BlackBerry UEM

Guide de configuration

12.9

Table des matières

Modification des certificats BlackBerry UEM..... 8
Considérations pour changer les certificats BlackBerry Dynamics..... 9
Modification d'un certificat BlackBerry UEM..... 10

Configurer BlackBerry UEM pour envoyer les données via un serveur proxy....12
Envoi de données via un serveur proxy TCP vers BlackBerry Infrastructure..... 12
Comparaison des proxys TCP..... 12
Configurer BlackBerry UEM pour utiliser un serveur proxy TCP transparent..... 13
Activer SOCKS v5 sur un serveur proxy TCP..... 14
Envoi de données via BlackBerry Router vers BlackBerry Infrastructure..... 14
Configurer BlackBerry UEM pour utiliser BlackBerry Router..... 14
Envoi de données via un proxy HTTP vers BlackBerry Dynamics NOC..... 15
Configurer les paramètres proxy HTTP..... 15

Configuration de connexions par le biais de serveurs proxy internes..... 16
Configurer les paramètres proxy côté serveur..... 16

Connexion à vos annuaires d'entreprise..... 17
Configuration de l'authentification Microsoft Active Directory dans un environnement qui inclut une f orêt de ressources..... 17
Se connecter à une instance de Microsoft Active Directory..... 18
Se connecter à un annuaire LDAP..... 19
Activer les groupes liés par annuaire..... 21
Activer l'intégration..... 22
Activer et configurer l'intégration et la suppression..... 23
Synchroniser une connexion à un répertoire d'entreprise..... 24
Prévisualiser un rapport de synchronisation..... 24
Afficher un rapport de synchronisation..... 24
Ajouter un calendrier de synchronisation..... 24

Se connecter à un serveur SMTP pour envoyer des notifications par e-mail... 26
Se connecter à un serveur SMTP pour envoyer des notifications par e-mail..... 26

Configuration de l'authentification unique pour BlackBerry UEM..... 27
Configurer la délégation contrainte pour permettre au compte Microsoft Active Directory de prendre e n charge l'authentification unique..... 27
Configurer l'authentification unique pour BlackBerry UEM..... 28
URL des consoles pour l'authentification unique..... 28
Configuration requise pour le navigateur : authentification unique..... 29

Obtention d'un certificat APNs pour gérer les terminaux iOS et macOS..... 31
Obtenir un fichier CSR signé auprès de BlackBerry..... 31
Demander des certificats APNs à Apple..... 32
Enregistrer le certificat APNs..... 32
Renouveler le certificat APNs..... 32
Dépannage de l'APNs..... 33
Le certificat APNs ne correspond pas au fichier CSR. Fournissez le fichier APNs (.pem) qui con vient ou envoyez un nouveau fichier CSR..... 33
Je reçois le message « Le système a rencontré une erreur » lorsque j'essaye d'obtenir un CSR signé..... 33
Je ne peux pas activer de terminaux iOS ou macOS..... 34

Désignation des terminaux autorisés à accéder à Exchange ActiveSync..... 35
Étapes à suivre pour configurer Exchange ActiveSync et BlackBerry Gatekeeping Service..... 35
Configuration des autorisations à des fins de contrôle d'accès..... 36
Autorisez uniquement les terminaux approuvés à accéder à Exchange ActiveSync 37
Configurer Microsoft Exchange pour autoriser uniquement les terminaux approuvés à accéder à Exchange ActiveSync..... 38
Configurer la stratégie d'accès des terminaux dans Microsoft Office 365..... 38
Configurer les autorisations Microsoft IIS à des fins de contrôle d'accès..... 39
Création d'une configuration de contrôle d'accès..... 39

Connexion de BlackBerry UEM à Microsoft Azure..... 41
Créer un compte Microsoft Azure..... 41
Synchroniser Microsoft Active Directory avec Microsoft Azure..... 41
Create an enterprise endpoint in Azure..... 42
Configurer BlackBerry UEM pour la synchronisation avec Microsoft Intune..... 43
Configurer BlackBerry UEM pour la synchronisation avec Microsoft Intune..... 43
Configuration de BlackBerry UEM pour la synchronisation avec Windows Store for Business..... 44
Configurer BlackBerry UEM pour une synchronisation avec Windows Store for Business..... 44
Créer un administrateur pour Windows Store pour Entreprises..... 45
Activez l'application dans Windows Store for Business..... 45

Configurer BlackBerry UEM pour la prise en charge des terminaux Android q ui possèdent un profil professionnel..... 46
Configurez BlackBerry UEM pour prendre en charge les périphériques Android qui ont un profil de travail... 47
Supprimez la connexion au profil de travail Android à votre domaine Google..... 49
Supprimer la connexion de domaine Google à l'aide de votre compte Google..... 49
Modifier ou tester la connexion au domaine Google..... 50

Ajouter une licence E-FOTA..... 51

Gestion de l'attestation des terminaux Samsung KNOX..... 52

Gestion de l'attestation des terminaux Windows 10..... 53

Configuration de BlackBerry UEM pour le programme d'inscription des appareils.....54
Créer un compte du programme d'inscription des appareils.....54
Télécharger une clé publique.....54
Générer un jeton de serveur.....55
Enregistrer le jeton de serveur avec BlackBerry UEM.....55
Ajouter la première configuration d'inscription.....55
Mettre à jour le jeton de serveur.....57
Supprimer une connexion DEP.....57

Configuration de BlackBerry UEM Self-Service pour les utilisateurs.....58
Configurer BlackBerry UEM Self-Service.....58

Configuration de la haute disponibilité pour un domaine BlackBerry UEM.....59
Haute disponibilité pour les composants qui gèrent des terminaux BlackBerry OS.....60
Architecture : haute disponibilité pour BlackBerry UEM.....60
Équilibrer la charge des données des terminaux BlackBerry 10.....61
Haute disponibilité et BlackBerry Connectivity Node.....62
Comment BlackBerry UEM évalue-t-il l'intégrité des composants ?.....62
Installer une instance supplémentaire de BlackBerry UEM.....63
Configurer la haute disponibilité pour la console de gestion.....63

Configuration d'une base de données haute disponibilité à l'aide de la mise en miroir.....65
Base de données haute disponibilité pour les composants qui gèrent des terminaux BlackBerry OS.....65
Étapes à suivre pour configurer la mise en miroir de bases de données.....66
Configuration requise : mise en miroir de bases de données.....66
Conditions préalables : configurer la mise en miroir de bases de données.....67
Créer et configurer la base de données miroir.....67
Connecter BlackBerry UEM à la base de données miroir.....68
Configurer une nouvelle base de données miroir.....69

Configurer des connexions TLS/SSL à Exchange ActiveSync lors de l'activation de BlackBerry Secure Gateway.....70
Configurer BlackBerry UEM pour faire confiance au certificat du serveur Exchange ActiveSync.....70
Configurer BlackBerry UEM afin d'utiliser les versions TLS et les codages pris en charge par Exchange ActiveSync.....70

Simplification des activations Windows 10.....71
Déployer un service de détection pour simplifier les activations Windows 10.....71

Migration d'utilisateurs, de terminaux, de groupes et d'autres données depuis un serveur source.....74

Conditions préalables : migrer des utilisateurs, terminaux, groupes et autres données depuis un serveur source....74
Connexion à un serveur source....76
Export the self-signed root certificate for the Good Control server....79
Considérations : migration des stratégies informatiques, des profils et des groupes depuis un serveur source....80
Migrer des stratégies informatiques, des profils et des groupes depuis un serveur source....84
Migration des stratégies et des profils de Good Control à BlackBerry UEM....84
Good Control features in BlackBerry UEM....85
Considérations : migration d'utilisateurs à partir d'un serveur source....86
Migrer des utilisateurs depuis un serveur source....88
Considérations : migration de terminaux à partir d'un serveur source....88
Référence rapide pour la migration des terminaux....91
Migrer des terminaux depuis un serveur source....91
Migrations de terminaux DEP....92
Migration de terminaux DEP sur lesquels BlackBerry UEM Client est installé....92
Migration de terminaux DEP sur lesquels BlackBerry UEM Client n'est pas installé....93

Configuring BlackBerry UEM to support BlackBerry Dynamics apps....94
Gérer les clusters BlackBerry Proxy....94
Configurer Direct Connect ou un proxy Web pour les connections à BlackBerry Proxy....95
Configurer les propriétés BlackBerry Dynamics....95
Propriétés globales de BlackBerry Dynamics....96
Propriétés de BlackBerry Dynamics....100
Propriétés de BlackBerry Proxy....100
Configurer les paramètres de communication pour les applications BlackBerry Dynamics....102

Configurer des certificats pour les applications BlackBerry Dynamics....103
Configurer une valeur TTL pour les certificats client....103
Configurer des connexions PKI pour les applications BlackBerry Dynamics....103
Interactions du connecteur PKI....104

Intégration de BlackBerry UEM avec Cisco ISE....107
Exigences : intégration de BlackBerry UEM à Cisco ISE....107
création d'un compte d'administrateur pouvant être utilisé par Cisco ISE....108
Ajout du certificat BlackBerry Web Services au magasin de certificats Cisco ISE....109
Connexion de BlackBerry UEM à Cisco ISE....110
Exemple : règles de stratégie d'autorisation pour BlackBerry UEM....111
Gestion de l'accès au réseau et des contrôles de terminaux à l'aide de Cisco ISE....112
Redirection des terminaux qui ne sont pas activés sur BlackBerry UEM....113

Surveillance de BlackBerry UEM à l'aide des outils SNMP....114
Opérations SNMP prises en charge....114
Configuration requise : analyse SNMP....115
MIB de BlackBerry UEM....115
Compiler la MIB et configurer l'outil de gestion SNMP....116
Utiliser SNMP pour surveiller les composants....117
Configurer SNMP pour surveiller les composants....117

Glossaire..... 119

Informations juridiques..... 121

Modification des certificats BlackBerry UEM

Lorsque vous installez BlackBerry UEM, l'application de configuration génère plusieurs certificats auto-signés qui sont utilisés pour authentifier la communication entre différents composants UEM et avec des périphériques. Vous pouvez modifier les certificats si la stratégie de sécurité de votre organisation requiert que les certificats soient signés par l'Autorité de certification de votre organisation ou si vous souhaitez utiliser des certificats émis par une autorité de certification dont les périphériques et les navigateurs font déjà confiance.

Remarque : Si des problèmes surviennent lorsque vous modifiez un certificat, la communication entre les composants UEM et entre UEM et les périphériques peut être perturbée. Si vous choisissez de modifier les certificats, planifiez et testez le changement avec attention.

Vous pouvez modifier les certificats suivants:

Certificats	La description
Certificat SSL pour consoles	Un certificat SSL que la console de gestion BlackBerry UEM Self-Service autonome BlackBerry UEM utilisent pour authentifier les navigateurs. Si vous configurez une haute disponibilité, le certificat doit avoir le nom du domaine BlackBerry UEM. Vous pouvez trouver le nom de 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 authentifier les applications qui utilisent les API de BlackBerry Web Services pour gérer BlackBerry UEM. Si vous configurez une haute disponibilité, le certificat doit avoir le nom du domaine BlackBerry UEM. Vous pouvez trouver le nom de domaine BlackBerry UEM dans la console de gestion sous Paramètres> Infrastructure> Instances.
Apple certificat de signature de profil	Un certificat que BlackBerry UEM utilise pour signer le profil MDM que les utilisateurs doivent accepter lorsqu'ils activent les périphériques iOS. Si vous utilisez un certificat signé par une autorité de certification, assurez-vous que le certificat racine de l'autorité de certification est installé sur les périphériques iOS des utilisateurs avant leur activation.
Certificat SSL pour les applications	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	An SSL certificate that authenticates connections between BlackBerry UEM and BlackBerry Proxy. Ensure that the names of any additional instances of BlackBerry UEM Core or BlackBerry Connectivity Node are added to the Subject Alternative Name of this certificate.

Certificats	La description
Certificate for application management	An SSL certificate that is used for authentication between BlackBerry UEM and BlackBerry Dynamics apps. 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. Assurez-vous que les noms des instances supplémentaires de BlackBerry UEM Core ou BlackBerry Connectivity Node sont ajoutés à l'autre nom de l'objet de ce certificat.
Certificat pour Direct Connect	Un certificat SSL utilisé pour l'authentification entre BlackBerry Dynamics Direct Connect et d'autres composants. Si vous modifiez ce certificat et que la modification prend effet avant que BlackBerry UEM ne pousse le certificat à toutes les applications BlackBerry Dynamics, toutes les applications qui n'ont pas reçu le certificat doivent être réactivées. Assurez-vous que les noms de toute instance supplémentaire de BlackBerry UEM Core ou BlackBerry Connectivity Node sont ajoutés au Nom alternatif du sujet de ce certificat.

Considérations pour changer les certificats BlackBerry Dynamics

If you want to change any of the BlackBerry Dynamics SSL certificates, keep the following considerations in mind. If problems occur when you change a certificate, communication between BlackBerry UEM components and between BlackBerry UEM and BlackBerry Dynamics apps could be disrupted. Plan and test certificate changes carefully.

Ajouter de nouveaux certificats à tout équipement périphérique

Si vous avez ajouté des certificats BlackBerry Dynamics à des périphériques sur votre réseau, ajoutez le nouveau certificat aux périphériques avant de l'ajouter à BlackBerry UEM.

Mettre à jour les applications BlackBerry Dynamics

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

Any BlackBerry Dynamics apps developed by your organization must be built with version 3.2 or later of the BlackBerry Dynamics SDK. Older apps can't receive the new certificate from BlackBerry UEM.

BlackBerry Dynamics les applications doivent être ouvertes pour recevoir un certificat

Users must open a BlackBerry Dynamics app for the app to receive a certificate from BlackBerry UEM. If you are replacing the BlackBerry Dynamics certificate for application management or Direct Connect and the change becomes effective before BlackBerry UEM pushes the certificate to all BlackBerry Dynamics apps, any apps that did not receive the certificate must be reactivated. Apps do not receive certificates while they are suspended on iOS devices or while Android devices are in Doze mode.

Assurer le BlackBerry Connectivity Node est accessible

If any BlackBerry Proxy instances are unreachable by BlackBerry UEM when BlackBerry Dynamics certificates are replaced, BlackBerry Dynamics apps will not be able to connect to those instances following the certificate replacement.

Le certificat d'horaire change de manière appropriée

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

Laissez suffisamment de temps pour que les nouveaux certificats se propagent aux applications BlackBerry Proxy et BlackBerry Dynamics. Si vous ne remplissez que le certificat pour les serveurs BlackBerry Dynamics, autorisez au moins 10 minutes avant le redémarrage du serveur.

Si vous remplacez le certificat BlackBerry Dynamics pour la gestion des applications ou Direct Connect, il est recommandé que le temps jusqu'à ce que la date d'entrée en vigueur soit plus long que le paramètre Vérification de connectivité "Dernier moment de contact" dans le profil de conformité.

Si vous remplacez les certificats BlackBerry Dynamics pour la gestion des applications et Direct Connect, réglez les temps effectifs d'au moins 30 minutes d'intervalle. Si vous avez un grand nombre d'utilisateurs et des applications BlackBerry Dynamics, vous devez attendre plus de 30 minutes entre chaque certificat.

Modification d'un certificat BlackBerry UEM

Avant de commencer :

- Obtenir un certificat signé par une autorité de certification approuvée. Le certificat doit être dans un format de stockage de clés (.pfx, .pkcs12).
- Si vous remplacez le certificat BlackBerry Dynamics pour la gestion des applications ou Direct Connect, assurez-vous que les applications BlackBerry Dynamics des utilisateurs sont mises à jour pour les versions les plus récentes.

1. Sur la barre de menus, cliquez sur **Paramètres > Infrastructure > Certificats de serveur**.
2. Dans la section du certificat que vous souhaitez remplacer, cliquez sur **Afficher les détails**.
3. Cliquez sur **Remplacer le certificat**.
4. Parcourez le fichier de certificat et sélectionnez-le.
5. Entrez un mot de passe de cryptage 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 pour la gestion des applications ou Direct Connect, spécifiez la date d'entrée en vigueur pour le changement de certificat.

Il est recommandé que la date d'entrée en vigueur soit plus loin que le paramètre de vérification de connectivit é "Dernier moment de contact" dans le profil de conformité. Si vous modifiez plus d'un certificat, vous devez sé parer les temps effectifs d'au moins 30 minutes.

8. Cliquez sur **Remplacer**.

À la fin :

- Si vous avez remplacé l'un des certificats sur l'onglet **Certificats du serveur**, redémarrez le service BlackBerry UEM Core sur tous les serveurs. Il est recommandé de choisir une période de faible activité pour redémarrer le s serveurs.
- Pour les certificats sur l'onglet certificats BlackBerry Dynamics, vous pouvez cliquer sur **Revenir à la valeur par défaut** pour revenir à l'utilisation d'un certificat auto-signé.
- Sous l'onglet Certificats BlackBerry Dynamics, vous pouvez effacer les cases à cocher **Trust BlackBerry UEM CA** et **Trust BlackBerry Dynamics CA** si vous n'avez plus besoin de faire confiance aux certificats auto-signés. Vous pouvez effacer la case à cocher **Confidentialité de BlackBerry Trust** uniquement si vous avez remplacé t ous les certificats sur l'onglet Certificats BlackBerry Dynamics.
- Si les applications BlackBerry Dynamics cessent de communiquer après avoir changé les certificats, assurez-v ous que les applications sont à jour et que les utilisateurs doivent réactiver les applications.

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 ou une instance de BlackBerry Router 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 BlackBerry Router ou un serveur proxy TCP. BlackBerry Router ou le serveur proxy TCP fait office d'intermédiaire entre BlackBerry UEM et BlackBerry Infrastructure.

Vous pouvez installer BlackBerry Router ou un serveur proxy en dehors du pare-feu de votre organisation dans une zone démilitarisée. L'installation de BlackBerry Router ou d'un serveur proxy TCP dans une zone démilitarisée offre un niveau de sécurité plus élevé pour BlackBerry UEM. Seul BlackBerry Router ou 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 BlackBerry Router ou le serveur proxy.

Pour les terminaux BlackBerry OS (versions 5.0 à 7.1), BlackBerry Router envoie/reçoit également directement les données vers/depuis les terminaux connectés à un réseau Wi-Fi professionnel ou à un ordinateur doté de BlackBerry Device Manager.

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 et un autre serveur proxy TCP transparent pour le service BlackBerry Affinity Manager. Ces services requièrent 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 d'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
Transparent TCP proxy	• Intercepte la communication normale au niveau de la couche réseau sans qu'aucune configuration particulière ne soit nécessaire de la par t 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 l a bande passante en amont et améliorer les temps de réponse des cli ents grâce à la mise en cache
SOCKS v5 proxy	• Protocole Internet permettant de gérer le trafic Internet via un serveu r proxy • Peut être géré avec pratiquement n'importe quelle application TCP/U DP, 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 serv eur 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 : installez un serveur proxy TCP transparent compatible dans le domaineBlackBerry 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 Servic e**, saisissez le FQDN ou l'adresse IP et le numéro de port du serveur proxy. C haque champ requiert une seule valeur.
Acheminer le trafic SRP via un serveur proxy TCP	Dans les champs **Affinity Manager**, saisissez le FQDN ou l'adresse IP et le n uméro de port du serveur proxy. Chaque champ requiert une seule valeur.
Acheminer le trafic BlackBer ry Secure Connect Plus via u n serveur proxy TCP	Dans les champs **BlackBerry Secure Connect Plus**, saisissez le FQDN ou l'a dresse 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**.

Envoi de données via BlackBerry Router vers BlackBerry Infrastructure

Vous pouvez configurer plusieurs instances de BlackBerry Router pour la haute disponibilité. Vous ne pouvez configurer qu'un seul port d'écoute pour les instances de BlackBerry Router.

BlackBerry UEM ne prend en charge aucune instance de BlackBerry Router initialement utilisée avec BES5.

Par défaut, BlackBerry UEM se connecte à BlackBerry Router avec le port 3102 pour les services BlackBerry UEM et au port 3101 pour les services BES5. BlackBerry Router prend en charge tout le trafic sortant depuis BlackBerry UEM Core et BlackBerry Affinity Manager.

Remarque : Si vous souhaitez utiliser un autre port que le port par défaut pour BlackBerry Router, rendez-vous sur http://support.blackberry.com/kb et consultez l'article KB36385.

Configurer BlackBerry UEM pour utiliser BlackBerry Router

Avant de commencer : Installez BlackBerry Router dans le domaine BlackBerry UEM. Pour obtenir des instructions sur la configuration de BlackBerry Router, reportez-vous au contenu relatif à l'installation et à la mise à niveau.

1. Sur la barre de menus, cliquez sur **Paramètres > Infrastructure > BlackBerry Router et proxy**.
2. Sélectionnez l'option **BlackBerry Router**.
3. Cliquez sur +.
4. Saisissez l'adresse IP ou le nom d'hôte de l'instance de BlackBerry Router que vous souhaitez connecter à BlackBerry UEM.
5. Cliquez sur **Ajouter**.
6. Répétez les étapes 1 à 5 pour chaque instance de BlackBerry Router que vous souhaitez configurer.
7. Dans le champ **Port**, saisissez le numéro du port d'écoute de toutes les instances de BlackBerry Router. La valeur par défaut est 3102.
8. Cliquez sur **Enregistrer**.

Envoi de données via un proxy HTTP vers BlackBerry Dynamics NOC

Vous pouvez configurer BlackBerry UEM pour envoyer les données via un proxy HTTP entre BlackBerry UEM et BlackBerry Dynamics NOC.

Remarque : Le proxy doit être en mesure d'accéder au port 443 vers BlackBerry Dynamics NOC. Pour plus d'informations sur les exigences relatives aux ports, reportez-vous à l'article Connexions sortantes :BlackBerry UEM vers BlackBerry Dynamics NOC.

Configurer les paramètres proxy HTTP

1. Sur la barre de menus, cliquez sur **Paramètres > Infrastructure > BlackBerry Router et proxy**.
2. Sélectionnez **Activer le proxy HTTP**.
3. 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**
4. Si vous voulez utiliser le serveur proxy pour vous connecter aux serveurs spécifiés, cliquez sur + pour spécifier tous les serveurs supplémentaires.
5. Dans le champ **Adresse**, saisissez l'adresse du serveur proxy.
6. Dans le champ **Port**, saisissez le numéro de port écouté par le serveur proxy.
7. 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 BlackBerry UEM doit utiliser pour l'authentification.
8. 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 vers BlackBerry MDS Connection Service.

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 Configurer BlackBerry UEM pour envoyer les 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 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 au répertoire de votre entreprise pour lui permettre d'accéder à la liste de s utilisateurs de votre entreprise. Vous pouvez connecter BlackBerry UEM à plusieurs répertoires et ceux-ci peuve nt 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 du rép ertoire, et BlackBerry UEM peut authentifier les administrateurs pour la console de gestion et les utilisateurs po ur BlackBerry UEM Self-Service.
- Vous pouvez lier les groupes de répertoires d'entreprise à des BlackBerry UEM groupes pour organiser les utili sateurs de BlackBerry UEM tels qu'ils sont organisés dans votre répertoire d'entreprise. Reportez-vous à la sect ion Activer les groupes liés par annuaire..
- Vous pouvez activer l'intégration pour des groupes spécifiques de votre répertoire d'entreprise afin de créer au tomatiquement des utilisateurs de BlackBerry UEM. Si vous activez l'intégration, vous pouvez également confi gurer la suppression afin de supprimer des données ou comptes d'utilisateur lorsque des utilisateurs sont sup primés 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 com ptes utilisateur locaux et authentifier les administrateurs à l'aide de l'authentification par défaut.

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

Étape	Action
1	Créez une connexion à une instance Microsoft Active Directory ou à un répertoire LDAP. Si votre environnement inclut une forêt de ressources, consultez la section Configuration de l'authentification Microsoft Active Directory dans un environnement qui inclut une forêt de ressources .
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 u n environnement qui inclut une forêt de ressources

Si l'environnement de votre entreprise inclut une forêt de ressources dédiée à l'exécution de Microsoft Exchange, vous pouvez configurer l'authentification Microsoft Active Directory pour les comptes d'utilisateur situés dans les forêts de compte approuvées.

S'il existe une forêt de ressources dans l'environnement de votre organisation, vous devez installer BlackBerry UE M dans la forêt de ressources. Dans la forêt de ressources, vous devez créer une boite aux lettres pour chaque co mpte d'utilisateur et vous devez associer les boites aux lettres aux comptes d'utilisateur. Lorsque vous associez l

es boites aux lettres dans la forêt de ressources à des comptes d'utilisateur dans les forêts de compte, les compt es d'utilisateur obtiennent l'accès complet aux boites aux lettres et les comptes d'utilisateur sont connectés au se rveur Microsoft Exchange.

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

Pour plus d'informations, rendez-vous sur technet.microsoft.com et lisez 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 se rveurs 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 suivan te.
- Si vous avez configuré l'authentification unique, la délégation contrainte doit être configurée pour le compte.

1. Sur la barre de menus, cliquez sur **Paramètres > Intégration externe > Annuaire d'entreprise**.
2. Cliquez sur **Ajouter une connexion Microsoft Active Directory**.
3. Dans le champ **Nom de connexion du répertoire**, saisissez le nom de la connexion à l'annuaire.
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 suivan tes :
   - Pour autoriser BlackBerry UEM à détecter automatiquement les centres de distribution clés (KDC), cliquez s ur **Automatique**.
   - Pour spécifier la liste de KDC à utiliser pour l'authentification de BlackBerry UEM, cliquez sur **Manuel**. Dans l e 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 (p ar exemple kdc01.exemple.com:88). Cliquez sur + pour spécifier les contrôleurs de domaine KDC supplém entaires 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 **Manuell e**. Dans le champ **Noms des serveurs**, saisissez le nom DNS du serveur de catalogue global auquel vous so uhaitez 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:326 8). 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**.

    Pour configurer un domaine de groupe global, dans la section **Liste des domaines de groupes globaux**, cliquez sur +. Dans le champ **Domaine**, entrez 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 principaux centres de distribution ou Manuel pour spécifier la liste de KDC que BlackBerry UEM peut utiliser pour l'authentification. Cliquez sur **Ajouter**.
12. 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 plus d'informations sur l'identification unique, reportez-vous à Configuration de l'authentification unique pour BlackBerry UEM.
14. Pour synchroniser plus d'informations utilisateur à partir de votre annuaire d'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.

Tâches connexes

Configurer la délégation contrainte pour permettre au compte Microsoft Active Directory de prendre en charge l'authentification unique

Référence connexe

Configuration requise pour le navigateur : authentification unique

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 con forme 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 pas se lors de la connexion suivante.
- Si la connexion LDAP est cryptée SSL, vérifiez que vous disposez du certificat de serveur correspondant à la c onnexion LDAP.
- 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 domain e 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**. Da ns le champ **Serveur LDAP**, saisissez le nom du serveur LDAP. Pour ajouter d'autres 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 son t 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 D N 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 r echerches d'informations d'utilisateur.
9. Dans le champ **Filtre de recherche d'utilisateurs LDAP**, saisissez le filtre de recherche LDAP requis pour trouve r des objets utilisateur dans le serveur de répertoires 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, saisis sez `(&(objectclass=user)(logindisabled=false))`.
10. Dans la liste déroulante **Étendue de la recherche d'utilisateurs LDAP**, effectuez l'une des opérations suivante s :
    - Pour rechercher tous les objets qui suivent l'objet de base, cliquez sur **Tous les niveaux**. Il s'agit du paramè tre par défaut.
    - Pour rechercher les objets situés un niveau après le DN de base, cliquez sur **Un seul niveau**.
11. In the **Unique identifier** field, type the name of the attribute that uniquely identifies each user in your organizat ion's LDAP directory (must be a string that is immutable and globally unique). For example, `dominoUNID` in IB M Domino LDAP 7 and later.
12. Dans le champ **Prénom**, saisissez l'attribut de prénom de chaque utilisateur (par exemple, `givenName`).
13. Dans le champ **Nom**, saisissez l'attribut de 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 d'adresse électronique 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 de 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 de 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'appartenance au groupe**, saisissez l'attribut de l'identifiant d'appartenance à chaque groupe. Cet attribut doit être immuable et globalement unique (par exemple, saisissez `member`).
    - 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 c haque synchronisation.

   Le paramètre par défaut est cinq. Si le nombre de modifications à synchroniser dépasse la limite de synchroni sation, 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 i ntégrer, utilisateurs à supprimer.
6. Dans le champ **Niveau d'imbrication maximal des groupes de répertoires**, saisissez le nombre de niveaux imbr iqués 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 à la rubrique « Créer des gr oupes liés par répertoire » du 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 d'annuaires d'entreprise. Les comptes d'utilisateur sont ajoutés à Black Berry 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 supp rimé 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 d'un cycle de synchronisation pour éviter toute suppression inattendue en raison de l a latence de la réplication du répertoire. Quel que soit l'intervalle de synchronisation, le délai de protection contre l a suppression requiert un minimum de deux heures.

Remarque : Les paramètres de suppression s'appliquent également aux utilisateurs d'annuaires existants de Blac kBerry UEM. Il est recommandé de cliquer sur l'icône d'aperçu pour générer le rapport de synchronisation de l'ann uaire et vérifier les modifications.

Synchronisation

Lorsque vous avez activé la suppression, lors de la prochaine synchronisation, les règles de suppression sont app liquées à tous les utilisateurs que vous avez ajoutés manuellement dans la console de gestion, avant l'activation d e 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, mêm e s'ils appartiennent déjà à un groupe associé à un répertoire. Si la suppression est activée, les utilisateurs que vo us ajoutez manuellement à BlackBerry UEM verront les règles de répression appliquées à leurs terminaux lors de l a prochaine synchronisation s'ils ne sont pas membres d'un groupe de la synchronisation d'intégration au momen t de la synchronisation.

Activer et configurer l'intégration et la suppression

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 > 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 sa uf si leur compte d'utilisateur est absent des groupes de répertoires d'intégration pendant deux cycles de sync hronisation consécutifs. Quel que soit l'intervalle de synchronisation, le délai de protection contre la suppressi on requiert un minimum de deux heures.

11. Pour forcer la synchronisation des groupes de répertoires d'entreprise, cochez la case **Forcer la synchronisati on**.

    Si cette case est cochée, lorsqu'un groupe est supprimé de votre répertoire d'entreprise, les liaisons vers ce gr oupe 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 c haque processus de synchronisation (cinq par défaut).

    Si le nombre de modifications à synchroniser dépasse la limite de synchronisation, vous pouvez empêcher l'ex écution 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 imbriq ués 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 vo s attentes avant la synchronisation.

1. Sur la barre de menus, cliquez sur **Paramètres > Intégration externe > Annuaire d'entreprise**.
2. Dans la colonne **Aperçu**, cliquez sur l'icône .
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.

Ajouter un calendrier de synchronisation

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

- Intervalle : vous spécifiez la durée entre chaque synchronisation, la période et les jours où elle se produit.
- Une fois par jour : vous spécifiez l'heure à laquelle la synchronisation démarre et les jours où elle se produit.
- Aucune récurrence : vous spécifiez 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. 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 s ynchronisations. **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 c ommence. **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 c ommence. **b.** Sélectionnez le jour où vous souhaitez que la synchronisation inter vienne.

5. Cliquez sur **Ajouter**.

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 en savoir plus 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 FQDN du serveur SMTP. Par exemple, `mail.example.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 spécifié dans le champ **Adresse de l'expéditeur**.

Configuration de l'authentification unique pour BlackBerry UEM

Si vous connectez BlackBerry UEM à Microsoft Active Directory, vous pouvez configurer l'authentification unique pour permettre aux administrateurs ou aux utilisateurs de contourner la page Web de connexion et d'accéder directement à la console de gestion ou à BlackBerry UEM Self-Service. Lorsque des administrateurs ou des utilisateurs se connectent à Windows, le navigateur utilise leurs informations d'identification pour les authentifier automatiquement auprès de BlackBerry UEM. Les informations de connexion Windows peuvent inclure les informations d'identification Microsoft Active Directory ou les informations d'identification dérivées (par exemple, à partir de lecteurs CAC ou de jetons numériques).

Avant d'activer l'authentification unique à BlackBerry UEM pour une connexion Microsoft Active Directory, vous devez configurer la délégation contrainte sur le compte Microsoft Active Directory qui utilise BlackBerry UEM pour la connexion à l'annuaire.

Remarque : si vous activez l'authentification unique, toutes les modifications que vous apporterez au compte Microsoft Active Directory nécessiteront un redémarrage des services BlackBerry UEM sur tous les ordinateurs qui hébergent une instance de BlackBerry UEM. Les administrateurs et utilisateurs doivent se déconnecter de leurs ordinateurs et se reconnecter pour utiliser l'authentification unique de BlackBerry UEM.

Lorsque vous configurez l'authentification unique pour BlackBerry UEM, vous pouvez effectuer ce qui suit :

Étape	Action
1	Configurer la délégation contrainte pour permettre au compte Microsoft Active Directory de prendre en charge l'authentification unique.
2	Activez l'authentification unique pour une connexion Microsoft Active Directory.
3	Consultez la configuration requise du navigateur pour l'authentification unique.

Configurer la délégation contrainte pour permettre au compte Microsoft Active Directory de prendre en charge l'authentification unique

Pour permettre à BlackBerry UEM de prendre en charge l'authentification unique, vous devez configurer la délégation contrainte sur le compte Microsoft Active Directory qui utilise BlackBerry UEM pour la connexion à l'annuaire. La délégation contrainte permet aux navigateurs de s'authentifier auprès de BlackBerry UEM au nom des administrateurs ou utilisateurs lorsqu'ils accèdent à la console de gestion ou à BlackBerry UEM Self-Service.

1. Utilisez l'outil Éditeur ADSI de Windows Server ou l'outil de ligne de commande setspn pour ajouter les SPN (noms principaux de services) suivants de BlackBerry UEM au compte Microsoft Active Directory :
   - HTTP/ *<host_FQDN_or_pool_name>* (par exemple, HTTP/domaine123.exemple.com)
   - BASPLUGIN111/*<host_FQDN_or_pool_name>* (par exemple, BASPLUGIN111/domaine123.exemple.com)

   Si vous avez configuré la haute disponibilité sur les consoles de gestion d'un domaine BlackBerry UEM, spécifiez le nom du pool. Sinon, spécifiez le FQDN de l'ordinateur qui héberge la console de gestion.

   Remarque : vérifiez qu'aucun autre compte de la forêt Microsoft Active Directory ne possède le même SPN.

2. Ouvrez Microsoft Active Directory Users and Computers.
3. Dans les propriétés du compte Microsoft Active Directory de l'onglet **Délégation**, sélectionnez l'une des option s suivantes :
   - N'approuver cet utilisateur que pour la délégation aux services spécifiés
   - Utiliser uniquement Kerberos
4. Ajoutez les SPN de l'étape 1 à la liste des services.

Concepts connexes

Configurer la haute disponibilité pour la console de gestion

Configurer l'authentification unique pour BlackBerry UEM

Lorsque vous configurez l'authentification unique pour les administrateurs et les utilisateurs qui se connectent à BlackBerry UEM, vous la configurez pour la console de gestion et pour BlackBerry UEM Self-Service.

Avant de commencer :

- Configurez la délégation contrainte pour le compte Microsoft Active Directory que BlackBerry UEM utilise pour la connexion à l'annuaire.
- Si vous activez l'authentification unique pour plusieurs connexions Microsoft Active Directory, vérifiez qu'aucu ne relation de confiance n'existe entre les forêts Microsoft Active Directory.

1. Sur la barre de menus, cliquez sur **Paramètres > Intégration externe > Annuaire d'entreprise**.
2. Dans la section **Connexions au répertoire configurées**, cliquez sur le nom d'une connexion Microsoft Active Di rectory.
3. Dans l'onglet **Authentification**, cochez la case **Activer l'authentification unique Windows**.
4. Cliquez sur **Enregistrer**.
5. Cliquez sur **Enregistrer**.
   BlackBerry UEM valide les informations d'authentification de Microsoft Active Directory. Si les informations ne sont pas valides, BlackBerry UEM vous invite à spécifier les informations qui conviennent.
6. Cliquez sur **Fermer**.

À la fin :

- Redémarrez les services BlackBerry UEM sur tous les ordinateurs qui hébergent une instance de BlackBerry UE M.
- Demandez aux administrateurs et aux utilisateurs de BlackBerry UEM Self-Service de configurer leur navigateu r afin qu'il prenne en charge l'authentification unique de BlackBerry UEM.

Tâches connexes

Configurer la délégation contrainte pour permettre au compte Microsoft Active Directory de prendre en charge l'au thentification unique

URL des consoles pour l'authentification unique

Si vous configurez l'authentification unique pour BlackBerry UEM, vous devez demander aux administrateurs d'ac céder à la console de gestion et aux utilisateurs d'accéder à BlackBerry UEM Self-Service via l'URL suivante :

Console	URL relative à l'authentification unique
Console de gestion de BlackBerry UEM	https://<*host_FQDN_or_pool_name*>:<*port*>/admin
BlackBerry UEM Self-Service	https://<*host_FQDN_or_pool_name*>:<*port*>/mydevice

L'authentification unique est prioritaire sur les autres méthodes d'authentification qui permettent aux administrateurs de se connecter à la console de gestion et aux utilisateurs de se connecter à BlackBerry UEM Self-Service. Si les normes de sécurité de votre organisation exigent que les administrateurs ou utilisateurs utilisent une autre méthode d'authentification, vous devez leur demander d'accéder à la console de gestion ou à BlackBerry UEM Self-Service via l'URL suivante :

Console	URL relative aux autres méthodes d'authentification
Console de gestion BlackBerry UEM	https://<*host_FQDN_or_pool_name*>:<*port*>/admin?sso=n
BlackBerry UEM Self-Service	https://<*host_FQDN_or_pool_name*>:<*port*>/mydevice?sso=n

Remarque : lorsque vous installezBlackBerry UEM, par défaut, l'application de configuration essaie d'attribuer le port 8000 àBlackBerry UEM Self-Serviceet le port 443 à la console de gestion. Si le port 443 n'est pas disponible, l'application de configuration essaie d'utiliser le port 8008. Si les ports par défaut ne sont pas disponibles, l'application d'installation attribue une valeur de port comprise entre 12 000 et 12 999. Pour confirmer les ports attribués àBlackBerry UEM Self-Serviceet à la console de gestion,reportez-vous à la section « Vérifier les valeurs de ports attribuées par l'application de configuration »BlackBerry UEMdans le contenu relatif à l'installation et à la mise à niveau.

Configuration requise pour le navigateur : authentification unique

Si vous configurez l'authentification unique pour BlackBerry UEM, la configuration suivante est requise pour les navigateurs utilisés par les administrateurs et utilisateurs de BlackBerry UEM Self-Service.

Élément	Configuration requise
Navigateur	Un des navigateurs suivants : • Internet Explorer • Microsoft Edge • Mozilla Firefox • Google Chrome Pour plus d'informations sur les versions prises en charge, reportez-vous à la Matrice de compatibilité.

Élément	Configuration requise
Paramètres du navigateur	Internet Explorer avec les paramètres suivants : • Les URL de la console de gestion et de BlackBerry UEM Self-Service sont attribuées à la zone Intranet local (Options Internet > Sécurité). • L'option Activer l'authentification Windows intégrée est sélectionnée (Options Internet > Avancées). Firefox avec les paramètres suivants : • Dans la liste about:config, https://, *<host_FQDN_or_pool_name>* est ajouté à la préférence « network.negotiate-auth.trusted-uris ». Pour plus d'informations, rendez-vous sur kb.mozillazine.org/about:config. Google Chrome utilise les paramètres de la zone Intranet local de Internet Explorer. Les URL de la console de gestion et de BlackBerry UEM Self-Service doivent être attribuées à la zone Intranet local (Options Internet > Sécurité).

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 créer une notification d'événement 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 (requête de signature de certificat) signé auprès de BlackBerry.

1. Sur la barre de menus, cliquez sur **Paramètres > Intégration externe > Apple Push Notification**.
2. Cliquez sur **Obtenir les certificats APNs**.
   Si vous souhaitez renouveler votre certificat APNs, cliquez plutôt sur **Renouveler les certificats**.
3. Dans la section **Étape 1 sur 3 - Télécharger le certificat CSR signé de BlackBerry**, cliquez sur **Télécharger le c ertificat**.
4. Cliquez sur **Enregistrer** pour enregistrer le fichier CSR signé (.scsr) sur votre ordinateur.

À la fin : Demander des certificats APNs à Apple .

Demander des certificats APNs à Apple

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

1. Sur la barre de menus, cliquez sur **Paramètres > Intégration externe > Apple Push Notification**.
2. Dans la section **Étape 2 sur 3 - Obtenir un certificat APNs d'Apple**, cliquez sur **Apple Push Certificate Portal**. V ous 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 télécharger le fichier CSR signé (.scsr).
5. Téléchargez et enregistrez le certificat APNs (.pem) sur votre ordinateur.

À la fin : Enregistrer le certificat APNs.

Enregistrer le certificat APNs

Avant de commencer : Demander des certificats APNs à 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 **Certificat APNs test**.
- Pour afficher l'état et la date d'expiration du certificat APNs, cliquez sur **Paramètres > Intégration externe > Gestion iOS**. Pour plus d'informations sur le renouvèlement du certificat APNs, reportez-vous à la section Renouveler 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.

Vous pouvez créer une notification d'événement 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 > Apple Push Notification**.
2. Dans la section **Étape 2 sur 3 - Obtenir un certificat APNs d'Apple**, cliquez sur **Apple Push Certificate Portal**. V ous êtes dirigé vers le portail Apple Push Certificates Portal.
3. Connectez-vous au portail Apple Push Certificates Portal en utilisant l'ID Apple utilisé pour obtenir le certificat APNs d'origine.
4. Suivez les instructions pour renouveler le certificat APNs (.pem). Vous devrez alors télécharger le nouveau fich ier CSR signé.
5. Téléchargez et enregistrez le certificat APNs renouvelé sur votre ordinateur.
6. Dans la section **Étape 3 sur 3 - Inscrire le certificat APNs**, cliquez sur **Parcourir**. Accédez au certificat APNs re nouvelé et sélectionnez-le.
7. Cliquez sur **Envoyer**.

À la fin :

- Pour tester la connexion entre BlackBerry UEM et le serveur APNs, cliquez sur **Certificat APNs test**.
- Pour afficher l'état et la date d'expiration du certificat APNs, cliquez sur **Paramètres > Intégration externe > Ge stion iOS**.

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 e nvoyez 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 vo us savez quel fichier CSR est le plus récent, revenez au portail Apple Push Certificates Portal pour le charger. Si vo us l'ignorez, procurez-vous un nouveau fichier CSR auprès de BlackBerry, puis revenez au portail Apple Push Certif icates 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 http://support.blackberry.com/kb pour lire l'article KB37266.

Je ne peux pas activer de 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 le certificat APNs affiche l'état « Installé ». Si l'état est incorrect, tentez de réenregistrer le certificat APNs.
- Cliquez sur **Certificat APNs test** 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.

Désignation des terminaux autorisés à accéder à Exchange ActiveSync

Vous pouvez empêcher les terminaux non autorisés d'utiliser Exchange ActiveSync sauf s'ils sont ajoutés expressément à la liste des terminaux autorisés. Les terminaux qui ne figurent pas dans la liste autorisée n'ont pas accès à la messagerie professionnelle et aux données de l'organiseur. BlackBerry Gatekeeping Service vous permet d'ajouter des terminaux à la liste autorisée en toute simplicité.

Pour utiliser BlackBerry Gatekeeping Service, vous devez créer une configuration de contrôle d'accès pour Microsoft Exchange Server ou Microsoft Office 365 et attribuer un profil de contrôle d'accès et un profil de messagerie (ou une application de messagerie avec une configuration d'application) aux utilisateurs pour lesquels le serveur de contrôle d'accès automatique est sélectionné.

Une fois le contrôle d'accès configuré et les profils de contrôle d'accès et de messagerie (ou une application de messagerie avec une configuration d'application) attribués aux utilisateurs, les terminaux des utilisateurs sont automatiquement ajoutés à la liste autorisée. Si le profil de contrôle d'accès, le profil de messagerie ou l'application de messagerie d'un utilisateur est supprimé, le terminal correspondant est supprimé de la liste autorisée et ne peut plus se connecter à Microsoft Exchange, sauf si vous l'autorisez par un autre moyen (par exemple, Windows PowerShell).

Vous pouvez installer une ou plusieurs instances deBlackBerry Connectivity Nodepour ajouter des instances supplémentaires de composants de connectivité de terminal au domaine de votre organisation. ChaqueBlackBerry Connectivity Nodecontient une instance deBlackBerry Gatekeeping Service. Chaque instance doit être en mesure d'accéder au serveur de contrôle d'accès de votre organisation. Si vous souhaitez que les données de contrôle d'accès soient gérées uniquement par l'instance deBlackBerry Gatekeeping Serviceinstallée avec les composants principaux deBlackBerry UEM, vous pouvez modifier les paramètres par défaut pour désactiver l'instance deBlackBerry Gatekeeping Servicedans chaque instance deBlackBerry Connectivity Node. Pour plus d'informations sur l'installation et la configuration deBlackBerry Connectivity Node,reportez-vous au contenu relatif à la planificationetau contenu relatif à l'installation et à la mise à niveau.

Vous pouvez configurer des groupes de serveurs pour qu'ils dirigent le trafic de connectivité des terminaux vers une connexion locale spécifique à BlackBerry Infrastructure. Lorsque vous associez un profil de contrôle d'accès à un groupe de serveurs, tout utilisateur auquel est attribué ce profil de contrôle d'accès utilise n'importe quelle instance active de BlackBerry Gatekeeping Service dans ce groupe de serveurs. Lorsque vous configurez un groupe de serveurs, vous pouvez choisir de désactiver les instances de BlackBerry Gatekeeping Service dans le groupe.

Reportez-vous au contenu relatif à l'administrationpour savoir comment :

- Ajouter un serveur de contrôle d'accès automatique à un profil de contrôle d'accès
- Autoriser ou bloquer des terminaux qui ne sont pas ajoutés automatiquement à la liste approuvée

Étapes à suivre pour configurer Exchange ActiveSync et BlackBerry Gatekeeping Service

Pour configurer BlackBerry Gatekeeping Service, procédez comme suit :

Étape	Action
1	Configuration des autorisations à des fins de contrôle d'accès.

Étape	Action
2	Autorisez uniquement les terminaux approuvés à accéder à Exchange ActiveSync ..
3	Configurer les autorisations Microsoft IIS à des fins de contrôle d'accès.
4	Création d'une configuration de contrôle d'accès.
5	Créez un profil de contrôle d'accès et attribuez-le aux comptes d'utilisateurs, aux groupes d'utilisateurs ou aux groupes de terminaux. Pour obtenir des instructions, reportez-vous à la section relative à la création d'un profil de contrôle d'accès dans le contenu relatif à l'administration.

Configuration des autorisations à des fins de contrôle d'accès

Pour utiliser le contrôle d'accès Exchange ActiveSync, vous devez créer un compte d'utilisateur dans Microsoft Exchange Server ou Microsoft Office 365 et lui donner les autorisations nécessaires pour le contrôle d'accès.

Si vous utilisez Microsoft Office 365, créez un compte d'utilisateur Microsoft Office 365 et attribuez-lui les rôles Destinataires de messagerie et Accès client dans l'entreprise.

Si vous utilisez Microsoft Exchange Server 2010 ou version ultérieure, suivez les instructions ci-dessous pour configurer les rôles de gestion avec les autorisations appropriées pour gérer les boîtes aux lettres et l'accès client de Exchange ActiveSync. Pour exécuter cette tâche, vous devez être un administrateur Microsoft Exchange doté des autorisations suffisantes pour créer et modifier les rôles de gestion.

Avant de commencer :

- Sur l'ordinateur qui héberge Microsoft Exchange, créez un compte et une boite aux lettres pour gérer le contrôle d'accès dans BlackBerry UEM (par exemple, BUEMAdmin). Vous devez spécifier les informations de connexion de ce compte lors de la création d'une configuration Exchange ActiveSync. Notez le nom de ce compte, vous devrez l'indiquer à la fin de la tâche ci-dessous.
- WinRM doit être configuré sur les paramètres par défaut sur l'ordinateur qui héberge l'instance de Microsoft Exchange Server que vous configurez à des fins de contrôle d'accès. Ouvrez une invite de commande en tant qu'administrateur et exécutez la commande `Winrm quickconfig` . Lorsque l'outil affiche `Effectuer ces modifications [y/n]`, saisissez `y`. Lorsque la commande aboutit, vous voyez apparaitre le message suivant.

```
WinRM has been updated for remote management.


WinRM service type changed to delayed auto start.

WinRM service started.

Created a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this

 machine.
```

1. Ouvrez Microsoft Exchange Management Shell.
2. Saisissez `New-ManagementRole -Name "<name_new_role_mail_recipients>" -Parent "Mail Recipients"`. Appuyez sur la touche ENTRÉE.
3. Saisissez `New-ManagementRole -Name "<name_new_role_org_ca>" -Parent "Organization Client Access"`. Appuyez sur la touche ENTRÉE.

4. Saisissez `New-ManagementRole -Name "<name_new_role_exchange_servers>" -Parent "Exchange Servers"`. Appuyez sur la touche ENTRÉE.
5. Saisissez `Get-ManagementRoleEntry "<name_new_role_mail_recipients>\*" | Where {$_.Name -ne "Get-ADServerSettings"} | Remove-ManagementRoleEntry`. Appuyez sur la touche ENTRÉE.
6. Saisissez `Get-ManagementRoleEntry "<name_new_role_org_ca>\*" | Where {$_.Name -ne "Get-CasMailbox"} | Remove-ManagementRoleEntry`. Appuyez sur la touche ENTRÉE.
7. Saisissez `Get-ManagementRoleEntry "<name_new_role_exchange_servers>\*" | Where {$_.Name -ne "Get-ExchangeServer"} | Remove-ManagementRoleEntry`. Appuyez sur la touche ENTRÉE.
8. Saisissez `Add-ManagementRoleEntry "<name_new_role_mail_recipients>\Get-ActiveSyncDeviceStatistics" -Parameters Mailbox`. Appuyez sur la touche ENTRÉE.
9. Saisissez `Add-ManagementRoleEntry "<name_new_role_mail_recipients>\Get-ActiveSyncDevice" -Parameters Identity`. Appuyez sur la touche ENTRÉE.
10. Effectuez cette étape uniquement si vous utilisez Microsoft Exchange 2013. Saisissez `Add-ManagementRoleEntry “<name_new_role_mail_recipients>\Get-MobileDeviceStatistics” –Parameters Mailbox`. Appuyez sur la touche ENTRÉE.
11. Effectuez cette étape uniquement si vous utilisez Microsoft Exchange 2013. Saisissez `Add-ManagementRoleEntry “<name_new_role_mail_recipients>\Get-MobileDevice” –Parameters Mailbox`. Appuyez sur la touche ENTRÉE.
12. Saisissez `Add-ManagementRoleEntry "<name_new_role_org_ca>\Set-CasMailbox" -Parameters Identity, ActiveSyncBlockedDeviceIDs, ActiveSyncAllowedDeviceIDs`. Appuyez sur la touche ENTRÉE.
13. Saisissez`New-RoleGroup "<name_new_group>" -Roles "<name_new_role_mail_recipients>", "<name_new_role_org_ca>", "<name_new_role_exchange_servers>"`. Appuyez sur la touche ENTRÉE.
14. Saisissez `Add-RoleGroupMember -Identity "<name_new_group>" -Member "BUEMAdmin"`. Appuyez sur la touche ENTRÉE.
15. Saisissez `Add-ManagementRoleEntry "<name_new_role_mail_recipients>\Set-AdServerSettings"`. Appuyez sur la touche ENTRÉE.
16. Saisissez `Add-ManagementRoleEntry "<name_new_role_mail_recipients>\Remove-ActiveSyncDevice" -Parameters Identity,Confirm`. Appuyez sur la touche ENTRÉE.
17. Effectuez cette étape uniquement si vous utilisez Microsoft Exchange 2013. Type `Add-ManagementRoleEntry "<name_new_role_mail_recipients>\Remove-MobileDevice" -Parameters Identity,Confirm`. Appuyez sur la touche ENTRÉE.

À la fin : Autorisez uniquement les terminaux approuvés à accéder à Exchange ActiveSync ..

Autorisez uniquement les terminaux approuvés à accéder à Exchange ActiveSync .

Si votre entreprise utilise Microsoft Exchange Server 2010 ou ultérieur, reportez-vous à Configurer Microsoft Exchange pour autoriser uniquement les terminaux approuvés à accéder à Exchange ActiveSync .

Si votre entreprise utilise Microsoft Office 365, reportez-vous à Configurer la stratégie d'accès des terminaux dans Microsoft Office 365.

Configurer Microsoft Exchange pour autoriser uniquement les terminaux approuvés à accéder à Exchang e ActiveSync

Vous devez configurer Microsoft Exchange Server 2010 ou ultérieur pour autoriser uniquement les terminaux app rouvés à accéder à Exchange ActiveSync. Les terminaux des utilisateurs existants non explicitement ajoutés à la l iste autorisée de Microsoft Exchange doivent être mis en quarantaine jusqu'à ce que BlackBerry UEM leur autoris e l'accès.

Pour exécuter cette tâche, vous devez être un administrateur Microsoft Exchange disposant des autorisatio ns appropriées pour configurer les paramètres Set-ActiveSyncOrganization. Pour plus d'informations sur la f açon d'autoriser uniquement les terminaux approuvés à accéder à Exchange ActiveSync, consultez https:// technet.microsoft.com pour lire l'article *Activer un terminal pour Exchange ActiveSync*

Avant de commencer :

- Configuration des autorisations à des fins de contrôle d'accès.
- Vérifiez auprès de votre administrateur Microsoft Exchange si des utilisateurs utilisent ou non Exchange Active Sync actuellement.

Si le niveau d'accès par défaut de votre organisation à Exchange ActiveSync est défini sur Autoriser et que vos uti lisateurs sont configurés et synchronisent leurs terminaux avec succès, vous devez vous assurer que ces utilisate urs ont une dispense personnelle ou une règle de terminal associée à leur compte d'utilisateur ou à leur terminal a vant de définir le niveau d'accès par défaut sur Quarantaine. Si ce n'est pas le cas, ils sont mis en quarantaine et le urs terminaux ne se synchronisent pas tant qu'ils n'y sont pas autorisés par BlackBerry UEM.

Pour plus d'informations sur la définition du niveau d'accès par défaut à Exchange ActiveSync pour la mise en qua rantaine, consultez http://support.blackberry.com/kb pour lire l'article KB33531.

1. Sur un ordinateur hébergeant Microsoft Exchange Management Shell, ouvrez Microsoft Exchange Managemen t Shell.
2. Saisissez `Set-ActiveSyncOrganizationSettings –DefaultAccessLevel Quarantine`. Appuyez s ur la touche ENTRÉE.

À la fin : Configurer les autorisations Microsoft IIS à des fins de contrôle d'accès.

Configurer la stratégie d'accès des terminaux dans Microsoft Office 365

Pour utiliser BlackBerry Gatekeeping Service avec Microsoft Office 365, vous devez configurer la stratégie d'accès des terminaux mobiles dans Microsoft Office 365 pour la mise en quarantaine de terminaux par défaut.

Avant de commencer : Configuration des autorisations à des fins de contrôle d'accès.

Si le niveau d'accès par défaut de votre organisation à Exchange ActiveSync est défini sur Autoriser et que vos uti lisateurs sont configurés et synchronisent leurs terminaux avec succès, vous devez vous assurer que ces utilisate urs ont une dispense personnelle ou une règle de terminal associée à leur compte d'utilisateur ou à leur terminal a vant de définir le niveau d'accès par défaut sur Quarantaine. Si ce n'est pas le cas, ils sont mis en quarantaine et le urs terminaux ne se synchronisent pas tant qu'ils n'y sont pas autorisés par BlackBerry UEM.

Pour plus d'informations sur la définition du niveau d'accès par défaut à Exchange ActiveSync pour la mise en qua rantaine, consultez http://support.blackberry.com/kb pour lire l'article KB33531.

1. Connectez-vous au portail d'administration de Microsoft Office 365
2. Dans le menu latéral, cliquez sur **Admin**.
3. Cliquez sur **Exchange**.
4. Dans la section **Mobile**, cliquez sur **accès des terminaux mobiles**.
5. Cliquez sur **Modifier**.
6. Cliquez sur **Quarantaine - Me laisser décider de bloquer ou d'autoriser plus tard**.

À la fin : Configurer les autorisations Microsoft IIS à des fins de contrôle d'accès.

Configurer les autorisations Microsoft IIS à des fins de contrôle d'accès

BlackBerry UEM utilise les commandes Windows PowerShell pour gérer la liste des terminaux autorisés. Pour utiliser BlackBerry Gatekeeping Service, vous devez configurer les autorisations Microsoft IIS. Procédez comme suit sur l'ordinateur qui héberge le rôle de serveur d'accès client Microsoft.

Avant de commencer : Autorisez uniquement les terminaux approuvés à accéder à Exchange ActiveSync ..

1. Ouvrez Microsoft Internet Information Services (IIS) Manager.
2. Dans le volet de gauche, développez le serveur.
3. Développez **Sites** > **Site Web par défaut**.
4. Cliquez avec le bouton droit sur le dossier PowerShell. Sélectionnez **Modifier les autorisations**.
5. Cliquez sur l'onglet **Sécurité**. Cliquez sur **Modifier**.
6. Cliquez sur **Ajouter** et saisissez le <nouveau_groupe> créé lors de la configuration des autorisations Microsoft Exchange à des fins de contrôle d'accès.
7. Cliquez sur **OK**.
8. Vérifiez que les paramètres **Lecture et exécution**, **Affichage du contenu du dossier** et **Lecture** sont sélectionnés. Cliquez sur **OK**.
9. Sélectionnez le dossier **PowerShell**. Double-cliquez sur l'icône **Authentification**.
10. Sélectionnez **Authentification Windows**. Cliquez sur **Activer**.
11. Fermez Microsoft Internet Information Services (IIS) Manager.

À la fin : Création d'une configuration de contrôle d'accès.

Création d'une configuration de contrôle d'accès

Vous pouvez créer une configuration de contrôle d'accès permettant aux terminaux conformes aux stratégies de sécurité de votre entreprise de se connecter à Microsoft Exchange Server ou Microsoft Office 365.

Avant de commencer :

- Configuration des autorisations à des fins de contrôle d'accès.
- Autorisez uniquement les terminaux approuvés à accéder à Exchange ActiveSync ..
- Configurer les autorisations Microsoft IIS à des fins de contrôle d'accès.

1. Sur la barre de menus, cliquez sur **Paramètres > Intégration externe > Service de contrôle Microsoft Exchange**.
2. Dans la section de la liste de Microsoft Exchange Server, cliquez sur +.
3. Dans le champ **Nom du serveur**, saisissez le nom de l'environnement Microsoft Exchange Server ou Microsoft Office 365 dont vous souhaitez gérer l'accès.

4. Saisissez le nom d'utilisateur et le mot de passe du compte que vous avez créé pour gérer le contrôle d'accès de Exchange ActiveSync.
5. Dans la liste déroulante **Type d'authentification**, sélectionnez le type d'authentification utilisé pour Microsoft Exchange Server ou Microsoft Office 365.
6. Pour activer l'authentification SSL entre BlackBerry UEM et Microsoft Exchange Server ou Microsoft Office 365, cochez la case **Utiliser SSL**. Vous pouvez également sélectionner d'autres contrôles de certificats.
7. Dans la liste déroulante **Type de proxy**, sélectionnez le type de configuration proxy utilisé entre BlackBerry UEM et Microsoft Exchange Server ou Microsoft Office 365, le cas échéant.
8. Si vous avez sélectionné une configuration proxy à l'étape précédente, sélectionnez le type d'authentification utilisé sur le serveur proxy.
9. Si nécessaire, sélectionnez **Authentification requise** et saisissez le nom d'utilisateur et le mot de passe.
10. Cliquez sur **Test de connexion** pour vérifier que la connexion a abouti.
11. Cliquez sur **Enregistrer**.
12. Dans la section **Liste des clients e-mail Android for Work**, cliquez sur +.

Remarque : BlackBerry Hub + Services est ajouté à la liste par défaut.

13. Sélectionnez une application de messagerie et cliquez sur **Suivant**.
14. Dans la liste déroulante **ID du terminal**, sélectionnez le champ de la configuration d'application qui correspond à l'identifiant du terminal.
15. Dans la liste déroulante **Adresse électronique**, sélectionnez le champ de la configuration d'application qui correspond à l'adresse électronique de l'utilisateur.

À la fin :

- Créez un profil de contrôle d'accès et attribuez-le aux comptes d'utilisateurs, aux groupes d'utilisateurs ou aux groupes de terminaux. Reportez-vous aux sections « Création d'un profil de contrôle d'accès » dans le contenu relatif à l'administration..
- Si vous avez configuré un groupe de serveurs avec une ou plusieurs instances actives de BlackBerry Gatekeeping Service, associez le profil de contrôle d'accès au groupe de serveurs approprié. Tout utilisateur auquel est attribué ce profil de contrôle d'accès peut utiliser n'importe quelle instance active de BlackBerry Gatekeeping Service dans ce groupe de serveurs.

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 déploy er des applications iOS et Android gérées par Microsoft Intune ou si vous souhaitez gérer des applications Windo ws 10 dans BlackBerry UEM.

BlackBerry UEM prend en charge la configuration d'un seul locataire Azure. Pour connecter BlackBerry UEM à Azu re, vous effectuez les actions suivantes:

Step	Action
1	Créer un compte Microsoft Azure.
2	Synchroniser Microsoft Active Directory avec Microsoft Azure.
3	Create an enterprise endpoint in Azure.
4	Configurer BlackBerry UEM pour une synchronisation de avec Microsoft Intune et Windows Store for Business.

Créer un compte Microsoft Azure

To deploy apps protected by Microsoft Intune to iOS and Android devices or manage Windows 10 apps in BlackBe rry UEM, you must have a Microsoft Azure account and authenticate BlackBerry UEM with Azure.

Complete this task if your organization doesn't have a Microsoft Azure account.

1. Go to https://azure.microsoft.com and click **Free account**, then follow the prompts to create the account.
   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 no m 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 p rotégées par Microsoft Intune à des terminaux iOS et Android , les utilisateurs doivent exister dans Microsoft Azur eActive Directory. Vous devez synchroniser les utilisateurs et groupes entre vos locaux Active Directory et AzureA ctive Directory à l'aide de Microsoft Azure Active Directory Connect. Pour plus d'informations, accédez à https://d ocs.microsoft.com/fr-fr/azure/active-directory/connect/active-directory-aadconnect.

Avant de commencer : Créer un compte Microsoft Azure

1. Téléchargez Azure AD Connect à l'adresse http://www.microsoft.com/en-us/download/details.aspx?id=47594.

2. Installez le logiciel Azure AD Connect.
3. Configurez Azure AD Connect pour connecter votre instance Active Directory sur site avec AzureActive Directory.

À la fin : Create an enterprise endpoint in Azure

Create an enterprise endpoint in Azure

To provide BlackBerry UEM access to Microsoft Azure, you must create an enterprise endpoint within Azure. The enterprise endpoint allows BlackBerry UEM to authenticate with Microsoft Azure. For more information, see https://docs.microsoft.com/en-us/azure/active-directory/active-directory-app-registration.

If you are connecting BlackBerry UEM to both Microsoft Intune and the Windows Store for Business, use a different enterprise application for each purpose due to differences in permissions and potential future changes.

Avant de commencer : Synchroniser Microsoft Active Directory avec Microsoft Azure

1. Connectez-vous à Azure portal.
2. Aller a **Microsoft Azure > Azure Active Directory > App registrations**.
3. Cliquez **Endpoints**.
4. Copiez le **OAUTH 2.0 TOKEN ENDPOINT** valorisez et collez-le dans un fichier texte.
   C'est le **OAUTH 2.0 token endpoint** requis dans BlackBerry UEM.
5. Fermer la **Endpoints** listez et selectionnez **New application registration**.
6. Entrez les informations suivantes pour votre application:

Field	Setting
Name	<A name for your application>
Application type	Web app / API
Sign-on URL	Any valid URL **Remarque :** If you don't have a registered domain you can use: http://localhost/

7. Cliquez **Create**.
8. Cliquez sur l'application que vous venez de créer.
9. Copiez le **Application ID** de votre application et collez-la dans un fichier texte.
   C'est la **Client ID** requis dans BlackBerry UEM.
10. Si vous créez l'application pour utiliser Microsoft Intune, cliquez sur **Autorisations requises** dans le menu **Paramètres**. Procédez comme suit :
    a) Cliquez **Add**.
    b) Cliquez **Select an API**.
    c) Selectionner **Microsoft Graph**.
    d) Cliquez **Select**.
    e) Faites défiler vers le bas dans la liste des autorisations et sous **Delegated Permissions**, Définissez les autorisations suivantes pour Microsoft Intune:
       - Lire et écrire Microsoft Intune applications (prévisualisation)
       - Lire le profil de base de tous les utilisateurs

- Lire tous les groupes

f) Cliquez **Select**.
g) Cliquez **Done**.
h) Dans le volet **Autorisations requises**, cliquez sur **Octroyer des autorisations**.

Remarque : You must be a global administrator to grant permissions.

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

Vous pouvez utiliser les autorisations par défaut si vous créez l'application pour vous connecter à Windows St ore for Business.

11. Selectionner **Keys** dans le **Settings** menu. Procédez comme suit:

a) Entrez un nom pour votre clé.
b) Sélectionnez une durée pour votre clé.
c) Cliquez **Save**.
d) Copiez la valeur de votre clé.

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 no uvelle clé, car la valeur ne s'affiche pas après avoir quitté cet écran.

À la fin : Configurer BlackBerry UEM pour la synchronisation avec Microsoft Intune or Configurer BlackBerry UEM pour une synchronisation avec Windows Store for Business.

Configurer BlackBerry UEM pour la synchronisation avec Microsoft In tune

Microsoft Intune est un service EMM cloud qui fournit des fonctions MDM et MAM. Intune MAM fournit des foncti ons de sécurité pour les applications, notamment les applications Office 365, qui protègent les données que conti ennent les applications. Par exemple, Intune peut exiger que les données contenues dans les applications soient c hiffrées et empêcher le copier-coller, l'impression et l'utilisation de la commande Enregistrer sous.

Après avoir connecté BlackBerry UEM à Microsoft Intune, vous pouvez utiliser la console de gestion UEM pour cré er des profils de protection des applications Microsoft Intune comme décrit dans le contenu relatif à l'administrat ion .

Before you configure BlackBerry UEM to synchronize with Microsoft Intune, you must connect BlackBerry UEM to Microsoft Azure.

Configurer BlackBerry UEM pour la synchronisation avec Microsoft Intune

Avant de commencer : Create an enterprise endpoint in Azure

1. Connectez-vous à la console de gestion BlackBerry UEM.
2. Accédez à **Paramètres > Intégration externe > Microsoft Intune**.
3. Entrez les informations que vous avez copiées à partir du portail Azure lorsque vous avez créé l'application d'e ntreprise dans Azure.

- **ID client** : ID d'application généré par l'enregistrement d'application Azure
- **Clé client** : secret de client généré par l'enregistrement d'application Azure
- **Point de terminaison du jeton OAUTH 2.0** : URL de point de terminaison OAuth spécifique au domaine pour demander des jetons d'authentification

- **Username**: The administrator account that BlackBerry UEM uses to access Intune. Visit https://support.blackberry.com/kb to read article 50341 for information on the permissions required for the Intune administrator account.
- **Password**: The password for the Intune administrator account

4. Cliquez sur **Suivant**.

À la fin : Créer un profil de protection de l'application Microsoft Intune

Configuration de BlackBerry UEM pour la synchronisation avec Windows Store for Business

Si vous souhaitez gérer des applications Windows 10, vous devez configurer BlackBerry UEM pour qu'il se synchronise avec Windows Store for Business avant de pouvoir ajouter des applications Windows 10 à la liste d'applications.

Si vous supprimez ultérieurement la connexion à Windows Store for Business, toutes les applications Windows 10 qui ont été synchronisées avec BlackBerry UEM seront supprimées et les applications seront désattribuées des utilisateurs et des groupes.

Configuration de BlackBerry UEM pour une synchronisation avec Windows Store for Business, vous effectuez les opérations suivantes :

Étape	Action
1	Créer un compte Microsoft Azure.
2	Synchroniser Microsoft Active Directory avec Microsoft Azure.
3	Create an enterprise endpoint in Azure.
4	Configurer BlackBerry UEM pour une synchronisation avec Windows Store for Business.
5	Créer un administrateur pour Windows Store pour Entreprises.

Configurer BlackBerry UEM pour une synchronisation avec Windows Store for Business

Avant de commencer : Créer un compte Microsoft Azure.

1. Connectez-vous à la console de gestion BlackBerry UEM.
2. Accédez à **Paramètres > Gestion de l'application > Applications Windows 10**.
3. Entrez les informations que vous avez copiées à partir du portail Azure lorsque vous avez créé l'application d'entreprise dans Azure.
   - **ID client** : ID d'application généré par l'enregistrement d'application Azure
   - **Clé client** : secret de client généré par l'enregistrement d'application Azure

- **Point de terminaison du jeton OAUTH 2.0** : URL de point de terminaison OAuth spécifique au domaine pour demander des jetons d'authentification
- **Nom d'utilisateur** : nom d'utilisateur de l'administrateur pour BlackBerry UEM afin d'accéder à Intune
- **Mot de passe** : mot de passe du nom d'utilisateur

4. Cliquez sur **Suivant**.

À la fin : Créer un administrateur pour Windows Store pour Entreprises.

Créer un administrateur pour Windows Store pour Entreprises

Pour gérer les applications Windows 10 sur des terminaux, vous devez créer un catalogue d'applications dans Win dows Store pour Entreprises et synchroniser les applications avec BlackBerry UEM. Pour créer ce catalogue dans Windows Store pour Entreprises, vous devez créer au moins un compte administrateur pour vous connecter au m agasin.

Avant de commencer :

- Créer un compte Microsoft Azure.
- Create an enterprise endpoint in Azure.
- Configurer BlackBerry UEM pour une synchronisation avec Windows Store for Business.

1. Sur le portail Microsoft Azure, accédez à **Microsoft Azure > Azure Active Directory > Utilisateurs et groupes > Tous les utilisateurs**.
2. Cliquez sur **Ajouter un utilisateur**.
3. Sur l'écran, entrez les informations de l'utilisateur requises.
4. Cliquez sur la flèche en regard de **Rôle de répertoire** et sélectionnez **Administrateur général**, puis cliquez sur **O K**.
5. Créez un mot de passe ou sélectionnez **Afficher le mot de passe** et copiez le mot de passe généré.
6. Cliquez sur **Créer**.
7. Cliquez sur **Azure Active Directory > Applications d'entreprise > Toutes les applications** et sélectionnez l'appl ication d'entreprise que vous avez créée.
8. Ajoutez le compte administrateur général que vous avez créé en tant qu'utilisateur de l'application.

Activez l'application dans Windows Store for Business

Avant de commencer :

- Configurer BlackBerry UEM pour une synchronisation avec Windows Store for Business.
- Créer un administrateur pour Windows Store pour Entreprises

1. Connectez-vous à Windows Store for Business à l'aide du compte d'administrateur général que vous avez créé.
2. Cliquez sur **Paramètres** > **Outil de gestion**.
3. Choisissez l'application créée pour faire office d'outil MDM à synchroniser avec Windows Store for Business.
4. Cliquez sur **Activer**.

Configurer BlackBerry UEM pour la prise en charge des terminaux Android qui possèdent un profil professionnel

Les terminaux Android ayant un profil professionnel offrent une sécurité supplémentaire aux entreprises qui souhaitent gérer les terminaux Android. Pour plus d'informations sur les terminaux Android ayant un profil professionnel, rendez-vous sur https://support.google.com/work/android/.

Remarque : Vous pouvez utiliser des stratégies d'applications pour configurer l'application Gmail. Toutefois, vous devez utiliser un type d'activation Travail et Personnel ou Travail seulement et non le mode MDM pour activer le terminal.

Il existe deux façons de configurer BlackBerry UEM pour qu'il prenne en charge les terminaux Android dotés d'un profil professionnel :

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. Autorisez BlackBerry UEM à gérer des terminaux Android qui ont des comptes de profil professionnel (maintenant appelés 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 résume les différentes options de configuration des terminaux Android dotés d'un profil professionnel :

Méthode de configuration de BlackBerry UEM pour la prise en charge des terminaux Android qui possèdent un profil professionnel	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.
Connectez 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 la prise en charge des terminaux Android qui possèdent un profil professionnel	Quand choisir cette méthode	Type de compte d'utilisateur	Services Google pris en charge
Autoriser BlackBerry UEM à gérer des terminaux Android qui ont des comptes de profil professionnel (maintenant appelés comptes gérés Google Play)	• Vous ne disposez pas de domaine Google dans votre entreprise • Vous disposez d'un domaine Google déjà connecté à un domaine BlackBerry UEM et vous souhaitez utiliser des terminaux Android dotés d'un profil professionnel sur un deuxième domaine BlackBerry UEM	Terminaux Android qui possèdent des comptes de profil professionnel	Prend en charge la gestion d'applications via Google Play. Les services Google ne sont pas pris en charge.

Configurez BlackBerry UEM pour prendre en charge les périphériques Android qui ont un profil de travail

Avant de commencer :

- BlackBerry UEM prend en charge les terminaux Android qui possèdent un profil professionnel et qui exécutent Android 5.1 et versions ultérieures.
- Si vous configurez BlackBerry UEM pour prendre en charge les appareils Android disposant d'un profil professionnel utilisant l'option Comptes Google Play, l'activation des appareils avec un type d'activation «Espace de travail uniquement» est prise en charge uniquement sur les appareils fonctionnant sous Android 6.0 et versions ultérieures.
- 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. Voir Supprimez la connexion au profil de travail Android à votre domaine Google.

1. Dans la barre de menus, cliquez sur **Paramètres > Intégration externe > Connexion à un domaine Google**.
2. Effectuez l'une des tâches suivantes :

Tâche	Étapes
Utiliser un domaine Google	**a.** Sélectionnez **Connecter BlackBerry UEM à votre domaine Google e xistant**. **b.** Cliquez sur **Suivant**. **c.** Renseignez les champs pour créer un compte de service et cliquez sur **Suivant**. Pour obtenir des instructions pas à pas, rendez-vous s ur le site http://support.blackberry.com/kb et lisez l'article 0000377 48.
Utilisez des terminaux Android qu i possèdent des comptes de profi l professionnel	**a.** Sélectionnez **Autoriser BlackBerry UEM à gérer les comptes Andro id for Work**. **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. L e 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 d e gestion BlackBerry UEM.

3. Lorsque vous êtes invité, cliquez sur **Accepter** pour accepter les autorisations définies pour certaines ou toutes les applications suivantes:

- Google Chrome
- BlackBerry Connectivity
- Services BlackBerry Hub +
- BlackBerry Hub
- BlackBerry Calendrier
- Contacts par BlackBerry
- Notes par BlackBerry
- Tâches par BlackBerry

4. Cliquez sur **Terminé**.

À la fin : Complétez les étapes pour activer les périphériques Android qui ont un profil de travail. Pour plus d'info rmations sur l'activation de l'appareil, see "Device activation" in the Administration content.

Supprimez la connexion au profil de travail Android à votre domaine G oogle

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

Supprimez la connexion au profil de travail Android avant de terminer l'une des tâches suivantes:

- Désinstaller une instance de BlackBerry UEM
- Revenez à un instantané de machine virtuelle que vous avez créé avant d'établir la connexion au profil de tr avail Android
- Connectez une autre instance BlackBerry UEM à votre domaine Google Cloud ou G Suite

Si vous ne supprimez pas la connexion au profil de travail Android, il est possible que vous ne puissiez pas con necter votre domaine Google Cloud ou G Suite à une nouvelle instance de BlackBerry UEM. Lorsque vous sup primez la connexion au profil de travail Android dans BlackBerry UEM, vous désactivez également tous les périphé riques activés avec un type d'activation de profil de travail Android.

1. Dans la barre de menus, cliquez sur **Paramètres > Intégration externe**.
2. Cliquez sur **Google domain connection**.
3. Cliquez sur **Remove connection**.
4. Cliquez sur **Supprimer**.

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

Si vous avez configuré BlackBerry UEM pour prendre en charge les terminaux Android disposant d'un profil profes sionnel, vous pouvez supprimer la connexion dans Google.

1. À l'aide du compte Google que vous avez utilisé pour configurer les terminaux Android disposant d'un profil pr ofessionnel , connectez-vous à https://play.google.com/work.
2. Cliquez sur **Paramètres d'administration**.

3. Dans la section **Informations d'entreprise**, 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 **Google domain connection**.
8. Cliquez sur **Tester la connexion.**
9. Cliquez sur **Remove connection**.
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 G oogle que vous utilisez pour gérer les périphériques Android qui ont un profil de travail ou pour tester la connexion au domaine Google. Lorsque vous modifiez ou testez la connexion, les périphériques déjà activés ne sont pa s affectés.

1. Dans la barre de menus, cliquez sur **Paramètres > Intégration externe**.
2. Cliquez sur **Google domain connection**.
3. Cliquez sur  .
4. Effectuez l'une des tâches suivantes :

   - Cliquez sur **Testez la connexion** pour voir l'état actuel de la connexion.
   - Sélectionnez le type de domaine pour gérer les périphériques Android qui ont un profil de travail et cliqu ez sur **Enregistrer**..

Ajouter une licence E-FOTA

Vous pouvez utiliser E-FOTA (Enterprise Firmware Over the Air) pour contrôler quand les mises à jour du micrologiciel de Samsung sont installées sur les terminaux Samsung KNOX. Le contrôle des versions du micrologiciel garantit que les terminaux des utilisateurs utilisent des versions du micrologiciel prises en charge par leurs applications et conformes aux stratégies de votre entreprise.

Before you can create a device SR requirements profile to control firmware versions, you must add an E-FOTA license in UEM.

1. Sur la barre de menus, cliquez sur **Gestion des licences** > **Résumé des licences**.
2. Dans la section **E-FOTA**, cliquez sur **Ajouter une licence**.
3. In the **Add an E-FOTA license** dialog box, enter the name, client ID, client secret, customer ID, and license key.
4. Cliquez sur **Enregistrer**.

À la fin : Créer un profil de configuration logicielle minimale requise du terminal pour les terminaux Android.

Gestion de l'attestation des terminaux Samsung KNOX

Lorsque vous activez l'attestation, BlackBerry UEM vérifie l'authenticité et l'intégrité des terminaux Samsung KNO X activés avec les types d'activation suivants :

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

1. Dans la barre de menus, cliquez sur **Paramètres > Paramètres généraux > Attestation**.
2. Pour activer l'attestation pour les terminaux Samsung KNOX, sélectionnez **Activer les vérifications d'attestatio n périodiques pour les terminaux KNOX Workspace**.
3. Dans la section **Fréquence des vérifications**, spécifiez la fréquence, en jours ou en heures, à laquelle le termina l doit renvoyer une réponse d'attestation à BlackBerry UEM.
4. Dans la section **Période de grâce**, spécifiez une période de grâce en heures ou en jours. Après l'expiration du d élai de grâce sans réponse d'attestation, un terminal est considéré comme non conforme et le terminal est sou mis aux conditions spécifiées dans le profil de conformité attribué à l'utilisateur. Autre élément à prendre en co mpte : si le terminal d'un utilisateur est en dehors de la zone de couverture, éteint ou a une batterie déchargée, celui-ci ne pourra pas répondre aux défis d'attestation que BlackBerry UEM envoie et BlackBerry UEM considèr era le terminal comme non conforme. Si vous avez défini la politique de conformité de votre organisation pour effacer le terminal lorsqu'il n'est pas conforme, lorsque le terminal ne répond pas avant l'expiration du délai de grâce, les données du terminal seront supprimées.
5. Cliquez sur **Enregistrer**.

À la fin : Créez un profil de conformité définissant les actions prises si un terminal est considéré comme débridé. Pour obtenir des instructions, reportez-vous à la section Application des règles de conformité aux terminaux du c ontenu relatif à l'administration de BlackBerry UEM.

Gestion de l'attestation des terminaux Windows 10

Lorsque vous activez l'attestation, BlackBerry UEM vérifie l'authenticité et l'intégrité des terminaux Windows 10. L e terminal communique avec le service d'attestation d'intégrité de Microsoft pour vérifier la conformité en fonctio n des paramètres définis dans le profil de conformité de votre entreprise.

1. Dans la barre de menus, cliquez sur **Paramètres > Paramètres généraux > Attestation**.
2. Pour activer l'attestation pour les terminaux Windows 10, sélectionnez **Activer les vérifications d'attestation p ériodiques pour les terminaux Windows 10**.
3. Dans la section **Fréquence des vérifications**, spécifiez la fréquence, en jours ou en heures, à laquelle le termina l doit renvoyer une réponse d'attestation à BlackBerry UEM.
4. Dans la section **Période de grâce**, spécifiez une période de grâce en heures ou en jours. Lorsque la période de grâce expire, un terminal est considéré comme débridé et soumis aux conditions spécifiées dans le profil de c onformité attribué à l'utilisateur.
5. Cliquez sur **Enregistrer**.

Vous pouvez afficher les violations de conformité sur la page des détails du terminal.

À la fin :

Créez un profil de conformité définissant les actions prises si un terminal est considéré comme débridé. Pour obt enir des instructions, reportez-vous à la section Application des règles de conformité aux terminaux du Contenu re latif à l'administration BlackBerry UEM.

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

Vous devez configurer BlackBerry UEM pour qu'il utilise le programme d'inscription des appareils 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.

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. Click +.
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. Click +.
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. Click +.
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 où 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 termina ux que vous enregistrez dans le programme d'inscription des terminaux d'Apple, cochez la case Attribuer a utomatiquement cette configuration à tous les nouveaux terminaux.
- Si vous souhaitez utiliser la console de BlackBerry UEM pour attribuer automatiquement la configuration d' inscription aux terminaux concernés, ne cochez pas la case Attribuer automatiquement cette configuration à tous les nouveaux terminaux.

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 du terminal**, cochez les cases suivantes :

   - Autoriser le couplage : cette option permet aux utilisateurs de coupler le terminal à un ordinateur.
   - Activer le mode supervisé : cette option permet d'activer le mode supervisé des terminaux. Vous devez séle ctionner au moins l'une des deux options suivantes : Activer le mode supervisé ou Autoriser la suppression du profil MDM.
   - Obligatoire : cette option permet aux utilisateurs d'activer les terminaux avec le nom d'utilisateur et le mot d e passe du répertoire de leur entreprise.
   - Autoriser la suppression du profil MDM : cette option permet aux utilisateurs de désactiver les terminaux. V ous devez sélectionner au moins l'une des deux options suivantes : Activer le mode supervisé ou Autoriser l a suppression du profil MDM.
   - Veuillez patienter pendant la configuration du terminal : cette option empêche les utilisateurs d'annuler la c onfiguration des terminaux tant que l'activation avec BlackBerry UEM n'est pas terminée. Ce paramètre n'es t disponible que si vous sélectionnez l'option Activer le mode supervisé.

5. Dans la section **Ignorer pendant la configuration**, sélectionnez les éléments que vous ne souhaitez pas inclure dans la configuration des terminaux :

   - Mot de passe : avec cette option, les utilisateurs ne sont pas invités à créer un mot de passe pour le termin al.
   - 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 sauvegard e.
   - Déplacer depuis Android : cette option vous empêche de restaurer les données à partir d'un terminal Andro id.
   - ID Apple : cette option empêche les utilisateurs de se connecter avec leur identifiant Apple et iCloud.
   - Conditions générales : cette option permet de masquer les conditions générales de iOS.
   - Siri : cette option permet de désactiver Siri sur les terminaux.
   - Diagnostics : cette option bloque l'envoi automatique des informations de diagnostic au terminal pendant l a 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

6. Cliquez sur **Enregistrer**.

   Si le message « Une erreur est survenue. Impossible de décrypter le fichier de jeton du serveur. » s'affiche, rend ez-vous sur http://support.blackberry.com/kb et consultez l'article 37282.
7. Si vous avez sélectionné "Attribuer automatiquement de nouveaux terminaux à cette configuration", cliquez su r **Oui**.

À la fin : Activez les terminaux iOS. Pour plus d'informations sur l'activation des terminaux inscrits dans le Progra mme d’inscription des terminaux, reportez-vous au 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. Po ur afficher l'état actuel du jeton, reportez-vous à la date d'expiration dans la fenêtre du programme d'inscription de s 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 du compte d'utilisateur.
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 Ap ple**, cliquez sur **Ouvrez le portail du programme d'inscription des appareils 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 ter minaux iOS dans le programme d'inscription des terminaux 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 config urations d'inscription attribuées aux terminaux. La suppression de la connexion n'affecte pas les terminau x actifs sur BlackBerry UEM.

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

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

Configuration de BlackBerry UEM Self-Service pour les utilisateurs

BlackBerry UEM Self-Service est une application Web que vous pouvez mettre à la disposition des utilisateurs pour leur permettre d'effectuer des tâches de gestion telles que la création de mots de passe d'activation, le verrouillage à distance de leurs terminaux ou la suppression des données de leurs terminaux. Les utilisateurs n'ont aucun logiciel à installer pour utiliser BlackBerry UEM Self-Service. L'adresse Web et les informations de connexion doivent être fournies aux utilisateurs par vos soins.

Vous pouvez contraindre les utilisateurs à lire et accepter un avis avant de se connecter àBlackBerry UEM Self-Service. Pour plus d'informations sur cet avis, reportez-vous à la section« Créer un avis de connexion pour les consoles » dans le contenu relatif à l'administration.

Configurer BlackBerry UEM Self-Service

Set up BlackBerry UEM Self-Service so that users can log in and perform some self-service tasks.

1. Dans la barre de menus, cliquez sur **Paramètres > Self-Service**.
2. Cliquez sur **Paramètres Self-Service**.
3. Vérifiez que l'option **Autoriser les utilisateurs à accéder à la console en libre-service** est sélectionnée.
4. Spécifiez le nombre de minutes, d'heures ou de jours pendant lesquels l'utilisateur est autorisé à activer un terminal avant que son mot de passe d'activation expire.
5. Spécifiez le nombre minimum de caractères requis dans le mot de passe d'activation.
6. Dans la liste déroulante **Complexité minimale des mots de passe**, sélectionnez le niveau de complexité requis pour les mots de passe d'activation.
7. Pour envoyer automatiquement un e-mail d'activation aux utilisateurs lorsqu'ils créent un mot de passe d'activation dans BlackBerry UEM Self-Service, cochez la case **Envoyer un e-mail d'activation** . Vous pouvez utiliser le modèle d'e-mail d'activation par défaut ou sélectionner un autre modèle dans la liste déroulante.
8. To send a login notification email to the user each time they log in to BlackBerry UEM Self-Service, select the **Send self-service login notification** check box.
9. Cliquez sur **Enregistrer**.

À la fin : fournissez l'adresse Web et les informations de connexion à BlackBerry UEM Self-Service aux utilisateurs.

Configuration de la haute disponibilité pour un domaine BlackBerry UEM

BlackBerry UEM utilise un modèle haute disponibilité actif-actif afin de réduire les risques d'interruptions de service pour les utilisateurs des terminaux. Pour configurer la haute disponibilité, vous devez installer plusieurs instances de BlackBerry UEM, chacune sur un ordinateur distinct. Chaque instance se connecte à la base de données BlackBerry UEM et gère activement les comptes d'utilisateur et les terminaux.

Dans BlackBerry UEM, la haute disponibilité comprend les fonctionnalités suivantes :

Fonctionnalité	Description
Déplacer automatiquement les terminaux BlackBerry 10 vers une instance saine de BlackBerry UEM	Si les terminaux BlackBerry 10 d'une instance de BlackBerry UEM ne parviennent pas à se connecter aux ressources professionnelles via la connectivité d'entreprise, ces terminaux sont réattribués à des instances saines de BlackBerry UEM. Les terminaux BlackBerry 10 peuvent utiliser la connectivité d'entreprise pour accéder aux données de messagerie et de calendrier, au navigateur professionnel et au réseau de l'entreprise. La plupart des tâches de gestion (comme l'attribution de profils) requièrent une connectivité d'entreprise.
Les terminaux iOS, Android et Windows peuvent se connecter à n'importe quelle instance de BlackBerry UEM	En cas de problème d'intégrité sur une ou plusieurs instances de BlackBerry UEM, les terminaux iOS, Android et les terminaux Windows se connectent à l'une des instances saines. Aucune interruption de service n'est donc à déplorer pour les terminaux.
Basculement de BlackBerry Affinity Manager	BlackBerry Affinity Manager attribue les terminaux BlackBerry 10 à une instance de BlackBerry UEM, analyse la connectivité d'entreprise de chaque instance et déplace les utilisateurs BlackBerry 10 en cas de problèmes de connectivité d'entreprise. BlackBerry Affinity Manager ne peut pas attribuer de terminaux iOS, Android ou Windows à une instance BlackBerry UEM spécifique. Une seule instance de BlackBerry Affinity Manager est active. Les autres instances de BlackBerry Affinity Manager sont des instances de secours. En cas de problème sur l'instance active de BlackBerry Affinity Manager, chacune des instances de secours lance un processus pour déterminer laquelle d'entre elles doit devenir l'instance active. L'instance qui termine le processus en premier devient l'instance active de BlackBerry Affinity Manager.
Gérer les terminaux à partir de n'importe quelle instance de BlackBerry UEM	En cas de problème au niveau de la console de gestion ou de BlackBerry UEM Core sur une instance de BlackBerry UEM, vous pouvez continuer à gérer n'importe quel terminal (BlackBerry 10, iOS, Android et Windows) à l'aide de la console de gestion et de l'instance de BlackBerry UEM Core d'une instance saine.
Pool DNS Round Robin pour la console de gestion	Vous pouvez utiliser des logiciels tiers pour configurer un pool DNS Round Robin qui se connecte à la console de gestion de chaque instance de BlackBerry UEM. En cas de problème au niveau d'une console, le pool vous permettra de vous connecter à une console qui fonctionne.

Fonctionnalité	Description
BlackBerry Connectivity Node	Vous pouvez installer une ou plusieurs instances de BlackBerry Connectivity Node pour ajouter des instances supplémentaires de composants de connectivité de terminal au domaine de votre organisation. Vous pouvez également créer des groupes de serveurs pour spécifier des chemins de données locaux pour la connectivité sécurisée et pour configurer la haute disponibilité pour les composants de BlackBerry Connectivity Node. Pour plus d'informations, reportez-vous à Haute disponibilité et BlackBerry Connectivity Node.

Lorsque BlackBerry UEM effectue une action de récupération, les utilisateurs concernés sont confrontés à une brève interruption de service. La durée de cette interruption dépend de différents facteurs, comme le nombre de terminaux BlackBerry 10 et le nombre d'instances de BlackBerry UEM. Lorsque des utilisateurs BlackBerry 10 sont réattribués à une autre instance, le délai d'interruption moyen est de 3 minutes. Lorsqu'un basculement de BlackBerry Affinity Manager intervient, le délai d'interruption moyen est de 10 minutes.

Haute disponibilité pour les composants qui gèrent des terminaux BlackBerry OS

Si vous avez configuré la haute disponibilité pour BES5 avant la mise à niveau de BES5 vers BlackBerry UEM, la configuration continue à fonctionner à l'issue de la mise à niveau. La configuration de la haute disponibilité s'applique uniquement aux composants qui gèrent des terminaux BlackBerry OS.

Pour en savoir plus sur la configuration de la haute disponibilité pour les composants qui gèrent des terminaux BlackBerry OS, rendez-vous sur la page help.blackberry.com/detectLang/category/enterprise-services et consultez le *Guide d'administration de BlackBerry Enterprise Server 5*.

Architecture : haute disponibilité pour BlackBerry UEM

Le schéma suivant illustre un domaine haute disponibilité composé de deux instances deBlackBerry UEM. Vous pouvez installer autant d'instances deBlackBerry UEMque vous le souhaitez. Cette rubrique explique comment certains composants sont impliqués dans une configuration à haute disponibilité. Pour en savoir plus sur l'architecture et les composants deBlackBerry UEM,consultez le contenu relatif à l'architecture.

Composants	Description
Base de données BlackBerry UEM	Chaque instance de BlackBerry UEM se connecte à la base de données BlackBerry UEM pour accéder aux données des utilisateurs et des terminaux.

Composants	Description
Console de gestion et BlackBerry UEM Core	Vous pouvez utiliser n'importe quelle console de gestion pour gérer les comptes d'utilisateur et les terminaux du domaine. L'instance de BlackBerry UEM Core associée à cette console effectue les tâches de gestion. Vous pouvez configurer un pool DNS Round Robin qui se connecte à chaque console. En cas de problème au niveau de la console, le pool se connecte à une console qui fonctionne. Chaque instance gère la connectivité d'entreprise pour les terminaux BlackBerry 10 qui lui sont attribués par BlackBerry Affinity Manager. Toute instance saine peut effectuer des tâches de gestion sur tous types de terminaux.
BlackBerry MDS Connection Service et BlackBerry Dispatcher	Ces composants permettent aux terminaux BlackBerry 10 de se connecter aux ressources et de les utiliser.
BlackBerry Affinity Manager	BlackBerry Affinity Manager effectue les tâches suivantes : • Attribution des terminaux BlackBerry 10 aux instances de BlackBerry UEM • Connexion à BlackBerry Infrastructure • Configuration et démarrage du service BlackBerry Work Connect Notification Service actif • Contrôle de l'intégrité de BlackBerry MDS Connection Service et BlackBerry Dispatcher sur chaque instance afin d'analyser la connectivité d'entreprise Une seule instance de BlackBerry Affinity Manager est active (les autres sont des instances de secours). Si l'instance active détecte un problème de connectivité d'entreprise, elle réattribue les utilisateurs BlackBerry 10 aux instances saines de BlackBerry UEM. Chaque instance de secours de BlackBerry Affinity Manager analyse l'instance active de BlackBerry Affinity Manager. En cas de problème sur l'instance active de BlackBerry Affinity Manager, un basculement intervient et une des instances de secours devient active.

Équilibrer la charge des données des terminaux BlackBerry 10

If you install multiple instances of BlackBerry UEM in the same domain, data for BlackBerry 10 devices is load-balanced approximately equally across all healthy, running instances. For example, if you install three instances of BlackBerry UEM and the domain includes 3000 BlackBerry 10 devices, BlackBerry UEM assigns approximately 1000 devices to each of the three running instances.

BlackBerry UEM load-balances when the number of devices on a specific server is more than 500 devices above the average device count per server.

You cannot manually assign BlackBerry 10 devices to a specific instance. The BlackBerry Affinity Manager determines which instances manage BlackBerry 10 devices.

If an instance is temporarily unavailable, the remaining instances manage user and device data.

Each BlackBerry UEM instance uses the same SRP ID and connects to the same BlackBerry UEM database. The components on each instance are all running and actively managing data for all device types, except for the BlackB

erry Affinity Manager and BlackBerry Work Connect Notification Service. Only one instance of the BlackBerry Affinity Manager and the BlackBerry Work Connect Notification Service are active.

You can view the status of each instance in the management console.

Haute disponibilité et BlackBerry Connectivity Node

Vous pouvez installer une ou plusieurs instances de BlackBerry Connectivity Node pour ajouter des instances supplémentaires de composants de connectivité de terminal au domaine de votre organisation. Chaque BlackBerry Connectivity Node contient les composants BlackBerry UEM suivants : BlackBerry Secure Connect Plus, BlackBerry Gatekeeping Service, BlackBerry Secure Gateway, BlackBerry Proxy et BlackBerry Cloud Connector.

Chaque BlackBerry Connectivity Node fournit une nouvelle instance active de ces composants au domaine BlackBerry UEM qui peut traiter et gérer les connexions de terminaux sécurisées. Pour plus d'informations sur la planification et l'installation de BlackBerry Connectivity Node, reportez-vous au contenu relatif à la planification et au contenu relatif à l'installation et à la mise à niveau.

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

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

Comment BlackBerry UEM évalue-t-il l'intégrité des composants ?

Les composants BlackBerry UEM suivants possèdent des scores d'intégrité qui permettent de déterminer si une action de récupération est requise :

Composants	Intégrité analysée par	Facteurs associés au score d'intégrité	Action requise lorsque l'intégrité est inférieure au seuil
BlackBerry MDS Connection Service et BlackBerry Dispatcher (score d'intégrité agrégé)	Instance active de BlackBerry Affinity Manager	• Les composants sont-ils en cours d'exécution ? • Peuvent-ils se connecter à l'instance active de BlackBerry Affinity Manager ? • Peuvent-ils se connecter aux terminaux BlackBerry 10 ? • Peuvent-ils se connecter à la base de données ?	BlackBerry Affinity Manager déplace les terminaux BlackBerry 10 de l'instance BlackBerry UEM problématique vers les instances saines.

Composants	Intégrité analysée par	Facteurs associés au score d'intégrité	Action requise lorsque l'intégrité est inférieure au seuil
Instance active de BlackBerry Affinity Manager	Chaque instance de secours de BlackBerry Affinity Manager	• État de l'instance de BlackBerry Affinity Manager (instance active, instance de secours ou en lice pour devenir active) • Peut-elle se connecter à BlackBerry Dispatcher ? • Peut-elle recevoir des appels de BlackBerry UEM Core et de chaque instance de secours de BlackBerry Affinity Manager ? • Peut-elle se connecter à BlackBerry Infrastructure ? • Peut-elle se connecter et charger les paramètres de configuration de la base de données ?	Les instances de secours entament un processus de basculement et l'une d'elle devient l'instance active de BlackBerry Affinity Manager.

Installer une instance supplémentaire de BlackBerry UEM

Pour installer des instances supplémentaires deBlackBerry UEMet créer un domaine à haute disponibilité,consultez le contenu relatif à l'installation et à la mise à niveau. Vérifiez que l'ordinateur est conforme à la configuration requise pour installer une instance deBlackBerry UEM, puis effectuez les tâches pré-installation et post-installation nécessaires. Pour en savoir plus sur la compatibilité,consultez la Matrice de compatibilité.

Lorsque vous installez de nouvelles instances de BlackBerry UEM :

- Installez chaque instance sur un ordinateur distinct.
- Sur l'écran **Type d'installation** de l'application d'installation, sélectionnez **Utiliser un domaine existant**.
- Sur l'écran **Informations de la base de données**, spécifiez les informations de la base de données BlackBerry UEM que vous avez créée lors de l'installation de l'instance d'origine de BlackBerry UEM.

Une fois l'instance supplémentaire de BlackBerry UEM installée et les tâches post-installation terminées, la haute disponibilité active-active est disponible dans le domaine. La charge des données relatives aux utilisateurs et aux terminaux est équilibrée entre les instances de BlackBerry UEM, l'instance active de BlackBerry Affinity Manager analyse la connectivité d'entreprise de chaque instance, et les instances de secours de BlackBerry Affinity Manager analysent l'instance active pour déterminer si un basculement est nécessaire.

Configurer la haute disponibilité pour la console de gestion

Pour configurer la haute disponibilité pour les consoles de gestion BlackBerry UEM, vous pouvez utiliser l'équilibreur de charge matérielle ou le serveur DNS de votre organisation afin de configurer un pool Round Robin qui se connecte à chaque console de gestion du domaine. Si une console de gestion n'est pas disponible, l'équilibreur de charge ou le serveur DNS se connecte à l'une des autres consoles disponibles.

Pour plus d'informations sur la configuration d'un pool Round Robin, consultez la documentation de l'équilibreur de charge matérielle ou du serveur DNS de votre organisation.

Après la configuration d'un pool Round Robin, il est recommandé de mettre à jour les variables %AdminPortalURL% et %UserSelfServicePortalURL% de la console de gestion (Paramètres > Paramètres généraux > Variables par défaut) avec le nom du pool. Les e-mails qui utilisent ces variables pour se relier à la console de gestion et à BlackBerry UEM Self-Service pourront ainsi utiliser le pool Round Robin.

Si vous avez activé l'authentification unique, vous devez mettre à jour les SPN du compte Microsoft Active Directory avec le nom du pool et redémarrer les services BlackBerry UEM sur tous les ordinateurs qui hébergent une instance de BlackBerry UEM.

Une instance de la console de gestion de BlackBerry UEM dans le pool Round Robin peut se déconnecter du domaine BlackBerry UEM si le serveur DNS attribue une adresse IP différente à cette instance. L'instance est déconnectée parce que la nouvelle adresse IP ne reconnait pas les informations de connexion de l'utilisateur. Si cela se produit, l'utilisateur doit se déconnecter et se reconnecter.

Tâches connexes

Configurer la délégation contrainte pour permettre au compte Microsoft Active Directory de prendre en charge l'authentification unique

Configuration d'une base de données haute disponibilité à l'aide de la mise en miroir

Vous pouvez utiliser la mise en miroir pour configurer une base de données BlackBerry UEM haute disponibilité. L a mise en miroir de bases de données est une fonctionnalité Microsoft SQL Server qui vous permet de maintenir l e 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.

Remarque : dans la mesure où Microsoft envisage de supprimer la fonctionnalité de mise en miroir des bases de données dans les futures versions deMicrosoft SQL Server, il vous est recommandé d'utiliser la fonctionnalité Alw aysOn pour la haute disponibilité. Pour utiliser AlwaysOn, une procédure de configuration doit être suivie avant d'i nstallerBlackBerry UEM. Pour en savoir plus sur l'activation d'AlwaysOn,consultez le contenu relatif à l'installation et à la mise à niveau.Notez que la fonctionnalité AlwaysOn ne peut pas être utilisée si vous effectuez la mise à niv eau deBES5versBlackBerry UEM(la base de donnéesBES5est mise à niveau avec une base de donnéesBlackBerry UEM). AlwaysOn n'est pas pris en charge pour les composants qui gèrent des terminauxBlackBerryOS.

Lorsque vous configurez la mise en miroir de bases de données, vous devez sauvegarder la base de données Blac kBerry UEM principale (la base de données créée lors de l'installation) et utiliser les fichiers de sauvegarde pour cr éer une base de données miroir sur un autre ordinateur. Vous devez ensuite configurer la relation de mise en miro ir entre les deux bases de données afin que la base de données miroir exécute les mêmes actions et stocke les m êmes données.

Pour activer un basculement automatique, vous devez configurer un serveur témoin chargé d'analyser la base de données principale. Si la base de données principale cesse de répondre, le témoin entame un basculement autom atique vers la base de données miroir. Les composants BlackBerry UEM se connectent à la base de données miro ir et le service dédié aux terminaux se poursuit sans interruption. Un changement de rôle intervient : la base de do nnées miroir devient la base de données principale, et la base de données principale d'origine devient la base de d onnées miroir. Ce changement de rôle peut intervenir plusieurs fois au cours d'une même session de mise en mir oir.

Cette section explique comment créer une base de données miroir et configurer les composants BlackBerry UEM pour prendre en charge la mise en miroir de bases de données. Vous avez également la possibilité de configurer l a mise en miroir de bases de données pour les composants qui gèrent des terminaux BlackBerry OS. Pour plus d' informations, reportez-vous à Base de données haute disponibilité pour les composants qui gèrent des terminaux BlackBerry OS.

To learn more about database mirroring, visit technet.microsoft.com/sqlserver to read Database Mirroring - SQL S erver 2012 or Database Mirroring - SQL Server 2014.

Base de données haute disponibilité pour les composants qui gèrent des terminaux BlackBerry OS

Les composants BlackBerry UEM qui gèrent des terminaux BlackBerry 10, iOS, Android et Windows utilisent la mê me base de données que les composants qui gèrent des terminaux BlackBerry OS. Les composants qui gèrent de s terminaux BlackBerry OS ont recours à une méthode différente pour se connecter à la base de données miroir. S i vous souhaitez configurer la mise en miroir de bases de données pour les composants qui gèrent des terminaux BlackBerry OS, vous pouvez suivre d'autres étapes à l'issue de cette section.

Rendez-vous sur help.blackberry.com/detectLang/category/enterprise-services et consultez le chapitre « Configur ation de la haute disponibilité de BlackBerry Configuration Database » du *Guide d'administration de BlackBerry Enter*

prise Server 5. Ce chapitre explique comment connecter les composants qui gèrent des terminaux BlackBerry OS à la base de données miroir.

Remarque : le chapitre « Configuration de la haute disponibilité de BlackBerry Configuration Database » contient des références à Microsoft SQL Server 2005. Cette version de Microsoft SQL Server n'est plus prise en charge.

Si vous avez configuré la mise en miroir de bases de données BES5 avant la mise à niveau de BES5 vers BlackBerry UEM, la configuration continue à fonctionner à l'issue de la mise à niveau. La configuration s'applique uniquement aux composants qui gèrent des terminaux BlackBerry OS.

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	Vérifiez que le domaine BlackBerry UEM à la configuration système et aux conditions préalables requises.
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.

Configuration requise : mise en miroir de bases de données

Élément	Configuration requise
Microsoft SQL Server	BlackBerry UEM supports database mirroring using one of the following: • Microsoft SQL Server 2012 • Microsoft SQL Server 2014
Client natif SQL Server	Le client natif SQL Server 2012 doit être installé sur tous les ordinateurs qui héberg ent une instance de BlackBerry UEM. L'application d'installation de BlackBerry UEM installe le client natif SQL Server 2012.
Parité des versions	La version et l'édition de l'instance Microsoft SQL Server qui héberge la base de données miroir doivent être identiques à celles de l'instance Microsoft SQL Server qui héberge la base de données principale.
Centre de données unique	La base de données principale et la base de données miroir doivent se trouver dans le même centre de données.
Emplacement des bases de données	Créez la base de données miroir sur un ordinateur distinct de celui de la base de données principale.

Élément	Configuration requise
Mode d'opération	Configurez la mise en miroir de bases de données en utilisant le mode haute sécurité avec basculement automatique.
Témoin	Un serveur témoin est requis pour le basculement automatique. Le témoin doit être un serveur autre que le serveur principal et le serveur miroir. For more information, see Database Mirroring Witness – SQL Server 2012 or Database Mirroring Witness – SQL Server 2014.

Conditions préalables : configurer la mise en miroir de bases de données

- Configurez le serveur principal et le serveur miroir de manière ce qu'ils soient accessibles depuis des ordinateurs distants.
- Configurez le serveur principal et le serveur miroir de manière ce qu'ils disposent des mêmes autorisations.
- Set up a witness server that you will use to monitor the principal server.
- Configurez l'agent Microsoft SQL Server pour qu'il utilise un compte d'utilisateur de domaine doté des mêmes autorisations administratives locales comme 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 http://support.blackberry.com/kb et consultez l'article KB34373.
- To review additional prerequisites for your organization's version of Microsoft SQL Server, visit technet.microsoft.com/sqlserver to read Database Mirroring - SQL Server 2012 or Database Mirroring - 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 JDBC Driver and Database Mirroring (SQL 2005 JDBC - Pilote 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. Start the mirroring process. For more information, see Setting Up Database Mirroring – SQL Server 2012 or Setting Up Database Mirroring – SQL Server 2014.
10. To enable automatic failover, add a witness to the mirroring session. For more information, see Database Mirroring Witness – SQL Server 2012 or Database Mirroring Witness – 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. Vous ne devez pas arrêter et démarrer BlackBerry UEM - BlackBerry Work Connect Notification Service ; ce service est automatiquement redémarré lorsque vous redémarrez le service BlackBerry UEM - BlackBerry Affinity Manager.
- 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. Si le seul composant BlackBerry UEM présent sur un ordinateur est le BlackBerry Router, il n'est pas nécessaire d'effectuer cette tâche sur cet ordinateur.

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 http://support.blackberry.com/kb pour lire 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 ne devez pas arrêter et démarrer BlackBerry UEM - BlackBerry Work Connect Notification Service ; ce service est automatiquement redémarré lorsque vous redémarrez le ser vice BlackBerry UEM - BlackBerry Affinity Manager.
- 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 serve ur miroir à l'aide du pseudo du serveur.

Configurer 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.

Si nécessaire, configurez les composants qui gèrent des terminaux BlackBerry OS pour qu'ils se connectent au n ouveau serveur miroir (voir Base de données haute disponibilité pour les composants qui gèrent des terminaux BlackBerry OS).

Configurer des connexions TLS/SSL à Exchange ActiveSync lors de l'activation de BlackBerry Secure Gateway

Si vous activez BlackBerry Secure Gateway pour obtenir une connexion sécurisée via BlackBerry UEM entre le serveur de messagerie de votre organisation et des terminaux iOS avec le type d'activation Contrôles MDM, vous devrez peut-être configurer BlackBerry UEM afin d'établir des connexions TLS/SSL avec Exchange ActiveSync. Pour plus d'informations sur l'activation de BlackBerry Secure Gateway, reportez-vous à la section «Protéger les données de la messagerie à l'aide de BlackBerry Secure Gateway » dans le contenu relatif à l'administration.

Si la configuration de votre serveur Exchange ActiveSync exige une connexion TLS, vous devez ajouter le certificat du serveur Exchange ActiveSync (ou son certificat racine) à BlackBerry UEM. BlackBerry Secure Gateway requiert que le certificat fasse confiance au serveur Exchange ActiveSync lorsqu'il établit la connexion TLS/SSL.

En fonction des exigences de sécurité de votre serveur Exchange ActiveSync, vous devrez peut-être également mettre à jour la liste de versions TLS et de codages que BlackBerry Secure Gateway peut utiliser pour l'authentification avec Exchange ActiveSync.

Configurer BlackBerry UEM pour faire confiance au certificat du serveur Exchange ActiveSync

Avant de commencer : Exportez le certificat depuis le serveur Exchange ActiveSync au format X.509 (*.cer, *.der) et stockez-le dans un emplacement réseau auquel vous pouvez accéder depuis la console de gestion.

1. Sur la barre de menus, cliquez sur **Paramètres > Intégration externe > Certificats approuvés**.
2. Click + en regard de **Éléments approuvés du serveur Exchange ActiveSync**.
3. Cliquez sur **Parcourir**.
4. Sélectionnez le fichier de certificat à utiliser.
5. Cliquez sur **Ouvrir**.
6. Saisissez la description du certificat.
7. Cliquez sur **Ajouter**.

Configurer BlackBerry UEM afin d'utiliser les versions TLS et les codages pris en charge par Exchange ActiveSync

1. Sur la barre de menus, cliquez sur **Paramètres > Intégration externe > BlackBerry Secure Gateway**.
2. Click + dans le tableau que vous souhaitez modifier.
3. Cliquez sur la version TLS ou le codage que vous souhaitez ajouter ou supprimer de la liste **Sélectionné**.
4. Cliquez sur la flèche pour déplacer l'élément dans la liste souhaitée.
5. Cliquez sur **Attribuer**.

Simplification des activations Windows 10

Vous pouvez transformer une application Web Java de BlackBerry en 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 leur terminaux Windows 10 en saisissant l'adresse du serveur à l'invite.

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 DNS de type A sur l'hôte statique 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	Rendez-vous sur BlackBerry UEM Tools pour télécharger l'outil Auto Discovery Proxy Tool. 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.

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'ad resse 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 mo difiez 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 a pportez 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\<account name>\.key
store" />
```

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

```
C:\Program Files (x86)\Java\jre1.8.0_60\bin>keytool -genkey -alias tomcat -keya
lg RSA -keysize 2048
C:\Program Files (x86)\Java\jre1.8.0_60\bin> keytool -certreq -alias tomcat -ke
yalg RSA -file <filename>.csr
```

```
C:\Program Files (x86)\Java\jre1.8.0_60\bin>keytool -genkey -alias tomcat -keya
lg RSA -keysize 2048
Enter keystore password: changeit
What is your first and last name?
  [Unknown]:  enterpriseenrollment.example.com

What is the name of your organizational unit?
  [Unknown]:  IT Department
What is the name of your organization?
  [Unknown]:  Manufacturing Co.
What is the name of your City or Locality?
  [Unknown]:  Waterloo
What is the name of your State or Province?
  [Unknown]:  Ontario
What is the two-letter country code for this unit?
  [Unknown]:  CA
Is CN=enterpriseenrollment.example.com, OU=Business Unit, O=Example Company, L=
Waterloo, ST=Ontario, C=CA correct?
  [no]:  yes
C:\Program Files (x86)\Java\jre1.8.0_60\bin>keytool -certreq -alias tomcat -key
alg RSA -file <enterpriseenrollment.example.com>.csr
Enter key password for <enterpriseenrollment.example.com>
        (RETURN if same as keystore password):
```

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 `enterpris eenrollment.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 utilisate urs 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 -alia
s tomcat -file <filename>.p7b
```

9. Fermez Apache Tomcat.
10. Rendez-vous sur BlackBerry UEM Tools pour télécharger l'outil Auto Discovery Proxy Tool. 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, s upprimez le dossier `\ROOT`.
12. Renommez `W10AutoDiscovery-<version>.war` en `ROOT.war`. Déplacez-le dans le dossier `\webapps` da ns 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, ouvr ez `\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 da ns l'exemple ci-dessous. L'ID d'hôte de votre domaine BlackBerry UEM se trouve dans la console de gestion Bl ackBerry 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 > 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)
- BES10
- Good Control (autonome)

Remarque : Si vous voulez migrer uniquement des utilisateurs Good Control à partir d'un serveur Good Control qui est intégré à BES12 version 12.5, rendez-vous sur le site support.blackberry.com/kb pour lire l'article KB48870.

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 le site support.blackberry.com/kb et lisez 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 à partir d'un serveur Good Control source, Migration des stratégies et des profils de Good Control à BlackBerry UEM.
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.
Vérifier la version du log iciel	Pour migrer des données vers BlackBerry UEM : • The BlackBerry UEM instance you are migrating data from must be versio n 12.7 or later. • L'instance BES10 à partir de laquelle vous migrez les données doit correspondr e à la version 10.2.3 ou ultérieure. • The Good Control (standalone) instance that you are migrating data from must be at version 5.0 or later.
BlackBerry UEM synchro nization	If you are migrating from a Good Control source server, the destination BlackBerry UEM database must be synchronized before beginning migration. A Good Control source server must NOT be integrated with BlackBerry UEM i n any way before beginning migration.
Configurer la connexion au répertoire d'entreprise BlackBerry UEM	Configurez la connexion au répertoire d'entreprise BlackBerry UEM de destination t elle 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 dom aine exemple.com, configurez l'instance BlackBerry UEM de destination pour l'inté gration Active Directory et connectez-la au domaine exemple.com. **Important :** Migration does not work if the company directory on the destinat ion server does not match the company directory on the source server.
Défragmenter les bases de données (BES10 et Bl ackBerry UEM)	Défragmentez les bases de données sources et la base de données BlackBerry UE M de destination (le cas échéant) avant de commencer la migration. Si vous dépla cez 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 « Réorg aniser et reconstruire des index ».

Condition préalable	Détails
Check the status of BlackBerry Dynamics apps	Check the version of all BlackBerry Dynamics apps you want to migrate. This includes first-party apps, BlackBerry Dynamics apps, third-party ISV apps, and internal custom apps. All apps must be at BlackBerry Dynamics SDK version 4.0.0 or later. To determine the version of SDK used for the apps to be migrated, run the container activity report on Good Control. **BlackBerry Dynamics apps that are not supported for migration are wiped from the device when the administrator starts the migration.**
Check the status of BlackBerry Dynamics app entitlements	Make sure that: • The destination BlackBerry UEM has the same list of BlackBerry Dynamics app entitlements as the source Good Control server. • All migrated user accounts are assigned the same list of BlackBerry Dynamics app entitlements on the destination BlackBerry UEM as they have on the source Good Control server. • The authentication delegate is the same on the source Good Control server and the destination BlackBerry UEM. You can change the authentication delegate after migration. Missing entitlements will result in BlackBerry Dynamics apps being disabled after migration.
Review the Good Control organization IDs	Custom apps migrate only if the source and destination servers are the same Good Control organization ID. It is possible to merge two organizations. For more information, visit support.blackberry.com/kb/ to read article KB47626.

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.

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
BES10	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 Mot de passe	Si vous avez sélectionné l'authentification SQL, dans les champs Nom d'utilisateur et Mot de passe, saisissez vos informations de connexion pour vous connecter au serveur source.
	Nom de la base de données BDS	Entrez le nom de la base de données source (par exemple, BDSMgmt).
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.

Type de serveur source	Champ	Contenu
	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 (standalone)	Display name	Type a descriptive name for the source server.
	Source Good Control (standalone) host name	Type the FQDN of the Good Control management console.
	Source Good Control (standalone) certificate	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 auto-signé pour le serveur Good Control.

Type de serveur source	Champ	Contenu
	Username Password	Type your login information to log in to the administrator account for the source management console. **Remarque :** These credentials must correspond to a Good Control administrator with the access rights MANAGE_CONTAINERS and MANAGE_USERS_AND_GROUPS. The account can be either a Good Control service account or a regular administrator account, provided the password associated with the account allows access to the management console. You can't use an Active Directory user account with a hardware token and no password.
	Domain	Type the name of the domain where the administrator account for the source management console is located. You can leave this field blank if the administrator is a local user who does not have a domain.

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.

Export the self-signed root certificate for the Good Control server

Complete the following task if the Good Control certificate has not been replaced with a third-party certificate. BlackBerry UEM inherently trusts certificates from third-party providers, so you do not need to export the certificate from the Good Control server and import it in to BlackBerry UEM.

Remarque : The following task is not browser-specific. For specific instructions, see the documentation for the browser you are using.

1.

In a browser, navigate to the login screen of any of your Good Control servers. You may see a certificate err or message because the CA that signed the certificate was Good Control, and the browser does not recogni ze it as a well-known CA.

2. To open the Certificate dialog, click the certificate icon in the URL field.

3. Click **View certificate** or **Certificate information** to open the **Certificate management** menu.

4. Click the **Certification Path** tab.

5. Select the root certificate. The root certificate is the first item in the Certificate hierarchy (for example, GD12 345678 CA).

6. Click **View Certificate**.

7. Click the **Details** tab.

8. Click **Copy to file** or **Export**.

9. Select either the **DER encoded binary X.509 (.CER)** or the **Base-64 encoded X.509 (.CER)** format.

10. Enter a location and file name for the certificate.

11. Click **Next** or **Save**.

12. Click **Finish**.

Considérations : migration des stratégies informatiques, des profils e t des groupes depuis un serveur source

La migration d'une BlackBerry UEM ou BES10source copie les éléments suivants pour la base de données de dest ination :

- 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
- Profils SCEP
- Profils d'informations d'identification de l'utilisateur
- Paramètres d'autorité de certification
- Toutes les politiques et tous les profils associés aux politiques et aux profils sélectionnés

Remarque : Si la migration est effectuée depuis BES10, tous les groupes sont migrés. Cependant, les attributions d'utilisateurs, de rôles, de configuration logicielle et les attributs du système d'exploitation BlackBerry UEM des gr oupes BlackBerry ne sont pas migrés.

A migration from a Good Control (standalone) source copies the following items to the destination database:

- Policy sets
- Connectivity profiles
- App groups
- App usage (for certificates)
- Certificates

BlackBerry UEM

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

Élément	Considérations
Mots de passe de stratég ie informatique	Si le mot de passe d'une stratégie informatique source sélectionnée pour les termi naux Android comporte moins de 4 caractères ou plus de 16 caractères, aucune s tratégie informatique ni aucun profil BES12 ou BlackBerry UEM ne peut être migré . Désélectionnez ou mettez à jour la stratégie informatique source et redémarrez l a migration.
Noms de profil	Après la migration, vous devez vous assurer que tous les profils SCEP, d'informati ons d'identification de l'utilisateur, de certificats partagés ou de certificats d'autori té 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 destin ation doivent chacune disposer d'un répertoire configuré. Ce répertoire doit être co nfiguré de la même façon dans les bases de données source et de destination. Da ns le cas contraire, les groupes de répertoires ne seront pas migrés.
Groupes imbriqués	Si les bases de données source et destination sont des bases de données BES12 ou BlackBerry UEM intégrées à BES5, vous ne pouvez pas migrer les groupes d'uti lisateurs imbriqués. Si vous essayez de migrer des groupes imbriqués, la migratio n peut ne pas s'effectuer pour d'autres groupes, profils et informations de configu ration de PKI.

BES10

Lorsque vous migrez des stratégies informatiques, profils et groupes BES10 vers BlackBerry UEM, tenez compte d es recommandations suivantes :

Élément	Considérations
Groupes	Les groupes migrés conservent les stratégies informatiques et les profils qui leur sont attribués.
Utilisateurs	Les utilisateurs migrés ne conservent pas les stratégies informatiques, les profils et les groupes qui leur sont attribués. Après la migration, vous devez réattribuer les utilisateurs à chaque groupe dans B lackBerry UEM.
Mots de passe de stratég ie informatique	Si le mot de passe d'une stratégie informatique source sélectionnée pour les termi naux iOS ou Android comporte moins de 4 caractères ou plus de 16 caractères, au cune stratégie informatique ni aucun profil BES10 ne peut être migré. Désélection nez ou mettez à jour la stratégie informatique source et redémarrez la migration.
Variables personnalisées	Pendant la migration, BlackBerry UEM mappe les variables personnalisées BES10 %custom1% à %custom5% avec les variables de mot de passe personnalisées Bla ckBerry UEM %custom_pswd1% à %custom_pswd5%. Pour prévenir les erreurs lié es aux mots de passe, si vous avez utilisé ces variables dans BES10, veillez à les u tiliser de la même façon dans BlackBerry UEM. Par exemple, si la variable %custo m1% a été utilisée pour le mot de passe du profil de messagerie ActiveSync dans BES10, la variable %custom_pwd1% de BlackBerry UEM doit être utilisée dans le m ême but. Ces variables sont cryptées dans la base de données BlackBerry UEM.
Profils des certificats pa rtagés	Après la migration, les profils des certificats partagés contenant un certificat SCE P apparaissent dans la section SCEP.
Profils d'activation	Les profils d'activation ne sont pas migrés. Après la migration des utilisateurs, et a vant la migration des terminaux, vous devez attribuer à chaque utilisateur un profi l d'activation avec le même type d'activation que celui dont l'utilisateur disposait d ans BES10.
Certificats d'autorité de c ertification	Dans BlackBerry UEM, vous devez attribuer manuellement tous les certificats d'au torité de certification migrés vers les terminaux (dans BES10, les certificats d'auto rité de certification étaient automatiquement attribués). Avant d'attribuer un certifi cat d'autorité de certification migré vers des utilisateurs ou un groupe contenant d es utilisateurs qui possèdent des terminaux iOS, Android ou Windows, vous devez d'abord ouvrir le profil du certificat d'autorité de certification dans BlackBerry UEM, puis cliquer sur Modifier et sur Enregistrer.

Élément	Considérations
Règles de stratégie informatique	Les règles de stratégie informatique suivantes ne peuvent pas être migrées de BES10 vers BlackBerry UEM : • Sauvegarde et restauration de terminal • Sauvegarde et restauration de l'espace Travail • Accès au stockage dans le nuage à partir de l'espace Travail • Type de sécurité de point d'accès WPA2-Personal • Génération de clé de cryptage à deux facteurs • WebGL

Good Control (standalone)

When you migrate Good Control (standalone) security policy sets, connectivity profiles, app groups, and certificates to BlackBerry UEM, consider the following guidelines:

Item	Considerations
Policy sets	After migration, each Good Control policy set appears as the following items in BlackBerry UEM: • an app configuration for each app in the policy set • a security policy • a compliance policy
Connectivity profiles	When BlackBerry Dynamics connectivity profiles are migrated from Good Control (standalone) to BlackBerry UEM, the values from the App servers tab are not migrated. The values are populated using the default values from the destination UEM server, the same as when manually creating a new BlackBerry Dynamics connectivity profile in UEM. When BlackBerry Dynamics connectivity profiles are migrated from Good Control (standalone) to BlackBerry UEM, some of the values from the Infrastructure tab are not migrated. The administrator must manually edit each migrated profile and set the values for the Primary BlackBerry Proxy cluster and the Secondary BlackBerry Proxy cluster.
App groups	The Everyone group is migrated but has no users assigned to it and is not related to the All Users group on the destination BlackBerry UEM. The administrator must manually assign it to users if needed.
Apps	If an app entitlement from the source server doesn't exist in the destination server, that app assignment is not migrated. The app group is migrated.
App usage (for certificates)	App usage is migrated, except for: • App usages that already exist on the destination server • Non-BlackBerry Dynamics apps • Custom apps from another Good Control organization

Migrer des stratégies informatiques, des profils et des groupes depui s 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 séle ctionnez le bouton radio situé en regard du nom du serveur source à partir duquel vous souhaitez migrer les do nnées.
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 stratégie et chaque nom de profil lors de la migration vers la de stination.
6. Cliquez sur **Aperçu** pour consulter les politiques et les profils sélectionnés.
7. Cliquez sur **Migrer**.
8. Pour configurer les stratégies informatiques, les profils et les groupes, cliquez sur **Configurer les stratégies inf ormatiques et profils** afin d'accéder à l'écran **Stratégies informatiques 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 ut ilisateurs avant de migrer les terminaux. Pour des informations spécifiques sur ce qu'il faut faire lorsque vous effe ctuez la migration depuis un serveur Good Control source, reportez-vous à la section Migration des stratégies et d es profils de Good Control à BlackBerry UEM.

Migration des stratégies et des profils de Good Control à BlackBerry UEM

Après la migration des utilisateurs, terminaux, groupes et d'autres données de Good Control à BlackBerry UEM, vo us devez effectuer les tâches suivantes sur l'instance BlackBerry UEM de destination. Pour obtenir des informatio ns sur l'emplacement des fonctions Good Control dans BlackBerry UEM, reportez-vous à la section Good Control features in 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 politiques BlackBerry Dynamics migrées et des politiques de conformité aux utilisateurs.
- Définissez des profils de remplacement (profils BlackBerry Dynamics et profils de conformité).

Déplacez les configurations de fichier .json de Good Control à BlackBerry UEM.

Renseignez les profils de connectivité migrés :

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

Good Control features in BlackBerry UEM

The following table maps Good Control features to the location in BlackBerry UEM where you can perform the sim ilar task.

Good Control feature	Where to find it in BlackBerry UEM
Users and Groups	Click **Users**.
Administrators	Click **Settings** > **Administrators**.
Manage BlackBerry Dynamics app s and entitlements	**Apps** and click the app that you want to manage .
Wipe, unlock, lock, and manage log s for BlackBerry Dynamics apps	1. On the menu bar, click **Users**. 2. Search for a user account. 3. In the search results, click the name of the user account. 4. Select the device tab for the device that has installed the app that you want to manage. 5. In the **BlackBerry Dynamics Apps** section, beside the app that you wa nt to manage, choose the command.
Generate access keys	1. Click **Users**. 2. Select the user that you want to generate an access key for. 3. Click **Set activation password**. 4. Select the **BlackBerry Dynamics access key generation** option.
Manage services	Click **Settings** > **BlackBerry Dynamics** > **App services**.
App groups	Click **Groups** > **User**.
Security policies	Click **Policies and profiles** > **BlackBerry Dynamics**.
Compliance policies	Click **Policies and profiles** > **Compliance (BlackBerry Dynamics)**.
Provisioning profiles	Click **Settings** > **Activation defaults**.
App specific policies	Click **Apps** and then click the BlackBerry Dynamics app that you want to manage.
Add app servers	Click **Policies and profiles** > **Connectivity (BlackBerry Dynamics)**.
Connectivity profile	Click **Policies and profiles** > **BlackBerry Dynamics connectivity**.
Device policies	Click **Policies and profiles** > **Policy** > **IT policies**

Good Control feature	Where to find it in BlackBerry UEM
Device configurations	Click **Policies and profiles** > **Networks and Connections** and choose the f ollowing profiles: • Wi-Fi • VPN • Proxy • Email • Web icon • Custom payload
Apple DEP	Click **Settings** > **External integration** > **Apple Device Enrollment Program**
APNS management	Click **Settings** > **External integration** > **Apple Push Notification**
Manage user self-service	Click **Settings** > **Self-Service**
Direct Connect settings	Click **Settings** > **BlackBerry Dynamics** > **Direct Connect**
Server properties	Click **Settings** > **BlackBerry Dynamics** > **Properties**
Good Proxy cluster configuration	Click **Settings** > **BlackBerry Dynamics** > **Clusters**
Trusted Authorities	Click **Policies and profiles** > **Certificates** > **CA certificate** Click **Settings** > **External integration** > **Certification authority**
Certificate Definitions	Click **Policies and profiles** > **Certificates** > **User credential** Click **Settings** > **External integration** > **Certification authority**
Uploaded certificates for users	Click **Users**>**All Users**>**User Detail**>**Summary**>**IT Policy and profiles**
App usage	**Allow BlackBerry Dynamics apps to use user certificates and user crede ntial profiles** in corresponding application detail pages.
Reporting	Click **Settings** > **BlackBerry Dynamics** > **Reporting**
Server jobs	Click **Settings** > **BlackBerry Dynamics** > **Jobs**

Considérations : migration d'utilisateurs à partir d'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 la destination est une base de données BlackBerry UEM qui a été mise à niveau à partir d'une base de données BES5, vous pouvez migrer un maximum de 300 utilisateurs à la fois. 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 1000 utilisateurs, essayez de migrer un plus petit nombre d'utilisateurs.
Adresse e-mail,	• Les utilisateurs doivent disposer d'une adresse électronique avant d'être migrés. • Vous ne pouvez pas migrer un utilisateur qui utilise déjà la même adresse électronique dans le BlackBerry UEM de destination. Ces utilisateurs n'apparaissent pas dans la liste des utilisateurs à migrer. • Si deux utilisateurs de la source ont la même adresse électronique, un seul utilisateur apparait sur l'écran Migrer les utilisateurs. • Si deux utilisateurs de la source ont la même adresse électronique, les informations d'utilisateur affichées sur l'écran Migrer les terminaux peuvent se rapporter à l'un ou l'autre des utilisateurs. • Si deux utilisateurs d'un répertoire d'entreprise intégré à BES10 disposent de la même adresse e-mail, le premier utilisateur détecté sera migré. Cet utilisateur n'est pas forcément l'utilisateur créé dans la source.
Terminal	• Si un utilisateur de la source possède à la fois un terminal BlackBerry 10 et un terminal iOS ou Android, et que les terminaux utilisent la même adresse électronique avec des noms d'utilisateur différents, certains terminaux ne sont pas migrés. • Après la migration, si un utilisateur dispose à la fois d'un terminal BlackBerry 10 et d'un terminal iOS, Android, Windows ou macOS, il doit utiliser les mêmes informations de connexion pour BlackBerry UEM Self-Service que celles qu'il utilisait pour BES10 Self-Service, BES12 Self-Service ou BlackBerry UEM Self-Service avant la migration.
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 BES12 Self-Service ou 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.
Good Dynamics	Vous pouvez migrer les utilisateurs auxquels des profils Good Dynamics sont assignés.

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. Sur l'écran **Migrer des utilisateurs**, si la source est une configuration Good Control (autonome), 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 seulement pour le premier ensemble de migration des utilisateurs et est facultative par la suite.
3. Cliquez sur **Suivant**.
4. Sélectionnez les utilisateurs à migrer.

   Pour les migrations Good Control, seuls les premiers 20 000 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.

   Pour les migrations Good Control, 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, consultez le 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.

Élément	Considérations
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	• The users must exist in the destination BlackBerry UEM domain • Pour les migrations de BES10 et BlackBerry UEM, vous ne pouvez pas migrer plus de cinq terminaux à la fois par utilisateur.
iOS devices on a BlackBerry UEM or BES10 source	• La dernière version de iOS doit être installée sur les terminaux BlackBerry UEM Client. • Tous les terminaux iOS doivent être approuvés (les terminaux iOS non approuvés ne peuvent pas être migrés). • iOS devices that are assigned the App lock profile cannot be migrated because the BlackBerry UEM Client cannot be opened for the migration
Android devices on a BlackBerry UEM or BES10 source	• La dernière version de Android doit être installée sur les terminaux BlackBerry UEM Client. • Vous ne pouvez pas migrer les terminaux Android dotés d'un profil professionnel.
Windows	Vous ne pouvez pas migrer des terminaux Windows.
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
Good Control devices (from standalone Good Control)	**BlackBerry Dynamics apps** • All BlackBerry Dynamics apps compatible with migration are migrated. **BlackBerry Dynamics apps that are incompatible with migration are wiped from the device when the administrator triggers the migration.** These apps must be reactivated on the destination BlackBerry UEM. • Incompatible apps are apps that are built with BlackBerry Dynamics SDK versions earlier than 4.0.0. Before migration, you can run the container activity report to check the SDK versions of the apps. • In the Migrate devices screen, the Incompatible containers column displays the number of BlackBerry Dynamics apps for each device that cannot be migrated and the total number of BlackBerry Dynamics apps for each device. Click on the number to see the BlackBerry Dynamics apps that are incompatible with migration. • Make sure that the user has entitlements for the app on the destination BlackBerry UEM. If the app doesn't have the entitlement, after migration, the user will receive a message that the app is blocked. • BlackBerry Dynamics apps are not migrated if the destination BlackBerry UEM already has apps registered for that user. • Custom apps migrate only if the source and destination servers are the same Good Control organization ID. It is possible to merge two organizations. For more information, visit support.blackberry.com/kb/ to read article KB47626. **Device authentication** • Devices with a device authentication delegate of Good for Enterprise are not migrated. After removing Good for Enterprise as the authentication delegate, refresh the cache before continuing with the migration. It is a best practice to ensure that the user is assigned the same authentication delegate on BlackBerry UEM as they had on the source server. • The authentication delegate must be the same on the source Good Control server and the destination BlackBerry UEM. You can change the authentication delegate after migration. **Device management** • Good Dynamics MDM enrolments are not migrated. The user must unenroll from MDM. If the destination BlackBerry UEM requires MDM, the user must manually delete the old MDM profile and install and activate the BlackBerry UEM Client and re-enroll the device for MDM. **Operating system** • Devices with an unknown operating system are not migrated. **Chat sessions** • The source BEMS server may keep stale Connect chat sessions open for up to 24 hours so the user may temporarily appear to be logged into chat from two devices. • Unread Connect chat messages are deleted during migration. Users should log out of Connect before migration. **Users** • If a user has more than one device with BlackBerry Dynamics apps, all the devices are automatically selected for migration. • You can't migrate devices for the same user from multiple Good Control source servers. You can migrate devices from multiple Good Control sources, but the users cannot already have a BlackBerry Dynamics device on the destination BlackBerry UEM. **Unlock keys**

Référence rapide pour la migration des terminaux

Type de terminal	Type d'activation/configuration	Migration
BlackBerry 10	Indifférent	Pris en charge
Android	• Contrôles MDM • BlackBerry 2FA	Pris en charge
Android devices that have a work p rofile	Any	Not supported
Android Samsung KNOX Workspa ce devices	Any	Supported
iOS	• Contrôles MDM • Device registration for BlackBer ry 2FA only • DEP devices that have the Blac kBerry UEM Client installed	Pris en charge
iOS	• DEP devices that do have the Bl ackBerry UEM Client installed	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 le BlackBerry UEM de destination, vous pouvez migrer le urs terminaux. Les terminaux sont transférés du serveur source vers le 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 utilis ateurs que vous avez migrés.
- Pour les migrations depuis BlackBerry UEM et BES10, informez les utilisateurs de terminaux iOS qu'ils doivent ouvrir le BlackBerry UEM Client pour démarrer la migration vers BlackBerry UEM, et qu'ils doivent garder le Blac kBerry UEM Client ouvert jusqu'à ce que la migration soit terminée.

1. Sur la barre de menus, cliquez sur **Paramètres > Migration > Terminaux**.
2. On the **Migrate devices** screen, if the source is a Good Control (standalone) configuration, click **Refresh cac he**.

   The cache can take approximately 10 minutes for each 1000 devices to populate.

   BlackBerry UEM caches the device data to speed searching capabilities, but the device data is migrated dire ctly from the source. Refreshing the cache is mandatory only for the first set of device migration and option al afterward.
3. Cliquez sur **Suivant**.
4. Sélectionnez les terminaux à migrer.

   For Good Control migrations, only the first 20,000 devices are displayed. Search on the user name or email a ddress to locate specific users that may not be in the first 20,000. Selecting all selects only those devices o n the first page. Set the page size for the number of devices that you want to select.

   Remarque : You may see fewer line items than number of devices because the cache is displayed by user and some users may have more than one device.

   For Good Control migrations, if changes are made in the source after the cache is refreshed, those changes are not reflected in the cache data displayed. You should not make changes to the source server during mig ration, but if you do, refresh the cache periodically.
5. Cliquez sur **Aperçu**.
6. Cliquez sur **Migrer**.
7. Pour afficher l'état des terminaux en cours de migration, cliquez sur **Migration** > **État**.

   To determine which BlackBerry Dynamics apps have been migrated, run the container activity report on Go od Control.

   Make sure that the Good Control configuration remains running until all of the users' authentication delegate apps have completed migration, even if all devices are migrated.

Migrations de terminaux DEP

Vous pouvez migrer des terminaux iOS inscrits au programme d'inscription des appareils Apple (DEP) depuis une base de données BlackBerry UEM ou BES12 source vers une autre base de données BlackBerry UEM.

Migration de terminaux DEP sur lesquels BlackBerry UEM Client est installé

Vous pouvez migrer des terminaux iOS inscrits au programme d'inscription des appareils Apple et activés avec le s types d'activation « Travail et Personnel - Contrôle total » ou « 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**.

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'informati ons, reportez-vous à Configuration de BlackBerry UEM pour le programme d'inscription des appareils.

   Assurez-vous que le profil DEP de l'instance de BlackBerry UEM de destination correspond au profil DEP de l'in stance 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 de BlackBerry UEM source vers l'instance de destination.

Migration de terminaux DEP sur lesquels BlackBerry UEM Client n'est pas installé

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'informati ons, reportez-vous à Configuration de BlackBerry UEM pour le programme d'inscription des appareils.

   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.

Configuring BlackBerry UEM to support BlackBerry Dynamics apps

Follow the instructions in this section to configure BlackBerry UEM settings that are specific to BlackBerry Proxy and BlackBerry Dynamics apps.

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 nouveaux clusters sont considérés comme non attribués et doivent être ajoutés 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 **Cluster**, sélectionnez le cluster BlackBerry Proxy 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**.
Permettre à un BlackBerry Proxy d'être utilisé pour l'activation	Select the **Enabled for activation** option for the BlackBerry Proxy instance that you want to use for activation purposes. At least one instance must be selected.

Configurer Direct Connect ou un proxy Web pour les connections à BlackBerry Proxy

Par défaut, les applications BlackBerry Dynamics des terminaux des utilisateurs envoient des données au NOC BlackBerry Dynamics. Selon la distance physique entre les terminaux et le NOC BlackBerry Dynamics, les connexions peuvent se heurter à une certaine latence du réseau.

Pour limiter de tels problèmes, vous pouvez activer BlackBerry Dynamics Direct Connect. Direct Connect permet aux applications BlackBerry Dynamics de contourner la connexion au NOC et de se connecter directement à une instance de BlackBerry Proxy derrière le pare-feu de votre entreprise Si les terminaux sont physiquement plus proches des instances de BlackBerry Proxy de votre domaine que du NOC BlackBerry Dynamics, Direct Connect permet de réduire la latence du réseau.

Vous pouvez également configurer des applications BlackBerry Dynamics pour envoyer des données via un serveur proxy Web dans la zone démilitarisée lorsqu'elles se connectent à une instance de BlackBerry Proxy.

Avant de commencer :

- Si vous voulez router les connexions depuis les applications BlackBerry Dynamics via un serveur proxy Web, ce serveur proxy doit prendre en charge la commande HTTP Connect et ne pas exiger d'authentification. Le pare-feu interne de votre entreprise doit autoriser les connexions sur le port 17533.
- Si vous ne configurez pas de serveur proxy Web pour une instance de BlackBerry Proxy, les pare-feu interne et externe de votre entreprise doivent autoriser les connexions sur le port 17533.

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. To turn on Direct Connect, select the **Turn on Direct Connect** check box. In the **BlackBerry Proxy host name** field, verify that the host name is correct.

   Si vous modifiez le nom d'hôte, l'instance deBlackBerry Proxygénère un nouveau certificat pour les connexions client et demande à l'autorité de certificationBlackBerry Dynamicsde signer le certificat.
5. Pour configurer un proxy Web, cochez la case **Utiliser un proxy Web**. Spécifiez le nom d'hôte complet ainsi que le numéro de port.
6. Cliquez sur **Enregistrer**.

Configurer les propriétés BlackBerry Dynamics

Vous pouvez configurer des propriétés spécifiques à l'utilisation des applications BlackBerry Dynamics dans votre entreprise. Pour plus d'informations sur les différentes propriétés et les répercussions d'une modification de ses paramètres par défaut, reportez-vous aux sections Propriétés globales de BlackBerry Dynamics, Propriétés de BlackBerry Dynamics et Propriétés de BlackBerry Proxy. Pour découvrir les meilleures pratiques de configuration des propriétés BlackBerry Proxy, visitez le site http://support.blackberry.com/kb pour lire 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 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 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.

Gestion des certificats

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.	86400	—

Communication

Propriété	Description	Défaut	Redémarrer
cntmgmt.internal.port	Le port interne pour le service de gestion des conteneurs.	Null (par défaut, 17317)	Oui
cntmgmt.max.conns.above.limit	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

Propriété	Description	Défaut	Redémarrer
cntmgmt.max.active.sessions	Nombre maximum de sessions actives pour la gestion des conteneurs.	10000	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

Propriété	Description	Par défaut	Redémarrer
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.	259200	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.	86400	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
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	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.	1440	Oui

Vider les conteneurs inactifs

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

Propriété	Description	Défaut	Redémar rer
Activer la tâche pour supprim er automatiquement les cont eneurs inactifs (activer/désa ctiver)	Spécifiez si BlackBerry UEM planifie automatiquem ent des tâches pour identifier et supprimer les conte neurs inactifs des terminaux.	O	Non
Intervalle d'inactivité des cont eneurs en secondes	Délai, en secondes, avant lequel BlackBerry UEM co nsidère un conteneur comme inactif.	7776000	Non
Fréquence, en secondes, d'ex écution de la tâche de suppre ssion des conteneurs inactifs	Fréquence, en secondes, à laquelle BlackBerry UEM exécute une tâche pour identifier et supprimer les c onteneurs inactifs.	86400	Non
Nombre maximum de conten eurs à supprimer au cours d'u ne même tâche	Nombre maximum de conteneurs d'inactifs qu'une même tâche peut supprimer des terminaux.	100	Non

Rapports

Propriété	Description	Défaut	Redémar rer
Définissez la limite d'enregistr ements renvoyés dans les rap ports exportables pour éviter t out manque de mémoire.	Nombre maximum de lignes pouvant être incluses d ans un rapport. La valeur maximum possible est 10 00000.	5000	Non

Stratégie de rétention des données

Propriété	Description	Défaut	Redémar rer
Consigner les opérations de l ecture dans la base de donné es	Détermine si BlackBerry Control consigne les opéra tions de lecture dans la base de données BlackBerr y Control.	I	Oui
Vider les tâches du serveur	Spécifiez si BlackBerry UEM vide automatiquement les tâches du serveur à un intervalle régulier.	I	Oui

Propriété	Description	Défaut	Redémarrer
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 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
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 BlackBerry Proxy de votre organisation.

Propriété	Description	Par défaut	Redémarrer
gp.gps.max.sessions	Nombre maximal de sessions actives. **Remarque :** Cette propriété est en lecture seule. Vous ne pouvez pas la modifier.	15 000	—

Propriété	Description	Par défaut	Redémarrer
gp.gps.dns.server.ttl.ms	Délai pour l'attente (en millisecondes) de la réponse du serveur DNS. **Remarque :** Cette propriété est en lecture seule. Vous ne pouvez pas la modifier.	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
gp.eacp.command.service.nslookup.srv.ldap	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 par requête DNS pour un enregistrement du formulaire : _ldap._tcp. Dns DomainName. 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.proxy.auth.username	Nom d'utilisateur pour la connexion au serveur Web proxy externe	Non défini	Non
gp.proxy.auth.domain	Domaine Active Directory pour la connexion d'authentification à un serveur Web proxy externe	Non défini	Non
gp.proxy.auth.password	Mot de passe pour l'authentification auprès du serveur Web proxy externe	Non défini	Non

Propriété	Description	Par défaut	Redémarrer
gp.proxy.https.host	Nom du serveur Web proxy externe	Non défini	Non
gp.proxy.https.port	Numéro de port pour la connexion HTTPS au serveur Web proxy externe	Non défini	Non
GP Proxy URLs Control	Saisissez l'une des options suivantes : 1. NOC URLs (qp.proxy.urls est ignorée) 2. Route All (qp.proxy.urls est ignorée) 3. Custom URLs List (entrez les URL dans qp.proxy.urls. Vous devez inclure les URL du NOC dans la liste.)	1	Non
gp.proxy.urls	Les URL doivent renvoyer vers un proxy	Non défini	Oui
gp.proxy.use	Utiliser un serveur Web proxy externe	O	Non

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, TLSv1, v1.1 et v1.2 sont autorisés, et SSLv3 ne l'est pas. Vous devez choisir au moins un protocole.

Remarque : ne sélectionnez pas seulement SSLv3. Toutes les connexions aux clients risqueraient d'être abandonnées.

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**.

Configurer des certificats pour les applications BlackBerry Dynamics

Si vous souhaitez que les applications BlackBerry Dynamics présentes sur les terminaux des utilisateurs utilisent les certificats client, vous pouvez télécharger les certificats vers les comptes d'utilisateur individuels ou configurer un connecteur PKI afin de permettre à BlackBerry UEM d'inscrire automatiquement les certificats client à partir de votre autorité de certification et de les envoyer aux terminaux.

Si vous téléchargez des certificats vers des comptes d'utilisateur, vous devez configurer une valeur TTL pour les certificats utilisateur. Au terme de la valeur TTL, les certificats sont supprimés du serveur.

Si vous souhaitez inscrire automatiquement les certificats émis par votre autorité de certification pour les applications BlackBerry Dynamics, vous devez configurer un connecteur PKI.

Vous pouvez également utiliser une solution PKI basée sur une application, telle que Purebred, afin d'inscrire des certificats pour les applications BlackBerry Dynamics. Pour plus d'informations, reportez-vous au contenu relatif à l'administration.

Configurer une valeur TTL pour les certificats client

Si vous téléchargez des certificats pour des comptes d'utilisateur individuels pour les applications BlackBerry Dynamics, vous devez configurer une valeur TTL pour les certificats client. Au terme de la valeur TTL, les certificats sont supprimés du serveur. Ainsi, un certificat client ne peut rester longtemps sur le serveur après avoir été transmis au terminal. Par défaut, la valeur TTL est de 24 heures.

1. Dans la barre de menus, cliquez sur **Paramètres > Paramètres généraux > Certificats**.
2. Spécifiez la valeur TTL des certificats PKCS#12 sur le serveur.

À la fin : Si ce n'est pas déjà fait, ajoutez des certificats client aux comptes d'utilisateur.

Configurer des connexions PKI pour les applications BlackBerry Dynamics

Pour inscrire automatiquement les certificats émis par l'autorité de certification de votre entreprise avec les applications BlackBerry Dynamics, il vous faut communiquer avec l'autorité de certification via un connecteur PKI. 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.

Le connecteur PKI met en œuvre le protocole de gestion des certificats utilisateur. Pour un exemple de mise en œuvre de connecteur PKI, reportez-vous à la sectionCréation d'un certificat PKI via Good Control : mise en œuvre de référence. L'exemple illustrant la création et le déploiement du connecteur PKI dont il est question dans ce document s'applique aussi pourBlackBerry UEM, mais vous devez configurer la connexion entreBlackBerry UEMet le connecteur PKI dans la console de gestionBlackBerry UEMcomme décrit dans le contenu relatif à l'administration.

Interactions du connecteur PKI

BlackBerry UEM envoie les appels d'API vers le connecteur PKI à l'aide de la méthode HTTP POST. Le connecteur PKI prend en charge l'authentification du mot de passe et l'authentification basée sur certificat.

API GetInfo

Cette API détecte les commandes mises en œuvre par le connecteur PKI. Cette commande permet également de vérifier les informations d'authentification fournies dans BlackBerry UEM et de tester la connexion entre BlackBerr y UEM et le connecteur PKI.

If this command is not implemented, BlackBerry UEM will assume this is not a valid PKI connector.

Le composant de chemin de l'URI envoyé est le suivant : `customerSpecifiedPrefix/pki?operation=getI nfo`

Le composant `customerSpecifiedPrefix` est facultatif. Il indique l'endroit où le service est hébergé sur le ser veur s'il n'est pas hébergé dans le chemin par défaut.

La réponse au format JSON attendue dans le corps HTTP est la suivante :

Élément ou clé	Saisissez	Requise	Réponse
opérations	Tableau de cha ines	Y	Tableau répertoriant toutes les commandes mises en œuvre par le connecteur PKI

Exemple de demande/réponse

En supposant que l'URL du connecteur PKI soit définie comme suit dans la console de gestion BlackBerry UEM : h ttps://cert.example.com

```
GET /pki?operation=getInfo HTTP/1.0
Host: cert.example.com
Content-Type: application/json
Content-Length: 0
Réponse
HTTP/1.0 200 OK Host: cert.example.com
Content-Type: application/json
Content-Length: XYZ
{
      “operations” : [“getInfo”, “getUserKeyPair”]
}
```

API de demande de paire de clés

Cette API est utilisée pour récupérer un certificat utilisateur une fois la paire de clés créée. Cette demande peut êt re utilisée pour les demandes de certificats initiales.

Le composant de chemin de l'URI envoyé est le suivant : `customerSpecifiedPrefix/pki?operation=getU serKeyPair`.

Le composant `customerSpecifiedPrefix` est facultatif. Il indique l'endroit où le service est hébergé sur le ser veur s'il n'est pas hébergé dans le chemin par défaut.

L'entrée au format JSON envoyée dans le corps HTTP est la suivante :

Élément ou clé	Saisissez	Requise	Commentaire
mType	Chaine	Y	{"initialCert"]
Utilisateur de	Chaine	Y	Adresse électronique de l'utilisateur ou tout autre ide ntifiant Objet du certificat créé par l'émetteur
authToken	Chaine	N	OTP ou mot de passe (pour initialCert)
reqId	Chaine	Y	Pour aider l'expéditeur à mettre en correspondance la réponse

La réponse au format JSON du corps HTTP, une charge utile PKCS #12 susceptible d'être cryptée, est la suivante :

Élément/Clé	Saisissez	Requise	Commentaires
status	Chaine	Y	{success, failure}
failureInfo	Chaine	N	Voir *Motifs d'échec* ci-dessous
payloadType	Chaine	N	=pkcs12
payload	Base64 e ncoded	N	pkcs12 contenant la clé privée et le certificat public d e l'utilisateur. Il peut être crypté.
decryptionPassword	Base64 e ncoded	N	Si le mot de passe de cryptage est identique à l'OTP f ourni par l'utilisateur, il n'est pas nécessaire d'indiquer de descryptionPassword. Si pkcs12 correspondait au mot de passe crypté et qu e l'OTP n'a pas été utilisé, le mot de passe peut être re nvoyé dans decryptionPassword.
reqId	Chaine	Y	reqID reçu dans la demande

Exemple de demande/réponse

En supposant que l'URL du connecteur PKI soit définie comme suit dans la console de gestion BlackBerry UEM : h ttps://cert.example.com

Demande : au-delà de la connexion SSL au serveur cert.example.com, la charge utile suivante sera envoyée :

```
POST /pki?operation=getUserKeyPair HTTP/1.0
Host: cert.example.com
Content-Type: application/json
Content-Length: XYZ
{
      "mType": "initialCert",
      "user": "joe.foo@example.com",
      "authToken": "56ht12d0",
      "reqId": "12487"
}
```

If the server URL was set as https://cert.example.com/foo, the request will look like:

```
POST /foo/pki?operation=getUserKeyPair HTTP/1.0
Host: cert.example.com
Content-Type: application/json
Content-Length: XYZ
```

Response:

```
HTTP/1.0 200 OK
Host: cert.example.com
Content-Type: application/json
Content-Length: XYZ
 {
      "status":"success",
      "reqId": "12487"
      "payloadType":"pkcs12",
      "decryptionPassword":"NTZodDEyZDA=",
      "payload":"BASE64 Encoded PKCS#12"
}
```

Motifs d'échec

Les erreurs suivantes peuvent être renvoyées par l'autorité de certification :

Échec	Description
unknownUser	L'utilisateur n'existe pas ou ne dispose pas de l'autorisation requise
badRequest	La demande n'est pas correctement formatée
unknownRequest	L'opération demandée n'est pas prise en charge
authFailure	L'OTP ou le mot de passe a expiré ou est incorrect
badAlg	L'algorithme utilisé n'est pas pris en charge ou pas reconnu
unknownCert	Le certificat utilisé ou référencé dans l'opération est introuvable
badMessageCheck	La vérification de la signature ou de l'intégrité a échoué
badTime	L'heure de la signature n'était pas suffisamment proche
unknown	Les autres erreurs sont traitées en tant qu'erreurs inconnues

Intégration de BlackBerry UEM avec Cisco ISE

Cisco Identity Services Engine (ISE) est un logiciel de gestion de réseau qui permet à une entreprise de contrôler l 'accès au réseau professionnel des terminaux (par exemple, autorisant ou refusant les connexions Wi-Fi ou VPN). Les administrateurs Cisco ISE peuvent créer et appliquer les politiques d'accès pour s'assurer que seuls les termi naux 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 po ur 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 au x 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 ge stion 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 donn ées d'un terminal.

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

Étape	Action
1	Vérifiez que l'environnement de votre entreprise répond aux exigences d'intégration de Blac kBerry UEM à Cisco ISE.
2	Créez un compte administrateur BlackBerry UEM que Cisco ISE peut utiliser pour obtenir de s 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 stratégie s d'accès.

Exigences : intégration de BlackBerry UEM à Cisco ISE

Élément	Configuration requise
Cisco ISE version	BlackBerry UEM prend en charge l'intégration à Cisco ISE version 1.2 et ultérie ure.

Élément	Configuration requise
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 : • BlackBerry 10 OS version 10.3.2 ou antérieure (version 10.3.3 ou ultérieure requise) • Android 6.0 (Marshmallow) • BlackBerry OS (version 7.1 ou antérieure) • Windows 10 pour bureau Cisco ISE ne peut pas récupérer des données pour les terminaux iOS dotés du type d'activation Travail et Personnel - Confidentialité de l'utilisateur.
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.

création d'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 menu.
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 : création d'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 **Envoyer**.

À la fin : Connexion de BlackBerry UEM à Cisco ISE .

Connexion de BlackBerry UEM à Cisco ISE

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

Remarque : Les étapes suivantes sont basées sur Cisco ISE version 1.4. Pour consulter la documentation Cisco I SE à jour, accédez au site Web des Guides de configuration de Cisco ISE pour lire le Guide de l'administrateur *Cis co 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'installatio n a sélectionné un autre port disponible. Pour vérifier la valeur de port correcte, dans le fichier journal BlackBer ry UEM Core (CORE), recherchez `(^/ciscoise/.*)` et notez le numéro de port indiqué au-dessous de ce tex te.
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 I SE interroge BlackBerry UEM pour obtenir les données du terminal. Il est recommandé d'utiliser la valeur par dé faut de 240 minutes.

   Remarque : Si vous définissez cette valeur sur 60 minutes ou moins, vous remarquerez peut-être un impact im portant sur les performances de l'environnement de votre entreprise. Si vous définissez cette valeur sur 0, Cisc o 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 **Envoyer**.

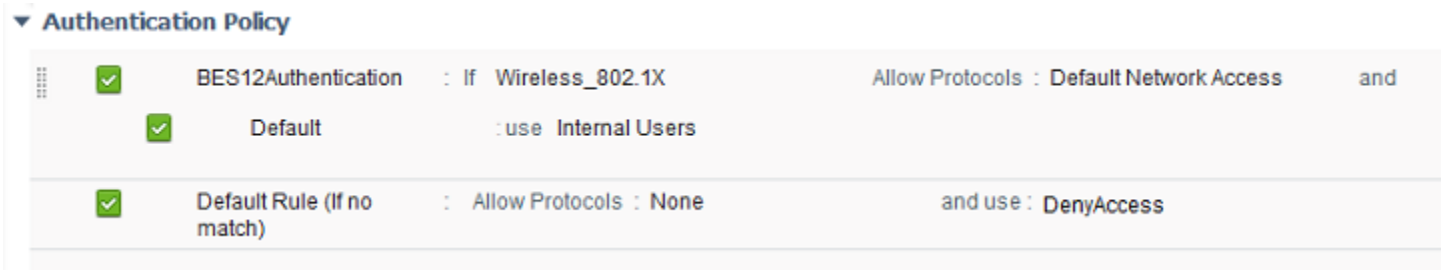
Une fois la connexion établie, vous pouvez consulter les attributs de dictionnaire de BlackBerry UEM dans **Stratégi e > Éléments de stratégie > Dictionnaires > Système > MDM > Attributs du dictionnaire**. Les entrées de journal po ur l'interrogation de Cisco ISEsont écrites dans le fichier journal BlackBerry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

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

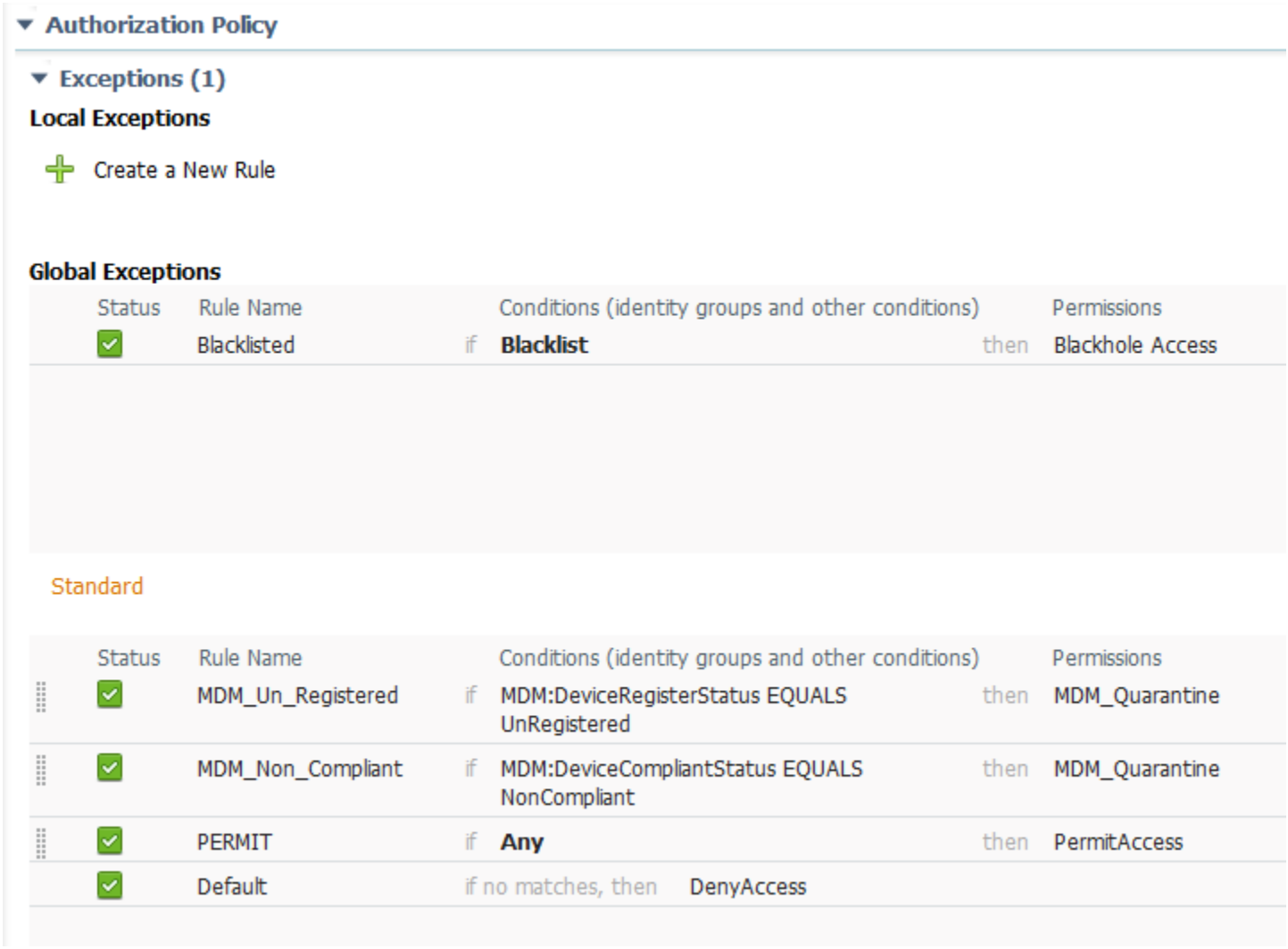
- Configurez des listes de contrôle d'accès sur le contrôleur LAN sans fil.
- Configurez un profil d'autorisation qui doit rediriger les terminaux qui ne sont pas activées sur BlackBerry UE M. Pour plus d'informations, reportez-vous à Redirection des terminaux qui ne sont pas activés sur BlackBerry UEM .
- Configurez les règles de stratégie d'autorisation qui déterminent comment Cisco ISE gère les terminaux qui n e 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	Verrouille le terminal iOS, Android ou Windows d'un utilisateur (les terminaux BlackBerry 10 ne prennent pas en charge cette fonction). 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.

Action	Description
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 terminaux qui ne sont pas activés sur BlackBerry UEM

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

L'utilisateur requiert un compte d'utilisateur BlackBerry UEM pour se connecter à BlackBerry UEM Self-Service et activer le terminal. 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 le terminal 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 de l'entreprise sur son terminal. Pour résoudre ce problème, lorsque vous supprimez un terminal de BlackBerry UEM, supprimez également ses données de Cisco ISE.

Surveillance de BlackBerry UEM à l'aide des outils SNMP

Vous pouvez utiliser des outils SNMP tiers pour analyser l'activité de plusieurs composants BlackBerry UEM. L'an alyse SNMP requiert un service SNMP et un outil de gestion SNMP. Vous devez exécuter le service SNMP sur l'ord inateur qui héberge BlackBerry UEM. Le service SNMP, situé dans Windows Services, comprend un agent SNMP q ui recueille les données des composants BlackBerry UEM.

Vous devez utiliser un outil de gestion SNMP (par exemple, un navigateur MIB) pour afficher et analyser les donné es transmises par l'agent. L'outil de gestion comprend généralement un outil de gestion des déroutements SNMP qui permet de récupérer et d'interpréter les messages de déroutement de l'agent. L'outil de gestion peut être instal lé sur l'ordinateur qui héberge BlackBerry UEM ou sur un ordinateur distinct.

Vous devez configurer SNMP aux deux emplacements suivants :

- Pour analyser BlackBerry UEM Core, BlackBerry Secure Connect Plus, BlackBerry Secure Gateway et BlackB erry Cloud Connector, vous devez configurer SNMP dans la console de gestion. Reportez-vous à la section Configurer SNMP pour surveiller les composants.
- Pour analyser les composants de connectivité d'entreprise BlackBerry UEM, vous devez configurer le service S NMP.

Par défaut, l'outil de gestion affiche l'identifiant d'objet (OID) d'une condition, lequel correspond à une suite de no mbres entiers qui identifie une valeur de classe dans une hiérarchie de classes. Tous les OID SNMP et tous les dé routements SNMP de BlackBerry UEM commencent par la valeur de classe 1.3.6.1.4.1.3530.8. Un suffixe (par exe mple, 25.1.1) permet d'identifier chaque valeur OID de façon unique.

Les bases d'informations de gestion (MIB) spécifient les conditions analysées par l'agent SNMP. Une MIB est une base de données qui définit et décrit les variables et les données de gestion des composants BlackBerry UEM, en i ndiquant notamment ce que représente chaque valeur de déroutement SNMP. La MIB détermine les types de don nées que le service SNMP peut recueillir au sujet des composants. Lorsque vous configurez l'analyse SNMP, vous utilisez l'outil de gestion pour compiler la MIB.

Pour en savoir plus sur la sécurité réseau de SNMP, rendez-vous sur support.microsoft.com.

Opérations SNMP prises en charge

Vous pouvez utiliser les opérations SNMP pour recueillir les données à partir de l'agent SNMP exécuté sur les ordi nateurs où BlackBerry UEM est installé. BlackBerry UEM prend en charge les opérations SNMP suivantes :

Opération	Description
Get	Récupère la valeur d'un élément MIB spécifique.
Get next	Récupère la valeur et l'OID des éléments en fonction de leur ordre d'apparition dans le fichier MIB.
Trap	Envoie les messages de déroutement SNMP de l'agent SNMP vers l'outil de ge stion des déroutements SNMP. Les messages de déroutement SNMP contien nent des données sur les actions spécifiques effectuées par un composant Bl ackBerry UEM.

Configuration requise : analyse SNMP

Élément	Configuration requise
Composants BlackBerry UEM pris en charge	Vous pouvez configurer l'analyse SNMP pour les composants BlackBerry UEM suivants : • BlackBerry Affinity Manager • BlackBerry Cloud Connector • BlackBerry Dispatcher • BlackBerry MDS Connection Service • BlackBerry Router • BlackBerry Secure Connect Plus • BlackBerry Secure Gateway • BlackBerry UEM Core Les autres composants BlackBerry UEM ne prennent pas en charge l'analyse SNMP.
Outil de gestion SNMP	Si l'outil de gestion ne comprend pas de compilateur de MIB, installez-en un sur l'ordinateur qui héberge l'outil de gestion. Si vous souhaitez que le service SNMP envoie des messages de déroutement pour établir des rapports sur l'activité du serveur, vérifiez que l'outil de gestion comprend un outil de gestion de déroutement SNMP. Vous pouvez aussi installer un outil de gestion des déroutements SNMP autonome sur un ordinateur qui héberge BlackBerry UEM, ou sur un ordinateur distinct.
Accès réseau	L'ordinateur qui héberge l'outil de gestion SNMP, ou un outil de gestion des déroutements SNMP autonome, doit être en mesure d'accéder aux données et de les récupérer depuis l'ordinateur où BlackBerry UEM est installé.
Service SNMP	Sur les ordinateurs où BlackBerry UEM est installé, installez un service SNMP comprenant un agent SNMP et un service de déroutement SNMP. Un service SNMP est disponible dans la plupart des versions de Windows. Pour plus d'informations, visitez le site support.microsoft.com.
Paramètres de service SNMP	Sur les ordinateurs où BlackBerry UEM est installé, dans Windows Services, configurez les paramètres de service SNMP suivants : • Nom de communauté SNMP valide • Autorisation de lecture seule (au minimum) pour la communauté SNMP • Adresses IP des ordinateurs dont le service SNMP peut accepter les données.

MIB de BlackBerry UEM

Par défaut, les MIB de BlackBerry UEM se trouvent sur l'ordinateur où BlackBerry UEM est installé, sous *<drive>*\Program Files\BlackBerry\UEM\Monitoring\bin\mib.

BlackBerry UEM comprend les MIB suivants que vous pouvez utiliser pour analyser les données des composants BlackBerry UEM :

Fichier MIB	Description
BES-BCCMIB-SMIV2	Contient une définition de la racine de l'arborescence OID de l'interface SNMP de BlackBerry Cloud Connector.
BES-BCCMonitoringMIB-SMIV2	Contient les définitions des objets gérés BlackBerry Cloud Connector accessibles et récupérables à l'aide de l'outil de gestion SNMP.
BES-BSCPMIB-SMIV2	Contient une définition de la racine de l'arborescence OID de l'interface SNMP de BlackBerry Secure Connect Plus.
BES-BSCPMonitoringMIB-SMIV2	Contient les définitions des objets gérés BlackBerry Secure Connect Plus accessibles et récupérables à l'aide de l'outil de gestion SNMP.
BES-BSGMIB-SMIV2	Contient une définition de la racine de l'arborescence OID de l'interface SNMP de BlackBerry Secure Gateway.
BES-BSGMonitoringMIB-SMIV2	Contient les définitions des objets gérés BlackBerry Secure Gateway accessibles et récupérables à l'aide de l'outil de gestion SNMP.
BES-CoreEventingMIB-SMIV2	Contient les définitions des déroutements et notifications émis par BlackBerry UEM Core.
BES-CoreMIB-SMIV2	Contient une définition de la racine de l'arborescence OID de l'interface SNMP de BlackBerry UEM Core.
BES-CoreMonitoringMIB-SMIV2	Contient les définitions des objets gérés accessibles et récupérables à l'aide de l'outil de gestion SNMP.
BES-EC-MIB-SMIV2	Contient les définitions des objets gérés, des déroutements et des notifications émis par les composants de connectivité d'entreprise suivants de BlackBerry UEM : • BlackBerry Affinity Manager • BlackBerry Dispatcher • BlackBerry MDS Connection Service • BlackBerry Router

Compiler la MIB et configurer l'outil de gestion SNMP

Pour permettre au logiciel d'analyse SNMP de votre organisation d'analyser les composants BlackBerry UEM, vous devez utiliser l'outil de gestion SNMP afin de compiler les fichiers MIB de BlackBerry UEM. Si l'outil ne comprend pas de compilateur de MIB, installez-en un sur l'ordinateur qui héberge l'outil.

Avant de commencer : pour plus d'informations sur l'utilisation de l'outil afin de compiler une MIB, reportez-vous à la documentation de l'outil de gestion SNMP.

1. Sur l'ordinateur qui héberge BlackBerry UEM, accédez à *<lecteur>*\Program Files\BlackBerry\UEM\Monitoring\bin\mib.

2. Utilisez l'outil de gestion SNMP (ou le compilateur de MIB installé séparément) pour compiler les fichiers .mib.

Utiliser SNMP pour surveiller les composants

Pour contrôler les composants suivants avec SNMP, vous devez configurer les paramètres dans la console de ge stion BlackBerry UEM.

- BlackBerry UEM Core
- BlackBerry Secure Connect Plus
- BlackBerry Secure Gateway

BlackBerry UEM Core comprend plusieurs sous-composants responsables de la gestion des périphériques. Black Berry Secure Connect Plus fournit un tunnel IP sécurisé entre les applications d'espace de travail sur BlackBerry 1 0, l'espace de KNOX Workspace et les appareils Android disposant d'un profil professionnel et du réseau de votre entreprise. BlackBerry Secure Gateway fournit une connexion sécurisée pour les appareils iOS au serveur de mess agerie de votre entreprise via BlackBerry Infrastructure.

Configurer SNMP pour surveiller les composants

Pour utiliser SNMP afin de surveiller BlackBerry UEM Core, BlackBerry Secure Connect Plus, BlackBerry Secure Ga teway ou BlackBerry Cloud Connector, vous devez configurer les paramètres requis dans la console de gestion.

1. Sur la barre de menus, cliquez sur **Paramètres > Infrastructure > SNMP**.
2. Développez **Paramètres globaux** et cochez la case **Activer la surveillance SNMP**.
3. Dans le champ **Communauté**, remplacez le paramètre par défaut en entrant un nouveau nom de communauté.
4. Dans le champ Adresse IP, saisissez l'adresse IPv4 UDP du serveur où est installé l'outil de gestion des dérout ements.
5. Dans le champ **Port**, saisissez le numéro de l'outil de gestion des déroutements. Le numéro de port par défaut est 1620.
6. Cliquez sur **Enregistrer**.
7. Développez chaque nom d'instance BlackBerry UEM. Si nécessaire, vous pouvez modifier les numéros de port que vous souhaitez que BlackBerry UEM utilise pour écouter les demandes de données SNMP. Les numéros d e port attribués par défaut sont les suivants :
   - BlackBerry UEM Core: 1610
   - BlackBerry Secure Connect Plus: 1611
   - BlackBerry Secure Gateway: 1612
   - BlackBerry Cloud Connector: 1613

   Remarque : Pour modifier le numéro de port de BlackBerry Cloud Connector, vous devez modifier la valeur de `com.rim.platform.mdm.zed.snmp.monitoring.udpport` dans la base de données BlackBerry U EM.
8. Cliquez sur **Enregistrer**.

À la fin : Effectuez l'une des tâches suivantes :

- Si vous activez le contrôle de BlackBerry UEM Core, dans les services Windows, redémarrez le service **BlackBe rry UEM - UEM Core**.
- Si vous activez le contrôle de BlackBerry Secure Connect Plus, dans les services Windows, redémarrez le servi ce **BlackBerry UEM - BlackBerry Secure Connect Plus**.

- Si vous activez le contrôle de BlackBerry Secure Gateway, dans les services Windows, redémarrez le service **BlackBerry UEM - BlackBerry Secure Gateway**.
- Si vous activez le contrôle de BlackBerry Cloud Connector, dans les services Windows, redémarrez le service **BlackBerry UEM - BlackBerry Cloud Connector**.

Glossaire

ADSI	Active Directory Service Interfaces
APNs	Apple Push Notification service (Service Apple Push Notification)
BES5	BlackBerry Enterprise Server 5
BES10	BlackBerry Enterprise Service 10
BlackBerry UEM instance	A BlackBerry UEM instance refers to one installation of the BlackBerry UEM Core and all associated BlackBerry UEM components that communicate with it. The components can be installed on the same server or multiple servers. There can be more than one BlackBerry UEM instance in a BlackBerry UEM domain.
BlackBerry UEM domain	A BlackBerry UEM domain consists of a BlackBerry UEM database and a BlackBerry Control database and any BlackBerry UEM instances that connect to them.
BES12	BlackBerry Enterprise Service 12
Instance de BES12	Le terme « instance de BES12 » désigne tous les composants BES12 installés sur un ordinateur, à l'exception de BlackBerry Router, qui est un composant facultatif installé séparément. Une instance de BES12 est parfois appelée « unité d'échelle ».
CAS	Client Access Server (serveur d'accès client)
CSR	Certificate Signing Request (demande de signature du certificat)
DEP	Programme d'inscription des appareils
DNS	Domain Name System (système DNS)
FQDN	Fully Qualified Domain Name (nom de domaine complet)
HTTPS	Hypertext Transfer Protocol over Secure Sockets Layer
IIS	Internet Information Services (services Internet)
LDAP	Lightweight Directory Access Protocol (protocole LDAP)

MIB	Management Information Base (base d'informations de gestion)
MMC	Microsoft Management Console
OID	identifiant d'objet
PAC	Proxy Auto-Configuration (configuration automatique de proxy)
PAP	Push Access Protocol (protocole PAP)
SCEP	Simple Certificate Enrollment Protocol (service d'inscription de périphériques réseau)
SMTP	Le protocole SMTP (Simple Mail Transfer Protocol) est un protocole TCP/IP utilisé avec les protocoles POP ou IMAP pour envoyer et recevoir des e-mails sur un réseau, par exemple Internet.
SNMP	Simple Network Management Protocol (protocole SNMP)
SPN	Un nom principal de service (SPN) est l'attribut d'un utilisateur ou groupe Microsoft Active Directory qui prend en charge l'authentification mutuelle entre un client d'un service Kerberos et le service Kerberos. Un compte Microsoft Active Directory peut avoir un ou plusieurs SPN.
SRP	Server Routing Protocol (protocole SRP)
SSL	Secure Sockets Layer (protocole SSL)
TCP	Transmission Control Protocol (protocole de contrôle de transmissions)
TCP/IP	Le protocole TCP/IP (Transmission Control Protocol/Internet Protocol) est un ensemble de protocoles de communication utilisé pour transmettre des données sur des réseaux, par exemple Internet.
TLS	Transport Layer Security (sécurité de la couche de transport)

Informations juridiques

PRODUITS ET SERVICES MENTIONNÉS AUX PRÉSENTES Y COMPRIS SANS LIMITATION LES DOMMAGES SUIVANTS : DOMMAGE DIRECT, CONSÉCUTIF, EXEMPLAIRE, FORTUIT, INDIRECT, SPÉCIAL, PUNITIF OU AGGRAVÉE, DOMMAGES-INTÉRÊTS POUR PERTE DE PROFITS OU DE REVENUS, ÉCHEC DE RÉALISER TOUT PRÉVU DES ÉCONOMIES, INTERRUPTION D'ACTIVITÉ, PERTES D'INFORMATIONS COMMERCIALES, PERTE D'OPPORTUNITÉ COMMERCIALE, DE CORRUPTION OU DE PERTE DE DONNÉES, PANNES POUR TRANSMETTRE OU RECEVOIR N'IMPORTE QUEL DA TA, PROBLÈMES LIÉS À TOUTES LES APPLICATIONS UTILISANT EN CONJONCTION AVEC BLACKBERRY PRODUITS OU SERVICES, DURÉE D'INDISPONIBILITÉ DES COÛTS, PERTE D'USAGE DU BLACKBERRY, PRODUITS, SERVICES OU TOUTE PARTIE DE CELLE-CI OU DE TOUT SERVICE DE TEMPS D'ANTENNE, COÛT DE MARCHANDISES DE REMPLACEMENT, LES COÛTS DE COUVERTURE, INSTALLATIONS OU SERVICES, COÛT DU CAPITAL OU AUTRES PERTES PÉCUNIAIRES SEMBLABLES, SI CES DOMMAGES ONT ÉTÉ PRÉVUES OU IMPRÉVUES, ET MÊME SI LE BLACKBERRY A ÉTÉ AVISÉ DE LA DEMAND Y DE TELS DOMMAGES.

DANS LA MESURE MAXIMALE PERMISE PAR LA LOI APPLICABLE DANS VOTRE JURIDICTION, BLACKBERRY N'AURA AUCUNE AUTRE OBLIGATION, OBLIGATION OU RESPONSABILITÉ QUE CE SOIT EN CONTRAT, UN TORT, OU AUTREMENT VOUS Y COMPRIS TOUTE RESPONSABILITÉ POUR NÉGLIGENCE OU STRICT RESPONSABILITÉ CIVILE.

LES LIMITATIONS ET EXCLUSIONS CI-DESSUS SERONT APPLIQUENT : (A) INDÉPENDAMMENT DE LA NATURE DE LA CAUSE D'ACTION, DEMANDE OU ACTION PAR VOUS, Y COMPRIS MAIS NON LIMITÉ À B PORTÉE DE CONTRAT, NÉGLIGENCE, RESPONSABILITÉ DÉLICTUELLE, RESPONSABILITÉ STRICTE OU TOUTE AUTRE THÉORIE JURIDIQUE ET DOIVENT SURVIVRE À UNE INEXÉCUTION FONDAMENTALE OU BRE DOULEURS OU L'ÉCHEC DE L'OBJECTIF ESSENTIEL DU PRÉSENT ACCORD OU DE TOUTE MESURE CORRECTIVE QU'IL CONTIENT ; ET (B) À BLACKBERRY ET SES SOCIÉTÉS AFFILIÉES, LEURS SUCCESSEURS, LES AYANTS DROIT, LES AGENTS, LES FOURNISSEURS (Y COMPRIS LES TEMPS D'ANTENNE SERVICE P ROVIDERS), DISTRIBUTEURS DE BLACKBERRY (Y COMPRIS LES FOURNISSEURS DE SERVICES DE TEMPS D'ANTENNE) AGRÉÉS ET LEURS DIRECTEURS RESPECTIFS, EMPL OY EES ET LES ENTREPRENEURS INDÉPENDANTS.

OUTRE LES LIMITATIONS ET EXCLUSIONS VISÉES CI-DESSUS, EN AUCUN CAS, N'IMPORTE QUEL DIRIGEANT, EMPLOYÉ, AGENT, DISTRIBUTEUR, FOURNISSEUR, ENTREPRENEUR INDÉPENDANT DE BLACKBERRY OU TOUT AFFILIÉ DE BLACKBERRY A TOUTE RESPONSABILITÉ DÉCOULANT D'OU LIÉS À LA DOCUMENTATION.

Avant de souscrire pour, installant ou utilisant des produits tiers et les Services, il est de votre responsabilité de vous assurer que votre fournisseur de service de temps d'antenne a accepté de prend en charge toutes leurs fonctionnalités. Certains fournisseurs de services de temps d'antenne ne pourraient pas offrir fonctionnalité de navigation Internet avec un abonnement à le BlackBerry® Interne t Service. Vérifiez auprès de votre fournisseur de services pour la disponibilité, des arrangements, des plans de service et des caractéristiques de l'itinérance. Installation ou l'utilisation des Services et produits tiers avec les produits et les services de BlackBerry peut exiger un ou plusieurs brevets, marque, droit d'auteur, ou d'autres licences afin d'éviter la contrefaçon ou violation des droits de tiers. Vous êtes seul responsable de déterminer s'il faut utiliser des produits tiers, et Services, si les licences de tiers sont tenus de le faire. Si vous êtes responsable de l'acquisition. Vous ne devriez pas installer ou utiliser les Services et produits tiers jusqu'à ce que toutes les autorisations nécessaires ont été acquis. Tous les produits de tiers et les Services qui sont fournis avec les produits et les services de BlackBerry sont fournis à titre utilitaire à vous et sont fournis « Tel quel » avec aucune conditions implicites ou explicites, endossements, garanties, représentations ou garantie d'aucune genre de BlackBerry et BlackBerry n'assume aucune responsabilité quelle qu'elle soit, en relation avec celui-ci. Votre utilisation des Services et des produits de tiers est régie par et sous réserve de vous accepta nt les conditions de licen séparé SSE et autres accords applicables s'y rapportant avec les tierces parties, sauf dans la mesure expressément couverte par une licence ou d'autre accord avec BlackBerry.

Les conditions d'utilisation de tout produit BlackBerry ou service figurent dans une licence distincte ou de toute autre entente avec BlackBerry applicables s'y rapportant. RIEN DANS LA PRÉSENTE DOCUMENTATION VISE À REMPLACER TOUTE ENTENTE ÉCRITE EXPRESSE OU GARANTIES FOURNIES PAR BLACKBERRY POUR UNE PARTIE DE N'IMPORTE QUEL BLACKBERRY PRODUIT OU SERVICE AUTRE QUE DE CETTE DOCUMENTATION.

BlackBerry Enterprise Software intègre certains logiciels de tierce partie. La licence et les informations de copyright associées à ce logiciel est disponible àhttp://Worldwide.BlackBerry.com/legal/thirdpartysoftware.jsp.

BlackBerry Limited 2200, Avenue University est Waterloo, Ontario Canada N2K 0 a 7 BlackBerry UK Limited 200 Ba th Road Slough, Berkshire SL1 3XE United Kingdom publié au Canada