil > Inscription Windows > Appareils Windows Autopilot**.
   b) Cliquez sur **Importer**.
   c) Sélectionnez le fichier .csv.
9. Dans la boîte de dialogue **Outil de préparation système**, procédez comme suit :

a) Dans le champ **Action de nettoyage du système**, sélectionnez **Entrer en mode OOBE (Out-of-Box Experience)** et désélectionnez **Généraliser**.
b) Dans le champ **Options d'extinction**, sélectionnez **Redémarrer**.

Déployer un service de détection pour simplifier les activations Windows 10

Les étapes suivantes décrivent comment déployer l'application Web du service de détection dans l'environnement décrit ci-dessous.

Avant de commencer : vérifiez que les logiciels suivants sont installés et fonctionnent dans votre environnement :

- Windows Server 2012 R2
- Java JRE 1.8 ou version ultérieure
- Apache Tomcat 8 v8.0 ou version ultérieure

1. Configurez une adresse IP statique pour l'ordinateur qui hébergera le service de détection.

   Remarque : si vous souhaitez autoriser les utilisateurs à activer leurs terminaux en dehors du réseau de l'organisation, l'adresse IP doit être accessible de l'extérieur via le port 443.
2. Créez un enregistrement DNS de type A pour le nom **enterpriseenrollment.<*email_domain*>** qui renvoie vers l'adresse IP statique configurée lors de l'étape 1.
3. Dans le répertoire d'installation de Apache Tomcat, recherchez la section **8080** dans le fichier server.xml et modifiez les balises de commentaire comme indiqué ci-dessous :

```
<!--
    <Connector port="8080" protocol="HTTP/1.1"
    connectionTimeout="20000"
    redirectPort="8443" />
    -->
```

4. Dans le fichier **server.xml**, remplacez toutes les occurrences de **8443** par **443**.
5. Recherchez la section **<Connector port="443"**, supprimez les balises de commentaire en haut et en bas, puis apportez les modifications comme indiqué ci-dessous :

```
<Connector port="443" protocol="org.apache.coyote.http11.Http11NioProtocol"
    maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
    clientAuth="false" sslProtocol="TLS" keystoreFile="C:\Users\<nom_compte>
\.keystore" />
```

6. Tout en étant connecté au compte configuré précédemment, générez un certificat en exécutant les deux commandes ci-dessous. Lorsque vous êtes invité(e) à saisir votre nom de famille et votre prénom, saisissez `enterpriseenrollment.<email _domain>` comme indiqué ci-dessous :

```
C:\Program Files (x86)\Java\jre1.8.0_60\bin>keytool -genkey -alias tomcat -
keyalg RSA -keysize 2048
```

```
C:\Program Files (x86)\Java\jre1.8.0_60\bin> keytool -certreq -alias tomcat -
keyalg RSA -file <filename>.csr
```

```
C:\Program Files (x86)\Java\jre1.8.0_60\bin>keytool -genkey -alias tomcat -
keyalg RSA -keysize 2048 Saisissez le mot de passe : changeit
    Quels sont votre prénom et votre nom ?
```

```
      [Unknown] :  enterpriseenrollment.example.com
   Quel est le nom de votre unité organisationnelle ?
     [Unknown] :  IT Department
   Quel est le nom de votre organisation ?
     [Unknown] :  Manufacturing Co.
   Quel est le nom de votre ville ou localité ?
     [Unknown] :  Waterloo
   Quel est le nom de votre état ou province ?
     [Unknown] :  Ontario
   Quel est le code pays (composé de deux lettres) pour cette unité ?
     [Unknown] :  CA
   Est-ce que CN=enterpriseenrollment.example.com, OU=Business Unit, O=Example
Company, L=Waterloo, ST=Ontario, C=CA sont corrects ?
     [no] :  oui

   C:\Program Files (x86)\Java\jre1.8.0_60\bin>keytool -certreq -alias tomcat
-keyalg RSA -file <enterpriseenrollment.example.com>.csr
   Saisissez le mot de passe de la clé de <enterpriseenrollment.example.com>
           (REVENIR EN ARRIÈRE si identique au mot de passe du magasin de
clés) :
```

7. Envoyez votre demande de signature de certificat à une autorité de certification. L'autorité de certification vous renverra un fichier .p7b. Dans l'exemple ci-dessus, l'autorité de certification doit renvoyer le fichier `enterpriseenrollment.example.com.p7b`.
   - Si vous envoyez votre demande de signature de certificat à une grande autorité de certification externe, les utilisateurs accepteront automatiquement ce certificat lors du processus d'activation.
   - Si vous envoyez votre demande de signature de certificat à une autorité de certification interne, les utilisateurs devront installer le certificat d'autorité de certification sur leur terminal avant de procéder à l'activation.
8. Pour installer le certificat, utilisez la commande indiquée ci-dessous :

```
C:\Program Files (x86)\Java\jre1.8.0_60\bin>keytool -import -trustcacerts -
alias tomcat -file <filename>.p7b
```

9. Fermez Apache Tomcat.
10. Rendez-vous sur myAccount pour télécharger l'outil de détection automatique de proxy. Extrayez le contenu du fichier .zip et exécutez le fichier **W10AutoDiscovery-<*version*>.exe**.
    Le fichier .exe extrait le fichier `W10découverte-<version>.war` vers `C:\BlackBerry`.
11. Dans le répertoire d'installation de Apache Tomcat, cherchez le dossier `\webapps\ROOT`. Si vous le trouvez, supprimez le dossier `\ROOT`.
12. Renommez `W10AutoDiscovery-<version>.war` en `ROOT.war`. Déplacez-le dans le dossier `\webapps` dans le répertoire d'installation d'Apache Tomcat.
13. Démarrez Apache Tomcat.
    Apache Tomcat déploiera la nouvelle application Web et créera un dossier `\webapp\ROOT folder`.
14. Exécutez notepad.exe en tant qu'administrateur. Dans le répertoire où vous avez installé Apache Tomcat, ouvrez `\webapps\ROOT\WEB-INF\classes\config\wdp.properties`.
15. Ajoutez l'ID d'hôte de votre domaine BlackBerry UEM à la ligne `wdp.whitelisted.srpid`, comme illustré dans l'exemple ci-dessous. L'ID d'hôte de votre domaine BlackBerry UEM se trouve dans la console de gestion BlackBerry UEM. Si vous disposez de plusieurs domaines BlackBerry UEM, spécifiez l'ID d'hôte de chacun d'eux. Procédez comme suit :
    a) Sur la barre de menus, cliquez sur **Paramètres > Gestion des licences > Résumé des licences**.
    b) Cliquez sur **Activer les licences**.

c) Dans la liste déroulante **Mode d'activation des licences**, cliquez sur **ID d'hôte**.

```
wdp.whitelisted.srpid=<Host ID>, <Host ID>, <Host ID>
```

16. Redémarrez Apache Tomcat.

Migration d'utilisateurs, de terminaux, de groupes et d'autres données depuis un serveur source

Vous pouvez utiliser la console de gestion BlackBerry UEM pour migrer les utilisateurs, terminaux, groupes et autres données depuis les serveurs source suivants :

- BlackBerry UEM (sur site)
- Good Control (autonome)

Remarque : Si vous voulez migrer des utilisateurs, des terminaux, des groupes et d'autres données depuis un serveur BES10 source, vous devez effectuer une migration vers BlackBerry UEM version 12.9, puis une mise à niveau vers BlackBerry UEM version 12.11, puis vers la version 12.14 et enfin vers la version 12.16. La migration directe de BES10 vers BlackBerry UEM version 12.10 et ultérieure n'est pas prise en charge.

Remarque : Pour plus d'informations sur la migration des utilisateurs et des terminaux BlackBerry Dynamics par lots à l'aide de fichiers .csv, rendez-vous sur support.blackberry.com/community pour consulter l'article 49442.

Pour migrer des utilisateurs, des terminaux, des groupes et d'autres données, procédez comme suit :

Étape	Action
1	Passez en revue les conditions préalables à une migration.
2	Connexion à un serveur source.
3	Facultatif : migrez les stratégies informatiques, les profils et les groupes.
4	Pour les migrations effectuées à partir d'un serveur BlackBerry UEM source avec des applications BlackBerry Dynamics inscrites, ou à partir d'un serveur Good Control source, migrer des stratégies et des profils pour les utilisateurs activés pour BlackBerry Dynamics.
5	Migrez les utilisateurs.
6	Migrez les terminaux.

Conditions préalables : migrer des utilisateurs, terminaux, groupes et autres données depuis un serveur source

Vous devez remplir les conditions préalables suivantes avant de lancer une migration.

Condition préalable	Détails
Se connecter	Connectez-vous à BlackBerry UEM en tant qu'administrateur de sécurité. Un seul administrateur doit effectuer des opérations de migration, à la fois.
Vérifier la version du logiciel	Pour migrer des données vers BlackBerry UEM : • L'instance BlackBerry UEM à partir de laquelle vous migrez les données doit correspondre à la version 12.15 ou ultérieure. • L'instance de Good Control (autonome) à partir de laquelle vous migrez les données doit correspondre à la version 5.0 ou ultérieure.
Configurez la connexion au répertoire d'entreprise BlackBerry UEM	Configurez la connexion au répertoire d'entreprise BlackBerry UEM de destination telle qu'elle est configurée dans l'instance source. Par exemple, si l'instance source est configurée pour l'intégration d'Active Directory et qu'elle est connectée au domaine exemple.com, configurez l'instance BlackBerry UEM de destination pour l'intégration Active Directory et connectez-la au domaine exemple.com. **Important :** La migration ne fonctionnera pas si le répertoire d'entreprise du serveur de destination ne correspond pas au répertoire d'entreprise du serveur source.
Défragmentez les bases de données (BlackBerry UEM)	Défragmentez les bases de données sources et la base de données BlackBerry UEM de destination (le cas échéant) avant de commencer la migration. Si vous déplacez un grand nombre d'utilisateurs, vous devrez défragmenter la base de données BlackBerry UEM de destination après la migration de chaque groupe d'utilisateurs. Pour en savoir plus sur la défragmentation d'une base de données Microsoft SQL Server, rendez-vous sur www.technet.microsoft.com et consultez l'article « Réorganiser et reconstruire des index ».
BlackBerry UEM Client	Pour la migration des applications BlackBerry Dynamics et des BlackBerry UEM Client inscrits par BlackBerry Dynamics à partir d'une base de données BlackBerry UEM source sur site, le dernier BlackBerry UEM Client doit être installé sur le terminal.
Vérifiez l'état des applications BlackBerry Dynamics	Vérifiez la version BlackBerry Dynamics SDK de toutes les applications BlackBerry Dynamics que vous souhaitez migrer. Cela inclut les applications principales, les applications BlackBerry Dynamics, les applications ISV et les applications personnalisées internes. Pour les migrations effectuées à partir d'une base de données BlackBerry UEM source sur site, toutes les applications BlackBerry Dynamics doivent correspondre à la version 7.1 ou ultérieure de BlackBerry Dynamics SDK. Vous trouverez la version du SDK dans les notes de version de l'application. Pour les migrations effectuées à partir d'une instance de Good Control (autonome), toutes les applications doivent correspondre à la version 4.0.0 ou ultérieure de BlackBerry Dynamics SDK. Pour déterminer la version du SDK utilisé pour les applications à migrer, exécutez le rapport d'activité du conteneur sur Good Control. **Les applications BlackBerry Dynamics qui ne sont pas prises en charge pour la migration sont effacées du terminal lorsque l'administrateur commence la migration.**

Condition préalable	Détails
Vérifiez l'état des autorisations des applications BlackBerry Dynamics	Assurez-vous que : • Le serveur BlackBerry UEM de destination dispose de la même liste d'autorisations d'applications BlackBerry Dynamics que le serveur source. • Tous les comptes utilisateur migrés se voient attribuer la même liste d'autorisations d'applications BlackBerry Dynamics sur le serveur BlackBerry UEM de destination que celle dont ils disposent sur le serveur source. • Le délégué d'authentification est le même sur le serveur source et le serveur de destination. Vous pouvez modifier le délégué d'authentification après la migration. • Le profil BlackBerry Dynamics de l'utilisateur permet à BlackBerry UEM Client d'être activé par BlackBerry Dynamics, si l'instance de BlackBerry UEM Client de l'utilisateur sur le serveur source est également activée par BlackBerry Dynamics.  **ATTENTION :** S'il manque des autorisations, les applications BlackBerry Dynamics sont désactivées après la migration.
Vérifiez les ID d'organisation	Les applications personnalisées sont migrées uniquement si les serveurs source et de destination ont le même ID d'organisation. Il est possible de fusionner les deux organisations. Pour en savoir plus, rendez-vous sur le site Web support.blackberry.com/community pour consulter l'article 47626.
Vérifiez que les ports requis ne sont pas bloqués par un pare-feu ou utilisés par un autre logiciel	Assurez-vous que les ports 1433 (TCP) et 1434 (UDP) sont débloqués sur Microsoft SQL Server.

Connexion à un serveur source

Vous devez connecter BlackBerry UEM au serveur source à partir duquel vous souhaitez migrer les données. Vous pouvez ajouter plusieurs sources, mais une seule peut être active à la fois.

Remarque : Assurez-vous que le compte de base de données associé aux informations d'identification que vous utilisez pour vous connecter à la base de données dispose des autorisations d'écriture.

Remarque : Si vous avez mis à niveau votre serveur BlackBerry UEM source depuis la dernière migration, vous devez supprimer la configuration du serveur source, puis la recréer avant de procéder à une autre migration.

1. Sur la barre de menus, cliquez sur **Paramètres > Migration > Configuration**.
2. Cliquez sur +.
3. Dans la liste déroulante **Type de source**, sélectionnez le type de serveur source.
4. En fonction du type de serveur source que vous avez sélectionné, remplissez les champs comme suit :

Type de serveur source	Champ	Contenu
BlackBerry UEM	nom d'affichage ;	Entrez un nom descriptif pour le serveur source.
	Serveur de base de données	Saisissez le nom de l'ordinateur qui héberge la base de données source, au format <hôte>\<instance> pour un port dynamique et au format <hôte>:<port> pour un port statique.
	Type d'authentification de la base de données	Sélectionnez le type d'authentification à utiliser pour vous connecter à la base de données source.
	Nom d'utilisateur SQL Mot de passe SQL	Si vous avez sélectionné l'authentification SQL, dans les champs Nom d'utilisateur SQL et Mot de passe SQL, saisissez vos informations de connexion pour vous connecter à la base de données source.
	Nom de la base de données	Entrez le nom de la base de données source.
	Type d'authentification UEM source	Sélectionnez le type d'authentification utilisé pour se connecter à la console de gestion BlackBerry UEM source.
	nom d'utilisateur ; Mot de passe	Saisissez vos informations de connexion pour vous connecter à la console de gestion source.
	Domaine	Si vous avez sélectionné l'authentification Microsoft Active Directory, saisissez le nom du domaine où est située la console de gestion source.
Good Control (autonome)	nom d'affichage ;	Entrez un nom descriptif pour le serveur source.
	Nom de l'hôte source Good Control (autonome)	Saisissez le FQDN de la console de gestion Good Control.
	Source du certificat Good Control (autonome)	Téléchargez le certificat racine CA Good Control pour établir des connexions SSL. Le fichier de certificat doit être au format CER. Pour obtenir des instructions, reportez-vous à la section Exporter le certificat racine autosigné pour le serveur Good Control.

Type de serveur source	Champ	Contenu
	nom d'utilisateur ; Mot de passe	Saisissez vos informations de connexion pour vous connecter au compte d'administrateur de la console de gestion source. **Remarque :** Ces informations d'identification doivent correspondre à un administrateur Good Control disposant des droits d'accès MANAGE_CONTAINERS et MANAGE_USERS_AND_GROUPS. Le compte peut être un compte de service Good Control ou un compte d'administrateur ordinaire, à condition que le mot de passe associé au compte permette d'accéder à la console de gestion. Vous ne pouvez pas utiliser un compte d'utilisateur Active Directory avec un jeton physique et aucun mot de passe.
	Domaine	Saisissez le nom du domaine où se situe le compte d'administrateur de la console de gestion source. Vous pouvez laisser ce champ vide si l'administrateur est un utilisateur local qui n'a pas de domaine.

5. Cliquez sur **Enregistrer**.
6. Pour tester la connexion entre la source et la destination, cliquez sur **Test de connexion**.
7. Cliquez sur **Enregistrer**.

À la fin :

- Si vous souhaitez migrer des stratégies informatiques, profils et groupes, consultez les meilleures pratiques et reportez-vous à la section Migrer des stratégies informatiques, des profils et des groupes depuis un serveur source.
- Si vous souhaitez migrer des utilisateurs, consultez les considérations et reportez-vous à la section Migrer des utilisateurs depuis un serveur source.
- Après avoir migré des utilisateurs, reportez-vous à la section Migrer des terminaux depuis un serveur source.

Exporter le certificat racine autosigné pour le serveur Good Control

Effectuez l'opération suivante si le certificat Good Control n'a pas été remplacé par un certificat tiers. BlackBerry UEM approuve par défaut les certificats tiers, ce qui signifie que vous n'avez pas à exporter le certificat du serveur Good Control ni à l'importer dans BlackBerry UEM.

Remarque : La tâche suivante n'est pas spécifique au navigateur. Pour obtenir des instructions spécifiques, reportez-vous à la documentation du navigateur que vous utilisez.

1. Dans un navigateur, accédez à l'écran de connexion de l'un de vos serveurs Good Control. Un message d'erreur de certificat peut s'afficher car l'autorité de certification qui a signé le certificat était Good Control et que le navigateur ne le reconnait pas comme une autorité de certification connue.
2. Pour ouvrir la boite de dialogue Certificat, cliquez sur l'icône de certificat dans le champ URL.
3. Cliquez sur **Afficher le certificat** ou sur **Informations de certificat** pour ouvrir le menu **Gestion des certificats**.
4. Cliquez sur l'onglet **Chemin de certification**.

5. Sélectionnez le certificat racine. Le certificat racine est le premier élément dans la hiérarchie des certificats (par exemple GD12345678 CA).
6. Cliquez sur **Afficher le certificat**.
7. Cliquez sur l'onglet **Détails**.
8. Cliquez sur **Copier dans un fichier** ou sur **Exporter**.
9. Sélectionnez le format **DER encoded binary X.509 (.CER)** ou **Base-64 encoded X.509 (.CER)**.
10. Saisissez un emplacement et un nom de fichier pour le certificat.
11. Cliquez sur **Suivant** ou sur **Enregistrer**.
12. Cliquez sur **Terminer**.

Considérations : Migration des stratégies informatiques, des profils et des groupes depuis un serveur source

La migration depuis une source BlackBerry UEM copie les éléments suivants dans la base de données de destination :

- Stratégies informatiques sélectionnées
- Profils de messagerie
- Profils Wi-Fi
- Profils VPN
- Profils proxy
- Profils BlackBerry Dynamics
- Profils de certificat d'autorité de certification
- Profils des certificats partagés
- Récupération de certificat
- Profils d'informations d'identification de l'utilisateur
- Profils SCEP
- Profils CRL
- Profils OSCP
- Paramètres d'autorité de certification (Entrust et connecteur PKI uniquement)
- Toutes les politiques et tous les profils associés aux politiques et aux profils sélectionnés
- Pour la migration à partir de BlackBerry UEM sur site version 12.12.1 et versions ultérieures uniquement : Paramètres de configuration de l'application, profils de connectivité BlackBerry Dynamics et certificats client (utilisation de l'application).

Remarque : Pour les groupes migrés depuis BlackBerry UEM, les attributions d'utilisateurs, de rôles et de configurations logicielles ne sont pas migrées. Vous devez recréer manuellement ces attributions sur le serveur BlackBerry UEM de destination.

La migration d'une source Good Control (autonome) copie les éléments suivants dans la base de données de destination :

- Ensembles de stratégies
- Profils de connectivité
- Groupes d'applications
- Utilisation des applications (pour les certificats)
- Certificats

BlackBerry UEM

Lorsque vous migrez des stratégies informatiques, des profils et des groupes BlackBerry UEM vers un autre domaine, tenez compte des recommandations suivantes :

Élément	Considérations
Mots de passe de stratégie informatique	Si le mot de passe d'une stratégie informatique source sélectionnée pour les terminaux Android comporte moins de 4 caractères ou plus de 16 caractères, aucune stratégie informatique ni aucun profil BlackBerry UEM ne peut être migré. Désélectionnez ou mettez à jour la stratégie informatique source et redémarrez la migration.
Noms de profil	Après la migration, vous devez vous assurer que tous les profils SCEP, d'informations d'identification de l'utilisateur, de certificats partagés et de certificats d'autorité de certification disposent de noms uniques. Si deux profils du même type ont le même nom, vous devez modifier l'un des noms de profils.
Groupes de répertoires	Pour migrer des groupes de répertoires, les bases de données source et de destination doivent chacune disposer d'un répertoire configuré. Ce répertoire doit être configuré de la même façon dans les bases de données source et de destination. Dans le cas contraire, les groupes de répertoires ne seront pas migrés.

Applications activées avec BlackBerry Dynamics

Lorsque vous migrez des ensembles de stratégies, des profils de connectivité, des groupes d'applications et des certificats vers BlackBerry UEM, tenez compte des recommandations suivantes :

Lorsque vous migrez les profils de connectivité et l'utilisation des certificats vers BlackBerry UEM, tenez compte des recommandations suivantes :

Élément	Considérations
Ensembles de stratégies (Good Control uniquement)	Après la migration, chaque ensemble de stratégies Good Control apparait comme les éléments suivants dans BlackBerry UEM : • Une configuration d'application pour chaque application dans l'ensemble de stratégies • stratégie de sécurité • stratégie de conformité
Profils de connectivité	Lorsque les profils de connectivité BlackBerry Dynamics sont migrés, les valeurs de l'onglet Serveurs d'applications ne sont pas migrées. Les valeurs sont renseignées à l'aide des valeurs par défaut du serveur BlackBerry UEM de destination. Lorsque les profils de connectivité BlackBerry Dynamics sont migrés, certaines valeurs de l'onglet Infrastructure ne sont pas migrées. L'administrateur doit modifier manuellement chaque profil migré et définir les valeurs du cluster BlackBerry Proxy principal et du cluster BlackBerry Proxy secondaire.

Élément	Considérations
Groupes d'applications (Good Control uniquement)	Le groupe Tout le monde est migré mais aucun utilisateur ne lui est attribué et il n'est pas lié au groupe Tous les utilisateurs dans le serveur BlackBerry UEM de destination. L'administrateur doit attribuer le groupe à des utilisateurs manuellement si nécessaire.
Applications	Si une autorisation d'application du serveur source n'existe pas dans le serveur de destination, cette attribution d'application n'est pas migrée. Le groupe d'applications est migré.
Utilisation des certificats (BlackBerry UEM)	L'utilisation des certificats est migrée, à l'exception des : • Utilisations des certificats qui existent déjà dans le serveur de destination • Applications non-BlackBerry Dynamics • Applications personnalisées d'une autre organisation Good Control

Migrer des stratégies informatiques, des profils et des groupes depuis un serveur source

Facultatif : vous pouvez migrer des stratégies informatiques, des profils et des groupes depuis un serveur source.

1. Sur la barre de menus, cliquez sur **Paramètres**.
2. Si plusieurs sources sont configurées, dans le volet de gauche, cliquez sur **Migration > Configuration**, puis sélectionnez le bouton radio situé en regard du nom du serveur source à partir duquel vous souhaitez migrer les données.
3. Cliquez sur **Migration** > **Stratégies informatiques, profils, groupes**.
4. Cliquez sur **Suivant**.
5. Cochez les cases pour indiquer les éléments à migrer.

   Le nom du serveur source est ajouté à chaque politique et chaque nom de profil lors de la migration vers la destination.
6. Cliquez sur **Aperçu** pour consulter les stratégies et les profils sélectionnés.
7. Cliquez sur **Migrer**.
8. Pour configurer les stratégies informatiques, les profils et les groupes, cliquez sur **Configurer les stratégies informatiques et les profils** afin d'accéder à l'écran **Stratégies et profils**.

À la fin : Sur le serveur de destination, créez les stratégies et profils qui n'ont pas été migrés et associez-les aux utilisateurs avant de migrer les terminaux.

À la fin : Pour des informations spécifiques sur ce qu'il faut faire lorsque vous effectuez la migration depuis un serveur source Good Control, reportez-vous à la section Effectuer la migration des stratégies et des profils de Good Control à BlackBerry UEM.

Migrer des stratégies et des profils pour les utilisateurs activés pour BlackBerry Dynamics

Après la migration des utilisateurs, terminaux, groupes et d'autres données de Good Control vers BlackBerry UEM, vous devez effectuer les tâches suivantes sur l'instance de BlackBerry UEM de destination. Pour obtenir des informations sur l'emplacement des fonctions Good Control dans BlackBerry UEM, reportez-vous à la section Fonctionnalités Good Control dans BlackBerry UEM.

Reconstruire les relations entre les applications, les stratégies et les utilisateurs :

- Attribuez des configurations d'application aux applications BlackBerry Dynamics dans les groupes.
- Attribuez des profils de connectivité aux groupes.
- Attribuez des stratégies BlackBerry Dynamics migrées et des stratégies de conformité Good Control aux utilisateurs.
- Définissez des profils de remplacement (profils BlackBerry Dynamics et profils de conformité).
- Déplacez les configurations de fichier .json de Good Control vers BlackBerry UEM (pour les migrations depuis Good Control uniquement).

Renseignez les profils de connectivité migrés :

- Entrez les informations des serveurs d'applications.
- Définissez les clusters BlackBerry Proxy dans l'onglet Infrastructure.

Fonctionnalités Good Control dans BlackBerry UEM

Le tableau suivant mappe les fonctionnalités Good Control à leur emplacement dans BlackBerry UEM, où vous pouvez effectuer la même tâche.

Fonctionnalité Good Control	Où la trouver dans BlackBerry UEM
Utilisateurs et groupes	Cliquez sur **Utilisateurs**.
Administrateurs	Cliquez sur **Paramètres** > **Administrateurs**.
Gérer des applications et des droits BlackBerry Dynamics	**Applications**, puis cliquez sur l'application que vous souhaitez gérer .
Balayer du doigt, déverrouiller, verrouiller et gérer les journaux des applications BlackBerry Dynamics	1. Sur la barre de menus, cliquez sur **Utilisateurs**. 2. Recherchez un compte d'utilisateur. 3. Dans les résultats de la recherche, cliquez sur le nom du compte d'utilisateur. 4. Sélectionnez l'onglet du terminal qui a installé l'application que vous souhaitez gérer. 5. Dans la section **Applications BlackBerry Dynamics**, en regard de l'application que vous souhaitez gérer, choisissez la commande.

Fonctionnalité Good Control	Où la trouver dans BlackBerry UEM
Générer des clés d'accès	1. Cliquez sur **Utilisateurs**. 2. Sélectionnez l'utilisateur pour lequel vous souhaitez générer une clé d'accès. 3. Cliquez sur **Définir le mot de passe d'activation**. 4. Sélectionnez l'option **Génération de clé d'accès BlackBerry Dynamics**.
Gérer des services	Cliquez sur **Paramètres** > **BlackBerry Dynamics** > **Services d'application**.
Groupes d'applications	Cliquez sur **Groupes** > **Utilisateur**.
Stratégies de sécurité	Cliquez sur **Stratégies et profils** > **BlackBerry Dynamics**.
Stratégies de conformité	Cliquez sur **Stratégies et profils** > **Conformité (BlackBerry Dynamics)**.
Déploiement de profils	Cliquez sur **Paramètres** > **Paramètres d'activation par défaut**.
Stratégies spécifiques d'application	Cliquez sur **Applications**, puis sur l'application BlackBerry Dynamics que vous souhaitez gérer.
Ajouter des serveurs d'applications	Cliquez sur **Stratégies et profils** > **Connectivité (BlackBerry Dynamics)**.
Profil de connectivité	Cliquez sur **Stratégies et profils** > **Connectivité BlackBerry Dynamics**.
Stratégies des terminaux	Cliquez sur **Stratégies et profils** > **Stratégie** > **Stratégies informatiques**.
Configurations de terminal	Cliquez sur **Stratégies et profils** > **Réseaux et connexions** et choisissez les profils suivants : • Wi-Fi • VPN • Proxy • E-mail • Icône Web • Charge utile personnalisée
Apple DEP	Cliquez sur **Paramètres** > **Intégration externe** > **Programme d'inscription de terminaux Apple**
Gestion d'APNs	Cliquez sur **Paramètres** > **Intégration externe** > **Notification push Apple**
Gérer le libre-service utilisateur	Cliquez sur **Paramètres** > **Libre-service**
Paramètres Direct Connect	Cliquez sur **Paramètres** > **BlackBerry Dynamics** > **Direct Connect**
Propriétés du serveur	Cliquez sur **Paramètres** > **BlackBerry Dynamics** > **Propriétés**
Configuration de cluster Good Proxy	Cliquez sur **Paramètres** > **BlackBerry Dynamics** > **Clusters**

Fonctionnalité Good Control	Où la trouver dans BlackBerry UEM
Autorités approuvées	Cliquez sur **Stratégies et profils** > **Certificats** > **Certificat CA**. Cliquez sur **Paramètres** > **Intégration externe** > **Autorité de certification**.
Définitions des certificats	Cliquez sur **Stratégies et profils** > **Certificats** > **Informations d'identification de l'utilisateur**. Cliquez sur **Paramètres** > **Intégration externe** > **Autorité de certification**.
Certificats téléchargés pour les utilisateurs	Cliquez sur **Utilisateurs** > **Tous les utilisateurs** > **Informations sur l'utilisateur** > **Résumé** > **Stratégie informatique et profils**.
Utilisation des applications	**Autoriser les applications BlackBerry Dynamics à utiliser les certificats et profils d'informations d'identification des utilisateurs** dans les pages d'informations des applications correspondantes.
Rapports	Cliquez sur **Paramètres** > **BlackBerry Dynamics** > **Rapports**
Tâches de serveur	Cliquez sur **Paramètres** > **BlackBerry Dynamics** > **Tâches**

Considérations : Migration des utilisateurs depuis un serveur source

Retenez ce qui suit lors de la migration d'utilisateurs vers un BlackBerry UEM de destination :

Élément	Considérations
Limite de migration	Vous pouvez simultanément migrer un maximum de 1000 utilisateurs à partir d'une source. Si vous sélectionnez un nombre d'utilisateurs supérieur au maximum autorisé, seul le nombre maximum sera migré vers le BlackBerry UEM de destination. Les autres utilisateurs seront ignorés. Répétez le processus de migration autant de fois que nécessaire pour migrer tous les utilisateurs à partir du serveur source. **Remarque :** Si BlackBerry UEM expire lors de la migration de 1 000 utilisateurs, essayez de migrer un plus petit nombre d'utilisateurs.
Adresse électronique	• Seuls les utilisateurs associés à une adresse e-mail peuvent être migrés. • Vous ne pouvez pas migrer un utilisateur qui utilise déjà la même adresse e-mail dans l'instance de BlackBerry UEM de destination. Ces utilisateurs n'apparaissent pas dans la liste des utilisateurs à migrer. • Si deux utilisateurs de la base de données source ont la même adresse électronique, un seul utilisateur apparait sur l'écran Migrer les utilisateurs.
Terminal	• Après la migration, l'utilisateur doit utiliser les mêmes informations de connexion qu'avant la migration pour BlackBerry UEM Self-Service.

Élément	Considérations
Mot de passe	Après la migration, les utilisateurs locaux doivent modifier leur mot de passe lorsqu'ils se connectent à BlackBerry UEM Self-Service pour la première fois. Les utilisateurs qui n'étaient pas autorisés à accéder à BlackBerry UEM Self-Service avant la migration ne disposent pas automatiquement d'une autorisation après la migration.
Groupes	• Vous pouvez filtrer les utilisateurs sans attribution de groupe pour inclure cet ensemble d'utilisateurs dans une migration. • Vous ne pouvez pas migrer un utilisateur qui est propriétaire d'un groupe de terminaux partagés. L'utilisateur n'apparait pas dans la liste des utilisateurs à migrer.

Migrer des utilisateurs depuis un serveur source

Vous pouvez migrer des utilisateurs depuis un serveur source vers le BlackBerry UEM de destination. Au terme de la migration, les utilisateurs sont conservés dans la source et la destination.

1. Sur la barre de menus, cliquez sur **Paramètres > Migration > Utilisateurs**.
2. Dans l'écran **Migrer les utilisateurs**, cliquez sur **Actualiser le cache**.

   La mise en cache des 1 000 utilisateurs peut prendre environ 10 minutes.

   BlackBerry UEM met en cache les données utilisateur pour accélérer les fonctions de recherche, mais les données utilisateur sont migrées directement depuis la source. L'actualisation du cache est obligatoire uniquement pour le premier ensemble d'utilisateurs migrés et est facultative par la suite.
3. Cliquez sur **Suivant**.
4. Sélectionnez les utilisateurs à migrer.

   Seuls les 20 000 premiers utilisateurs sont affichés. Recherchez le nom ou l'adresse e-mail de l'utilisateur pour localiser des utilisateurs spécifiques qui peuvent ne pas être compris dans les premiers 20 000. La sélection de tous les utilisateurs sélectionne uniquement les utilisateurs de la première page. Définissez le format de page en fonction du nombre d'utilisateurs que vous voulez sélectionner.

   Si des modifications sont apportées à la source après la mise à jour du cache, ces modifications ne sont pas prises en compte dans l'affichage des données du cache. Il est déconseillé d'apporter des modifications au serveur source lors de la migration, mais si vous le faites, actualisez le cache régulièrement.
5. Cliquez sur **Suivant**.
6. Attribuez un ou plusieurs groupes, ou une stratégie informatique et un ou plusieurs profils, aux utilisateurs sélectionnés.

   Pour plus d'informations, reportez-vous au contenu relatif à l'administration.
7. Cliquez sur **Aperçu**.
8. Cliquez sur **Migrer**.

À la fin : Migrer des terminaux depuis un serveur source.

Considérations : migration de terminaux à partir d'un serveur source

Retenez ce qui suit lors de la migration de terminaux vers un BlackBerry UEM de destination :

Élément	Considérations
Méthode recommandée	Il est préférable de migrer un terminal pour chaque configuration unique (par exemple, différents groupes, politiques, configurations d'application, etc.) pour s'assurer que le serveur de destination est configuré correctement avant de migrer le reste de vos terminaux.
Limite de migration	Vous pouvez simultanément migrer un maximum de 2 000 terminaux à partir d'un serveur source.
Destination BlackBerry UEM	Avant de migrer les terminaux, vérifiez que BlackBerry UEM prend en charge le type de terminal et le système d'exploitation correspondants.
Utilisateurs	• Les utilisateurs doivent exister dans le domaine BlackBerry UEM de destination. • Vous devez migrer tous les terminaux d'un utilisateur en même temps.
Terminaux iOS gérés sur une source BlackBerry UEM	• La dernière version de BlackBerry UEM Client doit être installée sur les terminaux iOS. • Les terminaux iOS auxquels est attribué un profil de verrouillage des applications ne peuvent pas être migrés, car BlackBerry UEM Client ne peut pas être ouvert à la migration. • Dans les paramètres d'application de toutes les applications, décochez la case **Supprimer l'application du terminal lorsque celui-ci est supprimé de BlackBerry UEM**. **Remarque :** Si vous tentez d'effectuer la migration sans effectuer cette étape, l'application est supprimée et le terminal peut être désinscrit de BlackBerry UEM. Cependant, même si vous décochez cette case, l'application peut toujours être supprimée pendant la migration si le paramètre n'a pas été transmis au terminal. Pour plus d'informations sur les commandes de suivi transmises à un terminal, rendez-vous sur support.blackberry.com/community et lisez l'article 102688.
Terminaux Android gérés sur une source BlackBerry UEM	• La dernière version de BlackBerry UEM Client doit être installée sur les terminaux Android Enterprise. • Vous ne pouvez pas migrer des terminaux Android qui utilisent un profil professionnel à l'aide d'un compte Google ou d'un domaine Google.
Terminaux Chrome OS sur une source BlackBerry UEM	Vous pouvez migrer des terminaux Chrome OS.
Terminaux Windows	Vous ne pouvez pas migrer des terminaux Windows.
Terminaux macOS	Vous ne pouvez pas migrer des terminaux macOS.
Contrôles MDM (BlackBerry UEM)	Lorsque la migration commence, les terminaux activés avec Contrôles MDM n'ont momentanément plus accès à la messagerie. Au terme de la migration, l'accès aux services de messagerie est rétabli.

Élément	Considérations
Groupes	Vous ne pouvez pas migrer un terminal appartenant à un groupe de terminaux partagés. Ces terminaux n'apparaissent pas dans la liste de migration.

Élément	Considérations
Terminaux compatibles avec BlackBerry Dynamics	**Applications BlackBerry Dynamics** • Toutes les applications BlackBerry Dynamics compatibles avec la migration sont migrées. **Les applications BlackBerry Dynamics qui sont incompatibles avec la migration sont effacées lorsque l'administrateur lance la migration.** Ces applications doivent être réactivées sur le BlackBerry UEM de destination. • Pour les migrations effectuées à partir d'une base de données BlackBerry UEM source sur site, toutes les applications BlackBerry Dynamics doivent correspondre à la version 7.1 ou ultérieure de BlackBerry Dynamics SDK. • Pour les migrations effectuées à partir d'une instance de Good Control (autonome), toutes les applications doivent correspondre à la version 4.0.0 ou ultérieure de BlackBerry Dynamics SDK. Pour déterminer la version du SDK utilisé pour les applications à migrer, exécutez le rapport d'activité du conteneur sur Good Control. • Dans l'écran Migrer les terminaux, la colonne des conteneurs incompatibles affiche, pour chaque terminal, le nombre d'applications BlackBerry Dynamics qui ne peuvent pas être migrées et le nombre total d'applications BlackBerry Dynamics. Cliquez sur le nombre pour afficher les applications BlackBerry Dynamics qui sont incompatibles avec la migration. • Assurez-vous que l'utilisateur dispose des autorisations requises pour l'application sur le BlackBerry UEM de destination. Si l'utilisateur ne dispose pas des autorisations requises, après la migration, il recevra un message indiquant que l'application est bloquée. • Les applications BlackBerry Dynamics ne sont pas migrées si le BlackBerry UEM de destination a déjà enregistré des applications pour cet utilisateur. • La migration de BlackBerry Access for Windows, de BlackBerry Access for macOS et de BlackBerry Enterprise BRIDGE n'est pas prise en charge. Une fois la migration terminée, les utilisateurs doivent réinscrire ces applications dans UEM. • Les applications personnalisées sont migrées uniquement si les serveurs source et de destination ont le même ID d'organisation. Il est possible de fusionner les deux organisations. Pour en savoir plus, rendez-vous sur le site Web support.blackberry.com/community pour consulter l'article 47626. • Les terminaux avec des applications BlackBerry Dynamics activées par plusieurs utilisateurs ne doivent pas être migrés. • Il est possible que les applications BlackBerry Dynamics qui sont verrouillées pour des raisons de conformité ou à distance par l'administrateur avant le processus de migration, ne fonctionnent plus après la migration et doivent être réactivées. Si BlackBerry UEM Client est verrouillé, l'utilisateur ne peut pas être migré. • Le processus de migration ne permet pas de suivre ou de garantir la migration de BlackBerry UEM Client et des applications activées sur un terminal après la mise en cache des données de ce terminal. Les administrateurs doivent actualiser le cache utilisateur avant chaque migration. **Authentification des terminaux** • Le délégué d'authentification doit être le même sur le serveur source et le BlackBerry UEM de destination. Vous pouvez modifier le délégué d'authentification après la migration. • Pour les migrations effectuées à partir d'une instance de Good Control (autonome), les terminaux avec un délégué d'authentification de terminal de Good for Enterprise ne sont pas migrés. Après la suppression de Good for Enterprise en tant que délégué d'authentification, actualisez le cache avant de poursuivre la migration. Il est recommandé de veiller à ce que l'utilisateur se voie attribuer le même délégué d'authentification sur le BlackBerry UEM que celui dont il disposait sur le serveur source.

Élément	Considérations
	Gestion des terminaux • Les terminaux avec BlackBerry Dynamics seul (et non BlackBerry UEM Client) sont visibles dans la base de données source jusqu'à ce que la migration de toutes les applications soit terminée. • Les terminaux compatibles avec BlackBerry Dynamics sont toujours inscrits pour BlackBerry Dynamics sur le serveur de destination. • Pour les migrations effectuées à partir d'une instance de Good Control (autonome), les inscriptions Good Dynamics MDM ne sont pas migrées. Les utilisateurs doivent se désinscrire de MDM. Si le BlackBerry UEM de destination nécessite MDM, l'utilisateur doit supprimer manuellement l'ancien profil MDM, installer et activer BlackBerry UEM Client, puis réinscrire le terminal pour MDM. **Système d'exploitation** • Les terminaux dotés d'un système d'exploitation inconnu ne sont pas migrés. **Sessions de chat** • Le serveur BEMS source peut garder d'anciennes sessions de chat Connect ouvertes pendant 24 heures. Par conséquent, l'utilisateur peut temporairement apparaitre connecté au chat depuis deux terminaux distincts. • Les messages de chat Connect non lus sont supprimés lors de la migration. Les utilisateurs doivent se déconnecter de Connect avant la migration. **Utilisateurs** • Si un utilisateur a plus d'un terminal avec des applications BlackBerry Dynamics, tous les terminaux sont automatiquement sélectionnés pour la migration. • Vous ne pouvez pas migrer des terminaux pour le même utilisateur à partir de plusieurs serveurs source Good Control. Vous pouvez migrer des terminaux à partir de sources Good Control multiples, mais les utilisateurs ne peuvent pas encore disposer d'un terminal BlackBerry Dynamics sur le BlackBerry UEM de destination. **Déverrouiller les clés** • Si un utilisateur oublie le mot de passe pour une application BlackBerry Dynamics alors que la migration a déjà été lancée, mais que la migration du conteneur n'est pas encore terminée, la clé d'accès de déverrouillage doit être obtenue depuis la source BlackBerry UEM. Une fois la migration terminée, la clé doit être obtenue à partir du BlackBerry UEM de destination. **Clés d'accès** • Après la migration, les clés d'accès ne peuvent plus être générées sur le serveur source. • Le terminal est supprimé du serveur source au début de la migration et les clés d'accès ne peuvent plus être générées. **Après le lancement de la migration** • Les utilisateurs de terminaux iOS doivent faire glisser leur doigt de bas en haut pour fermer les applications. • Pour déclencher la migration sur un terminal, il est préférable de commencer par ouvrir l'application qui est configurée en tant que délégué d'authentification sur ce terminal. • Tant que la migration n'est pas terminée, les applications ne s'affichent pas toutes sur le Launcher. • Après la migration, la disposition des icônes de l'application dans le Launcher est réinitialisée à la disposition par défaut. • Les terminaux chargent les règles VIP, les signets et les certificats d'utilisateur

	Configurations .json (Good Control uniquement) • Pour les migrations effectuées à partir d'une instance de Good Control (autonome), les configurations .json ne sont pas migrées. Étant donné que les configurations .json sont générales, la migration pourrait écraser les configurations .json dans la base de données de destination. Veillez à ce que toutes les configurations .json s'appliquent à nouveau dans le serveur de destination.

Référence rapide pour la migration des terminaux

Type de terminal	Type d'activation/configuration	Migration
Android	• Contrôles MDM • BlackBerry 2FA • Confidentialité de l'utilisateur • BlackBerry Dynamics (UEM à UEM)	Pris en charge
Terminaux Android Enterprisedotés d'un profil professionnel associé à un domaine Google	Indifférent	Non pris en charge
Terminaux Android Enterprise dotés d'un profil professionnel qui n'est pas associé à un compte Google ou un domaine Google	Indifférent	Pris en charge
Terminaux Android Samsung Knox Workspace dotés d'un profil professionnel associé à un compte Google ou un domaine Google	Indifférent	Non pris en charge
Terminaux Android Samsung Knox Workspace dotés d'un profil professionnel qui n'est pas associé à un compte Google ou un domaine Google	Indifférent	Pris en charge

Type de terminal	Type d'activation/configuration	Migration
iOS	• Contrôles MDM • Inscription du terminal pour BlackBerry 2FA uniquement • Terminaux DEP sur lesquels BlackBerry UEM Client est installé • Confidentialité de l'utilisateur • BlackBerry Dynamics (UEM à UEM)	Pris en charge
iOS	• Terminaux DEP sur lesquels BlackBerry UEM Client n'est pas installé • Inscription de l'utilisateur	Non pris en charge
Windows	Indifférent	Non pris en charge
macOS	Indifférent	Non pris en charge

Migrer des terminaux depuis un serveur source

Après avoir migré des utilisateurs du serveur source vers l'instance de BlackBerry UEM de destination, vous pouvez migrer leurs terminaux. Les terminaux sont transférés du serveur source vers l'instance de BlackBerry UEM de destination, et ne sont pas conservés dans la source après la migration.

Avant de commencer :

- Avant de migrer des terminaux, assurez-vous que les politiques et les droits appropriés sont affectés aux utilisateurs que vous avez migrés.
- Pour les migrations effectuées depuis BlackBerry UEM, informez les utilisateurs de terminaux iOS qu'ils doivent ouvrir BlackBerry UEM Client pour démarrer la migration vers BlackBerry UEM, et qu'ils doivent garder BlackBerry UEM Client ouvert jusqu'à ce que la migration soit terminée.

1. Sur la barre de menus, cliquez sur **Paramètres > Migration > Terminaux**.
2. Dans l'écran **Migrer les terminaux**, cliquez sur **Actualiser le cache**.

   La mise en cache des 1 000 utilisateurs peut prendre environ 10 minutes.

   BlackBerry UEM met en cache les données utilisateur pour accélérer les fonctions de recherche, mais les données utilisateur sont migrées directement depuis la source. L'actualisation du cache est obligatoire uniquement pour le premier ensemble de terminaux migrés et est facultative par la suite.
3. Cliquez sur **Suivant**.
4. Sélectionnez les terminaux à migrer.

   Seuls les 20 000 premiers terminaux sont affichés. Recherchez le nom ou l'adresse e-mail de l'utilisateur pour localiser des utilisateurs spécifiques qui peuvent ne pas être compris dans les premiers 20 000. La sélection de tous les utilisateurs sélectionne uniquement les utilisateurs de la première page. Définissez le format de page en fonction du nombre de terminaux que vous voulez sélectionner.

   Remarque : Il est possible que vous voyiez moins d'éléments de ligne que le nombre de terminaux, car le cache est affiché par l'utilisateur et certains utilisateurs disposent de plusieurs terminaux.

Si des modifications sont apportées à la source après la mise à jour du cache, ces modifications ne sont pas prises en compte dans l'affichage des données du cache. Il est déconseillé d'apporter des modifications au serveur source lors de la migration, mais si vous le faites, actualisez le cache régulièrement.

5. Cliquez sur **Aperçu**.
6. Cliquez sur **Migrer**.
7. (Facultatif. Pour les migrations d'une source UEM sur site vers une destination UEM sur site) Pour annuler la migration, cochez les cases en regard des terminaux dont vous souhaitez annuler la migration, puis cliquez sur ⃠.

   Si vous annulez la migration d'un terminal, celui-ci doit être effacé, puis réactivé sur le serveur de destination.
8. Pour afficher l'état des terminaux en cours de migration, cliquez sur **Migration** > **État**.

   Pour les migrations effectuées depuis Good Control pour déterminer quelles applications BlackBerry Dynamics ont été migrées, exécutez le rapport d'activité du conteneur sur Good Control.

   Assurez-vous que la configuration Good Control reste en cours d'exécution jusqu'à ce que la migration des applications déléguées d'authentification de l'utilisateur soit terminée, même si tous les terminaux sont migrés.

Migration de terminaux DEP

Vous pouvez migrer des terminaux iOS inscrits au programme d'inscription des terminaux Apple (DEP) depuis une base de données BlackBerry UEM source vers une autre base de données BlackBerry UEM.

Remarque : La configuration d'inscription DEP n'est pas migrée et les terminaux perdront les paramètres correspondants dans l'environnement de destination. Pour en savoir plus, rendez-vous sur support.blackberry.com et consultez l'article KB100525.

Migrer des terminaux DEP sur lesquels BlackBerry UEM Client est installé

Vous pouvez migrer des terminaux iOS inscrits au programme d'inscription des appareils Apple (DEP) et activés avec le type d'activation Contrôles MDM.

Avant de commencer : Dans les paramètres d'application de BlackBerry UEM Client, décochez la case **Supprimer l'application du terminal lorsque celui-ci est supprimé de BlackBerry UEM**.

Remarque : Si vous tentez d'effectuer la migration sans effectuer cette étape, l'application est supprimée et le terminal peut être désinscrit de BlackBerry UEM. Cependant, même si vous décochez cette case, l'application peut toujours être supprimée pendant la migration.

1. Dans le portail DEP, créez un nouveau serveur MDM virtuel.
2. Connectez l'instance de BlackBerry UEM de destination au nouveau serveur MDM virtuel. Pour plus d'informations, reportez-vous à Configuration de BlackBerry UEM pour le programme d'inscription des appareils (DEP).

   Assurez-vous que le profil DEP de l'instance de BlackBerry UEM de destination correspond au profil DEP de l'instance de BES12 ou BlackBerry UEM source.
3. Déplacez les terminaux DEP du serveur MDM virtuel source vers le nouveau serveur MDM virtuel.
4. Dans la console de gestion BlackBerry UEM, migrez les terminaux DEP de l'instance source vers l'instance de BlackBerry UEM de destination.

À la fin :

Remarque : Pour déclencher la migration sur un terminal, l'utilisateur doit d'abord ouvrir l'application qui est configurée en tant que délégué d'authentification sur ce terminal.

Migrer les terminaux DEP sur lesquels BlackBerry UEM Client n'est pas installé et qui ne sont pas compatibles avec BlackBerry Dynamics

Les terminaux iOS inscrits au programme d'inscription des appareils Apple (DEP) et sur lesquels BlackBerry UEM Client n'est pas installé apparaissent dans la liste de terminaux non pris en charge pour la migration.

1. Dans le portail DEP, créez un nouveau serveur MDM virtuel.
2. Connectez l'instance de BlackBerry UEM de destination au nouveau serveur MDM virtuel. Pour plus d'informations, reportez-vous à Configuration de BlackBerry UEM pour le programme d'inscription des appareils (DEP).

   Assurez-vous que l'instance de BlackBerry UEM de destination a le même profil DEP que l'instance source.
3. Déplacez les terminaux DEP du serveur MDM virtuel source vers le nouveau serveur MDM virtuel.
4. Effectuez une réinitialisation d'usine de chaque terminal DEP.
5. Réactivez chaque terminal DEP.

Configuration de BlackBerry UEM pour prendre en charge les applications BlackBerry Dynamics

Suivez les instructions de cette section pour configurer les paramètres de BlackBerry UEM qui sont spécifiques aux applications BlackBerry Proxy et BlackBerry Dynamics.

Pour plus d'informations sur la gestion des applications BlackBerry Dynamics sur les terminaux des utilisateurs, reportez-vous à la section Gestion des applications BlackBerry Dynamics du contenu relatif à l'administration.

Gérer les clusters BlackBerry Proxy

Lors de l'installation de la première instance de BlackBerry Proxy, BlackBerry UEM crée un BlackBerry Proxy cluster nommé « First ». En présence d'un seul cluster, les instances supplémentaires de BlackBerry Proxy sont ajoutées au cluster par défaut. Vous pouvez créer des clusters supplémentaires et déplacer les instances de BlackBerry Proxy entre les clusters disponibles. Lorsque plusieurs clusters BlackBerry Proxy sont disponibles, les nouvelles instances ne sont pas ajoutées à un cluster par défaut ; les nouvelles instances de clusters sont considérées comme non attribuées et doivent être ajoutées manuellement à l'un des clusters disponibles.

1. Dans la console de gestion, cliquez sur **Paramètres > BlackBerry Dynamics** à partir de la barre de menus.
2. Cliquez sur **Clusters**.
3. Effectuez l'une des tâches suivantes :

Tâche	Étapes
Créez un nouveau cluster BlackBerry Proxy.	**a.** Cliquez sur +. **b.** Saisissez un nom pour le cluster. **c.** Cliquez sur **Enregistrer**.
Renommez un cluster BlackBerry Proxy.	**a.** Cliquez sur le nom d'un cluster. **b.** Modifiez le nom du cluster. Chaque cluster doit avoir un nom unique. **c.** Cliquez sur **Enregistrer**.
Déplacez une instance de BlackBerry Proxy vers un cluster BlackBerry Proxy différent.	**a.** Dans la colonne **Serveurs**, cliquez sur le nom d'une instance de BlackBerry Proxy. **b.** Dans la liste déroulante BlackBerry Proxy**cluster**, sélectionnez le cluster auquel vous souhaitez ajouter l'instance. **c.** Cliquez sur **Enregistrer**.
Supprimez un cluster BlackBerry Proxy vide.	**a.** Cliquez sur × pour ce cluster. **b.** Cliquez sur **Supprimer**.
Définir les paramètres proxy d'application pour un cluster	**a.** Cliquez sur **Paramètres > BlackBerry Dynamics > Clusters** **b.** Cliquez sur le nom du cluster. **c.** Cliquez sur **Remplacer les paramètres globaux**. Pour plus d'informations, reportez-vous à la section Configurer les paramètres proxy de l'application BlackBerry Dynamics.

Tâche	Étapes
Téléchargez les mises à jour du fichier PAC pour tous les clusters.	• Cliquez sur **Actualiser le cache PAC**.
Spécifiez un certificat racine de confiance pour télécharger les fichiers PAC à partir du serveur.	**a.** Vérifiez que vous disposez du certificat au format X.509 (*.cer, *.der) stocké dans un emplacement réseau auquel vous pouvez accéder depuis la console de gestion. **b.** Sur la barre de menus, cliquez sur **Paramètres > Intégration externe > Certificats approuvés**. **c.** Cliquez sur + à côté de **Éléments approuvés du serveur PAC**. **d.** Cliquez sur **Parcourir**. **e.** Sélectionnez le fichier de certificat à utiliser. **f.** Cliquez sur **Ouvrir**. **g.** Saisissez la description du certificat. **h.** Cliquez sur **Ajouter**.
Permettre à un BlackBerry Proxy d'être utilisé pour l'activation	Sélectionnez l'option **Activé pour l'activation** pour l'instance BlackBerry Proxy que vous souhaitez utiliser à des fins d'activation. Vous devez sélectionner au moins une instance.

Configurer Direct Connect à l'aide de la redirection de port

Avant de commencer :

- Configurez une entrée DNS publique pour chaque serveur BlackBerry Connectivity Node (par exemple, bp01.mydomain.com, bp02.mydomain.com, etc.).
- Configurez le pare-feu externe pour autoriser les connexions entrantes sur le port 17533 et pour transférer ce port vers chaque serveur BlackBerry Connectivity Node.
- Si les instances de BlackBerry Connectivity Node sont installées dans une zone démilitarisée, assurez-vous que les ports appropriés sont ouverts entre chaque BlackBerry Connectivity Node et les serveurs d'applications auxquels les applications BlackBerry Dynamics doivent accéder (par exemple, Microsoft Exchange, serveurs Web internes et BlackBerry UEM Core).

1. Dans la console de gestion, cliquez sur **Paramètres > BlackBerry Dynamics** à partir de la barre de menus.
2. Cliquez sur **Direct Connect**.
3. Cliquez sur une instance de BlackBerry Proxy.
4. Pour activer Direct Connect, cochez la case **Activer Direct Connect**. Dans le champ **Nom d'hôte du proxy BlackBerry**, vérifiez que le nom d'hôte est correct. Si l'entrée DNS publique que vous avez créée est différente du FQDN du serveur, spécifiez plutôt le FQDN externe.
5. Répétez les étapes 3 et 4 pour toutes les instances de BlackBerry Proxy du cluster.

   Pour activer uniquement certaines instances de BlackBerry Proxy pour Direct Connect, créez un nouveau cluster BlackBerry Proxy. Tous les serveurs d'un cluster doivent avoir la même configuration. Pour plus d'informations, reportez-vous à la section Gérer les clusters BlackBerry Proxy dans le contenu relatif à la configuration.
6. Cliquez sur **Enregistrer**.

Configurer les propriétés BlackBerry Dynamics

Vous pouvez configurer des propriétés spécifiques à l'utilisation des applications BlackBerry Dynamics dans votre organisation. Pour plus d'informations sur les différentes propriétés et les répercussions d'une modification des paramètres par défaut, reportez-vous aux sections Propriétés globales de BlackBerry Dynamics, Propriétés de BlackBerry Dynamics, Propriétés de BlackBerry Proxy et Configurer les paramètres proxy de l'application BlackBerry Dynamics. Pour découvrir les meilleures pratiques de configuration des propriétés BlackBerry Proxy, rendez-vous sur support.blackberry.com/community pour consulter l'article 47875.

1. Dans la console de gestion, cliquez sur **Paramètres > BlackBerry Dynamics** à partir de la barre de menus.
2. Effectuez l'une des opérations suivantes :
   - Pour configurer les propriétés globales, cliquez sur **Propriétés globales**.
   - Pour configurer les propriétés d'une instance de BlackBerry UEM particulière, cliquez sur **Propriétés**. Dans la liste déroulante **Type de serveur**, cliquez sur **Serveurs BlackBerry** et sélectionnez le serveur BlackBerry UEM que vous souhaitez configurer.
   - Pour configurer les propriétés d'une instance de BlackBerry Proxy particulière, cliquez sur **Propriétés**. Dans la liste déroulante **Type de serveur**, cliquez sur **Serveurs BlackBerry Proxy** et sélectionnez le serveur BlackBerry Proxy que vous souhaitez configurer.
3. Si nécessaire, configurez les propriétés.
4. Cliquez sur **Enregistrer**.

Propriétés globales de BlackBerry Dynamics

Les tableaux suivants décrivent les propriétés globales de BlackBerry Dynamics que vous pouvez configurer.

La colonne Redémarrer indique si la modification de la propriété nécessite un redémarrage de BlackBerry UEM.

Remarque : Une propriété qui s'affiche dans la console de gestion sans être détaillée ici correspond à une propriété supprimée et donc plus utilisée.

Certificate Management

Propriété	Description	Par défaut	Redémarrer
Valeur TTL en secondes du magasin pour les certificats PKCS 12 des utilisateurs finaux individuels	Durée de vie (TTL), en secondes, du magasin de certificats pour les certificats PKCS 12 pendant laquelle les utilisateurs de terminaux peuvent effectuer un téléchargement pour signer des e-mails et à des fins d'authentification du client. **Remarque :** Cette propriété est en lecture seule. Vous ne pouvez pas la modifier.	86 400	—

Communication

Propriété	Description	Par défaut	Redémarrer
cntmgmt.internal.port	Le port interne pour le service de gestion des conteneurs.	Null (par défaut, 17317)	Oui
cntmgmt.max.conns.above.limi	Nombre maximum de connexions autorisées au-delà de la limite définie par la propriété cntmgmt.max.conns.persec. **Remarque :** Ne modifiez pas ce paramètre sans avoir consulté l'assistance technique BlackBerry.	3	Oui
cntmgmt.max.conns.persec	Nombre maximum de connexions par seconde pour la gestion des conteneurs. **Remarque :** Ne modifiez pas ce paramètre sans avoir consulté l'assistance technique BlackBerry.	30	Oui
cntmgmt.max.active.sessions	Nombre maximum de sessions actives pour la gestion des conteneurs.	10 000	Oui
cntmgmt.max.idle.count	Nombre maximum de connexions inactives autorisé pour la gestion des conteneurs. **Remarque :** Ne modifiez pas ce paramètre sans avoir consulté l'assistance technique BlackBerry.	0	Oui
cntmgmt.max.read.throughput	Nombre maximum d'opérations de lecture concurrentes pour la gestion des conteneurs. **Remarque :** Ne modifiez pas ce paramètre sans avoir consulté l'assistance technique BlackBerry.	500	Oui
cntmgmt.max.write.throughput	Nombre maximum d'opérations d'écriture concurrentes pour la gestion des conteneurs. **Remarque :** Ne modifiez pas ce paramètre sans avoir consulté l'assistance technique BlackBerry.	500	Oui
cntmgmt.ssl.external.enable	Détermine si SSL est activé pour la gestion des conteneurs externes.	I	Oui
cntmgmt.ssl.internal.enable	Détermine si SSL est activé pour la gestion des conteneurs internes.	I	Oui

Conteneurs en double

Si BlackBerry UEM identifie des conteneurs en double sur les terminaux, il planifie un traitement par lots pour les supprimer. Un conteneur en double a les mêmes ID d'utilisateur et ID d'autorisation (également appelé ID

d'application BlackBerry Dynamics) qu'un autre conteneur sur le même terminal. Lorsqu'un conteneur en double est supprimé, il est consigné dans le fichier journal BlackBerry UEM.

Propriété	Description	Par défaut	Redémarrer
Automatically remove older duplicate containers on same device for the user after provisioning.	Spécifiez si BlackBerry UEM supprime automatiquement les conteneurs en double lorsqu'une nouvelle version d'une application est déployée. Si ce paramètre est sélectionné, il a priorité sur les autres propriétés de conteneur en double.	I	Non
Activer la tâche pour supprimer automatiquement les conteneurs en double (activer/désactiver)	Spécifiez si BlackBerry UEM planifie automatiquement des tâches pour identifier et supprimer les conteneurs en double sur les terminaux.	I	Non
Délai d'inactivité, en secondes, avant la suppression du conteneur en double	Délai, en secondes, durant lequel un conteneur en double doit être inactif avant que BlackBerry UEM planifie une tâche pour le supprimer.	259 200	Non
Frequency in seconds that job to remove duplicate containers will run	Fréquence, en secondes, à laquelle BlackBerry UEM exécute une tâche pour identifier et supprimer les conteneurs en double.	86 400	Non
Nombre maximum de conteneurs à supprimer au cours d'une même tâche	Nombre maximum de conteneurs inactifs qu'une même tâche peut supprimer des terminaux.	100	Non

Délégation contrainte Kerberos

Propriété	Description	Par défaut	Redémarrer
Utiliser un UPN explicite	Spécifiez si les applications BlackBerry Dynamics utilisent un UPN (User Principal Name, nom d'utilisateur principal) explicite ou implicite lors de l'authentification auprès des services intégrés à Microsoft Active Directory ou Exchange ActiveSync dans Office 365. Selon votre environnement, l'Active Directory de votre organisation peut prendre en charge les deux options ou une seule.	O	Non
Activer KCD (gc.krb5.enabled)	Spécifiez si BlackBerry UEM prend en charge la délégation Kerberos contrainte pour les applications BlackBerry Dynamics.	O	Oui

Divers

Propriété	Description	Par défaut	Redémarrer
config.command.expiry	Délai d'attente, en secondes, durant lequel BlackBerry UEM attend avant de renvoyer un message non acquitté.	60	Oui
config.command.retry	Fréquence, en secondes, à laquelle BlackBerry UEM exécute une tâche pour identifier et supprimer les messages non acquittés. Si cette propriété est définie sur 0, BlackBerry UEM n'exécute pas la tâche.	900	Oui
gc.entgw.report.userinfo	Spécifiez si les noms d'affichage de l'utilisateur sont indiqués au NOC BlackBerry Dynamics.	O	Non
policy.compliance.interval	Fréquence, en minutes, à laquelle BlackBerry UEM récupère les stratégies de conformité pour tous les ensembles de stratégies de BlackBerry Dynamics.	1 440	Oui

Vider les conteneurs inactifs

Si BlackBerry UEM identifie des conteneurs inactifs sur les terminaux, il planifie un traitement par lots pour les supprimer. BlackBerry UEM considère un conteneur comme inactif s'il ne s'est pas connecté à BlackBerry UEM pendant une période par défaut de 90 jours. Lorsqu'un conteneur inactif est supprimé, il est consigné dans le fichier journal BlackBerry UEM.

Remarque : Les conteneurs pour lesquels un délégué d'authentification est configuré ne sont pas purgés par ce processus.

Propriété	Description	Par défaut	Redémarrer
Activer la tâche pour supprimer automatiquement les conteneurs inactifs (activer/désactiver)	Spécifiez si BlackBerry UEM planifie automatiquement des tâches pour identifier et supprimer les conteneurs inactifs des terminaux.	O	Non
Intervalle d'inactivité des conteneurs en secondes	Délai, en secondes, avant lequel BlackBerry UEM considère un conteneur comme inactif.	7 776 000	Non
Fréquence, en secondes, d'exécution de la tâche de suppression des conteneurs inactifs	Fréquence, en secondes, à laquelle BlackBerry UEM exécute une tâche pour identifier et supprimer les conteneurs inactifs.	86 400	Non
Nombre maximum de conteneurs à supprimer au cours d'une même tâche	Nombre maximum de conteneurs d'inactifs qu'une même tâche peut supprimer des terminaux.	100	Non

Rapports

Propriété	Description	Par défaut	Redémarrer
Définissez la limite d'enregistrements renvoyés dans les rapports exportables pour éviter tout manque de mémoire.	Nombre maximum de lignes pouvant être incluses dans un rapport. La valeur maximum possible est 1000000.	5 000	Non

Stratégie de rétention des données

Propriété	Description	Par défaut	Redémarrer
Consigner les opérations de lecture dans la base de données	Détermine si BlackBerry Control consigne les opérations de lecture dans la base de données BlackBerry Control.	I	Oui
Vider les tâches du serveur	Spécifiez si BlackBerry UEM vide automatiquement les tâches du serveur à un intervalle régulier.	I	Oui
Intervalle de vidage des tâches du serveur (en jours)	Si l'option « Vider les tâches du serveur » est activée, fréquence, en jours, à laquelle BlackBerry UEM vide les tâches du serveur.	30	Oui

Propriétés de BlackBerry Dynamics

Les tableaux suivants décrivent les propriétés que vous pouvez configurer pour chacune des instances de BlackBerry UEM Core de votre organisation.

Délégation contrainte Kerberos

Propriété	Description	Par défaut	Redémarrer
Emplacement du fichier krb5.config sur le serveur GC (gc.krb5.config.file)	Fichier krb5.conf utilisé à des fins d'authentification dans un environnement à plusieurs domaines en présence d'une relation approuvée CAPATH avec plusieurs domaines Kerberos.	Non défini	Oui
Activer le mode de débogage KCD (gc.krb5.debug)	Détermine si BlackBerry UEM consigne les données du niveau de débogage.	O	Oui
Nom entièrement qualifié pour le KCD (gc.krb5.kdc)	Nom de domaine complet du serveur qui héberge le service KDC (Key Distribution Center) Kerberos.	Non défini	Oui

Propriété	Description	Par défaut	Redémarrer
Emplacement du fichier keytab (gc.krb5.keytab.file)	Emplacement du fichier keytab Kerberos sur l'ordinateur qui héberge BlackBerry UEM.	Non défini	Oui
Nom du compte de service dans lequel le service KCD est en cours d'exécution (gc.krb5.principal.name)	Nom d'utilisateur du compte Kerberos. N'incluez pas le domaine.	Non défini	Oui
Domaine - Active Directory (gc.krb5.realm)	Domaine du compte Kerberos.	Non défini	Oui

Propriétés de BlackBerry Proxy

Les tableaux suivants décrivent les propriétés que vous pouvez configurer pour chacune des instances de BlackBerry Proxy de votre organisation.

Propriété	Description	Par défaut	Redémarrer
gp.gps.max.sessions	Nombre maximal de sessions actives.	15 000	—
gp.gps.dns.server.ttl.ms	Délai pour l'attente (en millisecondes) de la réponse du serveur DNS.	1 800 000	—
gp.gps.server.flowcontrol	Spécifiez si le contrôle de flux est activé pour le serveur.	O	—
gp.gps.tcp.keepalive	Spécifiez si TCP keepalive est activé pour le serveur.	O	—
gp.gps.unalias.hostname	Pour les recherches DNS des serveurs d'applications, utilisez l'adresse IP ou le nom d'hôte. Si vous sélectionnez cette option, BlackBerry Proxy utilise la recherche DNS inversée, avec l'adresse IP du serveur d'applications. Si vous ne sélectionnez pas cette option, BlackBerry Proxy utilise le nom d'hôte du serveur d'applications pour les recherches DNS.	O	Oui

Propriété	Description	Par défaut	Redémarrer
gps.directconnect.suppo	Ajoutez ou modifiez des suites de codes qui cryptent le pontage et les communications effectuées via BlackBerry Direct Connect. Vous pouvez choisir de configurer votre propre serveur proxy pour Direct Connect et de le placer entre les terminaux de votre client et le serveur BlackBerry Proxy. Si vous avez ajouté votre propre serveur proxy, assurez-vous que les codes du serveur BlackBerry Proxy correspondent à ceux requis par votre propre serveur proxy. **Remarque :** Tous les codes doivent être pris en charge par Java.	TLS_ECDHE_RSA_WI	Oui
gp.directconnect. supported.protocols	Ajoutez ou modifiez les protocoles cryptographiques que le pont de connexion directe de votre système doit prendre en charge.	TLSv1, TLSv1.1, TLSv1.2	Oui
gp.eacp.command.servic	Permet LDAP sur TCP pour les serveurs Active Directory. Les serveurs Active Directory offrent le service LDAP via le protocole TCP ; par conséquent, les clients trouvent un serveur LDAP en interrogeant DNS pour un enregistrement du formulaire : _ldap._tcp. DnsDomainName. Si vous sélectionnez cette option, BlackBerry Proxy utilise LDAP pour nslookup d'un nom d'hôte de service donné. Si vous ne sélectionnez pas cette option, BlackBerry Proxy utilise directement la recherche DNS inversée, en utilisant le nom d'hôte de service que vous fournissez.	O	Oui
gc.mdc.hb.timeout	Spécifiez le délai de pulsation.	0	—
gp.server.secure.ciphers	Ajoutez ou modifiez des suites de codes qui cryptent les communications effectuées via un serveur BlackBerry Proxy. **Remarque :** Tous les codes doivent être pris en charge par Java.	TLS_ECDHE_RSA_WI	—
gp.server.secure. protocols	Ajoutez ou modifiez les protocoles cryptographiques que votre serveur BlackBerry Proxy doit prendre en charge.	TLSv1, TLSv1.1, TLSv1.2	—

Configurer les paramètres de communication pour les applications BlackBerry Dynamics

Vous pouvez configurer les paramètres de communication des applications BlackBerry Dynamics dans le domaine de votre entreprise. Les paramètres de communication vous permettent d'assurer une communication sécurisée dans votre réseau en utilisant le protocole de votre choix. Par défaut, seul TLS v1.2 est autorisé. Vous pouvez également autoriser TLSv1 et v1.1. Vous devez choisir au moins un protocole.

1. Dans la console de gestion, cliquez sur **Paramètres > BlackBerry Dynamics** à partir de la barre de menus.
2. Cliquez sur **Paramètres de communication**.
3. Configurez les paramètres selon les besoins.
4. Cliquez sur **Enregistrer**.

Envoi de données d'application BlackBerry Dynamics via un proxy HTTP

Vous pouvez configurer BlackBerry UEM pour envoyer les données d'application BlackBerry Dynamics via un proxy HTTP entre BlackBerry Proxy et un serveur d'application. Les applications BlackBerry Dynamics prennent en charge les paramètres de proxy manuels et les fichiers PAC pour les connexions aux serveurs d'applications. Pour utiliser un fichier PAC, les applications doivent être développées avec BlackBerry Dynamics SDK 7.0 ou une version ultérieure. Si vous configurez les paramètres manuels et de fichier PAC, le fichier PAC est prioritaire pour les applications qui le prennent en charge. Les applications développées à l'aide d'une version plus ancienne de BlackBerry Dynamics SDK utilisent les paramètres manuels.

BlackBerry Access prend également en charge les paramètres de configuration d'application de fichier PAC et de proxy manuels qui s'appliquent uniquement à la navigation avec BlackBerry Access. Les paramètres de configuration du proxy pour BlackBerry Access, ou d'autres applications qui ont des paramètres de proxy distincts, remplacent les paramètres de proxy de BlackBerry UEM. Pour plus d'informations, reportez-vous au Guide d'administration de BlackBerry Access.

Remarque : Les paramètres de proxy manuels sont également utilisés pour les connexions à BlackBerry Dynamics NOC. Le proxy doit être en mesure d'accéder au port 443. Pour plus d'informations sur les exigences relatives aux ports, consultez l'article Connexions sortantes : BlackBerry UEM vers BlackBerry Dynamics NOC.

Considérations relatives au fichier PAC

Si vous utilisez des fichiers PAC avec BlackBerry Proxy, il vous faut tenir compte des considérations suivantes concernant la prise en charge.

BlackBerry UEM prend en charge les directives de fichier PAC suivantes :

- DIRECT
- PROXY (traité comme proxy HTTPS - connexion établie à l'aide de HTTP CONNECT)
- HTTPS (connexion établie à l'aide de HTTP CONNECT)

BlackBerry UEM ne prend pas en charge les directives de fichier PAC suivantes :

- BLOCK (traité comme DIRECT)
- SOCKS (erreur de connexion)
- SOCKS4 (erreur de connexion)
- SOCKS5 (erreur de connexion)
- HTTP (erreur de connexion)

- Directive « NATIVE » personnalisée, définie par BlackBerry Access (erreur de connexion)

BlackBerry UEM présente les restrictions supplémentaires suivantes pour les fichiers PAC :

- La fonction dnsDomainIs ne peut pas contenir les caractères « _ » et « * ».
- La fonction shExpMatch ne peut pas inclure les expressions « [0-9] », « ? », « /^d » ou « d+ »
- L'option permettant de supprimer le chemin et la requête de l'URI n'est pas prise en charge.

Remarque :

BlackBerry Proxy télécharge le fichier PAC et le met en cache pour améliorer les performances. Le cache PAC est mis à jour toutes les 24 heures.

Si un nouveau fichier PAC est publié et que vous devez mettre à jour le cache immédiatement, vous pouvez accéder à **Paramètres > Infrastructure > BlackBerry Router et proxy**, développer la section **Paramètres globaux** et cliquer sur **Mettre à jour le cache PAC**.

Configurer les paramètres proxy de l'application BlackBerry Dynamics

Vous pouvez configurer les paramètres proxy globaux de l'application BlackBerry Dynamics manuellement ou à l'aide d'un fichier PAC. Vous pouvez remplacer les paramètres globaux des clusters BlackBerry Proxy et des serveurs individuels ; toutefois, le niveau de complexité pour remplacer les paramètres de serveurs individuels n'est généralement pas requis et n'est pas recommandé.

1. Effectuez l'une des opérations suivantes :

Tâche	Étapes
Définir les paramètres proxy globaux de l'application	**a.** Cliquez sur **Paramètres > Infrastructure > BlackBerry Router et proxy**. **b.** Cliquez sur **Paramètres globaux**.
Définir les paramètres proxy d'application pour un cluster	**a.** Cliquez sur **Paramètres > BlackBerry Dynamics > Clusters** **b.** Cliquez sur le nom du cluster. **c.** Cliquez sur **Remplacer les paramètres globaux**.
Définir les paramètres manuels de proxy d'application pour un serveur	**a.** Cliquez sur **Paramètres > Infrastructure > BlackBerry Router et proxy**. **b.** Cliquez sur **Remplacer les paramètres globaux**. **Remarque :** Les fichiers PAC ne sont pas pris en charge lors du remplacement des paramètres proxy globaux d'un serveur.

2. Sélectionnez l'une des options suivantes.
   - **Activer le proxy HTTP manuel**
   - **Activer PAC**

   Les fichiers PAC ne sont pris en charge que pour les connexions aux serveurs d'applications. Si vous configurez les deux options, la configuration PAC est prioritaire pour les connexions aux serveurs d'applications. Les fichiers PAC sont pris en charge uniquement pour les applications développées avec BlackBerry Dynamics SDK 7.0 et versions ultérieures.
3. Si vous avez sélectionné **Activer le proxy HTTP manuel** , effectuez les opérations suivantes :
   a) Sélectionnez l'une des options suivantes.
      - **Utiliser le proxy pour se connecter uniquement aux serveurs BlackBerry Dynamics NOC**
      - **Utiliser le proxy pour se connecter à tous les serveurs**
      - **Utiliser le proxy pour se connecter uniquement aux serveurs spécifiés**

b) Si vous voulez utiliser le serveur proxy pour vous connecter aux serveurs spécifiés, cliquez sur + pour spécifier tous les serveurs supplémentaires.
c) Dans le champ **Adresse**, saisissez l'adresse du serveur proxy.
d) Dans le champ **Port**, saisissez le numéro de port écouté par le serveur proxy.
e) Si le serveur proxy requiert une authentification, sélectionnez **Utiliser l'authentification** et spécifiez le **nom d'utilisateur**, le **mot de passe** et, si nécessaire, le **domaine** que l'application doit utiliser pour l'authentification.

4. Si vous avez sélectionné **Activer PAC**, procédez comme suit :
   a) Dans le champ **URL du fichier PAC**, saisissez l'URL du fichier PAC.
   b) Si le serveur proxy spécifié dans le fichier PAC requiert une authentification, sélectionnez **Prise en charge de l'authentification proxy** et spécifiez le **nom d'utilisateur**, le **mot de passe** et, si nécessaire, le **domaine** que l'application doit utiliser pour l'authentification.

      Les informations d'authentification de l'utilisateur final ne sont pas prises en charge pour l'authentification proxy.
5. Cliquez sur **Enregistrer**.

Connectivité et comportement de routage de BlackBerry Dynamics

BlackBerry UEM propose plusieurs options qui permettent aux administrateurs de contrôler le routage du trafic de BlackBerry Dynamics. Le routage des applications BlackBerry Dynamics est affecté par les éléments suivants :

- Profil de connectivité BlackBerry Dynamics
- Configuration du serveur Web proxy BlackBerry Proxy

  Remarque : Pour utiliser le BlackBerry Proxy dans une configuration BlackBerry UEM Cloud, vous devez installer un BlackBerry Connectivity Node sur site.
- Paramètres spécifiques à l'application (par exemple, la configuration du serveur Web proxy BlackBerry Access)

Avant de configurer le routage, assurez-vous que les ports corrects sont ouverts et que vous disposez d'une connectivité réseau avec le BlackBerry Dynamics NOC. Pour plus d'informations, reportez-vous aux sections Exigences relatives au port dans le contenu relatif à la planification et Envoi de données d'application BlackBerry Dynamics via un proxy HTTP.

Cette documentation traite uniquement des configurations qui affectent le routage global. Une configuration spécifique à l'application peut être nécessaire pour que les applications se connectent à des serveurs spécifiques (par exemple, pour BlackBerry Work configuré avec l'URL du Microsoft Exchange Server). Consultez la documentation de chaque application pour connaître les configurations à appliquer.

Routage par défaut

Par défaut, lors d'une nouvelle installation de BlackBerry UEM, tout le trafic des applications BlackBerry Dynamics est acheminé directement vers Internet, sans configuration de serveur proxy Web.

Configuration de profil de connectivité BlackBerry Dynamics

Le seul élément configuré dans le profil de connectivité BlackBerry Dynamics par défaut est le **Type de chemin de domaine autorisé par défaut**, qui est défini sur **Direct**.

Avec le profil de connectivité BlackBerry Dynamics par défaut, aucun serveur ou domaine interne n'est accessible aux applications BlackBerry Dynamics. Les administrateurs peuvent modifier le profil de connectivité par défaut ou en créer un nouveau pour permettre la connectivité aux serveurs internes.

Pour plus d'informations, reportez-vous à la section Créer un profil de connectivité BlackBerry Dynamics.

Configuration du serveur Web proxy BlackBerry Proxy

Aucune configuration de serveur proxy Web n'est appliquée à la configuration par défaut des serveurs BlackBerry Proxy. Dans cette configuration, chaque serveur BlackBerry Proxy tente de se connecter directement à Internet pour établir des connexions. Cela s'applique à la fois au trafic du serveur d'applications et aux connexions BlackBerry Dynamics NOC.

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

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

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

Pour les applications développées avec BlackBerry Dynamics SDK versions 6.0 et ultérieures, vous pouvez spécifier les clusters BlackBerry Proxy via lesquels les données doivent être acheminées.

Si vous disposez de BlackBerry UEM dans un environnement sur site, pour les applications développées avec une version de BlackBerry Dynamics SDK antérieure à 6.0, sélectionnez l'option Acheminer tout le trafic pour acheminer toutes les données des applications BlackBerry Dynamics, quel que soit le domaine ou le sous-réseau, via BlackBerry Proxy.

Vous devez tenir compte des points suivants lorsque vous acheminez des données via BlackBerry Proxy :

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

Pour plus d'informations, reportez-vous aux sections Exigences relatives au port dans le contenu relatif à la planification et Envoi de données d'application BlackBerry Dynamics via un proxy HTTP.

Configuration du proxy spécifique à l'application

BlackBerry Access et certaines applications tierces permettent des configurations de serveur proxy Web au niveau des applications.

Aucune configuration de serveur proxy Web n'est appliquée à la configuration par défaut de BlackBerry Access. Consultez la documentation des applications tierces BlackBerry Dynamics pour comprendre la configuration par défaut de chacune d'elles.

Remarque : un serveur d'applications est un serveur auquel une application BlackBerry Dynamics se connecte, tel que l'URL d'un Microsoft Exchange Server, l'URL de BEMS, l'URL de Skype for Business, ou toute URL qui accède à BlackBerry Access. BlackBerry Dynamics NOC et le serveur BlackBerry UEM Core ne sont pas des serveurs d'applications.

Exemples de scénarios de routage

Les exemples de scénarios suivants reflètent les configurations les plus courantes. Si ces configurations ne répondent pas aux besoins de votre organisation ou si vous avez des exigences plus complexes, contactez BlackBerry Enterprise Consulting pour obtenir de l'aide.

Scénario 1 : acheminer le trafic vers des serveurs ou des domaines spécifiques via BlackBerry Proxy

Cette configuration est adaptée aux scénarios où certains serveurs d'applications internes doivent être accessibles aux applications BlackBerry Dynamics, mais où le trafic général vers les serveurs publics peut rester direct.

Par exemple, vous pouvez acheminer des connexions directement vers des sites publics tels que google.com et microsoft.com, mais vous devez effectuer un routage interne via BlackBerry Proxy pour accéder aux serveurs Microsoft Exchange Server et SharePoint internes.

Cette configuration suppose qu'une connexion de serveur Web proxy à Internet n'est pas nécessaire, soit parce qu'aucun serveur basé sur Internet ne sera jamais routé via le serveur BlackBerry Proxy, soit parce que le serveur BlackBerry Proxy lui-même a un accès direct à Internet sans nécessiter de connexion de serveur Web proxy.

Profil de connectivité BlackBerry Dynamics

1. Définissez l'option **Type de chemin de domaine autorisé par défaut** sur **Direct**.
2. Sous **Domaines autorisés**, ajoutez les domaines internes que vous souhaitez acheminer via le système BlackBerry Proxy et sélectionnez un cluster BlackBerry Proxy.
3. (Facultatif) Ajoutez des noms de serveurs spécifiques sous **Serveurs supplémentaires** et sélectionnez un cluster BlackBerry Proxy. Cette opération n'est requise que si les serveurs ne sont pas déjà couverts par les règles de **domaines autorisés**.

Pour plus d'informations sur l'utilisation des règles du profil de connectivité, reportez-vous à la section Paramètres du profil de connectivité BlackBerry Dynamics.

Serveur Web proxy du serveur BlackBerry Proxy

Aucune configuration de serveur Web proxy n'est nécessaire.

Remarque : Si votre organisation a des exigences particulières pour accéder à Internet à partir de serveurs internes, ou si tout le trafic doit être acheminé via un serveur Web proxy, reportez-vous aux exemples de configuration ci-dessous qui incluent les configurations de proxy.

Serveur Web proxy spécifique à l'application

Aucune configuration de serveur Web proxy spécifique à une application n'est nécessaire.

Scénario 2 : acheminer tout le trafic via BlackBerry Proxy, puis via un serveur proxy Web

Cette configuration convient aux organisations qui exigent que tout le trafic des applications professionnelles soit acheminé en interne. Un serveur proxy Web est requis pour que les serveurs internes se connectent à Internet.

Par exemple, les connexions à des sites publics tels que google.com et microsoft.com, ainsi qu'à des serveurs Microsoft Exchange Server s et SharePoint internes, doivent toutes être acheminées en interne via BlackBerry Proxy.

Dans cette configuration, nous supposons qu'une connexion de serveur proxy Web à Internet est également requise, car la plupart des organisations qui exigent que tout le trafic soit acheminé en interne exigent également que le trafic soit acheminé via un serveur proxy Web pour le filtrage ou la surveillance.

Profil de connectivité BlackBerry Dynamics

1. Définissez l'option **Type de chemin de domaine autorisé par défaut** sur **Cluster de BlackBerry Proxy**.

2. (Facultatif) Ajoutez des domaines internes à la liste **Domaines autorisés**. Cela n'est pas nécessaire lorsque le **Type de chemin de domaine autorisé par défaut** est défini pour acheminer le trafic via BlackBerry Proxy.
3. (Facultatif) Ajoutez des noms de serveurs spécifiques sous **Serveurs supplémentaires** et sélectionnez un cluster BlackBerry Proxy. Cela n'est pas nécessaire lorsque le **Type de chemin de domaine autorisé par défaut** est défini pour acheminer le trafic via BlackBerry Proxy.
4. (Facultatif) Si vous souhaitez que des serveurs spécifiques soient exclus du routage par défaut via BlackBerry Proxy, vous pouvez spécifier des domaines spécifiques (sous **Domaines autorisés** ou **Serveurs supplémentaires**) et sélectionner **Direct**. Cela vous permet d'acheminer la plupart du trafic via BlackBerry Proxy tout en en excluant une partie (par exemple, pour améliorer les performances de certains sites publics de confiance).

Pour plus d'informations sur l'utilisation des règles du profil de connectivité, reportez-vous à la section Paramètres du profil de connectivité BlackBerry Dynamics.

Serveur Web proxy du serveur BlackBerry Proxy

En fonction de la complexité de votre environnement, vous pouvez configurer le serveur BlackBerry Proxy pour acheminer le trafic via un serveur proxy Web plutôt que directement vers le serveur de destination.

Vous pouvez utiliser une configuration manuelle du serveur proxy Web ou un fichier PAC.

Remarque : Vous pouvez sélectionner à la fois le proxy HTTP manuel et le PAC. Cela peut être nécessaire dans les cas où le trafic NOC doit utiliser un serveur proxy différent du trafic de l'application. Évitez autant que possible ce niveau de complexité.

Proxy HTTP manuel : la configuration manuelle du serveur proxy Web est suffisante s'il n'existe aucune règle complexe régissant les URL qui doivent utiliser un serveur proxy Web et celles qui doivent être directes. Si tout le trafic doit utiliser un serveur proxy Web, la configuration manuelle d'un serveur proxy Web est la façon la plus simple d'y parvenir.

1. Activer le proxy HTTP manuel :

Dans un environnement sur site	a. Accédez à **Paramètres > Infrastructure > BlackBerry Router et proxy**. b. Développez **Paramètres globaux**, puis sélectionnez **Activer le proxy HTTP manuel**.
Dans un environnement Cloud	a. Accédez à **Paramètres > BlackBerry Dynamics > Clusters**. b. Cliquez sur le cluster que vous voulez modifier. c. Activez **Remplacer les paramètres globaux**, puis sélectionnez **Activer le proxy HTTP manuel**.

2. Sélectionnez **Utiliser le proxy pour se connecter à tous les serveurs**.
3. Saisissez l'adresse et le port du serveur proxy Web.

Fichier PAC (configuration automatique du proxy) : si votre organisation exige des règles plus complexes concernant les serveurs devant utiliser un proxy et ceux qui doivent se connecter directement, BlackBerry recommande d'utiliser un fichier PAC, car il est beaucoup plus facile à gérer.

Par exemple, si vous souhaitez que toutes les connexions à l'Internet public utilisent le serveur proxy Web, mais que tous les domaines internes se connectent directement, la meilleure pratique consiste à utiliser un fichier PAC.

Remarque : La configuration du fichier PAC ne fait pas partie du produit BlackBerry et doit être effectuée par l'équipe de réseau ou de proxy appropriée de votre organisation.

1. Ouvrez les paramètres du proxy :

Dans un environnement sur site	**a.** Accédez à **Paramètres > Infrastructure > BlackBerry Router et proxy**.
Dans un environnement Cloud	**a.** Accédez à **Paramètres généraux > BlackBerry Router et proxy**.

2. Développez **Paramètres globaux**, sélectionnez **Activer PAC**.
3. Saisissez l'URL du PAC et les informations d'authentification requises.

Serveur Web proxy spécifique à l'application

Aucune configuration du proxy spécifique à une application n'est nécessaire. Cette configuration suppose que tout le trafic est acheminé en interne et qu'un proxy manuel ou un PAC est configuré sur le serveur BlackBerry Proxy.

Scénario 3 : acheminer une partie du trafic en interne pour la plupart des applications, mais configurer un serveur proxy spécifiquement pour la navigation Web via BlackBerry Access

Cette configuration convient aux organisations qui exigent que le trafic des applications soit acheminé en interne, mais qui nécessitent un routage plus complexe via un serveur proxy Web spécifique au trafic du navigateur.

Par exemple, votre organisation peut décider qu'il est acceptable que BlackBerry Work se connecte directement aux serveurs Microsoft Office 365. SharePoint est toujours interne, une partie du trafic doit donc être acheminé via BlackBerry Proxy. Cependant, la navigation est plus étroitement contrôlée et tout le trafic provenant de BlackBerry Access doit être acheminé via un serveur proxy Web à des fins de surveillance et de journalisation.

Cette configuration peut également inclure une configuration de serveur proxy Web au niveau du serveur BlackBerry Proxy, mais pour cet exemple, nous supposons que la connectivité directe est disponible à partir du BlackBerry Proxy.

Profil de connectivité BlackBerry Dynamics

1. Définissez l'option **Type de chemin de domaine autorisé par défaut** sur **Direct**.
2. Sous **Domaines autorisés**, ajoutez tous les domaines internes que vous souhaitez acheminer via BlackBerry Proxy et sélectionnez un cluster BlackBerry Proxy.
3. (Facultatif) Ajoutez des serveurs spécifiques qui ne sont pas déjà inclus sous **Serveurs supplémentaires** et sélectionnez un cluster BlackBerry Proxy.

Important : Si vous prévoyez de spécifier un serveur proxy Web hébergé en interne dans la configuration spécifique à l'application, vous devez inclure cette URL de serveur proxy Web dans la liste Domaines autorisés ou dans la liste Serveurs supplémentaires. Si l'URL du serveur proxy Web n'est pas définie pour acheminer le trafic via BlackBerry Proxy, les connexions au serveur proxy Web échouent. Si le serveur proxy Web est accessible publiquement, cette étape n'est pas requise.

Pour plus d'informations sur l'utilisation des règles du profil de connectivité, reportez-vous à la section Paramètres du profil de connectivité BlackBerry Dynamics.

Serveur Web proxy du serveur BlackBerry Proxy

Cet exemple suppose que les serveurs BlackBerry Proxy disposent d'un accès direct à Internet. Si ce n'est pas le cas ou si vous avez besoin de configurer spécifiquement un proxy pour les connexions BlackBerry Dynamics NOC, configurez un serveur proxy Web selon vos besoins.

Serveur Web proxy spécifique à l'application

Si un serveur proxy Web est requis pour une application spécifique (par exemple BlackBerry Access pour la navigation ou d'autres applications tierces), vous devez utiliser la configuration des applications pour cette application.

Remarque : Consultez les fournisseurs tiers pour savoir si un proxy spécifique à une application est pris en charge et comment le configurer.

Si un serveur proxy Web spécifique à l'application est configuré, l'application BlackBerry Dynamics évalue les règles de proxy et de PAC localement sur le terminal avant que les règles de profil de connectivité BlackBerry Dynamics ne soient elles-mêmes évaluées. Par conséquent, il est important que toutes les URL de proxy configurées à l'aide du proxy manuel, ou qui peuvent être renvoyées par le fichier PAC, soient correctement configurées dans le profil de connectivité BlackBerry Dynamics.

1. Accédez à **Applications**, puis cliquez sur l'application que vous souhaitez configurer (par exemple, BlackBerry Access).
2. Sous **Configuration de l'application**, créez une nouvelle configuration ou modifiez une configuration existante.
3. Pour BlackBerry Access, dans l'onglet **Réseau**, sélectionnez **Activer le proxy Web** et **Utiliser la configuration automatique de proxy** selon vos besoins.

Pour plus d'informations, reportez-vous à la section Résolution des problèmes de routage dans le contenu relatif à BlackBerry Access.

Flux de données BlackBerry Dynamics

Il est important que les administrateurs comprennent les effets de certaines combinaisons de paramètres. Le tableau figurant dans cette section décrit l'interaction entre le profil de connectivité BlackBerry Dynamics et le serveur proxy HTTP configuré pour le service BlackBerry Proxy.

Comment BlackBerry UEM évalue les connexions aux hôtes

Le profil de connectivité BlackBerry Dynamics est toujours vérifié en premier. Lorsque le trafic arrive sur le serveur BlackBerry Proxy, la configuration du serveur Web proxy ou du PAC définie sur le serveur BlackBerry Proxy est évaluée en matière de connectivité. La configuration d'un serveur Web proxy sur le serveur BlackBerry Proxy contrôle la manière dont BlackBerry Proxy traite l'envoi du trafic vers Internet. Cela n'affecte pas la façon dont l'application BlackBerry Dynamics présente sur le terminal évalue les connexions.

	L'hôte dans le profil de connectivité est résolu en BlackBerry Proxy	L'hôte dans le profil de connectivité est résolu en Direct	L'hôte dans le profil de connectivité est bloqué
Proxy/PAC = URL proxy	Application BlackBerry Dynamics > Cluster BlackBerry Proxy > URL du serveur Web proxy > Destination	Application BlackBerry Dynamics > Destination	Contenu bloqué par BlackBerry Dynamics SDK
Proxy/PAC = Direct	Application BlackBerry Dynamics > Cluster BlackBerry Proxy > Destination	Application BlackBerry Dynamics > Destination	Contenu bloqué par BlackBerry Dynamics SDK
Proxy/PAC = Bloc	Contenu bloqué par le serveur Web proxy	Application BlackBerry Dynamics > Destination	Contenu bloqué par BlackBerry Dynamics SDK

Remarque : Certaines applications permettent de configurer un serveur Web proxy ou un PAC spécifiquement pour cette application. Par exemple, BlackBerry Access permet aux administrateurs de configurer un serveur Web proxy ou un PAC qui sera spécifiquement utilisé par BlackBerry Access. Dans ces scénarios, l'application évalue la configuration du serveur Web proxy spécifique à l'application avant d'évaluer le profil de connectivité BlackBerry Dynamics.

Pour plus d'informations, reportez-vous à la section Résolution des problèmes de routage dans le contenu relatif à l'administration de BlackBerry Access.

Configuration de Kerberos pour les applications BlackBerry Dynamics

Les applications BlackBerry Dynamics prennent en charge à la fois la délégation contrainte Kerberos et Kerberos PKINIT. La délégation contrainte Kerberos (KCD, Kerberos Constrained Delegation) et Kerberos PKINIT sont des implémentations distinctes de Kerberos. Vous pouvez prendre en charge l'un ou l'autre pour les applications BlackBerry Dynamics, mais pas les deux.

La délégation contrainte Kerberos (KCD) permet aux utilisateurs d'accéder aux ressources de l'entreprise sans avoir à entrer leurs informations d'identification réseau. La KCD utilise des tickets de service qui sont cryptés et décryptés par des clés ne contenant pas les informations d'identification de l'utilisateur.

Lorsque la *délégation* est configurée, l'application BlackBerry Dynamics délègue l'authentification à BlackBerry UEM qui demandera l'accès à une ressource professionnelle en son nom. La KCD *limite* les ressources accessibles : les administrateurs peuvent limiter les ressources réseau accessibles. Pour ce faire, configurez le compte sous lequel le délégué (BlackBerry UEM) s'exécute comme étant approuvé uniquement pour des services spécifiques.

Par exemple, si la KCD n'est pas configurée et qu'une application demande une ressource telle que mypage.mydomain.com, l'application demande des informations d'identification à l'utilisateur. Lorsque la KCD est configurée, l'infrastructure BlackBerry Dynamics gère l'authentification et l'utilisateur n'est pas invité à saisir les informations d'identification de la ressource.

Kerberos fait partie de Microsoft Active Directory. Avant de configurer la délégation contrainte Kerberos dans BlackBerry UEM, assurez-vous que votre environnement Kerberos fonctionne correctement et que vous comprenez les implications de la configuration de la délégation contrainte pour les ressources internes. Consultez la documentation Microsoft appropriée si vous avez besoin d'informations sur Kerberos en général ou sur la délégation contrainte.

L'authentification Kerberos PKINIT établit la confiance directement entre l'application BlackBerry Dynamics et Windows KDC. L'authentification de l'utilisateur est basée sur les certificats délivrés par les services de certificats Microsoft Active Directory. Pour pouvoir utiliser PKINIT, la délégation contrainte Kerberos ne doit pas être activée dans les paramètres d'application dans BlackBerry UEM.

Les informations contenues dans cette section sont fournies à titre indicatif. Si vous avez besoin d'informations supplémentaires sur Kerberos et BlackBerry UEM, contactez BlackBerry Technical Support Services.

Domaines, domaines (realms) et forêts

Le fonctionnement de BlackBerry UEM dans un environnement Kerberos à *domaine unique* comprend un ou plusieurs cœurs configurés de manière identique. Le fonctionnement de BlackBerry UEM dans un environnement Kerberos *multidomaine* comporte plusieurs cœurs configurés séparément.

Un *« realm » (domaine)* est un ensemble d'entités, qu'il s'agisse de domaines d'utilisateur ou de domaines de ressources. Un domaine de ressources est un domaine autre qu'un domaine utilisateur. Dans Kerberos, le nom de domaine doit toujours être saisi en majuscules.

Un *« domain » (domaine)* est un domaine de service de répertoire, le plus souvent issu d'Active Directory.

Les termes « realm » et « domain » sont interchangeables dans KCD.

Environnement Kerberos à domaine unique

1. Une application BlackBerry Dynamics fait une demande à un serveur ou service interne (la *cible*).

   La cible peut être un nom d'hôte (nom du serveur) ou un compte à protéger par Kerberos et BlackBerry Dynamics. Par exemple, si IIS est exécuté sur un serveur en tant que service réseau, la cible est le serveur exécutant IIS en tant que réseau. D'autre part, si IIS est exécuté en tant qu'utilisateur (par exemple, IISSrvUser), ce nom d'utilisateur, IISSrvUser, devient alors la cible.
2. La cible répond avec une vérification d'authentification interceptée par BlackBerry Dynamics.
3. BlackBerry Dynamics SDK envoie une demande à BlackBerry UEM pour qu'un ticket de service puisse accéder à la cible.
4. BlackBerry UEM authentifie l'utilisateur ou l'application (via des protocoles BlackBerry Dynamics internes) et demande un ticket de service pour le compte de l'utilisateur (délégation) pour le service sur la cible.
5. Active Directory vérifie sa stratégie locale. Si l'utilisateur a l'autorisation d'accéder à la ressource sur la cible et si la ressource sur la cible est autorisée (contrainte), Active Directory renvoie à un ticket de service BlackBerry UEM pour la ressource.
6. BlackBerry UEM envoie les informations nécessaires du ticket de service renvoyé à BlackBerry Dynamics SDK.
7. L'application BlackBerry Dynamics utilise les informations de BlackBerry UEM pour terminer l'authentification sur la cible.

Environnement Kerberos multidomaine, configuration à forêt unique

Dans un environnement KCD multidomaine, le client BlackBerry Dynamics sélectionne un BlackBerry UEM Core pour traiter la demande KCD en fonction du domaine DNS du serveur cible. Une fois que la cible est déterminée comme cible KCD, le client BlackBerry Dynamics détermine la liste des serveurs BlackBerry UEM Core qui se trouvent dans le même domaine DNS que la cible, puis sélectionne un BlackBerry UEM Core de manière aléatoire dans cette liste (en fonction des priorités) pour traiter la demande.

S'il n'y a pas de correspondance DNS de ce type (aucun BlackBerry UEM Core serveur ne se trouve dans le même domaine DNS que la cible), le client sélectionne de manière aléatoire dans la liste de tous les serveurs BlackBerry UEM Core.

Remarque : Lorsqu'une ressource (par exemple, Microsoft Exchange) a un nom de domaine complet qui ne reflète pas exactement le domaine Kerberos dans lequel se trouve la ressource, alors BlackBerry UEM peut ne pas être en mesure d'authentifier correctement la ressource. Par exemple, si le nom de pool DNS de la ressource est cas.domain.com mais que les serveurs réels derrière ce nom de pool DNS sont server1.alternatedomain.domain.com et server2.alternatedomain.domain.com, SDK ne pourra pas trouver de serveur BlackBerry UEM Core dans le domaine correct.

SDK compare le domaine DNS de l'hôte cible au domaine DNS de tous les serveurs BlackBerry UEM Core afin que la comparaison puisse être effectuée hors ligne sur le terminal dès que la requête Kerberos intervient, sans recherches supplémentaires. Si la liste des serveurs Core situés dans le même domaine DNS que la cible est vide, SDK renvoie la liste complète des serveurs. Sinon, il utilise la liste générée précédemment. La liste est ensuite randomisée et triée pour s'assurer qu'elle respecte également les priorités (les principaux en premier). SDK sélectionne les deux premières entrées et envoie la demande KCD au premier serveur Core de la liste. Si cette demande échoue, SDK envoie la demande au deuxième serveur Core.

Pour en savoir plus, rendez-vous sur support.blackberry.com/community pour consulter l'article 49304.

DNS pour BlackBerry UEM et BlackBerry Connectivity Node dans des domaines distincts

Le serveur BlackBerry UEM et le serveur BlackBerry Connectivity Node sont souvent installés dans le même domaine Kerberos, mais ce n'est pas nécessaire. Vous pouvez installer BlackBerry Connectivity Node dans une zone démilitarisée ou un groupe de travail « sacrificiel ». Si vous choisissez cette configuration, vous devez définir certaines configurations réseau requises, comme indiqué ci-dessous.

BlackBerry Dynamics fonctionne différemment entre la délégation Kerberos normale (ou authentification Kerberos) et la délégation contrainte Kerberos (KCD), ce qui affecte la configuration du réseau.

- Dans KCD, le service BlackBerry UEM Core demande des tickets d'authentification à partir du serveur de billetterie (le contrôleur de domaine) pour le compte des applications client.
- Dans Kerberos sans délégation contrainte, les applications client font les demandes de billetterie et les demandes passent par BlackBerry Proxy. Cela signifie que BlackBerry Proxy doit pouvoir découvrir le nom du contrôleur de domaine (serveur) Kerberos. Dans le système de noms de domaine (DNS), vous devez ajouter un enregistrement SRV spécifiant le service Kerberos qui active cette découverte. Cet enregistrement SRV doit être associé à un enregistrement A ou AAAA, et non à un enregistrement CNAME. La syntaxe ci-dessous s'adresse à un contrôleur de domaine Kerberos dans un domaine Internet nommé example.com :

  ```
  _kerberos._tcp.example.com. 86400 IN SRV 0 5 88 kerberos.example.com
  ```

  Il s'agit d'un serveur nommé curberos.example.com écoutant sur le port TCP 88 pour les requêtes Kerberos. La priorité est de 0 et le poids est de 5.

Conditions préalables

- Le port 88 du service Active Directory doit être accessible par tous les serveurs BlackBerry UEM.
- L'environnement Kerberos doit inclure les composants suivants :
  - Serveur Microsoft Active Directory : service du répertoire qui authentifie et autorise tous les utilisateurs et ordinateurs associés à votre réseau Windows
  - Centre de distribution de clés (KDC) Kerberos : service d'authentification sur le serveur Active Directory qui fournit des tickets de session et des clés aux utilisateurs et ordinateurs du domaine Active Directory
- Créez des noms principaux de service (SPN) pour tous les services HTTP (y compris BlackBerry Enterprise Mobility Server et d'autres services). Vous devez définir un SPN pour chaque ressource cible à laquelle vous souhaitez que les terminaux aient accès. Par exemple :

  ```
  setspn –S HTTP/SPHOST.FQDN:PORT domain\AppPoolUser
  ```

  Pour plus d'informations sur la création et la modification de SPN, rendez-vous sur docs.microsoft.com pour consulter l'article « Inscrire un nom principal de service pour les connexions Kerberos ». Les SPN doivent être configurés par les propriétaires des serveurs d'applications ou du serveur Active Directory.

Pour les environnements multidomaine Kerberos :

- Au moins un serveur BlackBerry UEM Core doit être installé dans chaque domaine Kerberos. BlackBerry UEM doit résider dans le même domaine Kerberos que la ressource, car la délégation de ressources inter-domaines n'est pas prise en charge.
- Assurez-vous que le KCD à domaine unique fonctionne avant de configurer le KCD multidomaine.
- Toutes les relations approuvées doivent correspondre à des approbations de forêts transitives bidirectionnelles.

  Important : Assurez-vous de maintenir une latence maximale de 5 ms entre les serveurs BlackBerry UEM Core et la base de données Microsoft SQL Server. Pour plus d'informations, reportez-vous au contenu relatif à la configuration matérielle requise de BlackBerry UEM.

Configurer la délégation contrainte Kerberos

Pour une configuration multidomaine, commencez toujours par configurer et tester un seul domaine, puis passez à l'ajout des autres domaines ou forêts.

Remarque : Si vous configurez la KCD pour BlackBerry Docs, reportez-vous à la section Configuration de la délégation contrainte Kerberos pour le service Docs.

Remarque : Pour plus d'informations sur le fichier keytab, rendez-vous sur support.blackberry.com pour consulter l'article 42712.

1. Associez le compte de service Kerberos à un nom principal de service (SPN). Ouvrez une invite de commande administrateur sur le serveur Active Directory et saisissez `setspn –s GCSvc/UEM_Core_host_machine DOMAIN\Kerberos_service_account`.

   Remplacez les variables de nom de serveur hôte, de domaine et de compte de service par des valeurs appropriées à votre environnement.

   Par exemple :

   ```
   setspn –s GCSvc/uem1.example.com example.com\kcdadmin
   ```

   Remarque : Le compte de service Kerberos est le nom du compte de service sous lequel le service KCD sera configuré dans BlackBerry UEM (gc.krb5.principal.name). Ce compte n'a pas besoin d'être identique au compte de service BlackBerry UEM, mais peut l'être.

2. Créez le fichier keytab Kerberos. Vous devez générer un nouveau fichier keytab et le copier sur le serveur BlackBerry UEM lorsque vous modifiez le mot de passe du compte Kerberos.

   La création du fichier keytab Kerberos définit également le mot de passe du compte Kerberos. Le mot de passe défini dans cette commande définit le mot de passe du compte que vous spécifiez dans la commande. Si vous avez déjà reçu un mot de passe, veillez à utiliser ce même mot de passe. Si vous en utilisez un autre, celui-ci est réinitialisé. Cela inclut le mot de passe du compte de service BlackBerry UEM, si vous utilisez le compte de service UEM pour créer le fichier keytab. Pour créer un fichier keytab, procédez comme suit :

   a) Ouvrez une fenêtre d'invite de commande sur le serveur KDC.
   b) Utilisez la commande ktpass. Pour plus d'informations sur la commande ktpass, rendez-vous sur docs.microsoft.com.

   ```
   ktpass -out outfilename.keytab -mapuser kerberos_account@REALM_IN_ALL_CAPS
   -princ kerberos_account@REALM_IN_UPPERCASE/ptype KRB5_NT_PRINCIPAL -pass
   kerberos_account_password
   ```

outfilename	Il s'agit du nom du fichier de sortie.
kerberos_account	Il s'agit du nom du compte Kerberos.
REALM_IN_UPPERCASE	Il s'agit du domaine Kerberos. Le nom ne doit utiliser que des lettres majuscules.
-pass kerberos_account_password	Il s'agit du mot de passe existant pour le compte Kerberos réutilisé. Si kerberos_account_password contient des caractères spéciaux, tels que ^, placez-les entre guillemets doubles.

   Par exemple :

   ```
   ktpass -out outfilename.keytab -mapuser kerberos_account@REALM_IN_UPPERCASE
    -princ kerberos_account@REALM_IN_UPPERCASE /ptype KRB5_NT_PRINCIPAL -pass
    kerberos_account_password
   ```

ou

```
ktpass /out outfilename.keytab /mapuser kerberos_account@REALM_IN_UPPERCASE /
princ kerberos_account@REALM_IN_UPPERCASE /ptype KRB5_NT_PRINCIPAL /pass
 kerberos_account_password
```

c) Copiez le nouveau fichier keytab (kcdadmin.keytab dans les exemples) enregistré dans ce répertoire sur le serveur BlackBerry UEM. Important : si plusieurs serveurs BlackBerry UEM Core sont configurés pour utiliser le même compte d'administrateur KCD, vous devez copier le fichier keytab sur chaque serveur BlackBerry UEM.

Vous pouvez copier le fichier keytab à n'importe quel emplacement sur les serveurs, par exemple, c:\keytab. Vous devrez y faire référence ultérieurement, alors notez-le.

3. Activez l'énumération des appartenances au groupe d'objets d'utilisateur AD. Pour plus d'informations, rendez-vous sur docs.microsoft.com et consultez la section « Comptes et groupes privilégiés dans Active Directory ».
4. Sur le serveur BlackBerry UEM, configurez les autorisations pour le compte de service BlackBerry UEM afin qu'il puisse envoyer les informations d'identification de l'utilisateur au système Kerberos. Il s'agit du compte associé au nom principal de service (SPN). Pour configurer les autorisations, procédez comme suit :
   a) Ouvrez le volet **Stratégie de sécurité locale** dans la console Windows.
   b) Sous **Stratégies locales**, sélectionnez **Attribution des droits d'utilisateur**, puis cliquez avec le bouton droit de la souris sur **Agir** comme partie intégrante du système d'exploitation dans le panneau de droite et sélectionnez **Propriétés**.
   c) Dans la fenêtre **Propriétés**, cliquez sur **Ajouter un utilisateur ou un groupe**, puis saisissez le nom du compte de service et cliquez sur **OK**.
5. Configurez les propriétés liées à Kerberos dans BlackBerry UEM.

   Vous ne pouvez spécifier qu'un seul KDC (contrôleur de domaine) dans la configuration BlackBerry UEM de chaque serveur BlackBerry UEM Core. Cela signifie que tous les appels liés à un KCD vers le contrôleur de domaine seront toujours dirigés vers ce même KCD. Cela signifie également que si ce KCD tombe en panne, tous les appels liées à ce KCD échoueront.

   - Dans Paramètres > BlackBerry Dynamics > Propriétés globales, les paramètres suivants sont requis pour activer KCD dans UEM.

Propriété	Description
Utiliser un UPN explicite	Activez cette propriété pour forcer BlackBerry UEM à effectuer l'authentification à l'aide de l'UPN (User Principal Name, nom d'utilisateur principal) explicite stocké dans Active Directory au lieu de l'UPN implicite généré en combinant l'alias et le domaine d'un utilisateur.
Activer KCD (gc.krb5.enabled)	Cochez cette case pour activer KCD.

   - Dans Paramètres > BlackBerry Dynamics > Propriétés (cliquez sur le nom du serveur), les paramètres suivants sont requis pour activer KCD dans UEM.

Propriété	Exemple	Description
gc.krb5.kdc=<kdc_host_name>	UEM1.EXAMPLE.COM	Nom complet de la KDC. Il correspond généralement au FQDN d'un contrôleur de domaine Active Directory.

Propriété	Exemple	Description
gc.krb5.keytab.file=<keytab_file_location>	c:/keytab/kcdadmin.keytab	Emplacement du fichier keytab. Dans le chemin d'accès, utilisez des barres obliques et non des barres obliques inverses.
gc.krb5.principal.name=<kcd_service_account>	kcdadmin@EXAMPLE.COM	Nom du compte de service utilisé par le service KCD.
gc.krb5.realm=<REALM>	EXAMPLE.COM	Nom du domaine Active Directory. La valeur doit être en majuscules.

6. (Facultatif) créez un fichier krb5.conf. Cela n'est nécessaire que s'il existe une relation approuvée CAPATH. Consultez votre équipe Active Directory si vous devez créer ce fichier.

   Le fichier krb5.conf est nécessaire pour établir des relations approuvées CAPATH de plusieurs domaines Kerberos. L'emplacement du fichier krb5.conf sur le serveur BlackBerry UEM doit être spécifié dans la propriété gc.krb5.config.file du serveur.

   Exemple de fichier krb5.conf :

```
[libdefaults] default_realm = NA.POD1.COM [realms] NA.POD1.COM = { kdc
 = pod1-na-ad.na.pod1.com } [ capaths] NA.POD1.COM = { APAC.POD2.COM =
 POD2.COM POD2.COM = POD1.COM POD1.COM = . } POD2.COM = { NA.POD1.COM =
 POD1.COM POD1.COM = . } APAC.POD2.COM = { NA.POD1.COM = POD1.COM POD1.COM =
 POD2POD2.COM POD2.COM = .}
```

Dépannage et diagnostics

Utilisez les fichiers journaux pour vous aider à détecter les problèmes que votre administrateur système peut résoudre ou envoyer à l' assistance technique BlackBerry à des fins d'enquête et de résolution. Vous pouvez également rechercher des informations dans la base de connaissances BlackBerry.

Activez la journalisation du débogage pour afficher les journaux.

Codes d'erreur de fichiers journaux Kerberos et KDC

Les informations saisies dans les journaux du serveur BlackBerry UEM peuvent souvent aider à expliquer les problèmes et erreurs d'authentification Kerberos et liés à KCD. Voici un exemple de journal d'erreurs Kerberos :

```
2019-06-26T13:23:19.424-0500 - CORE {ContainerMgmtServerThread#1}
 none|none [{{externalTenantId,S12345678}}] - ERROR KRB u=
 B32F95DF-4338-499A-A06D-7EAC36852A21 while requesting KRB ServiceTicket
 for serviceClass= HTTP server= uem1.example.com port= 443 serviceName=
 httpcom.rim.platform.mdm.dynamics.kerberos.KerberosException: Failed to
 impersonate userPrincipal KCDADMIN@UEM1.EXAMPLE.COM;
             krbErrCode: 63;
             krbErrText: Fail to create credential.
```

Les deux paramètres les plus importants dans les messages d'erreur sont krbErrCode et krbErrText, qui fournissent une description des conditions d'erreur possibles détectées.

Pour obtenir la liste complète des messages d'erreur Kerberos, rendez-vous sur docs.microsoft.com pour consulter l'article « Kerberos and LDAP error messages ».

Configuration de Kerberos PKINIT

BlackBerry UEM prend en charge Kerberos PKINIT pour l'authentification de l'utilisateur BlackBerry Dynamics à l'aide de certificats PKI.

Si vous souhaitez utiliser Kerberos PKINIT pour les applications BlackBerry Dynamics, votre organisation doit remplir les conditions suivantes :

Points clés

- La délégation Kerberos contrainte ne doit pas être activée.
- L'hôte KDC doit être ajouté à la liste des domaines autorisés dans le Profil de connectivité BlackBerry Dynamics.
- L'hôte KDC doit être à l'écoute sur le port TCP 88 (port Kerberos par défaut).
- BlackBerry Dynamics ne prend pas en charge le KDC sur UDP.
- Le KDC doit avoir un enregistrement A (IPv4) ou AAAA (IPv6) dans votre DNS.
- BlackBerry Dynamics n'utilise pas de fichiers de configuration Kerberos (comme `krb5.conf`) pour localiser le KDC approprié.
- Le KDC peut référer le client à un autre hôte KDC. BlackBerry Dynamics suivra l'instruction si l'hôte KDC auquel il est renvoyé a été ajouté à la liste des domaines autorisés dans le Profil de connectivité BlackBerry Dynamics.
- Le KDC peut obtenir le TGT de façon transparente pour BlackBerry Dynamics à partir d'un autre hôte KDC.

Certificats de serveur

- Les certificats de serveur Windows KDC émis via les services de certificats Active Directory doivent provenir exclusivement des versions suivantes de Windows Server. Aucune autre version n'est prise en charge.
  - Internet Information Server avec Windows Server 2008 R2
  - Internet Information Server avec Windows Server 2012 R2
- Des certificats de service KDC valides doivent se trouver soit dans le magasin de certificats BlackBerry Dynamics, soit dans le magasin de certificats du terminal.

Certificats client

- La longueur de clé minimale pour les certificats doit être de 2 048 octets.
- Les certificats client doivent inclure le nom d'utilisateur principal (par exemple, user@domain.com) dans l'autre nom d'objet de l'ID objet szOID_NT_PRINCIPAL_NAME 1.3.6.1.4.1.311.20.2.3
- Le domaine du Nom principal de l'utilisateur doit correspondre au nom de domaine du service KDC Windows.
- La propriété Utilisation de clé étendue du certificat doit avoir la valeur Ouverture de session par carte à puce Microsoft (1.3.6.1.4.1.311.20.2.2).
- Les certificats doivent être valides. Vérifiez leur validité par rapport aux serveurs listés ci-dessus.

Connecter BlackBerry UEM à un connecteur PKI BlackBerry Dynamics

Si vous souhaitez utiliser le logiciel PKI de votre organisation pour enregistrer des certificats pour les applications BlackBerry Dynamics et que votre logiciel PKI n'est pas pris en charge pour une connexion directe avec BlackBerry UEM, vous pouvez configurer un connecteur PKI BlackBerry Dynamics pour communiquer avec votre autorité de certification et relier BlackBerry UEM au connecteur PKI.

Remarque : Dans un environnement BlackBerry UEM Cloud, un BlackBerry Connectivity Node doit être installé pour permettre à BlackBerry UEM de communiquer avec le connecteur PKI via BlackBerry Cloud Connector.

Un connecteur PKI regroupe différents programmes Java et services Web sur un serveur principal permettant à BlackBerry UEM d'envoyer des demandes de certificat et de recevoir des réponses de l'autorité de certification. BlackBerry UEM utilise le protocole de gestion des certificats utilisateur BlackBerry Dynamics pour communiquer avec le connecteur PKI. Ce protocole s'exécute sur HTTPS et définit les messages au format JSON. Pour plus d'informations sur la configuration d'un connecteur PKI BlackBerry Dynamics, reportez-vous à la documentation relative au protocole de gestion des certificats utilisateur et au connecteur PKI.

Avant de commencer : Configurez un connecteur PKI BlackBerry Dynamics.

1. Sur la barre de menus, cliquez sur **Paramètres > Intégration externe > Autorité de certification**.
2. Cliquez sur **Ajouter une connexion PKI BlackBerry Dynamics**.
3. Dans le champ **Nom de connexion**, saisissez un nom de connexion.
4. Dans le champ **URL**, saisissez l'URL du connecteur PKI.
5. Sélectionnez l'une des options suivantes :
   - **Authentification avec nom d'utilisateur et mot de passe** : choisissez cette option si BlackBerry UEM s'authentifie auprès du connecteur PKI BlackBerry Dynamics en utilisant l'authentification par mot de passe.
   - **Authentification avec certificat client** : choisissez cette option si BlackBerry UEM s'authentifie auprès du connecteur PKI BlackBerry Dynamics en utilisant l'authentification basée sur les certificats.
6. Si vous avez sélectionné **Authentification avec nom d'utilisateur et mot de passe**, dans les champs **Nom d'utilisateur** et **Mot de passe**, saisissez le nom d'utilisateur et le mot de passe du connecteur PKI BlackBerry Dynamics.
7. Si vous avez sélectionné **Authentification avec certificat client**, cliquez sur **Parcourir** pour sélectionner et télécharger un certificat approuvé par le connecteur PKI BlackBerry Dynamics. Dans le champ **Mot de passe du certificat client**, saisissez le mot de passe du certificat.
8. Dans la section **Certificat approuvé pour le connecteur PKI**, vous pouvez spécifier le certificat que BlackBerry UEM utilise pour faire confiance aux connexions du connecteur PKI, sélectionnez une des options suivantes :
   - **Certificat de l'AC de BlackBerry Control TrustStore**
   - **Certificat d'autorité de certification** : si vous sélectionnez cette option, vous devez cliquer sur Parcourir pour naviguer et sélectionner le certificat d'autorité de certification de votre organisation.
   - **Certificat serveur du connecteur PKI** : si vous sélectionnez cette option, vous devez cliquer sur Parcourir pour naviguer et sélectionner le certificat de serveur de connecteur PKI de votre organisation.
9. Pour tester la connexion, cliquez sur **Tester la connexion**.
10. Cliquez sur **Enregistrer**.

À la fin :

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

Intégration de BlackBerry UEM avec Cisco ISE

Cisco Identity Services Engine (ISE) est un logiciel de gestion de réseau qui permet à une organisation de contrôler l'accès au réseau professionnel des terminaux (par exemple, autorisant ou refusant les connexions Wi-Fi ou VPN). Les administrateurs Cisco ISE peuvent créer et appliquer les politiques d'accès pour s'assurer que seuls les terminaux autorisés peuvent accéder au réseau professionnel.

Vous pouvez créer une connexion entre Cisco ISE et BlackBerry UEM de sorte que Cisco ISE puisse récupérer les données sur les terminaux qui sont activés sur BlackBerry UEM. Cisco ISE contrôle les données des terminaux pour déterminer si les terminaux sont conformes aux politiques d'accès. Par exemple :

- Cisco ISE vérifie si le terminal de l'utilisateur est activé sur BlackBerry UEM. Si le terminal n'est pas activé, une politique d'accès peut empêcher le terminal de se connecter aux points d'accès Wi-Fi ou VPN professionnels.
- Cisco ISE vérifie si le terminal de l'utilisateur est conforme à BlackBerry UEM. Si le terminal n'est pas conforme (terminal débridé ou cracké, par exemple), une politique d'accès peut empêcher le terminal de se connecter aux points d'accès Wi-Fi ou VPN professionnels.

Les administrateurs Cisco ISE peuvent afficher, trier et filtrer les données sur les terminaux dans la console de gestion Cisco ISE. Les administrateurs peuvent également effectuer des tâches de gestion de terminaux suivantes : verrouiller un terminal, supprimer les données professionnelles à partir d'un terminal ou supprimer toutes les données d'un terminal.

Pour intégrer BlackBerry UEM à Cisco ISE, effectuez les opérations suivantes :

Étape	Action
1	Vérifiez que l'environnement de votre organisation répond aux exigences d'intégration de BlackBerry UEM à Cisco ISE.
2	Créez un compte administrateur BlackBerry UEM que Cisco ISE peut utiliser pour obtenir des données sur les terminaux.
3	Ajoutez le certificat BlackBerry Web Services au magasin de certificats Cisco ISE.
4	Connectez BlackBerry UEM à Cisco ISE et configurez un profil d'autorisation et des stratégies d'accès.

Exigences : intégration de BlackBerry UEM à Cisco ISE

Élément	Configuration requise
Version de Cisco ISE	BlackBerry UEM prend en charge l'intégration à Cisco ISE version 1.2 et ultérieure.
Système d'exploitation pris en charge	Tout système d'exploitation pris en charge par BlackBerry UEM (voir la Matrice de compatibilité), à l'exception des systèmes d'exploitation suivants : • Windows 10 pour bureau

Élément	Configuration requise
Port d'écoute	Cisco ISE utilise le port d'écoute par défaut de BlackBerry Web Services, 18084, pour obtenir les données sur les terminaux de BlackBerry UEM. Si le port 18084 n'était pas disponible au moment de l'installation de BlackBerry UEM, l'application d'installation a sélectionné un autre port disponible. Pour vérifier la valeur de port correcte, dans le fichier journal BlackBerry UEM Core (CORE), recherchez (`^/ciscoise/.*`) et notez le numéro de port indiqué au-dessous de ce texte.
Pare-feu	Si un pare-feu existe entre BlackBerry UEM et Cisco ISE, configurez-le pour autoriser les sessions HTTPS entre les deux systèmes.

Créer un compte d'administrateur pouvant être utilisé par Cisco ISE

Cisco Identity Services Engine (ISE) nécessite un compte d'administrateur BlackBerry UEM dédié pour extraire des données sur les terminaux. Vous pouvez utiliser un compte d'administrateur existant ou en créer un nouveau. Il doit s'agir d'un compte d'administrateur local (et non d'un utilisateur de l'annuaire). Le compte d'administrateur nécessite un rôle disposant des autorisations suivantes :

- Afficher les utilisateurs et les terminaux activés
- Gérer les terminaux
- Verrouiller le terminal et définir un message
- Supprimer uniquement les données professionnelles
- Supprimer toutes les données du terminal

Les rôles d'administrateur de sécurité par défaut et d'administrateur d'entreprise ont ces autorisations. Pour créer un nouveau compte d'administrateur avec un rôle personnalisé, procédez comme suit en utilisant un compte d'administrateur ayant le rôle d'administrateur de sécurité.

Avant de commencer : Si vous souhaitez créer un rôle personnalisé pour le compte d'administrateur, dans la console de gestion BlackBerry UEM, cliquez sur **Paramètres > Administrateurs > Rôles >**. Sélectionnez les autorisations nécessaires. Cliquez sur **Enregistrer**.

1. Dans la console de gestion BlackBerry UEM, cliquez sur **Utilisateurs** sur la barre de menus.
2. Cliquez sur **Ajouter un utilisateur**.
3. Cliquez sur l'onglet **Local**.
4. Spécifiez les nom, prénom, nom d'affichage, nom d'utilisateur et l'adresse électronique.
5. Dans le champ **Mot de passe de console**, saisissez un mot de passe pour le compte d'administrateur.
6. Sélectionnez l'option **Ne pas définir de mot de passe d'activation du terminal**.
7. Cliquez sur **Enregistrer**.
8. Sur la barre de menus, cliquez sur **Paramètres**.
9. Cliquez sur **Administrateurs > Utilisateurs**.
10. Cliquez sur .
11. Recherchez et cliquez sur le compte d'utilisateur que vous avez créé.
12. Dans la liste déroulante **Rôle**, cliquez sur le rôle personnalisé que vous avez créé, le rôle d'administrateur de sécurité par défaut ou le rôle d'administrateur d'entreprise par défaut.
13. Cliquez sur **Enregistrer**.

À la fin : Ajout du certificat BlackBerry Web Services au magasin de certificats Cisco ISE

Ajout du certificat BlackBerry Web Services au magasin de certificats Cisco ISE

Pour permettre à Cisco Identity Services Engine (ISE) de se connecter à BlackBerry UEM, vous devez exporter le certificat BlackBerry Web Services et l'importer dans le magasin de certificats Cisco ISE. Si le domaine BlackBerry UEM de votre entreprise dispose de plusieurs instances de BlackBerry UEM, il vous suffit d'exporter le certificat à partir d'une seule instance.

Si vous ne disposez pas d'un compte d'administrateur Cisco ISE, envoyez ces instructions à un administrateur Cisco ISE.

Remarque : Les étapes 3 et ultérieures sont basées sur Cisco ISE version 1.4. Pour consulter la documentation Cisco ISE à jour, accédez au site Web des Guides de configuration de Cisco ISE pour lire le *Guide de l'administrateur Cisco Identity Services Engine*.

Avant de commencer : Créer un compte d'administrateur pouvant être utilisé par Cisco ISE.

1. Dans un navigateur, accédez à **https://<*server_name*>:<*BlackBerry_Web_Services_port*>/enterprise/admin/util/ws?wsdl** où *<server_name>* est le FQDN de l'ordinateur qui héberge le composant BlackBerry UEM Core. La valeur *<BlackBerry_Web_Services_port>* par défaut est 18084.
2. Exportez le certificat BlackBerry Web Services et enregistrez-le sur votre bureau. Pour obtenir des instructions, consultez la documentation du navigateur que vous utilisez.

   Exemple : dans Google Chrome, cliquez sur l'icône de verrouillage en regard de l'URL. Dans l'onglet **Connexion**, cliquez sur **Informations de certificat**. Dans l'onglet **Détails**, cliquez sur **Copier dans un fichier** et suivez les instructions à l'écran.
3. Connectez-vous à la console de gestion Cisco ISE.
4. Sur la barre de menus, cliquez sur **Administration > Système > Certificats**.
5. Dans le volet de gauche, cliquez sur **Certificats approuvés**.
6. Cliquez sur **Importer**. Parcourez l'arborescence et sélectionnez le certificat BlackBerry Web Services.
7. Cochez la case **Certificat approuvé pour l'authentification client et Syslog**.
8. Cochez la case **Approbation d'authentification des services Cisco**.
9. Cliquez sur **Submit**.

À la fin : Connecter BlackBerry UEM à Cisco ISE.

Connecter BlackBerry UEM à Cisco ISE

Si vous ne disposez pas d'un compte d'administrateur Cisco Identity Services Engine (ISE), envoyez ces instructions à un administrateur Cisco ISE, ainsi que les informations requises concernant BlackBerry UEM et le compte d'administrateur BlackBerry UEM.

Remarque : Les étapes suivantes sont basées sur Cisco ISE version 1.4. Pour consulter la documentation Cisco ISE à jour, accédez au site Web des Guides de configuration de Cisco ISE pour lire le *Guide de l'administrateur Cisco Identity Services Engine*.

Avant de commencer : Ajout du certificat BlackBerry Web Services au magasin de certificats Cisco ISE.

1. Connectez-vous à la console de gestion Cisco ISE.
2. Sur la barre de menus, cliquez sur **Administration > Ressources réseau > MDM externe**.

3. Cliquez sur **Ajouter**.
4. Dans le champ **Nom**, saisissez un nom convivial pour la connexion.
5. Dans le champ **Nom d'hôte ou adresse IP**, saisissez le FQDN ou l'adresse IP du domaine BlackBerry UEM.
6. Dans le champ **Port**, saisissez `18084`.

   Si le port 18084 n'était pas disponible au moment de l'installation de BlackBerry UEM, l'application d'installation a sélectionné un autre port disponible. Pour vérifier la valeur de port correcte, dans le fichier journal BlackBerry UEM Core (CORE), recherchez (`^/ciscoise/.*`) et notez le numéro de port indiqué au-dessous de ce texte.
7. Dans le champ **Nom d'utilisateur**, saisissez le nom d'utilisateur du compte d'administrateur BlackBerry UEM.
8. Dans le champ **Mot de passe**, saisissez le mot de passe du compte d'administrateur BlackBerry UEM.
9. Dans le champ **Intervalle d'interrogation**, indiquez, en minutes, la fréquence à laquelle vous voulez que Cisco ISE interroge BlackBerry UEM pour obtenir les données du terminal. Il est recommandé d'utiliser la valeur par défaut de 240 minutes.

   Remarque : Si vous définissez cette valeur sur 60 minutes ou moins, vous remarquerez peut-être un impact important sur les performances de l'environnement de votre entreprise. Si vous définissez cette valeur sur 0, Cisco ISE n'interroge pas BlackBerry UEM.
10. Cochez la case **Activer**.
11. Cliquez sur **Tester la connexion** pour vérifier que Cisco ISE peut se connecter à BlackBerry UEM.
12. Cliquez sur **Submit**.

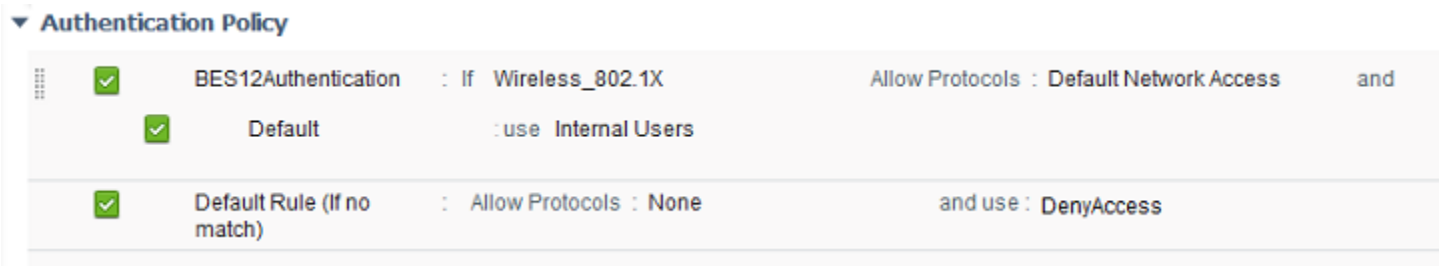
Une fois la connexion établie, vous pouvez consulter les attributs de dictionnaire de BlackBerry UEM dans **Stratégie > Éléments de stratégie > Dictionnaires > Système > MDM > Attributs du dictionnaire**. Les entrées de journal pour l'interrogation de Cisco ISE sont écrites dans le fichier journal BlackBerry UEM Core (CORE).

À la fin : Effectuez les tâches de configuration suivantes dans la console de gestion Cisco ISE. Pour obtenir les dernières instructions, accédez au site Web des Guides de configuration de Cisco ISE pour lire le *Guide de l'administrateur Cisco Identity Services Engine* (voir Configuration des serveurs MDM avec Cisco ISE).

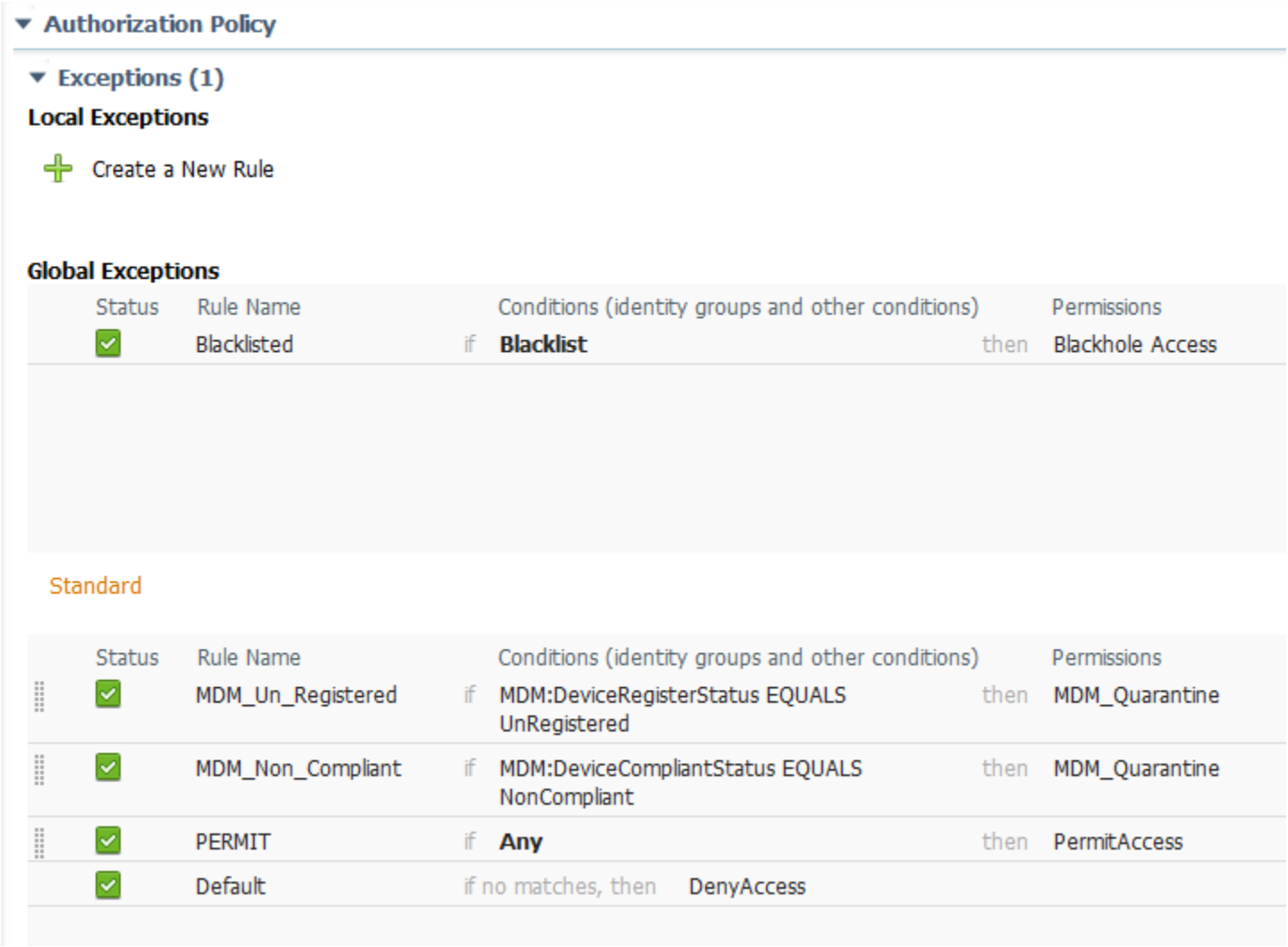
- Configurez des listes de contrôle d'accès sur le contrôleur LAN sans fil.
- Configurez un profil d'autorisation qui redirigera les terminaux qui ne sont pas activées sur BlackBerry UEM. Pour plus d'informations, reportez-vous à Redirection des appareils qui ne sont pas activés sur BlackBerry UEM.
- Configurez les règles de stratégie d'autorisation qui déterminent comment Cisco ISE gère les terminaux qui ne sont pas activés sur BlackBerry UEM ou qui ne sont pas compatibles avec BlackBerry UEM. Dans **Stratégie > Ensembles de stratégies** , créez une stratégie. Pour voir un exemple de stratégie, reportez-vous à Exemple : Règles de stratégie d'autorisation pour BlackBerry UEM.

Exemple : Règles de stratégie d'autorisation pour BlackBerry UEM

Stratégie d'authentification



Stratégie d'autorisation



Gestion de l'accès au réseau et des contrôles de terminaux à l'aide de Cisco ISE

Les administrateurs Cisco Identity Services Engine (ISE) peuvent effectuer les opérations suivantes. Pour obtenir des instructions, reportez-vous à la section Configuration des serveurs MDM avec Cisco ISE du *Guide de l'administrateur Cisco Identity Services Engine*.

Action	Description
Afficher les données du terminal	Vous pouvez afficher des informations sur les terminaux qui sont associés à BlackBerry UEM, notamment les informations suivantes : • Adresse MAC : adresse MAC unique du terminal • Conformité : indique si l'appareil est compatible avec BlackBerry UEM • Cryptage de disque : indique si les données du terminal sont cryptées • Inscription : indique si le terminal est activé sur BlackBerry UEM • Terminal cracké : indique si l'appareil est « débridé » ou « cracké » • Verrouillage PIN : indique si le terminal utilise un mot de passe • Fabricant • Modèle • Numéro de série • Version OS
Configurer les stratégies NAC	Permet de configurer les stratégies d'accès qui déterminent si des terminaux peuvent se connecter à des points d'accès d'un réseau Wi-Fi ou VPN professionnel. Par exemple, vous pouvez configurer une stratégie d'accès qui empêche les terminaux qui ne sont pas conformes à BlackBerry UEM d'accéder au réseau d'entreprise.
Verrouiller un terminal	Verrouiller le terminal iOS, Android ou Windows d'un utilisateur. Cette fonction est utile si l'utilisateur a égaré temporairement son terminal. BlackBerry UEM verrouille le terminal à l'aide d'une commande d'administration informatique. L'utilisateur doit saisir le mot de passe du terminal pour le déverrouiller. Les utilisateurs de terminaux peuvent également effectuer cette action à l'aide du portail Mon terminal.
Supprimer des données professionnelles	Permet de supprimer uniquement des données et applications professionnelles sur un terminal, sans toucher aux données et aux applications personnelles de l'utilisateur. Cette fonction est utile si le terminal de l'utilisateur est perdu ou si l'utilisateur n'est plus un employé. BlackBerry UEM supprime les données professionnelles à l'aide d'une commande d'administration informatique. Les utilisateurs de terminaux peuvent également effectuer cette action à l'aide du portail Mon terminal.
Supprimer toutes les données	Supprime toutes les données et applications d'un terminal et restaure les paramètres par défaut du terminal. Cette fonction est utile si le terminal de l'utilisateur est perdu ou volé, ou s'il est attribué à un autre utilisateur. BlackBerry UEM supprime toutes les données du terminal à l'aide d'une commande d'administration informatique. Les utilisateurs de terminaux peuvent également effectuer cette action à l'aide du portail Mon terminal.

Pour plus d'informations sur les commandes d'administration informatique et sur les types d'activation qui prennent en charge les commandes de verrouillage, de suppression des données professionnelles et de toutes les données, consultez le contenu relatif à l'administration.

Redirection des appareils qui ne sont pas activés sur BlackBerry UEM

Si Cisco Identity Services Engine (ISE) identifie un appareil qui tente d'accéder au réseau professionnel (Wi-Fi ou VPN), et que l'appareil n'est pas activé sur BlackBerry UEM, Cisco ISE ouvre une page d'inscription dans le navigateur de l'appareil pour rediriger l'utilisateur vers la console BlackBerry UEM Self-Service.

L'utilisateur nécessite un compte d'utilisateur BlackBerry UEM pour se connecter à BlackBerry UEM Self-Service et activer l'appareil. Demandez aux utilisateurs de contacter l'administrateur BlackBerry UEM si Cisco ISE les redirige vers la page d'inscription.

Pour plus d'informations sur l'ajout et l'activation de comptes d'utilisateurs, consultez le contenu relatif à l'administration.

Remarque : Si l'appareil d'un utilisateur a été précédemment activé avec BlackBerry UEM, puis désactivé, l'utilisateur n'est pas redirigé vers BlackBerry UEM Self-Service lorsqu'il tente d'accéder au réseau professionnel sur son appareil. Pour résoudre ce problème, lorsque vous supprimez un appareil de BlackBerry UEM, supprimez également ses données de Cisco ISE.

Informations juridiques

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

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

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

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

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

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

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

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

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

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

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

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

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

Maidenhead, Berkshire SL6 1RL
Royaume-Uni

Publié au Canada