BlackBerry UEM Cloud

Configuration

Table des matières

Première configuration de BlackBerry UEM Cloud

Le tableau suivant récapitule les tâches de configuration décrites dans ce guide. Les tâches sont facultatives en fonction des besoins de votre entreprise. Utilisez ce tableau pour déterminer les tâches de configuration requises.

Une fois les tâches appropriées accomplies, vous êtes prêt pour configurer les administrateurs, définir les commandes des terminaux, créer les utilisateurs et les groupes, et activer les terminaux.

Tâche	Description
Connectez-vous à l'annuaire d'entreprise sur site de votre organisation et activez les fonctions de connectivité sécurisée	Vous pouvez installer, activer et configurer BlackBerry Connectivity Node de manière à permettre l'accès à l'annuaire d'entreprise de votre organisation et d'activer les fonctions de connectivité sécurisée.
Configurer BlackBerry Connectivity Node pour envoyer les données via un serveur proxy	Vous pouvez configurer les composants BlackBerry Connectivity Node de manière à envoyer les données via un serveur proxy situé dans l'environnement de votre entreprise.
Connecter BlackBerry UEM à Microsoft Azure	Si vous souhaitez connecter BlackBerry UEM à Azure Active Directory, utilisez BlackBerry UEM pour déployer iOS et les applications Android gérées par Microsoft Intune, ou gérez des applications Windows 10 dans BlackBerry UEM, connectez BlackBerry UEM à Microsoft Azure.
Lier les groupes d'annuaire d'entreprise aux groupes BlackBerry UEM	Si vous connectez BlackBerry UEM à votre annuaire d'entreprise, vous pouvez activer les groupes reliés à l'annuaire pour simplifier l'intégration et la gestion des utilisateurs.
Obtenir et enregistrer un certificat APNs	Si vous souhaitez gérer et envoyer des données aux terminaux iOS ou macOS, vous devez vous procurer un fichier CSR signé auprès de BlackBerry, l'utiliser pour obtenir un certificat APNs auprès de Apple et enregistrer le certificat APNs auprès du domaine BlackBerry UEM.
Configuration de BlackBerry UEM pour la prise en charge des terminaux Android qui possèdent un profil professionnel	Pour prendre en charge les terminaux Android qui possèdent un profil professionnel, vous devez configurer votre domaine G Suite ou Google Cloud pour la prise en charge de fournisseurs de gestion de terminaux mobiles tiers et configurer BlackBerry UEM pour communiquer avec votre domaine G Suite ou Google Cloud.
Configurer BlackBerry UEM pour le programme d'inscription des appareils Apple	Si vous voulez utiliser la console de gestion de BlackBerry UEM pour gérer les terminaux iOS que votre organisation a achetés auprès de Apple pour DEP, vous devez configurer cette fonctionnalité.
Configurer BlackBerry UEM Cloud pour la prise en charge des applications BlackBerry Dynamics	Si vous souhaitez autoriser les utilisateurs à utiliser des applications BlackBerry Dynamics, vous pouvez configurer BlackBerry UEM Cloud pour prendre en charge ces applications.
Migrer des utilisateurs, groupes et autres données depuis BlackBerry UEM	Vous pouvez utiliser la console de gestion pour migrer les utilisateurs, terminaux, groupes et autres données depuis une base de données BES12 ou BlackBerry UEM source sur site.

Droits d'administrateur requis pour configurer BlackBerry UEM

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

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

Obtention et activation des licences

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

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

Installation de BlackBerry Connectivity Node pour vous connecter aux ressources derrière le pare-feu de votre entreprise

BlackBerry Connectivity Node est un ensemble de composants que vous pouvez installer sur un ordinateur dédié pour activer des fonctionnalités supplémentaires pour BlackBerry UEM Cloud. Les composants suivants sont inclus dans BlackBerry Connectivity Node.

Composant	Objectif
BlackBerry Cloud Connector	BlackBerry Cloud Connector autorise BlackBerry UEM Cloud à accéder au répertoire d'entreprise sur site de votre organisation. Vous pouvez créer des comptes utilisateur de répertoire en recherchant et important des données utilisateur depuis le répertoire de l'entreprise. Les données utilisateur sont synchronisées avec l'e répertoire en fonction de la planification configurée. BlackBerry UEM Cloud doit être en mesure d'accéder à votre répertoire d'entreprise si vous souhaitez utiliser SCEP. Les utilisateurs du répertoire peuvent utiliser leurs informations d'identification d'accès au répertoire pour accéder à BlackBerry UEM Self-Service. Si vous attribuez un rôle d'administration à des utilisateurs du répertoire, les utilisateurs peuvent également utiliser les informations d'identification du répertoire pour se connecter à la console de gestion. BlackBerry Cloud Connector permet également à un connecteur PKI d'envoyer des certificats aux applications BlackBerry Dynamics. Pour plus d'informations, reportez-vous à Connecter BlackBerry UEM à un connecteur PKI BlackBerry Dynamics.
BlackBerry Proxy	BlackBerry Proxy maintient une connexion sécurisée entre votre organisation et BlackBerry Dynamics NOC, qui permet aux applications BlackBerry Dynamics de communiquer en toute sécurité avec les ressources de votre organisation derrière le pare-feu. Il prend également en charge BlackBerry Dynamics Direct Connect, qui permet aux données d'application de contourner BlackBerry Dynamics NOC. Pour plus d'informations, reportez-vous à Configuration de BlackBerry UEM Cloud pour prendre en charge les applications BlackBerry Dynamics.
BlackBerry Secure Connect Plus	BlackBerry Secure Connect Plus permet aux utilisateurs d'accéder à des ressources professionnelles derrière le pare-feu de votre organisation tout en assurant la sécurité des données à l'aide des protocoles standard et du cryptage de bout en bout. Pour plus d'informations, reportez-vous au contenu relatif à l'administration.
BlackBerry Secure Gateway	BlackBerry Secure Gateway fournit aux terminaux iOS qui utilisent le type d'activation Contrôles MDM une connexion sécurisée au serveur de messagerie de votre organisation via BlackBerry Infrastructure. Pour plus d'informations, reportez-vous au contenu relatif à l'administration.

Composant	Objectif
BlackBerry Gatekeeping Service	BlackBerry Gatekeeping Service facilite le contrôle des terminaux ouvant accéder à Exchange ActiveSync. Pour plus d'informations, reportez-vous au contenu relatif à l'administration.

L'installation et les fichiers d'activation de BlackBerry Connectivity Node sont disponibles dans la console de gestion. Vous pouvez utiliser ces fichiers pour installer de nouvelles instances de BlackBerry Connectivity Node et mettre à niveau les instances existantes. Vous devez mettre à niveau les instances existantes de BlackBerry Connectivity Node après le déploiement d'une nouvelle version de BlackBerry UEM Cloud.

Informations de planification BlackBerry Connectivity Node

Avant d'installer BlackBerry Connectivity Node, tenez compte des informations suivantes.

Matériel

BlackBerry Connectivity Node doit être installé sur un ordinateur dédié, réservé à des fins techniques, et non sur un ordinateur utilisé pour le travail quotidien. L'ordinateur doit disposer d'un accès à Internet et à votre annuaire d'entreprise. Vous ne pouvez pas installer d'instance de BlackBerry Connectivity Node sur un ordinateur qui héberge déjà une instance de BlackBerry UEM sur site.

L'ordinateur qui héberge BlackBerry Connectivity Node doit répondre à la configuration matérielle suivante :

- 6 cœurs de processeur, E5-2670 (2,6 GHz), E5-2683 v4 (2,1 GHz) ou équivalent
- 12 Go de mémoire disponible
- 64 Go d'espace disque

Si vous activez le mode Performances de service unique, l'ordinateur qui héberge BlackBerry Connectivity Node doit répondre à la configuration matérielle suivante :

BlackBerry Connectivity Node avec le mode Performances de service unique activé pour BlackBerry Proxy uniquement	• 6 cœurs de processeur, E5-2670 (2,6 GHz), E5-2683 v4 (2,1 GHz) ou équivalent • 12 Go de mémoire disponible • 64 Go d'espace disque
BlackBerry Connectivity Node avec le mode Performances de service unique activé pour BlackBerry Secure Connect Plus uniquement	• 4 cœurs de processeur, E5-2670 (2,6 GHz), E5-2683 v4 (2,1 GHz) ou équivalent • 12 Go de mémoire disponible • 64 Go d'espace disque
BlackBerry Connectivity Node avec le mode Performances de service unique activé pour BlackBerry Secure Gateway uniquement	• 8 cœurs de processeur, E5-2670 (2,6 GHz), E5-2683 v4 (2,1 GHz) ou équivalent • 12 Go de mémoire disponible • 64 Go d'espace disque

Logiciel

Pour vérifier que votre environnement est conforme aux exigences d'installation de BlackBerry Connectivity Node, reportez-vous à la matrice de compatibilité.

Évolutivité et haute disponibilité

Chaque instance de BlackBerry Connectivity Node peut prendre en charge jusqu'à 5 000 terminaux. Vous pouvez installer des instances de BlackBerry Connectivity Node supplémentaires pour prendre en charge jusqu'à 50 000 terminaux supplémentaires.

Vous pouvez installer une ou plusieurs instances de BlackBerry Connectivity Node pour assurer la redondance. Vous devez installer chaque instance sur un ordinateur dédié. Utilisez la même configuration de répertoire d'entreprise pour toutes les instances.

Déployez plusieurs instances de BlackBerry Connectivity Node dans un groupe de serveurs pour permettre une haute disponibilité et un équilibrage de la charge.

Vous pouvez également désigner chaque BlackBerry Connectivity Node d'un groupe de serveurs pour gérer un seul type de connexion : BlackBerry Secure Connect Plus uniquement, BlackBerry Secure Gateway uniquement ou BlackBerry Proxy uniquement. Cette opération libère des ressources de serveur pour permettre de réduire le nombre de serveurs requis pour le même nombre d'utilisateurs ou de conteneurs. Chaque instance de BlackBerry Connectivity Node activé pour le mode Performances de service unique peut prendre en charge jusqu'à 10 000 terminaux.

Étapes à suivre pour installer et activer BlackBerry Connectivity Node

Pour installer et activer BlackBerry Connectivity Node, effectuez les opérations suivantes :

1	Vérifiez que votre organisation répond aux conditions préalables à l'installation de BlackBerry Connectivity Node.
2	Téléchargez les fichiers d'installation et d'activation pour BlackBerry Connectivity Node à partir de la console de gestion.
3	Installez, activez et configurez BlackBerry Connectivity Node.
4	Si nécessaire, configurez les paramètres de proxy des composants BlackBerry Connectivity Node.
5	Effectuez une configuration supplémentaire des applications BlackBerry Secure Connect Plus, BlackBerry Secure Gateway, BlackBerry Gatekeeping Service et BlackBerry Dynamics.

Conditions préalables : Installation de BlackBerry Connectivity Node

- Vérifiez que l'ordinateur exécute Windows PowerShell 2.0 ou version ultérieure. Il s'agit d'une condition requise pour l'application d'installation pour installer RRAS pour BlackBerry Secure Connect Plus et BlackBerry Gatekeeping Service.

  Remarque : Si l'application de configuration ne peut pas installer RRAS sur l'ordinateur, vous devez arrêter l'installation, installer RRAS manuellement, puis redémarrer l'installation.
- Choisissez un compte de répertoire disposant des autorisations de lecture pour chaque connexion au répertoire configurée que BlackBerry Cloud Connector peut utiliser pour accéder aux répertoires d'entreprise.

- Utilisez un compte BlackBerry UEM Cloud disposant des autorisations de télécharger les fichiers d'installation et de configuration de BlackBerry Connectivity Node (par exemple administrateur de sécurité).
- Utilisez un compte Windows disposant des autorisations nécessaires pour installer et configurer le logiciel sur l'ordinateur qui hébergera BlackBerry Connectivity Node.
- Vérifiez que les ports de sortie suivants sont ouverts dans le pare-feu de votre organisation, afin que les composants BlackBerry Connectivity Node (et tout serveur proxy associé) puissent communiquer avec BlackBerry Infrastructure (*<région>*.bbsecure.com, par exemple na.region.com ou eu.region.com) :
  - 443 (HTTPS) pour activer BlackBerry Connectivity Node
  - 3101 (TCP) pour toute autre connexion sortante

Définir une variable d'environnement pour l'emplacement Java

BlackBerry UEM nécessite l'installation d'une implémentation JRE 8 sur les serveurs sur lesquels vous allez installer BlackBerry UEM, et qu'une variable d'environnement pointe vers l'emplacement d'accueil Java. Pour plus d'informations sur les versions JRE prises en charge, reportez-vous à la matrice de compatibilité. Au début de l'installation, BlackBerry UEM vérifie qu'il peut trouver Java. Si vous avez installé l'environnement d'exécution Oracle Java SE à l'emplacement par défaut, BlackBerry UEM le recherche et définit automatiquement la variable d'environnement. Si BlackBerry UEM ne trouve pas Java, l'application de configuration s'arrête et vous devez définir une variable d'environnement pour l'emplacement Java et vous assurer que le dossier bin de Java est inclus dans la variable système Path.

Rendez-vous sur support.blackberry.com pour consulter l'article 52117.

Avant de commencer : Vérifiez que vous avez installé une instance de JDK prise en charge sur le serveur sur lequel vous allez installer BlackBerry UEM.

1. Ouvrez la boite de dialogue **Paramètres système avancés Windows**.
2. Cliquez sur **Variables d'environnement**.
3. Dans la liste **Variables système**, cliquez sur **Nouveau**.
4. Dans le champ **Nom de variable**, saisissez `BB_JAVA_HOME`.
5. Dans le champ **Valeur de la variable**, saisissez le chemin d'accès au dossier JRE (Java Runtime Environment) et cliquez sur **OK**.
6. Dans la liste **Variables système**, sélectionnez **Path** et cliquez sur **Modifier**.
7. Si le chemin n'inclut pas le dossier bin de Java, cliquez sur **Nouveau** et ajoutez `%BB_JAVA_HOME%\bin` au chemin.
8. Déplacez l'entrée %BB_JAVA_HOME%\bin suffisamment haut dans la liste pour qu'elle ne soit pas remplacée par une autre entrée, puis cliquez sur **OK**.

Installation et mise à niveau de BlackBerry Connectivity Node

Suivez les instructions de cette section pour installer ou mettre à niveau BlackBerry Connectivity Node.

Vous pouvez installer une ou plusieurs instances de BlackBerry Connectivity Node pour assurer la redondance.

Vous devez installer chaque instance sur un ordinateur dédié.

Vous pouvez configurer une ou plusieurs connexions au répertoire, mais si vous avez plusieurs BlackBerry Connectivity Node, toutes les connexions au répertoire doivent être configurées de la même manière. Si une connexion au répertoire est manquante ou mal configurée, ce BlackBerry Connectivity Node apparaît comme désactivé dans la console de gestion.

Si vous avez plusieurs BlackBerry Connectivity Node, vous devez tous les mettre à niveau vers la même version logicielle.

Remarque : Si vous mettez à niveau plusieurs BlackBerry Connectivity Node, les services de répertoire sont désactivés après la mise à niveau du premier nœud jusqu'à ce que tous les nœuds soient mis à niveau vers la même version.

Télécharger les fichiers d'installation et d'activation de BlackBerry Connectivity Node

1. Dans la console de gestion, cliquez sur **Paramètres > Intégration externe > Configuration de BlackBerry Connectivity Node** dans la barre de menus.
2. Cliquez sur .
3. Cliquez sur **Télécharger**.
4. Sur la page de téléchargement du logiciel, répondez aux questions requises et cliquez sur **Télécharger**. Enregistrez le package d'installation.
5. Pour ajouter l'instance de BlackBerry Connectivity Node à un groupe de serveurs existant lorsque vous l'activez, dans la liste déroulante **Groupe de serveurs**, cliquez sur le groupe de serveurs qui convient.
6. Cliquez sur **Générer**.
7. Enregistrez le fichier d'activation (.txt).

   Le fichier d'activation est valide 60 minutes. Si vous attendez plus de 60 minutes avant d'utiliser le fichier d'activation, vous devez générer un nouveau fichier d'activation. Seul le dernier fichier d'activation est valide.

À la fin : Installer et configurer BlackBerry Connectivity Node.

Installer et configurer BlackBerry Connectivity Node

Avant de commencer : Télécharger les fichiers d'installation et d'activation de BlackBerry Connectivity Node.

1. Ouvrez le fichier d'installation (.exe) de BlackBerry Connectivity Node que vous avez téléchargé à partir de la console de gestion.

   Si un message Windows s'affiche pour vous demander l'autorisation d'apporter des modifications sur l'ordinateur, cliquez sur **Oui**.
2. Choisissez votre langue. Cliquez sur **OK**.
3. Cliquez sur **Suivant**.
4. Sélectionnez votre pays ou région. Lisez et acceptez le contrat de licence. Cliquez sur **Suivant**.
5. Le programme d'installation vérifie que votre ordinateur répond aux exigences d'installation. Cliquez sur **Suivant**.
6. Pour modifier le chemin du fichier d'installation, cliquez sur **...** et accédez au chemin d'accès du fichier que vous souhaitez utiliser. Cliquez sur **Installer**.
7. Lorsque l'installation est terminée, cliquez sur **Suivant**.

   L'adresse de la console BlackBerry Connectivity Node s'affiche (http:/localhost:8088). Cliquez sur le lien et enregistrez le site dans votre navigateur.
8. Sélectionnez votre langue. Cliquez sur **Suivant**.
9. Lorsque vous activez BlackBerry Connectivity Node, celui-ci envoie les données via le port 443 (HTTPS) à BlackBerry Infrastructure (par exemple na.bbsecure.com ou eu.bbsecure.com). Une fois activé, BlackBerry Connectivity Node utilise le port 3101 (TCP) pour toutes les autres connexions sortantes via BlackBerry Infrastructure. Si vous voulez envoyer des données depuis BlackBerry Connectivity Node via un serveur proxy existant derrière le pare-feu de votre organisation, cliquez sur **Cliquez ici pour configurer les paramètres proxy de l'environnement de votre organisation**, sélectionnez l'option **Serveur proxy** et effectuez l'une des tâches suivantes :

   - Pour envoyer des données d'activation via un serveur proxy, dans les champs **Proxy d'inscription**, saisissez le FQDN ou l'adresse IP et le numéro de port du serveur proxy. Le serveur proxy doit être capable d'envoyer

des données via le port 443 à bbsecure.com (par exemple na.bbsecure.com ou eu.bbsecure.com). Cliquez sur **Enregistrer**.

- Pour envoyer d'autres connexions sortantes depuis les composants de BlackBerry Connectivity Node via un serveur proxy, saisissez le FQDN ou l'adresse IP et le numéro de port du serveur proxy dans les champs appropriés. Le serveur proxy doit être capable d'envoyer des données via le port 3101 à bbsecure.com (par exemple na.bbsecure.com ou eu.bbsecure.com). Cliquez sur **Enregistrer**.

10. Dans le champ **Nom convivial**, saisissez un nom pour BlackBerry Connectivity Node. Cliquez sur **Suivant**.
11. Cliquez sur **Parcourir**. Sélectionnez le fichier d'activation que vous avez téléchargé à partir de la console de gestion.
12. Cliquez sur **Activer**.

    Si vous souhaitez ajouter une instance de BlackBerry Connectivity Node à un groupe de serveurs existant lorsque vous l'activez, le pare-feu de votre organisation doit autoriser les connexions à partir de ce serveur sur le port 443 via BlackBerry Infrastructure (par exemple na.bbsecure.com ou eu.bbsecure.com) pour activer BlackBerry Connectivity Node et dans la même région bbsecure.com que l'instance principale de BlackBerry Connectivity Node.
13. Cliquez sur + et sélectionnez le type de répertoire d'entreprise que vous souhaitez configurer.
14. Suivez les étapes pour le type d'annuaire de votre organisation :

Type d'annuaire	Étapes
Microsoft Active Directory	**a.** Dans le champ **Nom de connexion**, saisissez un nom pour cette connexion au répertoire d'entreprise. **Remarque :** Si vous avez configuré un répertoire Microsoft Azure, ce nom de connexion doit être différent du nom de la connexion au répertoire Azure. **Remarque :** Vous ne pouvez pas modifier le nom après avoir enregistré la configuration. **b.** Dans le champ **Nom d'utilisateur**, saisissez le nom d'utilisateur du compte Microsoft Active Directory. **c.** Dans le champ **Domaine**, saisissez le FQDN du domaine qui héberge Microsoft Active Directory. Par exemple : domain.example.com. **d.** Dans le champ **Mot de passe**, saisissez le mot de passe du compte Microsoft Active Directory. **e.** Dans la liste déroulante **Détection du contrôleur de domaine**, cliquez sur l'une des opérations suivantes : • Si vous souhaitez utiliser la détection automatique, cliquez sur **Automatique**. • Si vous souhaitez spécifier l'ordinateur du contrôleur de domaine, cliquez sur **Sélectionner dans la liste ci-dessous**. Cliquez sur + et saisissez le FQDN de l'ordinateur. Répétez cette étape pour ajouter d'autres ordinateurs. **f.** Dans le champ **Base de recherche du catalogue global**, saisissez la base de recherche à laquelle vous souhaitez accéder (par exemple, OU=Users,DC=example,DC=com). Pour effectuer des recherches dans le catalogue global, laissez le champ vide. **g.** Dans la liste déroulante **Détection du catalogue global**, cliquez sur l'une des opérations suivantes : • Si vous souhaitez utiliser la détection automatique de catalogue, cliquez sur **Automatique**. • Si vous souhaitez spécifier l'ordinateur du catalogue, cliquez sur **Sélectionner dans la liste ci-dessous**. Cliquez sur + et saisissez le FQDN de l'ordinateur. Répétez cette étape pour ajouter d'autres ordinateurs, si nécessaire. **h.** 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 Cloud ait accès, dans la section **Liste des forêts de comptes**, cliquez sur +. Spécifiez le nom de la forêt, le nom du domaine de l'utilisateur (l'utilisateur peut appartenir à n'importe quel domaine de la forêt de comptes), le nom d'utilisateur et le mot de passe. **i.** 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. **j.** Cliquez sur **Enregistrer**.

Type d'annuaire	Étapes
Annuaire LDAP	**a.** Dans le champ **Nom de connexion**, saisissez un nom pour cette connexion au répertoire d'entreprise. **Remarque :** Si vous avez configuré un répertoire Microsoft Azure, ce nom de connexion doit être différent du nom de la connexion au répertoire Azure. **Remarque :** Vous ne pouvez pas modifier le nom après avoir enregistré la configuration. **b.** Dans la liste déroulante **Détection du serveur LDAP**, cliquez sur l'une des opérations suivantes : • Si vous souhaitez utiliser la détection automatique, cliquez sur **Automatique**. Dans le champ **Nom du domaine DNS**, saisissez le nom du domaine DNS. • Si vous souhaitez spécifier l'ordinateur LDAP, cliquez sur **Sélectionner le serveur dans la liste ci-dessous**. Cliquez sur + et saisissez le FQDN de l'ordinateur. Répétez cette étape pour ajouter d'autres ordinateurs. **c.** Dans la liste déroulante **Activer SSL**, choisissez si vous souhaitez activer l'authentification SSL pour le trafic LDAP ou non. Si vous cliquez sur **Oui**, cliquez sur **Parcourir** et sélectionnez le certificat SSL pour l'ordinateur LDAP. **d.** Dans le champ du port **LDAP**, saisissez le numéro de port de l'ordinateur LDAP. **e.** Dans la liste déroulante **Autorisation requise**, choisissez si BlackBerry UEM Cloud doit s'authentifier avec l'ordinateur LDAP. Si vous cliquez sur **Oui**, saisissez le nom d'utilisateur et le mot de passe du compte LDAP. Le nom d'utilisateur doit être en format DN (par exemple, CN=Megan Ball,OU=Sales,DC=example,DC=com). **f.** Dans le champ **Base de recherche**, saisissez la base de recherche à laquelle vous souhaitez accéder (par exemple, OU=Users,DC=example,DC=com). **g.** Dans le champ **Filtre de recherche de l'utilisateur LDAP**, saisissez le filtre que vous voulez utiliser pour les utilisateurs LDAP. Par exemple : (&(objectCategory=person)(objectclass=user)(memberOf=CN=Local,OU=Users,DC=example,DC=com)). **h.** Dans la liste déroulante **Étendue de recherche de l'utilisateur LDAP**, cliquez sur l'une des opérations suivantes : • Si vous souhaitez que les recherches de l'utilisateur s'appliquent à tous les niveaux en dessous du DN de base, cliquez sur **Tous les niveaux**. • Si vous souhaitez limiter les recherches de l'utilisateur à un niveau en dessous du DN de base, cliquez sur **Un niveau**. **i.** Dans le champ **Identificateur unique**, saisissez l'attribut de chaque identificateur unique de l'utilisateur (par exemple, uid). L'attribut doit être immuable et globalement unique pour chaque utilisateur. **j.** Dans le champ **Prénom**, saisissez l'attribut du prénom de chaque utilisateur (par exemple, givenName). **k.** Dans le champ **Nom**, saisissez l'attribut du nom de chaque utilisateur (par exemple, sn). **l.** Dans le champ **Attribut de connexion**, saisissez l'attribut de connexion de chaque utilisateur (par exemple, cn). Cet attribut est utilisé pour la valeur que les utilisateurs saisissent pour se connecter à BlackBerry UEM Self-Service avec leurs informations d'identification d'annuaire. **m.** Dans le champ **Adresse électronique**, saisissez l'attribut de messagerie de chaque utilisateur (par exemple, mail). **n.** Dans le champ **Nom d'affichage**, saisissez l'attribut du nom d'affichage de chaque utilisateur (par exemple, displayName). **o.** 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. Dans la console de gestion, cliquez sur **Paramètres > Intégration externe > Configuration de BlackBerry Connectivity Node**.
16. Dans la section **Étape 4 : tester la connexion**, cliquez sur **Suivant**.

Pour afficher l'état d'une instance de BlackBerry Connectivity Node, dans la console de gestion, sur la barre de menus, cliquez sur **Paramètres > Intégration externe > État de BlackBerry Connectivity Node**.

À la fin :

- Pour installer une deuxième instance de BlackBerry Connectivity Node pour la redondance, téléchargez un autre jeu de fichiers d'installation et d'activation puis répétez cette tâche sur un autre ordinateur. Cette opération doit être effectuée après l'activation de la première instance.
- Vous pouvez configurer une ou plusieurs connexions de répertoire, mais si vous avez plusieurs BlackBerry Connectivity Node, toutes les connexions au répertoire doivent être configurées de la même manière. Si une connexion au répertoire est manquante ou mal configurée, ce BlackBerry Connectivity Node apparaît comme désactivé dans la console de gestion. Vous pouvez faciliter cette tâche en copiant les configurations de connexion de répertoire d'un répertoire BlackBerry Connectivity Node à un autre.
- Si nécessaire, configurez les paramètres de proxy de BlackBerry Connectivity Node. Pour obtenir des instructions, reportez-vous à Configuration de BlackBerry Connectivity Node pour qu'il utilise BlackBerry Router ou un serveur proxy TCP.
- Pour modifier les paramètres de répertoire que vous avez configurés, dans la console BlackBerry Connectivity Node (http:/localhost:8088), cliquez sur **Paramètres généraux > Répertoire d'entreprise**. Cliquez sur ✎ pour la connexion au répertorie.
- Pour envoyer des données via un proxy HTTP avant d'atteindre BlackBerry Dynamics NOC, dans la console BlackBerry Connectivity Node (http://localhost:8088), cliquez sur **Paramètres généraux > BlackBerry Router et proxy**. Cochez la case **Activer le proxy HTTP** et configurez les paramètres de proxy.
- Pour obtenir des instructions sur l'activation de BlackBerry Secure Connect Plus, reportez-vous à la section « Utilisation de BlackBerry Secure Connect Plus pour des connexions sécurisées aux ressources professionnelles » dans le contenu relatif à l'administration.
- Pour plus d'informations sur l'activation de BlackBerry Secure Gateway, reportez-vous à la section « Protection des données de la messagerie électronique à l'aide de BlackBerry Secure Gateway » dans le contenu relatif à l'administration.
- Pour obtenir des instructions sur la configuration de BlackBerry Gatekeeping Service, reportez-vous à la section « Désigner les terminaux autorisés à accéder à Exchange ActiveSync » dans le contenu relatif à l'administration.

Copier les configurations de connexion au répertoire

Si votre environnement comporte plusieurs BlackBerry Connectivity Node s, les connexions au répertoire doivent être configurées de manière identique sur tous les nœuds. Pour faciliter cette tâche, vous pouvez exporter la configuration de la connexion au répertoire à partir d'un BlackBerry Connectivity Node et l'importer dans un autre.

Remarque : Avant de pouvoir importer des configurations de répertoire d'entreprise dans un BlackBerry Connectivity Node, vous devez supprimer toutes les connexions existantes au répertoire d'entreprise de ce nœud.

1. Sur le BlackBerry Connectivity Node à partir duquel vous souhaitez copier la configuration, sur l'écran **Connexion au répertoire d'entreprise**, cliquez sur **Exporter les connexions au répertoire dans un fichier .txt**.

   Un fichier .txt contenant des informations sur les connexions au répertoire d'entreprise est téléchargé sur votre ordinateur.
2. Sur le BlackBerry Connectivity Node vers lequel vous souhaitez copier la configuration, sur l'écran **Connexion au répertoire d'entreprise**, accédez au fichier .txt que vous avez téléchargé.
3. Cliquez sur **Importer des connexions**.

   Les connexions au répertoire d'entreprise sont ajoutées à BlackBerry Connectivity Node.

Modifier les paramètres par défaut des instances de BlackBerry Connectivity Node

Par défaut, BlackBerry Gatekeeping Service de chaque instance de BlackBerry Connectivity Node est actif. Si vous souhaitez que les données de contrôle d'accès soient gérées uniquement par l'instance de BlackBerry Gatekeeping Service installée avec les composants principaux de BlackBerry UEM, vous pouvez modifier le comportement par défaut pour désactiver BlackBerry Gatekeeping Service dans chaque instance. Vous pouvez spécifier les paramètres de journalisation par défaut pour toutes les instances de BlackBerry Connectivity Node. Vous pouvez également activer les paramètres de BlackBerry Secure Gateway pour toutes les instances de BlackBerry Connectivity Node et spécifier le point de terminaison de détection et la ressource de serveur de messagerie que les terminaux iOS exécutant iOS version 13.0 ou versions ultérieures doivent utiliser pour s'authentifier à Microsoft Exchange Online à l'aide de l'authentification moderne.

Les paramètres par défaut s'appliquent à chaque instance de BlackBerry Connectivity Node qui n'appartient pas à un groupe de serveurs. Lorsqu'une instance appartient à groupe de serveurs, elle utilise les paramètres par défaut configurés pour ce groupe.

1. Dans la console de gestion BlackBerry UEM, sur la barre de menus, cliquez sur **Paramètres > Intégration externe > Configuration de BlackBerry Connectivity Node**.
2. Cliquez sur .
3. Pour désactiver BlackBerry Gatekeeping Service dans chaque instance, cochez la case **Remplacer les paramètres de BlackBerry Gatekeeping Service**.
4. Pour configurer les paramètres de journalisation, cochez la case **Remplacer les paramètres de journalisation**. Effectuez l'une des tâches suivantes :
   - Dans la liste déroulante **Niveaux de débogage du journal de serveur**, sélectionnez le niveau de journalisation qui convient.
   - Pour router les évènements du journal vers un serveur syslog, cochez la case **Syslog** et spécifiez le nom d'hôte et le port du serveur syslog.
   - Pour spécifier les limites de taille et d'ancienneté maximales du fichier journal, cochez la case **Activer la destination des fichiers locaux**. Spécifiez la limite de taille (en Mo) et la limite d'ancienneté (en jours).
5. Pour spécifier BlackBerry Secure Gateway dans chaque instance, cochez la case **Remplacer les paramètres BlackBerry Secure Gateway**. Pour les terminaux iOS qui exécutent la version 13.0 ou une version ultérieure et utilisent l'authentification moderne pour se connecter à Microsoft Exchange Online, procédez comme suit pour spécifier le point de terminaison de détection et la ressource de serveur de messagerie :
   a) Cochez la case **Activer OAuth pour l'authentification du serveur de messagerie**.
   b) Dans le champ **Point de terminaison de détection**, spécifiez l'URL à utiliser pour les demandes de détection utilisant OAuth. Saisissez le point de terminaison de détection au format suivant : https://<*fournisseur d'identité*>/.well-known/openid-configuration (par exemple, `https://login.microsoftonline.com/common/.well-known/openid-configuration`) ou `https://login.windows.net/common/.well-known/openid-configuration`).
   c) Dans le champ **Ressource de serveur de messagerie**, spécifiez l'URL de la ressource de serveur de messagerie à utiliser pour les demandes d'autorisation et de jeton via OAuth (par exemple, `https://outlook.office365.com`).
6. Cliquez sur **Enregistrer**.

À la fin : Si vous avez désactivé les instances de BlackBerry Gatekeeping Service et que vous souhaitez les activer à nouveau, cochez la case **Activer BlackBerry Gatekeeping Service**. Chaque instance doit être en mesure d'accéder au serveur de contrôle d'accès de votre organisation.

Mise à niveau de BlackBerry Connectivity Node

Lorsque vous êtes averti d'une mise à jour de BlackBerry UEM Cloud, utilisez les instructions suivantes pour mettre à niveau les composants BlackBerry Connectivity Node avec la dernière version.

1. Sur l'ordinateur qui héberge BlackBerry Connectivity Node, ouvrez la console BlackBerry Connectivity Node (http:/localhost:8088).
2. Enregistrez les paramètres de configuration du répertoire actuel.
3. Connectez-vous à la console de gestion BlackBerry UEM Cloud.
4. Téléchargez les fichiers d'installation et d'activation de BlackBerry Connectivity Node. Pour obtenir des instructions, reportez-vous à Télécharger les fichiers d'installation et d'activation de BlackBerry Connectivity Node.
5. Installez et configurez BlackBerry Cloud Connector à l'aide des informations que vous avez enregistrées à l'étape 2. Pour obtenir des instructions, reportez-vous à Installer et configurer BlackBerry Connectivity Node.

Création d'un groupe de serveurs

Vous pouvez configurer des connexions régionales pour les fonctionnalités de connectivité d'entreprise en déployant une ou plusieurs instances de BlackBerry Connectivity Node dans une région dédiée. Ce processus est connu sous le nom de groupe de serveurs.

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. 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.

Le déploiement de plusieurs instances de BlackBerry Connectivity Node dans un groupe de serveurs permet aussi une haute disponibilité et un équilibrage de la charge.

Vous pouvez installer une ou plusieurs instances de BlackBerry Connectivity Node pour assurer la redondance.

Créer un groupe de serveurs

Avant de commencer : Installer un autre BlackBerry Connectivity Node

1. Sur la barre de menus, cliquez sur **Paramètres > Intégration externe > Configuration de BlackBerry Connectivity Node**.
2. Cliquez sur .
3. Saisissez le nom et la description du profil du groupe de serveurs.
4. Dans la liste déroulante **Pays**, sélectionnez le pays dans lequel une ou plusieurs instances de BlackBerry Connectivity Node seront installées. Les instances de BlackBerry Connectivity Node ajoutées au groupe de serveurs utiliseront la connexion régionale du pays sélectionné vers BlackBerry Infrastructure.

   Remarque : Vous ne pouvez pas modifier ce paramètre une fois le groupe de serveurs créé.
5. Par défaut, chaque instance de BlackBerry Connectivity Node doit être configurée sur les mêmes répertoires d'entreprise. Si vous souhaitez désactiver le connecteur du répertoire d'entreprise pour les instances de BlackBerry Connectivity Node dans le groupe de serveurs, cochez la case **Remplacer les paramètres de service du répertoire**.
6. Par défaut, BlackBerry Gatekeeping Service de chaque instance de BlackBerry Connectivity Node est actif. Si vous souhaitez que les données de contrôle d'accès soient exclusivement gérées par l'instance principale de BlackBerry Connectivity Node, cochez la case **Remplacer les paramètres de BlackBerry Gatekeeping Service** pour désactiver chaque BlackBerry Gatekeeping Service dans le groupe de serveurs.
7. Si vous souhaitez utiliser des paramètres DNS pour le BlackBerry Secure Connect Plus autres que les paramètres par défaut qui sont configurés dans **Paramètres > Infrastructure > BlackBerry Secure Connect Plus**, cochez la case **Remplacer les serveurs DNS**. Procédez comme suit :

a) Dans la section **Serveurs DNS**, cliquez sur +. Saisissez l'adresse du serveur DNS au format décimal séparé par des points (par exemple 192.0.2.0). Cliquez sur **Ajouter**. Si nécessaire, répétez l'opération.

b) Dans la section **Suffixe de recherche DNS**, cliquez sur +. Saisissez le suffixe de recherche DNS (par exemple, domaine.com). Cliquez sur **Ajouter**. Si nécessaire, répétez l'opération.

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

8. Si vous souhaitez configurer les paramètres de journalisation des instances de BlackBerry Connectivity Node du groupe de serveurs, cochez la case **Remplacer les paramètres de journalisation**. Effectuez l'une des tâches suivantes :
   - Dans la liste déroulante **Niveaux de débogage du journal de serveur**, sélectionnez le niveau de journalisation qui convient.
   - Pour router les évènements du journal vers un serveur syslog, cochez la case **Syslog** et spécifiez le nom d'hôte et le port du serveur syslog.
   - Pour spécifier les limites de taille et d'ancienneté maximales du fichier journal, cochez la case **Activer la destination des fichiers locaux**. Spécifiez la limite de taille (en Mo) et la limite d'ancienneté (en jours).
9. Si vous souhaitez désigner BlackBerry Connectivity Node pour un seul type de connexion, cochez la case **Activer le mode Performances de service unique**. Dans le menu déroulant, sélectionnez le type de connexion (**BlackBerry Secure Connect Plus uniquement**, **BlackBerry Secure Gateway uniquement** ou **BlackBerry Proxy uniquement**).
10. Si vous souhaitez spécifier les paramètres BlackBerry Secure Gateway de l'instance de BlackBerry Connectivity Node du groupe de serveurs, cochez la case **Remplacer les paramètres BlackBerry Secure Gateway**. Pour les terminaux iOS exécutant iOS 13.0 ou une version ultérieure qui utilisent l'authentification moderne pour se connecter à Microsoft Exchange Online, spécifiez le point de terminaison de détection et la ressource de serveur de messagerie.
    a) Cochez la case **Activer OAuth pour l'authentification du serveur de messagerie**.
    b) Dans le champ **Point de terminaison de détection**, spécifiez l'URL à utiliser pour les demandes de détection utilisant OAuth pour l'authentification. Saisissez le point de terminaison de détection au format https://<*fournisseur d'identité*>/.well-known/openid-configuration (par exemple, `https://login.microsoftonline.com/common/.well-known/openid-configuration`) ou `https://login.windows.net/common/.well-known/openid-configuration`).
    c) Dans le champ **Ressource du serveur de messagerie**, spécifiez l'URL de la ressource de serveur de messagerie à utiliser pour les demandes d'autorisation et de jeton via OAuth. Par exemple, `https://outlook.office365.com`.
11. Cliquez sur **Enregistrer**.

À la fin :

- Si vous avez désactivé les instances de BlackBerry Gatekeeping Service du groupe de serveurs et que vous souhaitez les activer à nouveau, dans **Paramètres > Intégration externe > Configuration de BlackBerry Connectivity Node**, sélectionnez le groupe de serveurs et cochez la case **Activer BlackBerry Gatekeeping Service**. Chaque instance doit être en mesure d'accéder au serveur de contrôle d'accès de votre organisation.
- Installez et configurez BlackBerry Connectivity Node, puis ajoutez l'instance à un groupe de serveurs.

Gérer les groupes de serveurs

Vous pouvez à tout moment ajouter une instance de BlackBerry Connectivity Node à un groupe de serveurs ou supprimer une instance d'un groupe de serveurs. Si vous ajoutez une instance à un groupe de serveurs, cette instance utilise les paramètres configurés pour ce groupe de serveurs (par exemple, les composants de l'instance utiliseront la connexion régionale spécifiée vers BlackBerry Infrastructure). Si vous supprimez une instance d'un groupe de serveurs, cette instance utilise les paramètres par défaut configurés sur l'écran de

configuration BlackBerry Connectivity Node (reportez-vous à Modifier les paramètres par défaut des instances de BlackBerry Connectivity Node).

1. Dans la console de gestion BlackBerry UEM, sur la barre de menus, cliquez sur **Paramètres > Intégration externe > Configuration de BlackBerry Connectivity Node**.
2. Sélectionnez une instance de BlackBerry Connectivity Node.
3. Effectuez l'une des tâches suivantes :
   a) Pour ajouter une instance à un groupe de serveurs, cliquez sur . Sélectionnez le groupe de serveurs qui convient. Cliquez sur **OK**.
   b) Pour supprimer une instance d'un groupe de serveurs, cliquez sur . Dans la boite de dialogue de confirmation, cliquez sur **OK**.

Dépannage des problèmes de BlackBerry Connectivity Node

Lorsque vous dépannez des problèmes avec BlackBerry Connectivity Node, prenez en compte les problèmes courants suivants.

Pour plus d'informations sur les ressources de référence de BlackBerry, rendez-vous sur l'assistance technique de BlackBerry.

BlackBerry Connectivity Node ne s'active pas avec BlackBerry UEM Cloud

Description

Après avoir téléchargé le fichier d'activation et cliqué sur Activer, vous recevez un message d'erreur indiquant que l'activation a échoué.

Solutions possibles

Effectuez l'une des actions suivantes :

- Vérifiez que vous avez téléchargé le dernier fichier d'activation que vous avez généré dans la console de gestion. Seul le dernier fichier d'activation est valide.
- Les fichiers d'activation expirent au bout de 60 minutes. Générez et téléchargez un nouveau fichier d'activation, puis essayez d'activer de nouveau.
- Rendez-vous sur support.blackberry.com/community pour consulter l'article 38964.

BlackBerry Connectivity Node ne se connecte pas avec le répertoire d'entreprise

Description

Une fois que vous avez spécifié les informations relatives à votre annuaire d'entreprise et cliqué sur Enregistrer, vous recevez un message d'erreur indiquant que BlackBerry Connectivity Node ne peut pas se connecter au répertoire d'entreprise.

Solutions possibles

Effectuez l'une des actions suivantes :

- Si vous avez plusieurs BlackBerry Connectivity Node s, vérifiez qu'ils ont tous la même version du logiciel.

- Vérifiez que vous avez spécifié les paramètres corrects pour le répertoire d'entreprise.
- Vérifiez que tous les BlackBerry Connectivity Node s disposent d'une connexion au répertoire et que les connexions au répertoire sont configurées de manière identique sur tous les BlackBerry Connectivity Node s inscrits.
- Vérifiez que vous avez spécifié les informations de connexion correctes pour le compte de répertoire et que le compte dispose des autorisations nécessaires pour accéder au répertoire d'entreprise.
- Vérifiez que les ports adaptés sont ouverts dans le pare-feu de votre organisation.
- Vérifiez que vous n'avez pas utilisé le même fichier d'activation pour deux installations différentes.
- Vérifiez que vous utilisez le fichier d'activation le plus récent.
- Examinez le fichier journal le plus récent pour obtenir des détails sur l'échec de connexion de BlackBerry Connectivity Node au répertoire d'entreprise. Par défaut, les fichiers journaux de BlackBerry Connectivity Node se trouvent dans <*lecteur:*>:\Program Files\BlackBerry\BlackBerry Connectivity Node\Logs.
- Si vous utilisez Microsoft Active Directory, rendez-vous sur support.blackberry.com/community pour consulter l'article 36955.

BlackBerry Connectivity Node ne se connecte pas à BlackBerry UEM Cloud

Description

Lorsque vous testez la connexion entre BlackBerry Connectivity Node et BlackBerry UEM Cloud, vous recevez un message d'erreur indiquant que le test a échoué.

Solutions possibles

Effectuez l'une des actions suivantes :

- Vérifiez que les ports de sortie suivants sont ouverts dans le pare-feu de votre organisation, afin que les composants BlackBerry Connectivity Node (et tout serveur proxy associé) puissent communiquer avec BlackBerry Infrastructure (*region*.bbsecure.com) :
  - 443 (HTTPS) pour activer BlackBerry Connectivity Node
  - 3101 (TCP) pour toute autre connexion sortante
- Examinez le fichier journal le plus récent pour obtenir des informations sur la raison de l'échec de la connexion de BlackBerry Connectivity Node à BlackBerry UEM Cloud. Par défaut, les fichiers journaux de BlackBerry Cloud Connector se trouvent dans <*lecteur:*>:\Program Files\BlackBerry\BlackBerry Connectivity Node\Logs.

La liste des instances de BlackBerry Connectivity Node ne se charge pas dans la console de gestion.

Description

Lorsque vous essayez d'afficher une liste des instances de BlackBerry Connectivity Node dans la console de gestion, le message « Chargement...» s'affiche, mais pas la liste des instances.

Solution possible

Rendez-vous sur support.blackberry.com/community pour consulter l'article 38878.

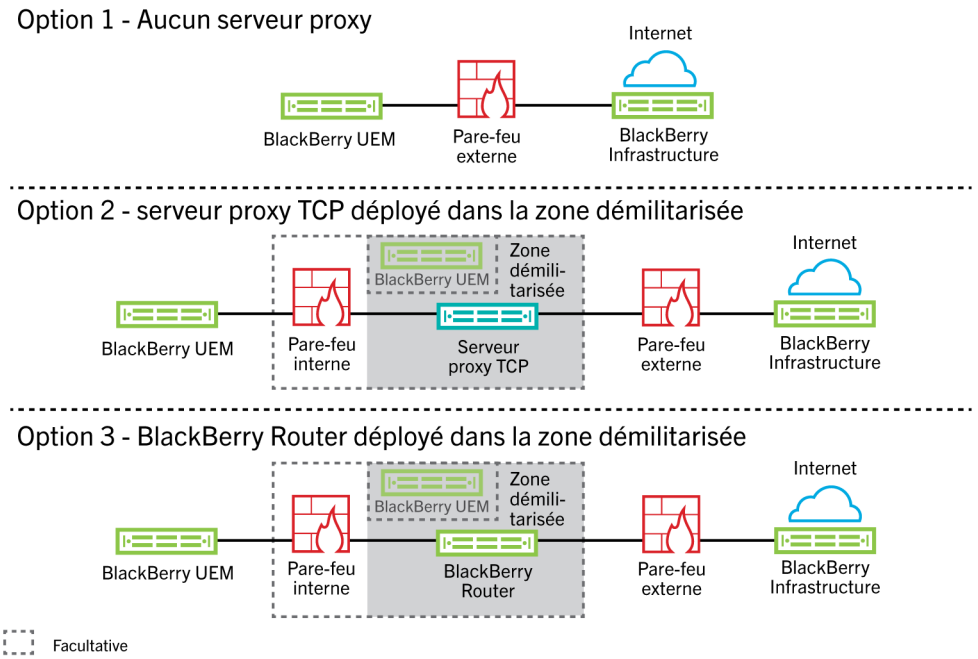
Configuration de BlackBerry Connectivity Node pour qu'il utilise BlackBerry Router ou un serveur proxy TCP

Pour utiliser un serveur proxy avec BlackBerry Connectivity Node, vous pouvez installer BlackBerry Router en tant que serveur proxy, ou bien utiliser un serveur proxy TCP déjà installé dans l'environnement de votre organisation.

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. Seul BlackBerry Router ou le serveur proxy se connecte à BlackBerry Connectivity Node en dehors du pare-feu. Toutes les connexions vers BlackBerry Infrastructure entre BlackBerry Connectivity Node et des terminaux passent par BlackBerry Router ou le serveur proxy.

Par défaut, BlackBerry Connectivity Node se connecte directement à BlackBerry Infrastructure à l'aide du port 3101. Toutefois, 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 Connectivity Node et BlackBerry Infrastructure.

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

Lorsque vous activez BlackBerry Connectivity Node, celui-ci envoie les données via le port 443 (HTTPS) pour activer BlackBerry UEM Cloud. Après son activation, BlackBerry Connectivity Node envoie et reçoit des données via le port 3101 (TCP). Vous pouvez configurer BlackBerry Connectivity Node pour acheminer des

données HTTPS ou TCP via un serveur proxy qui se trouve derrière le pare-feu de votre organisation. BlackBerry Connectivity Node ne prend pas en charge l'authentification avec un serveur proxy.

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

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

Comparaison des proxys TCP

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

Configurer BlackBerry UEM pour utiliser un serveur proxy TCP transparent

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

1. Dans la console BlackBerry Connectivity Node (http:/localhost:8088), cliquez sur **Paramètres généraux > Proxy**.
2. Sélectionnez l'option **Serveur proxy**.
3. Effectuez l'une des tâches suivantes :

Tâche	Étapes
Acheminer les données d'activation HTTPS pour BlackBerry Connectivity Node via un serveur proxy.	Dans les champs **Proxy d'inscription**, saisissez le FQDN ou l'adresse IP et le numéro de port du serveur proxy. Le serveurs proxy doit être capable d'envoyer des données via le port 443 à <*region*>.bbsecure.com.
Acheminer les connexions sortantes depuis les composants de BlackBerry Connectivity Node via un serveur proxy.	Dans les champs appropriés, saisissez le FQDN ou l'adresse IP et le numéro de port du serveur proxy. Le serveur proxy doit être capable d'envoyer des données via le port 3101 à <*region*>.bbsecure.com.

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. Dans la console BlackBerry Connectivity Node (http:/localhost:8088), cliquez sur **Paramètres généraux > 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**.

Installation d'une instance autonome de BlackBerry Router

BlackBerry Router est un composant facultatif que vous pouvez installer dans une zone démilitarisée à l'extérieur du pare-feu de votre organisation. BlackBerry Router se connecte à Internet pour envoyer des données entre BlackBerry Connectivity Node et les terminaux qui utilisent BlackBerry Infrastructure.

BlackBerry Router fait office de serveur proxy et peut prendre en charge SOCKS v5 (sans authentification).

Remarque : Si votre environnement actuel contient un serveur proxy TCP, il est inutile d'installer BlackBerry Router.

Installer une instance autonome de BlackBerry Router

Avant de commencer :

- Vous devez installer un routeur BlackBerry Router autonome sur un ordinateur qui n'héberge aucun autre composant BlackBerry UEM Vous ne pouvez pas installer BlackBerry Router sur un ordinateur qui héberge BlackBerry Connectivity Node.

- Vérifiez que vous disposez du nom d'hôte SRP. Le nom d'hôte SRP est généralement `<country code>.srp.blackberry.com` (par exemple `fr.srp.blackberry.com`). Pour vérifier le nom d'hôte SRP de votre pays, accédez à la page Recherche d'adresses SRP.

1. Dans la console de gestion, sur la barre de menus, cliquez sur **Paramètres > Intégration externe > BlackBerry Cloud Connector**.
2. Cliquez sur **Ajouter BlackBerry Connectivity Node**.
3. Dans la section **Étape 1 : télécharger BlackBerry Connectivity Node**, cliquez sur **Télécharger**.
4. Sur la page de téléchargement du logiciel, répondez aux questions requises et cliquez sur **Télécharger**. Enregistrez et extrayez le package d'installation.
5. Dans le dossier **router**, extrayez le fichier .zip **setupinstaller**. Ce fichier .zip contient un dossier **Installer** avec un fichier **Setup.exe** permettant d'installer BlackBerry Router.
6. Double-cliquez sur le fichier **Setup.exe**.

   L'installation s'exécute en arrière-plan et n'affiche aucune boite de dialogue. Une fois l'installation terminée, le service BlackBerry Router apparait dans la fenêtre Services.

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.

Par défaut, BlackBerry Connectivity Node se connecte à BlackBerry Router via le port 3102. BlackBerry Router prend en charge tout le trafic sortant depuis les composants BlackBerry Connectivity Node.

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

Configurer BlackBerry UEM pour utiliser BlackBerry Router

Avant de commencer : Installer une instance autonome de BlackBerry Router.

1. Dans la console BlackBerry Connectivity Node (http:/localhost:8088), cliquez sur **Paramètres généraux > Proxy**.
2. Sélectionnez l'option **Routeur BlackBerry**.
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**.

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. Connexion de BlackBerry UEM à Azure fournit à votre organisation les fonctionnalités suivantes :

- Connectez BlackBerry UEM à Azure Active Directory et créez des comptes d'utilisateur de répertoire dans BlackBerry UEM en recherchant et en important des données utilisateur depuis le répertoire d'entreprise. Les utilisateurs du répertoire peuvent utiliser leurs informations d'identification d'accès au répertoire pour accéder à BlackBerry UEM Self-Service. Si vous attribuez un rôle d'administration à des utilisateurs du répertoire, les utilisateurs peuvent également utiliser les informations d'identification du répertoire pour se connecter à la console de gestion.
- Utiliser BlackBerry UEM pour déployer les applications iOS et Android gérées par Microsoft Intune.
- Gérer des applications Windows 10 dans BlackBerry UEM

Si votre organisation utilise Microsoft Active Directory au lieu de Azure Active Directory, afin de vous connecter à Azure, vous devez installer la version la plus récente de BlackBerry Connectivity Node pour permettre à BlackBerry UEM Cloud d'accéder à votre répertoire d'entreprise.

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

Étape	Action
1	Créer un compte Microsoft Azure.
2	Si votre organisation utilise Azure Active Directory, configurer BlackBerry UEM Cloud pour synchroniser avec Azure Active Directory.
3	Si votre organisation utilise Microsoft Active Directory sur site et que vous souhaitez utiliser BlackBerry UEM pour déployer des applications gérées par Microsoft Intune ou gérer des applications Windows 10, Synchroniser Microsoft Active Directory avec Microsoft Azure.
4	Créer des applications d'entreprise dans Azure pour permettre à BlackBerry UEM Cloud de se connecter à Microsoft Intune et Windows Store pour Business.
5	Configurer BlackBerry UEM pour une synchronisation de avec Microsoft Intune et Windows Store for Business.
6	(Facultatif) Configurer l'accès conditionnel Azure Active Directory.

Créer un compte Microsoft Azure

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

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

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

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

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

Configurer BlackBerry UEM pour la synchronisation avec Azure Active Directory

Si votre organisation utilise Microsoft Azure Active Directory, vous pouvez le connecter à BlackBerry UEM pour créer des comptes utilisateur de répertoire dans BlackBerry UEM en recherchant et en important des données utilisateur depuis le répertoire d'entreprise. Les utilisateurs du répertoire peuvent utiliser leurs informations d'identification d'accès au répertoire pour accéder à BlackBerry UEM Self-Service.

Vous pouvez vous connecter à plusieurs instances de Azure Active Directory. Si vous installez BlackBerry Connectivity Node, vous pouvez également vous connecter à un annuaire sur site.

1. Connectez-vous au portail Azure.
2. Accédez à **Microsoft Azure > Azure Active Directory > Inscriptions des applications**.
3. Cliquez sur **+ Nouvelle inscription**.
4. Dans le champ **Nom**, saisissez un nom pour l'application.
5. Sélectionnez les types de compte qui peuvent utiliser l'application ou accéder à l'API.
6. Dans la section **Rediriger l'URI**, sélectionnez **Web** dans la liste déroulante, puis saisissez `http://localhost`.
7. Cliquez sur **S'inscrire**.
8. Copiez l'**ID d'application** de votre application et collez-le dans un fichier texte.

   Il s'agit de l'**ID client** requis dans BlackBerry UEM.
9. Dans la section **Gérer**, cliquez sur **Autorisations API**.
10. Cliquez sur **+ Ajouter une autorisation** et procédez comme suit :
    a) Cliquez sur **Microsoft Graph**.
    b) Sélectionnez **Autorisations de l'application**.
    c) Définissez les autorisations suivantes :
       - Group.Read.All (Application)
       - User.Read (Délégué)
       - User.Read.All (Application)
    d) Cliquez sur **Ajouter des autorisations**.
    e) Sous **Accorder le consentement**, cliquez sur **Accorder le consentement de l'administrateur**.

       Remarque : Vous devez être administrateur général pour octroyer des autorisations.
    f) Lorsque vous y êtes invité, cliquez sur **Oui** pour accorder des autorisations à tous les comptes du répertoire actuel.
11. Dans la section **Gérer**, cliquez sur **Certificats et secrets**. Procédez comme suit :
    a) Sous **Secrets de client**, cliquez sur **Nouveau secret de client**.
    b) Saisissez la description du secret du client.
    c) Sélectionnez une durée pour le secret du client.

d) Cliquez sur **Ajouter**.
e) Copiez la valeur du nouveau secret du client.

Il s'agit de la clé client qui est requise pour BlackBerry UEM.

12. Dans la console de gestion, cliquez sur **Paramètres > Intégration externe > + Répertoire d'entreprise > Connexion Microsoft Azure Active Directory**.
13. Renseignez les champs **Nom de connexion du répertoire** et **Domaine** de votre Azure Active Directory.
14. Effectuez l'une des opérations suivantes :

- S'il s'agit d'une nouvelle connexion à Azure, saisissez 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
- S'il s'agit d'une connexion existante à Azure, cliquez sur **Activer l'enregistrement d'une application à locataire unique** et saisissez 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

15. Cliquez sur **Continuer**.
16. Cliquez sur **Enregistrer**.

À la fin : Lier les groupes d'annuaire d'entreprise aux groupes BlackBerry UEM

Synchroniser Microsoft Active Directory avec Microsoft Azure

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

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

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

Créer un point de terminaison d'entreprise dans Azure

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

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

Remarque :

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

Avant de commencer :

- Si votre organisation utilise Microsoft Active Directory sur site, Synchroniser Microsoft Active Directory avec Microsoft Azure
- Assurez-vous d'être en possession de l'URL de réponse. Pour des instructions sur l'obtention de l'URL de réponse en vue d'une authentification moderne, reportez-vous à la section Configurer BlackBerry UEM pour la synchronisation avec Microsoft Intune.

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

   Il s'agit de l'**ID client** requis dans BlackBerry UEM.
9. Si vous créez l'application pour utiliser Microsoft Intune, cliquez sur **Autorisations API** dans la section **Gérer**. Procédez comme suit :
   a) Cliquez sur **Ajouter une autorisation**.
   b) Cliquez sur **Microsoft Graph**.
   c) Sélectionnez **Autorisations déléguées**.
   d) Faites défiler la liste des autorisations vers le bas, puis, sous **Autorisations déléguées**, définissez les autorisations suivantes pour Microsoft Intune :
      - Lire et écrire les applications Microsoft Intune (**DeviceManagementApps > DeviceManagementApps.ReadWrite.All**)
      - Lire tous les groupes (**Groupe > Group.Read.All**)
      - Lire tous les profils de base des utilisateurs (**Utilisateur > User.ReadBasic.All**)

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

      Remarque : Vous devez être administrateur général pour octroyer des autorisations.
   g) Lorsque vous y êtes invité, cliquez sur **Oui** pour octroyer des autorisations pour tous les comptes dans l'annuaire actuel.

   Vous pouvez utiliser les autorisations par défaut si vous créez l'application pour vous connecter à Windows Store Entreprise.
10. Cliquez sur **Certificats et secrets** dans la section **Gérer**. Procédez comme suit :
    a) Sous **Secrets de client**, cliquez sur **Nouveau secret de client**.
    b) Saisissez la description du secret du client.
    c) Sélectionnez une durée pour le secret du client.
    d) Cliquez sur **Ajouter**.
    e) Copiez la valeur du nouveau secret du client.

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

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

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

Configuration de l'accès conditionnel Azure Active Directory

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

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

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

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

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

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

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

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

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

Configurer l'accès conditionnel Azure Active Directory

Avant de commencer : Vous devez utiliser des licences Microsoft 365 E5. Pour en savoir plus, rendez-vous sur support.blackberry.com et consultez les articles KB91041 et KB50341. Pour plus d'informations sur les licences, consultez les détails de Microsoft.

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

   Si vous prenez en charge les terminaux iOS et Android, vous devez ajouter BlackBerry UEM en tant que partenaire de conformité pour chaque plateforme. Pour plus d'informations, consultez la documentation Microsoft.
2. Dans la console de gestion BlackBerry UEM, cliquez sur **Paramètres > Intégration externe > Accès conditionnel Azure Active Directory**.
3. Sélectionnez **Activer l'accès conditionnel**.
4. Dans la liste déroulante **Cloud Azure**, sélectionnez **Global**.
5. Saisissez votre **ID de locataire Azure**.

   Vous pouvez saisir le nom du locataire qui est au format FQDN, ou l'ID de locataire unique qui est au format GUID.
6. Cliquez sur **Enregistrer**.
7. Sélectionnez le compte administrateur que vous souhaitez utiliser pour vous connecter à votre locataire Azure.

   Le compte administrateur doit pouvoir accorder des autorisations à l'application pour accéder aux ressources de votre entreprise. comme l'administrateur général, l'administrateur d'application cloud ou l'administrateur d'application.
8. Acceptez la demande d'autorisation de Microsoft.
9. Dans la console de gestion BlackBerry UEM, modifiez chaque BlackBerry Dynamics profil de connectivité et effectuez les actions suivantes :
   a) Sous **Services d'applications**, cliquez sur **Ajouter**.
   b) Sélectionnez **Feature-Azure Conditional Access** dans la liste des applications.
   c) Cliquez sur + pour ajouter un nouveau serveur d'applications.
   d) Si vous utilisez BlackBerry UEM dans un environnement sur site, spécifiez les paramètres de serveur suivants :

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

   Si votre environnement comprend BlackBerry UEM Cloud et BEMS cloud, et que vous avez configuré les notifications par e-mail ou BEMS-Docs pour créer un locataire BEMS, la priorité, le numéro de port et l'URL de BEMS cloud sont automatiquement ajoutés à la section de charge utile du serveur d'applications.
10. Attribuez l'application **Feature-Azure Conditional Access** aux utilisateurs ou aux groupes.
11. Dans le profil BlackBerry Dynamics, assurez-vous que le paramètre **Autoriser UEM Client à s'inscrire dans BlackBerry Dynamics** est sélectionné.

À la fin :

- L'application Microsoft Authenticator doit être installée sur les terminaux des utilisateurs. Vous pouvez attribuer l'application dans UEM ou demander aux utilisateurs de l'installer depuis leur App Store.
- Une fois l'accès conditionnel Active Directory configuré, les utilisateurs activant des terminaux sont invités à s'inscrire à l'accès conditionnel Active Directory lors de l'activation. Les utilisateurs disposant de terminaux activés sont invités à s'inscrire à l'accès conditionnel Active Directory la prochaine fois qu'ils ouvrent le UEM Client.

Supprimer les terminaux Azure Active Directory de l'accès conditionnel

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

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

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

Lier les groupes de répertoires d'entreprise aux groupes de BlackBerry UEM

Vous pouvez créer des groupes dans BlackBerry UEM liés aux groupes de votre répertoire d'entreprise. L'activation des groupes liés au répertoire vous permet de bénéficier des fonctionnalités suivantes :

- Possibilité d'ajouter à BlackBerry UEM des groupes qui sont liés aux groupes de répertoires d'entreprise afin d'attribuer et de gérer les stratégies informatiques, les profils et les applications pour les utilisateurs. Ces groupes sont appelés « groupes liés au répertoire ».

  Pour plus d'informations sur la création de groupes liés par répertoire, consultez le contenu relatif à l'administration.
- Possibilité d'ajouter à BlackBerry UEM des groupes qui sont liés aux groupes de répertoires d'entreprise afin de synchroniser automatiquement l'adhésion à un groupe. Ces groupes sont appelés « groupes de répertoires d'intégration ». Reportez-vous à la section Activer l'intégration.

Activer les groupes liés par annuaire

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

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

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

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

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

Activer l'intégration

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

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

Suppression

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

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

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

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

Synchronisation

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

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

Activer et configurer l'intégration et la suppression

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

Avant de commencer :

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

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

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

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

Si le nombre de modifications à synchroniser dépasse la limite de synchronisation, vous pouvez empêcher l'exécution du processus de synchronisation. Les modifications sont calculées en ajoutant ce qui suit : utilisateurs à ajouter aux groupes, utilisateurs à supprimer des groupes, utilisateurs à intégrer, utilisateurs à supprimer.

13. Dans le champ **Niveau d'imbrication maximal des groupes de répertoire**, saisissez le nombre de niveaux imbriqués à synchroniser pour les groupes de répertoires d'entreprise.
14. Cliquez sur **Enregistrer**.

Synchroniser une connexion à un répertoire d'entreprise

Avant de commencer : Prévisualiser un rapport de synchronisation

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

À la fin : Afficher un rapport de synchronisation

Prévisualiser un rapport de synchronisation

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

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

Afficher un rapport de synchronisation

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

Ajouter un calendrier de synchronisation

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

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

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

1. Sur la barre de menus, cliquez sur **Paramètres > Intégration externe > Répertoire d'entreprise**.
2. Cliquez sur le nom du répertoire d'entreprise que vous souhaitez modifier.
3. Dans l'onglet **Calendrier de synchronisation**, cliquez sur .

4. Pour réduire la quantité d'informations synchronisées, dans la liste déroulante **Type de synchronisation**, choisissez une des options suivantes :
   - **Tous les groupes et utilisateurs** : Il s'agit du paramètre par défaut. Si vous choisissez cette option, les utilisateurs seront intégrés, supprimés et liés aux groupes reliés au répertoire approprié au cours de la synchronisation, les utilisateurs qui ne sont pas intégrés ou supprimés mais dont les groupes reliés au répertoire ont été modifiés, et les utilisateurs dont les attributs ont été modifiés seront synchronisés.
   - **Groupes d'intégration** : si vous choisissez cette option, les utilisateurs seront intégrés, supprimés et liés aux groupes reliés au répertoire approprié au cours de la synchronisation, et les utilisateurs dont les attributs ont été modifiés seront synchronisés. Les utilisateurs qui ne sont pas intégrés ou supprimés mais dont les groupes reliés au répertoire ont été modifiés ne sont pas synchronisés.
   - **Groupes associés à un répertoire** : si vous choisissez cette option les utilisateurs ne pourront pas être intégrés et supprimés lors de la synchronisation. Les utilisateurs dont les groupes reliés au répertoire ont été modifiés seront liés de manière appropriée. Les utilisateurs dont les attributs ont été modifiés seront synchronisés.
   - **Attributs de l'utilisateur** : si vous choisissez cette option les utilisateurs ne pourront pas être intégrés et supprimés lors de la synchronisation. Les utilisateurs dont les groupes reliés au répertoire ont été modifiés ne sont pas synchronisés. Les utilisateurs dont les attributs ont été modifiés seront synchronisés.
5. Dans la liste déroulante **Récurrence**, sélectionnez l'une des options suivantes :

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

6. Cliquez sur **Ajouter**.

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.

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

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

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

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

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

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

Obtenir un fichier CSR signé auprès de BlackBerry

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

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

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

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

Demander un certificat APNs auprès d'Apple

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

1. Sur la barre de menus, cliquez sur **Paramètres > Intégration externe > Apple Push Notification**.
2. Dans la section **Étape 2 sur 3 : obtenir un certificat APNs auprès d'Apple**, cliquez sur **Apple Push Certificate Portal**. Vous êtes dirigé vers le portail Apple Push Certificates Portal.
3. Connectez-vous au portail Apple Push Certificates Portal en utilisant un ID Apple valide.
4. Suivez les instructions pour charger le fichier CSR signé (.scsr).
5. Téléchargez et enregistrez le certificat APNs (.pem) sur votre ordinateur.
6. (Facultatif) Cliquez sur pour afficher une fenêtre **Remarque**.
7. Dans la fenêtre **Remarque**, saisissez l'ID Apple que vous avez utilisé pour demander le certificat APNs. Vous devez utiliser le même ID Apple pour renouveler le certificat.
8. Cliquez n'importe où en dehors de la fenêtre **Remarque** pour la fermer.

À la fin : Enregistrer le certificat APNs.

Enregistrer le certificat APNs

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

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

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

Renouveler le certificat APNs

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

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

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

1. Sur la barre de menus, cliquez sur **Paramètres > Intégration externe > Apple Push Notification**.
2. Cliquez sur **Renouveler le certificat**.
3. Dans la section **Étape 1 sur 3 - Télécharger le certificat CSR signé de BlackBerry**, cliquez sur **Télécharger le certificat**.
4. Cliquez sur **Enregistrer** pour enregistrer le fichier CSR signé (.scsr) sur votre ordinateur.
5. Dans la section **Étape 2 sur 3 : obtenir un certificat APNs auprès d'Apple**, cliquez sur **Apple Push Certificate Portal**. Vous êtes dirigé vers le portail Apple Push Certificates Portal.
6. Connectez-vous au portail Apple Push Certificates Portal en utilisant l'ID Apple utilisé pour obtenir le certificat APNs d'origine.
7. Suivez les instructions pour renouveler le certificat APNs (.pem). Vous devrez alors télécharger le nouveau fichier CSR signé.

8. Téléchargez et enregistrez le certificat APNs renouvelé sur votre ordinateur.
9. Dans la section **Étape 3 sur 3 : inscrire le certificat APNs**, cliquez sur **Parcourir**. Accédez au certificat APNs renouvelé et sélectionnez-le.
10. Cliquez sur **Envoyer**.

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

Dépannage de l'APNs

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

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

Description

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

Solution possible

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

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

Description

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

Solution possible

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

Je ne peux pas activer des terminaux iOS ou macOS

Cause possible

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

Solution possible

Effectuez une ou plusieurs des opérations suivantes :

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

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

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

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

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

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

Créer un compte du programme d'inscription des appareils

1. Sur la barre de menus, cliquez sur **Paramètres > Intégration externe > Programme d'inscription des appareils Apple**.
2. 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**.
3. Remplissez les champs et suivez les instructions à l'écran pour créer votre compte.

À la fin : Télécharger une clé publique.

Télécharger une clé publique

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

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

À la fin : Générer un jeton de serveur.

Générer un jeton de serveur

Avant de commencer : Télécharger une clé publique.

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

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

Enregistrer le jeton de serveur avec BlackBerry UEM

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

Avant de commencer : Générer un jeton de serveur.

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

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

Ajouter la première configuration d'inscription

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

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

1. Saisissez un nom pour la configuration.
2. Effectuez l'une des tâches suivantes :

- Si vous souhaitez que BlackBerry UEM attribue automatiquement la configuration d'inscription aux appareils lorsque vous les enregistrez dans le programme d'inscription des appareils d'Apple, cochez la case Attribuer automatiquement cette configuration à tous les nouveaux appareils.
- Si vous souhaitez utiliser la console BlackBerry UEM pour attribuer manuellement la configuration d'inscription aux appareils concernés, ne cochez pas la case Attribuer automatiquement cette configuration à tous les nouveaux appareils.

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

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

6. Cliquez sur **Enregistrer**.

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

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

Mettre à jour le jeton de serveur

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

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

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

Supprimer une connexion DEP

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

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

1. Sur la barre de menus, cliquez sur **Paramètres > Intégration externe > Programme d'inscription des appareils Apple**.
2. Cliquez sur **Supprimer la connexion au programme d'inscription des appareils**.
3. Cliquez sur **Supprimer**.

4. Cliquez sur **OK**.

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

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

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

Il existe deux façons de configurer BlackBerry UEM pour prendre en charge les appareils Android Enterprise :

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

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

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

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

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

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

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

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

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

Tâche	Étapes
Utilisez un domaine Google.	a. Sélectionnez **Connecter BlackBerry UEM à votre domaine Google existant**. 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 sur support.blackberry.com/community pour consulter l'article 37748.

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

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

Supprimer la connexion à votre domaine Google

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

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

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

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

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

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

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

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

Modifier ou tester la connexion au domaine Google

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

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

Simplification des activations Windows 10

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

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

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

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

Intégration de UEM avec la jonction à Azure Active Directory

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

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

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

Intégrer UEM avec la jonction à Azure Active Directory

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

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

Configuration de Windows Autopilot dans Microsoft Azure

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

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

Créer un profil de déploiement Windows Autopilot dans Azure

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

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

Importer des terminaux Windows Autopilot dans Azure

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

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

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

Déployer un service de détection pour simplifier les activations Windows 10

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

16. Redémarrez Apache Tomcat.

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

Suivez les instructions de cette section pour configurer BlackBerry UEM Cloud afin de prendre en charge les applications BlackBerry Dynamics.

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

Gérer les clusters BlackBerry Proxy

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

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

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

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

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

Avant de commencer :

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

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

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

Connexion de BlackBerry Proxy à BlackBerry Dynamics NOC

Si vous avez l'intention d'utiliser BlackBerry Proxy pour permettre aux applications BlackBerry Dynamics de se connecter aux ressources de votre organisation, le pare-feu de votre organisation doit autoriser les connexions TCP vers les plages IP suivantes afin que BlackBerry Proxy puisse se connecter au NOC BlackBerry Dynamics :

- 206.124.114.1 à 206.124.114.254 (206.124.114.0/24) sur le port 443
- 206.124.121.1 à 206.124.121.254 (206.124.121.0/24) sur le port 443
- 206.124.122.1 à 206.124.122.254 (206.124.122.0/24) sur le port 443

Vous pouvez également configurer le pare-feu de votre entreprise de manière à autoriser les connexions aux noms d'hôte suivants :

- gdentgw.good.com sur le port 443
- gdrelay.good.com sur le port 443
- gdweb.good.com sur le port 443
- gdmdc.good.com sur le port 443

Connecter BlackBerry UEM à un connecteur PKI BlackBerry Dynamics

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

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

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

Avant de commencer : Configurez un connecteur PKI BlackBerry Dynamics.

1. Sur la barre de menus, cliquez sur **Paramètres > Intégration externe > Autorité de certification**.
2. Cliquez sur **Ajouter une connexion PKI BlackBerry Dynamics**.
3. Dans le champ **Nom de connexion**, saisissez un nom de connexion.
4. Dans le champ **URL**, saisissez l'URL du connecteur PKI.
5. Sélectionnez l'une des options suivantes :
   - **Authentification avec nom d'utilisateur et mot de passe** : choisissez cette option si BlackBerry UEM s'authentifie auprès du connecteur PKI BlackBerry Dynamics en utilisant l'authentification par mot de passe.
   - **Authentification avec certificat client** : choisissez cette option si BlackBerry UEM s'authentifie auprès du connecteur PKI BlackBerry Dynamics en utilisant l'authentification basée sur les certificats.
6. Si vous avez sélectionné **Authentification avec nom d'utilisateur et mot de passe**, dans les champs **Nom d'utilisateur** et **Mot de passe**, saisissez le nom d'utilisateur et le mot de passe du connecteur PKI BlackBerry Dynamics.

7. Si vous avez sélectionné **Authentification avec certificat client**, cliquez sur **Parcourir** pour sélectionner et télécharger un certificat approuvé par le connecteur PKI BlackBerry Dynamics. Dans le champ **Mot de passe du certificat client**, saisissez le mot de passe du certificat.
8. Dans la section **Certificat approuvé pour le connecteur PKI**, vous pouvez spécifier le certificat que BlackBerry UEM utilise pour faire confiance aux connexions du connecteur PKI, sélectionnez une des options suivantes :
   - **Certificat de l'AC de BlackBerry Control TrustStore**
   - **Certificat d'autorité de certification** : si vous sélectionnez cette option, vous devez cliquer sur Parcourir pour naviguer et sélectionner le certificat d'autorité de certification de votre organisation.
   - **Certificat serveur du connecteur PKI** : si vous sélectionnez cette option, vous devez cliquer sur Parcourir pour naviguer et sélectionner le certificat de serveur de connecteur PKI de votre organisation.
9. Pour tester la connexion, cliquez sur **Tester la connexion**.
10. Cliquez sur **Enregistrer**.

À la fin :

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

Remplacement des paramètres de proxy HTTP globaux pour BlackBerry Connectivity Node

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

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

Considérations relatives au fichier PAC

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

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

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

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

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

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

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

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

Remarque :

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

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

Configurer les paramètres proxy de l'application BlackBerry Dynamics pour BlackBerry Cloud Connector

Vous pouvez configurer les paramètres proxy BlackBerry Cloud Connector pour les applications BlackBerry Dynamics manuellement ou à l'aide d'un fichier PAC.

1. Dans BlackBerry Cloud Connector, cliquez sur **Paramètres généraux > BlackBerry Router et proxy**.
2. Sélectionnez **Paramètres globaux**.
3. Sélectionnez l'une des options suivantes.
   - **Activer le proxy HTTP manuel**
   - **Activer PAC**

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

   b) Si vous voulez utiliser le serveur proxy pour vous connecter aux serveurs spécifiés, cliquez sur + pour spécifier tous les serveurs supplémentaires.
   c) Dans le champ **Adresse**, saisissez l'adresse du serveur proxy.
   d) Dans le champ **Port**, saisissez le numéro de port écouté par le serveur proxy.
   e) Si le serveur proxy requiert une authentification, sélectionnez **Utiliser l'authentification** et spécifiez le **nom d'utilisateur**, le **mot de passe** et, si nécessaire, le **domaine** que l'application doit utiliser pour l'authentification.
5. Si vous avez sélectionné **Activer PAC**, procédez comme suit :
   a) Dans le champ **URL du fichier PAC**, saisissez l'URL du fichier PAC.
   b) Si le serveur proxy spécifié dans le fichier PAC requiert une authentification, sélectionnez **Prise en charge de l'authentification proxy** et spécifiez le **nom d'utilisateur**, le **mot de passe** et, si nécessaire, le **domaine** que l'application doit utiliser pour l'authentification.

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

Configurer les notifications e-mail de BlackBerry Work

Le cloud BEMS accepte les demandes d'inscription push envoyées par les terminaux, tels que iOS et Android, puis communique avec le serveur Microsoft Exchange Server ou Microsoft Office 365 sur site pour vérifier si la boîte aux lettres de l'utilisateur contient des changements. Lorsque vous spécifiez les informations du serveur Microsoft Exchange Server ou Microsoft Office 365 sur site, vous indiquez les paramètres de création du cloud BEMS locataire de votre entreprise.

Lorsque le locataire est créé, les services suivants sont automatiquement activés :

- BlackBerry Directory Lookup : ce service permet aux utilisateurs de rechercher d'autres utilisateurs par prénom, nom et photo ou avatar associé à partir du répertoire de l'entreprise.
- BlackBerry Follow-Me : cette fonction prend en charge le BlackBerry Dynamics Launcher sur BlackBerry Work.

Un environnement d'authentification moderne hybride (par exemple, Microsoft Exchange Server sur site et Microsoft Office 365) permet à Microsoft Exchange Server sur site d'utiliser une authentification et une autorisation utilisateur plus sécurisées par le biais de jetons d'accès OAuth obtenus à partir du cloud. Pour savoir comment configurer Microsoft Exchange Server sur site afin d'utiliser une authentification moderne hybride, rendez-vous sur https://docs.microsoft.com/en-us/microsoft-365/enterprise/configure-exchange-server-for-hybrid-modern-authentication?view=o365-worldwide.

Avant de commencer : Vérifiez que vous disposez des informations suivantes et que vous avez effectué les tâches appropriées.

- Vérifiez que les autorisations d'emprunt d'identité sont appliquées au compte de service.
- Si vous disposez d'un environnement Microsoft Office 365 hybride et Microsoft Exchange Server sur site, et que vous activez l'authentification moderne, assurez-vous que Microsoft Exchange Server sur site est configuré pour utiliser l'authentification moderne hybride. Pour plus d'informations, rendez-vous sur https://docs.microsoft.com/en-us/microsoft-365/enterprise/configure-exchange-server-for-hybrid-modern-authentication?view=o365-worldwide. Si le Microsoft Exchange Server n'est pas configuré correctement, les utilisateurs ne recevront pas de notifications par e-mail.
- Dans un environnement Microsoft Office 365, si vous prévoyez d'activer l'authentification moderne, vérifiez que vous remplissez les conditions suivantes :
  - Si vous activez l'authentification moderne à l'aide de l'authentification des informations d'identification, obtenez l'ID de l'application client.
  - Si vous activez l'authentification moderne à l'aide de l'authentification du certificat client, effectuez l'une des actions suivantes :
    - obtenez l'ID de l'application client à l'aide de l'authentification basée sur des certificats ;
    - Créez un certificat .pfx autosigné et associez-le à l'ID d'application Azure pour BEMS
  - Si vous avez configuré l'accès conditionnel Azure AD pour votre entreprise, assurez-vous que BlackBerry Connectivity Node est installé et configuré dans votre environnement.
  - Configurer les notifications e-mail de BlackBerry Work
  - Dans un environnement Microsoft Exchange sur site, assurez-vous que Microsoft Exchange Server a été mis à jour pour prendre en charge TLS 1.2 ou les notifications Push échoueront. Les suites de codes les plus faibles, telles que TLSv1 ou TLS 1.0, sont désactivées par défaut. La désactivation des suites de codes renforce la sécurité.
- Si vous utilisez l'authentification passive, vérifiez que vous disposez de l'ID d'application pour BEMS à l'aide de l'authentification des informations d'identification.
- Si vous utilisez SSL pour la recherche SCP, vérifiez que vous avez exporté le certificat SSL Microsoft Active Directory.

1. Dans la console de gestion, cliquez sur **Paramètres > BlackBerry Dynamics > Notifications par e-mail**.

2. Dans la section **Type d'authentification**, sélectionnez un type d'authentification en fonction de votre environnement et effectuez les tâches associées pour permettre à BEMS de communiquer avec Microsoft Exchange Server ou Microsoft Office 365 :

Type d'authentification	Description	Tâche
Informations d'identification	Cette option utilise un nom d'utilisateur BEMS et un mot de passe définis pour s'authentifier auprès de Microsoft Exchange Server ou Microsoft Office 365 à l'aide de l'authentification de base.	**a.** Dans le champ **Nom d'utilisateur du compte de service**, saisissez le nom d'utilisateur du compte de service BEMS. • Pour Microsoft Office 365, saisissez le nom d'utilisateur principal du compte de service. • Pour Microsoft Exchange Server sur site, utilisez le format <*domaine*>\<*nom d'utilisateur*>. **b.** Dans le champ **Mot de passe du compte de service**, saisissez le mot de passe du compte de service.
Certificat client	Cette option utilise un certificat client pour permettre au compte de service BEMS de s'authentifier auprès de Microsoft Exchange Server ou Microsoft Office 365.	**a.** En regard du champ **Fichier de certificat (.pfx)**, cliquez sur **Parcourir**. Accédez au fichier du certificat client et sélectionnez-le. **b.** Dans le champ **Mot de passe**, saisissez le mot de passe du certificat client.

Type d'authentification	Description	Tâche
Authentification passive	Cette option utilise un fournisseur d'identité (IDP) pour authentifier l'utilisateur et fournir à BEMS des jetons OAuth pour s'authentifier auprès de Microsoft Office 365. Dans un environnement hybride, l'authentification se fait pour Microsoft Exchange Server sur site*.	**a.** Dans le champ **Autorité d'authentification**, saisissez l'URL du serveur d'authentification utilisé par BEMS pour accéder au jeton OAuth et le récupérer pour l'authentification avec Microsoft Office 365 (par exemple, https://login.microsoftonline.com/common). **b.** Dans le champ **ID de l'application client**, saisissez l'ID de l'application Azure pour l'authentification des informations d'identification. Pour obtenir des instructions, reportez-vous à la section relative à l'ID d'application de BEMS à l'aide de l'authentification des informations d'identification. **c.** Dans le champ **Nom de serveur**, saisissez le FQDN du serveur Microsoft Office 365. Par défaut, le nom du serveur est https://outlook.office365.com. **d.** Le champ **Rediriger l'URI** affiche l'URL vers laquelle l'IDP redirige l'administrateur lorsque l'ID d'application client est autorisé et que les jetons d'authentification sont fournis. Ce champ est prérempli avec les informations de partition et ne peut pas être modifié. **e.** Cliquez sur **Connexion**. **f.** Saisissez les informations d'identification associées au compte de service. **g.** Cliquez sur **OK** pour confirmer que les jetons d'authentification ont été obtenus. **h.** Important : BEMS cloud n'actualise pas automatiquement les jetons OAuth. Répétez les étapes e à g pour actualiser les jetons OAuth. Le délai d'expiration des jetons dépend de votre stratégie de locataire (par défaut, le délai d'expiration des jetons est de 90 jours). Lorsque les jetons OAuth expirent, l'envoi des notifications par e-mail cesse sur les terminaux des utilisateurs. L'expiration du jeton OAuth s'affiche après la connexion à l'IDP.

* Le Microsoft Exchange Server sur site doit être configuré pour utiliser l'authentification moderne hybride. Pour plus d'informations, rendez-vous sur https://docs.microsoft.com/en-us/microsoft-365/enterprise/configure-exchange-server-for-hybrid-modern-authentication?view=o365-worldwide.

3. Si vous vous connectez à un environnement Microsoft Office 365, procédez comme suit pour activer l'authentification moderne :
   a) Cochez la case **Activer l'authentification moderne**.
   b) Dans le champ **Autorité d'authentification**, saisissez l'URL du serveur d'authentification utilisé par BEMS pour récupérer le jeton OAuth pour l'authentification avec Microsoft Office 365 (par exemple, https://login.microsoftonline.com/<*nomdelocataire*> ou https://login.microsoftonline.com/<*iddelocataire*>).
   c) Dans le champ **ID de l'application client**, saisissez l'un des ID d'application Azure suivants en fonction du type d'authentification que vous avez sélectionné. Effectuez l'une des opérations suivantes pour obtenir un ID d'application Azure :
      - Obtenir un ID d'application Azure pour BEMS avec une authentification basée sur les informations d'identification
      - Obtenir un ID d'application Azure pour BEMS avec l'authentification basée sur des certificats

d) Dans le champ **Nom du serveur**, saisissez le FQDN du serveur Microsoft Office 365 (par exemple, https://outlook.office365.com).
e) Vous pouvez également cocher la case **Utiliser les informations d'identification si l'authentification moderne échoue** pour autoriser BEMS à communiquer avec Microsoft Office 365 dans le cas où BEMS ne peut pas accéder à la source d'authentification moderne. Si vous cochez cette case, vous devez spécifier les informations d'identification du compte de service BEMS.

Remarque : lorsque vous configurez l'authentification moderne, tous les nœuds utilisent la configuration spécifiée.

4. Dans le champ **Nom d'utilisateur du compte de service**, saisissez le nom d'utilisateur utilisé pour la connexion au serveur Microsoft Exchange Server ou Microsoft Office 365. Le nom d'utilisateur doit être dans l'un des formats suivants :
   - Si votre environnement utilise une Microsoft Exchange Server sur site, utilisez < > *Domaine*>\<*Utilisateur* > ou UPN.
   - Si votre environnement utilise Microsoft Office 365, suivez le format <*utilisateur*>@<*domaine*>.com.
5. Dans le champ **Mot de passe du compte de service**, saisissez le mot de passe du compte de service que vous avez défini.
6. Vous pouvez, si vous le souhaitez, saisir dans le champ **Remplacement de l'URL de détection automatique**, l'URL de détection automatique permettant à BEMS d'obtenir des informations sur l'utilisateur depuis le serveur Microsoft Exchange Server ou Microsoft Office 365 lorsqu'il détecte des utilisateurs de BlackBerry Push Notifications.

   Remarque : Si vous n'indiquez pas d'URL, BEMS utilise la détection automatique pour localiser le serveur Microsoft Exchange Server ou Microsoft Office 365 afin d'obtenir des informations sur l'utilisateur.
7. Cochez la case **Autoriser la redirection HTTP et l'enregistrement SRV du DNS** pour autoriser la redirection HTTP et les recherches DNS SRV afin de récupérer l'URL automatiquement détectée lors de la détection des utilisateurs de BlackBerry Push Notifications. Par défaut, ce paramètre est activé.
8. Sélectionnez **Utiliser un itinéraire de BlackBerry Connectivity Node** pour permettre au cloud BEMS de se connecter à Microsoft Exchange Server ou Microsoft Office 365 à l'aide du réseau d'entreprise plutôt que d'utiliser une connexion directe à partir de l'infrastructure cloud BlackBerry BEMS. Ce paramètre exige que le BlackBerry Connectivity Node soit installé et configuré dans votre environnement. Si votre environnement utilise l'accès conditionnel Azure AD, assurez-vous que cette option est sélectionnée.
9. Si votre environnement utilise une URL interne pour accéder à une instance de Microsoft Exchange Server sur site et communiquer avec elle, cochez la case **Utiliser l'URL des services Web Exchange internes**. Ce paramètre nécessite que le paramètre « Utiliser un itinéraire de BlackBerry Connectivity Node » soit activé. Cette option n'est pas disponible si l'authentification moderne est activée.
10. Vous pouvez également cocher la case **Activer les recherches SCP** pour interroger Microsoft Active Directory à l'aide de LDAP et localiser les URL de point de terminaison de détection automatique. Ce paramètre est valide uniquement si l'authentification Informations d'identification est sélectionnée et si BlackBerry Connectivity Node est installé et configuré dans votre environnement. Cette option n'est pas disponible lorsque l'option « Remplacement de l'URL de détection automatique » est spécifiée.
11. Cochez la case **Activer SSL pour SCP**. Cela permet à BEMS de communiquer avec Microsoft Active Directory à l'aide de SSL. Ce paramètre nécessite que l'option « Activer les recherches SCP » soit sélectionnée. Si vous activez cette fonction, vous devez ajouter le certificat SSL Microsoft Active Directory à la base de données cloud BEMS. Pour plus d'informations sur l'ajout du certificat, reportez-vous à la section Création d'une connexion sécurisée entre BEMS Cloud et Microsoft Exchange Server.
12. Si vous avez activé **Activer les recherches SCP** ou **Activer les recherches SCP** et **Activer SSL pour SCP**, spécifiez l'option **Domain Controllers for SCP** pour configurer LDAP sur SCP. Si vous disposez de plusieurs contrôleurs de domaine, séparez-les à l'aide de virgules (par exemple, contrôleurdedomaine1.exemple.com,contrôleurdedomaine2.exemple.com, etc.).

13. Si vous le souhaitez, dans le champ **Saisir une adresse électronique de l'utilisateur**, saisissez une adresse e-mail pour tester la connexion au serveur Microsoft Exchange Server ou Microsoft Office 365. Cliquez sur **Tester la connexion**. Si le test échoue, corrigez les problèmes identifiés et réessayez. Vous pouvez supprimer l'adresse e-mail, une fois le test terminé.
14. Cliquez sur **Enregistrer**.

À la fin :

- Testez la connexion au serveur Microsoft Exchange Server ou Microsoft Office 365 sur site et la détection automatique. Actualisez ou rouvrez l'écran des notifications par e-mail. Cliquez sur **Tester la connexion**. **Remarque :** S'assurer que le test de connexion est réussi avant d'attribuer des terminaux afin d'éviter les problèmes liés à Autodiscover. Si les terminaux sont activés avant la configuration du service de notification par e-mail, demandez aux utilisateurs de se déconnecter de BlackBerry Work, puis de se reconnecter. Si le test renvoie un message d'erreur, effectuez les tâches pour résoudre le problème, puis testez à nouveau la connexion.
- Attribuez le droit d'accès à BlackBerry Cloud Enterprise Services (com.blackberry.gdservice-autorisation.cloud) aux utilisateurs devant recevoir des notifications par e-mail pour BlackBerry Work. Pour obtenir des instructions, consultez le contenu relatif à l'administration suivant :
  - Attribuer une application à un groupe d'utilisateurs
  - Attribuer un groupe d'applications à un groupe d'utilisateurs
  - Attribuer une application à un compte d'utilisateur
  - Attribuer un groupe d'applications à un compte d'utilisateur
- Si vous le souhaitez, vous pouvez créer une connexion sécurisée entre BEMS cloud et Microsoft Exchange Server. Pour obtenir des instructions, reportez-vous à Création d'une connexion sécurisée entre BEMS Cloud et Microsoft Exchange Server.
- Configurez BlackBerry Work. Pour obtenir des instructions, consultez le contenu de l'administration de BlackBerry Work, Notes et Tasks.
- Vous pouvez également configurer le service BEMS-Docs. Pour obtenir des instructions, reportez-vous à Activer le service BEMS-Docs.

Accorder l'autorisation d'emprunt d'identité d'application au compte de service

Afin que le service BlackBerry Push Notifications puisse surveiller les mises à jour éventuelles des boites aux lettres, le compte de service BlackBerry Push Notifications doit disposer des autorisations d'emprunt d'identité.

Exécutez la commande Microsoft Exchange Management Shell suivante pour appliquer des autorisations d'emprunt d'identité d'application au compte de service :

- Accorder l'autorisation d'emprunt d'identité d'application à l'aide du centre d'administration Exchange
- Accorder l'autorisation d'emprunt d'identité d'application à l'aide de Microsoft Exchange Management Shell

Accorder l'autorisation d'emprunt d'identité d'application à l'aide du centre d'administration Exchange

1. En fonction de votre environnement, connectez-vous à l'une des consoles suivantes :

Console	Étapes
Console du centre d'administration Microsoft Office 365 Exchange	**a.** Connectez-vous à https://portal.office.com. **b.** Cliquez sur l'icône App Launcher dans l'angle supérieur gauche. **c.** Cliquez sur **Admin**. **d.** Dans le menu de la console du **Centre d'administration Microsoft 365**, cliquez sur **Afficher tout**. **e.** Dans la section **Centres d'administration**, cliquez sur **Tous les centres d'administration**. **f.** Cliquez sur **Exchange**.
Console Web du centre d'administration Microsoft Exchange	**a.** Ouvrez un navigateur, accédez à `https://<url_to_on-premises_client_access_server>/ecp` et connectez-vous avec un compte valide.

2. Cliquez sur **Autorisations**.
3. Cliquez sur +.
4. Saisissez le nom et la description du groupe de rôles.
5. Dans la section **Rôles**, cliquez sur +. Cliquez sur **ApplicationImpersonation > Ajouter > OK**.
6. Dans la section **Membres**, cliquez sur +. Cliquez sur un compte à ajouter, puis sur **Ajouter > OK**.

Accorder l'autorisation d'emprunt d'identité d'application à l'aide de Microsoft Exchange Management Shell

1. Ouvrir Microsoft Exchange Management Shell.
2. Saisir `Attribution d'un nouveau rôle de gestion -Nom :<ImpersonationAssignmentName> -Rôle : emprunt d'identité d'application -Utilisateur :<ServiceAccount>`. Par exemple, `Attribution d'un nouveau rôle de gestion -Nom : emprunt d'identité de l'application BlackBerry -Rôle : emprunt d'identité de l'application -Utilisateur : administrateur BEMS`.

À la fin :

Pour plus d'informations sur la façon de limiter les droits d'emprunt d'identité d'application à des utilisateurs spécifiques, des unités organisationnelles ou des groupes de sécurité, reportez-vous à la bibliothèque MSDN pour consulter Comment : configurer l'emprunt d'identité.

Obtenir un ID d'application Azure pour BEMS avec une authentification basée sur les informations d'identification

1. Connectez-vous à portal.azure.com.
2. Dans la colonne de gauche, cliquez sur **Azure Active Directory**.
3. Cliquez sur **App registrations**.
4. Cliquez sur **New application registration**.
5. Dans le champ **Nom**, saisissez un nom pour l'application.
6. Dans la liste déroulante **Type d'application**, sélectionnez **Natif**.
7. Dans le champ **URI de redirection**, saisissez `https://localhost:8443`.
8. Appuyez sur la touche **Entrée**.
9. Cliquez sur **Créer**.
10. Sélectionnez le nom de l'application que vous avez créée.

11. Cliquez sur **Paramètres**.
12. Cliquez sur **Autorisations requises**.
13. Cliquez sur **Ajouter**.
14. Cliquez sur **Sélectionner une API**.
15. Sélectionnez **Office 365 Exchange Online (Microsoft Exchange)**.
16. Cliquez sur **Sélectionner**.
17. Définissez l'autorisation **Accéder aux boites aux lettres en tant qu'utilisateur connecté via Exchange Web Service** pour Microsoft Office 365.
18. Cliquez sur **Sélectionner**.
19. Cliquez sur **Terminé**.
20. Cliquez sur **Accorder les autorisations**.
21. Cliquez sur **Oui**.
22. Cliquez sur **Ajouter**.
23. Cliquez sur **Sélectionner une API**.
24. Cliquez sur **Microsoft Graph**.
25. Cliquez sur **Sélectionner**.
26. Dans la section **Autorisations déléguées**, cochez la case **Se connecter et lire le profil de l'utilisateur**.
27. Cliquez sur **Sélectionner**.
28. Cliquez sur **Terminé**.
29. Cliquez sur **Accorder les autorisations**.
30. Cliquez sur **Oui**.
31. Copiez l'**ID d'application**. L'ID d'application s'affiche dans la page principale d'**inscriptions des applications** pour l'application spécifiée. Celui-ci est utilisé comme **ID de l'application client**.

Obtenir un ID d'application Azure pour BEMS avec l'authentification basée sur des certificats

1. Connectez-vous à portal.azure.com.
2. Dans la colonne de gauche, cliquez sur **Azure Active Directory**.
3. Cliquez sur **App registrations**.
4. Cliquez sur **New application registration**.
5. Dans le champ **Nom**, saisissez un nom pour l'application.
6. Dans la liste déroulante **Type d'application**, sélectionnez **Application Web / API**.
7. Dans le champ **URI d'authentification**, saisissez `http://<nom de l'application indiquée à l'étape 5>`.

   Cette application est un démon, non une application Web, et n'a pas d'URL d'authentification.
8. Appuyez sur la touche **Entrée**.
9. Cliquez sur **Créer**.
10. Sélectionnez le nom de l'application que vous avez créée.
11. Cliquez sur **Paramètres**.
12. Dans la colonne **Paramètres** , cliquez sur **Propriétés**.
13. Dans la colonne **Propriétés** , copiez l'**URI de l'identifiant Apple**.
14. Cliquez sur **Autorisations requises**.
15. Cliquez sur **Ajouter**.
16. Cliquez sur .
17. Sélectionnez **Office 365 Exchange Online (Microsoft Exchange)Sélectionner une API**.

18. Cliquez sur **Sélectionner**.
19. Dans la section **Sélectionner les autorisations d'application**, cochez la case **Utiliser le service Web Exchange avec accès complet à toutes les boites aux lettres**.
20. Cliquez sur **Sélectionner**.
21. Cliquez sur **Terminé**.
22. Cliquez sur **Accorder les autorisations**.
23. Cliquez sur **Oui**.
24. Cliquez sur **Ajouter**.
25. Cliquez sur **Sélectionner une API**.
26. Cliquez sur **Microsoft Graph**.
27. Cliquez sur **Sélectionner**.
28. Dans la section **Autorisations déléguées**, cochez la case **Se connecter et lire le profil de l'utilisateur**.
29. Cliquez sur **Sélectionner**.
30. Cliquez sur **Terminé**.
31. Cliquez sur **Accorder les autorisations**.
32. Cliquez sur **Oui**.
33. Copiez l'**ID d'application**. L'ID d'application s'affiche dans la page principale d'**inscriptions des applications** pour l'application spécifiée. Celui-ci est utilisé comme **ID de l'application client**.
34. Ne fermez pas portal.azure.com.

À la fin : Associer un certificat avec l'ID d'application Azure pour BEMS

Associer un certificat avec l'ID d'application Azure pour BEMS

Vous pouvez utiliser un certificat existant de votre serveur CA ou la commande New-SelfSignedCertificate pour créer un certificat auto-signé. Pour plus d'informations, visitez le site docs.microsoft.com et lisez le contenu relatif à la commande New-SelfSignedCertificate.

Avant de commencer : Vérifiez que vous avez le nom de l'application que vous avez attribué dans BEMS avec l'authentification basée sur des certificats.

1. Si vous avez un certificat émis par un serveur CA, passez à l'étape 2. Créez un certificat auto-signé.
   a) Sur l'ordinateur exécutant Microsoft Windows, ouvrez Windows PowerShell.
   b) Saisissez la commande suivante : `$cert=New-SelfSignedCertificate -Subject "CN=<nom de l'application>" -CertStoreLocation "Cert:\CurrentUser\My" -KeyExportPolicy Exportable -KeySpec Signature`.
      - Où <*nom de l'application*> correspond au nom que vous avez attribué à l'application à l'étape 5 de la section Obtenir un ID d'application Azure pour BEMS avec l'authentification basée sur des certificats.
   c) Appuyez sur la touche **Entrée**.
2. Exportez le certificat à partir du gestionnaire de certificats. Ceci permet de créer le certificat public. Assurez-vous de sauvegarder le certificat public en tant que fichier .CER ou .PEM.
   a) Sur l'ordinateur exécutant Windows, ouvrez le gestionnaire de certificats pour l'utilisateur connecté.
   b) Développez **Personnel**.
   c) Cliquez sur **Certificats**.
   d) Cliquez avec le bouton droit sur <*utilisateur*>@<*domaine*, puis cliquez sur **Toutes les tâches > Exporter**.
   e) Dans l'**Assistant d'exportation de certificat**, cliquez sur **Non, ne pas exporter la clé privée.**.
   f) Cliquez sur **Suivant**.
   g) Sélectionnez **Base-64 encoded X.509 (.CER)**. Cliquez sur **Suivant**.
   h) Donnez un nom au certificat et enregistrez-le sur votre bureau.

i) Cliquez sur **Suivant**.
j) Cliquez sur **Terminer**.
k) Cliquez sur **OK**.

3. Chargez le certificat public pour associer les informations d'identification du certificat à l'ID d'application Azure pour BEMS.
   a) Dans portal.azure.com, ouvrez le <*nom d'application*> que vous avez attribué à l'application à l'étape 5 de la section Obtenir un ID d'application Azure pour BEMS avec l'authentification basée sur des certificats.
   b) Cliquez sur **Paramètres > Clés**.
   c) Cliquez sur **Charger la clé publique**.
   d) Cliquez sur , puis sélectionnez l'emplacement où vous avez exporté le certificat à l'étape 2.
   e) Cliquez sur **Ouvrir**.
   f) Cliquez sur **Enregistrer**.

À la fin : Exportez le certificat au format .pfx à l'aide du composant logiciel enfichable MMC Gérer les certificats utilisateur. Veillez à inclure la clé privée. Pour obtenir des instructions, visitez le site docs.microsoft.com et lisez le document Exporter un certificat avec la clé privée.

Création d'une connexion sécurisée entre BEMS Cloud et Microsoft Exchange Server

Par défaut, BEMS ne connait que les certificats d'autorité de certification publics. Si vous activez la notification par e-mail pour BlackBerry Work et que le serveur Microsoft Exchange Server de votre organisation n'utilise pas un certificat SSL émis par une autorité de certification approuvée, la connexion entre BEMS Cloud et Microsoft Exchange Server n'est pas fiable. Pour créer une connexion sécurisée avec le serveur Microsoft Exchange Server, téléchargez le certificat SSL du serveur (ou la chaîne de certificat racine ou intermédiaire) dans la base de données Cloud de BEMS. Vous pouvez charger un fichier codé en base64 ou au format binaire qui inclut un ou plusieurs certificats SSL. Lorsque vous chargez un seul fichier qui inclut plusieurs certificats SSL, les certificats s'affichent dans la console de gestion et peuvent être supprimés et remplacés individuellement, si nécessaire. BEMS Cloud prend en charge les extensions de fichier suivantes : .der, .cer, .pem et .crt.

Avant de commencer :

- Configurer les notifications par e-mail de BlackBerry Work Pour obtenir des instructions, reportez-vous à Configurer les notifications e-mail de BlackBerry Work.
- Exportez le certificat SSL depuis le serveur Microsoft Exchange Server au format binaire ou codé en base64 et stockez-le dans un emplacement réseau auquel vous pouvez accéder depuis la console de gestion. Pour plus d'informations sur les certificats numériques et le chiffrement dans Microsoft Exchange Server, consultez la page, https://docs.microsoft.com/en-us/exchange/architecture/client-access/certificates?view=exchserver-2016

1. Dans la barre de menus, cliquez sur **Paramètres > BlackBerry Dynamics**.
2. Cliquez sur **Notifications par e-mail**.
3. Cliquez sur l'onglet **Certificats**.
4. Cliquez sur .
5. Cliquez sur **Ajouter**.
6. Cliquez sur **Parcourir** et accédez à l'emplacement du fichier de certificat que vous souhaitez charger.
7. Cliquez sur **Ajouter**.
8. Si vous chargez des certificats SSL individuels, répétez les étapes 5 à 7 pour chaque fichier supplémentaire.

Remplacer ou supprimer la connexion sécurisée des certificats SSL

Lorsque vous remplacez les certificats SSL (par exemple, lorsque les certificats expirent), tous les certificats SSL existants dans la base de données BEMS sont remplacés. Vous pouvez choisir de charger des certificats SSL

individuels selon vos besoins ou d'inclure plusieurs certificats SSL dans un seul fichier. Les types de fichiers pris en charge sont les suivants : .der, .cer, .pem et .crt.

Avant de commencer :

- Exportez les nouveaux certificats SSL depuis le serveur Microsoft Exchange Server au format binaire ou codé en base64 et stockez-les dans un emplacement réseau auquel vous pouvez accéder depuis la console de gestion. Pour plus d'informations sur les certificats numériques et le chiffrement dans Microsoft Exchange Server, consultez la page, https://docs.microsoft.com/en-us/exchange/architecture/client-access/certificates?view=exchserver-2016

1. Dans la barre de menus, cliquez sur **Paramètres > BlackBerry Dynamics**.
2. Cliquez sur **Notifications par e-mail**.
3. Cliquez sur l'onglet **Certificats**.
4. Cliquez sur .
5. Cliquez sur **Supprimer** sous le certificat que vous souhaitez supprimer.
6. Cliquez sur **Supprimer** pour confirmer la suppression.
7. Ajoutez le nouveau certificat. Pour obtenir des instructions, reportez-vous à Création d'une connexion sécurisée entre BEMS Cloud et Microsoft Exchange Server.

Configurer le message d'avertissement d'expiration du mot de passe

Pour les utilisateurs Active Directory et les groupes d'utilisateurs qui utilisent la méthode PSO (Password Settings Object) pour définir le délai d'expiration du mot de passe, vous pouvez configurer BEMS Cloud pour permettre aux applications BlackBerry Work des utilisateurs d'afficher un message d'avertissement lorsque leur mot de passe Active Directory est sur le point d'expirer.

Remarque : Dans la console de gestion BlackBerry UEM, les notifications par e-mail pour BlackBerry Work doivent être configurées à l'aide du type d'authentification Informations d'identification pour afficher l'onglet Expiration du mot de passe.

Pour plus d'informations sur l'affichage d'un message d'avertissement pour les utilisateurs qui utilisent la méthode GPO (Global Policy Object) pour définir le délai d'expiration du mot de passe, reportez-vous au contenu relatif à l'administration de BlackBerry Work.

Avant de commencer :

- Assurez-vous d'être en possession des informations suivantes :
  - Informations de connexion pour le compte de service utilisé pour s'authentifier auprès du contrôleur de domaine.
  - Nom du serveur LDAP et numéro de port. Le nom du serveur LDAP doit être l'un des contrôleurs de domaine.
- Vérifiez que le compte de service dispose des autorisations READ sur le « Password Settings Container ». Pour obtenir des instructions, reportez-vous à Ajouter une autorisation de lecture au compte utilisé pour l'authentification auprès du serveur LDAP.
- Vérifiez que BlackBerry Connectivity Node est installé et activé dans votre environnement. Pour plus d'informations, reportez-vous à Étapes à suivre pour installer et activer BlackBerry Connectivity Node.
- Vérifiez que les administrateurs utilisent la méthode PSO pour définir le délai d'expiration du mot de passe pour les utilisateurs.
- Vérifiez que les utilisateurs de votre environnement exécutent BlackBerry Work 3.8 ou une version ultérieure.

1. Dans la console de gestion, cliquez sur **Paramètres > BlackBerry Dynamics > Notifications par e-mail**.
2. Cliquez sur l'onglet **Expiration du mot de passe**.
3. Cliquez sur .

4. Cochez la case **Activer l'expiration du mot de passe** pour permettre à BEMS d'interroger Active Directory concernant les détails de l'expiration du mot de passe pour les utilisateurs.
5. Dans le champ **Nom du serveur LDAP**, saisissez le nom du serveur LDAP (par exemple, ldap.<*nom_domaine_DNS*>).
6. Dans le champ **Port LDAP**, saisissez le numéro de port de l'ordinateur LDAP. Le port par défaut est 389.
7. Saisissez le compte de connexion LDAP et le mot de passe. Vous pouvez saisir le compte de connexion au format `domaine\nomd'utilisateur` ou le nom principal de l'utilisateur au format `nomd'utilisateur@domaine`.
8. Dans le champ **DN de base (contrôleur de domaine)**, saisissez le DN de base pour la recherche LDAP. Si cette entrée n'est pas définie, BEMS tente de trouver le DN de base dans l'attribut namingContexts.
9. Vous pouvez également cocher la case **Activer SSL LDAP** pour tunneliser les données via une connexion chiffrée SSL. Si vous activez SSL LDAP, saisissez le numéro de port de l'ordinateur LDAP que vous avez utilisé à l'étape 6. Le numéro de port par défaut est 636. Cette étape nécessite l'importation du certificat LDAP dans le magasin de clés BEMS. Pour obtenir des instructions, reportez-vous à Création d'une connexion sécurisée entre BEMS Cloud et Microsoft Exchange Server.
10. Cliquez sur **Test** pour tester la connexion au serveur LDAP.
11. Cliquez sur **Enregistrer**.

Ajouter une autorisation de lecture au compte utilisé pour l'authentification auprès du serveur LDAP

Vous pouvez utiliser l'outil Éditeur ADSI de Windows Server pour ajouter des autorisations de lecture au compte utilisé pour l'authentification auprès du serveur LDAP. Vous devez être membre du groupe des administrateurs de domaine ou disposer d'autorisations équivalentes pour effectuer cette tâche.

1. Démarrez l'utilitaire Éditeur ADSI.
2. Cliquez avec le bouton droit de la souris sur l'icône de l'**éditeur ADSI**, puis cliquez sur **Connect to** (Se connecter à).
3. Sur l'écran **Connection Settings** (Paramètres de connexion), dans la section **Connection Point** (Point de connexion), sélectionnez **Select a well known Naming Context** (Sélectionner un contexte de nommage connu), puis **Default naming context** (Contexte de nommage par défaut) dans la liste déroulante.
4. Cliquez sur **OK**.
5. Cliquez sur votre domaine.
6. Accédez à **CN=System** et développez-le.
7. Cliquez avec le bouton droit de la souris sur **CN=Password Settings Container** et cliquez sur **Properties** (Propriétés).
8. Dans l'onglet **Security** (Sécurité), cliquez sur **Add** (Ajouter) pour ajouter le compte, ou le groupe d'utilisateurs auquel appartient le compte, utilisé pour l'authentification auprès du serveur LDAP.
9. Sous la zone **Group or user names** (Noms de groupe ou d'utilisateur), avec le compte ou le groupe d'utilisateurs ajouté sélectionné, cochez la case **Read** (Lecture) dans la colonne **Allow** (Autoriser).
10. Cliquez sur **Apply** (Appliquer).
11. Cliquez sur **OK**.

Configuration de BlackBerry Dynamics Launcher

BlackBerry Dynamics Launcher est un composant de l'interface utilisateur auquel on accède dans les applications BlackBerry Dynamics (par exemple, BlackBerry Work) à l'aide du bouton BlackBerry Dynamics Launcher. BlackBerry Dynamics Launcher crée un emplacement d'espace réservé pour les paramètres de

l'application. BlackBerry Dynamics Launcher est un module de bibliothèque doté de nombreuses fonctions, comprenant actuellement les éléments suivants :

- Nom, photo, présence et état de l'utilisateur.
- Liste des modules et des applications optimisés par BlackBerry Dynamics qui sont installés sur le terminal.
- Options de création rapide permettant de rédiger facilement un e-mail, créer une note, planifier un évènement de calendrier ou ajouter un contact, quelle que soit l'application actuellement ouverte.

Dans la console de gestion BlackBerry UEM, les notifications par e-mail émises pour BlackBerry Work doivent être configurées pour afficher BlackBerry Dynamics Launcher et définir une icône personnalisée pour BlackBerry Dynamics Launcher sur les terminaux de l'utilisateur.

Définition d'une icône personnalisée pour BlackBerry Dynamics Launcher

Vous pouvez spécifier une icône personnalisée par défaut pour BlackBerry Dynamics Launcher sur les terminaux des utilisateurs. Lorsque vous spécifiez une icône personnalisée, celle-ci remplace l'icône BlackBerry Dynamics pour tous les utilisateurs gérés par l'instance de BEMS.

Lorsque vous spécifiez une icône personnalisée, assurez-vous que le fichier répond aux exigences suivantes :

- Taille inférieure à 500 Ko. Les icônes de tailles supérieures à 500 Ko ne sont pas ajoutées à la liste des icônes personnalisées.
- Nom au format suivant : <*nom du fichier*>_<*type_périphérique*>_<*résolution*>.png. Par exemple, Icon_iOS_2x.png.

  Où *résolution* représente la résolution prise en charge par le terminal. Par exemple :

  - Terminaux Android : ldpi, mdpi, hdpi, xhdpi, xxhdpi et xxxhdpi
  - Terminaux iOS : 1x, 2x, 3x, etc.
- Enregistré au format .png

Définir une icône personnalisée pour BlackBerry Dynamics Launcher

BEMS Cloud vous permet de définir une icône personnalisée pour les utilisateurs de votre environnement. Lorsque vous ajoutez des icônes personnalisées, BEMS Cloud vérifie la validité des images chargées. Pour plus d'informations sur les exigences relatives aux icônes personnalisées, reportez-vous à la section Définition d'une icône personnalisée pour BlackBerry Dynamics Launcher.

Avant de commencer :

- Vérifiez que les notifications par e-mail émises pour BlackBerry Work sont configurées.
- Vérifiez que vous avez accès à une icône personnalisée prise en charge pour BlackBerry Dynamics Launcher. Pour plus d'informations sur les exigences relatives aux fichiers, reportez-vous à la section Définition d'une icône personnalisée pour BlackBerry Dynamics Launcher.

1. Dans la console de gestion BlackBerry UEM, cliquez sur **Paramètres > BlackBerry Dynamics > Launcher Branding** dans la barre de menus.
2. Cochez la case **Afficher l'icône personnalisée dans le lanceur d'applications**.
3. Cliquez sur l'onglet correspondant au terminal pour lequel vous souhaitez spécifier l'icône de lancement. Android est sélectionné par défaut.
4. Cliquez sur +.
5. Accédez à l'emplacement du fichier d'icône. Cliquez sur le fichier, puis sur **Ouvrir**.
6. Cliquez sur **Submit**.
7. Cliquez sur **Enregistrer**.
8. Répétez les étapes 4 à 6 pour chaque résolution de fichier d'icône de terminal Android personnalisée.
9. Suivez les étapes 3 à 6 pour la résolution de fichier d'icône de terminal iOS personnalisée.

Supprimer une icône personnalisée pour BlackBerry Dynamics Launcher

Vous pouvez choisir de supprimer une icône personnalisée que vous avez spécifiée pour BlackBerry Dynamics Launcher. Si vous supprimez tous les fichiers d'icônes personnalisées, l'icône Launcher par défaut est utilisée sur les terminaux clients de l'application Launcher.

1. Dans la console de gestion BlackBerry UEM, cliquez sur **Paramètres > BlackBerry Dynamics > Launcher Branding** dans la barre de menus.
2. Cliquez sur l'onglet du terminal dont vous souhaitez supprimer l'icône Launcher personnalisée.
3. Cliquez sur ✕ en regard de l'icône personnalisée que vous souhaitez supprimer.
4. Cliquez sur **Enregistrer**.

Configuration de BEMS-Docs

Vous pouvez utiliser la console BlackBerry UEM pour configurer et gérer les référentiels de documents et de fichiers, ainsi que les stratégies d'accès pour les utilisateurs des applications mobiles du service. Lorsqu'elle est activée, les utilisateurs peuvent accéder aux documents, les synchroniser et les partager à l'aide des services de stockage suivants : Microsoft SharePoint Online, Microsoft SharePoint, Microsoft OneDrive for Business et Box. Les fournisseurs de stockage de référentiel basés sur le partage de fichiers et sur le système CMIS ne sont pas pris en charge.

Remarque : Si votre environnement exige que les utilisateurs accèdent à des partages de fichiers ou à des référentiels basés sur CMIS, configurez BEMS-Docs dans une instance BEMS sur site. L'activation de BEMS-Docs dans BlackBerry UEM Cloud et dans une instance BEMS sur site dans un environnement BlackBerry UEM Cloud n'est pas prise en charge. Pour plus d'informations, reportez-vous à Configuration d'une instance de BEMS sur site dans un environnement BlackBerry UEM Cloud.

Référentiels : le service BEMS-Docs permet à vos utilisateurs d'accéder aux données professionnelles stockées à partir de leurs terminaux mobiles. Un référentiel Docs (également appelé « partage ») existe sur un serveur professionnel. Le référentiel contient des fichiers partagés par des utilisateurs autorisés. Pour plus d'informations sur la configuration et la gestion de vos partages dans BlackBerry UEM et sur l'accès utilisateur associé, reportez-vous à Gestion des référentiels. Avant de configurer vos référentiels, activez et configurez le service BEMS-Docs et configurez BlackBerry Work dans BlackBerry UEM pour permettre à vos utilisateurs d'accéder aux référentiels que vous ajoutez et définissez depuis leur terminal.

Services de stockage : le service BEMS-Docs prend en charge un certain nombre de services de stockage.

Étapes de configuration de BEMS-Docs

Pour configurer BEMS-Docs, procédez comme suit :

Étape	Action
1	Activer le service BEMS-Docs.
2	Configurer les paramètres BEMS-Docs.
3	Créer une connexion sécurisée entre BEMS-Docs et Microsoft SharePoint.

Étape	Action
4	Gestion des référentiels.
5	Attribuez le droit Feature - Docs Service Entitlement (com.good.feature.share) aux utilisateurs pour permettre à BlackBerry Work Docs de se connecter au service BEMS-Docs. Pour obtenir des instructions, consultez le contenu relatif à l'administration suivant : • Attribuer une application à un groupe d'utilisateurs • Attribuer un groupe d'applications à un groupe d'utilisateurs • Attribuer une application à un compte d'utilisateur • Attribuer un groupe d'applications à un compte d'utilisateur

Activer le service BEMS-Docs

Pour permettre aux utilisateurs d'accéder aux référentiels de documents et de fichiers dans votre environnement, vous devez activer le service BEMS-Docs. Lorsque vous activez ce service, un locataire BEMS est créé et l'autorisation pour le service BlackBerry Cloud Docs (com.blackberry.gdservice-entitlement.docs.cloud) est ajoutée au profil de connectivité BlackBerry Dynamics. Si votre environnement utilise à la fois le service BEMS-Docs et les notifications par e-mail pour BlackBerry Work, configurez d'abord les notifications par e-mail. Pour obtenir des instructions, reportez-vous à Configurer les notifications e-mail de BlackBerry Work.

Pour activer le service BEMS-Docs, l'autorisation pour le service BlackBerry Cloud Docs (com.blackberry.gdservice-entitlement.docs.cloud) doit être présent dans la section Organisation > Autorisations dans https://account.blackberry.com. Cette autorisation d'application n'a pas besoin d'être attribuée aux utilisateurs dans BlackBerry UEM Cloud.

1. Dans la console de gestion, cliquez sur **Paramètres > BlackBerry Dynamics > Docs**.
2. Cliquez sur **Activer**.

Configurer les paramètres BEMS-Docs

Avant de commencer :

- Vérifiez que le service BEMS-Docs est activé.
- Si votre environnement est configuré pour Microsoft SharePoint Online ou Azure-IP, assurez-vous que l'application BlackBerry Work est enregistrée dans Azure pour pouvoir accéder à l'application BEMS-Docs Azure. Pour obtenir des instructions, reportez-vous à la section Obtenir un ID d'application Azure pour BlackBerry Work dans le contenu d'administration BlackBerry Work, Notes et Tasks.
- Si votre environnement est configuré pour Azure-IP, munissez-vous des informations suivantes :
  - Nom du locataire Azure
  - ID d'application Azure du service BEMS
  - Clé d'application Azure du service BEMS
- Si BEMS-Docs est configuré pour communiquer avec un système sur site Microsoft SharePoint, assurez-vous que les référentiels Microsoft SharePoint utilisent des ports sécurisés https. L'utilisation de ports non sécurisés http n'est pas prise en charge.

1. Dans la console de gestion, cliquez sur **Paramètres > BlackBerry Dynamics > Docs**.
2. Cliquez sur l'onglet **Paramètres**.
3. Effectuez l'une ou l'autre des tâches suivantes, ou les deux.

Environnement	Étapes
Votre environnement est configuré pour utiliser Microsoft SharePoint Online ou Azure-IP et Microsoft SharePoint Online	**a.** Si nécessaire, cochez la case **Activer la protection des données Azure** pour permettre à BEMS-Docs de s'authentifier sur Azure-IP. **b.** Saisissez le nom du locataire Azure. **c.** Saisissez l'ID d'application Azure du service BEMS que vous avez obtenu lorsque vous avez enregistré le service de composants BEMS-Docs. Pour obtenir des instructions, reportez-vous à la section Obtenir un ID d'application Azure pour le service de composants BEMS-Docs. **d.** Saisissez la clé d'application Azure du service BEMS que vous avez obtenue lorsque vous avez enregistré l'application Docs dans Azure. Pour obtenir des instructions, reportez-vous à la section Obtenir un ID d'application Azure pour le service de composants BEMS-Docs.
Votre environnement est configuré pour utiliser un environnement Microsoft SharePoint sur site	**a.** Cochez la case **Activer le routage BlackBerry Connectivity Node** pour permettre à BEMS Cloud de se connecter à BlackBerry Infrastructure au lieu d'utiliser un port d'entrée. Ce paramètre exige que le BlackBerry Connectivity Node soit installé et configuré dans votre environnement. **b.** Pour permettre à BEMS-Docs de communiquer avec un serveur Microsoft SharePoint sur site, extrayez le certificat du serveur Microsoft SharePoint et envoyez-le à l'assistance BlackBerry. Si les sites Microsoft SharePoint sur site utilisent des certificats qui ne sont pas publiquement approuvés (par exemple, des certificats auto-signés ou des certificats d'AC d'entreprise), envoyez ces certificats à l'assistance BlackBerry.

4. Cliquez sur **Enregistrer**.

Obtenir un ID d'application Azure pour le service de composants BEMS-Docs

Lorsque votre environnement est configuré pour Microsoft SharePoint Online, Microsoft OneDrive for Business ou Microsoft Azure-IP, vous devez enregistrer les services de composants BEMS dans Azure.

Si votre environnement utilise à la fois Microsoft SharePoint Online et Microsoft Azure-IP ou Microsoft OneDrive for Business et Microsoft Azure-IP, vous devez enregistrer le service Microsoft SharePoint Online ou Microsoft OneDrive for Business. Microsoft Azure-IP utilisera les mêmes informations que le service enregistré.

Avant de commencer : Pour accorder des autorisations, vous devez utiliser un compte disposant des autorisations d'administrateur de locataires.

1. Connectez-vous à portal.azure.com.
2. Dans la colonne de gauche, cliquez sur **Azure Active Directory**.
3. Cliquez sur **App registrations**.
4. Cliquez sur **Nouvelle inscription**.
5. Dans le champ **Nom**, saisissez un nom pour l'application. Par exemple, AzureAppIDforBEMS.
6. Sélectionnez un type de compte pris en charge.
7. Dans la liste déroulante **Rediriger l'URI**, sélectionnez **Web** et saisissez `https://localhost:8443`.
8. Cliquez sur **S'inscrire**.
9. Notez l'**ID d'application (client)**. Il s'agit de la valeur de l'**ID d'application Azure du service BEMS** dans la console de gestion BlackBerry UEM.Il s'agit de la valeur de l'**l'ID d'application Azure du service BEMS** pour le service Docs > Paramètres dans le tableau de bord BEMS.
10. Dans la section **Gérer**, cliquez sur **Autorisations d'API**.

11. Cliquez sur **Ajouter une autorisation**.

12. Effectuez une ou plusieurs des tâches suivantes :

Service	autorisations ;
Si vous configurez BEMS-Docs pour utiliser Microsoft SharePoint Online ou Microsoft OneDrive for Business	**a.** Recherchez **SharePoint** et cliquez dessus. **b.** Définissez les autorisations suivantes : • Dans les autorisations de l'application, supprimez toutes les autorisations. **1.** Cliquez sur **Autorisations de l'application**. **2.** Cliquez sur Développer tout. Assurez-vous que toutes les options sont désactivées. • Dans les autorisations déléguées, cochez la case **Lire et écrire les éléments et les listes dans toutes les collections de sites**. Aucun. Décochez les cases correspondant à toutes les options. • Dans les **autorisations déléguées**, cochez la case **Lire et écrire les éléments et les listes dans toutes les collections de sites**. (**AllSite > AllSites.Manage**) **c.** Cliquez sur **Ajouter des autorisations**.
Si vous utilisez Microsoft Azure-IP	**a.** Cliquez sur **Microsoft Graph**. Si Microsoft Graph n'est pas répertorié, ajoutez Microsoft Graph. **b.** Définissez les autorisations suivantes : • Dans les autorisations de l'application, cochez la case **Lire les données du répertoire** (**Directory > Directory.Read.All**). • Dans les autorisations déléguées, cochez la case **Lire les données du répertoire** (**Directory > Directory.Read.All**). **c.** Cliquez sur **Mettre à jour des autorisations**. **d.** **Ajouter une autorisation**. **e.** Dans la section **Sélectionner une API**, cliquez sur **Services Azure Rights Management**. Définissez les autorisations suivantes : • Dans les autorisations de l'application, sélectionnez toutes les autorisations. **1.** Cliquez sur **Autorisations de l'application**. **2.** Assurez-vous que toutes les options de contenu sont sélectionnées. • Dans les autorisations déléguées, cochez la case **user_impersonation**. **f.** Cliquez sur **Ajouter des autorisations**. **g.** Cliquez sur **Ajouter une autorisation**. **h.** Dans la section **Sélectionner une API**, cliquez sur **API utilisées par mon organisation**. **i.** Recherchez **Service de synchronisation de la protection des données Microsoft** et cliquez dessus. Définissez l'autorisation suivante : • Dans les autorisations déléguées, cochez la case **Lire toutes les stratégies unifiées auxquelles un utilisateur a accès** (**UnifiedPolicy > UnifiedPolicy.User.Read**). **j.** Cliquez sur **Ajouter des autorisations**.

13. Patientez quelques minutes, puis cliquez sur **Accorder le consentement de l'administrateur**. Cliquez sur **Oui**.

Important : Cette étape nécessite des privilèges d'un administrateur locataire.

14. Pour permettre à la découverte automatique de fonctionner comme prévu, définissez les autorisations d'authentification. Procédez comme suit :
    a) Dans la section **Gérer**, cliquez sur **Authentification**.
    b) Dans la section **Autoriser les flux de client public**, sélectionnez **Oui** pour **Activer les flux mobiles et de bureau suivants**.
    c) Cliquez sur **Enregistrer**.
15. Définissez l'étendue et la fiabilité de cette API. Dans la section **Gérer**, cliquez sur **Exposer une API**. Réalisez les tâches ci-dessous.

Tâche	Étapes
Ajouter une étendue	L'étendue limite l'accès aux données et aux fonctionnalités protégées par l'API. **a.** Cliquez sur **Ajouter une étendue**. **b.** Cliquez sur **Enregistrer et continuer**. **c.** Renseignez les champs et les paramètres suivants : • Nom d'étendue : indiquez un nom unique pour l'étendue. • Qui peut donner son accord : cliquez sur **Administrateurs et utilisateur**. • Nom d'affichage du consentement de l'administrateur : saisissez un nom descriptif. • Description du consentement de l'administrateur : saisissez une description de l'étendue. • État : Cliquez sur **Activé**. Par défaut, l'état est Activé. **d.** Cliquez sur **Ajouter une étendue**.
Ajouter une application client	L'autorisation d'une application client indique que l'API fait confiance à l'application et que les utilisateurs ne doivent pas être invités à donner leur consentement. **a.** Cliquez sur **Ajouter une application client**. **b.** Dans le champ **ID client**, saisissez l'ID client que vous avez enregistré à l'étape 9 ci-dessus. **c.** Cochez la case **Étendues autorisées** pour spécifier le type de jeton renvoyé par le service. **d.** Cliquez sur **Ajouter une application**.

16. Dans la section **Gérer**, cliquez sur **Certificats et secrets** et ajoutez un secret de client. Procédez comme suit :
    a) Cliquez sur **Nouveau secret de client**.
    b) Dans le champ **Description**, saisissez une description de clé comportant jusqu'à 16 caractères, espaces compris.
    c) Définissez une date d'expiration (par exemple, Dans 1 an, Dans 2 ans, N'expire jamais).
    d) Cliquez sur **Ajouter**.
    e) Copiez la **Valeur** de la clé.

    Important : La valeur n'est disponible que lorsque vous la créez. Vous ne pouvez pas y accéder après avoir quitté la page. Il s'agit de la valeur de la **Clé d'application Azure du service BEMS** dans la console BlackBerry UEM.

Autoriser l'authentification sur BEMS-Docs à l'aide d'une autre adresse e-mail

Vous pouvez configurer BEMS Cloud pour permettre aux utilisateurs de s'authentifier auprès de Microsoft SharePoint Online et Microsoft OneDrive for Business avec une adresse e-mail différente de l'adresse e-mail utilisée pour installer et activer BlackBerry Work. Pour activer cette fonctionnalité, contactez l'assistance technique BlackBerry.

Créer une connexion sécurisée entre BEMS-Docs et Microsoft SharePoint

Par défaut, BEMS Cloud ne connait que les certificats d'autorité de certification publics. Si vous activez le service BEMS-Docs et que l'instance de Microsoft SharePoint sur site de votre organisation n'utilise pas de certificat SSL émis par une autorité de certification approuvée pour les sites HTTPS, la connexion entre le service BEMS-Docs et l'instance de Microsoft SharePoint sur site n'est pas fiable et les utilisateurs ne pourront pas accéder aux fichiers et documents depuis l'application BlackBerry Work Docs. Pour créer une connexion sécurisée avec Microsoft SharePoint, chargez le certificat SSL du serveur, s'il s'agit d'un certificat autosigné, ou la chaine de certificat racine ou intermédiaire dans la base de données BEMS Cloud. Vous pouvez charger un fichier codé en base64 ou au format binaire qui inclut un ou plusieurs certificats SSL. Lorsque vous chargez un seul fichier qui inclut plusieurs certificats SSL, les certificats s'affichent dans la console de gestion et peuvent être supprimés et remplacés individuellement, si nécessaire. BEMS Cloud prend en charge les extensions de fichier suivantes : .der, .cer, .pem et .crt.

Avant de commencer :

- Vérifiez que vous avez activé le service BEMS-Docs.
- Exportez le certificat SSL depuis le serveur Microsoft SharePoint au format binaire ou codé en base64 et stockez-le dans un emplacement réseau auquel vous pouvez accéder depuis la console de gestion.

1. Dans le menu, cliquez sur **Paramètres > BlackBerry Dynamics > Docs**.
2. Cliquez sur l'onglet **Certificat**.
3. Cliquez sur **Ajouter** et accédez à l'emplacement du fichier de certificat que vous souhaitez charger.
4. Cliquez sur **Ajouter**.
5. Si le chargement échoue, corrigez le problème identifié et réessayez.
6. Si vous chargez des certificats SSL individuels, répétez les étapes 3 à 4 pour chaque fichier supplémentaire.

Remplacer ou supprimer le certificat de connexion sécurisée de BEMS-Docs

Lorsque vous remplacez les certificats SSL (par exemple, lorsque les certificats expirent), tous les certificats SSL existants dans la base de données BEMS Cloud sont remplacés. Vous pouvez choisir de charger des certificats SSL individuels selon vos besoins ou d'inclure plusieurs certificats SSL dans un seul fichier. Les types de fichiers pris en charge sont les suivants : .der, .cer, .pem et .crt.

Avant de commencer : Exportez les nouveaux certificats SSL depuis l'instance de Microsoft SharePoint sur site au format binaire ou codé en base64 et stockez-les dans un emplacement réseau auquel vous pouvez accéder depuis la console de gestion.

1. Dans le menu, cliquez sur **Paramètres > BlackBerry Dynamics > Docs**.
2. Cliquez sur l'onglet **Certificat**.
3. Cliquez sur **Supprimer** sous chacun des certificats que vous souhaitez supprimer. Cliquez sur **Supprimer**.
4. Ajoutez les nouveaux fichiers de certificat selon vos besoins. Pour obtenir des instructions, reportez-vous à Créer une connexion sécurisée entre BEMS-Docs et Microsoft SharePoint.

Gestion des référentiels

BEMS Cloud possède les fournisseurs de stockage de référentiel suivants :

Référentiel de stockage	Description
SharePoint	Serveur Web sécurisé contenant des fichiers partagés accessibles via Internet.
SharePoint Online	Si votre environnement est configuré pour Microsoft OneDrive for Business, le référentiel de stockage SharePoint Online est utilisé.
Box	Compte de stockage Cloud sécurisé fourni par box.com contenant des fichiers partagés accessibles via Internet.

Un référentiel est ensuite classé dans le service BEMS-Docs à l'aide du nom de l'utilisateur qui l'a ajouté et défini.

Référentiel de stockage	Description
Défini par l'administrateur	Sites de fournisseurs de stockage ajoutés et entretenus par les administrateurs BlackBerry UEM auxquels les utilisateurs individuels et les groupes d'utilisateurs ont accès.
Défini par l'utilisateur	Sites ajoutés par des utilisateurs finaux individuels à partir de leurs terminaux mobiles auxquels vous, en tant qu'administrateur BlackBerry UEM, pouvez annuler et rétablir l'accès mobile conformément aux politiques d'utilisation du matériel informatique de votre entreprise.

Configuration des référentiels

La page Configuration des référentiels comporte les trois onglets suivants que vous pouvez configurer :

Onglets	Description
Défini par l'administrateur	Cet onglet vous permet de créer et de gérer des référentiels, d'ajouter et de supprimer des utilisateurs et des groupes d'utilisateurs, et d'attribuer aux utilisateurs et aux groupes d'utilisateurs des droits d'accès aux fichiers et des droits d'utilisation.
Défini par l'utilisateur	Cet onglet vous permet d'ajouter et de supprimer des utilisateurs et des groupes d'utilisateurs, d'activer et de désactiver la possibilité de créer des référentiels définis par l'utilisateur, et d'accorder et d'annuler les autorisations d'effectuer une série d'actions liées aux fichiers sur leurs référentiels définis par l'utilisateur.
Utilisateurs	Vous permet de rechercher un utilisateur sur une instance de BlackBerry UEM Cloud pour afficher les référentiels autorisés par chemin ou par priorité, et l'utilisateur qui a défini le partage (par exemple, administrateur ou utilisateur).

Partages définis par l'administrateur

Les partages sont des référentiels de documents pour un fournisseur de stockage particulier.

Lorsque vous définissez des référentiels et des listes, procédez comme suit :

Étape	Action
1	Définir un référentiel.
2	Définissez les autorisations d'accès des utilisateurs et des groupes d'utilisateurs.

Octroi des autorisations d'accès aux utilisateurs

Les autorisations d'accès sont définies pour un référentiel unique ou héritées d'une liste existante de référentiels. Les autorisations peuvent être accordées de manière sélective aux utilisateurs de domaine Microsoft Active Directory et aux groupes d'utilisateurs existants. Au moins un utilisateur ou un groupe d'utilisateurs doit être ajouté à la définition du référentiel pour configurer les autorisations d'accès.

Le tableau suivant répertorie les autorisations d'accès et le paramètre par défaut disponibles.

Autorisation	Attributs des autorisations	Paramètre par défaut
Liste (Parcourir)	Afficher et parcourir le contenu du référentiel (par exemple, les sous-dossiers et les fichiers) dans une liste affichée, et trier les listes par nom, date, taille ou type	Activé
Supprimer des fichiers	Supprimer des fichiers du référentiel	Activé
Lire (Télécharger)	Télécharger les fichiers de référentiel sur le terminal de l'utilisateur et les ouvrir pour les lire	Activé
Écrire (charger)	Télécharger des fichiers (nouveaux/modifiés) à partir du terminal de l'utilisateur vers le référentiel pour le stockage	Activé
Cache (fichiers hors ligne)	Stockez temporairement un cache de fichiers de référentiel sur le terminal pour un accès hors ligne. Vous pouvez désigner les fichiers et les dossiers à synchroniser avec le dossier hors ligne de l'application BlackBerry Work Docs des utilisateurs.	Activé
Ouvrir dans	Ouvrir un fichier dans une application compatible avec le format sur le terminal	Activé
Créer un dossier	Ajouter de nouveaux dossiers au référentiel	Activé
Copier/Coller	Copier le contenu du fichier de référentiel et le coller dans un autre fichier ou une autre application	Activé
Enregistrer/ Désenregistrer	Lorsqu'un fichier est désenregistré, l'utilisateur peut le modifier, le fermer, le rouvrir et travailler hors ligne. Les autres utilisateurs ne peuvent pas modifier le fichier ou afficher les modifications tant qu'il n'est pas réenregistré	Activé (SharePoint uniquement)

Autorisation	Attributs des autorisations	Paramètre par défaut
Générer un lien partagé	Les utilisateurs peuvent générer un lien vers un fichier et un dossier et envoyer ce lien à des destinataires La fonction Générer un lien partagé nécessite une application BlackBerry Work mise à jour.	Activé (Box uniquement)

Modifier les autorisations d'accès

1. Dans la console de gestion, cliquez sur **Paramètres > BlackBerry Dynamics > Docs**.
2. Cliquez sur **Référentiels**.
3. Cliquez sur l'onglet **Défini par l'administrateur**.
4. Cliquez sur un référentiel.
5. Sous **Autorisations d'accès**, en regard de l'utilisateur ou du groupe d'utilisateurs, cochez ou décochez la case des autorisations que vous souhaitez modifier.
6. Cliquez sur ⊗ en regard d'un utilisateur ou de groupes d'utilisateurs que vous souhaitez supprimer.
7. Cliquez sur **Enregistrer**.

Définir un référentiel

Les utilisateurs et les groupes BlackBerry UEM doivent être ajoutés à une définition de référentiel avant que les autorisations d'accès puissent être configurées. Les utilisateurs et les groupes ajoutés reçoivent automatiquement les autorisations d'accès par défaut.

Avant de commencer : Pour que les utilisateurs puissent accéder à leurs référentiels Microsoft SharePoint sur leurs terminaux, assurez-vous qu'ils disposent du niveau d'autorisation Lecture et de l'autorisation Parcourir les répertoires.

1. Dans la console de gestion, cliquez sur **Paramètres > BlackBerry Dynamics > Docs**.
2. Cliquez sur **Référentiels**.
3. Cliquez sur l'onglet **Défini par l'administrateur**.
4. Cliquez sur +.
5. Dans le champ **Nom**, saisissez le nom du référentiel qui sera affiché aux utilisateurs ayant un accès mobile au référentiel.

   Le nom du référentiel doit être unique et peut contenir des espaces. Les caractères spéciaux suivants ne peuvent pas être utilisés en raison des limitations de tiers :

   - Microsoft SharePoint 2010, 2013, 2016 et 2019 : ~ " # % & * : < > ? / \ { | }
   - Box : \ /|
6. Dans la liste déroulante **Stockage**, sélectionnez un fournisseur de stockage.

   Si vous sélectionnez **SharePoint** ou **SharePoint Online** et que le partage exécute SharePoint 2013 ou une version ultérieure, cochez la case **Ajouter des sites, puis les utilisateurs de ce site** pour que cette fonctionnalité soit disponible pour les utilisateurs de ce partage. Ce paramètre s'applique uniquement aux (my) sites SharePoint ou OneDrive for Business personnels.

   Si votre environnement est configuré pour Microsoft OneDrive for Business, sélectionnez le fournisseur de stockage SharePoint Online.
7. Dans le champ **Chemin**, spécifiez le chemin d'accès au partage. Effectuez une des tâches suivantes en fonction du type de stockage que vous avez sélectionné à l'étape 6.

Les variables suivantes sont prises en charge dans le champ Chemin :

- username
- NomDeCompteSAM
- mail
- dnsdomain
- Si le site personnel comprend des noms d'utilisateur, saisissez le chemin d'accès comprenant ces variables. Par exemple, https://sharepoint.exemple.com/my/<NomDeCompteSAM>.

Type de stockage	Description
Box	Saisissez une URL entièrement qualifiée avec ou sans les variables prises en charge listées ci-dessus.
SharePoint SharePoint Online	Si votre fournisseur de stockage estMicrosoft OneDrive for Business, effectuez cette tâche. Saisissez une URL entièrement qualifiée avec ou sans les variables prises en charge listées ci-dessus. Pour ajouter « my » (mes) sites ou des sites SharePoint personnels, spécifiez l'URL de « my » (mon) site. Par exemple, • Si votre environnement utilise SharePoint et SharePoint Online, https://<*serveur Microsoft SharePoint*>/my. • Si votre environnement utilise Microsoft OneDrive for Business, *https://<votre domaine O365>-my.sharepoint.com/personal/admin_<domain>_onmicrosoft_com/_layouts/15/onedrive.aspx* Sinon, pour ajouter automatiquement les sites suivis, procédez comme suit : **a.** Ajoutez un référentiel pour « my » (mon) ou un site SharePoint personnel. **b.** Sélectionnez **Ajouter des sites, puis les utilisateurs de ce site** pour le référentiel. **c.** Dans l'onglet **Définis par l'utilisateur**, activez une autorisation de référentiel définie par l'utilisateur. Veillez à cocher les cases **Activer les partages définis par l'utilisateur** et **Ajouter automatiquement des sites suivis par les utilisateurs**. Pour obtenir des instructions, reportez-vous à Activer les autorisations de référentiel définies par l'utilisateur.

8. Dans la section **Autorisations d'accès**, cliquez sur +.
9. Sélectionnez l'une des options suivantes :
   - **Utilisateurs** : dans la boîte de dialogue **Ajouter un utilisateur**, saisissez une chaîne de recherche complète ou partielle. Cliquez sur l'utilisateur que vous souhaitez ajouter.
   - **Groupes** : dans l'écran **Ajouter un groupe**, sélectionnez un ou plusieurs groupes. Cliquez sur →. Cliquez sur **Ajouter**.
10. Cliquez sur **Ajouter**.
11. Cliquez sur **Enregistrer**. Si l'enregistrement échoue et que le problème est identifié, le message d'erreur adéquat s'affiche (par exemple, si vous avez un référentiel nommé Marketing et que vous créez un autre référentiel portant le même nom, le message d'erreur **Un référentiel nommé Marketing existe déjà** s'affiche). Corrigez l'erreur indiquée et procédez à un nouvel enregistrement.

Ajouter des utilisateurs et des groupes d'utilisateurs aux référentiels

Les utilisateurs et les groupes Microsoft Active Directory doivent être ajoutés à une définition de référentiel avant que les autorisations d'accès puissent être configurées. Les utilisateurs et les groupes ajoutés reçoivent automatiquement les autorisations d'accès par défaut.

1. Dans la console de gestion, cliquez sur **Paramètres > BlackBerry Dynamics > Docs**.
2. Cliquez sur **Référentiels**.
3. Cliquez sur l'onglet **Défini par l'administrateur**.
4. Cliquez sur un référentiel.
5. Sous **Autorisations d'accès**, cliquez sur +.
6. Sélectionnez l'une des options suivantes :
   - **Utilisateurs** : dans le champ **Ajouter un utilisateur**, saisissez une chaîne de recherche complète ou partielle. Cliquez sur l'utilisateur que vous souhaitez ajouter.
   - **Groupes** : dans l'écran **Ajouter un groupe**, sélectionnez un ou plusieurs groupes. Cliquez sur →. Cliquez sur **Ajouter**.
7. Cliquez sur **Ajouter**.
8. Cliquez sur **Enregistrer**.

À la fin : Accordez des droits d'accès aux utilisateurs et aux groupes d'utilisateurs.

Modifier un référentiel

1. Dans la console de gestion, cliquez sur **Paramètres > BlackBerry Dynamics > Docs**.
2. Cliquez sur **Référentiels**.
3. Cliquez sur l'onglet **Défini par l'administrateur**.
4. Cliquez sur un référentiel que vous voulez modifier.
5. Apportez les modifications nécessaires.
6. Cliquez sur **Enregistrer**.

Autoriser les référentiels définis par l'utilisateur

Lorsque vous autorisez les utilisateurs à définir leurs propres référentiels, vous effectuez les opérations suivantes :

1. Activer les autorisations de référentiel définies par l'utilisateur
2. Modifier les autorisations d'accès utilisateur

Activer les autorisations de référentiel définies par l'utilisateur

Avant de commencer : Pour que les utilisateurs puissent accéder à leurs référentiels Microsoft SharePoint sur leurs terminaux, assurez-vous qu'ils disposent du niveau d'autorisation Lecture et de l'autorisation Parcourir les répertoires.

1. Dans la console de gestion, cliquez sur **Paramètres > BlackBerry Dynamics > Docs**
2. Cliquez sur **Référentiels**.
3. Cliquez sur l'onglet **Définis par l'utilisateur**.
4. Cochez la case **Activer les partages définis par l'utilisateur** pour permettre à vos utilisateurs mobiles de définir leurs propres sources de données.

5. Si nécessaire, cochez la case **Ajouter automatiquement des sites suivis des utilisateurs** pour les référentiels Microsoft SharePoint autorisés avec le plug-in MySite requis activé.

   Pour ajouter automatiquement les sites suivis, procédez comme suit :

   a. Dans l'onglet Définis par l'administrateur, ajoutez un référentiel pour « mon » site ou un site SharePoint personnel. Pour obtenir des instructions, reportez-vous à Définir un référentiel.
   b. Sélectionnez **Ajouter des sites, puis les utilisateurs de ce site** pour le référentiel.
   c. Dans l'onglet Définis par l'utilisateur, veillez à cocher les cases **Activer les partages définis par l'utilisateur** et **Ajouter automatiquement des sites suivis par les utilisateurs**.
6. Dans la section **Stockage**, sélectionnez un ou plusieurs services de stockage.

   Si vous ne sélectionnez pas au moins une option de stockage, l'option définie par l'utilisateur est désactivée.
7. Dans la section **Autorisations d'accès**, cliquez sur +.
8. Sélectionnez **Utilisateurs** ou **Groupes**.
9. Sélectionnez l'une des options suivantes :

   - **Utilisateurs** : Dans le champ **Ajouter un utilisateur**, saisissez une chaîne de recherche complète ou partielle. Cliquez sur l'utilisateur que vous souhaitez ajouter.
   - **Groupes** : Dans l'écran **Ajouter un groupe**, sélectionnez un ou plusieurs groupes. Cliquez sur →. Cliquez sur **Ajouter**.
10. Cliquez sur **Ajouter**. Les utilisateurs et les groupes ajoutés reçoivent automatiquement les autorisations d'accès par défaut.
11. Cliquez sur **Enregistrer**.

Autorisations d'accès

Les autorisations peuvent être accordées de manière sélective aux groupes d'utilisateurs et aux utilisateurs de domaine Microsoft Active Directory existants. Les autorisations les plus restrictives (définies par l'administrateur ou définies par l'utilisateur) sont appliquées.

Le tableau suivant répertorie les autorisations fournies par défaut lorsque vous ajoutez des utilisateurs et des groupes aux référentiels définis par l'utilisateur.

Autorisation	Attributs des autorisations	Paramètre par défaut
Liste (Parcourir)	Afficher et parcourir le contenu du référentiel (par exemple, les sous-dossiers et les fichiers) dans une liste affichée, et trier les listes par nom, date, taille ou type	Activé
Supprimer des fichiers	Supprimer des fichiers du référentiel	Activé
Lire (Télécharger)	Télécharger les fichiers de référentiel sur le terminal de l'utilisateur et les ouvrir pour les lire	Activé
Écrire (charger)	Télécharger des fichiers (nouveaux/modifiés) à partir du terminal de l'utilisateur vers le référentiel pour le stockage	Activé

Autorisation	Attributs des autorisations	Paramètre par défaut
Cache (fichiers hors ligne)	Stocker temporairement un cache de fichiers de référentiel sur le terminal pour un accès hors ligne Vous pouvez désigner les fichiers et les dossiers à synchroniser avec le dossier hors ligne de l'application BlackBerry Work Docs des utilisateurs.	Activé
Ouvrir dans	Ouvrir un fichier dans une application compatible avec le format sur le terminal	Activé
Créer un dossier	Ajouter de nouveaux dossiers au référentiel	Activé
Copier/Coller	Copier le contenu du fichier de référentiel et le coller dans un autre fichier ou une autre application	Activé
Enregistrer/ Désenregistrer	Lorsqu'un fichier est désenregistré, l'utilisateur peut le modifier, le fermer, le rouvrir et travailler hors ligne. Les autres utilisateurs ne peuvent pas modifier le fichier ou afficher les modifications tant qu'il n'est pas réenregistré	Activé (SharePoint uniquement)
Ajouter de nouveaux référentiels	Permet l'ajout de nouveaux référentiels à partir du terminal mobile de l'utilisateur	Désactivé
Générer un lien partagé	Les utilisateurs peuvent générer un lien vers un fichier et un dossier et envoyer ce lien à des destinataires La fonction Générer un lien partagé nécessite une application BlackBerry Work mise à jour.	Activé (Box uniquement)

Modifier les autorisations d'accès utilisateur

1. Dans la console de gestion, cliquez sur **Paramètres > BlackBerry Dynamics > Docs**.
2. Cliquez sur **Référentiels**.
3. Cliquez sur l'onglet **Définis par l'utilisateur**.
4. Sous **Autorisations d'accès**, en regard de l'utilisateur ou du groupe d'utilisateurs, cochez ou décochez la case des autorisations que vous souhaitez modifier.
5. Cliquez sur ⊗ en regard d'un utilisateur ou de groupes d'utilisateurs que vous souhaitez supprimer.
6. Cliquez sur **Enregistrer**.

Afficher les droits du référentiel utilisateur

Dans certains scénarios, vous devrez peut-être rechercher un utilisateur particulier pour vérifier quels référentiels sont configurés pour son accès, ainsi que les autorisations spécifiques accordées. Par exemple, lorsqu'un utilisateur est membre d'un groupe Microsoft Active Directory configuré pour les référentiels et qu'il n'est pas répertorié individuellement dans vos configurations de référentiel définies par l'administrateur ou par l'utilisateur et que vous envisagez d'apporter des modifications spécifiques aux autorisations d'accès de l'utilisateur.

1. Dans la console de gestion, cliquez sur **Paramètres > BlackBerry Dynamics > Docs**.
2. Cliquez sur l'onglet **Référentiels**.

3. Cliquez sur l'onglet **Utilisateurs**.
4. Dans le champ **Rechercher**, commencez à saisir le nom du compte Microsoft Active Directory de l'utilisateur. Si l'utilisateur recherché n'apparait pas, élargissez ou réduisez la chaine de recherche.
5. Cliquez sur le nom d'utilisateur. La colonne **Défini par** indique si le référentiel est défini par l'administrateur ou par l'utilisateur.
6. Cliquez sur le nom du référentiel pour afficher les autorisations d'accès de l'utilisateur. Pour modifier les autorisations d'accès, reportez-vous à la section Modifier les autorisations d'accès utilisateur.
7. Si le référentiel est défini par l'administrateur, vous pouvez saisir un chemin de remplacement dans le champ **Remplacer le chemin pour cet utilisateur**.
8. Si le référentiel est défini par l'utilisateur, vous pouvez saisir un nouveau nom de référentiel dans le champ **Nom du référentiel**.

Configuration d'une instance de BEMS sur site dans un environnement BlackBerry UEM Cloud

Vous pouvez configurer BEMS sur site de sorte qu'il communique avec BlackBerry Proxy pour authentifier les jetons GDAuth dans un environnement BlackBerry UEM Cloud. Lorsque vous configurez votre environnement avec BEMS sur site, vous autorisez les utilisateurs iOS et Android à utiliser les services BEMS-Connect, BEMS-Presence et BEMS-Docs, en plus des notifications par e-mail émises par BEMS Cloud et le service BEMS-Docs pour BlackBerry Work.

Si votre environnement exige que les utilisateurs accèdent à des partages de fichiers ou à des référentiels basés sur CMIS, configurez BEMS-Docs dans une instance de BEMS sur site. L'activation de BEMS-Docs dans BlackBerry UEM Cloud et dans une instance de BEMS sur site dans un environnement BlackBerry UEM Cloud n'est pas prise en charge.

Remarque : Vous pouvez configurer BEMS avec un seul environnement BlackBerry UEM ou BlackBerry UEM Cloud sur site à la fois.

Étapes de configuration de BlackBerry UEM Cloud pour assurer la communication avec BEMS sur site

Lorsque vous configurez BlackBerry UEM Cloud pour assurer la communication avec BEMS, vous devez effectuer les actions suivantes :

Remarque : certaines des tâches suivantes ont peut-être déjà été effectuées lorsque vous avez configuré BlackBerry UEM Cloud.

Étape	Action
1	Configurez BlackBerry UEM Cloud dans votre environnement.
2	Dans la console BlackBerry UEM Cloud, installez BlackBerry Connectivity Node ou effectuez sa mise à niveau vers la dernière version. 1. Vérifiez que votre organisation répond aux conditions préalables à l'installation de BlackBerry Connectivity Node 2. Téléchargez les fichiers d'installation et d'activation pour BlackBerry Connectivity Node à partir de la console de gestion 3. Installez, activez et configurez BlackBerry Connectivity Node
3	Si vous utilisez Connect, installez et configurez les services BEMS sur site suivants. Pour obtenir des instructions sur l'installation d'un serveur BEMS sur site, reportez-vous au contenu relatif à l'installation de BEMS et au contenu relatif aux services BEMS suivants : • BEMS-Connect • BEMS-Presence • BEMS-Docs

Étape	Action
4	Dans le tableau de bord BEMS, suivez les instructions de la section Configurer le serveur BlackBerry Dynamics dans BEMS. Vous pouvez également configurer la communication SSL entre BlackBerry Connectivity Node et BEMS sur site sur le port 17433. 1. Exporter le certificat BlackBerry Proxy vers l'ordinateur local 2. Importer le certificat dans le magasin de clés BEMS Windows 3. Importer le certificat dans le magasin de clés Java sur BEMS **Remarque :** si vous ne configurez pas la communication SSL, décochez la case **Enforce SSL Certificate Validation when communicating with BlackBerry Dynamics**.
5	Dans le tableau de bord BEMS, suivez les instructions de la section Configurer une connectivité BEMS avec BlackBerry Dynamics.

6	Dans la console BlackBerry UEM Cloud, attribuez les applications BlackBerry Connect et BlackBerry Presence Service aux utilisateurs.
	• Vous pouvez affecter les applications à l'aide de l'une des méthodes suivantes. Pour obtenir des instructions, consultez le contenu relatif à l'administration de BlackBerry UEM Cloud :
	  • Attribuer une application à un groupe d'utilisateurs
	  • Attribuer un groupe d'applications à un groupe d'utilisateurs
	  • Attribuer une application à un compte d'utilisateur
	  • Attribuer un groupe d'applications à un compte d'utilisateur

7	Dans la console BlackBerry UEM Cloud, créez un profil de connectivité BlackBerry Dynamics et ajoutez le serveur d'applications qui héberge les applications BlackBerry Connect, BlackBerry Presence Service et Feature - Docs Service Entitlement.

Importer le certificat dans le magasin de clés BEMS Windows

Pour que le service Connect fasse confiance au certificat du serveur BlackBerry Proxy, vous devez importer le certificat BlackBerry Proxy dans le magasin de clés Windows du service Connect. Répétez cette tâche sur chaque instance BEMS.

Avant de commencer : enregistrez une copie du certificat ca.cer que vous avez exporté dans un emplacement pratique sur l'ordinateur qui héberge BEMS. Pour obtenir des instructions, reportez-vous à Exporter le certificat BlackBerry Proxy vers l'ordinateur local.

1. Ouvrez la Console de gestion Microsoft.
2. Cliquez sur **Racine console**.
3. Cliquez sur **Fichier > Ajouter/Supprimer un composant logiciel enfichable**.
4. Cliquez sur **Certificats**.
5. Sélectionnez **Compte d'ordinateur > Ordinateur local > OK**.
6. Développez **Certificats (ordinateur local) > Autorités de certification racines de confiance**.
7. Cliquez avec le bouton droit sur **Certificats**, puis cliquez sur **Toutes les tâches > Importer**.
8. Cliquez sur **Suivant**.

9. Accédez à l'emplacement où vous avez enregistré le certificat que vous avez exporté (par exemple <*lecteur*>: \bemscert\ca.cer). Cliquez sur **Ouvrir**.
10. Cliquez sur **Suivant**.
11. Cliquez sur **Terminer**. Cliquez sur **OK**.

À la fin : Configurez le service BEMS Core pour pouvoir communiquer avec BlackBerry Dynamics. Pour obtenir des instructions, reportez-vous à Configurer une connectivité BEMS avec BlackBerry Dynamics.

Importer le certificat dans le magasin de clés Java sur BEMS

Pour que le service Presence et Docs puisse faire confiance au certificat du serveur BlackBerry Proxy, vous devez importer le certificat BlackBerry Connectivity Node. Utilisez DBmanager pour importer le certificat dans le magasin de clés BEMS Java. Par défaut, DBmanager est situé dans le dossier d'installation à l'emplacement `<lecteur>:\GoodEnterpriseMobilityServer<version>\GoodEnterpriseMobilityServer\DBManager`.

Avant de commencer : enregistrez une copie du certificat ca.cer que vous avez exporté dans un emplacement pratique sur l'ordinateur qui héberge BEMS. Pour obtenir des instructions, reportez-vous à Exporter le certificat BlackBerry Proxy vers l'ordinateur local.

1. Sur l'ordinateur qui héberge le serveur BEMS sur site, vérifiez que la variable PATH System inclut le chemin d'accès au répertoire JAVA.
   a) Dans une invite de commande, saisissez `set | findstr "Path"`.
   b) Appuyez sur la touche **Entrée**.

   Pour plus d'informations sur le réglage de la variable PATH System, reportez-vous à la section « Configurer l'environnement d'exécution Java » dans le contenu d'installation d'un environnement BEMS dans BlackBerry UEM.
2. Effectuez une sauvegarde du fichier du magasin de clés Java. Le fichier du magasin de clés Java se trouve à l'emplacement `%JAVA_HOME%\lib\security\cacerts`, où JAVA_HOME est confirmé à l'étape 1.
3. Importez le certificat racine BlackBerry Proxy.
   a) Ouvrez une invite de commande et accédez au dossier DBManager. Par exemple, si les fichiers d'installation sont enregistrés dans votre dossier Téléchargements, saisissez `C:\Users\besadmin\Downloads\GoodEnterpriseMobilityServer<version>\GoodEnterpriseMobilityServer\DBManager`
   b) Importez le certificat. Saisissez `java -jar dbmanager-<version>-jar-with-dependencies.jar -moduleName pushnotify -dbType sqlserver -dbName <nom_BD_SQLServer> -dbHost <Nom de l'ordinateur hébergeant la base de données SQL> -dbPort 1433 -userName gems_sa -password <motdepasse_du_compte_de_service_BEMS> -action addcertificate -pemFile "C:\<chemin_d'accès_au_fichier_pemfile>\<nom de certificat>.cer" -alias gdcert`
4. Redémarrez le service Good Technology Common Services dans le Gestionnaire de services Windows.

À la fin : Configurez le service BEMS Core pour pouvoir communiquer avec BlackBerry Dynamics. Pour obtenir des instructions, reportez-vous à Configurer le serveur BlackBerry Dynamics dans BEMS.

Configurer le serveur BlackBerry Dynamics dans BEMS

Votre environnement BEMS doit être configuré pour faire confiance à l'autorité de certification racine pour la configuration HTTPS BlackBerry Proxy ou pour implémenter la solution de contournement Karaf. Pour obtenir

des instructions, reportez-vous à « Importation et configuration des certificats » dans le contenu de configuration BEMS-Core.

1. Dans **BlackBerry Enterprise Mobility Server Dashboard**, sous **BEMS System Settings**, cliquez sur **BEMS Configuration**.
2. Cliquez sur **BlackBerry Dynamics**.
3. Effectuez l'une des tâches suivantes :

Tâche	Étapes
Si un serveur BlackBerry Proxy n'est pas défini	**a.** Cliquez sur **Ajouter un proxy BlackBerry**. **b.** Dans le champ **Nom d'hôte**, saisissez le nom d'hôte du serveur BlackBerry Proxy. **c.** Dans la liste déroulante **Protocole**, sélectionnez le protocole utilisé pour communiquer avec le serveur BlackBerry Proxy. • Si vous sélectionnez HTTPS, le champ **Port** est pré-renseigné avec la valeur 17433. Cette configuration est sécurisée. • Si vous sélectionnez HTTP, le champ **Port** est pré-renseigné avec la valeur 17080. **Remarque :** Si vous configurez votre environnement pour HTTPS, vous devez Exporter le certificat BlackBerry Proxy vers l'ordinateur local puis Importer le certificat dans le magasin de clés Java sur BEMS. **d.** Cliquez sur **Tester** pour tester la connexion. **e.** Répétez les étapes 1 à 4 pour ajouter des serveurs BlackBerry Proxy supplémentaires et assurer la continuité de la redondance.
Si un ou plusieurs serveurs BlackBerry Proxy sont définis	Aucune action n'est requise. Les serveurs BlackBerry Proxy précédemment définis sont répertoriés.

4. Cochez la case **Apply to other nodes in the BEMS cluster** pour communiquer les informations du serveur BlackBerry Proxy à tous les nœuds BEMS du cluster.
5. Vous pouvez aussi cocher la case **Enforce the SLL Certificate validation when communicating with BlackBerry Dynamics** lorsque vous utilisez le protocole https pour communiquer avec le serveur BlackBerry Proxy.
6. Cliquez sur **Enregistrer**.

Configurer une connectivité BEMS avec BlackBerry Dynamics

1. Dans **BlackBerry Enterprise Mobility Server Dashboard**, sous **BlackBerry Services Configuration**, cliquez sur **Connect**.
2. Cliquez sur **Compte de service**.
3. Saisissez le nom d'utilisateur et le mot de passe du service.
4. Cliquez sur **Enregistrer**.
5. Cliquez sur **BlackBerry Dynamics**.
6. Dans le champ **Nom d'hôte**, saisissez le nom d'hôte du serveur BlackBerry Proxy.
7. Dans le champ **Port**, le numéro de port est pré-renseigné en fonction du type de communication que vous sélectionnez.

- Si vous sélectionnez HTTP, le champ Port est pré-renseigné avec la valeur 17080.
- Si vous sélectionnez HTTPS, le champ Port est pré-renseigné avec la valeur 17433. Cette configuration est sécurisée.

Remarque : Si vous configurez votre environnement pour HTTPS, vous devez Exporter le certificat BlackBerry Proxy vers l'ordinateur local puis Importer le certificat dans le magasin de clés BEMS Windows.

8. Cliquez sur **Test** pour vérifier la connexion au serveur BlackBerry Proxy.
9. Cliquez sur **Enregistrer**.

À la fin : Si vous avez sélectionné le protocole HTTPS, vous devez configurer l'application BlackBerry Connect pour pouvoir utiliser les communications SSL. Pour obtenir des instructions, reportez-vous à « Configuration des paramètres de l'application BlackBerry Connect » pour votre environnement dans le contenu d'administration BlackBerry Connect.

Ajouter un serveur d'applications hébergeant les applications d'attribution de droits d'accès à un profil de connectivité BlackBerry Dynamics

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Réseaux et connexions > Connectivité BlackBerrry Dynamics**.
3. Cliquez sur l'+ pour créer un nouveau profil de connectivité ou cliquez sur le profil de connectivité BlackBerry Dynamics auquel vous souhaitez ajouter un serveur d'applications.
4. Si nécessaire, cliquez sur l'✎.
5. Sous **Serveurs d'applications**, cliquez sur **Ajouter**.
6. Sélectionnez l'application **Feature - Docs Service Entitlement** à laquelle vous souhaitez ajouter un serveur d'applications.
7. Cliquez sur **Enregistrer**.
8. Dans le tableau de l'application, cliquez sur l'+.
9. Dans le champ **Serveur**, spécifiez le nom de domaine complet (FQDN) du serveur BEMS sur site.
10. Dans le champ **Port**, spécifiez le port du cluster BlackBerry Proxy utilisé pour accéder au serveur. Le numéro de port par défaut est 8443.
11. Dans la liste déroulante **Priorité**, indiquez la priorité du ou des serveurs principaux.
12. Dans la liste déroulante **Cluster de proxy BlackBerry principal**, spécifiez le nom du cluster BlackBerry Proxy que vous souhaitez définir comme cluster principal.
13. Dans la liste déroulante **Cluster de proxy BlackBerry secondaire**, spécifiez le nom du cluster BlackBerry Proxy que vous souhaitez définir comme cluster secondaire.
14. Cliquez sur **Enregistrer**.
15. Répétez les étapes 5 à 14 pour les applications suivantes :

    - BlackBerry Connect
    - BlackBerry Presence Service

Exporter le certificat BlackBerry Proxy vers l'ordinateur local

Si vous devez configurer la communication SSL pour permettre la communication entre les services BlackBerry Connectivity Node et BEMS sur site (par exemple, les services Connect, Docs et Mail), exportez les chaînes de certificats racines et intermédiaires de BlackBerry Proxy et importez-les dans le magasin de clés Java sur BEMS et le magasin de clés Windows.

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

Avant de commencer : Assurez-vous que BlackBerry Connectivity Node est installé avec l'état En cours d'exécution.

1. Sur l'ordinateur qui héberge BlackBerry Connectivity Node, exportez le certificat BlackBerry Proxy vers votre ordinateur. Dans un navigateur, saisissez `https://localhost:17433`. Un message d'erreur de certificat s'affiche, car le certificat a été signé par une autorité de certification qui n'est pas reconnue comme une autorité de certification connue.
2. Pour ouvrir la boite de dialogue Certificat, cliquez sur l'icône de certificat dans le champ URL.
3. Cliquez sur **Certificat**.
4. Cliquez sur **Certificate Path**.
5. Cliquez sur le certificat racine. Le certificat racine est le premier élément dans la hiérarchie des certificats.
6. Cliquez sur **Afficher le certificat**.
7. Cliquez sur l'onglet **Détails**.
8. Cliquez sur **Copier dans un fichier**.
9. Cliquez sur **Suivant**.
10. Sélectionnez **Base-64 encoded X.509 (.CER)**.
11. Cliquez sur **Suivant**.
12. Cliquez sur **Parcourir**.
13. Saisissez un nom pour le certificat (par exemple, ca.cer) et exportez-le vers l'ordinateur local.
14. Cliquez sur **Enregistrer**.
15. Cliquez sur **Terminer**.
16. Cliquez sur **OK**.

À la fin :

- Si vous configurez le service Connect, vous devez copier le certificat BlackBerry Proxy exporté sur l'ordinateur qui héberge BEMS, puis suivez les instructions de la section Importer le certificat dans le magasin de clés BEMS Windows.
- Si vous configurez le service Presence et le service Docs, vous devez copier le certificat BlackBerry Proxy exporté sur l'ordinateur qui héberge BEMS, puis suivez les instructions de la section Importer le certificat dans le magasin de clés Java sur BEMS.

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 un serveur BlackBerry UEM source sur site.

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

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

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

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

Condition préalable	Détails
Se connecter	Connectez-vous à BlackBerry UEM en tant qu'administrateur de sécurité. Un seul administrateur doit effectuer des opérations de migration, à la fois.
Vérifier la version du logiciel	Pour migrer des données vers BlackBerry UEM Cloud, l'instance de BlackBerry UEM sur site à partir de laquelle vous migrez les données doit correspondre à BlackBerry UEM version 12.13 ou ultérieure.
BlackBerry Connectivity Node	Pour utiliser toutes les fonctionnalités de migration, activez au moins une instance de BlackBerry Connectivity Node exécutant la version 2.13 ou ultérieure.

Condition préalable	Détails
Configurez la connexion au répertoire d'entreprise BlackBerry UEM	Configurez la connexion au répertoire d'entreprise BlackBerry UEM de destination telle qu'elle est configurée dans l'instance source. Par exemple, si l'instance source est configurée pour l'intégration d'Active Directory et qu'elle est connectée au domaine exemple.com, configurez l'instance BlackBerry UEM de destination pour l'intégration Active Directory et connectez-la au domaine exemple.com. **Important :** La migration ne fonctionnera pas si le répertoire d'entreprise du serveur de destination ne correspond pas au répertoire d'entreprise du serveur source.
BlackBerry UEM Client	BlackBerry UEM Client doit correspondre à BlackBerry Dynamics SDK version 8.0 ou ultérieure. Vous trouverez la version du SDK dans les notes de version de l'application.
Vérifiez l'état des applications BlackBerry Dynamics	Vérifiez la version BlackBerry Dynamics SDK de toutes les applications BlackBerry Dynamics que vous souhaitez migrer. Cela inclut les applications principales, les applications BlackBerry Dynamics, les applications ISV et les applications personnalisées internes. Pour les migrations effectuées à partir d'une base de données BlackBerry UEM source sur site, toutes les applications BlackBerry Dynamics doivent correspondre à la version 8.0 ou ultérieure de BlackBerry Dynamics SDK. Vous trouverez la version du SDK dans les notes de version de l'application. **Les applications BlackBerry Dynamics qui ne sont pas prises en charge pour la migration sont effacées du terminal lorsque l'administrateur commence la migration.**
Vérifiez l'état des autorisations des applications BlackBerry Dynamics	Assurez-vous que : • Le serveur BlackBerry UEM de destination dispose de la même liste d'autorisations d'applications BlackBerry Dynamics que le serveur source. • Tous les comptes utilisateur migrés se voient attribuer la même liste d'autorisations d'applications BlackBerry Dynamics sur le serveur BlackBerry UEM de destination que celle dont ils disposent sur le serveur source. • Le délégué d'authentification est le même sur le serveur source et le serveur de destination. Vous pouvez modifier le délégué d'authentification après la migration. • Le profil BlackBerry Dynamics de l'utilisateur permet à BlackBerry UEM Client d'être activé par BlackBerry Dynamics, si l'instance de BlackBerry UEM Client de l'utilisateur sur le serveur source est également activée par BlackBerry Dynamics. **ATTENTION :** S'il manque des autorisations, les applications BlackBerry Dynamics sont désactivées après la migration.
Vérifiez les ID d'organisation	Les applications personnalisées sont migrées uniquement si les serveurs source et de destination ont le même ID d'organisation. Il est possible de fusionner les deux organisations. Pour en savoir plus, rendez-vous sur le site Web support.blackberry.com/community pour consulter l'article 47626.

Condition préalable	Détails
Vérifiez que les ports requis ne sont pas bloqués par un pare-feu ou utilisés par un autre logiciel	Assurez-vous que le port 8887 (TCP) est ouvert entre le serveur BlackBerry UEM sur site et BlackBerry Connectivity Node. Le serveur sur site écoute les connexions émises par BlackBerry Connectivity Node sur le port 8887. Assurez-vous que le port utilisé par l'instance de Microsoft SQL Server qui héberge la base de données BlackBerry UEM sur site est ouvert et accessible par BlackBerry Connectivity Node (par exemple, le port 1433).

Connexion à un serveur source

Vous devez connecter BlackBerry UEM au serveur source à partir duquel vous souhaitez migrer les données.

Remarque : Si plusieurs instances BlackBerry Connectivity Node sont activées, assurez-vous de configurer toutes les instances de BlackBerry Connectivity Node pour qu'elles se connectent à la même base de données source. Toutes les instances de BlackBerry Connectivity Node doivent être en cours d'exécution.

Remarque : Pour vous connecter à un autre serveur source que celui configuré, supprimez la configuration source existante, puis ajoutez la nouvelle.

1. Sur la console de gestion de BlackBerry Connectivity Node, cliquez sur **Paramètres généraux > Migration** dans la barre de menus.
2. Cliquez sur +.
3. Dans le champ **Nom d'affichage**, saisissez un nom descriptif pour la base de données source.
4. Dans le champ **Serveur de base de données**, saisissez le nom de l'ordinateur qui héberge la base de données source, au format <host>\<instance> pour un port dynamique et au format <host>:<port> pour un port statique.
5. Dans la liste déroulante **Type d'authentification de la base de données**, sélectionnez le type d'authentification à utiliser pour vous connecter à la base de données source.
6. Effectuez l'une des opérations suivantes :

Option	Description
Si vous avez sélectionné l'authentification SQL	a. 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. b. Dans le champ **Nom de la base de données**, saisissez le nom de la base de données source.
Si vous avez sélectionné Windows l'authentification NT	a. Modifiez les propriétés de connexion du service BlackBerry UEM - BlackBerry Cloud Connector avec le même compte que celui utilisé pour installer l'instance source de BlackBerry UEM. Pour plus d'informations sur les comptes de connexion, reportez-vous à l' Microsoft article TechNet relatif aux autorisations de services. **Remarque :** Une fois la migration à partir de cette source terminée, rétablissez le paramètre de propriétés de connexion sur le compte du système local. b. Dans le champ **Nom de la base de données**, saisissez le nom de la base de données source.

7. Cliquez sur **Enregistrer**.

8. Dans la console de gestion de BlackBerry UEM, cliquez sur **Paramètres > Migration > Configuration** dans la barre de menus.
9. Cliquez sur +.
10. Saisissez un nom descriptif pour la base de données source.
11. Pour tester la connexion entre la source et la destination, cliquez sur **Test de connexion**.
12. 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.

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

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

- Stratégies informatiques sélectionnées
- Profils de messagerie
- Profils Wi-Fi
- Profils VPN
- Profils proxy
- Profils de connectivité BlackBerry Dynamics
- Profils BlackBerry Dynamics
- Paramètres de configuration d'application
- Profils de certificat d'autorité de certification
- Profils des certificats partagés
- Récupération de certificat
- Profils d'informations d'identification de l'utilisateur
- Profils SCEP
- Profils CRL
- Profils OSCP
- Paramètres d'autorité de certification (Entrust et connecteur PKI uniquement)
- Certificats client (utilisation des applications)
- Toutes les politiques et tous les profils associés aux politiques et aux profils sélectionnés

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

BlackBerry UEM

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

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

Applications activées avec BlackBerry Dynamics

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

Élément	Considérations
Profils de connectivité	Lorsque les profils de connectivité BlackBerry Dynamics sont migrés, les valeurs de l'onglet Serveurs d'applications ne sont pas migrées. Les valeurs sont renseignées à l'aide des valeurs par défaut du serveur BlackBerry UEM de destination. Lorsque les profils de connectivité BlackBerry Dynamics sont migrés, certaines valeurs de l'onglet Infrastructure ne sont pas migrées. L'administrateur doit modifier manuellement chaque profil migré et définir les valeurs du cluster BlackBerry Proxy principal et du cluster BlackBerry Proxy secondaire.
Applications	Si une autorisation d'application du serveur source n'existe pas dans le serveur de destination, cette attribution d'application n'est pas migrée. Le groupe d'applications est migré.
Utilisation des certificats	L'utilisation des certificats est migrée, à l'exception des : • Utilisations des certificats qui existent déjà dans le serveur de destination • Applications non-BlackBerry Dynamics

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

Après la migration des utilisateurs, terminaux, groupes et d'autres données vers BlackBerry UEM, vous devez effectuer les tâches suivantes sur l'instance de BlackBerry UEM de destination.

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

- Attribuez des configurations d'application aux applications BlackBerry Dynamics dans les groupes.
- Attribuez des profils de connectivité aux groupes.
- Attribuez des stratégies BlackBerry Dynamics migrées aux utilisateurs.
- Définissez des profils de remplacement (profils BlackBerry Dynamics et profils de conformité).

Renseignez les profils de connectivité migrés :

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

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

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

1. Sur la barre de menus, cliquez sur **Paramètres**.
2. Cliquez sur **Migration** > **Stratégies informatiques, profils, groupes**.
3. Cliquez sur **Suivant**.
4. Cochez les cases pour indiquer les éléments à migrer.

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

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

Considérations : Migration des utilisateurs depuis un serveur source

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

Élément	Considérations
Limite de migration	Vous pouvez simultanément migrer un maximum de 1000 utilisateurs à partir d'une source. Si vous sélectionnez un nombre d'utilisateurs supérieur au maximum autorisé, seul le nombre maximum sera migré vers le BlackBerry UEM de destination. Les autres utilisateurs seront ignorés. Répétez le processus de migration autant de fois que nécessaire pour migrer tous les utilisateurs à partir du serveur source. **Remarque :** Si BlackBerry UEM expire lors de la migration de 1 000 utilisateurs, essayez de migrer un plus petit nombre d'utilisateurs.
Adresse électronique	• Seuls les utilisateurs associés à une adresse e-mail peuvent être migrés. • Vous ne pouvez pas migrer un utilisateur qui utilise déjà la même adresse e-mail dans l'instance de BlackBerry UEM de destination. Ces utilisateurs n'apparaissent pas dans la liste des utilisateurs à migrer. • Si deux utilisateurs de la base de données source ont la même adresse électronique, un seul utilisateur apparait sur l'écran Migrer les utilisateurs.
Mot de passe	Après la migration, les utilisateurs locaux doivent modifier leur mot de passe lorsqu'ils se connectent à BlackBerry UEM Self-Service pour la première fois. Les utilisateurs qui n'étaient pas autorisés à accéder à BlackBerry UEM Self-Service avant la migration ne disposent pas automatiquement d'une autorisation après la migration.
Groupes	• Vous pouvez filtrer les utilisateurs sans attribution de groupe pour inclure cet ensemble d'utilisateurs dans une migration. • Vous ne pouvez pas migrer un utilisateur qui est propriétaire d'un groupe de terminaux partagés. L'utilisateur n'apparait pas dans la liste des utilisateurs à migrer.

Migrer des utilisateurs depuis un serveur source

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

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

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

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

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

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

5. Cliquez sur **Suivant**.
6. Attribuez un ou plusieurs groupes, ou une stratégie informatique et un ou plusieurs profils, aux utilisateurs sélectionnés.

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

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

Considérations : Migration des terminaux depuis un serveur source

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

Élément	Considérations
Limite de migration	Vous pouvez simultanément migrer un maximum de 2 000 terminaux à partir d'un serveur source.
Destination BlackBerry UEM	Avant de migrer les terminaux, vérifiez que BlackBerry UEM prend en charge le type de terminal et le système d'exploitation correspondants.
Utilisateurs	• Les utilisateurs doivent exister dans le domaine BlackBerry UEM de destination. • Vous devez migrer tous les terminaux d'un utilisateur en même temps.
Terminaux iOS gérés	• La dernière version de BlackBerry UEM Client doit être installée sur les terminaux iOS. • Les terminaux iOS auxquels est attribué un profil de verrouillage des applications ne peuvent pas être migrés, car BlackBerry UEM Client ne peut pas être ouvert à la migration. • Dans les paramètres d'application de toutes les applications, décochez la case **Supprimer l'application du terminal lorsque celui-ci est supprimé de BlackBerry UEM**. **Remarque :** Si vous tentez d'effectuer la migration sans effectuer cette étape, l'application est supprimée et le terminal peut être désinscrit de BlackBerry UEM. Cependant, même si vous décochez cette case, l'application peut toujours être supprimée pendant la migration.
Terminaux Android gérés	• La dernière version de BlackBerry UEM Client doit être installée sur les terminaux Android Enterprise. • Vous ne pouvez pas migrer des terminaux Android qui utilisent un profil professionnel à l'aide d'un compte Google ou d'un domaine Google.
Terminaux Windows	Vous ne pouvez pas migrer des terminaux Windows.
Terminaux macOS	Vous ne pouvez pas migrer des terminaux macOS.

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

Élément	Considérations
Terminaux compatibles avec BlackBerry Dynamics	**Applications BlackBerry Dynamics** • Toutes les applications BlackBerry Dynamics compatibles avec la migration sont migrées. **Les applications BlackBerry Dynamics qui sont incompatibles avec la migration sont effacées lorsque l'administrateur lance la migration.** Ces applications doivent être réactivées sur le BlackBerry UEM de destination. • Pour les migrations effectuées à partir d'une base de données BlackBerry UEM source sur site, toutes les applications BlackBerry Dynamics doivent correspondre à la version 8.0 ou ultérieure de BlackBerry Dynamics SDK. • Dans l'écran Migrer les terminaux, la colonne des conteneurs incompatibles affiche, pour chaque terminal, le nombre d'applications BlackBerry Dynamics qui ne peuvent pas être migrées et le nombre total d'applications BlackBerry Dynamics. Cliquez sur le nombre pour afficher les applications BlackBerry Dynamics qui sont incompatibles avec la migration. • Assurez-vous que l'utilisateur dispose des autorisations requises pour l'application sur le BlackBerry UEM de destination. Si l'utilisateur ne dispose pas des autorisations requises, après la migration, il recevra un message indiquant que l'application est bloquée. • Les applications BlackBerry Dynamics ne sont pas migrées si le BlackBerry UEM de destination a déjà enregistré des applications pour cet utilisateur. • La migration de BlackBerry Access for Windows, BlackBerry Access for macOS et BlackBerry Enterprise BRIDGE n'est pas prise en charge. Une fois la migration terminée, les utilisateurs doivent réinscrire ces applications dans UEM. • Les applications personnalisées sont migrées uniquement si les serveurs source et de destination ont le même ID d'organisation. Il est possible de fusionner les deux organisations. Pour en savoir plus, rendez-vous sur le site Web support.blackberry.com/community pour consulter l'article 47626. • Les terminaux avec des applications BlackBerry Dynamics activées par plusieurs utilisateurs ne doivent pas être migrés. • Il est possible que les applications BlackBerry Dynamics qui sont verrouillées pour des raisons de conformité ou à distance par l'administrateur avant le processus de migration, ne fonctionnent plus après la migration et doivent être réactivées. Si BlackBerry UEM Client est verrouillé, l'utilisateur ne peut pas être migré. • Le processus de migration ne permet pas de suivre ou de garantir la migration de BlackBerry UEM Client et des applications activées sur un terminal après la mise en cache des données de ce terminal. Les administrateurs doivent actualiser le cache utilisateur avant chaque migration. **Authentification des terminaux** • Le délégué d'authentification doit être le même sur le serveur source et le BlackBerry UEM de destination. Vous pouvez modifier le délégué d'authentification après la migration.

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

Migrer des terminaux depuis un serveur source

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

Avant de commencer :

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

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

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

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

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

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

   Si des modifications sont apportées à la source après la mise à jour du cache, ces modifications ne sont pas prises en compte dans l'affichage des données du cache. Il est déconseillé d'apporter des modifications au serveur source lors de la migration, mais si vous le faites, actualisez le cache régulièrement.
5. Cliquez sur **Aperçu**.
6. Cliquez sur **Migrer**.
7. Pour afficher l'état des terminaux en cours de migration, cliquez sur **Migration** > **État**.

Référence rapide pour la migration des terminaux

Type de terminal	Type d'activation/configuration	Migration
Android	• Contrôles MDM • BlackBerry 2FA • Confidentialité de l'utilisateur • BlackBerry Dynamics (UEM à UEM)	Pris en charge
Terminaux Android Enterprisedotés d'un profil professionnel associé à un domaine Google	Indifférent	Non pris en charge

Type de terminal	Type d'activation/configuration	Migration
Terminaux Android Enterprise dotés d'un profil professionnel qui n'est pas associé à un compte Google ou un domaine Google	Indifférent	Pris en charge
Terminaux Android Samsung Knox Workspace dotés d'un profil professionnel associé à un compte Google ou un domaine Google	Indifférent	Non pris en charge
Terminaux Android Samsung Knox Workspace dotés d'un profil professionnel qui n'est pas associé à un compte Google ou un domaine Google	Indifférent	Pris en charge
iOS	• Contrôles MDM • Inscription du terminal pour BlackBerry 2FA uniquement • Terminaux DEP sur lesquels BlackBerry UEM Client est installé • Confidentialité de l'utilisateur • BlackBerry Dynamics (UEM à UEM)	Pris en charge
iOS	• Terminaux DEP sur lesquels BlackBerry UEM Client n'est pas installé • Inscription de l'utilisateur	Non pris en charge
Windows	Indifférent	Non pris en charge
macOS	Indifférent	Non pris en charge

Migration 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 source vers une autre base de données BlackBerry UEM.

Migrer des terminaux DEP sur lesquels BlackBerry UEM Client est installé

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

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

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

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

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

À la fin :

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

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

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

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

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

Informations juridiques

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

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

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

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

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

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

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

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

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

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

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

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

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

Maidenhead, Berkshire SL6 1RL
Royaume-Uni

Publié au Canada