BlackBerry UEM

Utilisation d'un PKI pour sécuriser les connexions

Administration

12.16

Table des matières

Certificats et PKI

Un certificat PKI est un document numérique émis par une autorité de certification qui vérifie l'identité de l'objet de certificat et la lie à une clé publique. Chaque certificat dispose d'une clé privée correspondante stockée séparément. La clé publique et la clé privée forment une paire de clés asymétriques qui peuvent être utilisées à des fins de cryptage des données et d'authentification de l'identité. Une autorité de certification signe le certificat pour vérifier que les entités qui approuvent l'autorité de certification peuvent également approuver le certificat.

Selon les fonctionnalités et le type d'activation du terminal, les terminaux et les applications peuvent utiliser des certificats pour :

- S'authentifier à l'aide du protocole SSL/TLS lorsqu'ils se connectent aux pages Web utilisant le protocole HTTPS
- S'authentifier auprès d'un serveur de messagerie professionnel
- S'authentifier auprès d'un réseau Wi-Fi ou VPN professionnel
- Crypter et signer les e-mails à l'aide de la protection S/MIME

De nombreux certificats utilisés à différentes fins peuvent être stockés sur un terminal.

Étapes à suivre pour utiliser les certificats

Pour utiliser des certificats PKI avec des terminaux ou des applications, vous devez procéder comme suit :

Étape	Action
1	Si nécessaire, connectez BlackBerry UEM au logiciel PKI de votre entreprise.
2	Créez un ou plusieurs profils de certificat d'autorité de certification pour envoyer des certificats d'autorité de certification aux terminaux et aux applications.
3	Créez des profils SCEP, d'informations d'identification utilisateur ou de certificat partagé, ou chargez les certificats d'un utilisateur spécifique, pour envoyer des certificats client aux terminaux et aux applications.
4	Si nécessaire, associez les profils de certificat aux profils Wi-Fi, VPN ou e-mail.
5	Si nécessaire, attribuez les profils de certificats aux comptes d'utilisateur, groupes d'utilisateurs ou groupes de terminaux.
6	Si vous utilisez des certificats avec une application BlackBerry Dynamics, sélectionnez Autoriser les applications BlackBerry Dynamics à utiliser les certificats utilisateur, les profils SCEP et les profils d'identification des utilisateurs dans les paramètres de l'application.

Intégration de BlackBerry UEM avec le logiciel PKI de votre entreprise

Si votre entreprise utilise une solution PKI, vous pouvez émettre des certificats en étendant l'authentification basée sur des certificats fournie par ces services PKI aux terminaux que vous gérez avec BlackBerry UEM.

Les produits Entrust (comme Entrust IdentityGuard et Entrust Authority Administration Services) ainsi que les produits OpenTrust (comme OpenTrust PKI et OpenTrust CMS) fournissent des autorités de certification qui émettent des certificats client. Vous pouvez configurer une connexion au logiciel PKI de votre organisation et utiliser des profils pour envoyer le certificat d'autorité de certification et les certificats client aux terminaux.

Pour les terminaux BlackBerry Dynamics activés, vous pouvez également configurer un connecteur PKI qui crée une connexion entre BlackBerry UEM et un serveur d'autorité de certification pour inscrire les certificats des applications BlackBerry Dynamics ou utiliser une application prenant en charge l'inscription des certificats sur application, comme Purebred.

Connecter BlackBerry UEM au logiciel Entrust de votre organisation

Pour permettre à BlackBerry UEM d'envoyer les certificats émis par le logiciel Entrust de de votre organisation (par exemple, Entrust IdentityGuard ou Entrust Authority Administration Services) à des terminaux et applications BlackBerry Dynamics, vous pouvez ajouter une connexion au logiciel Entrust de votre organisation à BlackBerry UEM.

Avant de commencer : Contactez l'administrateur Entrust de votre organisation pour obtenir :

- l'URL du service Web MDM de Entrust ;
- les informations de connexion d'un compte d'administrateur Entrust que vous pouvez utiliser pour connecter BlackBerry UEM au logiciel Entrust ;
- le certificat d'autorité de certification Entrust contenant la clé publique (.der, .pem ou .cert). BlackBerry UEM utilise ce certificat pour établir des connexions SSL avec le serveur Entrust.

1. Sur la barre de menus, cliquez sur **Paramètres**.
2. Cliquez sur **Intégration externe > Autorité de certification**.
3. Cliquez sur **Ajouter une connexion Entrust**.
4. Dans le champ **Nom de connexion**, saisissez un nom de connexion.
5. Dans le champ **URL**, saisissez l'URL du service Web Entrust.
6. Dans le champ **Nom d'utilisateur**, saisissez le nom d'utilisateur du compte d'administrateur Entrust.
7. Dans le champ **Mot de passe**, saisissez le mot de passe du compte d'administrateur Entrust.
8. Si vous souhaitez charger un certificat d'autorité de certification pour autoriser BlackBerry UEM à établir des connexions SSL avec le serveur Entrust, cliquez sur **Parcourir**. Accédez au certificat d'autorité de certification et sélectionnez-le.
9. Pour tester la connexion, cliquez sur **Tester la connexion**.
10. Cliquez sur **Enregistrer**.

À la fin :

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

Connecter BlackBerry UEM au serveur Entrust IdentityGuard de votre organisation pour utiliser les informations d'identification intelligentes

Si votre organisation utilise des informations d'identification intelligentes dérivées gérées par Entrust IdentityGuard, vous pouvez utiliser des informations d'identification intelligentes dérivées avec des terminaux Android et des applications BlackBerry Dynamics sur les terminaux iOS et Android.

Avant de commencer :

Contactez l'administrateur Entrust de votre organisation pour obtenir les informations suivantes :

- URL du serveur Entrust IdentityGuard
- Nom des informations d'identification intelligentes à activer sur les terminaux, comme indiqué dans Entrust IdentityGuard
- Certificat d'autorité de certification Entrust pour envoyer le certificat aux terminaux

1. Sur la barre de menus, cliquez sur **Paramètres**.
2. Cliquez sur **Intégration externe > Autorité de certification**.
3. Cliquez sur **Ajouter une connexion pour les informations d'identification intelligentes Entrust**.
4. Dans le champ **Nom des informations d'identification intelligentes**, entrez le nom des informations d'identification intelligentes spécifiées dans Entrust IdentityGuard.
5. Dans le champ **URL Entrust**, saisissez l'URL du serveur Entrust IdentityGuard.
6. Cliquez sur **Ajouter**.

À la fin :

- Créer un profil de certificat d'autorité de certification partagé pour envoyer le certificat d'autorité de certification Entrust aux terminaux et attribuer le profil aux utilisateurs ou groupes auxquels le profil d'informations d'identification utilisateur sera attribué.
- Créer un profil d'informations d'identification utilisateur pour utiliser les informations d'identification intelligentes Entrust sur les terminaux.

Connecter BlackBerry UEM au logiciel OpenTrust de votre entreprise

Pour étendre l'authentification basée sur des certificats OpenTrust aux terminaux, vous devez ajouter une connexion au logiciel OpenTrust de votre entreprise. BlackBerry UEM prend en charge l'intégration avec OpenTrust PKI 4.8.0 et version ultérieure et OpenTrust CMS 2.0.4 et version ultérieure. Cette connexion n'est pas prise en charge par les applications BlackBerry Dynamics.

Avant de commencer : Contactez l'administrateur OpenTrust de votre entreprise pour obtenir l'URL du serveur OpenTrust, le certificat côté client contenant la clé privée (au format .pfx ou .p12) et le mot de passe du certificat.

1. Sur la barre de menus, cliquez sur **Paramètres**.
2. Cliquez sur **Intégration externe > Autorité de certification**.
3. Cliquez sur **Ajouter une connexion OpenTrust**.
4. Dans le champ **Nom de connexion**, saisissez un nom de connexion.
5. Dans le champ **URL**, saisissez l'URL du logiciel OpenTrust.
6. Cliquez sur **Parcourir**. Accédez au certificat côté client utilisé par BlackBerry UEM pour authentifier la connexion au serveur OpenTrust, puis sélectionnez-le.

7. Dans le champ **Mot de passe du certificat**, saisissez le mot de passe du certificat du serveur OpenTrust.
8. Pour tester la connexion, cliquez sur **Tester la connexion**.
9. Cliquez sur **Enregistrer**.

À la fin :

- Créez un profil d'informations d'identification d'utilisateur pour envoyer les certificats de votre logiciel PKI vers les terminaux.
- Si vous utilisez la connexion BlackBerry UEM avec le logiciel OpenTrust pour distribuer des certificats aux terminaux, les certificats peuvent prendre un certain temps pour devenir valables. Ce retard pourrait entrainer des problèmes avec l'authentification par e-mail au cours du processus d'activation du terminal. Pour résoudre ce problème, dans le logiciel OpenTrust, configurez l'autorité de certification OpenTrust et définissez Antidater les certificats (secondes) sur 180.

Connecter BlackBerry UEM à un connecteur PKI BlackBerry Dynamics

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

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

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

Avant de commencer : Configurez un connecteur PKI BlackBerry Dynamics.

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

- **Certificat d'autorité de certification** : si vous sélectionnez cette option, vous devez cliquer sur Parcourir pour naviguer et sélectionner le certificat d'autorité de certification de votre organisation.
- **Certificat serveur du connecteur PKI** : si vous sélectionnez cette option, vous devez cliquer sur Parcourir pour naviguer et sélectionner le certificat de serveur de connecteur PKI de votre organisation.

9. Pour tester la connexion, cliquez sur **Tester la connexion**.
10. Cliquez sur **Enregistrer**.

À la fin :

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

Connecter BlackBerry UEM à la solution PKI basée sur des applications de votre organisation

Les solutions PKI basées sur des applications telles que Purebred comprennent une application installée sur un terminal qui communique avec une autorité de certification afin d'inscrire des certificats et de les ajouter au terminal. Vous pouvez utiliser une solution PKI basée sur les applications pour fournir des certificats à l'usage des applications BlackBerry Dynamics.

Pour utiliser une solution PKI basée sur les applications avec les terminaux iOS, vous devez ajouter une connexion entre BlackBerry UEM et le fournisseur PKI. Cette tâche n'est pas requise pour utiliser une solution PKI basée sur les applications uniquement avec des terminaux Android.

Si l'application PKI qui récupère les certificats de l'autorité de certification n'est pas une application BlackBerry Dynamics, le BlackBerry UEM Client communique avec l'application PKI afin d'obtenir les certificats et de les fournir aux applications BlackBerry Dynamics.

Avant de commencer : Vérifiez que l'application qui récupère les certificats à l'usage des applications BlackBerry Dynamics figure dans la liste des applications dans BlackBerry UEM.

1. Sur la barre de menus, cliquez sur **Paramètres > Intégration externe > Autorité de certification**.
2. Cliquez sur **Ajouter une connexion pour les certificats de terminal**.
3. Sélectionnez l'application qui récupère les certificats de l'application PKI qui seront utilisés par les applications BlackBerry Dynamics. Pour utiliser Purebred, sélectionnez BlackBerry UEM Client.
4. Cliquez sur **Ajouter**.

À la fin :

- Création de profils d'identification pour les certificats d'application.
- Créer un profil d'identification d'utilisateur pour utiliser des certificats d'application sur des terminaux iOS.
- Créer un profil d'identification d'utilisateur pour utiliser des certificats du magasin de clés natif

Fournir des certificats clients aux terminaux et aux applications

Vous et les utilisateurs pouvez envoyer des certificats clients aux terminaux et aux applications de plusieurs façons.

Comment le certificat est ajouté	Description	Terminaux pris en charge
Pendant l'activation du terminal	BlackBerry UEM envoie les certificats aux terminaux lors du processus d'activation. Les terminaux utilisent ces certificats pour établir des connexions sécurisées entre le terminal et BlackBerry UEM.	Tout
Profils SCEP	Vous pouvez créer des profils SCEP que les terminaux utilisent pour se connecter à l'autorité de certification de votre entreprise et en obtenir des certificats client à l'aide d'un service SCEP. Les terminaux et les applications BlackBerry Dynamics peuvent utiliser ces certificats pour l'authentification par certificat et pour se connecter à votre réseau Wi-Fi professionnel, au VPN professionnel et au serveur de messagerie professionnel.	iOS macOS Android Windows 10
Connexion à la solution PKI de votre entreprise	Si votre organisation utilise une solution PKI telle que des produits logiciels Entrust ou OpenTrust pour émettre et gérer les certificats, vous pouvez créer des profils d'informations d'identification d'utilisateur que les terminaux utiliseront pour obtenir les certificats client auprès de l'autorité de certification de votre organisation. Les terminaux compatibles BlackBerry Dynamics utilisent ces certificats pour l'authentification basée sur certificat à partir des applications BlackBerry Dynamics. D'autres terminaux utilisent ces certificats pour l'authentification basée sur certificat à partir du navigateur et pour se connecter à votre réseau Wi-Fi professionnel, VPN professionnel et serveur de messagerie professionnel.	iOS macOS (pour BlackBerry Access uniquement) Android Windows 10 (pour BlackBerry Access uniquement)
Profils des certificats partagés	Un profil de certificat partagé spécifie un certificat client que BlackBerry UEM envoie aux terminaux iOS, macOS et Android. BlackBerry UEM envoie le même certificat client à chaque utilisateur auquel le profil est attribué. L'administrateur doit avoir accès au certificat et à la clé privée pour créer un profil de certificat partagé.	iOS macOS Android

Comment le certificat est ajouté	Description	Terminaux pris en charge
Envoi de certificat client à un compte d'utilisateur individuel	Vous pouvez ajouter un certificat client à un compte d'utilisateur. BlackBerry UEM peut envoyer le certificat aux terminaux iOS et Android de l'utilisateur. Si le certificat est associé à un profil d'informations d'identification de l'utilisateur, les terminaux peuvent utiliser ce certificat pour se connecter à votre réseau Wi-Fi professionnel, VPN professionnel et serveur de messagerie professionnel. L'administrateur doit avoir accès au certificat et à la clé privée pour envoyer le certificat client à l'utilisateur.	iOS Android
Téléchargement de l'utilisateur sur UEM Self-Service	Si votre organisation dispose d'un environnement BlackBerry UEM sur site, les utilisateurs peuvent télécharger des certificats sur BlackBerry UEM Self-Service. Puis BlackBerry UEM transfère le certificat sur leur terminal. Si le certificat est associé à un profil d'informations d'identification d'un utilisateur, les terminaux et les applications BlackBerry Dynamicspeuvent utiliser ce certificat pour se connecter à votre réseau Wi-Fi professionnel, VPN professionnel et serveur de messagerie professionnel. Cette fonction n'est pas prise en charge dans BlackBerry UEM Cloud.	iOS Android
Importation par les utilisateurs	Sur les terminaux BlackBerry 10, les utilisateurs peuvent importer des certificats clients dans la liste de certificats du terminal dans la section « Sécurité et confidentialité » sous « Paramètres système ». Les certificats destinés à être utilisés par le Work Browser ou pour l'envoi de messages protégés par S/MIME à partir du compte de messagerie professionnel peuvent être importés dans le système de fichiers du terminal ou à partir d'un emplacement réseau accessible depuis l'espace Travail. Sur les terminaux Android, les utilisateurs peuvent ajouter des certificats au magasin de clés natif du terminal pour une utilisation avec des applications BlackBerry Dynamics.	Android

Envoi de certificats aux terminaux et applications à l'aide de profils

Vous pouvez envoyer des certificats aux terminaux et aux applications à l'aide des profils suivants, disponibles dans la bibliothèque des stratégies et des profils :

Profil	Description
Certificat d'AC	Les profils de certificat d'autorité de certification spécifient un certificat d'autorité de certification que les terminaux et les applications BlackBerry Dynamics peuvent utiliser pour approuver l'identité associée à n'importe quel certificat client ou serveur qui a été signé par cette autorité de certification.
Informations d'identification de l'utilisateur	Les profils d'informations d'identification de l'utilisateur envoient les certificats aux terminaux comme suit : • Ils peuvent spécifier une connexion au logiciel PKI de votre entreprise pour l'envoi des certificats client aux terminaux et aux applications BlackBerry Dynamics. • Ils vous permettent de télécharger manuellement les certificats dans BlackBerry UEM et, dans un environnement local, permettent aux utilisateurs de télécharger des certificats à l'aide de BlackBerry UEM Self-Service. • Ils peuvent autoriser les applications BlackBerry Dynamics sur les terminaux Android et l'application BlackBerry Access sur les terminaux macOS et Windows 10 à utiliser des certificats du magasin de clés natif du terminal. • Ils peuvent permettre aux applications BlackBerry Dynamics d'importer des certificats à partir d'autres solutions PKI basées sur des applications telles que Purebred.
SCEP	Les profils SCEP indiquent comment les terminaux et les applications BlackBerry Dynamics sont connectés à et obtiennent des certificats client de l'autorité de certification de votre entreprise à l'aide d'un service SCEP.
Certificat partagé	Les profils de certificats partagés spécifient un certificat client que BlackBerry UEM envoie aux terminaux iOS et Android. BlackBerry UEM envoie le même certificat client à chaque utilisateur auquel le profil est attribué.

Pour les terminaux iOS et Android, vous pouvez également envoyer un certificat client à un terminal en ajoutant directement ce certificat à un compte d'utilisateur. Pour plus d'informations, reportez-vous à Ajouter un certificat client à un compte d'utilisateur.

Pour les terminaux iOS et Android, si votre entreprise utilise des certificats pour S/MIME, vous pouvez également utiliser des profils pour permettre à des terminaux d'obtenir des clés publiques de destinataire et vérifier l'état du certificat. Pour plus d'informations, reportez-vous à la section Extension de la sécurité de la messagerie à l'aide de S/MIME.

Pour que les applications BlackBerry Dynamics utilisent les certificats envoyés par des profils, vous devez sélectionner l'option Autoriser les applications BlackBerry Dynamics à utiliser les certificats utilisateur, les profils SCEP et les profils d'informations d'identification des utilisateurs dans les paramètres de l'application.

Choix des profils pour envoyer des certificats client aux terminaux et aux applications

Vous pouvez utiliser différents types de profils pour fournir des certificats client aux terminaux et aux applications BlackBerry Dynamics. Le type de profil que vous choisissez dépend de la façon dont votre organisation utilise les certificats et des types de terminaux pris en charge. Prenez en compte les recommandations suivantes :

- Pour utiliser les profils SCEP, vous devez disposer d'une autorité de certification qui prend en charge le protocole SCEP.
- Si vous avez configuré une connexion entre BlackBerry UEM et la solution PKI de votre entreprise, utilisez les profils d'informations d'identification de l'utilisateur pour envoyer les certificats aux terminaux. Vous pouvez vous connecter directement à une autorité de certification Entrust ou OpenTrust. Vous pouvez également utiliser un connecteur PKI BlackBerry Dynamics afin de vous connecter à un serveur d'AC pour inscrire les certificats pour les terminaux BlackBerry Dynamics activés.
- Pour utiliser des certificats avec les applications BlackBerry Dynamics, vous devez utiliser un profil d'informations d'identification de l'utilisateur ou ajouter les certificats aux comptes d'utilisateur individuels.
- Pour permettre aux utilisateurs de charger les certificats leur permettant de se connecter à votre réseau Wi-Fi professionnel, VPN professionnel et serveur de messagerie professionnel, utilisez un profil d'informations d'identification de l'utilisateur.
- Pour utiliser des certificats client pour une authentification Wi-Fi, VPN et par serveur de messagerie, vous devez associer le profil de certificat avec un profil Wi-Fi, VPN ou de messagerie.

  Remarque : Les terminaux Android Enterprise ne prennent pas en charge l'utilisation de certificats envoyés aux terminaux par BlackBerry UEM pour l'authentification Wi-Fi.
- Les profils de certificats partagés et les certificats que vous ajoutez aux comptes utilisateur ne garantissent par le caractère privé de la clé, car vous devez avoir accès à cette clé privée. La connexion à une autorité de certification avec des profils SCEP ou des profils d'informations d'identification de l'utilisateur est plus sécurisée, car la clé privée n'est envoyée qu'au terminal auquel le certificat a été émis.

Envoi de certificats d'autorité de certification à des terminaux et des applications

Vous devrez peut-être distribuer des certificats CA aux terminaux si votre organisation utilise le protocole S/MIME ou si des terminaux ou des applications BlackBerry Dynamics utilisent une authentification basée sur des certificats pour se connecter à un réseau ou à un serveur dans l'environnement de votre organisation.

Lorsqu'un certificat CA est stocké sur un terminal, le terminal et les applications approuvent l'identité associée à tout certificat client ou à un certificat de serveur signé par l'autorité de certification. Lorsque le certificat de l'autorité de certification qui a signé les certificats réseau et serveur de votre organisation est stocké sur les terminaux, les terminaux et les applications peuvent approuver vos réseaux et serveurs lorsqu'ils établissent des connexions sécurisées. Lorsque le certificat d'autorité de certification qui a signé les certificats S/MIME de votre organisation est stocké sur des terminaux, le client de messagerie peut approuver le certificat de l'expéditeur lors de la réception d'un e-mail sécurisé.

De nombreux certificats d'autorité de certification utilisés à des fins différentes peuvent être stockés sur un terminal. Vous pouvez utiliser des profils de certificat CA pour envoyer des certificats CA à des terminaux.

Créer un profil de certificat d'autorité de certification partagé

Avant de commencer : Obtenez le fichier de certificat de l'AC auprès de votre administrateur PKI.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Certificats > Certificat CA**.
3. Cliquez sur +.
4. Saisissez le nom et la description du profil. Chaque profil de certificat d'autorité de certification doit avoir un nom unique. Certains noms (par exemple, ca_1) sont réservés.
5. Dans le champ **Fichier de certificat**, cliquez sur **Parcourir** pour localiser le fichier de certificat.
6. Si le certificat d'autorité de certification est envoyé aux terminaux BlackBerry 10, dans l'onglet BlackBerry, spécifiez un ou plusieurs des magasins de certificats suivants auxquels envoyer le certificat sur le terminal :
   - Magasin de certificats du navigateur
   - Magasin de certificats VPN
   - Magasin de certificats Wi-Fi
   - Magasin de certificats d'entreprise
7. Si le certificat d'autorité de certification est envoyé aux terminaux macOS, dans l'onglet macOS, dans la liste déroulante **Appliquer le profil à**, sélectionnez **Utilisateur** ou **Terminal**.
8. Cliquez sur **Ajouter**.

Envoi de certificats clients vers des terminaux et des applications à l'aide de profils d'authentification utilisateur

Les profils d'informations d'identification de l'utilisateur permettent aux terminaux d'utiliser des certificats client obtenus grâce aux méthodes suivantes :

- Téléchargement manuel de certificats vers la console de gestion BlackBerry UEM ou, dans un environnement local, vers BlackBerry UEM Self-Service
- Une connexion établie entre BlackBerry UEM et l'autorité de certification Entrust de votre organisation ou l'autorité de certification OpenTrust
- Pour les applications BlackBerry Dynamics sur les terminaux Android, les certificats sont stockés dans le magasin de clés natif du terminal
- Pour les applications BlackBerry Dynamics, le téléchargement est effectué via un connecteur PKI BlackBerry Dynamics établi
- Pour les applications BlackBerry Dynamics, à l'aide d'une solution PKI basée sur les applications telles que Purebred.

Si les utilisateurs chargent les certificats manuellement dans UEM Self-Service, ceux-ci s'affichent sur la page de l'utilisateur dans la console de gestion. Vous pouvez également supprimer ou remplacer le certificat. Cette fonction n'est pas prise en charge dans BlackBerry UEM Cloud.

Les profils d'identification de l'utilisateur ne sont pas pris en charge sur les terminaux iOS et Android. Les solutions PKI basées sur les applications sont prises en charge pour les applications BlackBerry Dynamics sur les terminaux iOS et Android. Le chargement manuel des certificats est pris en charge pour les terminaux iOS, Android Enterprise et Samsung Knox Workspace.

Pour plus d'informations sur la connexion de BlackBerry UEM au logiciel PKI de votre entreprise, reportez-vous à Intégration de BlackBerry UEM avec le logiciel PKI de votre entreprise.

Vous pouvez également utiliser des profils SCEP pour inscrire les certificats client sur les terminaux. Vous pouvez également charger des certificats directement vers un compte d'utilisateur. Le type de profil que vous choisissez dépend de la manière dont votre organisation utilise le logiciel PKI, des types de terminaux pris en charge par et de la manière dont vous souhaitez gérer les certificats.

Créer un profil d'informations d'identification de l'utilisateur pour télécharger manuellement les certificats

Les profils d'informations d'identification de l'utilisateur vous permettent, ainsi qu'aux utilisateurs, de télécharger manuellement un certificat à envoyer aux terminaux des utilisateurs.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Certificats > Informations d'identification de l'utilisateur**.
3. Cliquez sur +.
4. Saisissez le nom et la description du profil. Chaque profil de certificat doit avoir un nom unique.
5. Dans la liste déroulante **Connexion à l'autorité de certification**, cliquez sur **Certificat chargé manuellement**.
6. Si vous gérez des terminaux Android Enterprise et que vous souhaitez éviter que les utilisateurs ne sélectionnent le certificat pour l'utiliser à d'autres fins, sélectionnez **Masquer le certificat sur les terminaux Android Enterprise** dans l'onglet **Android**. Cette option s'applique uniquement aux terminaux Android 9.0 et versions ultérieures.
7. Cliquez sur **Ajouter**.

À la fin :

- Si les terminaux utilisent des certificats client pour s'authentifier auprès d'un réseau Wi-Fi, d'un VPN ou d'un serveur de messagerie, associez le profil d'informations d'identification de l'utilisateur à un profil Wi-Fi, VPN ou de messagerie.
- Attribuez le profil aux comptes d'utilisateur et groupes d'utilisateurs.
- Ajouter un certificat client à un profil d'informations d'identification de l'utilisateur Vous pouvez également demander aux utilisateurs d'utiliser BlackBerry UEM Self-Service pour télécharger leur propre certificat.

Créer un profil d'informations d'identification d'utilisateur pour la connexion au logiciel PKI de votre entreprise

Les profils d'identification de l'utilisateur qui se connectent au logiciel PKI de votre organisation peuvent enregistrer des certificats pour les terminaux iOS et Android. Si la connexion est établie avec un logiciel PKI Entrust, le profil d'identification de l'utilisateur peut également enregistrer des certificats pour les applications BlackBerry Dynamics.

Remarque : BlackBerry UEM ne prend pas en charge l'historique des clés pour les certificats émis aux applications BlackBerry Dynamics.

Avant de commencer :

- Configurer une connexion au logiciel Entrust ou OpenTrust de votre organisation.
- Contactez l'administrateur Entrust ou OpenTrust de votre organisation pour confirmer quel profil PKI vous devez sélectionner. BlackBerry UEM obtient une liste des profils du logiciel PKI.
- Demandez à l'administrateurEntrust ou OpenTrust quelles sont les valeurs de profil que vous devez fournir. Par exemple, les valeurs correspondant au type de terminal (devicetype), au groupe Entrust IdentityGuard (iggroup) et au nom d'utilisateur Entrust IdentityGuard (igusername).
- Si le système OpenTrust de votre entreprise est configuré pour renvoyer uniquement des clés sous séquestre, l'administrateur de OpenTrust doit vérifier que des certificats sont présents pour chaque utilisateur dans le système OpenTrust. L'attribution d'un profil d'informations d'identification aux utilisateurs dans BlackBerry UEM ne crée pas automatiquement des certificats pour les utilisateurs dans OpenTrust. Dans ce scénario, un profil d'informations d'identification de l'utilisateur peut uniquement distribuer des certificats aux utilisateurs qui ont déjà un certificat dans le système OpenTrust.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Certificats > Informations d'identification de l'utilisateur**.

3. Cliquez sur +.
4. Saisissez le nom et la description du profil. Chaque profil de certificat doit avoir un nom unique.
5. Dans la liste déroulante **Connexion à l'autorité de certification**, sélectionnez la connexion Entrust ou OpenTrust que vous avez configurée.
6. Dans la liste déroulante **Profil**, cliquez sur le profil qui convient.
7. Spécifiez les valeurs du profil.
8. Si nécessaire, vous pouvez spécifier un type et une valeur SAN pour un certificat client Entrust.
   a) Dans le tableau SAN, cliquez sur +.
   b) Dans la liste déroulante **Type SAN**, cliquez sur le type qui convient.
   c) Dans le champ **Valeur SAN**, tapez la valeur SAN.

      Si le type SAN est défini sur Nom RFC822, la valeur doit correspondre à une adresse électronique valide. Si cette option est définie sur URI, la valeur doit correspondre à une URL valide incluant le protocole et le FQDN ou l'adresse IP. Si cette option est définie sur Nom principal, la valeur doit correspondre à un nom principal valide. Si cette option est définie sur Nom DN, la valeur doit correspondre à un FQDN valide.
9. Indiquez la **Période de renouvellement** du certificat. Cette période peut être comprise entre 1 et 120 jours.
10. Cliquez sur **Ajouter**.

À la fin :

- Si les terminaux utilisent des certificats client pour s'authentifier auprès d'un réseau Wi-Fi, d'un VPN ou d'un serveur de messagerie, associez le profil d'informations d'identification de l'utilisateur à un profil Wi-Fi, VPN ou de messagerie.
- Attribuez le profil aux comptes d'utilisateur et groupes d'utilisateurs. Les utilisateurs Android sont invités à saisir un mot de passe lorsqu'ils reçoivent le profil (le mot de passe est affiché à l'écran).

Créer un profil d'informations d'identification utilisateur pour utiliser les informations d'identification intelligentes Entrust sur les terminaux

Les informations d'identification intelligentes dérivées Entrust sont prises en charge par les applications suivantes :

- Applications BlackBerry Dynamics sur les terminaux iOS
- Applications BlackBerry Dynamics sur les terminaux Android autres que les terminaux Samsung Knox Workspace
- Applications sur les terminaux Android Enterprise qui utilisent des certificats pour la signature, le cryptage et l'authentification d'identité, tels que BlackBerry Hub et les navigateurs Web pris en charge
- Applications sur les terminaux Samsung Knox Workspace qui utilisent des certificats pour la signature, le cryptage et l'authentification d'identité, tels que le client de messagerie natif Samsung et les navigateurs Web pris en charge

Remarque : BlackBerry UEM ne prend pas en charge l'historique des clés pour des informations d'identification intelligentes dérivées.

Avant de commencer :

- Connecter BlackBerry UEM au serveur Entrust IdentityGuard de votre organisation pour utiliser les informations d'identification intelligentes.
- Créer un profil de certificat d'autorité de certification partagé pour envoyer le certificat CA Entrust aux terminaux et attribuer le profil aux utilisateurs ou groupes auxquels ce profil d'informations d'identification utilisateur sera attribué.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Certificats > Informations d'identification de l'utilisateur**.

3. Cliquez sur +.
4. Saisissez le nom et la description du profil. Chaque profil de certificat doit avoir un nom unique.
5. Dans la liste déroulante **Connexion à l'autorité de certification**, sélectionnez la connexion via les informations d'identification intelligentes Entrust que vous avez configurée.
6. Dans la liste déroulante **Type de certificat**, spécifiez si les informations d'identification intelligentes seront utilisées pour l'authentification d'identité, la signature ou le cryptage.

   Si vous souhaitez envoyer des informations d'identification intelligentes aux applications dans plusieurs objectifs, créez d'autres profils d'informations d'identification utilisateur.
7. Si les informations d'identification intelligentes sont envoyées à des terminaux Samsung Knox Workspace ou à d'autres applications que les applications BlackBerry Dynamics sur des terminaux Android Enterprise, cliquez sur l'onglet **Android** et sélectionnez **Remettre à la clé native**.

   Si ce paramètre n'est pas sélectionné, les informations d'identification intelligentes ne peuvent être utilisées que par des applications BlackBerry Dynamics.
8. Si les informations d'identification intelligentes sont envoyées à des applications BlackBerry Dynamics, cliquez sur l'onglet **BlackBerry Dynamics** et procédez comme suit :
   a) Si vous souhaitez autoriser les utilisateurs à ignorer l'inscription du certificat et à l'effectuer ultérieurement, sélectionnez **Autoriser l'inscription de certificat (facultatif)**. L'inscription de certificat facultative est prise en charge pour les terminaux iOS et Android pour les types de profil d'informations d'identification d'utilisateur suivants : fournisseur basé sur le terminal (application), informations d'identification intelligentes Entrust et magasin de clés natif.
   b) Si vous souhaitez que le terminal supprime les informations d'identification en double, sélectionnez **Supprimer les certificats dupliqués**. Le terminal supprime les informations d'identification qui expirent en premier.
   c) Si vous souhaitez que le terminal supprime les informations d'identification ayant expiré, sélectionnez **Supprimer les certificats ayant expiré**.
   d) Pour permettre à toutes les applications BlackBerry Dynamics d'utiliser les informations d'identification intelligentes, sélectionnez **Autoriser toutes les applications à utiliser des certificats**.
   e) Pour permettre à certaines applications BlackBerry Dynamics d'utiliser les informations d'identification intelligentes, sélectionnez **Autoriser les applications spécifiées à utiliser des certificats** et cliquez sur + pour spécifier les applications. Vous devez inclure BlackBerry UEM Client dans la liste des applications.
9. Cliquez sur **Ajouter**.

À la fin :

- Attribuez le profil aux comptes d'utilisateur et groupes d'utilisateurs.
- Une fois le profil reçu par le terminal, les utilisateurs doivent se connecter au module Entrust IdentityGuard Self-Service pour activer leurs informations d'identification intelligentes et utiliser BlackBerry UEM Client pour lire le QR Code présenté par le module Entrust IdentityGuard Self-Service pour ajouter les informations d'identification intelligentes au terminal.
- Pour supprimer des informations d'identification intelligentes Entrust d'un terminal, l'utilisateur doit désactiver les informations d'identification intelligentes dans BlackBerry UEM Client avant de désattribuer le profil ou de supprimer le certificat.

Créer un profil d'identification d'utilisateur pour utiliser des certificats du magasin de clés natif

Vous pouvez configurer le profil d'informations d'identification de l'utilisateur pour qu'il utilise les certificats du magasin de clés natif dans les situations suivantes :

- Pour autoriser les applications BlackBerry Dynamics à utiliser un certificat du magasin de clés natif sur les terminaux Android
- Pour autoriser les applications BlackBerry Dynamics à utiliser un certificat du magasin de clés natif pour accéder aux jetons cryptographiques à partir des applications PKI sur les terminaux iOS

- Pour autoriser l'application BlackBerry Access à utiliser un certificat du magasin de clés natif sur les terminaux macOS ou Windows 10

Vous pouvez autoriser les applications à utiliser tout certificat qui a été ajouté au magasin de clés ou vous pouvez définir des restrictions sur les certificats que l'application peut choisir. Par exemple, si vous utilisez une solution PKI basée sur les applications, telle que Purebred qui ajoute des certificats au magasin de clés natif, vous pouvez forcer l'application à sélectionner un certificat délivré par votre solution PKI de Purebred et exiger que l'application utilise des certificats avec les fonctionnalités spécifiées.

Remarque : « Magasin de clés natif » fait référence au magasin de clés sur le terminal. Tous les profils d'informations d'identification d'utilisateur avec des connecteurs du magasin de clés natif doivent être attribués à l'utilisateur avant de commencer à découvrir les certificats. Si un certificat répond aux exigences de plusieurs UCP, la meilleure correspondance est choisie.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Certificats > Informations d'identification de l'utilisateur**.
3. Cliquez sur +.
4. Saisissez le nom et la description du profil. Chaque profil de certificat doit avoir un nom unique.
5. Dans la liste déroulante **Connexion à l'autorité de certification**, cliquez sur **Magasin de clés natif**.
6. Dans la section **Plateformes prises en charge**, sélectionnez les types du système d'exploitation du terminal que ce profil doit prendre en charge.
7. Dans la section **Inscription de certificat**, sélectionnez **Autoriser l'inscription de certificat (facultatif)** si vous souhaitez autoriser les utilisateurs à ignorer l'inscription de certificat et à la terminer plus tard.

   Cela s'applique uniquement aux terminaux Android.
8. Pour spécifier quel certificat l'application BlackBerry Dynamics utilisera, exécutez les actions suivantes :
   a) En regard de **Émetteurs**, cliquez sur + et saisissez le nom de l'émetteur.

      Les applications BlackBerry Dynamics utiliseront uniquement un certificat si l'émetteur indiqué correspond à l'OID abrégé de OpenSSL dans le certificat. Vous pouvez copier cette valeur du certificat de l'organisme certificateur. N'insérez pas d'espace avant ou après le signe égal (=). Par exemple :

      ```
      CN=Acme_cert SMIME,OU=Acme_Legal,O=Acme,C=Can
                                CN=Acme_cert SMIME,OU=Acme_Legal,O=Acme
                                CN=Acme_cert TLS
      ```

   b) Dans la section **Utilisation de la clé**, sélectionnez les opérations prises en charge par le certificat.

      Les applications BlackBerry Dynamics utiliseront uniquement les certificats qui ont au moins la valeur d'utilisation de la clé spécifiée. Par exemple, un certificat de chiffrement peut avoir une valeur d'utilisation de clé de **Cryptage de clé**. Un certificat d'authentification peut avoir une valeur d'utilisation de clé de **Signature numérique**. Un certificat de signature peut avoir une valeur d'utilisation de clé de **Signature numérique** et **Non-répudiation**.
   c) Dans la section **Utilisation étendue de la clé**, sélectionnez les fonctions pour lesquelles le certificat a été délivré.

      Les applications BlackBerry Dynamics utiliseront seulement des certificats si toutes les valeurs d'utilisation étendue de clé sélectionnées sont présentes dans le certificat. Les certificats peuvent avoir d'autres valeurs d'utilisation étendue de clé.
   d) Si le certificat a été délivré à des fins autres que la messagerie électronique, l'authentification des clients ou la connexion à une carte à puce, sélectionnez **Utilisation d'ID d'objet supplémentaire**, cliquez sur + et spécifiez l'OID pour l'utilisation de la clé. Par exemple, si le certificat doit servir à l'authentification du serveur, il peut avoir l'OID 1.3.6.1.5.5.7.3.1
9. Si vous souhaitez que le terminal supprime les certificats ayant expiré, sélectionnez **Supprimer les certificats ayant expiré**.

Les certificats de chiffrement expirés utilisés pour S/MIME doivent être conservés sur le terminal afin de permettre aux utilisateurs de lire les messages qui ont été chiffrés avant leur expiration.

10. Si vous souhaitez que le terminal supprime les certificats dupliqués, sélectionnez **Supprimer les certificats dupliqués**. Le terminal supprime le certificat qui expire en premier.
11. Cliquez sur **Ajouter**.

À la fin :

- Autorisez les applications BlackBerry Dynamics à utiliser les certificats.
- Attribuez le profil aux comptes d'utilisateur et groupes d'utilisateurs.

Créer un profil d'informations d'identification d'utilisateur pour la connexion à votre connecteur PKI BlackBerry Dynamics

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Certificats > Informations d'identification de l'utilisateur**.
3. Cliquez sur +.
4. Saisissez le nom et la description du profil. Chaque profil de certificat doit avoir un nom unique.
5. Dans la liste déroulante **Connexion à l'autorité de certification**, sélectionnez la connexion PKI BlackBerry Dynamics que vous avez configurée.
6. Si l'utilisateur doit fournir un mot de passe pour demander un certificat, sélectionnez **Exiger un mot de passe entré par l'utilisateur ou OTP**.
7. Si vous souhaitez permettre au terminal de demander automatiquement un nouveau certificat avant l'expiration du certificat actuel, sélectionnez **Activer le renouvellement du certificat** et indiquez le nombre de jours avant l'expiration pendant lesquels les terminaux peuvent demander un nouveau certificat.
8. Si vous souhaitez que le terminal supprime les certificats ayant expiré, sélectionnez **Supprimer les certificats ayant expiré**.
9. Si vous souhaitez que le terminal supprime les certificats dupliqués, sélectionnez **Supprimer les certificats dupliqués**. Le terminal supprime le certificat qui expire en premier.
10. Cliquez sur **Ajouter**.

À la fin :

- Autorisez les applications BlackBerry Dynamics à utiliser les certificats.
- Attribuez le profil aux comptes d'utilisateur et groupes d'utilisateurs.
- Si vous mettez à jour le connecteur PKI, cliquez sur **Actualiser les fonctionnalités PKI** pour mettre à jour les fonctionnalités PKI prises en charge pour le profil.

Renouveler les certificats qui sont inscrits par le biais du connecteur PKI BlackBerry Dynamics

Si vous avez besoin de mettre à jour les certificats utilisateur pour tous les utilisateurs BlackBerry Dynamics, vous pouvez envoyer une commande pour demander le renouvèlement de certificat à tous les terminaux auxquels le profil d'informations d'identification utilisateur est attribué.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Certificats > Informations d'identification de l'utilisateur**.
3. Cliquez sur le nom du profil que vous souhaitez modifier.
4. Cliquez sur **Actualiser les fonctionnalités PKI** pour vous assurer que BlackBerry UEM dispose des détails les plus récents pour le connecteur PKI.
5. Cliquez sur **Renouveler** pour indiquer à tous les terminaux activés BlackBerry Dynamics auxquels le profil est attribué de demander le renouvèlement du certificat.

Création de profils d'identification pour les certificats d'application

Les solutions PKI basées sur des applications telles que Purebred comprennent une application installée sur un terminal qui communique avec une autorité de certification afin d'inscrire des certificats et de les ajouter au terminal. Vous pouvez utiliser une solution PKI basée sur les applications pour fournir des certificats à l'usage des applications BlackBerry Dynamics.

Pour utiliser une solution PKI basée sur les applications avec les terminaux iOS, vous devez ajouter une connexion entre BlackBerry UEM et le fournisseur PKI. Cette tâche n'est pas requise pour utiliser une solution PKI basée sur les applications uniquement avec des terminaux Android.

Si l'application PKI qui récupère les certificats de l'autorité de certification n'est pas une application BlackBerry Dynamics, le BlackBerry UEM Client communique avec l'application PKI afin d'obtenir les certificats et de les fournir aux applications BlackBerry Dynamics.

Si vous envoyez plusieurs certificats aux terminaux à l'aide de cette méthode, il est recommandé de configurer plusieurs profils d'informations d'identification de l'utilisateur avec chaque profil en utilisant un type de certificat différent. Si vous utilisez une seul instance de profil pour plusieurs certificats, rien n'indique s'il manque des certificats. Par exemple, si un profil comprend des certificats de chiffrement, de signature et d'authentification distincts et que seuls les certificats de signature et d'authentification sont importés, un message indique sur le terminal que l'importation a été effectuée avec succès, même s'il manquait le certificat de chiffrement. En revanche, si vous configurez trois profils d'informations d'identification distincts et que le certificat de chiffrement est manquant, le problème est évident.

Étapes pour l'utilisation de certificats basés sur les applications

Certaines des étapes nécessaires à l'utilisation de la solution PKI basée sur les applications de votre entreprise ne sont nécessaires que si vous utilisez la solution avec des terminaux iOS.

Étape	Action
1	Pour utiliser une solution PKI basée sur les applications avec des terminaux iOS, dans le profil BlackBerry Dynamics , sélectionnez, **Autoriser UEM Client à s'inscrire dans BlackBerry Dynamics**, puis désignez BlackBerry UEM Client pour **Délégation d'authentification d'application**.
2	Pour utiliser une solution PKI basée sur les applications avec des terminaux iOS, connectez BlackBerry UEM à la solution PKI basée sur les applications de votre entreprise.
3	Pour utiliser une solution PKI basée sur les applications avec des terminaux iOS, si l'application PKI n'est pas une application BlackBerry Dynamics, configurez BlackBerry UEM Client pour prendre en charge les certificats d'applications.
4	Configurez les applications BlackBerry Dynamics pour l'utilisation de certificats d'application.
5	Vérifiez que l'application PKI (par exemple, Purebred) est installée sur les terminaux des utilisateurs.
6	Pour utiliser la solution PKI basée sur les applications avec des terminaux iOS, créez un profil d'informations d'identification d'utilisateur pour utiliser des certificats d'application.

Étape	Action
7	Pour utiliser la solution PKI basée sur les applications avec des terminaux Android, créez un profil d'informations d'identification d'utilisateur pour utiliser des certificats du magasin de clés natif.

Configurer le BlackBerry UEM Client pour la prise en charge des certificats d'applications

Cette tâche n'est requise que si vous utilisez la solution PKI d'application de votre entreprise avec des terminaux iOS et que si l'application PKI n'est pas une application BlackBerry Dynamics.

1. Sur la console de gestion BlackBerry UEM, dans la barre de menu, cliquez sur **Applications**.
2. Dans la liste des applications, sélectionnez BlackBerry UEM Client.
3. Dans la section Configuration application, cliquez sur +.
4. Dans le champ **Nom de l'application**, saisissez le nom de l'application.
5. Dans le champ **UTI schemes**, spécifiez les schémas UTI pour la solution PKI d'application de l'organisation. Par exemple, si vous utilisez l'application Purebred, utilisez les schémas suivants : `purebred.select.all-user`, `purebred.select.no-filter`, `purebred.zip.all-user`, `purebred.zip.no-filter`.
6. Cliquez sur **Enregistrer**.
7. Attribuez le BlackBerry UEM Client avec la configuration d'application que vous avez créée aux utilisateurs et aux terminaux que vous souhaitez utiliser avec la solution PKI d'application.

Configurer les applications BlackBerry Dynamics pour l'utilisation de certificats basés sur les applications

Les applications BlackBerry Dynamics sélectionnent automatiquement le certificat à utiliser pour S/MIME et pour l'authentification via les connexions TLS en fonction de l'utilisation de la clé et des propriétés d'utilisation de la clé étendue dans les certificats. Si au moins deux certificats ont le même ensemble de propriétés, les applications peuvent ne pas être en mesure de déterminer quel certificat utiliser pour l'authentification TLS. Vous pouvez aider les applications à déterminer quel certificat utiliser en suivant les étapes ci-dessous.

1. Sur la console de gestion BlackBerry UEM, dans la barre de menus, cliquez sur **Applications**.
2. Dans la liste des applications, sélectionnez l'application (par exemple, BlackBerry Work ou BlackBerry Access).
3. Sélectionnez l'option **Autoriser les applications BlackBerry Dynamics à utiliser les certificats et profils d'informations d'identification des utilisateurs**.
4. Si vous configurez BlackBerry Work, dans la section de configuration de l'application, cliquez sur + et effectuez l'une des tâches suivantes :

Tâche	Étapes
Configurer BlackBerry Work lorsque votre entreprise utilise BEMS	a. Sur l'onglet Paramètres de configuration, sélectionnez **Les clients doivent avoir des certificats de connexion individuels (SSL) téléchargés dans le GC**. b. Pour activer la détection automatique du serveur Microsoft Exchange sur lequel se trouvent les utilisateurs, sélectionnez **Utiliser BEMS pour effectuer la découverte automatique du point de terminaison EAS/EWS pour l'utilisateur**. c. Sur l'onglet **Paramètres Exchange**, dans le champ **Nom du profil d'informations d'identification de l'utilisateur**, entrez le nom du profil d'informations d'identification de l'utilisateur.

Tâche	Étapes
Configurer BlackBerry Work lorsque votre entreprise n'utilise pas BEMS	**a.** Sélectionnez l'onglet **Paramètres Exchange**. **b.** Si votre serveur utilise le format de connexion *nom de domaine\utilisateur*, dans le champ **Domaine par défaut**, spécifiez le domaine par défaut Windows NT auquel BlackBerry Work se connecte lorsque les utilisateurs ouvrent une session. **c.** Dans le champ **Serveur Active Sync**, spécifiez le serveur Exchange ActiveSync par défaut auquel BlackBerry Work se connecte lorsque les utilisateurs se connectent à BlackBerry Work (par exemple, cas.mydomain.com). **d.** Dans le champ **URL de découverte automatique**, spécifiez l'URL de détection automatique si connue. Ceci accélère le processus de configuration de découverte automatique (par exemple, https://autodiscover.mydomain.com). **e.** Dans le champ **Délai d'expiration de la découverte automatique de connexion (iOS seulement)**, spécifiez le délai d'expiration de la détection automatique de connexion en secondes. **f.** Dans le champ **Nom du profil d'informations d'identification de l'utilisateur**, entrez le nom du profil d'informations d'identification de l'utilisateur.

5. Cliquez sur **Enregistrer**.

Créer un profil d'identification d'utilisateur pour utiliser des certificats d'application sur des terminaux iOS

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Certificats > Informations d'identification de l'utilisateur**.
3. Cliquez sur +.
4. Saisissez le nom et la description du profil. Chaque profil de certificat doit avoir un nom unique.
5. Dans la liste déroulante **Connexion à l'autorité de certification**, sélectionnez le nom de l'application que vous avez spécifiée lors de la connexion de BlackBerry UEM à votre solution PKI. Si vous utilisez Purebred, sélectionnez le BlackBerry UEM Client
6. Pour spécifier quel certificat l'application BlackBerry Dynamics utilisera, exécutez les actions suivantes :
   a) Dans la section **Utilisation de la clé**, sélectionnez les opérations prises en charge par le certificat.

      Les applications BlackBerry Dynamics utiliseront uniquement les certificats qui ont au moins la valeur d'utilisation de la clé spécifiée. Par exemple, un certificat de chiffrement peut avoir une valeur d'utilisation de clé de **Cryptage de clé**. Un certificat d'authentification peut avoir une valeur d'utilisation de clé de **Signature numérique**. Un certificat de signature peut avoir une valeur d'utilisation de clé de **Signature numérique** et **Non-répudiation**.
   b) Dans la section **Utilisation étendue de la clé**, sélectionnez les fonctions pour lesquelles le certificat a été délivré.

      Les applications BlackBerry Dynamics utiliseront seulement des certificats si toutes les valeurs d'utilisation étendue de clé sélectionnées sont présentes dans le certificat. Les certificats peuvent avoir d'autres valeurs d'utilisation étendue de clé.
   c) Si le certificat a été délivré à des fins autres que la messagerie électronique, l'authentification des clients ou la connexion à une carte à puce, sélectionnez **Utilisation d'ID d'objet supplémentaire**, cliquez sur + et spécifiez l'OID pour l'utilisation de la clé. Par exemple, si le certificat doit servir à l'authentification du serveur, il peut avoir l'OID 1.3.6.1.5.5.7.3.1
   d) En regard de **Émetteurs**, cliquez sur + et saisissez le nom de l'émetteur.

Les applications BlackBerry Dynamics utiliseront uniquement un certificat si l'émetteur indiqué correspond à l'OID abrégé de OpenSSL dans le certificat. Vous pouvez copier cette valeur du certificat de l'organisme certificateur. N'insérez pas d'espace avant ou après le signe égal (=). Par exemple :

```
CN=Acme_cert SMIME,OU=Acme_Legal,O=Acme,C=Can
                                        CN=Acme_cert SMIME,OU=Acme_Legal,O=Acme
                                        CN=Acme_cert TLS
```

7. Si vous souhaitez que le terminal supprime les certificats ayant expiré, sélectionnez **Supprimer les certificats ayant expiré**.

   Les certificats de chiffrement expirés utilisés pour S/MIME doivent être conservés sur le terminal afin de permettre aux utilisateurs de lire les messages qui ont été chiffrés avant leur expiration.
8. Si vous souhaitez que le terminal supprime les certificats dupliqués, sélectionnez **Supprimer les certificats dupliqués**. Le terminal supprime le certificat qui expire en premier.
9. Cliquez sur **Ajouter**.

À la fin :

- Autorisez les applications BlackBerry Dynamics à utiliser les certificats.
- Attribuez le profil aux comptes d'utilisateur et groupes d'utilisateurs.

Envoyer de certificats clients vers des terminaux et des applications à l'aide de SCEP

Vous pouvez utiliser des profils SCEP pour spécifier la manière dont les terminaux et les applications BlackBerry Dynamics se procurent les certificats client auprès de l'autorité de certification de votre organisation via un service SCEP. SCEP est un protocole IETF qui simplifie le processus d'inscription des certificats client sur un grand nombre de terminaux sans nécessiter d'intervention ou d'approbation de l'administrateur pour délivrer chaque certificat. Les terminaux et les applications BlackBerry Dynamics peuvent utiliser le protocole SCEP pour demander et obtenir des certificats client auprès d'une autorité de certification compatible SCEP utilisée par votre organisation.

L'autorité de certification que vous utilisez doit prendre en charge les mots de passe de vérification. L'autorité de certification utilise les mots de passe de vérification pour vérifier que le terminal ou l'application est autorisé(e) à envoyer une demande de certificat.

Pour utiliser SCEP dans un environnement BlackBerry UEM Cloud, vous devez installer la version la plus récente de BlackBerry Connectivity Node afin de permettre à BlackBerry UEM Cloud d'accéder à votre répertoire d'entreprise.

Si votre organisation utilise une autorité de certification Entrust ou OpenTrust, les profils SCEP ne sont pas pris en charge pour les terminaux Windows 10.

Créer un profil SCEP

Les paramètres de profil requis dépendent de la configuration du service SCEP dans l'environnement de votre entreprise et varient si le certificat est utilisé par une application BlackBerry Dynamics ou par un type de terminal spécifié.

Vous pouvez utiliser une variable dans un champ de texte pour faire référence à une valeur plutôt que de spécifier la valeur réelle.

Remarque : Si vous souhaitez utiliser un profil SCEP pour distribuer des certificats client OpenTrust aux terminaux, vous devez appliquer un correctif à votre logiciel OpenTrust. Pour plus d'informations, contactez votre représentant de support technique OpenTrust et indiquez la référence de support SUPPORT-798.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Certificats > SCEP**.
3. Cliquez sur +.
4. Saisissez le nom et la description du profil. Chaque profil de certificat doit avoir un nom unique.
5. Dans la liste déroulante **Connexion à l'autorité de certification**, effectuez l'une des opérations suivantes :
   - Pour utiliser une connexion Entrust que vous avez configurée, cliquez sur la connexion qui convient. Dans la liste déroulante **Profil**, cliquez sur un profil. Spécifiez les valeurs du profil.
   - Pour utiliser une connexion OpenTrust que vous avez configurée, cliquez sur la connexion qui convient. Dans la liste déroulante **Profil**, cliquez sur un profil. Spécifiez les valeurs du profil.
     - Les paramètres suivants du profil SCEP ne s'appliquent pas aux certificats client OpenTrust : Utilisation de la clé, Utilisation étendue de la clé, Objet et SAN.
   - Pour utiliser une autre autorité de certification, cliquez sur **Générique**. Dans la liste déroulante **Type de challenge SCEP**, sélectionnez **Statique** ou **Dynamique**, puis spécifiez les paramètres requis pour le type de vérification.

     Remarque : Pour les terminaux Windows, seuls les mots de passe statiques sont pris en charge.
6. Dans le champ **URL**, saisissez l'URL du service SCEP. L'URL doit inclure le protocole, le FQDN, le numéro de port et le chemin SCEP.
7. Dans le champ **Nom de l'instance**, saisissez le nom de l'instance pour l'autorité de certification.
8. Vous pouvez également décocher la case correspondant aux types de terminaux pour lesquels vous ne souhaitez pas configurer le profil.
9. Procédez comme suit :
   a) Cliquez sur l'onglet correspondant à un type de terminal.
   b) Configurez les valeurs qui conviennent pour chaque paramètre de profil afin qu'elles correspondent à la configuration du service SCEP dans l'environnement de votre organisation.
10. Répétez l'étape 8 pour chaque type de terminal de votre organisation.
11. Cliquez sur **Ajouter**.

À la fin : Si les terminaux utilisent le certificat client pour s'authentifier auprès d'un réseau Wi-Fi professionnel, d'un VPN professionnel ou d'un serveur de messagerie professionnel, associez le profil SCEP à un profil Wi-Fi, un profil VPN ou un profil de messagerie.

Paramètres du profil SCEP

Les profils SCEP sont pris en charge sur les types de terminaux suivants :

- iOS
- macOS
- Android
- Windows 10

Communs : paramètres de profil SCEP

Commun : paramètre de profil SCEP	Description
Connexion à l'autorité de certification	Ce paramètre spécifie si l'autorité de certification correspond à Entrust, à OpenTrust ou à une autre autorité de certification. Si vous avez configuré une ou plusieurs connexions au logiciel Entrust ou OpenTrust de votre entreprise, vous pouvez en sélectionner une dans la liste déroulante. Sélectionnez Générique si vous utilisez une autre autorité de certification. Si vous sélectionnez une connexion Entrust ou OpenTrust, vous devez ensuite sélectionner le profil PKI qui convient et spécifier les valeurs nécessaires. Les profils disponibles varient en fonction de ce que l'administrateur Entrust ou OpenTrust a configuré dans le logiciel PKI. La valeur par défaut est Générique.
URL	Ce paramètre spécifie l'URL du service SCEP. L'URL doit inclure le protocole, le FQDN, le numéro de port et le chemin SCEP (chemin CGI défini dans la spécification SCEP). Vous devez définir la valeur de ce paramètre pour bien activer un terminal. Les URL SCEP HTTPS sont prises en charge par les terminaux iOS.
Nom de l'instance	Ce paramètre spécifie le nom de l'instance CA. La valeur peut correspondre à n'importe quelle chaine comprise par le service SCEP. Par exemple, il peut s'agir d'un nom de domaine comme exemple.org. Si une autorité de certification dispose de plusieurs certificats d'autorité de certification, ce champ permet de distinguer le certificat requis.
Vérifier la chaine de confiance de la connexion au serveur SCEP	Ce paramètre indique si BlackBerry UEM vérifie que l'autorité de certification racine du serveur SCEP est stockée dans le magasin de certificats BlackBerry UEM pour que BlackBerry UEM puisse faire confiance au serveur SCEP lors du test des connexions, de la récupération des mots de passe de vérification et lorsqu'il agit en tant que proxy pour les requêtes SCEP émises par les terminaux.
Type de challenge SCEP	Ce paramètre spécifie si le mot de passe de vérification SCEP est généré de manière dynamique ou fourni en tant que mot de passe statique. Si ce paramètre est défini sur Statique, chaque terminal utilise le même mot de passe de vérification. Si ce paramètre est défini sur Dynamique, chaque terminal reçoit un mot de passe de vérification unique. Valeurs possibles : • Statique • Dynamique La valeur par défaut est Dynamique. Pour les terminaux Windows, seuls les mots de passe Statiques sont pris en charge.

Commun : paramètre de profil SCEP	Description
URL de génération d'un mot de passe de vérification	Ce paramètre spécifie l'URL utilisée par les terminaux pour obtenir un mot de passe généré de manière dynamique à partir du service SCEP. L'URL doit inclure le protocole, le FQDN, le numéro de port et le chemin SCEP (chemin CGI défini dans la spécification SCEP). Ce paramètre est valide uniquement si le paramètre Type de challenge SCEP est défini sur Dynamique.
Type d'authentification	Ce paramètre spécifie le type d'authentification utilisé par les terminaux pour se connecter au service SCEP et obtenir un mot de passe de vérification. Ce paramètre est valide uniquement si le paramètre Type de challenge SCEP est défini sur Dynamique. Valeurs possibles : • De base • NTLM La valeur par défaut est De base.
Domaine	Ce paramètre spécifie le domaine utilisé pour l'authentification NTLM lorsque les terminaux se connectent au service SCEP afin d'obtenir un mot de passe de vérification. Ce paramètre est valide uniquement si le paramètre Type d'authentification est défini sur NTLM.
nom d'utilisateur ;	Ce paramètre spécifie le nom d'utilisateur requis pour obtenir un mot de passe de vérification à partir du service SCEP. Ce paramètre est valide uniquement si le paramètre Type de challenge SCEP est défini sur Dynamique.
Mot de passe	Ce paramètre spécifie le mot de passe requis pour obtenir le mot de passe de vérification à partir du service SCEP. Ce paramètre est valide uniquement si le paramètre Type de challenge SCEP est défini sur Dynamique.
Mot de passe de vérification	Ce paramètre spécifie le mot de passe de vérification utilisé par un terminal pour inscrire le certificat. Ce paramètre est valide uniquement si le paramètre Type de challenge SCEP est défini sur Statique.

iOS : Paramètres du profil SCEP

iOS : paramètre Profil SCEP	Description
Utiliser BlackBerry UEM comme proxy pour les demandes SCEP	Ce paramètre spécifie si toutes les demandes SCEP des terminaux sont envoyées via BlackBerry UEM. Si l'autorité de certification se situe derrière votre pare-feu, ce paramètre vous permet d'inscrire des certificats client pour les terminaux sans exposer l'autorité de certification en dehors du pare-feu.
Utiliser BlackBerry Connectivity Node pour la connectivité à l'autorité de certification	Ce paramètre indique si les demandes SCEP doivent être acheminées via BlackBerry Connectivity Node. Ce paramètre s'affiche uniquement dans BlackBerry UEM Cloud.
Objet	Ce paramètre spécifie l'objet du certificat, si requis pour la configuration SCEP de votre organisation. Saisissez l'objet au format « /CN=<*nom_commun*>/O=<*nom_domaine*> ». Si le profil concerne plusieurs utilisateurs, vous pouvez utiliser une variable, par exemple : %UserDistinguishedName%.
Nouvelles tentatives	Ce paramètre spécifie le nombre de nouvelles tentatives de connexion au service SCEP si la tentative de connexion échoue. Les valeurs possibles sont comprises entre 1 et 999. La valeur par défaut est 3.
Délai de nouvelle tentative	Ce paramètre spécifie le délai d'attente, en secondes, avant une nouvelle tentative de connexion au service SCEP. Les valeurs possibles sont comprises entre 1 et 999. La valeur par défaut est de 10 secondes.
Taille de la clé	Ce paramètre spécifie la taille de la clé du certificat. Valeurs possibles : • 1 024 • 2 048 • 4 096 La valeur par défaut est 1 024.
Empreinte	Ce paramètre spécifie l'empreinte d'inscription d'un certificat SCEP. Si votre autorité de certification utilise HTTP plutôt que HTTPS, les terminaux utilisent l'empreinte pour confirmer l'identité de l'autorité de certification lors du processus d'inscription. L'empreinte digitale ne peut pas contenir d'espace.

iOS : paramètre Profil SCEP	Description
Type SAN	Ce paramètre spécifie le type d'autre nom d'objet du certificat, si nécessaire. Valeurs possibles : • Aucun • Nom RFC822 • Nom DNS • Uniform Resource Identifier (Identificateur de ressources uniformes) La valeur par défaut est Aucune.
Valeur SAN	Ce paramètre spécifie l'autre représentation de l'objet du certificat. La valeur doit correspondre à une adresse électronique, le nom DNS du serveur CA ou l'URL complète du serveur. Le paramètre Type SAN détermine le type de valeur que vous spécifiez. Si cette option est définie sur Nom RFC822, la valeur doit correspondre à une adresse électronique valide. Si cette option est définie sur URI, la valeur doit correspondre à une URL valide incluant le protocole et le FQDN ou l'adresse IP. Si cette option est définie sur Nom principal, la valeur doit correspondre à un nom principal valide. Si cette option est définie sur Nom DN, la valeur doit correspondre à un FQDN valide.
Nom principal NT	Ce paramètre spécifie le Nom principal NT pour la génération du certificat. Ce paramètre est valide uniquement si le paramètre Type SAN est défini sur un autre paramètre que Aucun.
Expiration du profil	Indiquez le nombre de jours qui doit s'écouler après l'émission d'un certificat, avant que le terminal ne demande un nouveau certificat à l'autorité de certification. La valeur doit être inférieure à la période de validité du certificat définie par l'autorité de certification. La valeur par défaut est de 1 825 jours.

macOS : Paramètres du profil SCEP

macOS applique les profils aux terminaux ou comptes d'utilisateur. Vous pouvez configurer un profil SCEP à appliquer à l'un ou à l'autre.

macOS : paramètre Profil SCEP	Description
Utiliser BlackBerry UEM comme proxy pour les demandes SCEP	Ce paramètre spécifie si toutes les demandes SCEP des terminaux sont envoyées via BlackBerry UEM. Si l'autorité de certification se situe derrière votre pare-feu, ce paramètre vous permet d'inscrire des certificats client pour les terminaux sans exposer l'autorité de certification en dehors du pare-feu.

macOS : paramètre Profil SCEP	Description
Utiliser BlackBerry Connectivity Node pour la connectivité à l'autorité de certification	Ce paramètre indique si les demandes SCEP doivent être acheminées via BlackBerry Connectivity Node. Ce paramètre s'affiche uniquement dans BlackBerry UEM Cloud.
Appliquer le profil à	Ce paramètre indique si le profil SCEP est appliqué au compte d'utilisateur ou au terminal. Valeurs possibles : • Utilisateur • Terminal
Objet	Ce paramètre spécifie l'objet du certificat, si requis pour la configuration SCEP de votre organisation. Saisissez l'objet au format « /CN=<*nom_commun*>/O=<*nom_domaine*> ». Si le profil concerne plusieurs utilisateurs, vous pouvez utiliser une variable, par exemple : %UserDistinguishedName%.
Nouvelles tentatives	Ce paramètre spécifie le nombre de nouvelles tentatives de connexion au service SCEP si la tentative de connexion échoue. Les valeurs possibles sont comprises entre 1 et 999. La valeur par défaut est 3.
Délai de nouvelle tentative	Ce paramètre spécifie le délai d'attente, en secondes, avant une nouvelle tentative de connexion au service SCEP. Les valeurs possibles sont comprises entre 1 et 999. La valeur par défaut est de 10 secondes.
Taille de la clé	Ce paramètre spécifie la taille de la clé du certificat. Valeurs possibles : • 1 024 • 2 048 La valeur par défaut est 1 024.
Empreinte	Ce paramètre spécifie l'empreinte d'inscription d'un certificat SCEP. Si votre autorité de certification utilise HTTP plutôt que HTTPS, les terminaux utilisent l'empreinte pour confirmer l'identité de l'autorité de certification lors du processus d'inscription. L'empreinte digitale ne peut pas contenir d'espace.

macOS : paramètre Profil SCEP	Description
Type SAN	Ce paramètre spécifie le type d'autre nom d'objet du certificat, si nécessaire. Valeurs possibles : • Aucun • Nom RFC822 • Nom DNS • Uniform Resource Identifier (Identificateur de ressources uniformes) La valeur par défaut est Aucune.
Valeur SAN	Ce paramètre spécifie l'autre représentation de l'objet du certificat. La valeur doit correspondre à une adresse électronique, le nom DNS du serveur CA ou l'URL complète du serveur. Le paramètre Type SAN détermine le type de valeur que vous spécifiez. Si cette option est définie sur Nom RFC822, la valeur doit correspondre à une adresse électronique valide. Si cette option est définie sur URI, la valeur doit correspondre à une URL valide incluant le protocole et le FQDN ou l'adresse IP. Si cette option est définie sur Nom principal, la valeur doit correspondre à un nom principal valide. Si cette option est définie sur Nom DN, la valeur doit correspondre à un FQDN valide.
Nom principal NT	Ce paramètre spécifie le Nom principal NT pour la génération du certificat. Ce paramètre est valide uniquement si le paramètre Type SAN est défini sur un autre paramètre que Aucun.

Android : paramètres de profil SCEP

Pour obtenir un exemple de profil SCEP pour les terminaux Android, rendez-vous sur support.blackberry.com/community et lisez l'article 38248.

Android : paramètre de profil SCEP	Description
Utiliser BlackBerry UEM comme proxy pour les demandes SCEP	Ce paramètre spécifie si toutes les demandes SCEP des terminaux sont envoyées via BlackBerry UEM. Si l'autorité de certification se situe derrière votre pare-feu, ce paramètre vous permet d'inscrire des certificats client pour les terminaux sans exposer l'autorité de certification en dehors du pare-feu.
Masquer le certificat sur les terminaux Android Enterprise	Ce paramètre indique si le certificat est visible pour les utilisateurs sur les terminaux Android version 9.0 et ultérieureAndroid Enterprise. Si le certificat est masqué, les utilisateurs ne peuvent pas le sélectionner pour l'utiliser à d'autres fins.
Utiliser BlackBerry Connectivity Node pour la connectivité à l'autorité de certification	Ce paramètre indique si les demandes SCEP doivent être acheminées via BlackBerry Connectivity Node. Ce paramètre s'affiche uniquement dans BlackBerry UEM Cloud.

Android : paramètre de profil SCEP	Description
Algorithme de cryptage	Ce paramètre spécifie l'algorithme de cryptage utilisé par les terminaux Android pour la demande d'inscription de certificat. Valeurs possibles : • Aucun • Triple DES • AES (128 bits) • AES (196 bits) • AES (256 bits) La valeur par défaut est Triple DES.
Fonction de hachage	Ce paramètre spécifie la fonction de hachage utilisée par les terminaux Android pour la demande d'inscription de certificat. Valeurs possibles : • Aucun • SHA-1 • SHA-224 • SHA-256 • SHA-384 • SHA-512 La valeur par défaut est SHA-1.
Empreinte de certificat	Ce paramètre spécifie le hachage codé au format hexadécimal du certificat racine de l'autorité de certification. Vous pouvez utiliser les algorithmes suivants pour spécifier l'empreinte : SHA-1, SHA-224, SHA-256, SHA-384 et SHA-512. Vous devez définir la valeur de ce paramètre pour bien activer les terminaux Android Enterprise ou Samsung Knox.
Renouvellement automatique	Ce paramètre spécifie le nombre de jours avant renouvellement automatique d'un certificat qui arrive à expiration. Les valeurs possibles sont 1 à 365. La valeur par défaut est 30.
Android Enterprise/Samsung KNOX	
Objet	Ce paramètre spécifie l'objet du certificat, si requis pour la configuration SCEP de votre organisation. Saisissez l'objet au format « /CN=<*common_name*>/O=<*domain_name*> » Si le profil concerne plusieurs utilisateurs, vous pouvez utiliser une variable (%UserDistinguishedName%, par exemple).

Android : paramètre de profil SCEP	Description
Type SAN	Ce paramètre spécifie le type d'autre nom d'objet du certificat, si nécessaire. Valeurs possibles : • Nom RFC 822 • Uniform Resource Identifier (Identificateur de ressources uniformes) • Nom principal NT • Nom DNS La valeur par défaut est Nom RFC 822.
Valeur SAN	Ce paramètre spécifie l'autre représentation de l'objet de certificat. La valeur doit correspondre à une adresse électronique, le nom DNS du serveur CA, l'URL complète du serveur ou le nom principal. Le paramètre Type SAN détermine le type de valeur que vous spécifiez. Si cette option est définie sur Nom RFC822, la valeur doit correspondre à une adresse électronique valide. Si cette option est définie sur URI, la valeur doit correspondre à une URL valide incluant le protocole et le FQDN ou l'adresse IP. Si cette option est définie sur Nom principal, la valeur doit correspondre à un nom principal valide. Si cette option est définie sur Nom DN, la valeur doit correspondre à un FQDN valide.
Algorithme de clé	Ce paramètre spécifie l'algorithme utilisé par les terminaux Android Enterprise et Samsung Knox pour générer la paire de clés client. Vous devez sélectionner un algorithme pris en charge par votre autorité de certification. Valeurs possibles : • Aucun • RSA • ECC La valeur par défaut est RSA.
Puissance RSA	Ce paramètre spécifie la puissance RSA utilisée par les terminaux Android Enterprise et Samsung Knox pour générer la paire de clés client. Vous devez saisir une force de clé prise en charge par votre autorité de certification. Ce paramètre est valide uniquement si le paramètre Algorithme de clé est défini sur RSA. Valeurs possibles : • 1 024 • 2 048 • 4 096 • 8 192 • 16 384 La valeur par défaut est 1 024.

Android : paramètre de profil SCEP	Description
Utilisation de la clé	Ce paramètre spécifie les opérations cryptographiques pouvant être effectuées à l'aide de la clé publique contenue dans le certificat. Sélections possibles : • Signature numérique • Non-répudiation • Cryptage de clé • Cryptage de données • Accord de la clé • Signature du certificat clé • Signature CRL • Crypter uniquement • Décrypter uniquement Les sélections par défaut sont Signature numérique, Cryptage de clé et Accord de la clé.
Utilisation étendue de la clé	Ce paramètre spécifie l'objectif de la clé contenue dans le certificat. Sélections possibles : • Authentification du serveur • Authentification du client • Signature de code • Protection des e-mails • Horodatage • Signature OCSP • Client Secure Shell • Serveur Secure Shell La sélection par défaut est Authentification du client.

Windows 10 : paramètres de profil SCEP

Windows 10 : paramètre de profil SCEP	Description
Magasin de certificats utilisateur	Ce paramètre spécifie si le certificat est stocké à l'emplacement des certificats utilisateur sur le terminal.
Objet	Ce paramètre spécifie l'objet du certificat, si requis pour la configuration SCEP de votre organisation. Saisissez l'objet au format « /CN=<*common_name*>/O=<*domain_name*> » Si le profil concerne plusieurs utilisateurs, vous pouvez utiliser une variable (%UserDistinguishedName%, par exemple).

Windows 10 : paramètre de profil SCEP	Description
Type SAN	Ce paramètre spécifie le type d'autre nom d'objet du certificat, si nécessaire. Valeurs possibles : • Aucun • Nom RFC 822 • Nom DNS • Uniform Resource Identifier (Identificateur de ressources uniformes) La valeur par défaut est Aucune.
Valeur SAN	Ce paramètre spécifie l'autre représentation de l'objet du certificat. La valeur doit correspondre à une adresse électronique, le nom DNS du serveur CA ou l'URL complète du serveur. La valeur appropriée pour ce paramètre dépend de la valeur sélectionnée pour le paramètre Type SAN.
Nouvelles tentatives	Ce paramètre spécifie le nombre de nouvelles tentatives de connexion au service SCEP si la tentative de connexion échoue. Les valeurs possibles sont comprises entre 1 et 999. La valeur par défaut est 3.
Délai de nouvelle tentative	Ce paramètre spécifie le délai d'attente, en secondes, avant une nouvelle tentative de connexion au service SCEP. Les valeurs possibles sont comprises entre 1 et 999. La valeur par défaut est de 10 secondes.
Taille de la clé	Ce paramètre spécifie la taille de la clé du certificat. Valeurs possibles : • 1 024 • 2 048 • 4 096 • 8 192 • 16 384 La valeur par défaut est 1 024.

Windows 10 : paramètre de profil SCEP	Description
Utilisation de la clé	Ce paramètre spécifie les opérations cryptographiques pouvant être effectuées à l'aide de la clé publique contenue dans le certificat. • Signature numérique • Non-répudiation • Cryptage de clé • Cryptage de données • Accord de la clé • Signature du certificat clé • Signature CRL • Crypter uniquement Les sélections par défaut sont « Signature du certificat clé » et « Crypter uniquement ».
Utilisation étendue de la clé	Ce paramètre spécifie l'objectif de la clé contenue dans le certificat. • Authentification du serveur • Authentification du client • Signature de code • Protection des e-mails • Horodatage • Signature OCSP • Client Secure Shell • Serveur Secure Shell La sélection par défaut est Authentification du client.
Stockage de clés SCEP	Ce paramètre spécifie l'emplacement de stockage de la clé privée. Valeurs possibles : • TPM • TMP si pris en charge • KSP La valeur par défaut est « KSP ».
Fonction de hachage	Ce paramètre spécifie la fonction de hachage utilisée par un terminal Windows 10 pour la demande d'inscription de certificat. Valeurs possibles : • SHA-1 • SHA-224 • SHA-256 • SHA-384 • SHA-512 La valeur par défaut est SHA-1.

Windows 10 : paramètre de profil SCEP	Description
Empreinte de certificat	Ce paramètre spécifie le hachage codé au format hexadécimal du certificat racine de l'autorité de certification. Vous pouvez utiliser les algorithmes suivants pour spécifier l'empreinte : SHA-1, SHA-224, SHA-256, SHA-384 et SHA-512.
Renouvellement automatique	Ce paramètre spécifie le nombre de jours avant renouvellement automatique d'un certificat qui arrive à expiration. Les valeurs possibles sont 1 à 365. La valeur par défaut est 30.

BlackBerry Dynamics : paramètres de profil SCEP

Ces paramètres s'appliquent aux certificats SCEP utilisés avec les applications BlackBerry Dynamics sur les terminaux iOS et Android.

BlackBerry Dynamics : paramètre de profil SCEP	Description
Objet	Ce paramètre spécifie l'objet du certificat, si requis pour la configuration SCEP de votre organisation. Saisissez l'objet au format « /CN=<*nom_commun*>/O=<*nom_domaine*> ». Si le profil concerne plusieurs utilisateurs, vous pouvez utiliser une variable (%UserDistinguishedName%, par exemple).
Type SAN	Ce paramètre spécifie le type d'autre nom d'objet du certificat, si nécessaire. Valeurs possibles : • Nom RFC 822 • Uniform Resource Identifier (Identificateur de ressources uniformes) • Nom principal NT • Nom DNS La valeur par défaut est Nom RFC 822.
Valeur SAN	Ce paramètre spécifie l'autre représentation de l'objet de certificat. La valeur doit correspondre à une adresse électronique, le nom DNS du serveur CA, l'URL complète du serveur ou le nom principal. Le paramètre Type SAN détermine le type de valeur que vous spécifiez. Si cette option est définie sur Nom RFC822, la valeur doit correspondre à une adresse électronique valide. Si cette option est définie sur URI, la valeur doit correspondre à une URL valide incluant le protocole et le FQDN ou l'adresse IP. Si cette option est définie sur Nom principal, la valeur doit correspondre à un nom principal valide. Si cette option est définie sur Nom DN, la valeur doit correspondre à un FQDN valide.

BlackBerry Dynamics : paramètre de profil SCEP	Description
Algorithme de clé	Ce paramètre spécifie l'algorithme utilisé pour générer la paire de clés client. Vous devez sélectionner un algorithme pris en charge par votre autorité de certification. Valeurs possibles : • RSA
Puissance RSA	Ce paramètre spécifie la puissance RSA utilisée pour générer la paire de clés client. Vous devez saisir une force de clé prise en charge par votre autorité de certification. Ce paramètre est valide uniquement si le paramètre Algorithme de clé est défini sur RSA. Valeurs possibles : • 2 048 • 4 096 La valeur par défaut est 2048.
Algorithme de cryptage	Ce paramètre spécifie l'algorithme de chiffrement utilisé pour la demande d'inscription de certificat. Valeurs possibles : • Triple DES • AES (128 bits) • AES (196 bits) • AES (256 bits) La valeur par défaut est Triple DES.
Fonction de hachage	Ce paramètre spécifie la fonction de hachage utilisée pour la demande d'inscription de certificat. Valeurs possibles : • SHA-256 • SHA-384 • SHA-512 La valeur par défaut est « SHA-256 ».
Empreinte de certificat	Ce paramètre spécifie le hachage codé au format hexadécimal du certificat racine de l'autorité de certification. Vous pouvez utiliser l'un des algorithmes suivants pour spécifier l'empreinte : SHA-1, SHA-224, SHA-256, SHA-384 et SHA-512. L'algorithme MD5 n'est pris en charge que si l'option Activer le mode FIPS n'est pas sélectionnée dans le profil BlackBerry Dynamics.
Renouvellement automatique	Ce paramètre spécifie le nombre de jours avant renouvellement automatique d'un certificat qui arrive à expiration. Les valeurs possibles sont 1 à 365. La valeur par défaut est 30.

BlackBerry Dynamics : paramètre de profil SCEP	Description
Utilisation de la clé	Ce paramètre spécifie les opérations cryptographiques pouvant être effectuées à l'aide de la clé publique contenue dans le certificat. Sélections possibles : • Signature numérique • Non-répudiation • Cryptage de clé • Cryptage de données • Accord de la clé • Signature du certificat clé • Signature CRL • Crypter uniquement • Décrypter uniquement Les sélections par défaut sont Signature numérique, Cryptage de clé et Accord de la clé.
Utilisation étendue de la clé	Ce paramètre spécifie l'objectif de la clé contenue dans le certificat. Sélections possibles : • Authentification du serveur • Authentification du client • Signature de code • Protection des e-mails • Horodatage • Signature OCSP • Client Secure Shell • Serveur Secure Shell La sélection par défaut est Authentification du client.
Restrictions d'applications	Ce paramètre spécifie les applications BlackBerry Dynamics qui peuvent utiliser le certificat. Valeurs possibles : • Autoriser toutes les applications à utiliser des certificats • Autoriser les applications spécifiées à utiliser des certificats La sélection par défaut est Autoriser toutes les applications à utiliser des certificats.
Applications autorisées à utiliser SCEP	Ce paramètre spécifie les applications BlackBerry Dynamics autorisées à utiliser des certificats SCEP. Ce paramètre est valide uniquement si le paramètre Restrictions d'applications est défini sur Autoriser les applications spécifiées à utiliser des certificats.
Supprimer les certificats expirés	Ce paramètre spécifie si le terminal supprime les certificats expirés.

BlackBerry Dynamics : paramètre de profil SCEP	Description
Supprimer les certificats en double	Ce paramètre spécifie si le terminal supprime les certificats en double. Le terminal supprime le certificat qui expire en premier.

Envoi du même certificat client à plusieurs terminaux

Vous pouvez utiliser des profils de certificat partagés pour envoyer des certificats client aux terminaux iOS, macOS et Android.

Les profils de certificats partagés envoient la même paire de clés à chaque utilisateur affecté au profil. Utilisez uniquement les profils de certificat partagé pour autoriser plusieurs utilisateurs à partager un certificat client.

macOS applique les profils aux terminaux ou comptes d'utilisateur. Vous pouvez configurer un profil de certificat partagé à appliquer à l'un ou à l'autre.

Créer un profil de certificat partagé

Avant de commencer : vous devez obtenir le fichier de certificat client que vous souhaitez envoyer aux terminaux. Le nom du fichier de certificat doit comprendre l'extension .pfx ou .p12.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Certificats > Certificat partagé**.
3. Cliquez sur +.
4. Saisissez le nom et la description du profil. Chaque profil de certificat doit avoir un nom unique. Certains noms (par exemple, ca_1) sont réservés.
5. Dans le champ **Mot de passe**, indiquez un mot de passe pour le profil de certificat partagé.
6. Dans le champ **Fichier de certificat**, cliquez sur **Parcourir** pour localiser le fichier de certificat.
7. Si vous gérez des terminaux Android Enterprise et que vous souhaitez éviter que les utilisateurs ne sélectionnent le certificat pour l'utiliser à d'autres fins, sélectionnez **Masquer le certificat sur les terminaux Android Enterprise** dans l'onglet **Android**. Cette option s'applique uniquement à Android 9.0 et versions ultérieures.
8. Si vous gérez des terminaux macOS, sous l'onglet **macOS**, dans la liste déroulante **Appliquer le profil à**, sélectionnez **Utilisateur** ou **Terminal**.
9. Cliquez sur **Ajouter**.

Spécifier le certificat utilisé par une application

Pour les terminaux Android, vous pouvez utiliser un profil de mappage de certificat pour spécifier les certificats client que les applications utilisent. Le profil de mappage de certificat n'est pas pris en charge pour les applications BlackBerry Dynamics.

Les profils de mappage de certificat vous permettent de spécifier les certificats que les applications Android utilisent. Vous pouvez exiger qu'une application utilise un certificat envoyé au terminal par un profil SCEP, les identifiants de l'utilisateur ou un certificat partagé. Vous pouvez utiliser un certificat avec une ou plusieurs applications spécifiées ou toutes les applications gérées. Vous pouvez également spécifier si une application utilise un certificat chaque fois qu'il est nécessaire ou uniquement pour des connexions à un URI spécifique.

Les mappages de certificat multiples peuvent être spécifiés dans un profil unique. Un seul profil de mappage de certificat peut être attribué à un utilisateur.

Créer un profil de mappage de certificat

Avant de commencer : Créez les profils SCEP, d' informations d'identification de l'utilisateur ou de certificats partagés requis pour envoyer des certificats aux terminaux et attribuer les profils aux utilisateurs ou aux groupes.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur Certificats > Cartographie de certificat.
3. Cliquez sur +.
4. Saisissez le nom et la description du profil. Chaque profil de certificat doit avoir un nom unique.
5. Dans la table de mappage, cliquez sur +.
6. Sous **URI de la destination**, sélectionnez l'une des options suivantes :
   - Sélectionnez **Aucun(e)** pour que l'application n'utilise pas le certificat pour authentifier une connexion avec une ressource.
   - Sélectionnez **Toute** pour que l'application utilise le certificat pour authentifier une connexion avec n'importe quelle ressource.
   - Sélectionnez **Port:hôte spécifié** et saisissez l'hôte et le port si l'application peut utiliser le certificat pour l'authentification avec une ressource spécifique.
7. Sous **Certificat d'application**, effectuez l'une des opérations suivantes :
   - Pour spécifier que l'application doit utiliser un certificat envoyé au terminal par un autre profil, sélectionnez **Certificat sélectionné**, puis le nom du profil dans la liste déroulante.
   - Pour spécifier que l'application doit utiliser un certificat envoyé au terminal par une source tierce, sélectionnez **Alias de certificat** et saisissez l'alias du certificat. Si vous ne connaissez pas l'alias, consultez la documentation ou l'administrateur pour connaitre le fournisseur de certificats.
   - Pour spécifier que l'application doit utiliser un certificat envoyé au terminal par un autre profil, sélectionnez **Certificat sélectionné**, puis le nom du profil dans la liste déroulante.
8. Sous **Applications autorisées pour l'URI de destination**, effectuez l'une des actions suivantes :
   - Pour autoriser toutes les applications gérées à demander le certificat spécifié, sélectionnez **Toutes les applications de l'espace Travail**.
   - Pour autoriser uniquement les applications spécifiées à demander le certificat, sélectionnez **Applications spécifiées** et cliquez sur + pour spécifier une ou plusieurs applications.
9. Si nécessaire, répétez les étapes 5 à 8 pour ajouter d'autres mappages au profil.
10. Cliquez sur **Ajouter**.

À la fin :

- Attribuez le profil aux comptes d'utilisateur et groupes d'utilisateurs.
- Si nécessaire, classez les profils.

Gestion des certificats clients pour les comptes d'utilisateur

Vous pouvez ajouter des certificats clients directement à des comptes d'utilisateur individuels ou à un profil d'informations d'identification de l'utilisateur affecté au compte d'utilisateur. L'ajout de certificats directement à un compte d'utilisateur est pris en charge pour les terminaux compatibles BlackBerry Dynamics, ou les autres terminaux gérés iOS et Android. Le téléchargement de certificats dans des profils d'informations d'identification d'utilisateur est pris en charge pour les terminaux iOS et les terminaux Android Enterprise.

Pour permettre aux utilisateurs de charger les certificats leur permettant de se connecter à votre réseau Wi-Fi professionnel, VPN professionnel et serveur de messagerie professionnel, utilisez un profil d'informations d'identification de l'utilisateur qui peut être associé à Wi-Fi, un VPN ou un e-mail

Si vous disposez d'un environnement sur site et que vous chargez des certificats pour les applications BlackBerry Dynamics vers des comptes d'utilisateur, vous devez configurer une valeur TTL pour les certificats utilisateur. Au terme de la valeur TTL, les certificats sont supprimés du serveur.

Ajouter un certificat client à un compte d'utilisateur

Vous pouvez ajouter un certificat client à un compte d'utilisateur individuel et envoyer ce certificat aux terminaux BlackBerry Dynamics activés ou à d'autres terminaux iOS et Android gérés.

Ajoutez des certificats client aux comptes d'utilisateurs lorsque les terminaux des utilisateurs ont besoin de certificats pour S/MIME ou l'authentification des clients et que le certificat ne peut pas être envoyé aux terminaux par le biais d'un profil d'informations d'identification de l'utilisateur ou d'un profil SCEP.

Le certificat client doit porter une extension .pfx ou .p12. Vous pouvez envoyer plusieurs certificats client aux terminaux.

Vous pouvez également utiliser les profils d'informations d'identification de l'utilisateur pour charger les certificats des utilisateurs individuels. Les profils d'informations d'identification de l'utilisateur peuvent être associés à un profil Wi-Fi, VPN ou de messagerie.

1. Sur la barre de menus, cliquez sur **Utilisateurs > Terminaux gérés**.
2. Recherchez un compte d'utilisateur.
3. Dans les résultats de la recherche, cliquez sur le nom d'un compte d'utilisateur.
4. Dans la section **Stratégie informatique et profils**, cliquez sur +.
5. Cliquez sur **Certificat utilisateur**.
6. Saisissez la description du certificat.
7. Dans la section **Appliquer le certificat à**, sélectionnez l'un des éléments suivants :
   - **Autres terminaux gérés** : choisissez cette option pour envoyer le certificat aux terminaux iOS et Android pour tous les usages pris en charge autres que pour des applications BlackBerry Dynamics.
   - **Terminaux BlackBerry Dynamics activés** : choisissez cette option pour envoyer le certificat aux terminaux à des fins d'utilisation avec des applications BlackBerry Dynamics.
8. Dans le champ **Fichier de certificat**, cliquez sur **Parcourir** pour localiser le fichier de certificat.
9. Si vous avez sélectionné **Autres terminaux gérés**, dans le champ **Mot de passe**, saisissez un mot de passe pour le certificat. Pour les terminaux iOS, un mot de passe est requis. Pour les terminaux Android, vous n'avez pas à fournir de mot de passe dans BlackBerry UEM si le terminal exécute la version la plus récente de BlackBerry UEM Client. Si vous ne définissez aucun mot de passe, l'utilisateur doit saisir le mot de passe du terminal.

10. Cliquez sur **Ajouter**.
    Le certificat est répertorié dans le tableau **Certificats utilisateur** sur la page de résumé de l'utilisateur.

À la fin :

- Pour les terminaux BlackBerry Dynamics activés, configurez la durée pendant laquelle les certificats chargés restent sur le serveur BlackBerry UEM avant d'être supprimés automatiquement du serveur. Le paramètre par défaut est 24 heures.

Modifier un certificat client pour un compte d'utilisateur

1. Sur la barre de menus, cliquez sur **Utilisateurs > Terminaux gérés**.
2. Recherchez un compte d'utilisateur.
3. Dans les résultats de la recherche, cliquez sur le nom d'un compte d'utilisateur.
4. Dans la section **Profils et stratégies informatiques**, cliquez sur le certificat d'utilisateur que vous souhaitez modifier.
5. Cliquez sur .
6. Procédez aux modifications nécessaires. Vous ne pouvez pas modifier les terminaux auxquels le certificat s'applique.
7. Cliquez sur **Enregistrer**.

À la fin : Si vous modifiez un certificat d'utilisateur BlackBerry Dynamics que vous ou un utilisateur a supprimé d'un terminal, le certificat est renvoyé au terminal.

Renouveler ou supprimer un certificat BlackBerry Dynamics pour un compte d'utilisateur

Vous pouvez envoyer une commande au terminal d'un utilisateur pour demander le renouvèlement du certificat de l'AC. Vous pouvez également supprimer un certificat BlackBerry Dynamics du terminal d'un utilisateur. Si vous supprimez un certificat, le connecteur PKI BlackBerry Dynamics envoie une notification à l'autorité de certification indiquant que le certificat n'est plus utilisé, mais le certificat n'est pas automatiquement révoqué.

1. Sur la barre de menus, cliquez sur **Utilisateurs > Terminaux gérés**.
2. Recherchez un compte d'utilisateur.
3. Dans les résultats de la recherche, cliquez sur le nom d'un compte d'utilisateur.
4. Effectuez l'une des opérations suivantes dans la section **Certificats utilisateur** :
   - Cliquez sur pour demander le renouvèlement du certificat de l'autorité de certification.
   - Cliquez sur pour supprimer le certificat du terminal de l'utilisateur.

   Remarque : Pour supprimer des informations d'identification intelligentes Entrust d'un terminal, l'utilisateur doit également désactiver les informations d'identification intelligentes dans BlackBerry UEM Client.

Ajouter un certificat client à un profil d'informations d'identification de l'utilisateur

Vous pouvez télécharger les certificats pour les utilisateurs individuels dans un profil d'informations d'identification de l'utilisateur. Les utilisateurs peuvent également télécharger leur certificat dans le profil

d'informations d'identification de l'utilisateur à l'aide de BlackBerry UEM Self-Service. Le téléchargement de certificats vers des profils d'informations d'identification utilisateur est pris en charge pour les terminaux iOS et pour les terminaux Android Enterprise.

Le certificat client doit porter une extension .pfx ou .p12. Le nouveau certificat que vous, ou un utilisateur, téléchargez dans le profil d'informations d'identification de l'utilisateur remplace le certificat existant sur les terminaux des utilisateurs.

Avant de commencer :

- Créer un profil d'informations d'identification de l'utilisateur pour télécharger manuellement les certificats.
- Attribuez le profil d'informations d'identification de l'utilisateur aux utilisateurs.

1. Sur la barre de menus, cliquez sur **Utilisateurs > Terminaux gérés**.
2. Recherchez un compte d'utilisateur.
3. Dans les résultats de la recherche, cliquez sur le nom d'un compte d'utilisateur.
4. Dans la section **Stratégie informatique et profils**, en regard du profil d'informations d'identification de l'utilisateur, cliquez sur **Ajouter un certificat**.
5. Cliquez sur **Parcourir** pour localiser le fichier de certificat.
6. Indiquez le mot de passe du certificat. Pour les terminaux iOS, le mot de passe est requis. Pour les terminaux Android, vous n'avez pas à fournir le mot de passe dans BlackBerry UEM si le terminal exécute la version la plus récente de BlackBerry UEM Client. Si vous ne spécifiez aucun mot de passe, l'utilisateur doit saisir le mot de passe du terminal.
7. Cliquez sur **Ajouter**.

Modifier un certificat client pour un profil d'informations d'identification de l'utilisateur

Vous pouvez modifier le certificat que vous, ou un utilisateur, avez ajouté à un profil d'informations d'identification de l'utilisateur. Le nouveau certificat remplace le certificat existant sur le terminal.

1. Sur la barre de menus, cliquez sur **Utilisateurs > Terminaux gérés**.
2. Recherchez un compte d'utilisateur.
3. Dans les résultats de la recherche, cliquez sur le nom d'un compte d'utilisateur.
4. Dans la section **Stratégie informatique et profils**, sur la ligne du profil d'informations d'identification de l'utilisateur, cliquez sur **Mettre à jour**.
5. Cliquez sur **Parcourir** pour localiser le fichier de certificat.
6. Saisissez un mot de passe (password) pour le certificat. Pour les terminaux iOS, un mot de passe est requis. Pour les terminaux Android, vous n'avez pas à fournir le mot de passe dans BlackBerry UEM si le terminal exécute la version la plus récente de BlackBerry UEM Client. Si vous ne spécifiez aucun mot de passe, l'utilisateur doit saisir le mot de passe du terminal.
7. Cliquez sur **Enregistrer**.

Configurer une valeur TTL pour les certificats client

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

Cette fonction n'est pas prise en charge dans BlackBerry UEM Cloud.

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

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

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