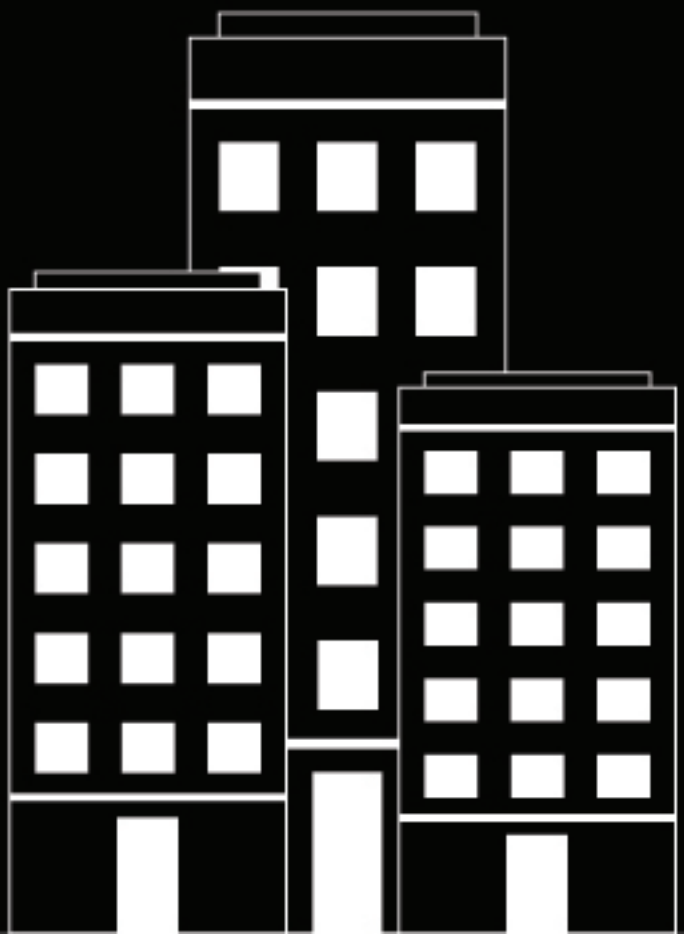

# BlackBerry UEM

## Guide de configuration

12.20

# Contents

# Configuration de BlackBerry UEM

Le tableau suivant récapitule les tâches de configuration initiales décrites dans ce guide. Passez ces tâches en revue pour déterminer lesquelles vous devez effectuer en fonction des besoins de votre organisation. Une fois les tâches appropriées terminées, vous êtes prêt à configurer les administrateurs, à créer et gérer des utilisateurs et des groupes, à configurer les contrôles des terminaux et à activer les terminaux.

Pour effectuer les tâches de configuration décrites dans ce guide, utilisez le compte d'administrateur que vous avez créé lors de l'installation de UEM. Si vous créez des comptes d'administrateur supplémentaires à configurer UEM, vous devez attribuer le rôle d'administrateur de sécurité aux comptes pour vous assurer que le niveau d'autorisation approprié est accordé.

| Tâche | Sur site | Cloud | Description |
|---|---|---|---|
| Modifier les certificats par défaut utilisés par UEM pour l'authentification | √ | | Vous pouvez remplacer les certificats autosignés par défaut utilisés par UEM pour authentifier la communication entre les composants et avec les terminaux. |
| Installation de BlackBerry Connectivity Node | | √ | Vous pouvez installer et configurer BlackBerry Connectivity Node dans un environnement UEM Cloud de manière à permettre l'accès au répertoire d'entreprise de votre organisation et d'activer les fonctions de connectivité sécurisée. |
| Configurer UEM pour envoyer les données via un serveur proxy | √ | √ | Vous pouvez configurer UEM pour envoyer les données via un serveur proxy avant d'atteindre BlackBerry Infrastructure. Dans les environnements UEM Cloud, vous pouvez installer un BlackBerry Router autonome de sorte qu'il fonctionne comme serveur proxy. |
| Configurer des connexions via des serveurs proxy internes | √ | | Si votre organisation utilise un serveur proxy pour établir la connexion entre les serveurs de votre réseau, vous devrez peut-être configurer les paramètres proxy côté serveur pour permettre aux composants UEM de communiquer avec les instances à distance de la console de gestion. |
| Se connecter à un serveur SMTP pour envoyer des notifications par e-mail | √ | | Si vous souhaitez que UEM envoie des e-mails d'activation et d'autres notifications aux utilisateurs, vous devez spécifier les paramètres de serveur SMTP que UEM peut utiliser. |
| Connecter UEM à des répertoires d'entreprise | √ | √ | Connectez UEM aux répertoires de votre entreprise pour créer des comptes d'utilisateur, activer des groupes liés au répertoire et configurer l'intégration des utilisateurs et la synchronisation du répertoire. |

| Tâche | Sur site | Cloud | Description |
|---|---|---|---|
| Connecter BlackBerry UEM à Entra ID pour créer des comptes d'utilisateur de répertoire | √ | √ | Connectez UEM à Entra pour créer des comptes d'utilisateur de répertoire dans UEM. |
| Configurer UEM pour gérer les profils de protection des applications Intune | √ | √ | Utilisez UEM pour créer, gérer et attribuer des profils de protection des applications Microsoft Intune afin de protéger les données des applications Office 365. |
| Configurer UEM en tant que partenaire de conformité Intune | √ | √ | Configurez UEM pour prendre en charge l'accès conditionnel à Entra ID. |
| Enregistrer un certificat APNs pour gérer les terminaux iOS et macOS | √ | √ | Obtenez et enregistrez un certificat APNs si vous souhaitez gérer des données et en envoyer aux terminaux iOS macOS. |
| Configurer UEM pour le programme d'inscription des appareils | √ | √ | Vous pouvez utiliser la console de gestion de UEM afin de gérer les terminaux iOS que votre organisation a achetés auprès de Apple pour DEP. |
| Configurer UEM pour prendre en charge des terminaux Android Enterprise | √ | √ | Pour prendre en charge des terminaux Android Enterprise, vous devez configurer votre domaine Google Workspace ou Google Cloud pour la prise en charge de fournisseurs de gestion de terminaux mobiles tiers et configurer UEM pour communiquer avec votre domaine Google Workspace ou Google Cloud. |
| Configurer UEM pour prendre en charge des terminaux Android Management | √ | √ | Pour prendre en charge des terminaux Android Management, configurez Android Management dans la console Google Cloud puis ajoutez une connexion Android Management dans UEM. |
| Configurer UEM pour gérer des terminaux Chrome OS | √ | √ | Vous pouvez configurer UEM pour prendre en charge certaines fonctionnalités de gestion Chrome OS. |
| Simplifier les activations Windows 10 | √ | √ | Vous pouvez simplifier le processus d'activation des terminaux Windows 10 de sorte que les utilisateurs n'aient pas besoin de spécifier une adresse de serveur. |
| Migration d'utilisateurs, de terminaux, de groupes et d'autres données depuis un serveur source | √ | √ | Vous pouvez migrer des utilisateurs, des terminaux, des groupes et d'autres données à partir de serveurs BlackBerry pris en charge. |

| Tâche | Sur site | Cloud | Description |
|---|---|---|---|
| Configurer la communication réseau et les propriétés des applications BlackBerry Dynamics | √ | √ | Vous pouvez configurer les communications réseau et d'autres propriétés des applications BlackBerry Dynamics. |
| Chiffrer la connexion entre BlackBerry UEM et Microsoft SQL Server | √ | | Vous pouvez chiffrer la connexion entre UEM et Microsoft SQL Server. |
| Intégrer UEM avec Cisco ISE | √ | | Vous pouvez créer une connexion à Cisco ISE de sorte qu'il récupérer des données de terminaux de UEM et appliquer des stratégies de contrôle d'accès au réseau. |
| Configurer un VPN à l'aide de Knox StrongSwan pour les environnements de site sombre UEM | √ | | Dans un environnement de site sombre UEM, vous devez configurer l'accès VPN afin que les terminaux Samsung Knox puissent accéder à vos serveurs et ressources internes. |

# Modification des certificats utilisés par BlackBerry UEM pour l'authentification

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

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

Vous pouvez modifier les certificats suivants :

| Certificat | Description |
|---|---|
| Certificat de signature de profil Apple | Il s'agit du certificat que UEM utilise pour signer le profil MDM que les utilisateurs doivent accepter lorsqu'ils activent des terminaux iOS.<br>Si vous utilisez un certificat signé par une autorité de certification, vérifiez que le certificat racine de l'autorité de certification est installé sur les terminaux iOS des utilisateurs avant l'activation. |
| Certificat SSL pour consoles | Il s'agit du certificat SSL que la console de gestion et UEM Self-Service utilisent pour l'authentification des navigateurs.<br>Si vous configurez la haute disponibilité, le certificat doit avoir le nom du domaine UEM. Vous trouverez le nom du domaine dans la console de gestion, sous Paramètres > Infrastructure > Instances. |
| Certificats SSL du BlackBerry Web Services | Il s'agit du certificat SSL que BlackBerry Web Services utilise pour l'authentification des applications utilisant les API BlackBerry Web Services pour gérer UEM.<br>Si vous configurez la haute disponibilité, le certificat doit avoir le nom du domaine UEM. Vous trouverez le nom du domaine dans la console de gestion, sous Paramètres > Infrastructure > Instances. |
| Certificat SSL des applications BlackBerry Dynamics | Il s'agit du certificat SSL utilisé par BlackBerry Dynamics Launcher pour établir un canal de communication sécurisé avec UEM. Les applications BlackBerry Dynamics qui incluent le système intégré BlackBerry Dynamics Launcher peuvent présenter le certificat à UEM pour l'authentification auprès du serveur. |
| Certificat destiné à la gestion des applications | Il s'agit du certificat SSL utilisé pour l'authentification entre UEM et les applications BlackBerry Dynamics.<br>Le certificat d'autorité de certification racine est stocké dans la liste des certificats d'autorité de certification de confiance sur le terminal. Lorsque le serveur s'authentifie auprès du terminal, il présente ce certificat au terminal pour validation. Si vous modifiez ce certificat et que la modification prend effet avant que UEM ne pousse le certificat vers toutes les applications BlackBerry Dynamics, toute application qui n'aura pas reçu le certificat devra être réactivée. |

| Certificat | Description |
|---|---|
| Certificat de Direct Connect | Il s'agit du certificat SSL utilisé pour l'authentification entre un serveur BlackBerry Proxy configuré pour les applications BlackBerry Dynamics Direct Connect et BlackBerry Dynamics sur des terminaux.<br><br>Lorsque vous mettez à jour ce certificat, la nouvelle version est toujours envoyée aux terminaux via une connexion non BlackBerry Dynamics Direct Connect. Tous les terminaux ou conteneurs qui ne sont pas en ligne au moment de la modification recevront la mise à jour lorsqu'ils seront de nouveau en ligne. La mise à jour de ce certificat doit être effectuée simultanément sur le serveur UEM et sur toutes les appliances réseau applicables.<br><br>Pour plus d'informations sur la configuration de Direct Connect, reportez-vous à la section Configuration de Direct Connect avec BlackBerry UEM. |
| Certificat des serveurs BlackBerry Dynamics | Il s'agit du certificat SSL qui permet d'authentifier les connexions entre UEM et BlackBerry Proxy. |

# Considérations pour la modification des certificats BlackBerry Dynamics

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

| Considération | Détails |
|---|---|
| Ajouter de nouveaux certificats à un équipement périphérique | Si vous avez ajouté des certificats BlackBerry Dynamics à un équipement périphérique sur votre réseau, ajoutez le nouveau certificat à l'équipement périphérique avant de l'ajouter à UEM |
| Utiliser les versions les plus récentes des applications BlackBerry Dynamics | Si vous remplacez le certificat BlackBerry Dynamics destiné à la gestion des applications ou Direct Connect, assurez-vous que les utilisateurs utilisent la dernière version des applications BlackBerry Dynamics avant de remplacer le certificat. |
| Les applications BlackBerry Dynamics doivent être ouvertes pour recevoir un certificat | Un utilisateur doit ouvrir une application BlackBerry Dynamics sur son terminal pour recevoir un certificat de UEM. Si vous remplacez le certificat BlackBerry Dynamics destiné à la gestion des applications ou Direct Connect et que la modification prend effet avant que UEM ne pousse le certificat vers toutes les applications BlackBerry Dynamics, toute application qui n'aura pas reçu le certificat devra être réactivée. Les applications ne reçoivent pas de certificats lorsqu'elles sont suspendues sur les terminaux iOS ou lorsque les terminaux Android sont en mode Doze. |

| Considération | Détails |
| --- | --- |
| Vérifier que le BlackBerry Connectivity Node est accessible | Si toutes les instances de BlackBerry Proxy sont inaccessibles par UEM lorsque les certificats BlackBerry Dynamics sont remplacés, les applications BlackBerry Dynamics ne seront pas en mesure de se connecter à ces instances une fois le certificat remplacé. |
| Programmer des modifications de certificat | Si vous remplacez le certificat des serveurs BlackBerry Dynamics, choisissez une période de faible activité pour redémarrer les serveurs.<br>Laissez suffisamment de temps aux nouveaux certificats pour qu'ils se propagent aux applications BlackBerry ProxyBlackBerry Dynamics. Si vous remplacez uniquement le certificat pour les serveurs BlackBerry Dynamics, patientez au moins 10 minutes avant que le serveur redémarre. |

# Modification d'un certificat BlackBerry UEM

**Avant de commencer :**

- Examinez Considérations pour la modification des certificats BlackBerry Dynamics.
- Obtenez un certificat signé par une autorité de certification approuvée. Le format du certificat doit être compatible avec la base de stockage de clés (.pfx, .pkcs12) et crypté selon le type de cryptage TripleDES-SHA1.

1. Dans la barre de menus de la console de gestion, cliquez sur **Paramètres > Infrastructure > Certificats de serveur**.
2. Dans la section relative au certificat que vous souhaitez remplacer de l'onglet **Certificats de serveur** ou **Certificats BlackBerry Dynamics**, cliquez sur **Afficher les détails**.
3. Cliquez sur **Remplacer le certificat**.
4. Cliquez sur **Parcourir**. Accédez au fichier de certificat et sélectionnez-le.
5. Dans le champ **Mot de passe de cryptage** ou **Mot de passe**, saisissez un mot de passe.
6. Cliquez sur **Remplacer**.

**À la fin :**

- Si vous avez remplacé l'un des certificats dans l'onglet Certificats de serveur, redémarrez le service UEM Core sur tous les serveurs.
- Pour les certificats dans l'onglet Certificats BlackBerry Dynamics, vous pouvez cliquer sur **Rétablir les valeurs par défaut** afin de revenir à l'utilisation d'un certificat autosigné.
- Dans l'onglet Certificats BlackBerry Dynamics, vous pouvez décocher les cases **Approuver l'autorité de certification BlackBerry UEM** et **Approuver l'autorité de certification BlackBerry Dynamics** si vous n'avez pas besoin d'approuver les certificats autosignés. Vous ne pouvez décocher la case **Approuver l'autorité de certification BlackBerry Dynamics** que si vous avez remplacé tous les certificats dans l'onglet Certificats BlackBerry Dynamics.
- Si les applications BlackBerry Dynamics cessent de communiquer une fois que vous avez modifié les certificats, vérifiez qu'elles sont à jour puis demandez aux utilisateurs de les réactiver.

# 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 UEM Cloud à accéder au répertoire d'entreprise sur site de votre organisation. Vous pouvez créer des comptes d'utilisateur de répertoire dans UEM en recherchant et en important des données utilisateur depuis le répertoire de l'entreprise. Les données utilisateur sont synchronisées avec le répertoire en fonction de la planification configurée.<br>UEM Cloud doit être en mesure d'accéder à votre répertoire d'entreprise si vous souhaitez utiliser SCEP.<br>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.<br>BlackBerry Cloud Connector permet également à un connecteur PKI d'envoyer des certificats aux applications BlackBerry Dynamics. |
| BlackBerry Proxy | BlackBerry Proxy maintient une connexion entre votre organisation et BlackBerry Dynamics NOC, qui permet aux applications BlackBerry Dynamics de communiquer en toute sécurité avec les ressources situées derrière le pare-feu de votre organisation. 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 la communication réseau et des propriétés des 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 à la section #Utilisation de BlackBerry Secure Connect Plus pour des connexions sécurisées aux ressources professionnelles. |
| 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 à la section Protection des données de messagerie électronique envoyées aux terminaux iOS à l'aide de BlackBerry Secure Gateway. |

| Composant | Objectif |
| --- | --- |
| BlackBerry Gatekeeping Service | BlackBerry Gatekeeping Service facilite le contrôle des terminaux ouvant accéder à Exchange ActiveSync. Pour plus d'informations, reportez-vous à la section Désignation des terminaux autorisés à accéder à Exchange ActiveSync. |

Les fichiers d'installation et d'activation de BlackBerry Connectivity Node sont disponibles dans la console de gestion de UEM. Vous pouvez utiliser ces fichiers pour installer de nouvelles instances de BlackBerry Connectivity Node et mettre à niveau les instances existantes.

# Étapes à suivre pour installer et activer BlackBerry Connectivity Node

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

| Étape | Action |
| --- | --- |
| 1 | Passez en revue la configuration requise et les considérations relatives à l'installation de BlackBerry Connectivity Node. |
| 2 | Installer et configurer BlackBerry Connectivity Node. |
| 3 | Vous pouvez également Créer un groupe de serveurs pour gérer les connexions régionales. |
| 4 | Effectuez une configuration supplémentaire pour BlackBerry Secure Connect Plus, BlackBerry Secure Gateway, BlackBerry Gatekeeping Service et les applications BlackBerry Dynamics. |

# Configuration requise : BlackBerry Connectivity Node

| Élément | Configuration requise ou considérations |
| --- | --- |
| Matériel | BlackBerry Connectivity Node doit être installé sur un ordinateur réservé à des fins techniques, et non 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.<br><br>Vous pouvez installer une ou plusieurs instances de BlackBerry Connectivity Node pour assurer la redondance. Vous devez installer chaque instance sur un ordinateur dédié.<br><br>Un ordinateur qui héberge BlackBerry Connectivity Node doit présenter la configuration requise suivante :<br><br>• 6 cœurs de processeur, E5-2670 (2,6 GHz), E5-2683 v4 (2,1 GHz) ou équivalent<br>• 12 Go de mémoire disponible<br>• 64 Go d'espace disque |
| Mode de performances de service unique | 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 peut libérer des ressources afin de prendre en charge moins de serveurs pour le même nombre d'utilisateurs ou de conteneurs. Chaque instance de BlackBerry Connectivity Node activée pour le mode de performances de service unique peut prendre en charge jusqu'à 10 000 terminaux.<br><br>Si vous activez le mode Performances de service unique pour une instance de BlackBerry Connectivity Node, notez les réglages suivants de la configuration matérielle requise indiquée ci-dessus :<br><br>• BlackBerry Secure Connect Plus uniquement : 4 cœurs de processeur, E5-2670 (2,6 GHz), E5-2683 v4 (2,1 GHz) ou équivalent<br>• BlackBerry Secure Gateway uniquement : 8 cœurs de processeur, E5-2670 (2,6 GHz), E5-2683 v4 (2,1 GHz) ou équivalent<br>• BlackBerry Proxy uniquement : aucune différence |
| Évolutivité et haute disponibilité | Chaque BlackBerry Connectivity Node peut prendre en charge jusqu'à 5 000 terminaux. Vous pouvez installer des instances supplémentaires pour prendre en charge jusqu'à 50 000 terminaux supplémentaires.<br><br>Vous pouvez déployer plusieurs BlackBerry Connectivity Node dans un groupe de serveurs pour permettre une haute disponibilité et un équilibrage de la charge. |

| Élément | Configuration requise ou considérations |
|---|---|
| Logiciel | Un ordinateur qui héberge une instance de BlackBerry Connectivity Node doit présenter la configuration requise suivante :<br>• Un système d'exploitation pris en charge<br>• Windows PowerShell 2.0 ou version ultérieure ; il s'agit d'une condition requise par l'application d'installation afin d'installer RRAS pour BlackBerry Secure Connect Plus et BlackBerry Gatekeeping Service.<br>• Installez la version requise de JRE et définissez la variable BB_JAVA_HOME. Pour plus d'informations, reportez-vous à la section Définir une variable d'environnement pour l'emplacement Java. |
| Connexions au répertoire | Vérifiez que vous utilisez un service de répertoire pris en charge.<br>Vous pouvez configurer une ou plusieurs connexions de répertoire, mais si vous avez plusieurs instances de BlackBerry Connectivity Node, toutes les connexions au répertoire doivent être configurées de la même manière. Si une connexion au répertoire est manquante ou incorrectement configurée, ce BlackBerry Connectivity Node apparait comme désactivé dans la console de gestion. |
| Ports | 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 :<br>• 443 (HTTPS) pour activer BlackBerry Connectivity Node<br>• 3101 (TCP) pour toute autre connexion sortante |
| Comptes d'administrateur | Lorsque vous installez et configurez le BlackBerry Connectivity Node, utilisez des comptes d'administrateur qui répondent aux exigences suivantes :<br>• Utilisez un compte Windows disposant des autorisations nécessaires pour installer et configurer le logiciel sur l'ordinateur.<br>• Choisissez un compte de répertoire disposant d'autorisations de lecture pour chaque connexion au répertoire que vous souhaitez configurer.<br>• Utilisez un compte d'administrateur UEM Cloud disposant des autorisations de télécharger les fichiers d'installation et de configuration de BlackBerry Connectivity Node (par exemple, administrateur de sécurité). |

# Installer et configurer BlackBerry Connectivity Node

**Avant de commencer :**

- Passez en revue la configuration requise et les considérations relatives à l'installation de BlackBerry Connectivity Node.
- Dans la console de gestion, sur la barre de menus, cliquez sur **Paramètres > Intégration externe > Configuration de BlackBerry Connectivity Node**. Cliquez sur et téléchargez l'application d'installation de BlackBerry Connectivity Node. Pour ajouter l'instance de BlackBerry Connectivity Node à un groupe de serveurs existant lorsque vous l'activez, cliquez sur le groupe de serveurs qui convient dans la liste déroulante **Groupe de serveurs**. Générez et enregistrez le fichier d'activation. Le fichier d'activation est valide 60 minutes.
- Transférez l'application d'installation et le fichier d'activation vers l'ordinateur devant héberger l'instance de BlackBerry Connectivity Node. Suivez les étapes ci-dessous sur cet ordinateur.

1. Exécutez l'application d'installation de BlackBerry Connectivity Node.
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 à bbsecure.com via le port 443. 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 à .bbsecure.com via le port 3101. 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.
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 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 le nom de la connexion au répertoire. Si vous avez configuré un répertoire Microsoft Entra ID, ce nom de connexion doit être différent du nom de la connexion au répertoire Entra.<br>**b.** Dans le champ **Nom d'utilisateur**, saisissez le nom d'utilisateur du compte Microsoft Active Directory.<br>**c.** Dans le champ **Domaine**, saisissez le FQDN du domaine qui héberge Microsoft Active Directory. Par exemple : domain.example.com.<br>**d.** Dans le champ **Mot de passe**, saisissez le mot de passe du compte Microsoft Active Directory.<br>**e.** Dans la liste déroulante **Détection du contrôleur de domaine**, cliquez sur l'une des opérations suivantes :<br>• Si vous souhaitez utiliser la détection automatique, cliquez sur **Automatique**.<br>• 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.<br>**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.<br>**g.** Dans la liste déroulante **Détection du catalogue global**, cliquez sur l'une des opérations suivantes :<br>• Si vous souhaitez utiliser la détection automatique de catalogue, cliquez sur **Automatique**.<br>• 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.<br>**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**.<br>Pour configurer le compte Microsoft Active Directory de chacune des forêts auxquelles vous souhaitez que 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.<br>**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.<br>**j.** Cliquez sur **Enregistrer**. |

| Type d'annuaire | Étapes |
| --- | --- |
| Annuaire LDAP | **a.** Dans le champ **Nom de connexion**, saisissez le nom de la connexion au répertoire. Si vous avez configuré un répertoire Microsoft Entra ID, ce nom de connexion doit être différent du nom de la connexion au répertoire Entra.<br>**b.** Dans la liste déroulante **Détection du serveur LDAP**, cliquez sur l'une des opérations suivantes :<br>• Si vous souhaitez utiliser la détection automatique, cliquez sur **Automatique**. Dans le champ **Nom du domaine DNS**, saisissez le nom du domaine DNS.<br>• 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.<br>**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.<br>**d.** Dans le champ du port **LDAP**, saisissez le numéro de port de l'ordinateur LDAP.<br>**e.** Dans la liste déroulante **Autorisation requise**, sélectionnez si UEM Cloud doivent 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).<br>**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).<br>**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)).<br>**h.** Dans la liste déroulante **Étendue de recherche de l'utilisateur LDAP**, cliquez sur l'une des opérations suivantes :<br>• 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**.<br>• Si vous souhaitez limiter les recherches de l'utilisateur à un niveau en dessous du DN de base, cliquez sur **Un niveau**.<br>**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.<br>**j.** Dans le champ **Prénom**, saisissez l'attribut du prénom de chaque utilisateur (par exemple, givenName).<br>**k.** Dans le champ **Nom**, saisissez l'attribut du nom de chaque utilisateur (par exemple, sn).<br>**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.<br>**m.** Dans le champ **Adresse électronique**, saisissez l'attribut de messagerie de chaque utilisateur (par exemple, mail).<br>**n.** Dans le champ **Nom d'affichage**, saisissez l'attribut du nom d'affichage de chaque utilisateur (par exemple, displayName).<br>**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.<br>**p.** Pour activer les groupes liés par répertoire, sélectionnez la case **Activer les groupes liés par répertoire**. Pour plus d'informations sur les groupes liés par répertoire, reportez-vous à la section Activer les groupes liés par annuaire.<br>**q.** Cliquez sur **Enregistrer**. |

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 des instances supplémentaires de BlackBerry Connectivity Node, téléchargez à nouveau les fichiers d'installation et d'activation et répétez cette tâche sur un autre ordinateur. Cette opération doit être effectuée après l'activation de la première instance.
- Si vous installez plusieurs instances de BlackBerry Connectivity Node, vous devez configurer des connexions au répertoire identiques sur chaque instance. Vous pouvez utiliser la console BlackBerry Connectivity Node pour exporter les connexions au répertoire d'une instance (fichier .txt), puis transférer et importer ces connexions vers une autre instance de BlackBerry Connectivity Node à l'aide de la console de cette instance. Supprimez toutes les connexions au répertoire existantes d'une instance avant d'importer les configurations de répertoire.
- Vous pouvez également Créer un groupe de serveurs pour gérer les connexions régionales.
- Si vous souhaitez envoyer des données via un proxy HTTP avant d'atteindre BlackBerry Dynamics NOC, dans la console de BlackBerry Connectivity Node, cliquez sur **Paramètres généraux > BlackBerry Router et proxy**. Cochez la case **Activer le proxy HTTP** et configurez les paramètres de proxy.
- Si vous souhaitez changer les paramètres par défaut des instances de BlackBerry Connectivity Node, dans la barre de menus de la console de gestion, cliquez sur **Paramètres > Intégration externe > Configuration de BlackBerry Connectivity Node**, puis cliquez sur . Vous pouvez changer les paramètres de journalisation, désactiver des instances de BlackBerry Gatekeeping Service et configurer des paramètres BlackBerry Secure Gateway.
- Lorsque vous êtes averti d'une mise à jour de BlackBerry Connectivity Node, répétez cette tâche pour mettre à niveau chaque instance. Utilisez la console BlackBerry Connectivity Node pour enregistrer ou exporter des configurations de répertoire. Vous devez mettre à niveau toutes les instances de BlackBerry Connectivity Node vers la même version. Lorsque vous mettez à niveau la première instance, les services de répertoire sont désactivés jusqu'à ce que tous les nœuds soient mis à niveau vers la même version.
- 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 obtenir des instructions sur l'activation de BlackBerry Secure Gateway, reportez-vous à la section Protection des données de messagerie électronique envoyées aux terminaux iOS 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 Désignation des terminaux autorisés à accéder à Exchange ActiveSync dans le contenu relatif à l'administration.

# Créer un groupe de serveurs pour gérer les connexions régionales

Si vous souhaitez gérer les connexions régionales pour les fonctions de connectivité d'entreprise offertes par le BlackBerry Connectivity Node, vous pouvez déployer plusieurs instances du BlackBerry Connectivity Node dans une région dédiée en tant que 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. Les groupes de serveurs prennent également en charge la redondance, la haute disponibilité et l'équilibrage de charge pour les instances BlackBerry Connectivity Node.

**Avant de commencer :** Installez et configurez plusieurs instances de BlackBerry Connectivity Node.

1. Dans la console de gestion, 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**, cliquez sur le pays approprié.
5. Si vous souhaitez désactiver la connexion du répertoire d'entreprise pour les instances 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 (**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.
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 opérations 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.
   - Si vous souhaitez modifier les paramètres du journal local, cochez la case **Activer la destination du fichier local**. Spécifiez la limite de taille (en Mo) et la limite d'âge (en jours) et indiquez si vous souhaitez compresser les dossiers de journaux.
   - Si vous souhaitez configurer différents niveaux de journalisation pour les composants BlackBerry Connectivity Node, dans la section **Remplacement de la journalisation des services**, cliquez sur + et sélectionnez le composant et le niveau de journalisation appropriés. Si nécessaire, répétez l'opération.
9. Si vous souhaitez utiliser les instances dans le groupe de serveurs pour un seul type de connexion, cochez la case **Activer le mode Performances de service unique**. Dans le menu déroulant **Type de connexion**, 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 des instances du groupe de serveurs, cochez la case **Remplacer les paramètres BlackBerry Secure Gateway**. Pour les terminaux iOS 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. Entrez le point de terminaison de détection au format https://<*identity provider*>/.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 :** Sélectionnez le groupe de serveurs et cliquez sur pour y ajouter des instances BlackBerry Connectivity Node. Vous pouvez à tout moment ajouter une instance à un groupe de serveurs ou en supprimer une instance.

# Dépannage : BlackBerry Connectivity Node

| Problème | Solution possible |
| --- | --- |
| BlackBerry Connectivity Node ne s'active pas avec UEM Cloud. | • 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.<br>• Un fichier d'activation expire au bout de 60 minutes. Générez et téléchargez un nouveau fichier d'activation, puis essayez d'activer de nouveau.<br>• Reportez-vous à l'article KB 38964. |
| BlackBerry Connectivity Node ne se connecte pas à UEM Cloud. | • 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) :<br>  • 443 (HTTPS) pour activer BlackBerry Connectivity Node<br>  • 3101 (TCP) pour toute autre connexion sortante<br>• 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 UEM Cloud. Par défaut, les fichiers journaux se trouvent dans *<drive:>*:\Program Files\BlackBerry\BlackBerry Connectivity Node\Logs. |

| Problème | Solution possible |
| --- | --- |
| BlackBerry Connectivity Node ne se connecte pas avec le répertoire d'entreprise. | • Si vous avez plusieurs instances de BlackBerry Connectivity Node, vérifiez qu'elles ont toutes la même version du logiciel.<br>• Vérifiez que vous avez spécifié les paramètres corrects pour le répertoire d'entreprise.<br>• Vérifiez que toutes les instances disposent d'une connexion au répertoire et que les connexions au répertoire sont configurées de manière identique sur toutes les instances.<br>• 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.<br>• Vérifiez que les ports adaptés sont ouverts dans le pare-feu de votre organisation.<br>• Vérifiez que vous n'avez pas utilisé le même fichier d'activation pour deux installations différentes.<br>• Vérifiez que vous utilisez le fichier d'activation le plus récent.<br>• 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 se trouvent dans *<drive:>*:\Program Files\BlackBerry\BlackBerry Connectivity Node \Logs.<br>• Si vous utilisez Microsoft Active Directory, reportez-vous à l'article KB 36955. |

# Configurer BlackBerry UEM pour envoyer les données via un serveur proxy

Vous pouvez utiliser les configurations de proxy suivantes dans votre environnement BlackBerry UEM :

| Environnement | Options de proxy |
|---|---|
| UEM sur site | Vous pouvez configurer UEM pour envoyer les données via un serveur proxy TCP avant d'atteindre BlackBerry Infrastructure.<br><br>Par défaut, UEM se connecte directement à BlackBerry Infrastructure à l'aide du port 3101. Si la stratégie de sécurité de votre organisation empêche les systèmes internes de se connecter directement à Internet, vous pouvez installer un serveur proxy TCP. Le serveur proxy TCP fait office d'intermédiaire entre UEM et BlackBerry Infrastructure.<br><br>Vous pouvez installer un serveur proxy en dehors du pare-feu de votre organisation dans une zone démilitarisée. L'installation d'un serveur proxy TCP dans une zone démilitarisée offre un niveau de sécurité plus élevé pour UEM. Seul le serveur proxy se connecte à UEM en dehors du pare-feu. Toutes les connexions vers BlackBerry Infrastructure entre UEM et des terminaux passent par le serveur proxy. |
| UEM Cloud | Pour utiliser un serveur proxy avec BlackBerry Connectivity Node, vous pouvez installer BlackBerry Router en tant que serveur proxy, ou utiliser un serveur proxy TCP déjà installé dans l'environnement de votre organisation.<br><br>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 le serveur proxy.<br><br>Par défaut, BlackBerry Connectivity Node se connecte directement à BlackBerry Infrastructure à l'aide du port 3101. Si la stratégie de sécurité de votre organisation empêche les systèmes internes de se connecter directement à Internet, vous pouvez installer BlackBerry Router ou un serveur proxy TCP. BlackBerry Router ou le serveur proxy TCP fait office d'intermédiaire entre BlackBerry Connectivity Node et BlackBerry Infrastructure. |

## Envoi de données via un serveur proxy TCP vers BlackBerry Infrastructure

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

Dans les environnements UEM Cloud, le BlackBerry Connectivity Node envoie des données d'activation sur le port 443 (HTTPS). 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 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.

### Configurer BlackBerry UEM pour utiliser un serveur proxy TCP transparent

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

1. Suivez les étapes correspondant à votre environnement :

| Environnement | Étapes |
|---|---|
| UEM sur site | **a.** Dans la barre de menus de la console de gestion, cliquez sur **Paramètres > Infrastructure > BlackBerry Router et proxy**.<br>**b.** Sous **Paramètres généraux**, sélectionnez **Serveur proxy**.<br>**c.** Pour chaque service devant utiliser le serveur proxy, spécifiez le FQDN ou l'adresse IP et le numéro de port du serveur proxy. Chaque champ requiert une seule valeur. |
| UEM Cloud | **a.** Dans la console BlackBerry Connectivity Node (http:/localhost:8088), cliquez sur **Paramètres généraux > Proxy**.<br>**b.** Sélectionnez **Serveur proxy**.<br>**c.** Si vous souhaitez acheminer des données HTTPS d'activation pour le 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 serveur proxy doit être capable d'envoyer des données via le port 443 à <*region*>.bbsecure.com.<br>**d.** Si vous souhaitez acheminer des 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 <*region*>.bbsecure.com. |

2. 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 UEM.

1. Effectuez l'une des opérations suivantes :
   - Dans un environnement sur site UEM, dans la barre de menus de la console de gestion, cliquez sur **Paramètres > Infrastructure > BlackBerry Router et proxy**.
   - Dans un environnement UEM Cloud, dans la console BlackBerry Connectivity Node (http:/localhost:8088), cliquez sur **Paramètres généraux > Proxy**.
2. Sélectionnez **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 2 à 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**.

# Installer un BlackBerry Router autonome dans un environnement UEM Cloud

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).

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 à l'aide du port 3102. BlackBerry Router prend en charge tout le trafic sortant depuis les composants BlackBerry Connectivity Node.

**Avant de commencer :**

- Vous devez installer un BlackBerry Router autonome sur un ordinateur qui n'héberge pas d'instance du 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, *us*.srp.blackberry.com).

1. Dans la console de gestion UEM, sur la barre de menus, cliquez sur **Paramètres > Intégration externe > Configuration de BlackBerry Connectivity Node**.
2. Cliquez sur .
3. 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. Transférez le fichier **Setup.exe** vers l'ordinateur sur lequel vous souhaitez installer le BlackBerry Router et double-cliquez dessus pour exécuter l'application d'installation.

   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.
7. Dans la console BlackBerry Connectivity Node (http:/localhost:8088), cliquez sur **Paramètres généraux > Proxy**.
8. Sélectionnez **BlackBerry Router**.
9. Cliquez sur +.
10. Saisissez l'adresse IP ou le nom d'hôte de l'instance de BlackBerry Router que vous souhaitez connecter à UEM.
11. Cliquez sur **Ajouter**.
12. Dans le champ **Port**, saisissez le numéro du port d'écoute de toutes les instances de BlackBerry Router. La valeur par défaut est 3102.

**13.**Cliquez sur **Enregistrer**.

# Configurer des connexions via des serveurs proxy internes

Si votre organisation utilise un serveur proxy pour les connexions entre les serveurs de votre réseau, vous devrez peut-être configurer votre environnement sur site BlackBerry UEM pour :

- Autorisez UEM Core à communiquer avec la console de gestion s'il est installé sur un ordinateur distinct.
- Autorisez UEM à communiquer avec d'autres services internes, tels que les autorités de certification et les serveurs hébergeant des applications push.

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

1. Dans la barre de menus de la console de gestion, cliquez sur **Paramètres > Infrastructure > Proxy côté serveur**.
2. Effectuez l'une des opérations suivantes :

| Tâche | Étapes |
|---|---|
| Configurez les paramètres de proxy globaux de la plupart ou de tous les serveurs de votre domaine UEM. | **a.** Développez **Paramètres de proxy globaux côté serveur**.<br>**b.** Dans la liste déroulante **Type**, cliquez sur **Configuration PAC** ou **Configuration manuelle**.<br>**c.** Remplissez les champs requis.<br>**d.** Cliquez sur **Enregistrer**. |
| Configurez pour un ou plusieurs serveurs des paramètres de proxy différents des paramètres de proxy globaux. | **a.** Développez le nom du serveur.<br>**b.** Dans la liste déroulante **Type**, cliquez sur **Aucun**, **Configuration PAC** ou **Configuration manuelle**.<br>**c.** Remplissez les champs requis.<br>**d.** Cliquez sur **Enregistrer**. |

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

Vous devez connecter BlackBerry UEM sur site à un serveur SMTP pour lui permettre d'envoyer des instructions d'activation, des avertissements de conformité du terminal, des mots de passe pour UEM Self-Service et des notifications par e-mail aux utilisateurs du terminal.

1. Dans la barre de menus de la console de gestion, cliquez sur **Paramètres > Intégration externe > Serveur SMTP**.
2. Cliquez sur .
3. Dans le champ **Nom d'affichage de l'expéditeur**, saisissez un nom à utiliser pour les notifications par e-mail de UEM (par exemple, `donotreply` ou `UEM Admin`.
4. Dans le champ **Adresse de l'expéditeur**, saisissez l'adresse électronique que UEM doit utiliser pour envoyer les notifications par e-mail.
5. Dans le champ **Serveur SMTP**, saisissez le FQDN du serveur SMTP.
6. Dans le champ **Port de serveur SMTP**, tapez le numéro de port du serveur SMTP. Le numéro de port par défaut est 25.
7. Dans la liste déroulante **Type de cryptage pris en charge**, sélectionnez le type de cryptage approprié.
8. Si le serveur SMTP nécessite une authentification, spécifiez le nom d'utilisateur et le mot de passe.
9. Si nécessaire, importez un certificat CA SMTP :
   a) Copiez le fichier de certificat SSL du serveur SMTP de votre organisation sur l'ordinateur que vous utilisez.
   b) Cliquez sur **Parcourir**.
   c) Accédez au fichier de certificat SSL et sélectionnez-le, puis cliquez sur **Charger**.
10. Cliquez sur **Enregistrer**.

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

# Connexion à vos annuaires d'entreprise

Vous pouvez connecter BlackBerry UEM au répertoire d'entreprise de votre organisation pour bénéficier des fonctionnalités suivantes :

- Vous pouvez créer des comptes d'utilisateur dans UEM en utilisant les données d'utilisateur du répertoire, et UEM peut authentifier les administrateurs pour la console de gestion et les utilisateurs pour BlackBerry UEM Self-Service.
- Vous pouvez lier des groupes de répertoires d'entreprise à des groupes UEM afin d'organiser les utilisateurs tel qu'ils sont organisés dans votre répertoire d'entreprise et de simplifier l'attribution et la gestion des stratégies informatiques, des profils et des applications pour les utilisateurs. Ces groupes sont appelés « groupes liés au répertoire ».
- Vous pouvez activer l'intégration pour des groupes spécifiques de votre répertoire d'entreprise afin de créer automatiquement des utilisateurs de UEM. Ces groupes sont appelés « groupes de répertoires d'intégration ». Lorsque vous ajoutez de nouveaux utilisateurs à ces groupes de répertoires, de nouveaux comptes d'utilisateur sont créés pour eux dans UEM. Si vous activez l'intégration, vous pouvez également configurer la suppression afin de supprimer les données du terminal et les comptes d'utilisateur UEM lorsque des utilisateurs sont désactivés ou supprimés du répertoire d'entreprise.

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

| Étape | Action |
|---|---|
| 1 | Dans un environnement sur site UEM, Se connecter à une instance de Microsoft Active Directory ou Se connecter à un annuaire LDAP.<br>Dans un environnement UEM Cloud, installez et configurez BlackBerry Connectivity Node pour vous connecter au répertoire de votre entreprise.<br>Pour obtenir des instructions sur la connexion de UEM sur site ou de UEM Cloud à Entra ID, reportez-vous à Connecter BlackBerry UEM à Entra ID pour créer des comptes d'utilisateur de répertoire. |
| 2 | Vous pouvez également Activer les groupes liés par annuaire. |
| 3 | Vous pouvez également Activer et configurer l'intégration et la suppression. |
| 4 | Vous pouvez également configurer la synchronisation du répertoire. |

# Se connecter à une instance de Microsoft Active Directory

La tâche ci-dessous s'applique à un environnement sur site UEM. Dans un environnement UEM Cloud, installez et configurez BlackBerry Connectivity Node pour vous connecter au répertoire de votre entreprise.

**Avant de commencer :**

- créez un compte Microsoft Active Directory utilisable par UEM. Le compte doit être conforme aux exigences suivantes :

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

- Si votre organisation utilise une forêt de ressources Microsoft Exchange, vous devez créer une boite aux lettres dans cette forêt de ressources pour chaque compte d'utilisateur et associer les ressources aux comptes d'utilisateur dans les forêts de comptes. UEM utilise les boites aux lettres pour rechercher les comptes d'utilisateur dans les domaines individuels. Afin d'authentifier les utilisateurs qui se connectent à UEM, UEM doit lire les informations utilisateur qui sont stockées sur les serveurs de catalogue global qui font partie de la forêt de ressources. Vous devez créer un compte Microsoft Active Directory pour UEM qui est situé dans un domaine Windows faisant partie de la forêt de ressources. Lorsque vous créez la connexion au répertoire, vous fournissez les informations d'identification Windows du compte Microsoft Active Directory et, si nécessaire, les noms des serveurs de catalogue global que UEM peut utiliser.

1. Dans la barre de menus de la console de gestion de UEM, cliquez sur **Paramètres > Intégration externe > Répertoire d'entreprise**.
2. Cliquez sur + **> Connexion Microsoft Active Directory**.
3. Dans le champ **Nom de connexion du répertoire**, saisissez le nom de la connexion à l'annuaire.
4. Dans le champ **Nom d'utilisateur**, saisissez le nom d'utilisateur du compte Microsoft Active Directory.
5. Dans le champ **Domaine**, saisissez le nom du domaine Windows qui fait partie de la forêt Microsoft Exchange au format DNS (par exemple : exemple.com).
6. Dans le champ **Mot de passe**, saisissez le mot de passe du compte.
7. Dans la liste déroulante **Sélection du centre de distribution clé Kerberos**, effectuez l'une des opérations suivantes :
   - Pour autoriser UEM à détecter automatiquement les centres de distribution clés (KDC), cliquez sur **Automatique**.
   - Pour spécifier la liste de KDC à utiliser pour l'authentification de UEM, cliquez sur **Manuel**. Dans le champ **Noms des serveurs**, saisissez le nom du contrôleur de domaine KDC au format DNS (par exemple, kdc01.exemple.com). Si vous le souhaitez, ajoutez le numéro de port utilisé par le contrôleur de domaine (par exemple kdc01.exemple.com:88). Cliquez sur + pour spécifier des contrôleurs de domaine KDC supplémentaires que UEM doit utiliser.
8. Dans la liste déroulante **Sélection du catalogue global**, effectuez l'une des opérations suivantes :
   - Si vous souhaitez que UEM détecte automatiquement les serveurs de catalogue global, cliquez sur **Automatique**.
   - Pour spécifier la liste de serveurs de catalogue global que UEM doit utiliser, cliquez sur **Manuelle**. Dans le champ **Noms des serveurs**, saisissez le nom DNS du serveur de catalogue global auquel vous souhaitez que UEM accède (par exemple : catalogueglobal01.exemple.com). Si vous le souhaitez, ajoutez le numéro de port utilisé par le serveur de catalogue global (par exemple, globalcatalog01.com:3268). Cliquez sur + pour spécifier des serveurs supplémentaires.
9. Cliquez sur **Continuer**.
10. Dans le champ **Base de recherche du catalogue global**, effectuez l'une des opérations suivantes :
    - Pour permettre à UEM d'effectuer des recherches dans tout le catalogue global, laissez le champ vide.
    - Pour désigner les comptes d'utilisateur que UEM peut authentifier, saisissez le nom distinctif du conteneur d'utilisateurs (par exemple, OU=sales,DC=example,DC=com).

11. Si vous voulez activer la prise en charge de groupes globaux, dans la liste déroulante **Prise en charge des groupes globaux**, cliquez sur **Oui**.

    Si vous voulez utiliser des groupes globaux pour l' intégration, vous devez sélectionner **Oui**. Pour configurer un domaine de groupe global, dans la section **Liste des domaines de groupes globaux**, cliquez sur +. Dans le champ **Domaine**, cliquez sur le domaine à ajouter. La sélection par défaut pour le champ **Spécifier le nom d'utilisateur et le mot de passe ?** est Non. Si vous conservez cette sélection par défaut, le nom d'utilisateur et le mot de passe pour la connexion de la forêt sont utilisés. Si vous sélectionnez Oui, vous devez fournir des informations d'identification valides pour un compte Active Directory dans le domaine que vous avez sélectionné. Dans le champ **Sélection KDC**, vous pouvez sélectionner Automatique pour permettre à UEM de découvrir automatiquement les principaux centres de distribution ou Manuel pour spécifier la liste de KDC que UEM peut utiliser pour l'authentification. Cliquez sur **Ajouter**.
12. Si votre environnement comprend une forêt de ressources Microsoft Exchange, pour 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 UEM ait accès, dans la section **Liste des forêts de comptes**, cliquez sur +. Spécifiez le nom du domaine de l'utilisateur (l'utilisateur peut appartenir à n'importe quel domaine de la forêt de comptes) et le nom d'utilisateur et le mot de passe. Si nécessaire, spécifiez les KDC dans lesquels UEM doit effectuer la recherche. Si nécessaire, spécifiez les serveurs de catalogue global auxquels UEM doit accéder. Cliquez sur **Ajouter**.
13. Pour activer l'authentification unique, cochez la case **Activer l'authentification unique Windows**. Pour plus d'informations sur l'authentification unique, reportez-vous à la section Configurer l'authentification unique pour BlackBerry UEM dans le contenu relatif à l'administration.
14. Pour synchroniser plus d'informations utilisateur à partir de votre annuaire d'entreprise, cochez la case **Synchroniser les informations complémentaires sur l'utilisateur**. Les informations supplémentaires comprennent le nom de l'entreprise et le téléphone du bureau.
15. Cliquez sur **Enregistrer**.
16. Cliquez sur **Fermer**.

**À la fin :**

- Effectuez l'une des tâches facultatives suivantes :
  - Activer les groupes liés par annuaire.
  - Activer et configurer l'intégration et la suppression.
  - Configurez la synchronisation des répertoires.
- Si vous supprimez une connexion à un répertoire, tous les utilisateurs ajoutés à UEM à partir de ce répertoire seront convertis en utilisateurs locaux. Une fois les utilisateurs convertis en utilisateurs locaux, ils ne peuvent plus être reconvertis en utilisateurs associés à un répertoire, même si vous ajoutez à nouveau la connexion au répertoire d'entreprise ultérieurement. Les utilisateurs continueront à fonctionner comme des utilisateurs locaux, mais UEM ne pourra pas synchroniser les mises à jour à partir du répertoire d'entreprise.

# Se connecter à un annuaire LDAP

La tâche ci-dessous s'applique à un environnement sur site UEM. Dans un environnement UEM Cloud, installez et configurez BlackBerry Connectivity Node pour vous connecter au répertoire de votre entreprise.

**Avant de commencer :**

- pour UEM, créez un compte LDAP situé dans l'annuaire LDAP qui convient. Le compte doit être conforme aux exigences suivantes :
  - Le compte doit avoir l'autorisation de lire tous les utilisateurs du répertoire.

    - Le mot de passe doit être configuré pour ne pas expirer et ne doit pas être modifié lors de la connexion suivante.
- Si la connexion LDAP est chiffrée SSL, vérifiez que vous disposez du certificat de serveur correspondant à la connexion LDAP et que le serveur LDAP prend en charge TLS 1.2. Si SSL est activé, la connexion LDAP à UEM doit utiliser TLS 1.2.
- Vérifiez les valeurs d'attribut LDAP que votre organisation utilise (les étapes ci-dessous donnent des exemples de valeurs d'attribut typiques) ; vous les utiliserez dans les étapes ci-dessous.

1. Dans la barre de menus de la console de gestion de UEM, cliquez sur **Paramètres > Intégration externe > Répertoire d'entreprise**.
2. Cliquez sur + **> Connexion LDAP**.
3. Dans le champ **Nom de connexion du répertoire**, saisissez le nom de la connexion à l'annuaire.
4. Dans la liste déroulante **Détection du serveur LDAP**, effectuez l'une des opérations suivantes :
    - Pour détecter automatiquement le serveur LDAP, cliquez sur **Automatique**. Dans le champ **Nom de domaine DNS**, saisissez le nom de domaine du serveur qui héberge le répertoire d'entreprise.
    - Pour spécifier une liste de serveurs LDAP, cliquez sur **Sélectionner un serveur dans la liste ci-dessous**. Dans le champ **Serveur LDAP**, saisissez le nom du serveur LDAP. Pour ajouter d'autres serveurs LDAP, cliquez sur +.
5. Dans la liste déroulante **Activer SSL**, effectuez l'une des opérations suivantes :
    - Si la connexion LDAP est cryptée SSL, cliquez sur **Oui**. En regard du champ **Certificat SSL du serveur LDAP**, cliquez sur **Parcourir** et sélectionnez le certificat du serveur LDAP.
    - Si la connexion LDAP n'est pas cryptée SSL, cliquez sur **Non**.
6. Dans le champ **Port LDAP**, saisissez le numéro de port TCP pour la communication. Les valeurs par défaut sont 636 si SSL est activé ou 389 si SSL est désactivé.
7. Dans la liste déroulante **Autorisation requise**, effectuez l'une des opérations suivantes :
    - Si une autorisation est requise pour la connexion, cliquez sur **Oui**. Dans le champ **Connexion**, saisissez le DN de l'utilisateur autorisé à se connecter au LDAP (par exemple, an=admin,o=Org1). Dans le champ **Mot de passe**, saisissez le mot de passe.
    - Si aucune autorisation n'est requise pour la connexion, cliquez sur **Non**.
8. Dans le champ **Base de recherche d'utilisateurs**, saisissez la valeur à utiliser en tant que DN de base pour les recherches d'informations sur les utilisateurs.
9. Dans le champ **Filtre de recherche d'utilisateurs LDAP**, saisissez le filtre de recherche LDAP requis pour trouver des objets utilisateur dans le serveur d'annuaires de votre organisation. Par exemple, pour un IBM Domino Directory, saisissez `(objectClass=Person)`.
10. Dans la liste déroulante **Étendue de recherche de l'utilisateur LDAP**, effectuez l'une des opérations suivantes :
    - Pour rechercher tous les objets qui suivent l'objet de base, cliquez sur **Tous les niveaux**. Il s'agit du paramètre par défaut.
    - Pour rechercher les objets situés un niveau après le DN de base, cliquez sur **Un seul niveau**.
11. Dans le champ **Identifiant unique**, saisissez le nom de l'attribut qui identifie de manière unique chaque utilisateur du répertoire LDAP de votre organisation (cet attribut doit être une chaine immuable et globalement unique). Par exemple, `dominoUNID`.
12. Dans le champ **Prénom**, saisissez l'attribut de prénom de chaque utilisateur (par exemple, `givenName`).
13. Dans le champ **Nom**, saisissez l'attribut de nom de chaque utilisateur (par exemple, `sn`).
14. Dans le champ **Attribut de connexion**, saisissez l'attribut de connexion à utiliser pour l'authentification (par exemple, `uid`).
15. Dans le champ **Adresse électronique**, saisissez l'attribut d'adresse électronique de chaque utilisateur (par exemple, `mail`). Si vous ne définissez rien, la valeur par défaut sera utilisée.

16. Dans le champ **Nom d'affichage**, saisissez l'attribut de nom d'affichage de chaque utilisateur (par exemple, `displayName`). Si vous ne définissez rien, la valeur par défaut sera utilisée.
17. Dans le champ **Nom de l'utilisateur principal**, saisissez le nom principal de l'utilisateur pour SCEP (par exemple, `mail`).
18. Dans le champ **Service**, saisissez l'attribut de service de chaque utilisateur.
19. Dans le champ **Intitulé du poste**, saisissez l'attribut d'intitulé de poste de chaque utilisateur.
20. Si vous souhaitez synchroniser des champs supplémentaires à partir du répertoire LDAP, cochez la case **Synchroniser les informations complémentaires sur l'utilisateur**. Saisissez les attributs des champs supplémentaires selon les besoins.
21. Pour activer des groupes liés par répertoire pour la connexion au répertoire, cochez la case **Activer les groupes liés par répertoire**.
    a) Dans le champ **Base de recherche de groupes**, saisissez la valeur à utiliser en tant que DN de base pour les recherches d'informations de groupe.
    b) Dans le champ **Filtre de recherche de groupes LDAP**, saisissez le filtre de recherche LDAP requis pour trouver des objets de groupe dans le répertoire de votre organisation. Par exemple, pour IBM Domino Directory, saisissez `(objectClass=dominoGroup)`.
    c) Dans le champ **Identifiant unique du groupe**, saisissez l'attribut de l'identifiant unique de chaque groupe. Cet attribut doit être immuable et globalement unique (par exemple, `cn`).
    d) Dans le champ **Nom d'affichage du groupe**, saisissez l'attribut du nom d'affichage de chaque groupe (par exemple, saisissez `cn`).
    e) Dans le champ **Attribut d'adhésion au groupe**, saisissez le nom de l'attribut d'adhésion au groupe. Les valeurs d'attribut doivent être au format DN (par exemple, `CN=jsmith,CN=Users,DC=example,DC=com`).
    f) Dans le champ **Nom du groupe test**, saisissez un nom de groupe existant pour valider les attributs de groupe spécifiés.
    g) Si vous souhaitez activer la recherche paginée pour les membres de groupes, cochez la case **Activer la recherche de groupe paginée**.
22. Cliquez sur **Enregistrer**.
23. Cliquez sur **Fermer**.

**À la fin :**

- Effectuez l'une des tâches facultatives suivantes :
  - Activer les groupes liés par annuaire.
  - Activer et configurer l'intégration et la suppression.
  - Configurez la synchronisation des répertoires.
- Si vous supprimez une connexion à un répertoire, tous les utilisateurs ajoutés à UEM à partir de ce répertoire seront convertis en utilisateurs locaux. Une fois les utilisateurs convertis en utilisateurs locaux, ils ne peuvent plus être reconvertis en utilisateurs associés à un répertoire, même si vous ajoutez à nouveau la connexion au répertoire d'entreprise ultérieurement. Les utilisateurs continueront à fonctionner comme des utilisateurs locaux, mais UEM ne pourra pas synchroniser les mises à jour à partir du répertoire d'entreprise.

# Activer les groupes liés par annuaire

Vous pouvez lier des groupes de BlackBerry UEM à des groupes de votre répertoire d'entreprise afin d'organiser les utilisateurs dans UEM tel qu'ils sont organisés dans le répertoire et afin de simplifier l'attribution et la gestion des stratégies informatiques, des profils et des applications pour les utilisateurs. Pour plus d'informations, reportez-vous à la section Gestion et création de groupes d'applications dans le contenu relatif à l'administration.

**Avant de commencer :**

- Connectez-vous au répertoire de votre organisation :
  - UEM sur site : Se connecter à une instance de Microsoft Active Directory ou Se connecter à un annuaire LDAP.
  - UEM Cloud : Installez et configurez BlackBerry Connectivity Node pour vous connecter à Microsoft AD ou LDAP.
  - Sur site ou dans le cloud : Connecter UEM à Microsoft Entra ID.
- 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. Dans la barre de menus de la console de gestion, cliquez sur **Paramètres > Intégration externe > Répertoire d'entreprise**.
2. Cliquez sur une connexion du répertoire d'entreprise.
3. Dans l'onglet **Paramètres de synchronisation**, cochez la case **Activer les groupes liés par répertoire**.
4. Si vous souhaitez 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 du 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.
5. Dans le champ **Limite de synchronisation**, saisissez le nombre maximal de modifications que chaque processus de synchronisation peut effectuer.

   Si le nombre de modifications à synchroniser dépasse la limite de synchronisation, vous pouvez empêcher l'exécution du processus de synchronisation. UEM détermine le total des modifications suivantes : utilisateurs à ajouter aux groupes, utilisateurs à supprimer des groupes, utilisateurs à intégrer et utilisateurs à supprimer.
6. Dans le champ **Niveau d'imbrication maximal des groupes d'annuaires**, saisissez le nombre de niveaux imbriqués à synchroniser pour les groupes de répertoires d'entreprise.
7. Cliquez sur **Enregistrer**.

**À la fin :**

- Vous pouvez également Activer et configurer l'intégration et la suppression.
- Vous pouvez également configurer la synchronisation du répertoire.
- Créez des groupes liés par répertoire. Pour plus d'informations, reportez-vous à la section Création et gestion de groupes d'utilisateurs dans le contenu relatif à l'administration.

# Activer et configurer l'intégration et la suppression

Lorsque vous activez l'intégration, vous ajoutez des groupes de répertoires universels ou globaux à UEM en tant que groupes de répertoires d'intégration (l'intégration n'est pas prise en charge pour les groupes locaux de domaines). Lors d'un processus de synchronisation, si UEM détecte un utilisateur de répertoire dans un groupe de répertoires d'intégration ne possédant pas de compte d'utilisateur UEM correspondant, il crée ce compte d'utilisateur dans UEM. Lorsque vous activez l'intégration, vous pouvez également configurer la suppression ; lorsque vous désactivez ou supprimez un utilisateur d'un groupe de répertoires d'intégration, UEM peut supprimer les données du terminal et supprimer l'utilisateur de UEM.

**Remarque :** Lorsque la suppression est activée, tous les comptes d'utilisateur UEM qui ne sont pas membres d'un groupe de répertoires d'intégration, quelle que soit la manière dont ils ont été ajoutés à UEM, sont supprimés lors du processus de synchronisation suivant.

**Avant de commencer :**

- Connectez-vous au répertoire de votre organisation :
  - UEM sur site : Se connecter à une instance de Microsoft Active Directory ou Se connecter à un annuaire LDAP.
  - UEM Cloud : Installez et configurez BlackBerry Connectivity Node pour vous connecter à Microsoft AD ou LDAP.
  - Sur site ou dans le cloud : Connecter UEM à Microsoft Entra ID.
- 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. Dans la barre de menus de la console de gestion, cliquez sur **Paramètres > Intégration externe > Répertoire d'entreprise**.
2. Cliquez sur une connexion du répertoire d'entreprise.
3. Dans l'onglet **Paramètres de synchronisation**, cochez la case **Activer les groupes liés par répertoire**.
4. Cochez la case **Activer l'intégration**.
5. Effectuez l'une des opérations suivantes :

| Tâche | Étapes |
| --- | --- |
| Ajoutez des groupes de répertoires d'intégration et configurez les options d'activation de terminal. | **a.** Cliquez sur +.<br>**b.** Recherchez et ajoutez des groupes de répertoires universels ou globaux.<br>**c.** Pour chaque groupe de répertoires, indiquez si vous souhaitez lier des groupes imbriqués.<br>**d.** Dans la section **Activation des terminaux**, indiquez si vous souhaitez que les utilisateurs intégrés reçoivent un mot de passe et un e-mail 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. |
| Intégrez les utilisateurs ne devant utiliser que des applications BlackBerry Dynamics. | Suivez ces étapes si vous souhaitez intégrer des utilisateurs qui n'utiliseront que des applications BlackBerry Dynamics. Ces utilisateurs n'activeront pas leurs terminaux sur UEM à l'aide de UEM Client et leurs terminaux ne seront pas gérés par UEM.<br>**a.** Cochez la case **Intégrer uniquement les utilisateurs disposant d'applications à BlackBerry Dynamics**.<br>**b.** Cliquez sur +.<br>**c.** Recherchez et ajoutez des groupes de répertoires universels ou globaux.<br>**d.** Pour chaque groupe de répertoires, indiquez si vous souhaitez lier des groupes imbriqués.<br>**e.** Spécifiez le nombre de clés d'accès à générer par utilisateur, la période d'expiration des clés d'accès et le modèle d'e-mail. |

| Tâche | Étapes |
| --- | --- |
| Configurez la suppression. | Si vous souhaitez supprimer les données d'un terminal lorsqu'un utilisateur est supprimé de UEM, cochez la case **Supprimer les données du terminal lorsque l'utilisateur est supprimé de tous les groupes de répertoires d'intégration**. Procédez comme suit :<br>• Sélectionnez l'option appropriée pour les données que vous souhaitez supprimer du terminal.<br>• Si vous souhaitez supprimer un utilisateur de UEM lorsque cet utilisateur est supprimé de tous les groupes de répertoires d'intégration, cochez la case **Supprimer l'utilisateur lorsqu'il est supprimé de tous les groupes de répertoires d'intégration**.<br>• Si vous souhaitez retarder la suppression des utilisateurs et des données du terminal de deux heures après un cycle de synchronisation, cochez la case **Protection contre la suppression**. Cette option permet d'éviter les suppressions inattendues liées à la latence de réplication de répertoire. |

6. Si vous souhaitez 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 du 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.
7. Dans le champ **Limite de synchronisation**, saisissez le nombre maximal de modifications que chaque processus de synchronisation peut effectuer.

   Si le nombre de modifications à synchroniser dépasse la limite de synchronisation, vous pouvez empêcher l'exécution du processus de synchronisation. UEM détermine le total des modifications suivantes : utilisateurs à ajouter aux groupes, utilisateurs à supprimer des groupes, utilisateurs à intégrer et utilisateurs à supprimer.
8. Dans le champ **Niveau d'imbrication maximal des groupes d'annuaires**, saisissez le nombre de niveaux imbriqués à synchroniser pour les groupes de répertoires d'entreprise.
9. Cliquez sur **Enregistrer**.

**À la fin :** Vous pouvez également configurer la synchronisation du répertoire.

# Synchroniser une connexion à un répertoire

Une fois que vous avez connecté UEM au répertoire d'entreprise de votre organisation, vous pouvez démarrer manuellement le processus de synchronisation à tout moment ou planifier des synchronisations récurrentes. Vous pouvez prévisualiser un rapport de synchronisation avant la prochaine synchronisation et afficher le rapport une fois le processus de synchronisation terminé.

**Avant de commencer :**

- Connectez-vous au répertoire de votre organisation :
  - UEM sur site : Se connecter à une instance de Microsoft Active Directory ou Se connecter à un annuaire LDAP.
  - UEM Cloud : Installez et configurez BlackBerry Connectivity Node pour vous connecter à Microsoft AD ou LDAP.
  - Sur site ou dans le cloud : Connecter UEM à Microsoft Entra ID.

- Si vous le souhaitez, Activer les groupes liés par annuaire et Activer et configurer l'intégration et la suppression.

1. Dans la barre de menus de la console de gestion, cliquez sur **Paramètres > Intégration externe > Répertoire d'entreprise**.
2. Effectuez l'une des opérations suivantes :

| Tâche | Étapes |
|---|---|
| Prévisualisez une synchronisation. | **a.** Cliquez sur pour la connexion au répertoire pour laquelle vous souhaitez prévisualiser la synchronisation.<br>**b.** Cliquez sur **Afficher un aperçu maintenant**.<br>**c.** Une fois le traitement du rapport terminé, cliquez sur la date de la colonne **Dernier rapport**. |
| Démarrez manuellement une synchronisation de répertoire. | **a.** Cliquez sur pour la connexion au répertoire que vous souhaitez synchroniser.<br>**b.** Une fois la synchronisation terminée, cliquez sur la date de la colonne **Dernier rapport**.<br>**c.** Pour exporter un rapport au format .csv, cliquez sur . |
| Ajoutez un calendrier de synchronisation. | **a.** Cliquez sur la connexion au répertoire pour laquelle vous souhaitez planifier la synchronisation.<br>**b.** Dans l'onglet **Planning de synchronisation**, cliquez sur .<br>**c.** Dans la liste déroulante **Type de synchronisation**, sélectionnez l'une des options suivantes :<br>• **Tous les groupes et utilisateurs** : les utilisateurs sont intégrés et supprimés selon les besoins et les modifications apportées à l'appartenance au groupe et aux attributs d'utilisateur sont synchronisées.<br>• **Groupes d'intégration** : les utilisateurs sont intégrés et supprimés selon les besoins et les modifications apportées aux attributs d'utilisateur sont synchronisées.<br>• **Groupes associés à un répertoire** : les modifications apportées à l'appartenance au groupe et aux attributs d'utilisateur sont synchronisées.<br>• **Attributs de l'utilisateur** : seules les modifications apportées aux attributs d'utilisateur sont synchronisées.<br>**d.** Dans la liste déroulante **Récurrence**, sélectionnez l'option appropriée et configurez les paramètres de récurrence selon les besoins.<br>**e.** Cliquez sur **Ajouter**.<br>**f.** Cliquez sur **Enregistrer**. |

# Connecter BlackBerry UEM à Entra ID pour créer des comptes d'utilisateur de répertoire

Vous pouvez connecter BlackBerry UEM à Microsoft Entra ID pour créer des comptes d'utilisateur de répertoire dans UEM. Après avoir configuré la connexion, vous pouvez rechercher et importer des données d'utilisateur à partir du répertoire pour créer des utilisateurs UEM. 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 un utilisateur du répertoire, ce dernier peut également utiliser les informations d'identification du répertoire pour se connecter à la console de gestion.

Si votre organisation utilise un Active Directory sur site et que les comptes sont synchronisés sur Entra ID, vous devez plutôt créer une connexion au répertoire pour votre Active Directory sur site (reportez-vous à Se connecter à une instance de Microsoft Active Directory). La connexion UEM à Entra ID est appropriée lorsque Entra ID est votre service de répertoire principal et que vous ne disposez pas d'un Active Directory sur site.

**Remarque :** Après avoir connecté UEM à Entra ID, les URL de la console UEM sont modifiées comme suit (« &redirect=no » est supprimé à la fin de l'URL) :

- Console de gestion : https://<*server_name*>:<*port*>/admin/index.jsp?tenant=<*tenant_ID*>
- Console Self-Service : https://<*server_name*>:<*port*>/monpériphérique/index.jsp?tenant=<*tenant_ID*>

**Avant de commencer :** Vous devez disposer d'un compte Microsoft Entra ID. Si vous ne possédez pas de compte, rendez-vous sur https://azure.microsoft.com pour en créer un. Utilisez ce compte pour vous connecter au portail Entra.

1. Connectez-vous au portail Entra.
2. Dans la section des enregistrements d'applications Entra ID, ajoutez un nouvel enregistrement.
3. Spécifiez les éléments suivants et terminez l'enregistrement :
   a) Saisissez un nom pour l'enregistrement.
   b) Sélectionnez les types de compte qui peuvent utiliser l'application ou accéder à l'API.
   c) Pour l'URI de redirection, cliquez sur **Web** et saisissez `http://localhost`.
4. Copiez l'ID d'application.

   Il s'agit de l'ID client que vous allez enregistrer avec UEM.
5. Dans la section relative à la gestion des autorisations d'API (bouton Enregistrer), ajoutez une autorisation et sélectionnez les éléments suivants :
   - **Microsoft Graph**
   - **Autorisations des applications**
   - Définissez les autorisations suivantes : **Group.Read.All (Application)**, **User.Read (Delegated)**, **User.Read.All (Application)**
6. Accordez le consentement de l'administrateur pour tous les comptes du répertoire actuel.
7. Dans la section relative à la gestion des certificats et des secrets, ajoutez un nouveau secret de client et spécifiez une description et une durée.
8. Copiez le champ Valeur du nouveau secret de client (et non l'ID de secret).

   Il s'agit de la clé client que vous enregistrerez avec UEM.
9. Dans la barre de menus de la console de gestion de UEM, cliquez sur **Paramètres > Intégration externe > Répertoire d'entreprise**.
10. Cliquez sur + > **Connexion Microsoft Entra ID**.
11. Dans le champ **Nom de connexion du répertoire**, saisissez le nom de la connexion.
12. Dans le champ **Domaine**, saisissez le domaine Entra ID.

**13.**Dans le champ **ID client**, saisissez l'ID que vous avez enregistré à l'étape 4.

**14.**Dans le champ **Clé client**, saisissez la valeur que vous avez enregistrée à l'étape 8.

**15.**Cliquez sur **Continuer**.

**16.**Cliquez sur **Enregistrer**.

**À la fin :** Vous pouvez effectuer l'une des tâches facultatives suivantes :

- Activer les groupes liés par annuaire
- Activer et configurer l'intégration et la suppression
- Synchroniser une connexion à un répertoire

# Configuration de BlackBerry UEM pour gérer les profils de protection des applications Microsoft Intune

Si vous souhaitez utiliser BlackBerry UEM pour créer, gérer et attribuer des profils de protection des applications Microsoft Intune afin de protéger les données des applications Office 365, vous devez procéder comme suit :

| Étape | Action |
|---|---|
| 1 | Examinez Conditions préalables à la prise en charge de la protection des applications Intune. |
| 2 | Créer un enregistrement d'application dans Entra. |
| 3 | Configurer BlackBerry UEM pour la synchronisation avec Microsoft Intune. |

## Conditions préalables à la prise en charge de la protection des applications Intune

- Pour synchroniser BlackBerry UEM avec Intune, vous devez utiliser un compte d'administrateur Microsoft avec une licence Intune et avec l'une des autorisations suivantes sur le portail Entra : administrateur global, administrateur limité avec rôle d'administrateur Intune Service ou rôle personnalisé avec les autorisations décrites dans l'article KB 50341.
- Les comptes d'utilisateur auxquels vous souhaitez attribuer des profils de protection des applications Intune doivent exister dans Entra ID.
- Les utilisateurs doivent être ajoutés à UEM en tant qu' utilisateurs de répertoire.
- Si vous avez intégré votre Microsoft Active Directory sur site, les utilisateurs doivent être synchronisés sur Entra ID. Pour plus d'informations, consultez la documentation Microsoft pour Entra ID Connect.

## Créer un enregistrement d'application dans Entra

Vous devez créer dans Entra un enregistrement d'application que UEM peut utiliser pour s'authentifier auprès de Entra.

**Avant de commencer :**

- Examinez Conditions préalables à la prise en charge de la protection des applications Intune.
- Dans la barre de menus de la console de gestion UEM, cliquez sur **Paramètres > Intégration externe > Microsoft Intune**. Enregistrez la valeur du champ **URL de réponse**. Vous utiliserez cette URL à l'étape 3.

1. Connectez-vous au portail Entra.
2. Dans la section des enregistrements d'applications, ajoutez un nouvel enregistrement.
3. Spécifiez les éléments suivants et terminez l'enregistrement :
   a) Saisissez un nom pour l'enregistrement.
   b) Sélectionnez les types de compte qui peuvent utiliser l'application ou accéder à l'API.

c) Pour l'URI de redirection, cliquez sur **Client mobile/Bureau** et saisissez l'URL de réponse à partir de la console de gestion.

4. Copiez l'ID d'application.

   Il s'agit de l'ID client que vous allez enregistrer avec UEM.

5. Dans la section relative à la gestion des autorisations d'API, ajoutez une autorisation et sélectionnez les éléments suivants :

   - **Microsoft Graph**
   - **Autorisations déléguées**
   - Définissez les autorisations déléguées suivantes :
     - **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)**

6. Accordez le consentement de l'administrateur pour tous les comptes du répertoire actuel.
7. Dans la section relative à la gestion des certificats et des secrets, ajoutez un nouveau secret de client et spécifiez une description et une durée.
8. Copiez le champ Valeur du nouveau secret de client (et non l'ID de secret).

   Il s'agit de la clé client que vous enregistrerez avec UEM.

**À la fin :** Configurer BlackBerry UEM pour la synchronisation avec Microsoft Intune.

# Configurer BlackBerry UEM pour la synchronisation avec Microsoft Intune

**Avant de commencer :** Créer un enregistrement d'application dans Entra.

1. Dans la barre de menus de la console de gestion, cliquez sur **Paramètres > Intégration externe > Microsoft Intune**.
2. Dans le champ **ID de locataire Entra**, saisissez l'ID du locataire Entra ID de votre organisation.
3. Dans le champ **ID client**, saisissez l'ID que vous avez enregistré dans Créer un enregistrement d'application dans Entra.
4. Dans le champ **Clé client**, saisissez la valeur que vous avez enregistrée dans Créer un enregistrement d'application dans Entra.
5. Cliquez sur **Suivant**.
6. Spécifiez les informations d'identification du compte d'administrateur Intune que vous souhaitez utiliser pour le processus de synchronisation.

**À la fin :**

- Reportez-vous à la section Gestion des applications protégées par Microsoft Intune dans le contenu relatif à l'administration.
- Si vous devez saisir à nouveau les informations d'identification du compte d'administrateur Intune (par exemple, vous changez le mot de passe du compte), dans **Paramètres > Intégration externe > Microsoft Intune**, cliquez sur **Mettre à jour les informations d'identification**.

# Configuration de BlackBerry UEM en tant que partenaire de conformité Intune dans Entra

Si vous avez configuré l'accès conditionnel Entra ID pour votre organisation, vous pouvez configurer BlackBerry UEM en tant que partenaire de conformité afin que les terminaux iOS et Android gérés par UEM puissent être reconnus comme conformes par Intune lors de l'accès à vos applications basées sur le cloud telles que Office 365.

Vous pouvez configurer plusieurs instances de UEM pour chaque locataire Entra, mais tous les locataires UEM partagent la même entrée de gestion de la conformité des partenaires. Entra ne peut pas identifier le locataire UEM dont une mise à jour de l'état de conformité provient. Vous pouvez configurer un locataire UEM pour connecter un ou plusieurs locataires Entra. Vous devez ajouter une connexion de répertoire à UEM pour chaque locataire Entra.

Lorsque les utilisateurs activent leurs terminaux sur UEM, UEM envoie l'état de conformité du terminal à Entra. L'exigence de conformité est satisfaite sans avoir à inscrire les terminaux directement auprès de Intune. UEM avertit Entra lorsqu'un terminal n'est pas conforme ou lorsqu'un terminal revient en conformité.

Si vous ne souhaitez pas utiliser le contrôle d'accès conditionnel « Terminal requis à marquer comme conforme » dans Entra, et vous souhaitez utiliser des emplacements sécurisés pour contrôler l'accès à partir des terminaux qui se trouvent à l'intérieur de votre réseau, dans UEM, vous pouvez acheminer le trafic vers les services Microsoft via les instances BlackBerry Connectivity Node de votre entreprise. Dans ce scénario, vous n'avez pas besoin de suivre les instructions de cette section pour connecter UEM à Entra ID pour un accès conditionnel.

## Conditions préalables pour configurer l'accès conditionnel Entra ID

- Vérifiez que vous disposez d'un compte Microsoft avec une licence Intune et avec l'une des autorisations suivantes sur le portail Entra : administrateur global, administrateur limité avec rôle d'administrateur Intune Service ou rôle personnalisé avec les autorisations décrites dans l'article KB 50341.
- Dans le centre d'administration Microsoft, dans la section de gestion des partenaires de conformité, ajoutez **Accès conditionnel BlackBerry UEM Entra** en tant que partenaire de conformité pour les terminaux iOS et Android et attribuez-le aux utilisateurs et aux groupes.
- Dans Entra ID, créez et configurez un profil d'accès conditionnel et activez l'option « Exiger que le terminal soit marqué comme conforme ». Notez qu'il s'agit du seul paramètre de profil d'accès conditionnel avec lequel UEM interagit.
- Pour pouvoir utiliser cette fonction, les utilisateurs de terminal doivent répondre aux exigences suivantes :
  - Les utilisateurs doivent exister dans Entra ID et disposer d'une licence Intune valide. Pour plus d'informations, reportez-vous à la section Licences Microsoft Intune.
  - Si vous synchronisez votre Active Directory sur site avec Entra ID, l'UPN Active Directory sur site des utilisateurs doit correspondre à leur UPN Entra ID.
  - Les utilisateurs doivent être ajoutés à UEM en tant qu' utilisateurs de répertoire.
- Après avoir vérifié les conditions préalables ci-dessus, suivez les étapes de la section Configurer l'accès conditionnel Entra ID.
  - Notez que les étapes de configuration vous indiquent d'activer UEM Client pour s'inscrire à BlackBerry Dynamics et installer UEM Client sur les terminaux.
  - Les étapes vous indiquent d'installer l'application Microsoft Authenticator sur les terminaux des utilisateurs avant activation avec UEM. Si vous souhaitez retarder l'inscription à l'accès conditionnel sur le terminal jusqu'à ce que l'application Microsoft Authenticator soit installée (manuellement par l'utilisateur ou déployée avec UEM), vous pouvez activer le paramètre « Démarrer l'inscription à l'accès conditionnel après l'installation du courtier d'authentification » dans le profil BlackBerry Dynamics attribué. Notez que

cette option n'est pas prise en charge pour les terminaux Android avec le type d'activation Confidentialité des données utilisateur (elle s'applique à la Confidentialité des données utilisateur Android Enterprise et Android Management). Si cette option est activée, une fois l'application Microsoft Authenticator installée, le processus d'inscription à l'accès conditionnel est lancé lorsque l'utilisateur ouvre UEM Client. Sur les terminaux Android, si l'espace travail est déverrouillé, l'utilisateur est invité à ouvrir UEM Client pour démarrer l'inscription à l'accès conditionnel.

# Configurer l'accès conditionnel Entra ID

**Avant de commencer :** Vérifiez que vous remplissez les conditions préalables pour l'accès conditionnel à Entra ID.

1. Dans la barre de menus de la console de gestion UEM, cliquez sur **Paramètres > Intégration externe > Accès conditionnel Entra ID**.
2. Cliquez sur +.
3. Saisissez un nom pour la configuration.
4. Dans la liste déroulante **Entra cloud**, cliquez sur **GLOBAL**.
5. Dans le champ **ID de locataire Entra**, saisissez le nom de locataire de votre organisation au format FQDN ou l'ID de locataire unique au format GUID.
6. Sous **Remplacement de mappage de terminal**, cliquez sur **UPN** ou **E-mail**.

   Si vous choisissez UPN, vérifiez que le locataire Entra ID et tous les répertoires mappés partagent la même valeur UPN pour les utilisateurs avant d'enregistrer la connexion. Une fois la connexion enregistrée, vous ne pouvez pas modifier le remplacement de mappage de terminal.
7. Dans la liste **Répertoires d'entreprise disponibles**, sélectionnez et ajoutez les répertoires d'entreprise appropriés.
8. Cliquez sur **Enregistrer**.
9. Sélectionnez le compte d'administrateur que vous souhaitez utiliser pour vous connecter au locataire Entra de votre organisation.
10. Acceptez la demande d'autorisation de Microsoft.
11. Dans la barre de menus, cliquez sur **Stratégies et profils > Stratégie > BlackBerry Dynamics**. Procédez comme suit pour tout profil BlackBerry Dynamics que vous prévoyez d'attribuer aux utilisateurs du terminal (par exemple, le profil par défaut et les profils personnalisés).
    a) Ouvrez et modifiez le profil.
    b) Sélectionnez **Autoriser UEM Client à s'inscrire dans BlackBerry Dynamics**.
    c) Si vous souhaitez retarder le processus d'inscription à l'accès conditionnel jusqu'à ce que l'application Microsoft Authenticator soit installée sur les terminaux, sélectionnez **Démarrer l'inscription à l'accès conditionnel après l'installation du courtier d'authentification**.
    d) Cliquez sur **Enregistrer**.
    e) Attribuez le profil aux utilisateurs et aux groupes selon les besoins.
12. Dans la barre de menus, cliquez sur **Stratégies et profils > Réseaux et connexions > Connectivité BlackBerry Dynamics**. Procédez comme suit pour tout profil de connectivité BlackBerry Dynamics que vous prévoyez d'attribuer aux utilisateurs du terminal (par exemple, le profil par défaut et les profils personnalisés).
    a) Ouvrez et modifiez le profil.
    b) Dans la section **Serveurs d'application**, cliquez sur **Ajouter**.
    c) Recherchez **Feature-Azure Conditional Access** et cliquez dessus.
    d) Cliquez sur **Enregistrer**.
    e) Dans le tableau **Accès conditionnel Azure**, cliquez sur +.
    f) Dans le champ **Serveur**, saisissez `gdas-<UEM_SRP_ID>.<region_code>.bbsecure.com`.

g) Dans le champ **Port**, saisissez 443.
h) Sous **Type de route**, cliquez sur **Direct**.
i) Cliquez sur **Enregistrer**.
j) Attribuez le profil aux utilisateurs et aux groupes selon les besoins.

13. Attribuez l'application **Feature-Azure Conditional Access** aux utilisateurs ou aux groupes. Pour plus d'informations, reportez-vous aux sections Gérer les comptes d'utilisateurs et Gérer un groupe d'utilisateurs.
14. Créez et configurez un profil de conformité et attribuez-le aux utilisateurs et aux groupes si nécessaire. Le tableau suivant détaille la manière dont les actions de conformité UEM sont signalées à Intune :

| Action d'application de la conformité UEM | Comportement |
|---|---|
| Action d'application : surveiller et consigner | Rien n'est signalé à Intune. |
| Action d'application :<br>• Ne pas faire confiance<br>• Supprimer uniquement les données professionnelles<br>• Supprimer toutes les données | UEM notifie Entra ID après que toutes les invites utilisateur ont expiré. |
| Action d'application pour les applications BlackBerry Dynamics : surveiller et consigner | Rien n'est signalé à Intune. |
| Action d'application pour BlackBerry Dynamics :<br>• Ne pas autoriser l'exécution d'applications BlackBerry Dynamics<br>• Supprimer les données d'applications BlackBerry Dynamics | UEM notifie Entra ID dès que la violation de conformité est détectée. |

15. Installez UEM Client et l'application Microsoft Authenticator sur les terminaux des utilisateurs. Vous pouvez attribuer et déployer l'application Microsoft Authenticator avec UEM (voir Ajout d'applications publiques à la liste d'applications), ou vous pouvez demander aux utilisateurs de la télécharger eux-mêmes.
16. En fonction du client de messagerie que votre entreprise souhaite utiliser, vous devez effectuer des étapes supplémentaires pour vous assurer que le client de messagerie peut valider et communiquer avec Entra :
    - Pour BlackBerry Work, reportez-vous à la section Configuration de l'application BlackBerry Work pour l'accès conditionnel à Entra ID dans le Guide d'administration BlackBerry Work.
    - Pour le client de messagerie natif iOS, reportez-vous à l'article KB 94163.
    - Pour Android Gmail, reportez-vous à l'article KB 94494.

**À la fin :**

- Lorsqu'un utilisateur active son terminal, UEM Client l'invite à s'inscrire à l'accès conditionnel Entra. Les utilisateurs disposant de terminaux activés sont invités à s'inscrire à l'accès conditionnel Entra la prochaine fois qu'ils ouvrent le UEM Client.
  **Remarque :** Demandez aux utilisateurs de lancer l'inscription à Entra à l'aide de UEM Client, sans utiliser d'options de connexion dans Microsoft Authenticator. L'invite à l'inscription de UEM Client ouvre Microsoft Authenticator pour inviter l'utilisateur à saisir ses informations d'identification et à terminer le processus d'inscription.
- Lorsqu'un utilisateur active un terminal avec UEM, vous pouvez vérifier les propriétés du terminal de l'utilisateur dans Microsoft Endpoint Manager pour confirmer qu'il a été inscrit avec Entra comme prévu. Le nom du terminal sera au format suivant : *<username>* - *<platform>* inconnu inconnu - *<xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxx>*.

- Si vous modifiez le périmètre des utilisateurs ou des groupes dans la configuration de la conformité des partenaires Entra, dans le portail Entra, accédez aux autorisations de sécurité pour l'accès conditionnel BlackBerry UEM et accordez à nouveau le consentement administrateur pour BlackBerry.
- Lorsque vous supprimez un terminal à partir de UEM, le terminal reste inscrit à l'accès conditionnel Entra ID. Les utilisateurs peuvent supprimer leur compte Entra ID dans les paramètres de compte de l'application Microsoft Authenticator ou vous pouvez supprimer le terminal du portail Entra.

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

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

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

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 UEM. Si vous enregistrez un nouveau certificat APNs, les utilisateurs de terminaux doivent réactiver leurs terminaux pour recevoir des données.

Il est recommandé d'accéder à la console de gestion et au portail Apple Push Certificates Portal via Google Chrome ou Safari, car ces navigateurs offrent une prise en charge optimale pour demander et enregistrer un certificat APNs.

## Demander et enregistrer un certificat APNs

1. Dans la barre de menus de la console de gestion, cliquez sur **Paramètres > Intégration externe > Apple Push Notification**.
2. Dans la section **Étape 1 sur 3 - Télécharger le certificat CSR signé de BlackBerry**, cliquez sur **Télécharger le certificat**.
3. Enregistrez le fichier CSR signé sur votre ordinateur.
4. Dans la section **Étape 2 sur 3 - Obtenir un certificat APNs auprès d'Apple**, cliquez sur **Apple Push Certificate Portal**.
5. Connectez-vous au portail Apple Push Certificates Portal en utilisant un ID Apple valide.
6. Suivez les instructions pour charger le fichier CSR signé.

   Si une erreur de type de fichier non valide s'affiche, vous pouvez renommer le fichier en fichier .txt et le charger à nouveau.
7. Téléchargez et enregistrez le certificat APNs sur votre ordinateur.
8. Dans la console de gestion, dans la section **Étape 3 sur 3 : inscrire le certificat APNs**, cliquez sur **Parcourir**.
9. Accédez au certificat APNs et sélectionnez-le.
10. Cliquez sur **Submit**.

**À la fin :**

- Pour tester la connexion entre UEM et le serveur APNs, cliquez sur **Tester le certificat APNs**.
- Le certificat APNs est valable un an. Vous devez renouveler le certificat APNs chaque année avant son expiration en utilisant le même ID Apple que celui utilisé pour obtenir le certificat APNs d'origine. Pour renouveler le certificat, répétez les étapes ci-dessus, mais cliquez sur **Renouveler le certificat** à l'étape 2.

# Dépannage : APNs

| Problème | Solution possible |
| --- | --- |
| Lorsque vous essayez d'obtenir un CSR signé, vous recevez l'erreur suivante : « Le système a rencontré une erreur. Réessayez. » | Reportez-vous à l'article KB 37266. |
| Lorsque vous essayez d'enregistrer le certificat APNs, le message d'erreur « Le certificat APNs ne correspond pas au fichier CSR » s'affiche. | 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. |
| Vous ne pouvez pas activer de terminaux iOS ou macOS | Il se peut que le certificat APNs ne soit pas correctement enregistré. Vérifiez les points suivants :<br>• Dans la barre de menus de la console de gestion, cliquez sur **Paramètres > Intégration externe > Apple Push Notification**. Vérifiez que l'état du certificat APNs indique Installé. Si cet état est incorrect, essayez à nouveau d'enregistrer le certificat APNs.<br>• Cliquez sur **Tester le certificat APNs** pour tester la connexion entre BlackBerry UEM et le serveur APNs.<br>• Si nécessaire, procurez-vous un nouveau fichier CSR signé auprès de BlackBerry ainsi qu'un nouveau certificat APNs. |

# Configurer BlackBerry UEM pour le programme d'inscription des appareils (DEP)

Vous pouvez configurer BlackBerry UEM pour qu'il se synchronise avec le programme d'inscription des appareils (DEP) Apple si vous souhaitez utiliser la console de gestion UEM afin de gérer l'activation des terminaux iOS que votre organisation a achetés pour le programme d'inscription des appareils.

1. Dans la console de gestion, accédez à **Paramètres > Intégration externe > Programme d'inscription des appareils Apple**.

   Si vous utilisez UEM sur site, cliquez sur + et saisissez le nom du compte.
2. Dans la section **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.
4. Dans la section **2 sur 4 : Télécharger une clé publique**, cliquez sur **Télécharger une clé publique**.
5. Enregistrez la clé publique sur votre ordinateur local.
6. Dans la section **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**.
7. Connectez-vous à votre compte du programme d'inscription des appareils. Dans les préférences de votre compte, téléchargez le jeton de serveur pour le serveur MDM.
8. Dans la section **4 sur 4 : Enregistrer le jeton de serveur avec BlackBerry UEM**, cliquez sur **Parcourir**.
9. Accédez au fichier de jeton de serveur .p7m et sélectionnez-le. Cliquez sur **Ouvrir** puis sur **Suivant**.
10. Dans la fenêtre de configuration d'inscription, saisissez le nom de la configuration.
11. Si vous souhaitez que UEM attribue automatiquement la configuration d'inscription aux terminaux lorsque vous les inscrivez avec le programme d'inscription des appareils Apple, cochez la case **Attribuer automatiquement tous les nouveaux terminaux à cette configuration**. Ne sélectionnez pas cette option si vous souhaitez utiliser la console de gestion UEM pour attribuer manuellement la configuration d'enrôlement à des terminaux spécifiques.
12. 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.
13. Dans la section **Configuration du terminal**, sélectionnez l'une des options suivantes :

    - **Autoriser le couplage** : les utilisateurs peuvent 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** : les utilisateurs peuvent désactiver les terminaux.
    - **Veuillez patienter pendant la configuration du terminal** : cette option empêche les utilisateurs d'annuler la configuration des terminaux tant que l'activation avec UEM n'est pas terminée.
14. Dans la section **Ignorer pendant la configuration**, sélectionnez les éléments que vous ne souhaitez pas inclure dans la configuration des terminaux :

| Option | Impact si sélectionné |
|---|---|
| Mot de passe | Les utilisateurs ne sont pas invités à créer un mot de passe pour le terminal. |
| Services de localisation | Les services de localisation sont désactivés sur le terminal. |

| Option | Impact si sélectionné |
|---|---|
| Restaurer | Les utilisateurs ne peuvent pas restaurer les données à partir d'un fichier de sauvegarde. |
| Déplacer depuis Android | Les données ne peuvent pas être restaurées depuis un terminal Android. |
| ID Apple | Les utilisateurs ne peuvent pas se connecter avec Apple ID et iCloud. |
| Conditions d'utilisation | Les utilisateurs ne voient pas les conditions d'utilisation iOS. |
| Siri | Siri est désactivé sur les terminaux. |
| Diagnostics | Les informations de diagnostic ne sont pas envoyées automatiquement par le terminal lors de la configuration. |
| Biométrique | Les utilisateurs ne peuvent pas configurer Touch ID. |
| Paiement | Les utilisateurs ne peuvent pas configurer Apple Pay. |
| Zoom | Les utilisateurs ne peuvent pas configurer Zoom. |
| Configuration de l'icône de l'écran d'accueil | Les utilisateurs ne peuvent pas régler le clic sur l'icône de l'écran d'accueil. |
| Temps d'écran | L'option de configuration du temps d'écran est ignorée lors de l'inscription DEP. |
| Mise à jour logicielle | Les utilisateurs ne voient pas l'écran de mise à jour obligatoire du logiciel sur le terminal. |
| iMessage et FaceTime | Les utilisateurs ne voient pas iMessage et l'écran FaceTime sur le terminal. |
| Ton d'affichage | Les utilisateurs ne voient pas l'écran Ton d'affichage sur le terminal. |
| Confidentialité | Les utilisateurs ne voient pas l'écran Confidentialité sur le terminal. |
| Intégration | Les utilisateurs ne voient pas l'écran d'intégration sur le terminal. |
| Migration Watch | Les utilisateurs ne voient pas l'écran Migration Watch sur le terminal. |
| Configuration SIM | Les utilisateurs ne voient pas l'écran permettant de configurer un forfait cellulaire sur le terminal. |
| Migration terminal à terminal | Les utilisateurs ne voient pas l'écran Migration terminal à terminal sur le terminal. |

15. Cliquez sur **Enregistrer**. 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 le programme d'inscription des appareils, consultez Activation de terminaux iOS inscrits dans DEP.
- 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. Pour renouveler le jeton, dans **Paramètres > Intégration externe > Programme d'inscription des appareils Apple**, cliquez sur le compte DEP puis sur **Mettre à jour le jeton de serveur**. Effectuez les deux étapes pour générer un nouveau jeton de serveur et l'enregistrer auprès de UEM.
- Vous pouvez supprimer n'importe quelle connexion DEP que vous créez. si vous supprimez toutes les connexions DEP, vous ne pouvez pas activer de nouveaux terminaux Apple dans le programme d'inscription des appareils . Si vous avez attribué des configurations d'inscription à des terminaux et que celles-ci n'ont pas été appliquées, UEM supprime les configurations d'inscription attribuées aux terminaux. La suppression de la connexion n'affecte pas les terminaux actifs sur UEM.

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

Les terminaux Android Enterprise offrent une sécurité supplémentaire aux entreprises qui souhaitent gérer des terminaux Android. Le tableau suivant récapitule les différentes options de configuration de BlackBerry UEM pour prendre en charge les terminaux Android Enterprise :

| Méthode | Quand choisir cette méthode | Type de compte d'utilisateur | Services Google pris en charge |
|---|---|---|---|
| Connectez un domaine UEM à un domaine Google Workspace. | Votre organisation utilise un domaine Google Workspace. | Comptes Google Workspace (pour les entreprises) | • Tous les services Google Workspace tels que Gmail, Google Calendar et Drive.<br>• Gestion des applications via Google Play |
| Connectez un domaine UEM à un domaine Google Cloud. | Votre organisation utilise un domaine Google Cloud. | Comptes Google Cloud, également appelés comptes Google gérés (pour les entreprises) | • Semblables à Google Workspace mais sans l'accès aux produits payants tels que Gmail, Google Calendar et Drive.<br>• Gestion des applications via Google Play |
| Autorisez UEM à gérer les terminaux Android Enterprise comme des comptes Google Play gérés. | Votre organisation n'utilise pas de domaine Google ou utilise un domaine Google déjà connecté à un domaine UEM et vous souhaitez utiliser les terminaux Android Enterprise sur un deuxième domaine UEM. | Les terminaux Android Enterprise qui ont des comptes gérés Google Play | • Gestion des applications via Google Play<br>• Les services Google ne sont pas pris en charge. |

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

**Avant de commencer :** Si vous avez précédemment connecté un domaine UEM à un domaine Google et souhaitez connecter un nouveau domaine UEM, vous devez supprimer la connexion existante. Dans la barre de menus de la console de gestion, cliquez sur **Paramètres > Intégration externe > Connexion au domaine Google** et supprimez la connexion. Vous pouvez également supprimer la connexion dans les paramètres d'administration de Google Play (https://play.google.com/work) en utilisant le même compte Google que celui utilisé pour créer

la connexion. Si vous supprimez une connexion, tous les terminaux activés avec un type d'activation Android Enterprise sont désactivés.

1. Dans la barre de menus de la console de gestion, cliquez sur **Paramètres > Intégration externe > Gestion d'Android et de Chrome**.
2. Effectuez l'une des opérations 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**.<br>**b.** Cliquez sur **Suivant**.<br>**c.** Dans la fenêtre **Bring Android to Work**, connectez-vous à l'aide d'un compte Google, Google ou Gmail. Le compte que vous utilisez devient le compte d'administrateur pour le service Bring Android to Work.<br>**d.** Cliquez sur **Mise en route**.<br>**e.** Saisissez le nom de votre entreprise Cliquez sur **Confirmer**.<br>**f.** Cliquez sur **Terminer l'enregistrement**. |
| Utilisez un domaine Google. | **a.** Sélectionnez **Connecter BlackBerry UEM à votre domaine Google existant**.<br>Notez que vous ne pouvez pas partager de domaines Google entre plusieurs domaines UEM. Cette option prend en charge Android Enterprise et Chrome OS Enterprise.<br>**b.** Cliquez sur **Suivant**.<br>**c.** Renseignez les champs pour créer un compte de service et cliquez sur **Suivant**. |

3. Effectuez l'une des opérations suivantes :
   - Pour envoyer les détails de configuration de l'application à l'aide de BlackBerry Infrastructure, sélectionnez **Envoyer la configuration de l'application à l'aide d'UEM Client**.
   - Pour envoyer les détails de configuration de l'application à l'aide de l'infrastructure Google, sélectionnez **Envoyer la configuration de l'application à l'aide de Google Play**.
4. Lorsque vous y êtes invité, cliquez sur **Accepter** afin d'accepter les autorisations définies pour certaines des applications Google et BlackBerry affichées ou toutes.
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, reportez-vous à la section Activation des terminaux Android dans le contenu relatif à l'administration.
- Vous pouvez modifier la connexion au domaine Google dans Paramètres > Intégration externe pour changer le type de domaine Google que vous utilisez ou pour tester la connexion au domaine.
- Si vous prévoyez de mettre hors service un domaine UEM connecté à un Google, supprimez la connexion avant de mettre le domaine hors service (Paramètres > Intégration externe > Connexion au domaine Google). Vous pouvez également supprimer la connexion dans les paramètres d'administration de Google Play (https://play.google.com/work) en utilisant le même compte Google que celui utilisé pour créer la connexion. Si vous supprimez une connexion, tous les terminaux activés avec un type d'activation Android Enterprise sont désactivés.

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

Les terminaux Android Management offrent une sécurité supplémentaire aux organisations qui souhaitent gérer des terminaux à l'aide de l'API Android Management.

Avant d'activer des terminaux avec des types d'activation Android Management, consultez Considérations relatives aux types d'activation Android Management.

| Étape | Action |
| --- | --- |
| 1 | Configurer Android Management dans la console Google Cloud. |
| 2 | Configurer Android Management dans BlackBerry UEM. |

## Configurer Android Management dans la console Google Cloud

Vous devez configurer Android Enterprise à l'aide d'un compte Google Play géré pour pouvoir accéder à l'option de configuration de Android Management.

Lorsque vous configurez Android Management, vous devez utiliser une adresse e-mail dédiée. Vous ne pouvez pas utiliser une adresse électronique ayant été utilisée pour configurer Android Enterprise.

1. Rendez-vous sur https://console.developers.google.com et connectez-vous à l'aide de l'adresse électronique allant être utilisée pour Android Management.
2. Dans la console Cloud, cliquez sur **Nouveau projet**.
3. Cliquez sur **API et services > Sélectionner une bibliothèque**.
4. Dans la barre de recherche, recherchez API Android Management.
5. Dans la liste des résultats de la recherche, activez **API Android Management** et **API Cloud Pub/Sub**.
6. Dans la barre de menus de la console Cloud, cliquez sur **IAM & Admin > Comptes de service > Sélectionner > Créer un compte de service**.
7. Dans la section **Accorder à ce compte de service l'accès au projet**, dans la liste déroulante **Rôle**, sélectionnez **Utilisateur d'Android Management**.
8. Dans la deuxième liste déroulante **Rôle**, sélectionnez **Admin Pub/Sub**.
9. Dans la section **Accorder aux utilisateurs l'accès au compte de service**, saisissez l'adresse électronique que vous avez utilisée à l'étape 1.
10. Cliquez sur **Terminé**.
11. Dans la barre de menus, cliquez sur **Comptes de service** et sélectionnez le compte que vous avez créé.
12. Cliquez sur **Clés > Ajouter une clé**.
13. Dans la boite de dialogue **Créer une clé privée pour "<*service_account_name*>"**, sélectionnez **JSON**. Cliquez sur **Créer**.
14. Enregistrez le nom du compte de service, l'adresse e-mail de l'administrateur du compte de service et la clé privée JSON.

**À la fin :** Configurer Android Management dans BlackBerry UEM.

# Configurer Android Management dans BlackBerry UEM

**Avant de commencer :**

- Configurer Android Management dans la console Google Cloud.
- Vérifiez que Android Enterprise a déjà été configuré dans UEM. Reportez-vous à la section Configuration de BlackBerry UEM pour la prise en charge des terminaux Android Enterprise.
- Vérifiez que vous disposez du nom du compte de service et de l'adresse e-mail de l'administrateur du compte de service Android Management et de la clé privée JSON.

1. Dans la barre de menus de la console de gestion UEM, cliquez sur **Paramètres > Intégration externe > Gestion d'Android et de Chrome**.
2. Cliquez sur **Ajouter une connexion de gestion Android**.
3. Dans le champ **Nom d'affichage de l'entreprise**, saisissez le nom du compte de service.
4. Dans le champ **Adresse e-mail de l'administrateur**, saisissez l'adresse e-mail du compte de service.
5. Dans le champ **Informations sur le compte de service (format json)**, saisissez la clé privée JSON.
6. Cliquez sur **Enregistrer**.
7. Dans la boite de dialogue **Nom de domaine ou nom d'entreprise**, dans le champ **Votre réponse**, saisissez le nom du compte de service Android Management. Cliquez sur **Suivant**.

# Extension de la gestion des terminaux Chrome OS à BlackBerry UEM

Vous pouvez intégrer BlackBerry UEM à un domaine géré Google pour étendre certaines fonctionnalités de Chrome OS à UEM. Le domaine Google doit inclure la mise à niveau de Chrome Enterprise. Notez que l'inscription et certaines tâches de gestion des terminaux Chrome OS s'effectuent toujours via la console de domaines gérés Google.

UEM synchronise les unités organisationnelles à partir de la console d'administration Google en groupes d'unités organisationnelles UEM. Après la synchronisation initiale, UEM s'enregistre auprès du domaine Google pour être averti de toute modification apportée aux unités organisationnelles, aux utilisateurs ou aux terminaux. Lorsque UEM est informé d'une modification, il synchronise et met à jour la base de données en conséquence.

| Étape | Action |
|---|---|
| 1 | Créer un compte de service pour s'authentifier auprès du domaine Google. |
| 2 | Activer UEM pour synchroniser les données Chrome OS. |
| 3 | Intégrer UEM au domaine Google. |

Si vous avez déjà configuré UEM pour prendre en charge les terminaux Android Enterprise, vous pouvez suivre ces étapes afin d'autoriser UEM à gérer les terminaux Chrome OS :

| Étape | Action |
|---|---|
| 1 | Vérifiez que le domaine Google de votre organisation est doté de Chrome OS Enterprise activé. |
| 2 | Vérifiez que l'API Chrome Policy est activée dans le domaine Google de votre organisation. Pour plus d'informations, reportez-vous à Créer un compte de service pour s'authentifier auprès du domaine Google. |
| 3 | Vérifiez que toutes les étendues sont ajoutées. Pour plus d'informations, reportez-vous à Activer UEM pour synchroniser les données Chrome OS. |
| 4 | Activez la gestion Chrome OS dans la console UEM. Pour plus d'informations, reportez-vous à Intégrer UEM au domaine Google. |

## Créer un compte de service pour s'authentifier auprès du domaine Google

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

1. Connectez-vous à la console Google Developers à l'aide du compte Google que vous souhaitez utiliser pour gérer votre projet.
2. Créez un projet.
3. Sélectionnez le projet et créez-lui un compte de service.
4. Attribuez au compte de service le rôle **De base > Éditeur**.
5. Sélectionnez le compte de service et ajoutez une nouvelle clé P12.
6. Copiez le mot de passe de la clé privée et enregistrez le certificat sur votre ordinateur local.
7. Localisez et copiez l'ID client unique et l'adresse électronique associés au compte de service.
8. Dans la section des API et des services activés, recherchez et activez les API suivantes :
   - **API Admin SDK**
   - **API EMM Google Play**
   - **API Chrome Policy**

**À la fin :** Activer UEM pour synchroniser les données Chrome OS.

# Activer UEM pour synchroniser les données Chrome OS

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

**Avant de commencer :** Créer un compte de service pour s'authentifier auprès du domaine Google.

1. Connectez-vous à la console d'administration Google à l'aide du compte d'administrateur de votre domaine Google.
2. Accédez à la section relative aux intégrations tierces pour les terminaux mobiles.
3. Vérifiez que la gestion mobile Android tierce est activée.
4. Dans la section d'ajout de fournisseurs EMM, générez un jeton.
5. Copiez le jeton.
6. Dans la section des contrôles d'API de sécurité, cliquez sur l'option de gestion de délégation à l'échelle du domaine.
7. Ajoutez une nouvelle configuration.
8. Pour l'ID client, collez l'ID client unique du compte de service Google.
9. Pour l'étendue OAuth, saisissez ou collez les éléments suivants dans une liste de valeurs délimitées par une virgule :
   - https://www.googleapis.com/auth/admin.directory.user
   - https://www.googleapis.com/auth/admin.directory.customer
   - https://www.googleapis.com/auth/admin.directory.device.chromeos
   - https://www.googleapis.com/auth/admin.directory.device.mobile
   - https://www.googleapis.com/auth/admin.directory.orgunit
   - https://www.googleapis.com/auth/admin.directory.user
   - https://www.googleapis.com/auth/chrome.management.policy
   - https://www.googleapis.com/auth/admin.reports.audit.readonly
10. Autorisez la connexion.

**À la fin :** Intégrer UEM au domaine Google.

# Intégrer UEM au domaine Google

**Avant de commencer :** Activer UEM pour synchroniser les données Chrome OS.

1. Connectez-vous à la console de gestion UEM à l'aide d'un compte d'administrateur de sécurité.
2. Sur la barre de menus, cliquez sur **Paramètres > Intégration externe > Gestion d'Android et de Chrome**.
3. Sélectionnez **Connecter BlackBerry UEM à votre domaine Google existant**.
4. Dans **Mode d'envoi des configurations d'application**, sélectionnez **Envoyer la configuration de l'application à l'aide de Google Play**.
5. Cliquez sur **Suivant**.
6. Dans le champ **Mot de passe de clé privée**, collez le mot de passe de la clé privée à partir de la console Google Developers.
7. Cliquez sur **Parcourir**.
8. Accédez au fichier de certificat et sélectionnez-le dans la console Google Developers.
9. Dans le champ **Adresse e-mail du compte de service**, collez l'adresse électronique du compte de service Google à partir de la console Google Developers.
10. Dans le champ **Adresse électronique de l'administrateur Google**, saisissez l'adresse électronique du compte d'administrateur utilisé pour gérer le domaine Google Cloud ou Google Workspace par Google.
11. Dans le champ **Jeton**, collez le jeton que vous avez généré.
12. Dans la section **Sélectionnez le type de domaine utilisé pour la gestion des terminaux Android avec profil professionnel**, sélectionnez le type approprié de domaine Google.
13. Si vous sélectionnez **Domaine Google Cloud**, choisissez l'une des options suivantes :
    - **Ne pas autoriser BlackBerry UEM à créer des utilisateurs dans le domaine** : si vous choisissez cette option, vous devez créer des utilisateurs dans votre domaine Google Cloud et créer des utilisateurs locaux avec les mêmes adresses électroniques dans UEM.
    - **Autoriser BlackBerry UEM à créer des utilisateurs dans le domaine** : si vous choisissez cette option, sélectionnez l'une des options suivantes :
      - **Ne pas autoriser BlackBerry UEM à supprimer des utilisateurs dans le domaine Google**
      - **Autoriser BlackBerry UEM à supprimer des utilisateurs dans le domaine Google**
14. Cliquez sur **Suivant** et choisissez les applications que vous souhaitez ajouter à UEM.
15. Cliquez sur **Suivant**.
16. Cliquez de nouveau sur **Suivant**.

**À la fin :** Pour synchroniser UEM avec la console d'administration Google, dans la barre de menus, cliquez sur **Paramètres > Intégration externe > Gestion d'Android et de Chrome**. Dans la section **Gestion de Chrome OS**, cliquez sur **Activer**. UEM effectue une synchronisation initiale des données en 10 minutes et planifie des synchronisations régulières. Une fois la synchronisation terminée, vous pouvez utiliser les options de cet écran afin de lancer des synchronisations non planifiées pour les unités organisationnelles, les utilisateurs et les appareils.

# Simplification des activations Windows 10

Lorsqu'un utilisateur active un terminal Windows 10 avec BlackBerry UEM, il doit spécifier l'adresse du serveur UEM. Vous pouvez simplifier le processus d'activation pour les utilisateurs à l'aide des méthodes suivantes :

| Méthode | Description |
|---|---|
| Intégrez UEM avec la jonction à Entra ID. | Si vous configurez la jonction à Entra ID, les utilisateurs peuvent activer leurs terminaux en utilisant uniquement leur nom d'utilisateur et leur mot de passe Entra ID. Une licence Entra ID Premium est requise.<br>Reportez-vous à la section Intégration de UEM avec la jonction à Entra ID. |
| Configurez Windows Autopilot. | Si vous configurez Windows Autopilot, l'inscription fait partie de la première expérience de configuration et le terminal est automatiquement activé lorsque l'utilisateur l'effectue en utilisant uniquement son nom d'utilisateur et son mot de passe Entra ID. Une intégration avec une jonction à Entra ID et une licence Entra ID Premium sont requises.<br>Reportez-vous à la section Configurer Windows Autopilot s pour l'activation du terminal. |
| Déployez un service de détection. | vous pouvez utiliser une application Web Java de BlackBerry comme service de détection. Vous pouvez utiliser différents systèmes d'exploitation et outils d'application Web pour déployer une application Web de détection.<br>Reportez-vous à la section Déployer un service de détection pour simplifier les activations Windows 10. |

## Intégration de UEM avec la jonction à Entra ID

Vous pouvez intégrer BlackBerry UEM avec la jonction à Entra ID Windows 10 pour simplifier le processus d'inscription des terminaux. 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 Entra ID. La jonction à Entra ID 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. Un certificat UEM peut être installé manuellement sur le terminal ou les administrateurs peuvent déployer le certificat à l'aide de SCCM.

**Avant de commencer :** Vous aurez besoin de l'URL des conditions d'utilisation de MDM, de l'URL de la détection de MDM et de l'URI de l'ID d'application pour effectuer les étapes ci-dessous. Pour déterminer ces URL, dans la console de gestion UEM, créez un compte d'utilisateur test et envoyez à l'utilisateur un e-mail d'activation à l'aide du modèle d'e-mail d'activation par défaut. Le modèle par défaut contient la variable %ClientlessActivationURL% qui correspond à la valeur appropriée figurant dans l'e-mail reçu. Utilisez cette valeur pour les URL suivantes dans les étapes ci-dessous :

- URL des conditions d'utilisation de MDM : *%ClientlessActivationURL%*/azure/termsofuse
- URL de la détection de MDM : *%ClientlessActivationURL%*/azure/discovery
- URI de l'ID d'application : *%ClientlessActivationURL%*

1. Connectez-vous au portail de gestion Microsoft Entra ID.

2. Dans la section relative à la gestion de MDM et de MAM, ajoutez une application MDM sur site et attribuez-lui un nom convivial (par exemple, `BlackBerry UEM`).
3. Cliquez sur l'application que vous avez ajoutée pour en configurer les paramètres.
4. Spécifiez l'étendue de l'utilisateur. Le cas échéant, sélectionnez des groupes.
5. Spécifiez l'URL des conditions d'utilisation de MDM et l'URL de sa détection.
6. Enregistrez les modifications.
7. Dans les propriétés des paramètres d'application MDM sur site, spécifiez l'URI de l'ID d'application.
8. Enregistrez les informations.

**À la fin :** Vous pouvez également Configurer Windows Autopilot s pour l'activation du terminal.

### Configurer Windows Autopilot s pour l'activation du terminal

Si vous configurez Windows Autopilot, le terminal est automatiquement activé lorsque l'utilisateur effectue la configuration initiale avec uniquement son nom d'utilisateur et son mot de passe Entra ID.

**Avant de commencer :** Intégration de UEM avec la jonction à Entra ID.

1. Connectez-vous au portail de gestion Microsoft Entra ID.
2. Dans la section relative à l'inscription des appareils Windows, créez un profil de déploiement Windows Autopilot.
3. Saisissez le nom et la description du profil.
4. Configurez les paramètres de configuration initiale.
5. Attribuez le profil aux groupes d'utilisateurs appropriés.
6. Enregistrez le profil.
7. Effectuez les étapes suivantes sur chaque terminal Windows 10 que vous souhaitez activer avec Windows Autopilot :
   a) Allumez le terminal pour charger la configuration initiale et vous connecter à un réseau Wi-Fi.
   b) Appuyez sur les touches CTRL + MAJ + F3 pour redémarrer et passer en mode audit.
   c) Exécutez Windows PowerShell en tant qu'administrateur et exécutez les commandes suivantes :

   ```
   Save-Script -Name Get-WindowsAutoPilotInfo -Path C:\Windows\Temp
   ```

   ```
   Install-Script -Name Get-WindowsAutoPilotInfo
   ```

   ```
   Get-WindowsAutoPilotInfo.ps1 -OutputFile C:\Windows\Temp\MyComputer.csv
   ```

   d) Récupérez le fichier .csv résultant de chaque terminal.
8. Dans le portail de gestion Microsoft Entra ID, dans la section relative à l'inscription des appareils Windows et aux appareils Windows Autopilot, importez le fichier .csv à partir de chaque terminal.
9. Dans la boite de dialogue Outil de préparation système, procédez comme suit :
   a) Pour le nettoyage du système, sélectionnez l'option d'accès à la configuration initiale (OOBE) et désélectionnez l'option de généralisation.
   b) Dans les options d'arrêt, sélectionnez l'option de redémarrage.

# Déployer un service de détection pour simplifier les activations Windows 10

Vous pouvez transformer une application Web Java de BlackBerry en service de détection afin de simplifier le processus d'activation pour les utilisateurs dotés de terminaux Windows 10. Si vous utilisez le service de détection, les utilisateurs n'auront plus besoin de saisir l'adresse du serveur lors du processus d'activation.

Vous pouvez utiliser différents systèmes d'exploitation et outils d'application Web pour déployer une application Web de détection. Les étapes ci-dessous concernent les tâches de haut niveau ; les actions spécifiques dépendent de l'environnement de votre organisation.

1. Configurez une adresse IP statique pour l'ordinateur qui hébergera le service de détection.
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 un enregistrement DNS de type A pour le nom **enterpriseenrollment**<*email_domain*> pointant vers l'adresse IP statique que vous avez configurée.
4. Créez et installez un certificat pour sécuriser les connexions TLS entre les terminaux Windows 10 et le service de détection.
5. Connectez-vous à myAccount pour télécharger l'outil de détection automatique de proxy. Exécutez le fichier .exe pour extraire un fichier .war.
   Le fichier .exe permet d'extraire le fichier `W10AutoDiscovery-<version>.war` dans `C:\BlackBerry`.
6. Remplacez le nom du fichier `W10AutoDiscovery-<version>.war` par `ROOT.war`. Déplacez le fichier vers la racine du dossier de votre serveur d'applications Java.
7. Mettez à jour le fichier wdp.properties de l'application Web du service de détection afin d'inclure une liste des ID SRP (UEM sur site) ou des ID de locataire (UEM Cloud) pour vos instances UEM. Les ID figurent dans myAccount.

# 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 UEM source sur site. Dans les environnements sur site UEM, vous pouvez également effectuer une migration à partir d'un serveur Good Control autonome.

| Étape | Action |
|---|---|
| 1 | Passez en revue les conditions préalables à la migration et les bonnes pratiques et considérations. |
| 2 | Connexion à un serveur source. |
| 3 | Migrer des stratégies informatiques, des profils et des groupes depuis un serveur source. |
| 4 | Migrer des utilisateurs depuis un serveur source. |
| 5 | Migrer des terminaux depuis un serveur source. |

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

| Élément | Conditions préalables |
|---|---|
| Autorisations des administrateurs de sécurité | Suivez les instructions de cette section en tant qu'administrateur de sécurité. |
| Versions prises en charge du serveur source | Pour UEM sur site, vous pouvez effectuer une migration à partir des serveurs source suivants :<br>• UEM sur site version 12.18 ou ultérieure<br>• Good Control (autonome) version 5.0 ou ultérieure<br>Pour UEM Cloud, vous pouvez migrer des données depuis UEM sur site uniquement. L'instance UEM sur site source doit être l'une des trois versions majeures les plus récentes. Les versions plus anciennes ne sont pas prises en charge pour la migration. |
| BlackBerry Connectivity Node (UEM Cloud uniquement) | Pour prendre en charge toutes les fonctions de migration, vous devez activer au moins une instance de BlackBerry Connectivity Node version 2.13 ou ultérieure. |

| Élément | Conditions préalables |
| --- | --- |
| Connexion au répertoire d'entreprise UEM | Configurez la connexion au répertoire d'entreprise UEM de destination telle qu'elle est configurée sur le serveur source. La migration ne fonctionne pas si la connexion au répertoire d'entreprise ne correspond pas. |
| Défragmentez les bases de données (UEM sur site uniquement) | Défragmentez les bases de données UEM source et de destination avant de commencer la migration. Si vous déplacez un grand nombre d'utilisateurs ou de terminaux, vous devrez défragmenter la base de données UEM de destination après la migration de chaque groupe d'utilisateurs ou de terminaux. |
| BlackBerry UEM Client | • UEM sur site : si vous prévoyez de migrer les applications UEM Client et BlackBerry Dynamics inscrites à BlackBerry Dynamics, vous devez installer la dernière version de UEM Client sur les terminaux.<br>• UEM Cloud : UEM Client doit correspondre à la version 12.x ou ultérieure. |
| Applications BlackBerry Dynamics | • UEM sur site : toutes les applications BlackBerry Dynamics que vous prévoyez de migrer doivent utiliser la version 7.1 ou ultérieure du SDK BlackBerry Dynamics. Pour les migrations depuis Good Control, les applications doivent utiliser la version 4.0.0 ou ultérieure du SDK.<br>• UEM Cloud : toutes les applications BlackBerry Dynamics que vous prévoyez de migrer doivent utiliser la version 8.0 ou ultérieure du SDK BlackBerry Dynamics.<br>• Les applications BlackBerry Dynamics qui ne sont pas prises en charge pour la migration sont supprimées du terminal pendant le processus de migration. |

| Élément | Conditions préalables |
| --- | --- |
| Autorisations d'applications BlackBerry Dynamics | • Le serveur UEM de destination doit disposer de la même liste d'autorisations d'applications BlackBerry Dynamics que le serveur source.<br>• Les comptes d'utilisateur migrés doivent se voir attribuer la même liste d'autorisations d'applications BlackBerry Dynamics sur le serveur UEM de destination que celle dont ils disposent sur le serveur source.<br>• Le délégué d'authentification doit être le même sur le serveur source et le serveur de destination. Vous pouvez modifier le délégué d'authentification après la migration.<br>• Si le profil BlackBerry Dynamics sur le serveur source permet à UEM Client d'être activé par BlackBerry Dynamics, configurez-le sur le serveur de destination.<br>• Le délégué d'authentification doit être le même sur le serveur source et le serveur UEM de destination. Vous pouvez modifier le délégué d'authentification après la migration.<br>• Pour les migrations effectuées à partir d'une instance de Good Control, les terminaux possédant un délégué d'authentification de terminal de Good for Enterprise ne sont pas migrés. Après la suppression de Good for Enterprise en tant que délégué d'authentification, actualisez le cache avant de poursuivre la migration.<br>Si les autorisations ne correspondent pas entre le serveur source et le serveur de destination, les applications BlackBerry Dynamics sont désactivées après la migration. |
| Applications BlackBerry Dynamics personnalisées | Les applications personnalisées sont migrées uniquement si les serveurs source et de destination ont le même ID d'organisation. Pour plus d'informations sur la fusion d'organisations, reportez-vous à l'article KB 47626. |
| Ports | • UEM sur site : vérifiez que les ports 1433 (TCP) et 1434 (UDP) sont débloqués sur Microsoft SQL Server.<br>• UEM Cloud : le port 8887 (TCP) doit être ouvert entre le serveur UEM sur site et BlackBerry Connectivity Node. Vérifiez que le port utilisé par l'instance de Microsoft SQL Server qui héberge la base de données UEM sur site est ouvert et accessible par BlackBerry Connectivity Node (par exemple, le port 1433). |

# Bonnes pratiques et considérations relatives à la migration de UEM

**Migration des stratégies informatiques, des profils et des groupes**

| Élément | Considérations et bonnes pratiques |
|---|---|
| Éléments copiés à partir d'un serveur UEM source | • Stratégies informatiques sélectionnées<br>• Profils de messagerie<br>• Profils Wi-Fi<br>• Profils VPN<br>• Profils proxy<br>• Profils de connectivité BlackBerry Dynamics<br>• Profils BlackBerry Dynamics<br>• Paramètres de configuration d'application<br>• Profils de certificat d'autorité de certification<br>• Profils des certificats partagés<br>• Récupération de certificat<br>• Profils d'informations d'identification de l'utilisateur<br>• Profils SCEP<br>• Profils CRL<br>• Profils OSCP<br>• Paramètres d'autorité de certification (Entrust et connecteur PKI uniquement)<br>• Certificats client (utilisation des applications)<br>• Toutes les politiques et tous les profils associés aux politiques et aux profils sélectionnés |
| Éléments copiés d'un serveur Good Control source vers UEM sur site uniquement | • Ensembles de stratégies<br>• Profils de connectivité<br>• Groupes d'applications<br>• Utilisation des applications (pour les certificats)<br>• Certificats |
| Migration d'un groupe | Les attributions d'utilisateurs, de rôles et de configurations logicielles ne sont pas migrées. Vous devez recréer manuellement ces attributions sur le serveur UEM de destination. |
| Mots de passe de stratégie informatique | Si une stratégie informatique source sélectionnée pour les terminaux Android présente une longueur de mot de passe minimum inférieure à 4 caractères ou supérieure à 16 caractères, aucune stratégie informatique ni aucun profil UEM ne peut être migré. Changez la stratégie informatique source en conséquence. |
| 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. |

| Élément | Considérations et bonnes pratiques |
| --- | --- |
| Profils de connectivité BlackBerry Dynamics | 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 UEM de destination. 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. |
| Groupes d'applications (Good Control sur UEM sur site uniquement) | Le groupe Tout le monde est migré mais aucun utilisateur ne lui est attribué et il n'est pas lié au groupe Tous les utilisateurs sur le serveur UEM de destination. |
| Utilisation des certificats (UEM) | L'utilisation des certificats est migrée, à l'exception des :<br>• Utilisations des certificats qui existent déjà dans le serveur de destination<br>• Applications non-BlackBerry Dynamics<br>• Applications personnalisées d'une autre organisation Good Control |
| Tâches post-migration pour les utilisateurs de BlackBerry Dynamics | Après avoir migré les utilisateurs, les terminaux, les groupes et d'autres données de Good Control vers UEM sur site ou d'un serveur sur site UEM source vers UEM Cloud, effectuez les tâches suivantes :<br>• Attribuez des configurations d'application aux applications BlackBerry Dynamics dans les groupes.<br>• Attribuez des profils de connectivité aux groupes.<br>• Attribuez des stratégies BlackBerry Dynamics migrées et des stratégies de conformité Good Control aux utilisateurs.<br>• Définissez des profils de remplacement (profils BlackBerry Dynamics et profils de conformité).<br>• Déplacez les configurations de fichier .json de Good Control à UEM.<br>• Dans les profils de connectivité migrés, spécifiez les informations des serveurs d'applications et des clusters BlackBerry Proxy. |

**Migration d'utilisateurs**

| Élément | |
| --- | --- |
| Nombre maximal d'utilisateurs | Vous pouvez migrer un maximum de 500 utilisateurs à la fois à partir d'un serveur source. Si vous sélectionnez un nombre d'utilisateurs supérieur au maximum autorisé, seul le nombre maximum est migré, tandis que le reste des utilisateurs est ignoré. Vous pouvez répéter le processus de migration selon les besoins pour migrer tous les utilisateurs depuis le serveur source. |

| Élément | |
|---|---|
| Adresse électronique | • Seuls les utilisateurs associés à une adresse e-mail peuvent être migrés.<br>• Vous ne pouvez pas migrer un utilisateur qui utilise déjà la même adresse e-mail sur le serveur UEM de destination.<br>• Si deux utilisateurs de la base de données source ont la même adresse électronique, un seul utilisateur apparait sur l'écran Migrer les utilisateurs. |
| Groupes | • Vous pouvez filtrer les utilisateurs sans attribution de groupe pour inclure cet ensemble d'utilisateurs dans une migration.<br>• 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. |
| BlackBerry UEM Self-Service | • Après la migration, l'utilisateur doit utiliser les mêmes informations de connexion qu'avant la migration pour BlackBerry UEM Self-Service.<br>• 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.<br>• 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. |

**Migration des terminaux depuis un serveur source**

| Élément | Considérations et bonnes pratiques |
|---|---|
| Valider la configuration | Il est recommandé de migrer un terminal pour chaque configuration spécifique (par exemple, différents groupes, politiques, configurations d'application, etc.) afin de s'assurer que le serveur de destination est configuré correctement avant de migrer le reste de vos terminaux. |
| Nombre maximum de terminaux | Vous pouvez simultanément migrer un maximum de 2 000 terminaux à partir d'un serveur source. |
| Utilisateurs | • Les utilisateurs du terminal doivent exister dans le domaine UEM de destination.<br>• Vous devez migrer tous les terminaux d'un utilisateur en même temps. |

| Élément | Considérations et bonnes pratiques |
| --- | --- |
| Terminaux iOS gérés d'une source UEM | • La dernière version de UEM Client doit être installée sur les terminaux.<br>• Les terminaux auxquels est attribué un profil de verrouillage des applications ne peuvent pas être migrés, car UEM Client ne peut pas être ouvert à la migration.<br>• La migration des terminaux DEP  Apple n'est pas prise en charge. Les terminaux DEP doivent être réinitialisés aux paramètres d'usine et réactivés sur la nouvelle instance UEM. Pour plus d'informations, consultez l'article KB 100525.<br>• Les terminaux d'inscription des utilisateurs ne peuvent pas être migrés.<br>• 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**. Si vous tentez d'effectuer la migration sans effectuer cette étape, l'application est supprimée et le terminal peut être désinscrit de UEM. |
| Terminaux Android gérés d'une source UEM | • La dernière version de UEM Client doit être installée sur les terminaux Android Enterprise.<br>• Vous ne pouvez pas migrer des terminaux Android qui utilisent un profil professionnel à l'aide d'un compte Google ou d'un domaine Google. |
| Terminaux Chrome OS | Vous pouvez migrer des terminaux Chrome OS à partir d'un serveur source UEM. |
| Terminaux non pris en charge pour la migration | • Windows<br>• macOS |
| Groupe de terminaux partagés | 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 et bonnes pratiques |
| --- | --- |
| Terminaux compatibles avec BlackBerry Dynamics | • 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.<br>• La migration de BlackBerry Access for Windows, de BlackBerry Access for macOS et de BlackBerry BRIDGE n'est pas prise en charge. Une fois la migration terminée, les utilisateurs doivent réinscrire ces applications.<br>• Le processus de migration ne permet pas de suivre ou de garantir la migration de UEM Client et des applications activées sur un terminal après la mise en cache des données de ce terminal. Il est recommandé d'actualiser le cache utilisateur avant chaque migration.<br>• Les terminaux compatibles avec BlackBerry Dynamics sont toujours inscrits pour BlackBerry Dynamics sur le serveur de destination.<br>• Pour les migrations effectuées à partir d'une instance de Good Control (autonome), les inscriptions Good Dynamics MDM ne sont pas migrées.<br>• Si un utilisateur a plus d'un terminal avec des applications BlackBerry Dynamics, tous les terminaux sont automatiquement sélectionnés pour la migration.<br>• Si un utilisateur oublie le mot de passe associé à 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 le serveur source UEM. Une fois la migration terminée, la clé doit être obtenue à partir du serveur UEM de destination.<br>• 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. |

# Connexion à un serveur source

Pour migrer des données, vous devez vous connecter BlackBerry UEM au serveur source. Vous ne pouvez avoir qu'un seul serveur source actif à la fois.

**Avant de commencer :**

- Passez en revue les conditions préalables à la migration et les bonnes pratiques et considérations.
- Dans les environnements sur site UEM, vérifiez que le compte de base de données associé à vos informations d'identification de connexion dispose d'autorisations d'écriture.
- Dans les environnements UEM Cloud, si plusieurs instances de BlackBerry Connectivity Node sont activées, configurez toutes les instances de BlackBerry Connectivity Node pour qu'elles se connectent à la même base de données source.

Suivez les étapes correspondant à votre type d'environnement UEM :

| Environnement | Étapes |
| --- | --- |
| UEM sur site | **a.** Dans la barre de menus de la console de gestion, cliquez sur **Paramètres > Migration > Configuration**.<br>**b.** Cliquez sur +.<br>**c.** Dans la liste déroulante **Type de source**, cliquez sur le type de serveur source approprié.<br>**d.** Spécifiez les informations du serveur source.<br>Si vous migrez des données à partir d'un serveur Good Control source, il vous suffit d'exporter et de télécharger le certificat si celui-ci n'a pas été remplacé par un certificat tiers. UEM approuve les certificats de fournisseurs tiers de manière inhérente.<br>**e.** Cliquez sur **Tester la connexion**.<br>**f.** Cliquez sur **Enregistrer**. |
| UEM Cloud | **a.** Sur la console de gestion de BlackBerry Connectivity Node, cliquez sur **Paramètres généraux > Migration** dans la barre de menus.<br>**b.** Cliquez sur +.<br>**c.** Spécifiez les informations du serveur source.<br>• Pour le champ **Serveur de base de données**, utilisez le format *<host>\<instance>* pour un port dynamique et le format *<host>:<port>* pour un port statique.<br>• Si vous sélectionnez l'authentification Windows NT, redéfinissez les propriétés de connexion du service BlackBerry UEM - BlackBerry Cloud Connector sur le même compte que celui utilisé pour installer le serveur source. Une fois la migration terminée, redéfinissez à nouveau les propriétés de connexion sur le compte système local.<br>**d.** Cliquez sur **Enregistrer**.<br>**e.** Dans la console de gestion de UEM, cliquez sur **Paramètres > Migration > Configuration**.<br>**f.** Cliquez sur +.<br>**g.** Entrez le nom de la base de données source.<br>**h.** Cliquez sur **Tester la connexion**.<br>**i.** Cliquez sur **Enregistrer**. |

**À la fin :** Effectuez l'une des opérations suivantes :

- Migrer des stratégies informatiques, des profils et des groupes depuis un serveur source.
- Migrer des utilisateurs depuis un serveur source.
- Migrer des terminaux depuis un serveur source.

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

**Avant de commencer :** Connexion à un serveur source.

1. Dans la barre de menus de la console de gestion, cliquez sur **Paramètres > Migration**.

Si vous avez configuré plusieurs serveurs sources dans un environnement sur site UEM, sélectionnez le serveur source à partir duquel vous souhaitez migrer les données.

2. Cliquez sur **Stratégies informatiques, profils, groupes**.
3. Cliquez sur **Suivant**.
4. Sélectionnez les éléments que vous souhaitez migrer.

   Le nom du serveur source est ajouté au nom de chaque stratégie et profil lors de la migration vers la destination.
5. Cliquez sur **Aperçu**.
6. Cliquez sur **Migrer**.

**À la fin :**

- Pour configurer les stratégies informatiques, les profils et les groupes, cliquez sur **Configurer les stratégies informatiques et profils** afin d'accéder à l'écran **Stratégies informatiques et profils**.
- 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.
- Migrer des utilisateurs depuis un serveur source.

# Migrer des utilisateurs depuis un serveur source

**Avant de commencer :**

- Connexion à un serveur source.
- Migrer des stratégies informatiques, des profils et des groupes depuis un serveur source.

1. Dans la barre de menus de la console de gestion, cliquez sur **Paramètres > Migration > Utilisateurs**.
2. Cliquez sur **Actualiser le cache**.

   L'actualisation prend environ 10 minutes pour 1 000 utilisateurs. L'actualisation du cache n'est obligatoire que pour le premier ensemble d'utilisateurs à migrer. Si vous apportez des modifications au serveur source lors de la migration, il est recommandé de réactualiser le cache.
3. Cliquez sur **Suivant**.
4. Sélectionnez les utilisateurs que vous souhaitez migrer.

   Par défaut, seuls les 20 000 premiers utilisateurs sont affichés. Vous pouvez rechercher des utilisateurs spécifiques selon vos besoins. Notez que le fait de sélectionner tous les utilisateurs ne sélectionne que ceux affichés sur la première page.
5. Cliquez sur **Suivant**.
6. Attribuez une stratégie informatique, des groupes et des profils aux utilisateurs sélectionnés.
7. Cliquez sur **Aperçu**.
8. Cliquez sur **Migrer**.

Notez que les comptes d'utilisateur migrés ne sont pas supprimés du serveur source.

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

# Migrer des terminaux depuis un serveur source

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

**Avant de commencer :**

- Connexion à un serveur source.
- Migrer des stratégies informatiques, des profils et des groupes depuis un serveur source.
- Migrer des utilisateurs depuis un serveur source.
- Informez les utilisateurs de terminaux iOS qu'ils doivent ouvrir BlackBerry UEM Client et le laisser ouvert jusqu'à ce que la migration soit terminée.

1. Dans la barre de menus de la console de gestion, cliquez sur **Paramètres > Migration > Terminaux** dans la barre de menus.
2. Cliquez sur **Actualiser le cache**.

   L'actualisation prend environ 10 minutes pour 1 000 terminaux. L'actualisation du cache n'est obligatoire que pour le premier ensemble de terminaux à migrer. Si vous apportez des modifications au serveur source lors de la migration, il est recommandé de réactualiser le cache.
3. Cliquez sur **Suivant**.
4. Sélectionnez les terminaux que vous souhaitez migrer.

   Par défaut, seuls les 20 000 premiers terminaux sont affichés. Vous pouvez rechercher des terminaux spécifiques selon vos besoins. Notez que le fait de sélectionner tous les terminaux ne sélectionne que ceux affichés sur la première page.
5. Cliquez sur **Aperçu**.
6. Cliquez sur **Migrer**.
7. Cliquez sur **Migration** > **État**.

**À la fin :** Pour afficher l'état des terminaux en cours de migration, cliquez sur **Migration > État**.

# Configuration de la communication réseau et des propriétés des applications BlackBerry Dynamics

Suivez les instructions de cette section afin de configurer la communication réseau et d'autres propriétés pour les applications BlackBerry Dynamics.

| Tâche | Description |
| --- | --- |
| Gérer les clusters BlackBerry Proxy. | Créez et gérez des clusters BlackBerry Proxy qui acheminent les données pour les applications BlackBerry Dynamics. |
| Configurer Direct Connect à l'aide de la redirection de port. | Configurez Direct Connect pour des instances BlackBerry Proxy. |
| Configurer les propriétés BlackBerry Dynamics (Sur site uniquement) | Configurez les propriétés des applications BlackBerry Dynamics que vous prévoyez de déployer dans l'environnement de votre organisation. |
| Configurer les paramètres de communication pour les applications BlackBerry Dynamics (Sur site uniquement) | Configurez les paramètres de communication des applications BlackBerry Dynamics que vous prévoyez de déployer dans l'environnement de votre entreprise, y compris le protocole de communication qu'elles utiliseront. |
| Envoi de données d'application BlackBerry Dynamics via un proxy HTTP. | Configurez UEM pour envoyer les données d'application BlackBerry Dynamics via un proxy HTTP entre BlackBerry Proxy et un serveur d'application. |
| Méthodes de routage du trafic des applications BlackBerry Dynamics. | Détails des différentes méthodes que vous pouvez utiliser pour acheminer le trafic des applications BlackBerry Dynamics |
| Configuration de l'authentification Kerberos pour les applications BlackBerry Dynamics (Sur site uniquement) | Configurez la délégation contrainte Kerberos ou Kerberos PKINIT pour simplifier l'authentification des utilisateurs. |

Pour plus d'informations sur le déploiement et la gestion des applications BlackBerry Dynamics, reportez-vous à la section Gestion des applications BlackBerry Dynamics dans le contenu relatif à l'administration.

## Gérer les clusters BlackBerry Proxy

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

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

| Tâche | Étapes |
| --- | --- |
| Créez un nouveau cluster BlackBerry Proxy. | **a.** Cliquez sur +.<br>**b.** Saisissez un nom pour le cluster.<br>**c.** Cliquez sur **Enregistrer**. |
| Renommez un cluster BlackBerry Proxy. | **a.** Cliquez sur le nom d'un cluster.<br>**b.** Modifiez le nom du cluster. Chaque cluster doit avoir un nom unique.<br>**c.** Cliquez sur **OK**. |
| 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.<br>**b.** Dans la liste déroulante **Cluster BlackBerry Proxy**, sélectionnez le cluster auquel vous souhaitez ajouter l'instance.<br>**c.** Cliquez sur **Enregistrer**. |
| Supprimez un cluster BlackBerry Proxy vide. | **a.** Cliquez sur × pour ce cluster.<br>**b.** Cliquez sur **Supprimer**. |
| Définissez les paramètres proxy d'application d'un cluster. | **a.** Cliquez sur le nom du cluster.<br>**b.** Cliquez sur **Remplacer les paramètres globaux**.<br>**c.** Reportez-vous à la section Configurer les paramètres proxy de l'application BlackBerry Dynamics. |
| 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.<br>**b.** Sur la barre de menus, cliquez sur **Paramètres > Intégration externe > Certificats approuvés**.<br>**c.** Cliquez sur + en regard de **Éléments approuvés du serveur PAC**.<br>**d.** Cliquez sur **Parcourir**.<br>**e.** Accédez au fichier de certificat à utiliser et sélectionnez-le.<br>**f.** Cliquez sur **Ouvrir**.<br>**g.** Saisissez la description du certificat.<br>**h.** Cliquez sur **Ajouter**. |
| Permettez à un BlackBerry Proxy d'être utilisé pour l'activation (UEM sur site uniquement). | Sélectionnez l'option **Activé pour l'activation** pour l'instance BlackBerry Proxy que vous souhaitez utiliser à des fins d'activation. Vous devez sélectionner au moins une instance. |

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

**Avant de commencer :**

- Configurez une entrée DNS publique pour chaque serveur BlackBerry Connectivity Node (par exemple, bp01.mydomain.com, bp02.mydomain.com, etc.).
- Configurez le pare-feu externe pour autoriser les connexions entrantes sur le port 17533 et 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 barre de menus de la console de gestion, cliquez sur **Paramètres > BlackBerry Dynamics > Direct Connect**.
2. Cliquez sur une instance de BlackBerry Proxy.
3. 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.
4. Répétez les étapes pour toutes les instances 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 Gérer les clusters BlackBerry Proxy.
5. Cliquez sur **Enregistrer**.

# Configurer les propriétés BlackBerry Dynamics

Dans un environnement sur site UEM, vous pouvez configurer diverses propriétés liées à la sécurité, au comportement et aux communications des applications BlackBerry Dynamics.

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

| Tâche | Étapes |
|---|---|
| Modifiez les propriétés globales des applications BlackBerry Dynamics. | • Cliquez sur **Propriétés globales**.<br>• Si nécessaire, configurez les propriétés. Reportez-vous à la section Propriétés globales de BlackBerry Dynamics.<br>• Cliquez sur **Enregistrer**. |
| Modifiez les propriétés BlackBerry Dynamics d'un serveur UEM spécifique. | • Cliquez sur **Propriétés**.<br>• Dans la liste déroulante **Type de serveur**, cliquez sur **Serveurs BlackBerry** et sélectionnez le serveur UEM que vous souhaitez configurer.<br>• Si nécessaire, configurez les propriétés. Reportez-vous à la section Propriétés de BlackBerry Dynamics.<br>• Cliquez sur **Enregistrer**. |

| Tâche | Étapes |
| --- | --- |
| Modifiez les propriétés d'une instance BlackBerry Proxy. | • Cliquez sur **Propriétés**.<br>• Dans la liste déroulante **Type de serveur**, cliquez sur **Serveurs BlackBerry Proxy** et sélectionnez le serveur BlackBerry Proxy que vous souhaitez configurer.<br>• Si nécessaire, configurez les propriétés. Reportez-vous à la section Propriétés de BlackBerry Proxy.<br>• Cliquez sur **Enregistrer**. |

## Propriétés globales de BlackBerry Dynamics

Les tableaux suivants décrivent les propriétés globales de BlackBerry Dynamics que vous pouvez configurer. La colonne Redémarrer indique si la modification de la propriété nécessite un redémarrage de BlackBerry UEM.

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

### Certificate Management

| Propriété | Description | Par défaut | Redémarrer |
| --- | --- | --- | --- |
| Valeur TTL en secondes du magasin pour les certificats PKCS 12 des utilisateurs finaux individuels | Durée de vie, en secondes, du magasin de certificats pour les certificats PKCS 12 pendant laquelle les utilisateurs de terminaux peuvent effectuer un téléchargement pour signer des e-mails et à des fins d'authentification du client.<br>Cette propriété est en lecture seule et ne peut pas être modifiée. | 86 400 | — |

### Communication

| Propriété | Description | Par défaut | Redémarrer |
| --- | --- | --- | --- |
| cntmgmt.internal.port | Le port interne pour le service de gestion des conteneurs. | 17317 | Oui |
| cntmgmt.max.conns.above.limit | Nombre maximum de connexions autorisées au-delà de la limite définie par la propriété cntmgmt.max.conns.persec.<br>**Remarque :** Ne modifiez pas ce paramètre sans avoir consulté l'assistance technique BlackBerry. | 3 | Oui |

| Propriété | Description | Par défaut | Redémarrer |
|---|---|---|---|
| cntmgmt.max.conns.persec | Nombre maximum de connexions par seconde pour la gestion des conteneurs.<br>**Remarque :** Ne modifiez pas ce paramètre sans avoir consulté l'assistance technique BlackBerry. | 30 | Oui |
| cntmgmt.max.active.sessions | Nombre maximum de sessions actives pour la gestion des conteneurs. | 10 000 | Oui |
| cntmgmt.max.idle.count | Nombre maximum de connexions inactives autorisé pour la gestion des conteneurs.<br>**Remarque :** Ne modifiez pas ce paramètre sans avoir consulté l'assistance technique BlackBerry. | 0 | Oui |
| cntmgmt.max.read.throughput | Nombre maximum d'opérations de lecture concurrentes pour la gestion des conteneurs.<br>**Remarque :** Ne modifiez pas ce paramètre sans avoir consulté l'assistance technique BlackBerry. | 500 | Oui |
| cntmgmt.max.write.throughput | Nombre maximum d'opérations d'écriture concurrentes pour la gestion des conteneurs.<br>**Remarque :** Ne modifiez pas ce paramètre sans avoir consulté l'assistance technique BlackBerry. | 500 | Oui |
| cntmgmt.ssl.external.enable | Détermine si SSL est activé pour la gestion des conteneurs externes.<br>Cette propriété est en lecture seule et ne peut pas être modifiée. | I | — |
| cntmgmt.ssl.internal.enable | Détermine si SSL est activé pour la gestion des conteneurs internes.<br>Cette propriété est en lecture seule et ne peut pas être modifiée. | I | — |

#### Conteneurs en double

Si UEM identifie des conteneurs en double sur les terminaux, il planifie un traitement par lots pour les supprimer. Un conteneur en double a les mêmes ID d'utilisateur et ID d'autorisation (également appelé ID d'application BlackBerry Dynamics) qu'un autre conteneur sur le même terminal. Lorsqu'un conteneur en double est supprimé, il est consigné dans le fichier journal UEM.

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

**Délégation contrainte Kerberos**

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

**Divers**

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

**Vider les conteneurs inactifs**

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

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

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

#### Rapports

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

#### Stratégie de rétention des données

| Propriété | Description | Par défaut | Redémarrer |
|---|---|---|---|
| gc.purge.dbJobs Vider les tâches du serveur | Spécifiez si UEM vide automatiquement les tâches du serveur à un intervalle régulier. | I | Oui |
| gc.purge.dbJobs.interval Intervalle de vidage des tâches du serveur | Si l'option « Vider les tâches du serveur » est activée, fréquence, en jours, à laquelle UEM vide les tâches du serveur. | 30 | Oui |

### Propriétés de BlackBerry Dynamics

#### Délégation contrainte Kerberos

| Propriété | Description | Par défaut | Redémarrer |
|---|---|---|---|
| Emplacement du fichier krb5.conf sur le serveur GC (gc.krb5.config.file) | L'emplacement du fichier krb5.conf est requis pour configurer KCD et activer l'authentification multidomaine lorsqu'il existe une relation de confiance CAPATH avec plusieurs domaines Kerberos. | Non défini | Oui |
| Activer le mode de débogage KCD (gc.krb5.debug) | Détermine si UEM consigne les données du niveau de débogage. | O | Oui |
| Nom entièrement qualifié pour le KCD (gc.krb5.kdc) | Nom de domaine complet du serveur qui héberge le service KDC (Key Distribution Center) Kerberos. | Non défini | Oui |
| Emplacement du fichier keytab (gc.krb5.keytab.file) | Emplacement du fichier keytab Kerberos sur l'ordinateur qui héberge BlackBerry UEM. | Non défini | Oui |

| Propriété | Description | Par défaut | Redémarrer |
|---|---|---|---|
| Nom du compte de service dans lequel le service KCD est en cours d'exécution (gc.krb5.principal.name) | Nom d'utilisateur du compte Kerberos. N'incluez pas le domaine. | Non défini | Oui |
| Domaine - Active Directory (gc.krb5.realm) | Domaine du compte Kerberos. | Non défini | Oui |

### Propriétés de BlackBerry Proxy

Le tableau suivant décrit les propriétés que vous pouvez configurer pour chacune des instances de BlackBerry Proxy de votre organisation.

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

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

# Configurer les paramètres de communication pour les applications BlackBerry Dynamics

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

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

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

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

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

### Considérations relatives à l'utilisation d'un fichier PAC avec BlackBerry Proxy

| Considérations | Détails |
|---|---|
| Directives sur les fichiers PAC pris en charge | • DIRECT<br>• PROXY (traité comme proxy HTTPS ; connexion établie à l'aide de HTTP CONNECT)<br>• HTTPS (connexion établie à l'aide de HTTP CONNECT) |
| Directives sur les fichiers PAC non pris en charge | Une erreur de connexion se produit pour les éléments suivants :<br>• SOCKS<br>• SOCKS4<br>• SOCKS5<br>• HTTP<br>• Directive « NATIVE » personnalisée définie par BlackBerry Access<br>Les directives sur les fichiers BLOCK sont traitées comme directives DIRECT. |

| Considérations | Détails |
|---|---|
| Limites | • La fonction dnsDomainIs ne peut pas contenir les caractères « _ » et « * ».<br>• La fonction shExpMatch ne peut pas inclure les expressions « [0-9] », « ? », « /^d » ou « d+ »<br>• L'option permettant de supprimer le chemin et la requête de l'URI n'est pas prise en charge. |
| Cache PAC | 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.<br>Si vous souhaitez mettre à jour le cache manuellement, dans la console de gestion, accédez à Paramètres > Infrastructure > BlackBerry Router et proxy > Paramètres globaux et cliquez sur Mettre à jour le cache PAC. |

## Configurer les paramètres proxy de l'application BlackBerry Dynamics

1. Suivez les étapes correspondant à votre environnement UEM :

| Environnement | Tâche |
|---|---|
| UEM sur site | Effectuez l'une des tâches suivantes dans la console de gestion de UEM :<br>• Si vous souhaitez définir les paramètres proxy globaux d'application, cliquez sur **Paramètres > Infrastructure > BlackBerry Router et proxy** et développez **Paramètres globaux**.<br>• Si vous souhaitez définir les paramètres proxy d'application pour un cluster, cliquez sur **Paramètres > BlackBerry Dynamics > clusters**. Cliquez sur le nom d'un cluster et cochez la case **Remplacer les paramètres globaux**.<br>• Si vous souhaitez définir manuellement les paramètres proxy d'application pour un serveur, cliquez sur **Paramètres > Infrastructure > BlackBerry Router et proxy**. Développez un serveur et cochez la case **Remplacer les paramètres globaux**. Notez que les fichiers PAC ne sont pas pris en charge lors du remplacement des paramètres proxy globaux d'un serveur. |
| UEM Cloud | Dans la console de gestion de BlackBerry Connectivity Node, cliquez sur **Paramètres généraux > BlackBerry Router et proxy > Paramètres globaux**. |

2. Sélectionnez l'option appropriée et suivez les étapes requises :

| Option | Étapes |
|---|---|
| Activer le proxy HTTP manuel | **a.** Sélectionnez la configuration de proxy appropriée. Si vous souhaitez utiliser un proxy pour vous connecter à des serveurs spécifiés, cliquez sur + afin d'ajouter des serveurs.<br>**b.** Spécifiez l'adresse du serveur proxy et le numéro de port sur lequel il écoute.<br>**c.** Si le serveur proxy nécessite une authentification, cochez la case **Utiliser l'authentification** et spécifiez les informations d'authentification. |

| Option | Étapes |
| --- | --- |
| Activer PAC | Dans le champ **URL du fichier PAC**, saisissez l'URL du fichier PAC.<br>Si les proxys spécifiés dans le fichier PAC nécessitent une authentification, cochez la case **Prendre en charge l'authentification proxy** et spécifiez les informations d'authentification. Les informations d'authentification de l'utilisateur final ne sont pas prises en charge pour l'authentification proxy. |

3. Cliquez sur **Enregistrer**.

# Méthodes de routage du trafic des applications BlackBerry Dynamics

BlackBerry UEM propose plusieurs options qui vous permettent de contrôler le routage du trafic de BlackBerry Dynamics. Par défaut, tout le trafic des applications BlackBerry Dynamics est acheminé directement vers Internet, sans configuration de serveur proxy Web. Cette section ne traite que des configurations qui affectent le routage global.

Le routage des applications BlackBerry Dynamics peut être modifié par les configurations suivantes :

| Configuration | Détails |
| --- | --- |
| Profil de connectivité BlackBerry Dynamics attribué | • Le seul élément configuré dans le profil de connectivité BlackBerry Dynamics par défaut est le Type de chemin de domaine autorisé par défaut, qui est défini sur Direct.<br>• Avec le profil de connectivité BlackBerry Dynamics par défaut, aucun serveur ou domaine interne n'est accessible aux applications BlackBerry Dynamics. Vous pouvez changer le profil de connectivité par défaut ou en créer un nouveau pour permettre la connectivité aux serveurs internes.<br>• Pour plus d'informations, reportez-vous à la section Créer un profil de connectivité BlackBerry Dynamics dans le contenu relatif à l'administration. |

| Configuration | Détails |
| --- | --- |
| Configuration du serveur Web proxy BlackBerry Proxy | • Par défaut, BlackBerry Proxy n'est pas configuré pour utiliser un serveur proxy Web. Dans cette configuration, chaque serveur BlackBerry Proxy tente de se connecter directement à Internet pour établir des connexions. Cela s'applique à la fois au trafic du serveur d'applications et aux connexions BlackBerry Dynamics NOC.<br>• Pour plus d'informations sur la configuration de BlackBerry Proxy, reportez-vous à la section Envoi de données d'application BlackBerry Dynamics via un proxy HTTP.<br>• Dans le profil de connectivité BlackBerry Dynamics, vous pouvez spécifier les serveurs auxquels les applications BlackBerry Dynamics sont autorisées à accéder via le pare-feu à l'aide de BlackBerry Proxy. Pour plus d'informations, reportez-vous à la section Créer un profil de connectivité BlackBerry Dynamics dans le contenu relatif à l'administration.<br>• Le routage du trafic via BlackBerry Proxy permet aux navigateurs Web et aux applications BlackBerry Dynamics des terminaux de se connecter à n'importe quel serveur derrière le pare-feu accessible par BlackBerry Proxy, et vous permet de surveiller facilement le trafic de données entre les applications BlackBerry Dynamics et les ressources de votre organisation.<br>• Tenez compte des points suivants lorsque vous choisissez d'acheminer des données via un serveur BlackBerry Proxy :<br>  • L'établissement de connexions à des serveurs sur Internet peut prendre plus longtemps.<br>  • Si vous utilisez un proxy Web pour permettre l'accès à des sites externes et que vous avez configuré les paramètres de votre proxy pour limiter l'accès à certains sites, vous devez également définir les propriétés du proxy dans BlackBerry Proxy lorsque vous sélectionnez l'option Acheminer tout le trafic. Sinon, les applications ne pourront pas accéder aux sites externes.<br>  • BlackBerry Access peut être configuré avec un fichier PAC qui détermine les sites autorisés. Dans ce cas, le fichier PAC détermine les paramètres de proxy. Pour plus d'informations, reportez-vous au Guide d'administration de BlackBerry Access. |
| Paramètres spécifiques à l'application | • Une configuration spécifique à l'application peut être nécessaire pour que les applications se connectent à des serveurs spécifiques (par exemple, pour BlackBerry Work configuré avec l'URL du Microsoft Exchange Server). Consultez la documentation des applications BlackBerry Dynamics pour connaitre les configurations à appliquer.<br>• BlackBerry Access et certaines applications tierces permettent des configurations de serveur proxy Web au niveau des applications. Aucune configuration de serveur proxy Web n'est appliquée à la configuration par défaut de BlackBerry Access.<br>• Un serveur d'applications est un serveur auquel une application BlackBerry Dynamics se connecte ; par exemple, l'URL d'un Microsoft Exchange Server, l'URL de BEMS, l'URL de Skype for Business ou toute URL qui accède à BlackBerry Access. BlackBerry Dynamics NOC et le serveur BlackBerry UEM Core ne sont pas des serveurs d'applications. |

Si vous configurez et attribuez un profil de connectivité BlackBerry Dynamics et une configuration de proxy Web pour les serveurs BlackBerry Proxy, le profil de connectivité BlackBerry Dynamics est toujours vérifié en premier. Lorsque le trafic arrive au serveur BlackBerry Proxy, la connectivité de la configuration du proxy Web ou du PAC définie sur le serveur BlackBerry Proxy est évaluée. La configuration d'un proxy Web sur le serveur BlackBerry Proxy détermine comment ce BlackBerry Proxy gère l'envoi du trafic vers Internet, et n'affecte pas la manière dont l'application BlackBerry Dynamics sur le terminal évalue les connexions.

## Exemples de scénarios de routage du trafic BlackBerry Dynamics

Les scénarios suivants sont des exemples de configurations courantes :

| Scénario | Profil de connectivité BlackBerry Dynamics | Configuration de proxy Web pour BlackBerry Proxy | Paramètres spécifiques à l'application |
|---|---|---|---|
| Acheminez le trafic vers des serveurs ou des domaines spécifiques via BlackBerry Proxy.<br>Convient aux scénarios où certains serveurs d'applications internes doivent être accessibles aux applications BlackBerry Dynamics, mais où le trafic général vers les serveurs publics peut rester direct. | • Type de chemin de domaine autorisé par défaut : direct<br>• Domaines autorisés : ajoutez les domaines internes que vous souhaitez acheminer via le système BlackBerry Proxy et sélectionnez un cluster.<br>• Serveurs supplémentaires : si nécessaire, ajoutez des noms de serveurs spécifiques et sélectionnez un cluster. | Aucune configuration nécessaire. | Aucune configuration nécessaire. |
| Acheminez tout le trafic via BlackBerry Proxy, puis via un serveur proxy Web.<br>Convient aux organisations qui exigent que tout le trafic des applications professionnelles soit acheminé en interne. | Type de chemin de domaine autorisé par défaut : cluster de BlackBerry Proxy | Utilisez une configuration manuelle du serveur proxy Web ou un fichier PAC. | Aucune configuration nécessaire. |

| Scénario | Profil de connectivité BlackBerry Dynamics | Configuration de proxy Web pour BlackBerry Proxy | Paramètres spécifiques à l'application |
|---|---|---|---|
| Acheminez une partie du trafic en interne pour la plupart des applications, mais configurez un serveur proxy spécifiquement pour la navigation Web via BlackBerry Access.<br>Convient aux organisations qui exigent que le trafic des applications soit acheminé en interne, mais qui exigent que le trafic du navigateur soit acheminé via un serveur proxy Web. | • Type de chemin de domaine autorisé par défaut : direct<br>• Domaines autorisés : ajoutez les domaines internes que vous souhaitez acheminer via le système BlackBerry Proxy et sélectionnez un cluster.<br>• Serveurs supplémentaires : si nécessaire, ajoutez des noms de serveurs spécifiques et sélectionnez un cluster. | Si les serveurs BlackBerry Proxy ne disposent pas d'un accès direct à Internet ou si un proxy est requis pour les connexions BlackBerry Dynamics NOC, configurez un serveur proxy Web selon vos besoins. | Dans la configuration de l'application pour BlackBerry Access, sélectionnez Enable Web Proxy et Use Proxy Auto Configuration. |

# Configuration de l'authentification Kerberos pour les applications BlackBerry Dynamics

Dans un environnement sur site BlackBerry UEM, les applications BlackBerry Dynamics prennent en charge la délégation contrainte (KCD) Kerberos et Kerberos PKINIT. Vous pouvez prendre en charge KCD ou Kerberos PKINIT pour les applications BlackBerry Dynamics, mais pas les deux.

| Authentification Kerberos | Description |
|---|---|
| KCD | La KCD permet aux utilisateurs d'accéder aux ressources de l'entreprise sans avoir à entrer leurs informations d'identification réseau. La KCD utilise des tickets de service qui sont cryptés et décryptés par des clés ne contenant pas les informations d'identification de l'utilisateur.<br><br>Lorsque la KCD est configurée, l'application BlackBerry Dynamics délègue l'authentification à UEM, qui demande l'accès à une ressource professionnelle en son nom. Vous pouvez limiter les ressources réseau accessibles aux utilisateurs en configurant le compte que UEM utilise de sorte qu'il ne soit approuvé que pour des services spécifiques.<br><br>Par exemple, si la KCD n'est pas configurée et qu'une application demande une ressource telle que mypage.mydomain.com, l'application demande des informations d'identification à l'utilisateur. Lorsque la KCD est configurée, l'infrastructure BlackBerry Dynamics gère l'authentification et l'utilisateur n'est pas invité à saisir les informations d'identification.<br><br>Reportez-vous aux sections Configuration requise pour configuration de KCD pour les applications BlackBerry Dynamics et Configuration de KCD pour les applications BlackBerry Dynamics. |
| Kerberos PKINIT | L'authentification Kerberos PKINIT établit la confiance directement entre l'application BlackBerry Dynamics et la KDC Windows. L'authentification de l'utilisateur est basée sur les certificats délivrés par les services de certificats Microsoft Active Directory.<br><br>Reportez-vous à la section Configuration requise pour la prise en charge de Kerberos PKINIT pour les applications BlackBerry Dynamics. |

### Configuration requise pour configuration de KCD pour les applications BlackBerry Dynamics

| Élément | Description |
|---|---|
| Port Active Directory | Le port 88 du service Active Directory doit être accessible par tous les serveurs UEM . |
| Environnement Kerberos | L'environnement Kerberos doit inclure les composants suivants :<br>• Serveur Microsoft Active Directory : service du répertoire qui authentifie et autorise tous les utilisateurs et ordinateurs associés à votre réseau Windows<br>• Centre de distribution de clés (KDC)Kerberos : service d'authentification sur le serveur Active Directory qui fournit des tickets de session et des clés aux utilisateurs et ordinateurs du domaine Active Directory<br>• Pour utiliser KCD avec des ressources Microsoft 365, le domaine Active Directory sur site doit être intégré à Entra. Pour plus d'informations, consultez l'article Microsoft « Intégrer AD sur site avec Entra ». |

| Élément | Description |
| --- | --- |
| fichier krb5.conf | Votre environnement UEM nécessite un fichier krb5.conf avec des valeurs spécifiques à votre KDC. Il doit inclure les paramètres minimaux suivants :<br>Chiffrement RC4 :<br>`[libdefaults]`<br>`allow_weak_crypto = true`<br>`forwardable = true`<br>Fichier Keytab AES :<br>`[libdefaults]`<br>`forwardable = true`<br>En cas d'utilisation d'un fichier Keytab AES, vous devez créer le fichier avec un indicateur AES `/crypto AES256-SHA1` :<br>`ktpass /out outfilename.keytab /mapuser kerberos_account@REALM_IN_ALL_CAPS /princ kerberos_account@REALM_IN_ALL_CAPS /pass kerberos_account_password /ptype KRB5_NT_PRINCIPAL / crypto AES256-SHA1`<br>Vous devez spécifier l'emplacement du fichier krb5.conf dans Paramètres > BlackBerry Dynamics > Propriétés (voir Configuration de KCD pour les applications BlackBerry Dynamics). Pour plus d'informations sur la construction d'un fichier krb5.conf, consultez la documentation MIT Kerberos. |
| Noms principaux de service (SPN) | Créez des SPN pour tous les services HTTP, y compris BlackBerry Enterprise Mobility Server. Vous devez définir un SPN pour chaque ressource cible à laquelle vous souhaitez que les terminaux aient accès.<br>Pour plus d'informations sur la création et la modification de SPN, reportez-vous à la section Inscrire un nom principal de service pour les connexions Kerberos. |

| Élément | Description |
| --- | --- |
| Environnements Kerberos multidomaine : | • Au moins un serveur UEM Core doit être installé dans chaque domaine Kerberos. UEM doit résider dans le même domaine Kerberos que la ressource car la délégation de ressources inter-domaines n'est pas prise en charge.<br>• Assurez-vous que le KCD à domaine unique fonctionne avant de configurer le KCD multidomaine.<br>• Toutes les relations approuvées doivent correspondre à des approbations de forêts transitives bidirectionnelles.<br>• Assurez-vous de maintenir une latence maximale de 5 ms entre les instances UEM Core et la base de données Microsoft SQL Server.<br><br>**Remarque :** Si vous effectuez une mise à niveau depuis UEM version 12.19 ou antérieure vers UEM version 12.20 ou ultérieure, procédez comme suit :<br><br>1. Générez un nouveau fichier keytab Kerberos et copiez-le sur chaque serveur UEM (voir l'étape 2 de Configuration de KCD pour les applications BlackBerry Dynamics).<br>2. Dans Paramètres > BlackBerry Dynamics > Propriétés, dans le Nom du compte de service sous lequel le service KCD est exécuté (gc.krb5.principal.name), spécifiez les éléments suivants :<br><br>`GCSvc/<UEM_Core_host_machine>` |

## Configuration de KCD pour les applications BlackBerry Dynamics

**Avant de commencer :**

- Examinez les Configuration requise pour configuration de KCD pour les applications BlackBerry Dynamics.
- Si vous configurez la KCD pour BlackBerry Docs, reportez-vous à la section Configuration de la délégation contrainte Kerberos pour le service Docs dans le contenu BlackBerry Enterprise Mobility Server.

1. Pour mapper le compte de service Kerberos sur un SPN, sur le serveur Active Directory, ouvrez l'invite de commande en tant qu'administrateur et saisissez ce qui suit, en spécifiant le nom, le domaine et le compte de service Kerberos du serveur hôte. Le compte de service Kerberos est le nom du compte de service sous lequel le service KCD sera configuré dans UEM (gc.krb5.principal.name). Ce compte n'a pas besoin d'être identique au compte de service UEM, mais peut l'être.

   ```
   setspn –s GCSvc/<UEM_Core_host_machine> <domain>\<Kerberos_service_account>
   ```

   Par exemple :

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

2. Procédez comme suit pour générer un nouveau fichier keytab Kerberos et définir le mot de passe du compte Kerberos :
   a) Sur le serveur KDC, ouvrez une invite de commande.
   b) Exécutez la commande suivante et spécifiez les valeurs appropriées :

   ```
   ktpass -out <output_filename>.keytab -mapuser
    <Kerberos_account>@<KERBEROS_REALM_IN_UPPERCASE> -princ
    <Kerberos_account>@<KERBEROS_REALM_IN_UPPERCASE> -ptype KRB5_NT_PRINCIPAL -
   pass <Kerberos_account_password>
   ```

Si votre organisation utilise un environnement multidomaine Kerberos, utilisez plutôt la commande suivante :

```
ktpass -out <output_filename>.keytab -mapuser
 <Kerberos_service_account>@<KERBEROS_REALM_IN_UPPERCASE>
 -princ GCSvc/<UEM_Core_host_machine> -princ GCSvc/
<UEM_Core_host_machine>@<KERBEROS_REALM_IN_UPPERCASE> -ptype
 KRB5_NT_PRINCIPAL -pass <Kerberos_account_password>
```

c) Copiez le nouveau fichier keytab sur chaque serveur UEM devant utiliser le même compte d'administrateur KCD.

3. Activez l'énumération des appartenances au groupe d'objets d'utilisateur Active Directory. Pour plus d'informations, reportez-vous à l' Annexe B : Comptes et groupes privilégiés dans Active Directory.
4. Sur chaque serveur UEM, procédez comme suit afin de configurer pour le compte de service UEM les autorisations lui permettant d'envoyer les informations d'identification d'utilisateur au système Kerberos (il s'agit du même compte associé au SPN) :
   a) Dans la console de gestion Microsoft, accédez à **Stratégie de sécurité locale > Stratégies locales > Attribution des droits d'utilisateur**.
   b) Ouvrez les propriétés de **Agir dans le cadre du système d'exploitation** et cliquez sur **Ajouter un utilisateur ou un groupe**.
   c) Saisissez le nom du compte de service puis cliquez sur **OK**.
5. Dans la barre de menus de la console de gestion UEM, cliquez sur **Paramètres > BlackBerry Dynamics > Propriétés globales**.
6. Cochez la case **Utiliser un UPN explicite**.
7. Cochez la case **Activer KCD**.
8. Cliquez sur **Enregistrer**.
9. Dans la barre de menus, cliquez sur **Paramètres > BlackBerry Dynamics > Propriétés** puis sur le nom du serveur.
10. Dans le champ **Nom entièrement qualifié pour le KDC (gc.krb5.kdc)**, saisissez le nom complet du KDC. Ce nom correspond généralement au FQDN d'un contrôleur de domaine Active Directory.
11. Dans le champ **Emplacement du fichier keytab (gc.krb5.keytab.file)**, saisissez l'emplacement du fichier keytab. Utilisez des barres obliques dans le nom du chemin.
12. Dans le champ **Nom du compte de service dans lequel le service KCD est en cours d'exécution (gc.krb5.principal.name)**, saisissez le nom du compte de service utilisé par le service KCD.

    Dans un environnement multidomaine Kerberos, spécifiez plutôt les éléments suivants :

    ```
    GCSvc/<UEM_Core_host_machine>
    ```

13. Dans le champ **Domaine - Active Directory (gc.krb5.realm)**, saisissez le nom du domaine Active Directory entièrement en majuscules.
14. Dans le champ **Emplacement du fichier krb5.config sur le serveur GC (gc.krb5.config.file)**, saisissez l'emplacement du fichier krb5.conf.

    Pour plus d'informations sur la configuration requise pour le fichier krb5.conf, reportez-vous à Configuration requise pour configuration de KCD pour les applications BlackBerry Dynamics.
15. Cliquez sur **Enregistrer**.

## Configuration requise pour la prise en charge de Kerberos PKINIT pour les applications BlackBerry Dynamics

BlackBerry UEM prend en charge Kerberos PKINIT pour l'authentification de l'utilisateur BlackBerry Dynamics à l'aide de certificats PKI. Si vous souhaitez utiliser Kerberos PKINIT pour les applications BlackBerry Dynamics, votre organisation doit remplir les conditions suivantes :

| Élément | Configuration requise |
| --- | --- |
| KDC | • Vous devez ajouter l'hôte KDC à la liste des domaines autorisés dans le profil de connectivité BlackBerry Dynamics attribué. Pour plus d'informations, reportez-vous à la section Créer un profil de connectivité BlackBerry Dynamics dans le contenu relatif à l'administration.<br>• L'hôte KDC doit être à l'écoute sur le port TCP 88 (port Kerberos par défaut).<br>• Le KDC doit avoir un enregistrement A (IPv4) ou AAAA (IPv6) dans votre DNS.<br>• BlackBerry Dynamics ne prend pas en charge le KDC sur UDP.<br>• BlackBerry Dynamics n'utilise pas de fichiers de configuration Kerberos (tel que krb5.conf) pour localiser le KDC approprié.<br>• Le KDC peut référer le client à un autre hôte KDC. BlackBerry Dynamics suivra l'instruction si l'hôte KDC auquel il est renvoyé a été ajouté à la liste des domaines autorisés dans le profil de connectivité BlackBerry Dynamics.<br>• Le KDC peut obtenir le TGT de façon transparente pour BlackBerry Dynamics à partir d'un autre hôte KDC.<br>• La délégation Kerberos contrainte ne doit pas être activée. |
| Certificats de serveur | • Les certificats de serveur Windows KDC émis via les services de certificats Active Directory doivent provenir exclusivement des versions suivantes de Windows Server. Aucune autre version n'est prise en charge.<br>  • Internet Information Server avec Windows Server 2008 R2<br>  • Internet Information Server avec Windows Server 2012 R2<br>• Des certificats de service KDC valides doivent se trouver dans le magasin de certificats BlackBerry Dynamics ou dans le magasin de certificats du terminal. |
| Certificats client | • La longueur de clé minimale pour les certificats doit être de 2 048 octets.<br>• La propriété d'utilisation de clé étendue du certificat doit avoir la valeur Ouverture de session par carte à puce Microsoft (1.3.6.1.4.1.311.20.2.2).<br>• Les certificats client doivent inclure le nom d'utilisateur principal (par exemple, user@domain.com) dans l'autre nom d'objet de l'ID objet szOID_NT_PRINCIPAL_NAME 1.3.6.1.4.1.311.20.2.3<br>• Si l'utilisateur reçoit plusieurs certificats client, le domaine du nom principal de l'utilisateur doit correspondre au domaine de la ressource à laquelle l'utilisateur accède pour s'assurer que le certificat correct est utilisé.<br>• Les certificats doivent être valides. Vérifiez leur validité par rapport aux serveurs listés ci-dessus. |

# Chiffrer la connexion entre BlackBerry UEM et Microsoft SQL Server

Vous pouvez configurer une connexion chiffrée entre BlackBerry UEM et Microsoft SQL Server. Par défaut, la connexion n'est pas chiffrée.

**Remarque :**

- Lorsque vous mettez à niveau UEM, les paramètres de chiffrement ne sont pas conservés. Après la mise à niveau, vous devez répéter l'étape 3 et les étapes suivantes pour chiffrer à nouveau la connexion.
- Veuillez noter que la connexion chiffrée peut entraîner une augmentation du CPU UOS sur l'ordinateur qui héberge le BlackBerry UEM Core.

**Avant de commencer :**

- Sur l'ordinateur qui héberge SQL Server, dans la console de gestion Microsoft, utilisez le composant logiciel enfichable de certificat pour demander le certificat de l'ordinateur (sélectionnez le compte de l'ordinateur, Certificats (ordinateur local) > cliquez avec le bouton droit sur Personnel > Toutes les tâches > Demander un nouveau certificat). Vous devriez voir le certificat dans Certificats (ordinateur local) > Personnel > Certificats. Selon la configuration de SQL Server, vous devrez peut-être accorder des autorisations au certificat au compte SQL Server.
- Dans le gestionnaire de configuration SQL Server, accédez à Configuration réseau et ouvrez les Propriétés des protocoles SQL Server. Dans l'onglet Certificat, sélectionnez le certificat de l'ordinateur. Redémarrez le service SQL Server.
- Dans la console de gestion Microsoft, utilisez le composant logiciel enfichable de certificats pour exporter le certificat de l'ordinateur depuis le magasin personnel (personal.cer). Copiez le certificat sur tous les ordinateurs qui hébergent une instance UEM.

Exécutez ces étapes sur tous les ordinateurs qui hébergent une instance de UEM Core :

1. Accédez au certificat personnel (personal.cer) et double-cliquez dessus. Affichez le certificat parent (parent.cer), exportez-le et enregistrez-le dans le même dossier que celui contenant le certificat personnel (par exemple, C:\blackberry\certs\).
2. Ouvrez l'invite de commande et exécutez les commandes suivantes pour importer les certificats personnels et parents dans le magasin de clés Java et générer un magasin de certificats approuvés :

```
keytool -importcert -keystore "<path_to_Java_CA_certs_store>" -
storepass <CA_certs_store_password> -file <path_to_personal_cert> -alias
 personal

keytool -importcert -keystore "<path_to_Java_CA_certs_store>" -
storepass <CA_certs_store_password> -file <path_to_parent_cert> -alias parent

keytool -import -v -trustcacerts -alias personal -file <path_to_personal_cert>
 -keystore <path_to_folder_with_personal_and_parent_certs>\truststore.jks -
storepass <password_to_set_for_trust_store> -storetype JKS
```

   Par exemple :

```
keytool -importcert -keystore "c:\Program Files\Eclipse Adoptium\jre-17.0.11.9-
hotspot\lib\security\cacerts" -storepass changeit -file c:\blackberry\certs
\personal.cer -alias personal
```

```
keytool -importcert -keystore "c:\Program Files\Eclipse Adoptium\jre-17.0.11.9-
hotspot\lib\security\cacerts" -storepass changeit -file c:\blackberry\certs
\parent.cer -alias parent

keytool -import -v -trustcacerts -alias personal -file c:\blackberry\certs
\personal.cer -keystore c:\blackberry\certs\truststore.jks -storepass password
 -storetype JKS
```

3. Arrêtez tous les services UEM.
4. Dans C:\Program Files\BlackBerry\UEM\common-settings, copiez et renommez **db.properties** pour créer un fichier de propriétés de base de données de sauvegarde.
5. Ouvrez **db.properties**.
6. Dans la section Paramètres de chiffrement de SQL Server, configurez les paramètres suivants (vous n'avez pas besoin de modifier d'autres paramètres) :

```
configuration.database.ng.encrypt=true
configuration.database.ng.trustservercertificate=false
configuration.database.ng.truststore=<path_to_the_jks_trust_store_generated_in_step_2>
configuration.database.ng.truststorepassword=<password_for_jks_trust_store_generated_in_st
```

7. Enregistrez et fermez **db.properties**.
8. Redémarrez les services UEM.

# Intégration de BlackBerry UEM avec Cisco ISE

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

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

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

Les administrateurs Cisco ISE peuvent afficher, trier et filtrer les données sur les terminaux dans la console de gestion Cisco ISE. Les administrateurs peuvent également verrouiller un terminal, supprimer les données professionnelles d'un terminal ou supprimer toutes les données d'un terminal. Pour plus d'informations sur l'accès au réseau et les contrôles de terminaux, reportez-vous à Gestion de l'accès au réseau et des contrôles de terminaux à l'aide de Cisco ISE.

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

| Étape | Action |
|---|---|
| 1 | Vérifiez que l'environnement de votre organisation répond aux exigences d'intégration d'UEM à Cisco ISE. |
| 2 | Connectez UEM à Cisco ISE et configurez un profil d'autorisation et des stratégies d'accès. |

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

Les administrateurs Cisco Identity Services Engine (ISE) peuvent effectuer les opérations suivantes.

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

# Exigences : intégration de BlackBerry UEM à Cisco ISE

| Élément | Configuration requise |
|---|---|
| Version de Cisco ISE | BlackBerry UEM prend en charge l'intégration à Cisco ISE version 1.2 et ultérieure. |
| Système d'exploitation pris en charge | Tout système d'exploitation pris en charge par UEM, à l'exception de Windows 10 pour les ordinateurs de bureau. |
| Port d'écoute | Cisco ISE utilise le port d'écoute par défaut de BlackBerry Web Services, 18084, pour obtenir les données sur les terminaux de UEM.<br>Si le port 18084 n'était pas disponible au moment de l'installation de UEM, l'application d'installation a sélectionné un autre port disponible. Pour vérifier la valeur de port correcte, dans le fichier journal BlackBerry UEM Core (CORE), recherchez (`^/ciscoise/.*`) et notez le numéro de port indiqué au-dessous de ce texte. |
| Pare-feu | Si un pare-feu existe entre UEM et Cisco ISE, configurez-le pour autoriser les sessions HTTPS entre les deux systèmes. |
| Compte d'administrateur | Cisco ISE nécessite un compte d'administrateur UEM dédié pour extraire des données sur les terminaux. Vous pouvez utiliser un compte d'administrateur existant ou en créer un nouveau. Il doit s'agir d'un compte d'administrateur local (et non d'un utilisateur de l'annuaire). Le compte d'administrateur nécessite un rôle disposant des autorisations suivantes :<br>• Afficher les utilisateurs et les terminaux activés<br>• Gérer les terminaux<br>• Verrouiller le terminal et définir un message<br>• Supprimer uniquement les données professionnelles<br>• Supprimer toutes les données du terminal<br>Les rôles d'administrateur de sécurité et d'administrateur d'entreprise par défaut possèdent ces autorisations, ou vous pouvez créer un rôle personnalisé avec ces autorisations. Pour plus d'informations, reportez-vous à la section Créer un administrateur dans le contenu relatif à l'administration. |

# Connecter BlackBerry UEM à Cisco ISE

Si vous ne disposez pas d'un compte d'administrateur Cisco Identity Services Engine (ISE), envoyez ces instructions à un administrateur Cisco ISE, ainsi que les informations requises concernant UEM et le compte d'administrateur UEM. Pour obtenir la documentation Cisco ISE la plus récente, consultez les guides de configuration de Cisco ISE.

**Avant de commencer :** Dans un navigateur, accédez à **https://<*server_name*>:<*BlackBerry_Web_Services_port*>/enterprise/admin/util/ws?wsdl** où <*server_name*> est le FQDN de l'ordinateur qui héberge le composant BlackBerry UEM Core. La valeur <*BlackBerry_Web_Services_port*> par défaut est 18084. Utilisez votre navigateur pour exporter le certificat BlackBerry Web Services et enregistrez-le sur votre bureau.

1. Connectez-vous à la console de gestion Cisco ISE.

2. Importez le certificat BlackBerry Web Services dans le magasin de certificats approuvés Cisco ISE. Sélectionnez les options à approuver pour l'authentification du client et syslog et à approuver pour l'authentification des services Cisco.
3. Ajoutez un service MDM externe et spécifiez les détails de l'instance UEM, y compris le FQDN ou l'adresse IP du domaine UEM, le port (18084 par défaut) et les informations d'identification du compte d'administrateur UEM.
4. Pour l'intervalle d'interrogation, indiquez, en minutes, la fréquence à laquelle vous voulez que Cisco ISE interroge UEM pour obtenir les données du terminal. Il est recommandé d'utiliser la valeur par défaut.

   Si vous définissez cette valeur sur 60 minutes ou moins, vous remarquerez peut-être un impact important sur les performances de l'environnement de votre entreprise. Si vous définissez cette valeur sur 0, Cisco ISE n'interroge pas UEM.
5. Activer et tester la connexion à UEM

Une fois la connexion établie, vous pouvez afficher les attributs de dictionnaire pour UEM dans la console de gestion Cisco ISE. Les entrées de journal pour l'interrogation de Cisco ISE sont écrites dans le fichier journal BlackBerry UEM Core (CORE).

**À la fin :** Effectuez les tâches de configuration suivantes dans la console de gestion Cisco ISE :

- Configurez des listes de contrôle d'accès sur le contrôleur LAN sans fil.
- Configurez un profil d'autorisation qui redirige les terminaux vers la console BlackBerry UEM Self-Service s'ils tentent d'accéder au réseau professionnel alors que le terminal n'est pas activé sur UEM. L'utilisateur requiert un compte d'utilisateur UEM pour se connecter à BlackBerry UEM Self-Service et activer le terminal. Demandez aux utilisateurs de contacter l'administrateur UEM si Cisco ISE les redirige vers la page d'inscription.
- Configurez les règles de stratégie d'autorisation qui déterminent comment Cisco ISE gère les terminaux non activés sur UEM ou non compatibles avec UEM.

# Configurer un VPN à l'aide de Knox StrongSwan pour les environnements de site sombre UEM

Dans un environnement de site sombre UEM, vous devez configurer l'accès VPN à votre environnement afin que les terminaux Samsung Knox puissent accéder à vos serveurs et ressources internes. Pour plus d'informations sur UEM dans les environnements de site sombre, reportez-vous à la section Installation ou mise à niveau de BlackBerry UEM dans un environnement de site sombre dans le contenu relatif à l'installation.

**Avant de commencer :** Téléchargez les applications Knox Service Plugin et Android VPN Management for KNOX StrongSwan, et ajoutez les fichiers .apk à l' emplacement réseau partagé des applications internes.

1. Ajoutez les applications Knox Service Plugin et Android VPN Management for KNOX StrongSwan à la liste des applications.
2. Sélectionnez l'application Knox Service Plugin et cliquez sur + pour définir les options de configuration de l'application.
   a) Sous **Profil VPN**, sélectionnez **VPN intégré KNOX**.
   b) Sous **Paramètres du VPN intégré KNOX (pour StrongSwan)**, définissez les options suivantes :
      - Définissez le **type d'authentification** sur « ipsec_ike2_rsa ».
      - Définissez l'**alias du certificat utilisateur** sur le nom d'utilisateur auquel est ajouté « _1 [Knox] ». Vous pouvez utiliser des variables pour le nom d'utilisateur (par exemple, `%UserFirstName % %UserLastName% _1 [Knox]`).
      - Définissez l'**alias du certificat d'autorité de certification** sur le nom d'utilisateur auquel est ajouté « [Knox] ». Vous pouvez utiliser des variables pour le nom d'utilisateur (par exemple, `%UserFirstName % %UserLastName% [Knox]`).
3. Attribuez l'application à l'utilisateur.
4. Créez un profil de certificat d'autorité de certification partagé pour envoyer le certificat de serveur VPN aux terminaux et l'attribuer aux utilisateurs.
5. Ajoutez un certificat client VPN pour chaque utilisateur.

# 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