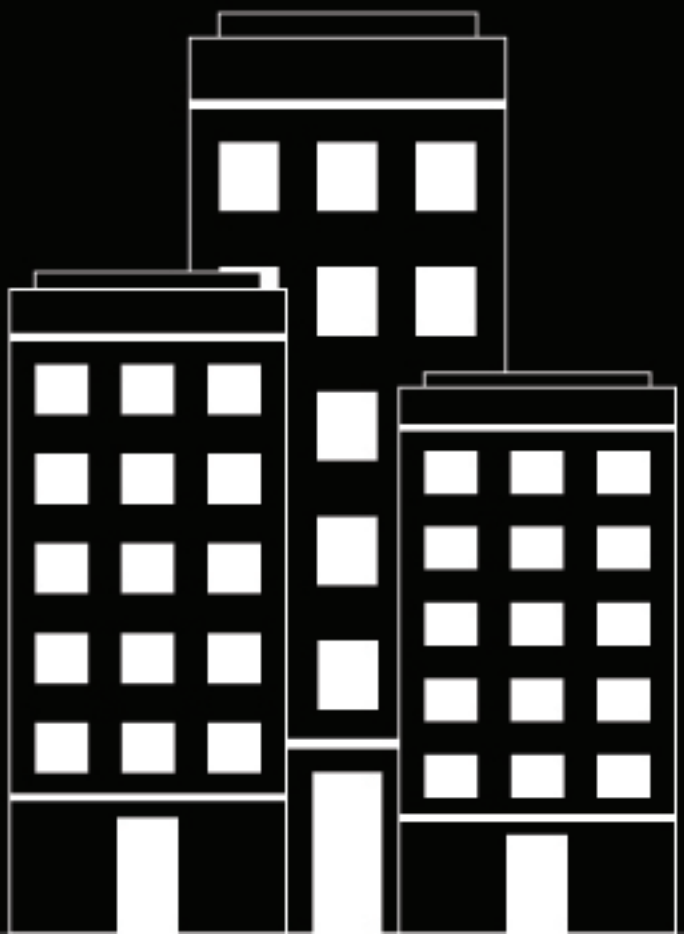

BlackBerry UEM

Gestion des connexions sécurisées

12.20

Contents

Gestion des connexions sécurisées avec BlackBerry UEM

Le tableau suivant récapitule les tâches d'administration décrites dans ce guide. Passez-les en revue pour déterminer les tâches à accomplir en fonction des besoins de votre organisation.

Tâche	Description
Créer un profil Wi-Fi	Vous pouvez créer un profil Wi-Fi pour spécifier la manière dont les terminaux doivent se connecter au réseau Wi-Fi professionnel.
Créer un profil VPN	Vous pouvez créer un profil VPN pour spécifier la manière dont les terminaux doivent se connecter à un VPN professionnel.
Créer un profil VPN par application	Vous pouvez spécifier quelles applications installées sur les terminaux doivent utiliser un VPN pour leurs données en transit.
Créer un profil proxy	Vous pouvez spécifier la manière dont les terminaux doivent utiliser un serveur proxy pour accéder à des services Web sur Internet ou un réseau professionnel.
Créer un profil de connectivité d'entreprise	Vous pouvez spécifier la manière dont les terminaux doivent se connecter aux ressources de votre organisation à l'aide de la connectivité d'entreprise et de BlackBerry Secure Connect Plus pour fournir un tunnel IP sécurisé entre les applications et le réseau de votre organisation.
Créer un profil BlackBerry 2FA	Vous pouvez activer l'authentification à deux facteurs pour les utilisateurs et spécifier la configuration des fonctionnalités de préauthentification et de résolution autonome.
Créer un profil d'extension d'identification unique	Vous pouvez activer les terminaux iOS et iPadOS à des fins d'authentification automatique auprès de domaines et services Web de votre réseau d'entreprise.
Créer un profil de connectivité BlackBerry Dynamics	Vous pouvez définir les connexions réseau, les domaines Internet, les plages d'adresses IP et les serveurs d'applications auxquels les terminaux peuvent se connecter lorsqu'ils utilisent des applications BlackBerry Dynamics. Pour plus d'informations, consultez Configuration de connexions réseau pour les applications BlackBerry Dynamics dans le contenu relatif à l'administration.
Créer un profil DNS	Vous pouvez désigner les serveurs DNS que vous souhaitez que les terminaux iOS et macOS utilisent pour accéder aux domaines spécifiés.
Créer un profil de messagerie	Vous pouvez spécifier la manière dont les terminaux doivent se connecter à un serveur de messagerie professionnel et synchroniser les e-mails, les entrées de calendrier et les données de l'organiseur à l'aide de Exchange ActiveSync ou IBM Notes Traveler. Pour plus d'informations, consultez Création de profils de messagerie dans le contenu relatif à l'administration.
Créer un profil de messagerie IMAP/POP3	Vous pouvez spécifier la manière dont les terminaux doivent se connecter à un serveur de messagerie IMAP ou POP3 et synchroniser les e-mails. Pour plus d'informations, consultez Création d'un profil de messagerie IMAP/POP3 dans le contenu relatif à l'administration.

Tâche	Description
Créer un profil d'utilisation du réseau	Vous pouvez gérer l'utilisation du réseau mobile pour les applications iOS et iPadOS.
Créer un profil de filtre de contenu Web	Vous pouvez limiter les sites Web qu'un utilisateur peut afficher dans Safari ou d'autres navigateurs sur un terminal supervisé iOS ou iPadOS.
Créer un profil AirPrint	Vous pouvez aider les utilisateurs à trouver des imprimantes.
Créer un profil AirPlay	Vous pouvez spécifier les terminaux AirPlay iOS et iPadOS auxquels les utilisateurs peuvent se connecter.
Créer un profil de nom de point d'accès	Vous pouvez spécifier les informations dont les terminaux Android ont besoin pour communiquer avec le réseau de l'opérateur.
Connecter UEM au logiciel PKI de votre organisation	Vous pouvez étendre l'authentification basée sur des certificats fournie par vos services PKI aux terminaux et applications que vous gérez avec UEM. Par exemple, vous pouvez : • Connexion de BlackBerry UEM au logiciel Entrust de votre organisation • Connecter BlackBerry UEM au serveur Entrust IdentityGuard de votre organisation pour utiliser les informations d'identification intelligentes • Connexion de BlackBerry UEM au logiciel OpenTrust de votre organisation • Connecter BlackBerry UEM à un connecteur PKI BlackBerry Dynamics • Connecter BlackBerry UEM à la solution PKI d'application de votre organisation
Envoyer des certificats à des terminaux et à des applications à l'aide de profils	Vous pouvez envoyer des certificats à des terminaux et à des applications à l'aide de profils UEM.
Gérer des certificats client 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.

Gestion des connexions professionnelles à l'aide des profils

Vous pouvez utiliser des profils pour configurer et gérer les connexions professionnelles des terminaux de votre organisation. Les connexions professionnelles définissent la manière dont les terminaux se connectent aux ressources professionnelles dans l'environnement de votre entreprise, comme les serveurs de messagerie, serveurs proxy, réseaux Wi-Fi et VPN. Vous pouvez spécifier les paramètres des terminaux iOS, macOS, Android et Windows 10 dans le même profil, puis attribuer le profil à des comptes d'utilisateur, groupes d'utilisateurs ou groupes de terminaux.

Certains profils de connexions professionnelles peuvent inclure un ou plusieurs profils associés. Lorsque vous spécifiez un profil associé, vous liez un profil existant à un profil de connexions professionnelles et les terminaux doivent utiliser le profil associé lorsqu'ils utilisent le profil de connexions professionnelles. Par exemple, vous pouvez associer des profils de certificat et des profils proxy à différents profils de connexions professionnelles. Vous devez créer ces profils dans l'ordre suivant :

1. Profils de certificat
2. Profils proxy
3. Profils de connexions professionnelles (messagerie, VPN et Wi-Fi, par exemple)

Par exemple, si vous créez un profil Wi-Fi, vous ne pouvez pas associer de profil proxy au profil Wi-Fi lorsque vous le créez. Après avoir créé un profil proxy, vous devez modifier le profil Wi-Fi pour lui associer le profil proxy.

Configuration de réseaux Wi-Fi professionnels pour les terminaux

Vous pouvez utiliser un profil Wi-Fi pour spécifier la manière dont les terminaux se connectent à un réseau Wi-Fi professionnel derrière le pare-feu. Vous pouvez attribuer un profil Wi-Fi à des comptes d'utilisateur, groupes d'utilisateurs ou groupes de terminaux.

Par défaut, les applications professionnelles et personnelles peuvent utiliser les profils Wi-Fi pour se connecter au réseau de votre organisation.

Créer un profil Wi-Fi

Les paramètres de profil requis varient pour chaque type de terminal et dépendent du type de sécurité Wi-Fi et du protocole d'authentification que vous sélectionnez. Vous pouvez utiliser une variable de paramètre de profil correspondant à un champ de texte pour faire référence à une valeur plutôt que de spécifier la valeur réelle.

Avant de commencer :

- Si les terminaux utilisent l'authentification basée sur des certificats pour les connexions Wi-Fi professionnelles, créez un profil de certificat d'autorité de certification et attribuez-le aux comptes d'utilisateur, groupes d'utilisateurs ou groupes de terminaux. Pour envoyer les certificats client aux terminaux, créez un profil SCEP, un profil de certificat partagé ou un profil d' informations d'identification de l'utilisateur à associer au profil Wi-Fi.
- Pour les terminaux iOS, iPadOS, macOS et Android Enterprise qui utilisent un serveur proxy pour les connexions Wi-Fi professionnelles, créez un profil proxy à associer au profil Wi-Fi.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Réseaux et connexions > Wi-Fi**.
3. Cliquez sur +.
4. Saisissez le nom et la description du profil Wi-Fi. Cette information s'affiche sur les terminaux.

5. Dans le champ **SSID**, saisissez le nom de réseau d'un réseau Wi-Fi.
6. Si le réseau Wi-Fi ne diffuse pas le SSID, cochez la case **Réseau masqué**.
7. Cliquez sur l'onglet correspondant à un type de terminal pour configurer les paramètres appropriés. Pour plus d'informations, reportez-vous aux paramètres de profil Wi-Fi relatifs à iOS et macOS, Android et Windows.

   Si votre organisation exige que les utilisateurs fournissent un nom d'utilisateur et un mot de passe pour se connecter au réseau Wi-Fi, saisissez `%UserName%` dans le champ **Nom d'utilisateur**.
8. Répétez l'étape 7 pour chaque type de terminal.
9. Cliquez sur **Ajouter**.

À la fin : Attribuez le profil Wi-Fi aux comptes d'utilisateur, groupes d'utilisateurs et groupes de terminaux

iOS et macOS : paramètres de profil Wi-Fi

iOS, iPadOS et macOS : paramètre de profil Wi-Fi	Description
Appliquer le profil à	Ce paramètre indique si le profil Wi-Fi sur un terminal macOS est appliqué au compte d'utilisateur ou au terminal.
Rejoindre automatiquement le réseau	Ce paramètre spécifie si un terminal peut automatiquement rejoindre le réseau Wi-Fi.
Désactiver la randomisation MAC	Ce paramètre indique si les terminaux peuvent randomiser leurs adresses MAC lorsqu'ils rejoignent le réseau Wi-Fi.
Profil proxy associé	Ce paramètre spécifie le profil proxy associé utilisé par un terminal pour se connecter à un serveur proxy lorsque le terminal est connecté au réseau Wi-Fi.
Type de réseau	Ce paramètre spécifie la configuration du réseau Wi-Fi. Les configurations de points d'accès s'appliquent uniquement aux terminaux iOS, iPadOS et macOS. Si vous sélectionnez l'une des options de point d'accès, n'utilisez pas le même profil Wi-Fi pour configurer les paramètres d'autres types de terminal.
Nom de l'opérateur affiché	Ce paramètre spécifie le nom convivial de l'opérateur de points d'accès. Ce paramètre est valide uniquement si le paramètre Type de réseau est défini sur Hotspot 2.0.
Nom de domaine	Ce paramètre spécifie le nom de domaine de l'opérateur de points d'accès. Ce paramètre est valide uniquement si le paramètre Type de réseau est défini sur Hotspot 2.0. Le paramètre SSID n'est pas requis lorsque vous utilisez ce paramètre.
Identifiants d'entreprise des consortiums d'itinérance	Ce paramètre spécifie les identifiants d'entreprise des consortiums d'itinérance et fournisseurs de services agissant en tant que partenaires d'itinérance de l'opérateur de points d'accès. Ce paramètre est valide uniquement si le paramètre Type de réseau est défini sur Hotspot 2.0.

iOS, iPadOS et macOS : paramètre de profil Wi-Fi	Description
Noms de domaine NAI	Ce paramètre spécifie les noms de domaine de l'identifiant d'accès réseau capables d'authentifier un terminal. Ce paramètre est valide uniquement si le paramètre Type de réseau est défini sur Hotspot 2.0.
MCC/MNC	Ce paramètre spécifie les combinaisons MCC et MNC qui identifient les opérateurs de réseaux mobiles. Chaque valeur doit contenir six chiffres. Ce paramètre est valide uniquement si le paramètre Type de réseau est défini sur Hotspot 2.0.
Autoriser la connexion aux réseaux des partenaires d'itinérance	Ce paramètre spécifie si un terminal peut se connecter aux partenaires d'itinérance pour le point d'accès. Ce paramètre est valide uniquement si le paramètre Type de réseau est défini sur Hotspot 2.0.
Type de sécurité	Ce paramètre indique le type de sécurité utilisé par le réseau Wi-Fi. Si le paramètre Type de réseau est défini sur Hotspot 2.0, ce paramètre est défini sur WPA2-Enterprise.
Clé WEP	Ce paramètre spécifie la clé WEP du réseau Wi-Fi. La clé WEP doit contenir 10 ou 26 caractères hexadécimaux (0-9, A-F) ou 5 ou 13 caractères alphanumériques (0-9, A-Z). Exemples de valeurs de clés hexadécimales : ABCDEF0123 ou ABCDEF0123456789ABCDEF0123. Exemples de valeurs de clés alphanumériques : abCD5 ou abCDefGHijKL1. Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini sur WEP personnel.
Clé pré-partagée	Ce paramètre spécifie la clé pré-partagée du réseau Wi-Fi. Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini sur WPA-Personal, WPA2-Personal ou WPA3-Personal.
Protocoles	
Protocole d'authentification	Ce paramètre spécifie la méthode EAP prise en charge par le réseau Wi-Fi. Vous pouvez sélectionner plusieurs méthodes EAP. Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini sur WEP Enterprise, WPA-Enterprise, WPA2-Enterprise ou WPA3-Enterprise.
Authentification interne	Ce paramètre indique la méthode d'authentification interne à utiliser avec TTLS. Ce paramètre est valide uniquement si le paramètre Protocole d'authentification est défini sur TTLS.

iOS, iPadOS et macOS : paramètre de profil Wi-Fi	Description
Utiliser PAC	Ce paramètre spécifie si la méthode EAP-FAST utilise des informations d'accès protégé (PAC). Ce paramètre est valide uniquement si le paramètre Protocole d'authentification est défini sur EAP-FAST.
Déployer PAC	Ce paramètre spécifie si la méthode EAP-FAST permet un déploiement PAC. Ce paramètre est valide uniquement si le paramètre Protocole d'authentification est défini sur EAP-FAST et si le paramètre Utiliser PAC est sélectionné.
Déployer PAC anonymement	Ce paramètre spécifie si la méthode EAP-FAST permet un déploiement PAC anonyme. Ce paramètre est valide uniquement si le paramètre Protocole d'authentification est défini sur Utiliser PAC et si le paramètre Déployer PAC est sélectionné.
Authentification	
Identité externe pour TTLS, PEAP et EAP-FAST	Ce paramètre spécifie l'identité externe d'un utilisateur envoyée en clair. Vous pouvez spécifier un nom d'utilisateur anonyme pour masquer l'identité réelle de l'utilisateur (par exemple, anonyme). Le tunnel crypté est utilisé pour envoyer le nom d'utilisateur réel à des fins d'authentification auprès du réseau Wi-Fi. Si l'identité externe comprend le nom de domaine pour l'acheminement de la demande, il doit correspondre au domaine réel de l'utilisateur (par exemple, anonyme@exemple.com). Ce paramètre est valide uniquement si le paramètre Protocole d'authentification est défini sur TTLS, PEAP ou EAP-FAST.
Utiliser le mot de passe inclus dans le profil Wi-Fi	Ce paramètre spécifie si le profil Wi-Fi inclut le mot de passe à des fins d'authentification. Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini sur WEP Enterprise, WPA-Enterprise, WPA2-Enterprise ou WPA3-Enterprise.
Mot de passe	Ce paramètre spécifie le mot de passe utilisé par un terminal pour s'authentifier auprès du réseau Wi-Fi. Ce paramètre est valide uniquement si le paramètre Utiliser le mot de passe inclus dans le profil Wi-Fi est sélectionné.
nom d'utilisateur ;	Ce paramètre spécifie le nom d'utilisateur utilisé par un terminal pour s'authentifier auprès du réseau Wi-Fi. Si le profil concerne plusieurs utilisateurs, vous pouvez utiliser la variable %UserName%. Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini sur WEP Enterprise, WPA-Enterprise, WPA2-Enterprise ou WPA3-Enterprise.

iOS, iPadOS et macOS : paramètre de profil Wi-Fi	Description
Type d'authentification	Ce paramètre spécifie le type d'authentification utilisé par un terminal pour se connecter au réseau Wi-Fi. Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini sur WEP Enterprise, WPA-Enterprise, WPA2-Enterprise ou WPA3-Enterprise.
Type de liaison de certificat	Ce paramètre spécifie le type de liaison du certificat client associé au profil Wi-Fi. Ce paramètre est valide uniquement si le paramètre Type d'authentification est défini sur Certificat partagé.
Profil de certificat partagé	Ce paramètre spécifie le profil de certificat partagé avec le certificat client utilisé par un terminal pour s'authentifier auprès du réseau Wi-Fi. Ce paramètre est valide uniquement si le paramètre Type de liaison de certificat est défini sur Référence unique.
Nom du certificat client	Ce paramètre spécifie le nom du certificat client utilisé par un terminal pour s'authentifier auprès du réseau Wi-Fi. Ce paramètre est valide uniquement si le paramètre Type de liaison de certificat est définir sur Injection de variable.
Profil SCEP associé	Ce paramètre spécifie le profil SCEP associé utilisé par un terminal pour obtenir un certificat client et s'authentifier auprès du réseau Wi-Fi. Ce paramètre est valide uniquement si le paramètre Type d'authentification est défini sur SCEP.
Profil des informations d'identification de l'utilisateur associé	Ce paramètre spécifie le profil d'informations d'identification de l'utilisateur associé utilisé par un terminal pour obtenir un certificat client et s'authentifier auprès du réseau Wi-Fi. Ce paramètre est valide uniquement si le paramètre Type d'authentification est défini sur Informations d'identification de l'utilisateur.
Se fier	
Noms usuels de certificat attendus par le serveur d'authentification	Ce paramètre spécifie les noms usuels du certificat envoyés par le serveur d'authentification au terminal (par exemple, * .exemple.com). Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini sur WEP Enterprise, WPA-Enterprise, WPA2-Enterprise ou WPA3-Enterprise.
Type de liaison de certificat	Ce paramètre spécifie le type de liaison des certificats client associés au profil Wi-Fi. Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini sur WEP Enterprise, WPA-Enterprise, WPA2-Enterprise ou WPA3-Enterprise.

iOS, iPadOS et macOS : paramètre de profil Wi-Fi	Description
Profils de certificat d'autorité de certification	Ce paramètre spécifie le profil de certificat d'autorité de certification avec le certificat client utilisé par un terminal pour établir une connexion approuvée au réseau Wi-Fi. Ce paramètre est valide uniquement si le paramètre Type de liaison de certificat est défini sur Référence unique.
Noms de certificats approuvés	Ce paramètre spécifie les noms des certificats approuvés utilisés par un terminal pour établir une connexion approuvée au réseau Wi-Fi. Ce paramètre est valide uniquement si le paramètre Type de liaison de certificat est définir sur Injection de variable.
Faire confiance aux décisions d'utilisateur	Ce paramètre spécifie si un terminal doit inviter l'utilisateur à approuver un serveur lorsque la chaine d'approbation ne peut pas être établie. Si ce paramètre n'est pas sélectionné, seules les connexions aux serveurs approuvés que vous spécifiez sont autorisées. Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini sur WEP Enterprise, WPA-Enterprise, WPA2-Enterprise ou WPA3-Enterprise.
Contourner le réseau captif	Ce paramètre spécifie si les terminaux peuvent contourner les réseaux captifs.
Activer le marquage QoS	Ce paramètre indique si vous pouvez activer les marquages L2 et L3 pour le trafic transitant par le réseau Wi-Fi.
Utiliser QoS pour les appels FaceTime	Ce paramètre indique si le trafic audio et vidéo des appels FaceTime peut utiliser les marquages L2 et L3.
Utiliser le marquage L2 uniquement pour le trafic QoS	Ce paramètre indique si le trafic transitant par le réseau Wi-Fi utilise uniquement le marquage L2.
Appliquer le marquage QoS aux applications sélectionnées	Ce paramètre spécifie les ID d'offre des applications pouvant utiliser les marquages L2 et L3.

Android : paramètres de profil Wi-Fi

Android : paramètre de profil Wi-Fi	Description
Profil proxy associé	Ce paramètre spécifie le profil proxy associé utilisé par un terminal Android pour se connecter à un serveur proxy lorsque le terminal est connecté au réseau Wi-Fi. Les terminaux Android auxquels est attribué le type d'activation Contrôles MDM ou Confidentialité de l'utilisateur ne prennent pas en charge les profils Wi-Fi avec des paramètres de proxy.
BSSID	Ce paramètre spécifie l'adresse MAC du point d'accès sans fil du réseau Wi-Fi.

Android : paramètre de profil Wi-Fi	Description
DNS primaire	Ce paramètre spécifie le serveur DNS primaire au format décimal séparé par des points (par exemple, 192.0.2.0). Ce paramètre s'applique uniquement aux terminaux utilisant Samsung Knox lorsque l'adresse IP est attribuée de façon statique par le réseau de l'entreprise.
DNS secondaire	Ce paramètre spécifie le serveur DNS secondaire au format décimal séparé par des points (par exemple, 192.0.2.0). Ce paramètre s'applique uniquement aux terminaux utilisant Samsung Knox lorsque l'adresse IP est attribuée de façon statique par le réseau de l'entreprise.
Type de sécurité	Ce paramètre indique le type de sécurité utilisé par le réseau Wi-Fi.
Type de sécurité personnelle	Ce paramètre indique le type de sécurité personnelle utilisé par le réseau Wi-Fi. Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini sur Personnelle.
Clé WEP	Ce paramètre spécifie la clé WEP du réseau Wi-Fi. La clé WEP doit contenir 10 ou 26 caractères hexadécimaux (0-9, A-F) ou 5 ou 13 caractères alphanumériques (0-9, A-Z). Exemples de valeurs de clés hexadécimales : ABCDEF0123 ou ABCDEF0123456789ABCDEF0123. Exemples de valeurs de clés alphanumériques : abCD5 ou abCDefGHijKL1. Ce paramètre est valide uniquement si le paramètre Type de sécurité personnelle est défini sur WEP personnel.
Clé pré-partagée	Ce paramètre spécifie la clé pré-partagée du réseau Wi-Fi. Ce paramètre est valide uniquement si le paramètre Type de sécurité personnelle est défini sur WPA-Personal/WPA2-Personal.
Protocole d'authentification	Ce paramètre spécifie la méthode EAP utilisée par le réseau Wi-Fi. Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini sur Entreprise. Le protocole LEAP n'est pas pris en charge par les terminaux utilisant Samsung Knox.
Authentification interne	Ce paramètre indique la méthode d'authentification interne à utiliser avec TTLS. Ce paramètre est valide uniquement si le paramètre Protocole d'authentification est défini sur TTLS. Le protocole CHAP n'est pas pris en charge par les terminaux utilisant Samsung Knox.

Android : paramètre de profil Wi-Fi	Description
Identité Externe pour TTLS	Ce paramètre spécifie l'identité externe d'un utilisateur envoyée en clair. Vous pouvez spécifier un nom d'utilisateur anonyme pour masquer l'identité réelle de l'utilisateur (par exemple, anonyme). Le tunnel crypté est utilisé pour envoyer le nom d'utilisateur réel à des fins d'authentification auprès du réseau Wi-Fi. Si l'identité externe comprend le nom de domaine pour l'acheminement de la demande, il doit correspondre au domaine réel de l'utilisateur (par exemple, anonyme@exemple.com). Ce paramètre est valide uniquement si le paramètre Protocole d'authentification est défini sur TTLS.
Identité Externe pour PEAP	Ce paramètre spécifie l'identité externe d'un utilisateur envoyée en clair. Vous pouvez spécifier un nom d'utilisateur anonyme pour masquer l'identité réelle de l'utilisateur (par exemple, anonyme). Le tunnel crypté est utilisé pour envoyer le nom d'utilisateur réel à des fins d'authentification auprès du réseau Wi-Fi. Si l'identité externe comprend le nom de domaine pour l'acheminement de la demande, il doit correspondre au domaine réel de l'utilisateur (par exemple, anonyme@exemple.com). Ce paramètre est valide uniquement si le paramètre Protocole d'authentification est défini sur PEAP.
nom d'utilisateur ;	Ce paramètre spécifie le nom d'utilisateur utilisé par un terminal Android pour s'authentifier auprès du réseau Wi-Fi. Si le profil concerne plusieurs utilisateurs, vous pouvez utiliser la variable %UserName%. Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini sur Entreprise.
Utiliser le mot de passe inclus dans le profil Wi-Fi	Ce paramètre spécifie si le profil Wi-Fi inclut le mot de passe à des fins d'authentification. Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini sur Entreprise.
Mot de passe	Ce paramètre spécifie le mot de passe utilisé par un terminal Android pour s'authentifier auprès du réseau Wi-Fi. Ce paramètre est valide uniquement si le paramètre Utiliser le mot de passe inclus dans le profil Wi-Fi est sélectionné.
Type d'authentification	Ce paramètre spécifie le type d'authentification utilisé par un terminal Android pour se connecter au réseau Wi-Fi. Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini sur Entreprise.
Type de liaison de certificat	Ce paramètre spécifie le type de liaison du certificat client associé au profil Wi-Fi. Ce paramètre est valide uniquement si le paramètre Type d'authentification est défini sur Certificat partagé.

Android : paramètre de profil Wi-Fi	Description
Profil de certificat partagé	Ce paramètre spécifie le profil de certificat partagé avec le certificat client utilisé par un terminal Android pour s'authentifier auprès du réseau Wi-Fi. Ce paramètre est valide uniquement si le paramètre Type de liaison de certificat est défini sur Référence unique. Le nom du profil de certificat partagé doit contenir moins de 36 caractères pour les terminaux utilisant un Knox Workspace.
Profil SCEP associé	Ce paramètre spécifie le profil SCEP associé utilisé par un terminal Android pour obtenir un certificat client et s'authentifier auprès du réseau Wi-Fi. Ce paramètre est valide uniquement si le paramètre Type d'authentification est défini sur SCEP. Le nom du profil SCEP doit contenir moins de 36 caractères pour les terminaux utilisant un Knox Workspace.
Profil des informations d'identification de l'utilisateur associé	Ce paramètre spécifie le profil d'informations d'identification de l'utilisateur associé utilisé par un terminal Android pour obtenir un certificat client et s'authentifier auprès du réseau Wi-Fi. Ce paramètre est valide uniquement si le paramètre Type d'authentification est défini sur Informations d'identification de l'utilisateur. Le nom du profil d'informations d'identification doit contenir moins de 36 caractères pour les terminaux utilisant un Knox Workspace.
Nom du certificat client	Ce paramètre spécifie le nom du certificat client utilisé par un terminal Android pour s'authentifier auprès du réseau Wi-Fi. Ce paramètre est valide uniquement si le paramètre Type de liaison de certificat est définir sur Injection de variable.
Noms usuels de certificat attendus par le serveur d'authentification	Ce paramètre spécifie les noms usuels du certificat envoyés par le serveur d'authentification au terminal (par exemple, * .exemple.com). Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini sur Entreprise.
Type de liaison de certificat	Ce paramètre spécifie le type de liaison des certificats client associés au profil Wi-Fi. Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini sur Entreprise.
Profil du certificat d'autorité de certification	Ce paramètre spécifie le profil de certificat d'autorité de certification avec le certificat client utilisé par un terminal Android pour établir une connexion approuvée au réseau Wi-Fi. Ce paramètre est valide uniquement si le paramètre Type de liaison de certificat est défini sur Référence unique.

Android : paramètre de profil Wi-Fi	Description
Noms de certificats approuvés	Ce paramètre spécifie les noms des certificats approuvés utilisés par un terminal Android pour établir une connexion approuvée au réseau Wi-Fi. Ce paramètre est valide uniquement si le paramètre Type de liaison de certificat est définir sur Injection de variable.

Windows : paramètres de profil Wi-Fi

Windows : paramètre de profil Wi-Fi	Description
Se connecter automatiquement lorsque ce réseau est à portée	Ce paramètre spécifie si les terminaux peuvent se connecter automatiquement au réseau Wi-Fi.
Type de sécurité	Ce paramètre indique le type de sécurité utilisé par le réseau Wi-Fi.
Type de cryptage	Ce paramètre spécifie la méthode de cryptage utilisée par le réseau Wi-Fi. Le paramètre « Type de sécurité » détermine les types de cryptage pris en charge et la valeur par défaut de ce paramètre.
Clé WEP	Ce paramètre spécifie la clé WEP du réseau Wi-Fi. La clé WEP doit contenir 10 ou 26 caractères hexadécimaux (0-9, A-F) ou 5 ou 13 caractères alphanumériques (0-9, A-Z). Exemples de valeurs de clés hexadécimales : ABCDEF0123 ou ABCDEF0123456789ABCDEF0123. Exemples de valeurs de clés alphanumériques : abCD5 ou abCDefGHijKL1. Ce paramètre est valide uniquement si le paramètre « Type de sécurité » est défini sur « Ouvert » et le paramètre « Type de cryptage » sur « WEP ».
Index de clé	Ce paramètre spécifie la position de la clé correspondante stockée sur le point d'accès sans fil. Ce paramètre est valide uniquement si le paramètre « Type de sécurité » est défini sur « Ouvert » et le paramètre « Type de cryptage » sur « WEP ».
Clé pré-partagée	Ce paramètre spécifie la clé pré-partagée du réseau Wi-Fi. Ce paramètre est valide uniquement si le paramètre « Type de sécurité » est défini sur WPA-Personal.
Activer l'identification unique	Ce paramètre spécifie si le réseau Wi-Fi prend en charge l'authentification avec identification unique. Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini WPA-Enterprise ou WPA2-Enterprise.

Windows : paramètre de profil Wi-Fi	Description
Type d'identification unique	Ce paramètre spécifie le moment où l'authentification avec identification unique intervient. Lorsque ce paramètre est défini sur Exécuter immédiatement avant la connexion d'utilisateur, l'identification unique est exécutée avant que l'utilisateur se connecte à Active Directory. Lorsque ce paramètre est défini sur Exécuter immédiatement après la connexion d'utilisateur, l'identification unique est exécutée après que l'utilisateur se connecte à Active Directory. Ce paramètre est valide uniquement si le paramètre « Activer l'identification unique » est sélectionné.
Délai de connectivité maximum	Ce paramètre spécifie, en secondes, le délai maximum avant que la tentative de connexion avec identification unique échoue. Ce paramètre est valide uniquement si le paramètre « Activer l'identification unique » est sélectionné.
Autoriser l'affichage de boites de dialogue supplémentaires lors de l'identification unique	Ce paramètre indique si un terminal peut afficher des boites de dialogue au-delà de l'écran de connexion. Par exemple, si un type d'authentification EAP nécessite que l'utilisateur confirme le certificat envoyé par le serveur lors de l'authentification, le terminal peut afficher la boite de dialogue. Ce paramètre est valide uniquement si le paramètre « Activer l'identification unique » est sélectionné.
Ce réseau utilise des réseaux LAN virtuels pour l'authentification de l'ordinateur et de l'utilisateur	Ce paramètre spécifie si le réseau VLAN utilisé par un terminal change en fonction des informations de connexion de l'utilisateur Par exemple, si le terminal se trouve sur un réseau VLAN lorsqu'il démarre, puis (selon les autorisations utilisateur) passe sur un autre réseau VLAN après que l'utilisateur se connecte. Ce paramètre est valide uniquement si le paramètre « Activer l'identification unique » est sélectionné.
Valider le certificat du serveur	Ce paramètre spécifie si un terminal doit valider le certificat du serveur qui vérifie l'identité du point d'accès sans fil. Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini WPA-Enterprise ou WPA2-Enterprise.
Ne pas inviter l'utilisateur à autoriser de nouveaux serveurs ou des autorités de certification approuvées	Ce paramètre spécifie si un utilisateur est invité à approuvé le certificat du serveur. Ce paramètre est valide uniquement si le paramètre « Valider le certificat du serveur » est sélectionné.

Windows : paramètre de profil Wi-Fi	Description
Profils de certificat d'autorité de certification	Ce paramètre spécifie le profil de certificat d'autorité de certification fournissant la racine approuvée pour le certificat du serveur utilisé par le point d'accès sans fil. Ce paramètre limite les autorités de certification racine que les terminaux approuvent avec les autorités de certification sélectionnées. Si vous ne sélectionnez aucune autorité de certification racine approuvée, les terminaux approuvent toutes les autorités de certification racine de leur magasin d'autorités de certification racine approuvées. Ce paramètre est valide uniquement si le paramètre « Valider le certificat du serveur » est sélectionné.
Activer la reconnexion rapide	Ce paramètre spécifie si le réseau Wi-Fi prend en charge la reconnexion rapide à des fins d'authentification PEAP sur plusieurs points d'accès sans fil. Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini WPA-Enterprise ou WPA2-Enterprise.
Appliquer la protection NAP	Ce paramètre spécifie si le réseau Wi-Fi utilise la protection NAP pour contrôler l'intégrité du système sur les terminaux et vérifier si ceux-ci répondent aux exigences d'intégrité avant d'être autorisés à se connecter au réseau. Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini WPA-Enterprise ou WPA2-Enterprise.
Activer le mode FIPS	Ce paramètre spécifie si le réseau Wi-Fi prend en charge la conformité avec la norme FIPS 140-2. Ce paramètre est valide uniquement si le paramètre « Type de passerelle » est défini sur « WPA2-Enterprise » ou « WPA2-Personal » et le « Type d'authentification » sur « AES ».
Activer la mise en cache du PMK	Ce paramètre spécifie si un terminal peut mettre en cache le PMK pour activer l'itinérance rapide WPA2. L'itinérance rapide ignore les paramètres 802.1X avec un point d'accès sans fil auprès duquel le terminal s'est précédemment authentifié. Ce paramètre est valide uniquement si le paramètre « Type de sécurité » est défini sur WPA2-Enterprise.
Durée de vie du PMK	Ce paramètre spécifie la durée, en minutes, pendant laquelle un terminal peut stocker le PMK dans le cache. Ce paramètre est valide uniquement si le paramètre « Activer la mise en cache du PMK » est sélectionné.
Nombre d'entrées du cache du PMK	Ce paramètre spécifie le nombre maximum d'entrées du PMK qu'un terminal peut stocker dans le cache. Ce paramètre est valide uniquement si le paramètre « Activer la mise en cache du PMK » est sélectionné.

Windows : paramètre de profil Wi-Fi	Description
Ce réseau utilise la pré-authentification	Ce paramètre spécifie si le point d'accès prend en charge la préauthentification pour l'itinérance rapide WPA2. La pré-authentification permet aux terminaux de se connecter à un point d'accès sans fil pour utiliser les paramètres 802.1X avec d'autres points d'accès sans fil à portée. La pré-authentification stocke le PMK et les informations qui s'y rapportent dans le cache du PMK. Lorsque le terminal se connecte à un point d'accès sans fil auprès duquel il s'est pré-authentifié, il utilise les informations mises en cache dans le PMK pour réduire le délai d'authentification et de connexion. Ce paramètre est valide uniquement si le paramètre « Activer la mise en cache du PMK » est sélectionné.
Tentatives de pré-authentification maximum	Ce paramètre spécifie le nombre maximum de tentatives de pré-authentification autorisées. Ce paramètre est valide uniquement si le paramètre « Ce réseau utilise une pré-authentification » est sélectionné.
Type de proxy	Ce paramètre spécifie le type de configuration proxy pour le profil Wi-Fi. Ce paramètre s'applique uniquement aux terminaux Windows 10 Mobile.
URL du fichier PAC	Ce paramètre spécifie l'URL du serveur Web qui héberge le fichier PAC et le nom du fichier PAC au format http://<web_server_URL>/<filename>.pac. Ce paramètre est valide uniquement si le paramètre Type de proxy est défini sur Configuration PAC.
Adresse	Ce paramètre spécifie le nom du serveur et le port du proxy du réseau. Utilisez le format hôte:port (par exemple, server01.example.com:123). L'hôte doit être l'un des suivants : • un nom enregistré (ex. : nom de serveur), un nom de domaine complet ou un nom d'étiquette unique (par exemple, serveur01 au lieu de serveur01.exemple.com) • une adresse IPv4 ou IPv6 Ce paramètre est valide uniquement si le paramètre Type de proxy est défini sur Configuration manuelle.
Web Proxy Autodiscovery	Ce paramètre permet d'activer le Web Proxy Autodiscovery Protocol (WPAD) pour la recherche de proxy. Ce paramètre est valide uniquement si le paramètre « Type de proxy » est défini sur « Web Proxy Autodiscovery ».
Désactiver les vérifications de la connectivité Internet	Ce paramètre permet de désactiver les vérifications de la connectivité Internet.
Profil SCEP associé	Ce paramètre spécifie le profil SCEP associé utilisé par un terminal pour obtenir un certificat client et s'authentifier auprès du réseau Wi-Fi.

Configuration de réseaux VPN professionnels pour les terminaux

Vous pouvez utiliser un profil VPN pour spécifier la manière dont les terminaux iOS, iPadOS, macOS, Samsung Knox et Windows 10 se connectent à un VPN professionnel. Vous pouvez attribuer un profil VPN à des comptes d'utilisateur, groupes d'utilisateurs ou groupes de terminaux.

Pour vous connecter à un VPN professionnel pour des terminaux Android autres que Samsung Knox, vous pouvez configurer les paramètres VPN à l'aide des paramètres de configuration d'application pour une application VPN, ou les utilisateurs peuvent configurer manuellement les paramètres VPN sur leurs terminaux.

Terminal	Applications et connexions réseau
iOS et iPadOS	Les applications professionnelles et personnelles peuvent utiliser les profils VPN stockés sur le terminal pour se connecter au réseau de votre organisation. Vous pouvez activer un VPN par application pour un profil VPN afin de limiter ce dernier aux applications professionnelles que vous spécifiez. Vous pouvez activer le VPN à la demande pour que les terminaux se connectent automatiquement à un VPN dans un domaine particulier. Par exemple, vous pouvez spécifier le domaine de votre organisation pour permettre aux utilisateurs d'accéder au contenu de votre intranet à l'aide d'un VPN à la demande.
macOS	Vous pouvez configurer des profils VPN pour permettre aux applications de se connecter au réseau de votre organisation. Vous pouvez activer le VPN à la demande pour que les terminaux se connectent automatiquement à un VPN dans un domaine particulier. Par exemple, vous pouvez spécifier le domaine de votre organisation pour permettre aux utilisateurs d'accéder au contenu de votre intranet à l'aide d'un VPN à la demande.
Samsung Knox	Sur les terminaux Samsung Knox avec des activations Android Enterprise ou Samsung Knox Workspace, les applications professionnelles peuvent utiliser les profils VPN stockés sur le terminal pour se connecter au réseau de votre organisation. Vous pouvez activer un VPN par application afin de limiter ce dernier aux applications professionnelles que vous spécifiez. Vous devez installer une application client VPN prise en charge qui utilise KNOX SDK sur le terminal.
Windows 10	Vous pouvez configurer des profils VPN pour permettre aux applications de se connecter au réseau de votre organisation. Dans le profil VPN, vous pouvez spécifier une liste d'applications que le VPN doit utiliser.

Pour créer un profil VPN, vous pouvez également choisir d'utiliser CylanceGATEWAY pour créer un profil d'accès réseau ZTNA (Zero Trust Network Access) reconnu par les terminaux en tant que fournisseur VPN. CylanceGATEWAY ne fait confiance à personne par défaut. Pour plus d'informations, reportez-vous à Intégration de BlackBerry UEM à CylanceGATEWAY pour créer un profil ZTNA.

Créer un profil VPN

Les paramètres de profil requis varient pour chaque type de terminal et dépendent du type de connexion VPN et du type d'authentification que vous sélectionnez. Vous pouvez utiliser une variable de paramètre de profil correspondant à un champ de texte pour faire référence à une valeur plutôt que de spécifier la valeur réelle.

Pour créer un profil VPN, vous pouvez également choisir d'utiliser CylanceGATEWAY pour créer un profil d'accès réseau ZTNA (Zero Trust Network Access) reconnu par les terminaux en tant que fournisseur VPN. CylanceGATEWAY ne fait confiance à personne par défaut. Pour plus d'informations, reportez-vous à Intégration de BlackBerry UEM à CylanceGATEWAY pour créer un profil ZTNA.

Avant de commencer :

- Si les terminaux utilisent l'authentification basée sur des certificats pour les connexions VPN, créez un profil de certificat d'autorité de certification et attribuez-le aux comptes d'utilisateur, groupes d'utilisateurs ou groupes de terminaux. Pour envoyer les certificats client aux terminaux, créez un profil SCEP, un profil de certificat partagé ou un profil d' informations d'identification de l'utilisateur à associer au profil VPN.
- Pour les terminaux iOS, iPadOS, macOS et Samsung Knox qui utilisent un serveur proxy, créez un profil proxy à associer au profil VPN.
- Pour les terminaux Samsung Knox, ajoutez l'application client VPN qui convient à la liste des applications et attribuez-la aux comptes d'utilisateur, groupes d'utilisateurs ou groupes de terminaux. Les applications client VPN prises en charge sont Cisco AnyConnect et Juniper.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Réseaux et connexions > VPN**.
3. Cliquez sur +.
4. Tapez le nom et la description du RPV. Cette information s'affiche sur les terminaux.
5. Cliquez sur l'onglet correspondant à un type de terminal pour configurer les paramètres appropriés. Pour plus d'informations, reportez-vous aux paramètres de profil VPN relatifs à iOS et macOS, Android et Windows.

   Si votre organisation exige que les utilisateurs fournissent un nom d'utilisateur et un mot de passe pour se connecter au réseau VPN, saisissez `%UserName%` dans le champ **Nom d'utilisateur**.
6. Cliquez sur **Ajouter**.

À la fin : Attribuez le profil Wi-Fi aux comptes d'utilisateur, groupes d'utilisateurs et groupes de terminaux.

iOS et macOS : paramètres de profil VPN

iOS, iPadOS et macOS : paramètre de profil VPN	Description
Appliquer le profil à	Ce paramètre indique si le profil VPN sur un terminal macOS est appliqué au compte d'utilisateur ou au terminal.
Type de connexion	Ce paramètre spécifie le type de connexion utilisé par un terminal pour une passerelle VPN. Certains types de connexion requièrent également que les utilisateurs installent l'application VPN sur le terminal. Si vous sélectionnez IKEv2 Always On, de nombreux paramètres ont des valeurs distinctes pour les connexions cellulaires et Wi-Fi.
ID d'offre VPN	Ce paramètre spécifie l'ID d'offre de l'application VPN pour un VPN SSL personnalisé. L'ID d'offre est au format DNS inversé (par exemple, com.exemple.VPNapp). Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur Personnalisée.
Serveur	Ce paramètre spécifie le FQDN ou l'adresse IP d'un serveur VPN.

iOS, iPadOS et macOS : paramètre de profil VPN	Description
nom d'utilisateur ;	Ce paramètre spécifie le nom d'utilisateur utilisé par un terminal pour s'authentifier auprès de la passerelle VPN. Si le profil concerne plusieurs utilisateurs, vous pouvez utiliser la variable %UserName%.
Valeurs et clés personnalisées	Ce paramètre spécifie les clés et les valeurs associées du VPN SSL personnalisé. Les informations de configuration sont spécifiques à l'application VPN du fournisseur. Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur Personnalisée.
Groupe de connexion ou domaine	Ce paramètre spécifie le groupe de connexion ou le domaine utilisé par la passerelle VPN pour authentifier un terminal. Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur SonicWALL Mobile Connect.
Domaine	Ce paramètre spécifie le nom de domaine d'authentification utilisé par la passerelle VPN pour authentifier un terminal. Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur Juniper ou Pulse Secure.
Rôle	Ce paramètre spécifie le nom du rôle d'utilisateur utilisé par la passerelle VPN pour vérifier les ressources réseau auxquelles un terminal peut accéder. Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur Juniper ou Pulse Secure.
Type d'authentification	Ce paramètre spécifie le type d'authentification de la passerelle VPN. Le paramètre Type de connexion détermine les types d'authentification pris en charge et la valeur par défaut de ce paramètre.
Plug-ins EAP	Ce paramètre spécifie les plug-ins d'authentification du VPN. Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur L2TP ou PPTP et le paramètre Type d'authentification sur RSA SecurID.
Protocole d'authentification	Ce paramètre spécifie les protocoles d'authentification du VPN. Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur L2TP ou PPTP et le paramètre Type d'authentification sur RSA SecurID.
Mot de passe	Ce paramètre spécifie le mot de passe utilisé par un terminal pour s'authentifier auprès de la passerelle VPN. Ce paramètre est valide uniquement si le paramètre Type d'authentification est défini sur Mot de passe.

iOS, iPadOS et macOS : paramètre de profil VPN	Description
Nom de groupe	Ce paramètre spécifie le nom de groupe pour la passerelle VPN. Ce paramètre est valide uniquement dans les conditions suivantes : • Le paramètre Type de connexion est défini sur Cisco AnyConnect. • Le paramètre Type de connexion est défini sur IPsec et le paramètre Type d'authentification est défini sur Secret partagé/Nom de groupe.
Secret partagé	Ce paramètre spécifie le secret partagé à utiliser pour l'authentification VPN. Ce paramètre est valide uniquement dans les conditions suivantes : • Le paramètre Type de connexion est défini sur L2TP. • Le paramètre Type de connexion est défini sur IPsec et le paramètre Type d'authentification est défini sur Secret partagé/Nom de groupe. • Le paramètre Type de connexion est défini sur IKEv2 ou IKEv2 Always On et le paramètre Type d'authentification est défini sur Secret partagé.
Profil de certificat partagé	Ce paramètre spécifie le profil de certificat partagé avec le certificat client utilisé par un terminal pour s'authentifier auprès de la passerelle VPN. Ce paramètre est valide uniquement si le paramètre Type d'authentification est défini sur Certificat partagé.
Profil SCEP associé	Ce paramètre spécifie le profil SCEP associé utilisé par un terminal pour obtenir un certificat client et s'authentifier auprès du VPN. Ce paramètre est valide uniquement si le paramètre Type d'authentification est défini sur SCEP.
Profil des informations d'identification de l'utilisateur associé	Ce paramètre spécifie le profil d'informations d'identification de l'utilisateur associé utilisé par un terminal pour obtenir un certificat client et s'authentifier auprès du VPN. Ce paramètre est valide uniquement si le paramètre Type d'authentification est défini sur Informations d'identification de l'utilisateur.
Niveau de cryptage	Ce paramètre spécifie le niveau de cryptage des données pour la connexion VPN. Si ce paramètre est défini sur Automatique, tous les niveaux de cryptage sont autorisés. Si ce paramètre est défini sur Maximum, seul le cryptage maximum est autorisé. Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur PPTP.
Acheminer le trafic réseau via VPN	Ce paramètre spécifie si vous souhaitez acheminer le trafic réseau via une connexion VPN. Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur L2TP ou PPTP.

iOS, iPadOS et macOS : paramètre de profil VPN	Description
Utiliser une authentification hybride	Ce paramètre spécifie si vous souhaitez utiliser un certificat côté serveur pour l'authentification. Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur IPsec et le paramètre Type d'authentification sur Secret partagé/Nom de groupe.
Demander un mot de passe	Ce paramètre spécifie si un terminal invite l'utilisateur à saisir un mot de passe. Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur IPsec et le paramètre Type d'authentification sur Secret partagé/Nom de groupe.
Demander un code PIN à l'utilisateur	Ce paramètre spécifie si le terminal invite l'utilisateur à saisir un code PIN. Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur IPsec et le paramètre Type d'authentification sur Certificat partagé, SCEP ou Informations d'identification de l'utilisateur.
Adresse distante	Ce paramètre spécifie l'adresse IP ou le nom d'hôte du serveur VPN. Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur IKEv2 ou IKEv2 Always On.
ID local	Ce paramètre spécifie l'identité du client IKEv2 dans l'un des formats suivants : FQDN, UserFQDN, Adresse et ASN1DN. Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur IKEv2 ou IKEv2 Always On.
ID distant	Ce paramètre spécifie l'identifiant distant du client IKEv2 à l'aide de l'un des formats suivants : FQDN, FQDN de l'utilisateur, Adresse ou ASN1DN. Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur IKEv2 ou IKEv2 Always On.
Activer VPN à la demande	Ce paramètre spécifie si un terminal peut automatiquement établir une connexion VPN lorsqu'il accède à certains domaines. Pour les terminaux iOS et iPadOS, ce paramètre s'applique aux applications professionnelles. Ce paramètre est valide uniquement dans les conditions suivantes : • Le paramètre Type de connexion est défini sur IPsec, Cisco AnyConnect, Juniper, Pulse Secure, F5, SonicWALL Mobile Connect, Aruba VIA, Check Point Mobile, OpenVPN ou Personnalisée et le paramètre Type d'authentification sur Certificat partagé, SCEP ou Identifiants de l'utilisateur. • Le paramètre Type de connexion est défini sur IKEv2 et le paramètre Type d'authentification est défini sur Certificat partagé.

iOS, iPadOS et macOS : paramètre de profil VPN	Description
Domaine ou noms d'hôte pouvant utiliser un VPN à la demande	Ce paramètre spécifie les domaines et actions associées pour utiliser un VPN à la demande. Ce paramètre est valide uniquement si le paramètre Activer VPN à la demande est sélectionné.
Règles de VPN à la demande pour iOS 7.0 ou version ultérieure	Ce paramètre spécifie les exigences de connexion pour utiliser un VPN à la demande. Vous devez utiliser une ou plusieurs clés de l'exemple de format de charge utile. Ce paramètre remplace le paramètre Domaine ou noms d'hôte pouvant utiliser un VPN à la demande. Ce paramètre est valide uniquement si le paramètre Activer VPN à la demande est sélectionné.
Déconnecter en mode veille	Ce paramètre spécifie si la connexion VPN se déconnecte lorsqu'elle est en veille pendant une période donnée. Ce paramètre est valide uniquement si le paramètre Activer VPN à la demande est sélectionné.
Déconnecter en mode veille - Délai	Ce paramètre spécifie le délai d'inactivité en secondes après lequel le VPN se déconnecte. Ce paramètre est valide uniquement si le paramètre Déconnecter en mode veille est sélectionné.
Ne pas autoriser l'utilisateur à désactiver le VPN à la demande	Ce paramètre spécifie si l'utilisateur peut désactiver le VPN à la demande. Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur IPsec, Cisco AnyConnect, Juniper, Pulse Secure, F5, SonicWALL Mobile Connect, Aruba VIA, Check Point Mobile, OpenVPN ou Personnalisée.
Exclure le réseau local	Ce paramètre spécifie si vous souhaitez empêcher le trafic du réseau local d'utiliser la connexion VPN. Si le paramètre Inclure tous les réseaux est également sélectionné, aucun trafic réseau local n'est acheminé via le VPN.
Tous les routages autres que ceux par défaut sont prioritaires sur les routages définis localement	Ce paramètre spécifie si les routages autres que ceux par défaut pour le VPN sont prioritaires sur les routages définis localement. Si le paramètre Inclure tous les réseaux est également sélectionné, ce paramètre est ignoré. Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur Cisco AnyConnect, Juniper, Pulse Secure, F5, SonicWALL Mobile Connect, Aruba VIA, Check Point Mobile, OpenVPN ou Personnalisé.
Inclure tous les réseaux	Ce paramètre spécifie si vous souhaitez acheminer l'ensemble du trafic via le VPN. Si le paramètre Exclure le réseau local est également sélectionné, le trafic du réseau local n'est pas acheminé via le VPN. Ce paramètre s'applique uniquement aux terminaux exécutant iOS et iPadOS 13 et version ultérieure.

iOS, iPadOS et macOS : paramètre de profil VPN	Description
Fournisseur désigné requis	Ce paramètre spécifie un fournisseur VPN désigné. Si le fournisseur VPN est mis en œuvre en tant qu'extension système, ce paramètre est requis. Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur IPsec, Cisco AnyConnect, Juniper, Pulse Secure, F5, SonicWALL Mobile Connect, Aruba VIA, Check Point Mobile, OpenVPN ou Personnalisée.
Autoriser l'utilisateur à désactiver la connexion automatique	Ce paramètre spécifie si les utilisateurs peuvent désactiver la connexion VPN. Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur IKEv2 Always On.
Utiliser la même configuration de tunnel pour les réseaux cellulaires et Wi-Fi	Ce paramètre spécifie si vous souhaitez définir des paramètres VPN distincts pour le terminal, selon que le terminal envoie des données sur un réseau cellulaire ou un réseau Wi-Fi. Si ce paramètre n'est pas sélectionné, vous pouvez définir différents paramètres cellulaires et Wi-Fi dans le même profil. Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur IKEv2 Always On.
Activer xAuth	Ce paramètre spécifie si le VPN prend en charge l'authentification étendue. Ce paramètre est valide uniquement si le paramètre « Type de connexion » est défini sur « IKEv2 » ou « IKEv2 Always On ».
Version TLS minimale	Ce paramètre spécifie la version TLS minimale utilisée par les terminaux pour l'authentification EAP-TLS. Ce paramètre est valide uniquement si le paramètre Activer xAuth est sélectionné et que le type d'authentification est défini sur Certificat.
Version TLS maximale	Ce paramètre spécifie la version TLS maximale utilisée par les terminaux pour l'authentification EAP-TLS. Ce paramètre est valide uniquement si le paramètre Activer xAuth est sélectionné et que le type d'authentification est défini sur Certificat.
Type de certificat	Ce paramètre spécifie le type de certificat utilisé pour l'authentification de la machine IKEv2. Ce paramètre est valide uniquement si le paramètre Activer xAuth est sélectionné et que le type d'authentification est défini sur Certificat.
Nom commun de l'émetteur du certificat de serveur	Ce paramètre spécifie le nom usuel de l'autorité de certification ayant émis le certificat de serveur que le serveur IKE envoie au terminal. Si vous activez XAuth à l'aide d'un certificat, ce paramètre est requis. Ce paramètre est valide uniquement si le paramètre Activer xAuth est sélectionné et que le type d'authentification est défini sur Certificat.

iOS, iPadOS et macOS : paramètre de profil VPN	Description
Nom commun du certificat de serveur	Ce paramètre spécifie le nom usuel du certificat de serveur que le serveur IKE envoie au terminal. Ce paramètre est valide uniquement si le paramètre Activer xAuth est sélectionné et que le type d'authentification est défini sur Certificat.
Intervalle keepalive	Ce paramètre spécifie la fréquence à laquelle un terminal envoie un paquet keepalive. Ce paramètre est valide uniquement si le paramètre « Type de connexion » est défini sur « IKEv2 » ou « IKEv2 Always On ».
Désactiver MOBIKE	Ce paramètre indique si le MOBIKE est désactivé. Ce paramètre est valide uniquement si le paramètre « Type de connexion » est défini sur « IKEv2 » ou « IKEv2 Always On ».
Désactiver la redirection IKEv2	Ce paramètre spécifie si la redirection IKEv2 est désactivée. Si ce paramètre n'est pas coché, la connexion IKEv2 est redirigée si une demande de redirection est reçue à partir du serveur. Ce paramètre est valide uniquement si le paramètre « Type de connexion » est défini sur « IKEv2 » ou « IKEv2 Always On ».
Activer Perfect Forward Secrecy (confidentialité totale des transferts)	Ce paramètre spécifie si la passerelle VPN prend en charge le PFS. Ce paramètre est valide uniquement si le paramètre « Type de connexion » est défini sur « IKEv2 » ou « IKEv2 Always On ».
Activer NAT keepalive	Ce paramètre spécifie si la passerelle VPN prend en charge les paquets keepalive NAT. Les paquets keepalive sont utilisés pour maintenir les mappages NAT pour les connexions IKEv2. Ce paramètre est valide uniquement si le paramètre « Type de connexion » est défini sur « IKEv2 » ou « IKEv2 Always On ».
Intervalle NAT keepalive	Ce paramètre spécifie la fréquence à laquelle un terminal envoie un paquet NAT keepalive (en secondes). Ce paramètre n'est valide que si le paramètre Type de connexion est défini sur IKEv2 ou IKEv2 Always On et si le paramètre Activer NAT keepalive est sélectionné.
Utiliser les sous-réseaux internes IPv4 et IPv6 IKEv2	Ce paramètre indique si le VPN peut utiliser l'attribut de configuration IKEv2 INTERNAL_IP4_SUBNET et INTERNAL_IP6_SUBNET. Ce paramètre est valide uniquement si le paramètre « Type de connexion » est défini sur « IKEv2 » ou « IKEv2 Always On ».
Nom commun du certificat de serveur	Ce paramètre spécifie le nom usuel du certificat envoyé par le serveur IKE au terminal. Ce paramètre est valide uniquement si le paramètre « Type de connexion » est défini sur « IKEv2 » ou « IKEv2 Always On ».

iOS, iPadOS et macOS : paramètre de profil VPN	Description
Nom commun de l'émetteur du certificat de serveur	Ce paramètre spécifie le nom usuel de l'émetteur du certificat dans le certificat envoyé par le serveur IKE au terminal. Ce paramètre est valide uniquement si le paramètre « Type de connexion » est défini sur « IKEv2 » ou « IKEv2 Always On ».
Activer la vérification de révocation de certificat	Ce paramètre indique si une vérification de révocation de certificat est tentée pour le certificat du serveur. La vérification n'échoue pas s'il n'y a pas de réponse. Ce paramètre est valide uniquement si le paramètre « Type de connexion » est défini sur « IKEv2 » ou « IKEv2 Always On ».
Activer la fonction de secours	Ce paramètre spécifie si le terminal peut établir un tunnel VPN sur le réseau mobile lorsque Wi-Fi Assist est activé. Ce paramètre s'applique uniquement aux terminaux exécutant iOS et iPadOS 13 et versions ultérieures, et exige que le serveur prenne en charge plusieurs tunnels pour les utilisateurs individuels. Ce paramètre est valide uniquement si le paramètre « Type de connexion » est défini sur « IKEv2 » ou « IKEv2 Always On ».
Appliquer les paramètres d'association de sécurité enfant	Ce paramètre spécifie s'il faut appliquer les paramètres d'association de sécurité enfant. Ce paramètre est valide uniquement si le paramètre « Type de connexion » est défini sur « IKEv2 » ou « IKEv2 Always On ».
Appliquer les paramètres d'association de sécurité IKE	Ce paramètre spécifie s'il faut appliquer les paramètres d'association de sécurité IKE. Ce paramètre est valide uniquement si le paramètre « Type de connexion » est défini sur « IKEv2 » ou « IKEv2 Always On ».
MTU	Ce paramètre spécifie l'unité de transmission maximale en octets. Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur IKEv2 Always On.
Messagerie vocale	Ce paramètre spécifie si les connexions au service de messagerie vocale sont envoyées via le tunnel VPN, envoyées en dehors du tunnel VPN ou bloquées. Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur IKEv2 Always On. Il s'applique uniquement aux connexions Wi-Fi.
AirPrint	Ce paramètre spécifie si les connexions AirPrint sont envoyées via le tunnel VPN, envoyées en dehors du tunnel VPN ou bloquées. Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur IKEv2 Always On. Il s'applique uniquement aux connexions Wi-Fi.
Autoriser le trafic d'une page Web captive en dehors du tunnel VPN	Ce paramètre spécifie si le trafic des feuilles Web captives peut être envoyé en dehors du tunnel VPN. Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur IKEv2 Always On. Il s'applique uniquement aux connexions Wi-Fi.

iOS, iPadOS et macOS : paramètre de profil VPN	Description
Autoriser le trafic des applications de réseaux sociaux captives en dehors du tunnel VPN	Ce paramètre spécifie si le trafic de toutes les applications de réseaux sociaux captives peut être envoyé en dehors du tunnel VPN. Si ce paramètre n'est pas sélectionné, vous pouvez spécifier des applications individuelles pour lesquelles le trafic peut être envoyé en dehors du tunnel. Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur IKEv2 Always On. Il s'applique uniquement aux connexions Wi-Fi.
Le trafic provenant de ces applications est autorisé en dehors du tunnel VPN	Ce paramètre spécifie les applications de réseaux sociaux captives individuelles pour lesquelles le trafic peut être envoyé en dehors du tunnel. Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur IKEv2 Always On. Il s'applique uniquement aux connexions Wi-Fi.
Autoriser le trafic des applications en dehors du tunnel VPN	Ce paramètre spécifie les applications dont le trafic peut être envoyé en dehors du tunnel. Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur IKEv2 Always On. Il s'applique uniquement aux connexions Wi-Fi.
Groupe DH	Ce paramètre spécifie le groupe DH utilisé par un terminal pour générer les clés. Ce paramètre n'est valide que si le paramètre Appliquer les paramètres de sécurité d'association enfant ou Appliquer les paramètres d'association de sécurité IKE est sélectionné.
Algorithme de cryptage	Ce paramètre spécifie l'algorithme de cryptage IKE. Ce paramètre n'est valide que si le paramètre Appliquer les paramètres de sécurité d'association enfant ou Appliquer les paramètres d'association de sécurité IKE est sélectionné.
Algorithme d'intégrité	Ce paramètre spécifie l'algorithme d'intégrité IKE. Ce paramètre n'est valide que si le paramètre Appliquer les paramètres de sécurité d'association enfant ou Appliquer les paramètres d'association de sécurité IKE est sélectionné.
Intervalle de renouvèlement de clés	Ce paramètre spécifie la durée de vie de la connexion IKE. Ce paramètre n'est valide que si le paramètre Appliquer les paramètres de sécurité d'association enfant ou Appliquer les paramètres d'association de sécurité IKE est sélectionné.

iOS, iPadOS et macOS : paramètre de profil VPN	Description
Activer un VPN par application	Ce paramètre spécifie si la passerelle VPN prend en charge un VPN par application. Cette fonction permet de diminuer la charge d'un VPN d'entreprise. Par exemple, vous pouvez activer un trafic professionnel spécifique sur le VPN, comme l'accès aux serveurs d'applications ou aux pages Web derrière un pare-feu. Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur Cisco AnyConnect, Juniper, Pulse Secure, F5, SonicWALL Mobile Connect, Aruba VIA, Check Point Mobile, OpenVPN, Personnalisée, IKEv2 ou IKEv2 Always On.
Autoriser la connexion automatique des applications	Ce paramètre spécifie si les applications associées au VPN par application peuvent établir automatiquement la connexion VPN. Ce paramètre est valide uniquement si le paramètre Activer VPN par application est sélectionné.
Domaines Safari	Ce paramètre spécifie les domaines pouvant établir la connexion VPN dans Safari. Ce paramètre est valide uniquement si le paramètre Activer VPN par application est sélectionné.
Domaines Calendrier	Ce paramètre spécifie les domaines pouvant établir la connexion VPN dans Calendrier. Ce paramètre est valide uniquement si le paramètre Activer VPN par application est sélectionné.
Domaines Contacts	Ce paramètre spécifie les domaines pouvant établir la connexion VPN dans Contacts. Ce paramètre est valide uniquement si le paramètre Activer VPN par application est sélectionné.
Domaines Messagerie	Ce paramètre spécifie les domaines pouvant établir la connexion VPN dans Messagerie. Ce paramètre est valide uniquement si le paramètre Activer VPN par application est sélectionné.
Domaines associés	Ce paramètre spécifie les domaines pouvant établir la connexion VPN sur le terminal. Les domaines doivent également être inclus dans le fichier apple-app-site-association. Ce paramètre est valide uniquement si le paramètre Activer VPN par application est sélectionné.
Domaines exclus	Ce paramètre spécifie les domaines ne pouvant pas établir de connexion VPN sur le terminal. Ce paramètre est valide uniquement si le paramètre Activer VPN par application est sélectionné.

iOS, iPadOS et macOS : paramètre de profil VPN	Description
Tunnellisation du trafic	Ce paramètre indique si le VPN achemine le trafic vers la couche d'application ou la couche IP. Ce paramètre est valide uniquement si le paramètre Activer VPN par application est sélectionné.
Profil proxy associé	Ce paramètre spécifie le profil proxy associé utilisé par un terminal pour se connecter à un serveur proxy lorsque le terminal est connecté au VPN.

Android : paramètres de profil VPN

Les paramètres de profil VPN suivants sont uniquement pris en charge sur les terminaux Samsung Knox.

Android : paramètre de profil VPN	Description
Adresse du serveur	Ce paramètre spécifie le FQDN ou l'adresse IP d'un serveur VPN.
Type de VPN	Ce paramètre spécifie si un terminal utilise le protocole IPsec ou SSL pour se connecter au serveur VPN. L'application Juniper VPN prend uniquement en charge le protocole SSL.
Authentification de l'utilisateur requise	Ce paramètre spécifie si un utilisateur de terminal doit fournir un nom d'utilisateur et un mot de passe pour se connecter au serveur VPN.
nom d'utilisateur ;	Ce paramètre spécifie le nom d'utilisateur utilisé par un terminal pour s'authentifier auprès de la passerelle VPN. Si le profil concerne plusieurs utilisateurs, vous pouvez utiliser la variable %UserName%. Ce paramètre est valide uniquement si le paramètre Authentification de l'utilisateur requise est sélectionné.
Mot de passe	Ce paramètre spécifie le mot de passe utilisé par un terminal pour s'authentifier auprès de la passerelle VPN. Ce paramètre est valide uniquement si le paramètre Authentification de l'utilisateur requise est sélectionné.
Type de tunnellisation fractionnée	Ce paramètre spécifie si un terminal peut utiliser la tunnellisation fractionnée pour contourner la passerelle VPN (sous réserve de prise en charge par la passerelle VPN). Si le paramètre Type de VPN est défini sur IPsec, ce paramètre doit être défini sur Désactivé.
Itinéraires de transfert	Ce paramètre spécifie le(s) cheminement(s) contournant la passerelle VPN. Vous pouvez spécifier une ou plusieurs adresses IP. Ce paramètre est valide uniquement si le paramètre Type de VPN est défini sur SSL et le paramètre Type de tunnellisation fractionnée sur Manuel.

Android : paramètre de profil VPN	Description
DPD	Ce paramètre indique si le protocole DPD est activé. Ce paramètre est valide uniquement si le paramètre Type de VPN est défini sur IPsec.
Version IKE	Ce paramètre spécifie la version du protocole IKE à utiliser avec la connexion VPN. Ce paramètre est valide uniquement si le paramètre Type de VPN est défini sur IPsec.
Type d'authentification IPsec	Ce paramètre spécifie le type d'authentification d'une connexion VPN IPsec. Le paramètre Version IKE détermine les types d'authentification IPsec pris en charge et la valeur par défaut de ce paramètre. Ce paramètre est valide uniquement si le paramètre Type de VPN est défini sur IPsec.
Type d'ID de groupe IPsec	Ce paramètre spécifie le type d'ID de groupe IPsec de la connexion VPN. Le paramètre Type d'authentification IPsec détermine les types d'ID de groupe IPsec pris en charge et la valeur par défaut de ce paramètre. Si le paramètre Type d'authentification IPsec correspond à Certificat, ce paramètre est automatiquement défini sur Par défaut. Ce paramètre est valide uniquement si le paramètre Type de VPN est défini sur IPsec.
ID de groupe IPsec	Ce paramètre spécifie l'ID de groupe IPsec de la connexion VPN. Ce paramètre est valide uniquement si le paramètre Type de VPN est défini sur IPsec.
Mode d'échange de clé de la phase 1 IKE	Ce paramètre spécifie le mode d'échange de la connexion VPN. Ce paramètre est valide uniquement si le paramètre Type de VPN est défini sur IPsec.
Durée de vie IKE	Ce paramètre spécifie la durée de vie de la connexion IKE (en secondes). Si vous définissez une valeur non prise en charge ou une valeur nulle, la valeur par défaut du terminal est utilisée. Ce paramètre est valide uniquement si le paramètre Type de VPN est défini sur IPsec.
Algorithme de cryptage IKE	Ce paramètre spécifie l'algorithme de cryptage utilisé pour la connexion IKE. Ce paramètre est valide uniquement si le paramètre Type de VPN est défini sur IPsec.
Algorithme d'intégrité IKE	Ce paramètre indique l'algorithme d'intégrité utilisé pour la connexion IKE. Ce paramètre est valide uniquement si le paramètre « Type de VPN » est défini sur « IPsec » et le paramètre « Version IKE » sur « IKEv2 ».

Android : paramètre de profil VPN	Description
Groupe DH IPsec	Ce paramètre spécifie le groupe DH utilisé par un terminal pour générer les clés. Ce paramètre est valide uniquement si le paramètre Type de VPN est défini sur IPsec.
Paramètre IPsec	Ce réglage définit le paramètre IPsec utilisé pour la connexion VPN. Ce paramètre est valide uniquement si le paramètre Type de VPN est défini sur IPsec.
Perfect Forward Secrecy (confidentialité totale des transferts)	Ce paramètre spécifie si la passerelle VPN prend en charge PFS. Ce paramètre est valide uniquement si le paramètre Type de VPN est défini sur IPsec.
Activer MOBIKE	Ce paramètre spécifie si la passerelle VPN prend en charge MOBIKE. Ce paramètre est valide uniquement si le paramètre Type de VPN est défini sur IPsec.
Durée de vie IPsec	Ce paramètre spécifie la durée de vie de la connexion IPsec (en secondes). Si vous définissez une valeur non prise en charge ou une valeur nulle, la valeur par défaut du terminal est utilisée. Ce paramètre est valide uniquement si le paramètre Type de VPN est défini sur IPsec.
Algorithme de cryptage IPsec	Ce paramètre spécifie l'algorithme de cryptage IPsec utilisé pour la connexion VPN. Ce paramètre est valide uniquement si le paramètre Type de VPN est défini sur IPsec.
Algorithme d'intégrité IPsec	Ce paramètre indique l'algorithme d'intégrité IPsec utilisé pour la connexion VPN. Ce paramètre est valide uniquement si le paramètre « Type de VPN » est défini sur « IPsec » et le paramètre « Version IKE » sur « IKEv2 ».
Type d'authentification	Ce paramètre spécifie le type d'authentification de la passerelle VPN. Ce paramètre est valide uniquement si le paramètre « Type de VPN » est défini sur « SSL ».
Algorithme SSL	Ce paramètre spécifie l'algorithme de cryptage requis pour une connexion VPN SSL. Ce paramètre est valide uniquement si le paramètre « Type de VPN » est défini sur « SSL ».
Ajouter des informations UID/PID	Ce paramètre spécifie si les informations UID et PID sont ajoutées aux paquets envoyés au client VPN. Ce paramètre doit être sélectionné pour l'application Cisco AnyConnect VPN.

Android : paramètre de profil VPN	Description
Chainage de prise en charge	Ce paramètre spécifie comment le chainage VPN est pris en charge.
Type de saisie de la chaine fournisseur	Ce paramètre spécifie les paires clé-valeur ou la chaine JSON du VPN. Les informations de configuration sont spécifiques à l'application VPN du fournisseur.
Paires clé-valeur du fournisseur	Ce paramètre spécifie les clés et les valeurs associées du VPN. Les informations de configuration sont spécifiques à l'application VPN du fournisseur. Ce paramètre est uniquement valide si le paramètre Type de saisie de la chaine fournisseur est défini sur Paires valeur-clé du fournisseur.
Valeur JSON du fournisseur	Ce paramètre spécifie les informations de configuration propres à l'application VPN du fournisseur au format .json. Ce paramètre est uniquement valide si le paramètre Type de saisie de la chaine fournisseur est défini sur Valeur JSON du fournisseur.
ID du progiciel client VPN	Ce paramètre spécifie l'ID de package de l'application VPN.
Essayer automatiquement de se reconnecter après une erreur	Ce paramètre spécifie si la connexion VPN doit être automatiquement redémarrée après que la connexion ait été perdue.
Activer le mode FIPS	Ce paramètre spécifie si le protocole FIPS est activé. L'activation du mode FIPS veille à ce que seuls les algorithmes cryptographiques soient utilisés pour la connexion VPN.
Connectivité d'entreprise pour les terminaux Android comprenant un espace Travail	Ce paramètre indique si les terminaux Samsung Knox utilisent une connexion VPN pour toutes les applications dans l'espace Travail ou seulement pour les applications spécifiées. • « VPN à l'échelle du conteneur » utilise une connexion VPN pour toutes les applications dans l'espace Travail sur le terminal. • « VPN par application » utilise une connexion VPN uniquement pour les applications spécifiées.
Applications autorisées à utiliser la connexion VPN	Ce paramètre indique les applications dans l'espace Travail qui peuvent utiliser une connexion VPN. Vous pouvez sélectionner les applications dans la liste des applications disponibles ou spécifier l'ID de package d'application. Ce paramètre est valide uniquement si le paramètre Connectivité d'entreprise pour les terminaux Android comprenant un espace Travail est défini sur VPN par application.
Profil proxy associé	Ce paramètre spécifie le profil proxy associé utilisé par un terminal pour se connecter à un serveur proxy lorsque le terminal est connecté au VPN.

Windows 10 : paramètres de profil VPN

Windows : paramètre de profil VPN	Description
Type de connexion	Ce paramètre spécifie le type de connexion utilisé par un terminal Windows 10 pour un VPN.
Serveur	Ce paramètre spécifie l'adresse IP publique ou routable ou le nom DNS pour le VPN. Ce paramètre peut pointer vers l'IP externe d'un VPN, ou une adresse IP virtuelle pour un parc de serveurs. Ce paramètre est valide uniquement si le Type de connexion est défini sur Microsoft.
Liste d'URL de serveur	Ce paramètre spécifie une liste séparée par des virgules des serveurs au format URL, nom d'hôte ou format IP. Ce paramètre est valide uniquement si le paramètre Type de connexion n'est pas défini sur Microsoft.
Type de stratégie de routage	Ce paramètre spécifie le type de stratégie de routage. Ce paramètre est valide uniquement si le Type de connexion est défini sur Microsoft.
Type de protocole intégré	Ce paramètre spécifie le type de stratégie de routage utilisé par le VPN. Ce paramètre est valide uniquement si le Type de connexion est défini sur Microsoft.
Authentification	Ce paramètre indique la méthode d'authentification utilisée pour le VPN natif. Le paramètre Type de protocole intégré détermine les méthodes d'authentification prises en charge et la valeur par défaut de ce paramètre.
Configuration EAP	Ce paramètre spécifie le code XML de la configuration EAP. Ce paramètre est valide uniquement si le paramètre Authentification est défini sur EAP.
Méthode utilisateur	Ce paramètre indique le type d'authentification de méthode utilisateur à utiliser. Ce paramètre est valide uniquement si le paramètre Authentification est défini sur Méthode utilisateur.
Méthode machine	Ce paramètre indique le type d'authentification de méthode machine à utiliser. Ce paramètre est valide uniquement si le paramètre Authentification est défini sur Méthode machine.
Configuration personnalisée	Ce paramètre indique le blob XML en code HTML pour une configuration de plug-in SSL-VPN spécifique, avec les informations d'authentification envoyées au terminal pour la prise en charge des plug-ins SSL-VPN. Ce paramètre est valide uniquement si le paramètre Type de connexion n'est pas défini sur Microsoft.

Windows : paramètre de profil VPN	Description
Nom de la famille de package de plug-ins	Ce paramètre spécifie le nom de famille de package du VPN SSL personnalisé. Ce paramètre est valide uniquement si le Type de connexion est défini sur Définition de la connexion manuelle.
Clé pré-partagée L2TP	Ce paramètre spécifie la clé pré-partagée utilisée pour une connexion L2TP.
Liste d'applications de déclenchement	Ce paramètre spécifie une liste d'applications qui démarrent la connexion VPN.
Liste d'applications de déclenchement > ID d'application	Ce paramètre identifie une application pour un VPN par application. Valeurs possibles : • Nom de la famille de package. Pour trouver le nom de famille de package, installez l'application et exécutez la commande Windows PowerShell, `Get-AppxPackage`. • Emplacement d'installation de l'application. Par exemple, C:\Windows\System\notepad.exe.
Liste des itinéraires	Ce paramètre spécifie une liste des itinéraires que le VPN peut emprunter. Si le VPN utilise la tunnellisation fractionnée, une liste des itinéraires est requise.
Adresse du sous-réseau	Ce paramètre spécifie l'adresse IP du préfixe de destination au format d'adresse IPv4 ou IPv6.
Préfixe de sous-réseau	Ce paramètre spécifie le préfixe de sous-réseau du préfixe de destination.
Exclusion	Ce paramètre indique si le routage qui est ajouté doit pointer vers l'interface VPN via la passerelle ou l'interface physique. Si vous cochez la case, le trafic est dirigé vers l'interface physique. Si vous ne la cochez pas, le trafic est dirigé vers le VPN.
Liste des noms de domaines	Ce paramètre spécifie les règles NRPT pour le VPN.
Nom de domaine	Ce paramètre spécifie le nom complet ou le suffixe du domaine.
Serveurs DNS	Ce paramètre spécifie la liste des adresses IP des serveurs DNS en les séparant par des virgules.
Serveur Web proxy	Ce paramètre spécifie l'adresse IP du serveur Web proxy.
Déclencheur de VPN	Ce paramètre indique si cette règle de nom de domaine déclenche le VPN.
Permanent	Ce paramètre indique si la règle de nom de domaine est appliquée lorsque le VPN n'est pas connecté.
Liste des filtres de trafic	Ce paramètre spécifie les règles autorisant le trafic via le VPN.

Windows : paramètre de profil VPN	Description
Liste des filtres de trafic > ID d'application	Ce paramètre identifie une application pour un filtre de trafic basé sur l'application. Valeurs possibles : • Nom de la famille de package. Pour trouver le nom de famille de package, installez l'application et exécutez la commande Windows PowerShell, `Get-AppxPackage`. • Emplacement d'installation de l'application. Par exemple, `C:\Windows\System\Notepad.exe`. • Tapez SYSTEM pour que les pilotes du noyau puissent envoyer le trafic par le biais du VPN (par exemple, PING ou SMB).
Protocole	Ce paramètre spécifie le protocole utilisé par le VPN.
Plages de ports locaux	Ce paramètre spécifie la liste des plages de ports locaux autorisées en les séparant par des virgules. Par exemple, 100-120, 200, 300-320.
Plages de ports distants	Ce paramètre spécifie la liste des plages de ports distants autorisées en les séparant par des virgules. Par exemple, 100-120, 200, 300-320.
Plages d'adresses locales	Ce paramètre spécifie la liste des plages d'adresses IP locales autorisées en les séparant par des virgules.
Plages d'adresses distantes	Ce paramètre spécifie la liste des plages d'adresses IP distantes autorisées en les séparant par des virgules.
Type de stratégie de routage	Ce paramètre spécifie la stratégie de routage utilisée par le filtre de trafic. Si vous le définissez sur Forcer le tunnel, tout le trafic passe par le VPN. Si vous le définissez sur Tunnel partagé, le trafic peut passer par le VPN ou Internet.
Mémoriser les informations d'identification	Ce paramètre spécifie si les identifiants doivent être mis en cache lorsque cela est possible.
Toujours activer	Ce paramètre spécifie si les terminaux se connectent automatiquement au VPN lors de l'authentification et restent connectés jusqu'à ce que l'utilisateur déconnecte manuellement le VPN.
Verrouiller	Ce paramètre spécifie si cette connexion VPN doit être utilisée lorsque le terminal se connecte à un réseau. Lorsque ce paramètre est activé, les points suivants s'appliquent : • Le terminal reste connecté au VPN. Il ne peut pas être déconnecté. • Le terminal doit être connecté à ce VPN pour disposer d'une connexion réseau. • Le terminal ne peut pas se connecter à, ou modifier, d'autres profils VPN.

Windows : paramètre de profil VPN	Description
Suffixe DNS	Ce paramètre spécifie un ou plusieurs suffixes DNS séparés par des virgules. Le premier suffixe DNS de la liste est également utilisé en tant que connexion principale pour le VPN. La liste est ajoutée à SuffixSearchList.
Détection de réseau sécurisé	Ce paramètre spécifie une chaine séparée par des virgules pour identifier le réseau sécurisé. Le VPN ne se connecte pas automatiquement lorsque les utilisateurs sont sur le réseau sans fil de leur entreprise.
Propriétés de la sécurité IP	
Constantes de transformation de l'authentification	Ce paramètre spécifie le niveau d'authentification d'un VPN. Ce paramètre doit correspondre au paramètre du serveur VPN.
Constantes de transformation du chiffrement	Ce paramètre spécifie le niveau de cryptage d'un VPN. Ce paramètre doit correspondre au paramètre du serveur VPN.
Méthode de cryptage	Ce paramètre spécifie le niveau de cryptage de la phase 1 d'un VPN. Ce paramètre doit correspondre au paramètre du serveur VPN.
Méthode de vérification de l'intégrité	Ce paramètre spécifie le niveau d'authentification de la phase 1 d'un VPN. Ce paramètre doit correspondre au paramètre du serveur VPN.
Groupe Diffie-Hellman	Ce paramètre spécifie le groupe de clés d'un VPN. Ce paramètre doit correspondre au paramètre du serveur VPN.
Groupe PFS	Ce paramètre spécifie le protocole de cryptage Perfect Forward Secrecy (confidentialité totale des transferts) utilisé pour le VPN. Ce paramètre doit correspondre au paramètre du serveur VPN.
Type de proxy	Ce paramètre spécifie le type de configuration proxy pour le VPN.
URL du fichier PAC	Ce paramètre spécifie l'URL du serveur Web qui héberge le fichier PAC, y compris le nom du fichier PAC. Par exemple, http://www.example.com/PACfile.pac. Ce paramètre est valide uniquement si le paramètre Type de proxy est défini sur Configuration PAC.
Adresse	Ce paramètre spécifie le FQDN ou l'adresse IP du serveur proxy. Ce paramètre est valide uniquement si le paramètre Type de proxy est défini sur Configuration manuelle.
Profil SCEP associé	Ce paramètre spécifie le profil SCEP associé utilisé par un terminal pour obtenir un certificat client et s'authentifier auprès du VPN.

Intégration de BlackBerry UEM à CylanceGATEWAY pour créer un profil ZTNA

Au lieu d'utiliser un profil VPN, vous pouvez intégrer votre instance d'UEM à CylanceGATEWAY. CylanceGATEWAY est une solution ZTNA (accès réseau Zero Trust) assistée par intelligence artificielle (IA) et basée sur le

cloud qui peut être activée pour votre locataire Cylance Endpoint Security. Vous pouvez ensuite configurer CylanceGATEWAY sur la console de gestion Cylance. Pour plus d'informations sur la configuration de CylanceGATEWAY, reportez-vous à la section Configuration de BlackBerry Gateway dans le contenu relatif à la configuration d'Cylance Endpoint Security. Lorsque CylanceGATEWAY est activé sur un terminal, vous créez un profil ZTNA que le terminal reconnait en tant que fournisseur VPN. CylanceGATEWAY ne fait confiance à personne par défaut.

CylanceGATEWAY protège les terminaux iOS, Android, Windows 10 et 11, et macOS de vos utilisateurs en vous permettant de bloquer les connexions aux destinations Internet auxquelles vous ne souhaitez qu'ils accèdent, même lorsque les terminaux ne sont pas connectés à votre réseau.

En plus de protéger les terminaux, CylanceGATEWAY protège l'accès au réseau privé et aux applications reposant sur le cloud de votre entreprise, en analysant en permanence si les habitudes d'utilisation des utilisateurs sont attendues ou anormales. Si le pourcentage d'évènements anormaux dépasse un seuil défini, CylanceGATEWAY peut remplacer dynamiquement la stratégie de contrôle d'accès réseau de l'utilisateur pour bloquer l'accès au réseau et demander à l'utilisateur de s'authentifier avant de continuer.

Les administrateurs CylanceGATEWAY peuvent configurer les destinations Internet et réseau privé auxquelles les utilisateurs peuvent accéder ou non.

Activation et attribution des paramètres VPN par application

Pour les terminaux iOS, iPadOS, Samsung Knox et Windows, vous pouvez configurer un VPN par application afin de spécifier les applications du terminal qui doivent utiliser un VPN pour leurs données en transit. Un VPN par application permet de diminuer la charge du VPN de votre organisation en limitant son utilisation à certaines charges du trafic professionnel (l'accès aux serveurs d'applications ou aux pages Web derrière le pare-feu, par exemple). Dans les environnements sur site, cette fonction prend également en charge la confidentialité de l'utilisateur et augmente la vitesse de connexion des applications personnelles en n'acheminant pas le trafic personnel via le VPN.

Terminaux	Paramètres d'application
iOS et iPadOS	Les applications sont associées à un profil VPN lorsque vous attribuez l'application ou le groupe d'applications à un utilisateur, un groupe d'utilisateurs ou un groupe de terminaux.
Terminaux Samsung Knox avec activations Android Enterprise et Samsung Knox Workspace	Les applications sont ajoutées au paramètre Applications autorisées à utiliser la connexion VPN dans le profil VPN.
Windows 10	Les applications sont ajoutées au paramètre Liste d'applications de déclenchement dans le profil VPN.

Un seul profil VPN peut être attribué à une application ou à un groupe d'applications.

BlackBerry UEM utilise les règles suivantes pour déterminer les paramètres VPN par application à attribuer à une application sur les terminaux iOS et iPadOS :

Paramètres VPN par application	Priorité
S'ils sont directement associés à une application	Sont prioritaires sur les paramètres VPN par application associés indirectement par un groupe d'applications.
S'ils sont directement associés à un utilisateur	Sont prioritaires sur les paramètres VPN par application associés indirectement par un groupe d'utilisateurs.
S'ils sont attribués à une application requise	Sont prioritaires sur les paramètres VPN par application attribués à une instance facultative de la même application.
S'ils sont associés au nom du groupe d'utilisateurs qui apparait plus haut dans la liste alphabétique	Sont prioritaires si les conditions suivantes sont remplies : • Une application est attribuée à plusieurs groupes d'utilisateurs • La même application apparait dans les groupes d'utilisateurs • L'application est attribuée de la même manière, en tant qu'application seule ou groupe d'applications • L'application a la même disposition dans toutes les attributions (obligatoire ou facultative) Par exemple, vous attribuez Cisco WebEx Meetings en tant qu'application facultative aux groupes d'utilisateurs Développement et Marketing. Lorsqu'un utilisateur est dans les deux groupes, les paramètres VPN d'application du groupe Développement sont appliqués à l'application WebEx Meetings pour cet utilisateur.

Si un profil VPN d'application est attribué à un groupe de terminaux, il est prioritaire sur le profil VPN d'application qui est attribué au compte d'utilisateur des terminaux qui appartiennent au groupe de terminaux.

Création de profils proxy pour les terminaux

Vous pouvez spécifier la manière dont les terminaux utilisent un serveur proxy pour accéder à des services Web sur Internet ou un réseau professionnel. Pour les terminaux iOS, iPadOS, macOS et Android, vous devez créer un profil proxy. Pour les terminaux Windows 10, vous devez ajouter les paramètres de proxy dans Wi-Fi ou dans le profil VPN.

Sauf indication contraire, les profils proxy prennent en charge les serveurs proxy qui utilisent l'authentification de base ou qui n'utilisent aucune authentification.

Terminal	Configuration du proxy
iOS et iPadOS	Créez un profil proxy et associez-le à un profil Wi-Fi ou VPN. Vous pouvez attribuer un profil proxy à des comptes d'utilisateur, à des groupes d'utilisateurs ou à des groupes de terminaux. Un profil proxy attribué à des comptes d'utilisateur, groupes d'utilisateurs ou groupes de terminaux est un proxy global réservé aux terminaux supervisés et prioritaire sur un profil proxy associé à un profil Wi-Fi ou VPN. Les terminaux supervisés utilisent les paramètres proxy globaux pour toutes les connexions HTTP.

Terminal	Configuration du proxy
macOS	Créez un profil proxy et associez-le à un profil Wi-Fi ou VPN. macOS applique les profils aux terminaux ou comptes d'utilisateur. Les profils de proxy sont appliqués aux terminaux.
Android	Pour les terminaux Android Enterprise, créez un profil proxy et associez-le à un profil Wi-Fi. Les terminaux Android auxquels est attribué le type d'activation Contrôles MDM ou Confidentialité de l'utilisateur ne prennent pas en charge les profils Wi-Fi avec des paramètres de proxy.
Samsung Knox	Créez un profil proxy et associez-le à un profil de connectivité, Wi-Fi, VPN ou d'entreprise. Les conditions suivantes s'appliquent : • Pour les profils Wi-Fi, seuls les profils proxy possédant une configuration manuelle sont pris en charge sur les terminaux Knox. Les profils proxy que vous associez aux profils Wi-Fi prennent en charge les serveurs proxy utilisant l'authentification de base, NTML ou aucune authentification. • Pour les profils VPN et de connectivité d'entreprise, les profils proxy avec une configuration manuelle sont pris en charge sur les terminaux Samsung Knox avec des activations Android Enterprise et des terminaux Samsung Knox Workspace qui utilisent Knox 2.5 et versions ultérieures. Les profils proxy avec configuration PAC sont pris en charge sur les terminaux Samsung Knox avec des activations Android Enterprise et des terminaux Knox Workspace qui utilisent une version de Knox ultérieure à la version 2.5. Vous pouvez attribuer un profil proxy à des comptes d'utilisateur, à des groupes d'utilisateurs ou à des groupes de terminaux. Les conditions suivantes s'appliquent : • Sur les terminaux Knox Workspace et Samsung Knox avec des activations Android Enterprise, le profil configure les paramètres de proxy du navigateur de l'espace Travail. • Sur les terminaux Samsung Knox MDM, le profil configure les paramètres de proxy du navigateur sur le terminal. • La configuration du CCP n'est pas prise en charge sur les terminaux Knox Workspace qui utilisent Knox 2.5 et versions antérieures et les terminaux Knox MDM.
Windows 10	Créez un profil Wi-Fi ou VPN et spécifiez les informations du serveur proxy dans les paramètres du profil. Les conditions suivantes s'appliquent : • Le proxy Wi-Fi prend uniquement en charge la configuration manuelle et est uniquement pris en charge sur les terminaux Windows 10 Mobile. • Le proxy VPN prend en charge la configuration PARC ou manuelle.

Créer un profil proxy

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Réseaux et connexions > Proxy**.
3. Cliquez sur +.

4. Saisissez le nom et la description du profil proxy.
5. Cliquez sur l'onglet correspondant à un type de terminal.
6. Effectuez l'une des tâches suivantes :

Tâche	Étapes
Spécifier les paramètres de configuration PAC	**a.** Dans la liste déroulante **Type**, cliquez sur **Configuration PAC**. **b.** Dans le champ **URL du fichier PAC**, saisissez l'URL du serveur Web hébergeant le fichier PAC et indiquez le nom du fichier PAC (par exemple, http://www.exemple.com/PACfile.pac). Le fichier PAC ne doit pas être hébergé sur un serveur qui héberge UEM ou l'un de ses composants.
Définir les paramètres de configuration manuelle	**a.** Dans la liste déroulante **Type**, cliquez sur **Configuration manuelle.** **b.** Dans le champ **Hôte**, saisissez le FQDN ou l'adresse IP du serveur proxy. **c.** Dans le champ **Port**, saisissez le numéro de port du serveur proxy. **d.** Si votre organisation requiert que les utilisateurs fournissent un nom d'utilisateur et un mot de passe pour se connecter au serveur proxy et que le profil correspond à plusieurs utilisateurs, dans le champ **Nom d'utilisateur**, saisissez `%UserName%`. Si le serveur proxy requiert le nom de domaine pour l'authentification, utilisez le format *<domain>**<username>*.

7. Répétez les étapes 4 à 6 pour chaque type de terminal.
8. Cliquez sur **Ajouter**.

À la fin :

- Associez le profil proxy à un profil Wi-Fi, VPN ou de connectivité d'entreprise.
- Si vous créez plusieurs profils proxy, classez-les (si nécessaire). Le classement que vous spécifiez s'applique uniquement si vous attribuez un profil proxy à des groupes d'utilisateurs ou à des groupes de terminaux. Sélectionnez un profil et cliquez sur ⇅ pour déplacer le profil vers le haut ou vers le bas du classement. Cliquez sur **Enregistrer**.

Utilisation de BlackBerry Secure Connect Plus pour des connexions aux ressources professionnelles

BlackBerry Secure Connect Plus est un composant BlackBerry UEM qui fournit un tunnel IP sécurisé entre des applications et un réseau d'entreprise :

- Pour les terminaux Android Enterprise, toutes les applications professionnelles utilisent le tunnel sécurisé.
- Pour les terminaux Samsung Knox Workspace et Samsung Knox avec des activations Android Enterprise, vous pouvez autoriser toutes les applications de l'espace Travail à utiliser le tunnel ou spécifier des applications utilisant un VPN par application.
- Pour les terminaux iOS et iPadOS, vous pouvez autoriser toutes les applications à utiliser le tunnel ou spécifier des applications utilisant un VPN par application.

Remarque : Si BlackBerry Secure Connect Plus n'est pas disponible dans votre région, vous devez le désactiver manuellement pour les terminaux Android dans le profil de connectivité d'entreprise.

Le tunnel IP sécurisé permet aux utilisateurs d'accéder aux ressources professionnelles derrière le pare-feu de votre entreprise tout en assurant la sécurité des données à l'aide des protocoles standard et du cryptage de bout en bout.

BlackBerry Secure Connect Plus et un terminal pris en charge établissent un tunnel IP sécurisé s'il s'agit de la meilleure option disponible à des fins de connexion au réseau de l'entreprise. Si un terminal se voit attribuer un profil Wi-Fi ou un profil VPN et que le terminal peut accéder au réseau Wi-Fi professionnel ou VPN, il utilise ces méthodes pour se connecter au réseau. Si ces options ne sont pas disponibles (par exemple, si l'utilisateur est hors de portée du réseau Wi-Fi professionnel), BlackBerry Secure Connect Plus et le terminal établissent un tunnel IP sécurisé.

Si vous configurez un VPN par application pour BlackBerry Secure Connect Plus pour les terminaux iOS et iPadOS, les applications configurées utilisent toujours une connexion de tunnel sécurisé via BlackBerry Secure Connect Plus, même si l'application peut se connecter au réseau Wi-Fi professionnel ou au VPN spécifié dans un profil VPN.

Les terminaux pris en charge communiquent avec BlackBerry UEM pour établir le tunnel sécurisé via BlackBerry Infrastructure. Un tunnel est établi pour chaque terminal. Le tunnel prend en charge les protocoles IPv4 standard (TCP et UDP) et le trafic IP qui est envoyé entre les terminaux et UEM est crypté de bout en bout via AES256. Tant que le tunnel est ouvert, les applications peuvent accéder aux ressources du réseau. Lorsque le tunnel n'est plus requis (si, par exemple, l'utilisateur est à portée du réseau Wi-Fi professionnel), il est désactivé.

Pour activer BlackBerry Secure Connect Plus, procédez comme suit :

Étape	Action
1	Vérifiez que le domaine BlackBerry UEM de votre organisation répond aux conditions d'utilisation de BlackBerry Secure Connect Plus.
2	Activez BlackBerry Secure Connect Plus dans le profil de connectivité d'entreprise par défaut ou dans un profil personnalisé que vous créez.
3	Vous pouvez également spécifier les paramètres DNS pour l'application BlackBerry Connectivity.
4	Si vous disposez d'un environnement sur site qui inclut des terminaux Android Enterprise et Samsung Knox Workspace compatibles avec BlackBerry Dynamics, optimisez les connexions de tunnel sécurisées.
5	Attribuez le profil de connectivité d'entreprise à des comptes d'utilisateur et à des groupes.

Exigences liées au serveur et au terminal pour BlackBerry Secure Connect Plus

Pour utiliser BlackBerry Secure Connect Plus, l'environnement de votre entreprise doit répondre aux exigences ci-dessous.

Pour le domaine BlackBerry UEM :

Environnement	Configuration requise
Tous les environnements UEM	• Le pare-feu de votre entreprise doit autoriser les connexions sortantes sur le port 3101 vers <*region*>.turnb.bbsecure.com et <*region*>.bbsecure.com. Si vous configurez UEM pour qu'il utilise un serveur proxy, vérifiez que ce serveur proxy autorise les connexions sur le port 3101 vers ces sous-domaines. • Dans chaque instance de UEM, le composant BlackBerry Secure Connect Plus doit être en cours d'exécution. • Par défaut, les terminaux Android Enterprise ne sont pas autorisés à utiliser BlackBerry Secure Connect Plus pour se connecter à Google Play et aux services sous-jacents (com.android.providers.media, com.android.vending et com.google.android.apps.gcs). Google Play ne prend pas en charge le proxy. Les terminaux Android Enterprise utilisent une connexion directe via Internet à Google Play. Vérifiez que ces restrictions sont configurées dans le profil de connectivité d'entreprise par défaut ou dans les nouveaux profils de connectivité d'entreprise personnalisés que vous créez. Il est recommandé de maintenir ces restrictions. Si vous supprimez l'une de ces restrictions, vous devez contacter l'assistance Google Play afin de vous renseigner au sujet de la configuration de pare-feu obligatoire pour autoriser les connexions à Google Play à l'aide de BlackBerry Secure Connect Plus. • Si vous utilisez un profil de messagerie pour activer BlackBerry Secure Gateway pour les terminaux iOS, il est recommandé de configurer un VPN par application pour BlackBerry Secure Connect Plus.
UEM sur site	• Si votre environnement inclut des terminaux Knox Workspace et Android Enterprise dotés d'applications BlackBerry Dynamics, consultez Optimiser les connexions de tunnel sécurisées pour les terminaux Android qui utilisent des applications BlackBerry Dynamics. • Vous pouvez également installer des instances BlackBerry Secure Connect Plus en installant plusieurs BlackBerry Connectivity Node. • Vous pouvez également créer un groupe de serveurs pour diriger le trafic BlackBerry Secure Connect Plus vers un chemin régional spécifique de BlackBerry Infrastructure.
UEM Cloud	• Vous devez installer BlackBerry Connectivity Node ou effectuer sa mise à niveau vers la dernière version. Lorsque vous installez ou mettez à niveau BlackBerry Connectivity Node, BlackBerry Secure Connect Plus est également installé ou mis à niveau. Assurez d'activer BlackBerry Connectivity Node avant d'activer BlackBerry Secure Connect Plus. • Si vous acheminez les données qui transitent entre BlackBerry Secure Connect Plus et BlackBerry Infrastructure via un serveur proxy TCP (transparent ou SOCKS v5), vous pouvez configurer les paramètres de proxy à l'aide de la console de gestion BlackBerry Connectivity Node (Paramètres généraux > Proxy).

Pour les terminaux pris en charge :

Profil	Description
iOS et iPadOS	• Les terminaux doivent être activés à l'aide de BlackBerry UEM Client ; pour les terminaux DEP Apple, vous devez distribuer UEM Client aux utilisateurs à partir de UEM, puis demander aux utilisateurs d'ouvrir UEM Client et de terminer le processus de configuration. • Type d'activation Commandes MDM
Android Enterprise	L'un des types d'activation suivants : • Espace Travail uniquement (Premium) • Travail et Personnel - Contrôle total (Premium) • Work and personal - Confidentialité de l'utilisateur (Premium)

Samsung Knox Workspace	• Version non prise en charge de Samsung Knox.
	• L'un des types d'activation suivants :
	  • Travail et Personnel - Contrôle total (Samsung Knox)
	  • Travail et Personnel - Confidentialité de l'utilisateur (Samsung Knox)

Activer BlackBerry Secure Connect Plus

Pour autoriser des terminaux à utiliser BlackBerry Secure Connect Plus, vous devez activer BlackBerry Secure Connect Plus dans un profil de connectivité d'entreprise et attribuer ce profil aux utilisateurs et aux groupes.

Lorsque le profil de connectivité d'entreprise est appliqué au terminal après activation, BlackBerry UEM installe l'application BlackBerry Connectivity sur le terminal (pour les terminaux Android Enterprise, l'application est installée automatiquement depuis Google Play ; pour les terminaux iOS et iPadOS, l'application est installée automatiquement depuis App Store).

Avant de commencer : Vérifiez que le domaine UEM de votre entreprise répond aux exigences pour utiliser BlackBerry Secure Connect Plus.

1. Sur la barre de menus de la console de gestion, cliquez sur **Stratégies et profils > Réseaux et connexions > Connectivité d'entreprise**.
2. Modifiez un profil de connectivité d'entreprise existant ou créez-en un nouveau.
3. Si vous avez créé et configuré un ou plusieurs groupes de serveurs pour diriger le trafic BlackBerry Secure Connect Plus vers un chemin régional spécifique de BlackBerry Infrastructure, dans la liste déroulante **Groupe de serveurs BlackBerry Secure Gateway Service**, cliquez sur le groupe de serveurs approprié.
4. Configurez les valeurs appropriées pour les paramètres de profil pour chaque type de terminal. Pour plus d'informations sur chaque paramètre de profil, reportez-vous à la section Paramètres de profil de connectivité d'entreprise.
5. Cliquez sur **Ajouter**.
6. Attribuez le profil aux groupes ou comptes d'utilisateur.

À la fin :

- Sur les terminaux Android Enterprise et Samsung Knox Workspace, l'application BlackBerry Connectivity invite les utilisateurs à l'autoriser à s'exécuter en tant que VPN et à autoriser l'accès aux clés privées du terminal. Demandez aux utilisateurs d'accepter ces demandes. Les utilisateurs des terminaux peuvent ouvrir l'application pour afficher l'état de la connexion. Aucune action supplémentaire n'est requise de la part des utilisateurs.
- Si vous créez plusieurs profils de connectivité d'entreprise, classez-les. Sélectionnez un profil et cliquez sur ↓↑ pour déplacer le profil vers le haut ou vers le bas du classement. Cliquez sur **Enregistrer**.

- Si vous dépannez un problème de connexion sur un terminal iOS, iPadOS, Android Enterprise ou Knox Workspace, l'application autorise l'utilisateur à envoyer les journaux du terminal à l'adresse e-mail d'un administrateur (l'utilisateur saisit l'adresse e-mail que vous devez fournir). Notez que les journaux ne sont pas visibles à l'aide de Winzip. Il est recommandé d'utiliser un autre utilitaire, par exemple 7-Zip.
- Si vous le souhaitez, vous pouvez également spécifier les paramètres DNS pour l'application BlackBerry Connectivity.

Mise à jour de l'application BlackBerry Connectivity

La dernière application BlackBerry Connectivity est disponible dans Google Play et à partir de BlackBerry myAccount Software Downloads.

- **Utilisateurs Android :** demandez aux utilisateurs du terminal d'effectuer une mise à jour vers les dernières versions de BlackBerry UEM Client et l'application BlackBerry Connectivity disponible dans Google Play. Pour les terminaux qui n'ont pas accès à Google Play, suivez les instructions de la section Mise à jour de l'application BlackBerry Connectivity pour les terminaux Samsung Knox Workspace et Android Enterprise qui n'ont pas accès à Google Play.
- **Utilisateurs Samsung Knox Workspace :**
  - Pour les terminaux Knox sur lesquels la gestion des applications Google Play est activée, demandez aux utilisateurs d'effectuer une mise à jour vers les dernières versions de BlackBerry UEM Client et l'application BlackBerry Connectivity disponible dans Google Play. Dans la console de gestion UEM, assurez-vous de définir l'application BlackBerry Connectivity à envoyer sur Tous les terminaux Android et de l'attribuer aux utilisateurs et groupes qui conviennent.
  - Pour les terminaux Knox sur lesquels la gestion des applications Google Play n'est pas activée, suivez les instructions de la section Mise à jour de l'application BlackBerry Connectivity pour les terminaux Samsung Knox Workspace et Android Enterprise qui n'ont pas accès à Google Play.

Remarque : Si vous utilisez des profils de certificat d'autorité de certification pour distribuer des certificats d'autorité de certification sur des terminaux Android ou Knox Workspace, vérifiez que les certificats que vous avez téléchargés sont codés DER avec une extension de fichier .der ou PEM avec une extension de fichier .pem. Les certificats d'autorité de certification ne répondant pas à ces exigences peuvent entrainer des problèmes de connexion pour l'application BlackBerry Connectivity.

Mise à jour de l'application BlackBerry Connectivity pour les terminaux Samsung Knox Workspace et Android Enterprise qui n'ont pas accès à Google Play

Suivez les instructions ci-dessous pour mettre à jour l'application BlackBerry Connectivity sur les terminaux des utilisateurs vers la dernière version.

Pour bénéficier des dernières mises à jour du serveur, il est recommandé de procéder à une mise à niveau vers la version la plus récente de BlackBerry UEM.

Avant de commencer :

- Rendez-vous sur la page BlackBerry myAccount Software Downloads pour télécharger la version la plus récente de l'application BlackBerry Connectivity. Enregistrez les fichiers sur tous les ordinateurs qui hébergent une instance UEM.
- Demandez aux utilisateurs de terminaux Knox Workspace de mettre à jour BlackBerry UEM Client vers la dernière version disponible dans Google Play.
- Pour les activations Knox Workspace, la dernière version de l'application BlackBerry Connectivity étant disponible dans Google Play, les utilisateurs peuvent mettre à jour l'application eux-mêmes. Vous devez systématiquement suivre les étapes ci-dessous pour configurer UEM à des fins de prise en charge de l'application.
- Pour les activations Android Enterprise , les utilisateurs peuvent procéder à une mise à jour vers la dernière version de l'application BlackBerry Connectivity à partir de Google Play eux-mêmes si Google Play est activé

dans l'espace Travail. Vous devez systématiquement suivre les étapes ci-dessous pour configurer UEM à des fins de prise en charge de l'application.

- Pour configurer UEM à des fins de prise en charge de l'application BlackBerry Connectivity pour les terminaux qui ont besoin de BlackBerry Secure Connect Plus :

1. Sur la console de gestion UEM, cliquez sur **Applications** dans la barre de menus.
2. Cliquez sur > **Applications internes**.
3. Cliquez sur **Parcourir** et sélectionnez le fichier .apk de la dernière application BlackBerry Connectivity pour Android.
4. Cliquez sur **Ajouter**.
5. Dans le champ **Envoyer à**, sélectionnez **Tous les terminaux Android**.
6. Décochez **Publier l'application dans le domaine Google**.
7. Cliquez sur **Ajouter**.
8. Attribuez l'application que vous avez ajoutée à l'étape précédente aux terminaux Samsung Knox Workspace et Android Enterprise qui n'ont pas accès à Google Play. La disposition de l'application doit être définie sur **Obligatoire**.

À la fin : UEM envoie une notification de mise à jour de stratégie à UEM Client sur les terminaux Knox Workspace. UEM Client met à jour l'application BlackBerry Connectivity lorsque celle-ci est attribuée en tant qu'application requise.

Paramètres de profil de connectivité d'entreprise

Les profils de connectivité d'entreprise sont pris en charge sur les types de terminaux suivants :

- iOS
- iPadOS
- Android

Communs : paramètres de profil de connectivité d'entreprise

Communs : paramètre de profil de conformité	Description
Groupe de serveurs BlackBerry Secure Connect Plus	Ce paramètre spécifie le groupe de serveurs utilisé par BlackBerry Secure Connect Plus pour diriger le trafic vers un chemin régional spécifique.

iOS : paramètres de profil de connectivité d'entreprise

Les paramètres pour iOS s'appliquent également aux terminaux iPadOS.

Paramètre	Description
Activer BlackBerry Secure Connect Plus	Ce paramètre indique si les applications professionnelles utilisent BlackBerry Secure Connect Plus pour l'envoi de données professionnelles entre les terminaux et votre réseau.

Paramètre	Description
Activer VPN à la demande	Sélectionnez ce paramètre pour autoriser uniquement certaines applications à utiliser BlackBerry Secure Connect Plus. **Remarque :** Si vous sélectionnez cette option, les utilisateurs doivent activer manuellement la connexion VPN sur leur terminal pour pouvoir utiliser BlackBerry Secure Connect Plus. Tant que la connexion VPN est activée, le terminal utilise BlackBerry Secure Connect Plus pour se connecter au réseau d'entreprise. L'utilisateur doit désactiver la connexion VPN pour utiliser une autre connexion, telle que le réseau Wi-Fi de l'entreprise. Indiquez aux utilisateurs à quel moment il est approprié d'activer et de désactiver la connexion VPN (par exemple, vous pouvez leur demander d'activer la connexion VPN lorsqu'ils sont hors de portée du réseau Wi-Fi de l'entreprise).
Règles de VPN à la demande pour iOS 9 ou version ultérieure	Ce paramètre spécifie les exigences de connexion pour le VPN à la demande à l'aide de BlackBerry Secure Connect Plus. Vous devez utiliser une ou plusieurs clés de l'exemple de format de charge utile. Ce paramètre est valide uniquement si le paramètre Activer VPN à la demande est sélectionné.
Activer un VPN par application	Ce paramètre indique si une application professionnelle peut lancer automatiquement une connexion VPN à l'aide de BlackBerry Secure Connect Plus lorsqu'elle accède à des ressources professionnelles. Sélectionnez ce paramètre pour spécifier des règles pour les connexions BlackBerry Secure Connect Plus.
Domaines Safari	Spécifiez les domaines autorisés à démarrer une connexion VPN dans Safari.
Domaines Calendrier	Spécifiez les domaines pouvant établir la connexion VPN dans Calendrier.
Domaines Contacts	Spécifiez les domaines pouvant établir la connexion VPN dans Contacts.
Domaines Messagerie	Spécifiez les domaines pouvant établir la connexion VPN dans Messagerie.
Domaines associés	Spécifiez les domaines associés.
Domaines exclus	Spécifiez les domaines exclus.
Autoriser la connexion automatique des applications	Spécifiez si les applications peuvent lancer la connexion VPN automatiquement.
Profil de proxy	Ce paramètre indique le profil proxy associé si vous souhaitez acheminer le trafic du tunnel sécurisé des terminaux au réseau professionnel via un serveur proxy. Le profil de proxy doit utiliser une configuration manuelle avec une adresse IP. La Configuration PAC n'est pas prise en charge. Pour plus d'informations, reportez-vous à Création de profils proxy pour les terminaux.

Android : paramètres de profil de connectivité d'entreprise

Paramètre	Description
Activer BlackBerry Secure Connect Plus	Ce paramètre indique si les applications professionnelles utilisent BlackBerry Secure Connect Plus pour l'envoi de données professionnelles entre les terminaux et votre réseau.
Connectivité d'entreprise pour les terminaux Android comprenant un espace Travail	Ce paramètre spécifie si les terminaux Android Enterprise et Samsung Knox Workspace utilisent BlackBerry Secure Connect Plus pour toutes les applications de l'espace Travail, ou seulement pour certaines applications. • « VPN à l'échelle du conteneur » utilise une connexion VPN pour toutes les applications dans l'espace Travail sur le terminal. • « VPN par application » utilise une connexion VPN uniquement pour les applications spécifiées.
Applications non autorisées à utiliser BlackBerry Secure Connect Plus	Ce paramètre spécifie les applications dans l'espace Travail sur les terminaux Android Enterprise qui ne sont pas autorisés à utiliser BlackBerry Secure Connect Plus. Si la stratégie informatique Forcer les applications professionnelles à utiliser VPN uniquement est appliquée au terminal, ce paramètre est ignoré et il n'est interdit à aucune application professionnelle, y compris BlackBerry UEM Client et Google Play, d'utiliser BlackBerry Secure Connect Plus. Dans ce cas, vous devez ouvrir les ports dans le pare-feu pour permettre à UEM Client de communiquer avec BlackBerry Infrastructure via UEM. Pour plus d'informations sur l'ouverture de ports dans le pare-feu lorsque les applications professionnelles utilisent BlackBerry Secure Connect Plus, consultez l'article KB 48330. Si votre organisation utilise des applications BlackBerry Dynamics, nous vous recommandons d'empêcher celles-ci d'utiliser BlackBerry Secure Connect Plus. Si vous ne le faites pas, vous devrez ouvrir des ports supplémentaires sur le pare-feu de votre organisation pour permettre aux applications d'envoyer des données à BlackBerry Dynamics NOC, et l'activité réseau depuis les applications pourra être retardée car les données seront acheminées à la fois vers BlackBerry Infrastructure et vers BlackBerry Dynamics NOC. Reportez-vous à la section Optimiser les connexions de tunnel sécurisées pour les terminaux Android qui utilisent des applications BlackBerry Dynamics. Ce paramètre est valide uniquement si le paramètre Connectivité d'entreprise pour les terminaux Android comprenant un espace Travail est défini sur VPN à l'échelle du conteneur.
Applications autorisées à utiliser la connectivité d'entreprise	Ce paramètre spécifie les applications dans l'espace Travail sur Android Enterprise et les terminaux Samsung Knox Workspace qui sont autorisés à utiliser BlackBerry Secure Connect Plus. Vous pouvez sélectionner les applications dans la liste des applications disponibles ou spécifier l'ID de package d'application. Ce paramètre est valide uniquement si le paramètre Connectivité d'entreprise pour les terminaux Android comprenant un espace Travail est défini sur VPN par application.

Paramètre	Description
Profil de proxy	Vous pouvez sélectionner un profil de proxy que vous avez configuré pour acheminer le trafic de tunnel sécurisé via un serveur proxy. Cette option est prise en charge pour les terminaux dotés des types d'activation Android Enterprise. BlackBerry Secure Connect Plus prend en charge la configuration PAC et la configuration manuelle du serveur proxy dans le profil de proxy, mais prenez note des limitations détaillées dans setHttpProxy à partir de developer.android.com. La prise en charge du proxy Web pour BlackBerry Secure Connect Plus nécessite l'application BlackBerry Connectivity version 1.0.25.x ou ultérieure et UEM Client version 12.44.x ou ultérieure.

Spécifier les paramètres DNS pour l'application BlackBerry Connectivity

Vous pouvez spécifier les serveurs DNS que l'application BlackBerry Connectivity doit utiliser pour les connexions de tunnel sécurisées. Si vous ne spécifiez pas de paramètres DNS, l'application récupère les adresses DNS depuis l'ordinateur qui héberge le composant BlackBerry Secure Connect Plus et le suffixe de recherche par défaut correspond au domaine DNS de cet ordinateur.

1. Effectuez l'une des opérations suivantes :
   - Dans un environnement sur site, sur la console de gestion de UEM, dans la barre de menus, cliquez sur **Paramètres > Infrastructure > BlackBerry Secure Connect Plus**.
   - Dans un environnement basé sur le cloud, dans la console BlackBerry Connectivity Node (http://localhost:8088), cliquez sur **Paramètres généraux > BlackBerry Secure Connect Plus** dans le volet de gauche.
2. Cochez la case **Configurer manuellement les serveurs DNS** et cliquez sur +.
3. Saisissez l'adresse du serveur DNS au format décimal séparé par des points (par exemple 192.0.2.0). Cliquez sur **Ajouter**.
4. Si nécessaire, répétez les étapes 2 et 3 pour ajouter d'autres serveurs DNS. Dans le tableau **Serveurs DNS**, cliquez sur les flèches de la colonne **Classement** pour définir la priorité des serveurs DNS.
5. Si vous souhaitez spécifier des suffixes de recherche DNS, procédez comme suit :
   a) Cochez la case **Gérer manuellement les suffixes de recherche DNS** et cliquez sur +.
   b) Saisissez le suffixe de recherche DNS (par exemple, domaine.com). Cliquez sur **Ajouter**.
6. Si nécessaire, répétez l'étape 5 pour ajouter d'autres suffixes de recherche DNS. Dans le tableau **Suffixe de recherche DNS**, cliquez sur les flèches de la colonne **Classement** pour définir la priorité des serveurs DNS.
7. Cliquez sur **Enregistrer**.

Optimiser les connexions de tunnel sécurisées pour les terminaux Android qui utilisent des applications BlackBerry Dynamics

Si vous activez BlackBerry Secure Connect Plus et que vous disposez d'un environnement sur site incluant des applications BlackBerry Dynamics installées sur des terminaux Android Enterprise ou Samsung Knox Workspace, nous vous conseillons de configurer le profil de connectivité BlackBerry Dynamics attribué à ces terminaux pour désactiver BlackBerry Proxy. L'utilisation à la fois de BlackBerry Proxy et de BlackBerry Secure Connect Plus peut retarder l'activité réseau des applications, car les données sont acheminées vers les deux composants de réseau.

1. Sur la barre de menus de la console de gestion, cliquez sur **Stratégies et profils > Réseaux et connexions > Connectivité BlackBerry Dynamics**.
2. Modifiez le profil attribué aux terminaux Android Enterprise et Samsung Knox Workspace.
3. Désactivez la case **Acheminer tout le trafic**.

4. Dans la section **Type de chemin de domaine autorisé par défaut**, sélectionnez **Direct** pour acheminer le trafic directement de l'application vers le domaine sans passer par BlackBerry Proxy.
5. Cliquez sur **Enregistrer**.

Résolution des problèmes BlackBerry Secure Connect Plus

Prenez note des problèmes suivants si vous avez des difficultés à configurer BlackBerry Secure Connect Plus.

BlackBerry Secure Connect Plus ne démarre pas

Cause possible

Les paramètres TCP/IPv4 de l'adaptateur BlackBerry Secure Connect Plus sont peut-être incorrects.

Solution possible

Dans **Connexions réseau > Adaptateur BlackBerry Secure Connect Plus > Propriétés > Protocole IPv4 (TCP/IPv4) > Propriétés**, vérifiez que la case **Utiliser l'adresse IP suivante** est cochée, avec les valeurs par défaut suivantes :

- Adresse IP : 172.16.0.1
- Masque de sous-réseau : 255.255.0.0

Si nécessaire, corrigez ces paramètres, puis redémarrez le serveur.

BlackBerry Secure Connect Plus cesse de fonctionner après une installation ou une mise à niveau BlackBerry UEM

Cause

Ce problème peut se produire si le serveur n'a pas redémarré lors d'une mise à jour RRAS avant la mise à niveau de BlackBerry UEM dans un environnement sur site, entrainant l'échec de la configuration de routage/NAT lors de la mise à niveau. Ce problème peut également survenir après une nouvelle installation de UEM.

Solution

1. Redémarrez le serveur.
2. Dans les services Windows, arrêtez le service **BlackBerry UEM – BlackBerry Secure Connect Plus**.
3. En tant qu'administrateur, démarrez Windows PowerShell (64 bits) ou ouvrez une invite de commande.
4. Accédez à `<drive>:\Program Files\BlackBerry\UEMSecureConnectPlus\config\blackberry\` et exécutez **configureRRAS.bat**
5. Accédez à `<drive>:\Program Files\BlackBerry\UEMSecureConnectPlus\config\` et exécutez **configure-network-interface.cmd**
6. Dans les services Windows, démarrez le service **BlackBerry UEM – BlackBerry Secure Connect Plus**.

Affichage des fichiers journaux pour BlackBerry Secure Connect Plus

Objectif	Fichier journal	Exemple
Vérifier que BlackBerry Secure Connect Plus est connecté à BlackBerry Infrastructure	BSCP	2015-01-19T13:17:47.540-0500 - BSCP {TcpClientConnectorNio#2} logging.feature.bscp.service|logging.component.bscp.pss.bcp [{}] - DEBUG Received Ping from [id: 0x60bce5a3, /10.90.84.22:28231 => stratos.bcp.bblabs.rim.net/206.53.155.152:3101], responding with Pong.2015-01-19T13:18:22.989-0500 - BSCP {ChannelPinger#1} logging.feature.bscp.service|logging.component.bscp.pss.bcp [{}] - DEBUG Sending Ping to [id: 0xb4a1677a, /10.90.84.22:28232 => stratos.bcp.bblabs.rim.net/206.53.155.152:3101]
Vérifier que BlackBerry Secure Connect Plus est prêt à recevoir des appels depuis l'application BlackBerry Connectivity sur les terminaux	BSCP-TS	47: [14:13:21.231312][][3][AsioTurnSocket-1] Connected, host=68-171-243-141.rdns.blackberry.net 48: [14:13:21.239312][][3][AsioTurnSocket-1] Creating TURN allocation 49: [14:13:21.405121][][3][AsioTurnSocket-1] TURN allocation created
Vérifier que les terminaux utilisent le tunnel sécurisé	BSCP-TS	74: [10:39:45.746926][][3][Tunnel-2FFEC51E] Sent: 2130.6 KB (1733), Received: 201.9 KB (1370), Running: 00:07:00.139249
Vérifier que BlackBerry Secure Connect Plus utilise les paramètres de transcodeur personnalisé	BSCP	"configuration_def" : "com.rim.p2e.vpn.server.cipherSuite" }], "TRANSCODER", ["provider", { "configuration_def" : "com.rim.p2e.vpn.transcoder.provider" }, "server_library", { "configuration_def" : "com.rim.p2e.vpn.transcoder.server.library" }, "server_config_blob", { "configuration_def" : "com.rim.p2e.vpn.transcoder.server.configBlob" }]]
Vérifier que les terminaux utilisent un transcodeur personnalisé	BSCP-TS	37: [13:41:39.800371][][3][BlackBerry_1.0.0.1-25B212A5] Connected

Utilisation de BlackBerry 2FA pour les connexions sécurisées aux ressources essentielles

BlackBerry 2FA protège l'accès aux ressources critiques de votre organisation à l'aide de l'authentification à deux facteurs. BlackBerry 2FA utilise un mot de passe que les utilisateurs saisissent et une invite sécurisée sur leur terminal mobile chaque fois qu'ils tentent d'accéder à des ressources.

Vous gérez BlackBerry 2FA à partir de la console de gestion BlackBerry UEM, où vous utilisez un profil BlackBerry 2FA afin d'activer l'authentification à deux facteurs pour vos utilisateurs. Pour utiliser la dernière version de BlackBerry 2FA et ses fonctionnalités associées, telles que la pré-authentification et la résolution autonome, le profil BlackBerry 2FA doit être attribué à vos utilisateurs. Pour plus d'informations, consultez le contenu relatif à BlackBerry 2FA.

Activation de l'authentification automatique pour les terminaux iOS

Vous pouvez activer les terminaux iOS à des fins d'authentification automatique auprès de domaines et services Web de votre réseau d'entreprise. Une fois le profil d'identification unique ou le profil d'extension avec identification unique attribué, l'utilisateur est invité à saisir un nom d'utilisateur et un mot de passe la première fois qu'il tente d'accéder au domaine que vous avez spécifié. Les informations de connexion sont enregistrées sur le terminal de l'utilisateur et automatiquement utilisées lorsqu'il tente d'accéder à l'un des domaines sécurisés spécifiés dans le profil. Si l'utilisateur change de mot de passe, celui-ci lui est demandé lorsqu'il tente à nouveau d'accéder à un domaine sécurisé.

Un profil d'extension avec identification unique permet aux terminaux de s'authentifier automatiquement auprès des domaines et des services Web du réseau de votre organisation. Vous pouvez spécifier les paramètres d'une extension personnalisée ou utiliser l'extension Kerberos fournie par Apple.

Avant de commencer : Si vous souhaitez utiliser l'authentification basée sur des certificats, créez le profil de certificat nécessaire.

1. Sur la barre de menus de la console de gestion, cliquez sur **Stratégies et profils > Réseaux et connexions > Extension d'identification unique**.
2. Cliquez sur +.
3. Saisissez le nom et la description du profil.
4. Dans la liste déroulante **Type d'extension d'identification unique**, cliquez sur l'option **Extension personnalisée** ou **Extension intégrée Kerberos** fournie par Apple.

Tâche	Étapes
Si vous sélectionnez **Extension personnalisée**	**a.** Dans le champ **Identifiant d'extension**, saisissez l'identifiant de l'application qui exécute l'identification unique. **b.** Sélectionnez un type d'identification qui convient. **c.** Si vous avez sélectionné **Informations d'identification** comme type d'identification, procédez comme suit : **1.** Dans le champ **Domaine**, saisissez le nom de domaine pour les informations d'identification. **2.** Dans la section **Domaines**, cliquez sur + pour ajouter un domaine. **3.** Dans le champ **Nom**, saisissez le domaine pour lequel l'extension d'application exécute l'identification unique. **4.** Ajoutez des domaines supplémentaires si nécessaire. **d.** Si vous avez sélectionné **Rediriger** comme type d'identification, procédez comme suit : **1.** Dans la section **URL**, cliquez sur + pour ajouter une URL. **2.** Dans le champ **Nom**, saisissez le préfixe de l'URL du fournisseur d'identité pour lequel l'extension d'application effectue une identification unique. Ajoutez des URL supplémentaires si nécessaire. **e.** Dans le champ **Code de charge utile personnalisée**, saisissez le code de charge utile personnalisée pour l'extension d'application.

Tâche	Étapes
Si vous sélectionnez **Extension intégrée Kerberos**	**a.** Dans la section **Domaines**, cliquez sur + pour ajouter un domaine. **b.** Dans le champ **Nom de domaine**, saisissez le nom de domaine pour les informations d'identification. **c.** Sélectionnez les **Données de l'extension pour l'authentification unique Kerberos Apple** appropriées pour votre environnement. Par défaut, la connexion automatique et la détection automatique Active Directory sont autorisées. Vous pouvez également spécifier le domaine par défaut, autoriser uniquement les applications gérées à utiliser l'authentification unique et demander aux utilisateurs de confirmer l'accès. **d.** Définissez le **Nom principal** de la connexion. **e.** Si vous souhaitez utiliser un profil de certificat pour fournir le certificat PKINIT pour l'authentification, sélectionnez le type de profil dans la liste déroulante **Sélectionner le certificat PKINIT pour l'authentification**, puis sélectionnez le profil approprié. **f.** Si vous utilisez l'API GSS (Generic Security Service), spécifiez le **Nom GSS du cache Kerberos**. **g.** Dans la section **Identifiants de l'offre d'application**, cliquez sur + pour spécifier les ID d'offre autorisés à accéder au ticket d'émission de ticket. **h.** Dans la section **Centres de distribution clés préférés**, cliquez sur + pour spécifier les serveurs préférés s'ils ne sont pas détectables à l'aide du DNS. Spécifiez chaque serveur au même format que celui utilisé dans un fichier krb5.conf. Les serveurs spécifiés sont utilisés pour les vérifications de connectivité et sont essayés en premier pour le trafic Kerberos. Si les serveurs ne répondent pas, le terminal utilise la découverte DNS. **i.** Dans le champ **Mappage domaine-domaine personnalisé**, saisissez tout mappage personnalisé requis entre les domaines et les noms de domaine au format de la charge utile, par exemple `<key>sample-realm1</key><array><string>org</string></array>`. **j.** Dans le champ **Indication de connexion**, spécifiez le texte à afficher en bas de la fenêtre de connexion à Kerberos.

5. Cliquez sur **Enregistrer**.

Spécification de serveurs DNS pour les terminaux iOS et macOS

Vous pouvez spécifier les serveurs DNS que vous souhaitez utiliser pour accéder à des domaines spécifiques. Ce paramètre permet d'accélérer et de sécuriser la navigation sur le Web.

1. Sur la barre de menus de la console de gestion, cliquez sur **Stratégies et profils > Réseaux et connexions > DNS**.
2. Cliquez sur +.
3. Saisissez le nom et la description du profil.
4. Cliquez sur l'onglet correspondant à un type de terminal.
5. Sélectionnez le protocole DNS utilisé pour communiquer avec le serveur DNS.
6. Effectuez l'une des opérations suivantes :
   a) Si vous avez sélectionné **HTTPS**, saisissez le modèle URI du serveur DoH (DNS-over-HTTPS) à l'aide du schéma https://.

b) Si vous avez sélectionné **TLS**, saisissez le nom d'hôte du serveur DoT (DNS-over-TLS).

7. Pour empêcher les utilisateurs de désactiver les paramètres, cochez la case **Ne pas autoriser l'utilisateur à désactiver les paramètres DNS**. Cette option concerne uniquement les terminaux surveillés.
8. Dans le champ **Adresses DNS**, indiquez la liste des adresses IP pour tous les serveurs DNS que vous souhaitez utiliser. Il peut s'agir d'un mélange d'adresses IPv4 et IPv6.
9. Dans le champ **Domaines**, indiquez la liste des chaînes de domaine qui seront utilisées pour déterminer les requêtes DNS qui utiliseront les serveurs DNS.
10. Dans le champ **Règles DNS à la demande**, spécifiez les règles DNS à la demande à l'aide de l'exemple de format de charge utile.
11. Répétez les étapes 5 à 10 pour chaque type de terminal.
12. Cliquez sur **Enregistrer**.

Spécification des domaines de messagerie et des domaines Web pour les terminaux iOS

Vous pouvez utiliser un profil de domaines gérés pour définir certains domaines de messagerie et domaines Web en tant que « domaines gérés » internes à votre entreprise. Les profils de domaines gérés s'appliquent uniquement aux terminaux iOS et iPadOS avec le type d'activation Contrôles MDM.

Après avoir attribué un profil de domaines gérés :

- Lorsqu'un utilisateur crée un e-mail et ajoute l'adresse électronique d'un destinataire dont le domaine n'est pas spécifié dans le profil de domaines gérés, le terminal affiche l'adresse en rouge pour avertir l'utilisateur que le destinataire est externe à l'entreprise. Le terminal n'empêche pas l'utilisateur d'envoyer des e-mails à des destinataires externes.
- Un utilisateur doit utiliser une application gérée par BlackBerry UEM pour afficher les documents provenant d'un domaine Web géré ou les documents téléchargés depuis un domaine Web géré. Le terminal n'empêche pas l'utilisateur de consulter des documents issus d'autres domaines Web. Le profil de domaines gérés s'applique uniquement au navigateur Safari.

1. Sur la barre de menus, cliquez sur **Stratégies et profils > Réseaux et connexions > Domaines gérés**.
2. Cliquez sur +.
3. Saisissez le nom et la description du profil.
4. Dans le champ **Description**, saisissez la description du profil.
5. Dans la section **Domaines gérés**, cliquez sur +.
6. Dans le champ **Domaines de messagerie**, saisissez un nom de domaine de niveau supérieur (par exemple, `example.com` plutôt que `example.com/canada`).
7. Cliquez sur **Ajouter**.
8. Dans la section **Domaines Web gérés**, cliquez sur +. Pour obtenir des exemples de formats de domaines Web, reportez-vous à Managed Safari Web Domains in the iOS Developer Library (Domaines Web Safari gérés dans la Bibliothèque du développeur iOS).
9. Dans le champ **Domaines Web**, saisissez un nom de domaine.
10. Si vous souhaitez autoriser le remplissage automatique du mot de passe pour les domaines Web que vous avez spécifiés, cochez la case **Autoriser le remplissage automatique du mot de passe**. Cette option est prise en charge sur les terminaux supervisés uniquement.
11. Cliquez sur **Ajouter**, puis de nouveau sur **Ajouter**.

À la fin : Attribuez les domaines gérés aux comptes d'utilisateur, groupes d'utilisateurs ou groupes de terminaux.

Contrôle de l'utilisation du réseau pour les applications sur les terminaux iOS

Vous pouvez utiliser un profil d'utilisation du réseau pour contrôler la façon dont les applications sur des terminaux iOS et iPadOS utilisent le réseau mobile. Pour mieux gérer l'utilisation du réseau, vous pouvez empêcher des applications spécifiques de transférer des données lorsque des terminaux sont connectés au réseau mobile ou lorsque des terminaux sont en itinérance. Un profil d'utilisation de réseau peut contenir des règles pour une ou plusieurs applications.

Les règles dans un profil d'utilisation de réseau s'appliquent aux applications professionnelles seulement. Si vous n'avez pas attribué d'applications à des utilisateurs ou groupes, le profil d'utilisation du réseau ne possède pas d'effet.

Avant de commencer : Ajoutez des applications à la liste des applications et attribuez-les à des utilisateurs ou à des groupes.

1. Sur la barre de menus de la console de gestion, cliquez sur **Stratégies et profils > Réseaux et connexions > Utilisation du réseau**.
2. Cliquez sur +.
3. Saisissez le nom et la description du profil.
4. Cliquez sur +.
5. Effectuez l'une des opérations suivantes :
   - Cliquez sur **Ajouter une application**, puis sur une application de la liste.
   - Sélectionnez l'option **Spécifier l'ID de package d'une application** et saisissez l'ID. L'ID du package d'applications est également appelé ID d'offre. Vous pouvez trouver l'ID de package de l'application en cliquant sur l'application dans la liste des applications. Utilisez un caractère générique (*) pour mettre en correspondance l'ID avec plusieurs applications. (Par exemple, **com.company.***).
6. Pour empêcher l'application ou les applications d'utiliser des données lorsque le terminal est en itinérance, décochez la case **Autoriser l'itinérance des données**.
7. Pour empêcher l'application ou les applications d'utiliser des données lorsque le terminal est connecté au réseau mobile, décochez la case **Autoriser les données cellulaires**.
8. Cliquez sur **Ajouter**.
9. Répétez les étapes 5 à 9 pour chacune des applications que vous souhaitez ajouter à la liste.

À la fin : Si vous avez créé plusieurs profils d'utilisation du réseau, classez-les. Sélectionnez un profil et cliquez sur ↓↑ pour déplacer le profil vers le haut ou vers le bas du classement. Cliquez sur **Enregistrer**

Attribuez le profil d'utilisation du réseau à des comptes d'utilisateur, groupes d'utilisateurs ou groupes de terminaux.

Création d'un profil de filtre de contenu Web sur les terminaux iOS

Vous pouvez utiliser les profils de filtre de contenu Web pour limiter les sites Web qu'un utilisateur peut afficher dans Safari ou d'autres applications de navigation sur un ou terminal supervisé iOS ou iPadOS. Vous pouvez attribuer des profils de filtre de contenu Web à des comptes d'utilisateur, groupes d'utilisateurs ou groupes de terminaux. Lorsque vous créez un profil de filtre de contenu Web, chaque URL que vous spécifiez doit commencer par http:// ou https://. Si nécessaire, vous devez ajouter des entrées distinctes pour les versions http:// ou https:// d'une même URL. La résolution DNS n'intervient pas et dès lors, les sites Web limités restent accessibles

(par exemple, si vous spécifiez http://www.exemple.com, les utilisateurs seront peut-être en mesure d'accéder au site Web à l'aide de leur adresse IP).

Lorsque vous créez un profil de filtre de contenu Web, vous pouvez choisir l'option de sites Web autorisés répondant aux normes de votre organisation en termes d'utilisation des terminaux mobiles.

Sites Web autorisés	Description
Sites Web spécifiques uniquement	Cette option permet d'accéder uniquement aux sites Web que vous spécifiez. Dans Safari, un signet est créé pour chaque site Web autorisé. Si vous autorisez uniquement l'accès à des sites Web spécifiques, vous devez vous assurer que tous les sites Web auxquels le terminal a besoin d'accéder sont spécifiés dans la liste des sites Web autorisés. Par exemple, si vous configurez l'authentification moderne de Microsoft Office 365 pour les applications BlackBerry Dynamics, le terminal doit pouvoir accéder au site Web des services de fédération Active Directory.
Limiter le contenu pour adultes	Cette option permet le filtrage automatique afin d'identifier et de bloquer tout contenu inapproprié. Vous pouvez également inclure certains sites Web en utilisant les paramètres suivants : • URL autorisées : vous pouvez ajouter une ou plusieurs URL pour autoriser l'accès à certains sites Web. Les utilisateurs peuvent afficher les sites Web de cette liste même si le filtrage automatique en bloque l'accès. • URL non autorisées : vous pouvez ajouter une ou plusieurs URL pour refuser l'accès à certains sites Web. Les utilisateurs ne peuvent pas afficher les sites Web de cette liste même si le filtrage automatique en autorise l'accès.

1. Sur la barre de menus, cliquez sur **Stratégies et profils > Réseaux et connexions > Filtre de contenu Web**.
2. Cliquez sur +.
3. Saisissez le nom et la description du profil de filtre de contenu Web.
4. Effectuez l'une des tâches suivantes :

Tâche	Étapes
Autoriser l'accès à des sites Web spécifiques uniquement	a. Dans la liste déroulante **Sites Web autorisés**, vérifiez que le paramètre **Sites Web spécifiques uniquement** est sélectionné. b. Dans la section **Signets de sites Web spécifiques**, cliquez sur +. c. Procédez comme suit : 1. Dans le champ **URL**, saisissez l'adresse Web dont vous souhaitez autoriser l'accès. 2. Dans le champ **Chemin du signet**, vous pouvez également saisir le nom d'un dossier de signets (par exemple, /Work/). 3. Dans le champ **Titre**, saisissez le nom du site Web. 4. Cliquez sur **Ajouter**. d. Répétez les étapes b et c pour chaque site Web autorisé.

Tâche	Étapes
Limiter le contenu pour adultes	**a.** Dans la liste déroulante **Sites Web autorisés**, cliquez sur **Limiter le contenu pour adultes** pour activer le filtrage automatique. **b.** Vous pouvez également procéder comme suit : 1. Cliquez sur + en regard de **URL autorisées**. 2. Saisissez l'adresse Web dont vous souhaitez autoriser l'accès. 3. Si nécessaire, répétez l'opération pour ajouter d'autres sites Web. **c.** Vous pouvez également procéder comme suit : 1. Cliquez sur + en regard de **URL non autorisées**. 2. Saisissez l'adresse Web dont vous souhaitez refuser l'accès. 3. Si nécessaire, répétez l'opération pour ajouter d'autres sites Web.

5. Cliquez sur **Ajouter**.

À la fin : Attribuez le profil de filtre de contenu Web à des comptes d'utilisateur, à des groupes d'utilisateurs ou à des groupes de terminaux.

Création d'un profil AirPrint sur les terminaux iOS

Les profils AirPrint peuvent aider les utilisateurs à trouver les imprimantes qui prennent en charge AirPrint, qui sont accessibles, et pour lesquelles ils disposent des autorisations requises. Dans les situations où des protocoles tels que Bonjour ne peuvent pas détecter les imprimantes AirPrint activées sur un autre sous-réseau, les profils AirPrint aident à spécifier l'emplacement des ressources. Vous pouvez configurer des profils AirPrint et les attribuer à des terminaux iOS et iPadOS afin que les utilisateurs n'aient pas à configurer les imprimantes manuellement.

1. Sur la barre de menus, cliquez sur **Stratégies et profils > Réseaux et connexions > AirPrint**.
2. Cliquez sur +.
3. Saisissez le nom et la description du profil.
4. Dans la section **Configuration d'AirPrint** , cliquez sur +.
5. Dans le champ **Adresse IP**, saisissez l'adresse IP de l'imprimante ou du serveur AirPrint.
6. Dans le champ **Chemin de ressource**, saisissez le chemin de ressource de l'imprimante.
   Le chemin de ressource de l'imprimante correspond au paramètre `rp` du dossier Bonjour `_ipps.tcp`. Par exemple :
   - printers/<*gamme de l'imprimante*>
   - printers/<*modèle de l'imprimante*>
   - ipp/print
   - IPP_Printer
7. Si les connexions AirPrint sont sécurisées par TLS, vous pouvez également cocher la case **Forcer TLS**.
8. Si le port diffère de celui par défaut du protocole d'impression Internet, saisissez le numéro de port dans le champ **Port**.
9. Cliquez sur **Ajouter**, puis de nouveau sur **Ajouter**.

À la fin : Attribuez le profil AirPrint à des comptes d'utilisateur, groupes d'utilisateurs ou groupes de terminaux.

Création d'un profil AirPlay sur les terminaux iOS

AirPlay est une fonctionnalité qui vous permet d'afficher des photos, ou de diffuser de la musique et des vidéos, vers des terminaux AirPlay compatibles, tels que Apple TV, AirPort Express ou des haut-parleurs compatibles AirPlay.

Avec un profil AirPlay, vous pouvez spécifier les terminaux AirPlay iOS et iPadOS auxquels les utilisateurs peuvent se connecter. Le profil AirPlay comporte deux options :

- Si les terminaux AirPlay de votre organisation sont protégés par mot de passe, vous pouvez spécifier des mots de passe pour les terminaux de destination autorisés afin que les utilisateurs de terminaux iOS et iPadOS puissent se connecter sans connaître le mot de passe.
- Pour les terminaux sous supervision, vous pouvez limiter les terminaux AirPlay auxquels les utilisateurs peuvent se connecter en spécifiant une liste de terminaux AirPlay autorisés pour les terminaux sous supervision. Les terminaux sous supervision ne peuvent se connecter qu'aux terminaux AirPlay spécifiés dans la liste. Si vous ne créez pas de liste, les terminaux sous supervision peuvent se connecter à n'importe quel terminal AirPlay.

1. Sur la barre de menus, cliquez sur **Stratégies et profils > Réseaux et connexions > AirPlay**.
2. Cliquez sur +.
3. Saisissez le nom et la description du profil AirPlay.
4. Cliquez sur + dans la section **Terminaux de destination autorisés**.
5. Dans le champ **Nom du terminal**, saisissez le nom du terminal AirPlay auquel vous souhaitez fournir un mot de passe. Vous pouvez trouver le nom du terminal AirPlay dans les paramètres du terminal ou rechercher le nom du terminal en sélectionnant **AirPlay** dans le centre de contrôle d'un terminal iOS ou iPadOS pour afficher la liste des terminaux AirPlay disponibles autour de vous.
6. Dans le champ **Mot de passe**, saisissez un mot de passe.
7. Cliquez sur **Ajouter**.
8. Cliquez sur + dans la section **Terminaux de destination autorisés pour les terminaux supervisés**.
9. Dans le champ **ID du terminal**, saisissez l'ID du terminal AirPlay auquel des terminaux sous supervision seront autorisés à se connecter. Vous trouverez l'ID du terminal AirPlay dans ses paramètres. Les terminaux sous supervision ne peuvent se connecter qu'aux terminaux AirPlay de la liste.
10. Cliquez sur **Ajouter**.

À la fin : Attribuez le profil AirPlay à des comptes d'utilisateur, groupes d'utilisateurs ou groupes de terminaux.

Création d'un profil de nom de point d'accès sur les terminaux Android

Un nom de point d'accès (APN) spécifie les informations dont un terminal mobile a besoin pour se connecter au réseau d'un opérateur. Vous pouvez utiliser un ou plusieurs profils de nom de point d'accès pour envoyer des APN pour les opérateurs aux terminaux Android de vos utilisateurs. Les profils de nom de point d'accès sont pris en charge par les terminaux dotés d'activations Espace Travail uniquement ou Travail et Personnel - Contrôle total.

Les terminaux ont généralement des APN prédéfinis pour les opérateurs courants. Les utilisateurs peuvent également ajouter de nouveaux APN à un terminal. Si vous souhaitez forcer un terminal à utiliser un APN qui lui est envoyé par un profil de nom de point d'accès, cochez la case Forcer le terminal à utiliser les paramètres de profil de nom de point d'accès dans la règle de stratégie informatique.

Avant de commencer : Obtenez tous les paramètres de nom de point d'accès (APN) nécessaires auprès de votre opérateur.

1. Sur la barre de menus, cliquez sur **Stratégies et profils > Réseaux et connexions > Nom du point d'accès**.
2. Cliquez sur +.
3. Saisissez le nom et la description du profil. Cette information s'affiche sur les terminaux.
4. Dans le champ **Nom du point d'accès**, saisissez le nom du point d'accès.
5. Indiquez les valeurs qui correspondent aux spécifications de l'opérateur pour chaque paramètre de profil. Pour plus d'informations, reportez-vous à Paramètres du profil de nom de point d'accès.
6. Cliquez sur **Enregistrer**.

À la fin : Attribuez le profil de nom de point d'accès à des comptes d'utilisateur, groupes d'utilisateurs ou groupes de terminaux.

Paramètres du profil de nom de point d'accès

Paramètre du profil de nom de point d'accès	Description
Nom du point d'accès	Ce paramètre spécifie le nom du point d'accès (APN) que votre terminal doit utiliser lorsqu'il communique avec l'opérateur. L'APN est une courte chaine de texte.
Masque binaire de type APN	Ce paramètre spécifie les types de communication de données qui utilisent cette configuration APN. Différents types de communications peuvent utiliser des configurations différentes.
Adresse proxy	Ce paramètre spécifie le proxy HTTP à utiliser pour l'ensemble du trafic Web sur la connexion. Ce paramètre n'est pas obligatoire pour la plupart des opérateurs.
Port de proxy	Ce paramètre spécifie le port de proxy HTTP à utiliser pour l'ensemble du trafic Web sur la connexion. Ce paramètre n'est pas obligatoire pour la plupart des opérateurs.
MMSC	Ce paramètre spécifie le centre de service de messagerie multimédia (MMSC) à utiliser pour l'envoi et la réception de messages MMS.
Adresse de proxy MMS	Ce paramètre spécifie le proxy HTTP utilisé pour communiquer avec le MMSC afin d'envoyer et de recevoir des messages MMS.
Port de proxy MMS	Ce paramètre spécifie le port de proxy HTTP utilisé pour communiquer avec le MMSC afin d'envoyer et de recevoir des messages MMS.
Type d'authentification	Ce paramètre spécifie le type d'authentification utilisé pour les communications.
nom d'utilisateur ;	Si le paramètre Type d'authentification est défini sur une option autre que AUCUN, spécifiez un nom d'utilisateur si l'authentification l'exige.
Mot de passe	Si le paramètre Type d'authentification est défini sur une option autre que AUCUN, spécifiez un mot de passe si l'authentification l'exige.

Paramètre du profil de nom de point d'accès	Description
Code de pays mobile (MCC)	Ce paramètre spécifie le code de pays mobile du réseau de l'opérateur pour lequel la configuration APN doit être utilisée.
Code de réseau mobile (MNC)	Ce paramètre spécifie le code de réseau mobile du réseau de l'opérateur pour lequel la configuration APN doit être utilisée.
Protocole	Ce paramètre indique s'il faut activer IPv4, IPv6 ou les deux sur le réseau domestique pour les terminaux qui prennent en charge la mise en réseau IPv6.
Protocole d'itinérance	Ce paramètre indique s'il faut activer IPv4, IPv6 ou les deux en itinérance pour les terminaux qui prennent en charge la mise en réseau IPv6.
Opérateur activé	Ce paramètre indique si l'APN est activé pour l'opérateur.
Type MVNO	Ce paramètre spécifie s'il faut restreindre l'utilisation de cet APN à certains MVNO (revendeurs de réseaux mobiles) ou comptes d'abonnés.

Utilisation de certificats PKI avec des terminaux ou des applications

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 en toute sécurité 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. L'autorité de certification peut ensuite révoquer l'approbation du certificat en cas de violation.

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

- Vous authentifier à l'aide de SSL/TLS lorsque vous vous connectez à des serveurs Web prenant en charge le protocole TLS mutuel, y compris un serveur de messagerie professionnel.
- Vous authentifier auprès d'un réseau Wi-Fi ou VPN professionnel.
- Cryptez et signez les e-mails à l'aide de la protection S/MIME.

De nombreux certificats utilisés à différentes fins peuvent être stockés sur un terminal. BlackBerry UEM fournit un certain nombre de profils pour faciliter la gestion des certificats PKI sur le terminal. Par exemple,

- La confiance du serveur d'autorité de certification peut être attribuée aux terminaux et aux applications à l'aide d'un profil de certificat d'autorité de certification.
- L'inscription automatique des certificats peut être attribuée aux terminaux et aux applications à l'aide de SCEP et de profils d'informations d'identification de l'utilisateur.
- La récupération des certificats de cryptage publics peut être attribuée aux terminaux et aux applications à l'aide du profil de récupération de certificat.
- La vérification de l'état de révocation du certificat peut être attribuée aux terminaux et aux applications à l'aide de profils OCSP et CRL.

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

Étape	Action
1	Si nécessaire, intégrez 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.

Étape	Action
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'informations d'identification des utilisateurs dans les paramètres de l'application.

Intégration de BlackBerry UEM avec le logiciel PKI de votre organisation

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 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.

Connexion de BlackBerry UEM au logiciel Entrust de votre organisation

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

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

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

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

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 avec des applications BlackBerry Dynamics installées sur des 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 CA Entrust pour envoyer le certificat aux terminaux

1. Sur la barre de menus de la console de gestion, cliquez sur **Paramètres > Intégration externe > Autorité de certification**.
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 CA 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.

Connexion de BlackBerry UEM au logiciel OpenTrust de votre organisation

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

Avant de commencer : Contactez l'administrateur OpenTrust de votre organisation 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 > Intégration externe > Autorité de certification**.
2. Cliquez sur **Ajouter une connexion OpenTrust**.
3. Dans le champ **Nom de connexion**, saisissez un nom de connexion.
4. Dans le champ **URL**, saisissez l'URL du logiciel OpenTrust.
5. Cliquez sur **Parcourir**. Naviguez jusqu'au et sélectionnez le certificat côté client utilisé par BlackBerry UEM pour authentifier la connexion au serveur OpenTrust.
6. Dans le champ **Mot de passe du certificat**, saisissez le mot de passe du certificat du serveur OpenTrust.
7. Pour tester la connexion, cliquez sur **Tester la connexion**.
8. 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 UEM avec le logiciel OpenTrust pour distribuer des certificats aux terminaux, il peut s'écouler un certain temps avant que les certificats ne soient valides. 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 l'option 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 UEM au connecteur PKI. Dans un environnement BlackBerry UEM Cloud, un BlackBerry Connectivity Node doit être installé pour permettre à UEM de communiquer avec le connecteur PKI via BlackBerry Cloud Connector.

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 de la console de gestion, 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 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 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 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, cliquez sur **Parcourir** pour accéder au certificat d'autorité de certification de votre organisation et le sélectionner.
   - **Certificat serveur du connecteur PKI** : si vous sélectionnez cette option, cliquez sur **Parcourir** pour accéder au certificat serveur du connecteur PKI de votre organisation et le sélectionner.
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 d'application 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 UEM.

1. Sur la barre de menus de la console de gestion, 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 le UEM Client.
4. Cliquez sur **Ajouter**.

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

- Créez des 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 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

Comment le certificat est ajouté	Description	Terminaux pris en charge
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 UEM envoie aux terminaux iOS, macOS et Android. 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
Envoi de certificat client à un compte d'utilisateur individuel	Vous pouvez ajouter un certificat client à un compte d'utilisateur. 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	Les utilisateurs peuvent charger des certificats sur BlackBerry UEM Self-Service. Puis UEM transfère le certificat sur les terminaux des utilisateurs. 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.	iOS Android
Importation par les utilisateurs	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 :

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 : • Spécifier une connexion au logiciel PKI de votre entreprise pour l'envoi des certificats client aux terminaux et aux applications BlackBerry Dynamics. • Télécharger manuellement les certificats dans BlackBerry UEM et, dans un environnement sur site, pour permettre aux utilisateurs de télécharger des certificats à l'aide de BlackBerry UEM Self-Service. • 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. • 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 UEM envoie aux terminaux iOS et Android. 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 Ajout et gestion d'un certificat client pour 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 de 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 l'écran **Application**, sous l'onglet **Paramètres > 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 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.
- Les terminaux Android Enterprise ne prennent pas en charge l'utilisation de certificats envoyés aux terminaux par 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 de la console de gestion, cliquez sur **Stratégies et profils > Certificats > Certificat d'autorité de certification**.
2. Cliquez sur +.
3. 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.
4. Dans le champ **Fichier de certificat**, cliquez sur **Parcourir** pour localiser le fichier de certificat.
5. 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**.
6. Cliquez sur **Ajouter**.

À la fin : Attribuez le profil de certificat d'autorité de certification à des comptes d'utilisateur, groupes d'utilisateurs ou groupes de terminaux.

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 :

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

Les profils d'informations 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.

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 > Certificats > Informations d'identification de l'utilisateur**.
2. Cliquez sur +.
3. Saisissez le nom et la description du profil. Chaque profil de certificat doit avoir un nom unique.
4. Dans la liste déroulante **Connexion à l'autorité de certification**, cliquez sur **Certificat chargé manuellement**.
5. Si vous gérez des terminaux Android Enterprise et que vous souhaitez empêcher les utilisateurs de sélectionner le certificat pour l'utiliser à d'autres fins, cochez la case **Masquer le certificat sur les terminaux Android Enterprise** dans l'onglet **Android**.
6. 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.
- Ajoutez un certificat client à un profil d'informations d'identification d'utilisateur ou demandez aux utilisateurs de charger leur propre certificat via BlackBerry UEM Self-Service.

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.

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.
- Demandez à l'administrateur Entrust ou OpenTrust quelles sont les valeurs de profil que vous devez fournir.
- 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 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 > Certificats > Informations d'identification de l'utilisateur**.
2. Cliquez sur +.
3. Saisissez le nom et la description du profil. Chaque profil de certificat doit avoir un nom unique.
4. Dans la liste déroulante **Connexion à l'autorité de certification**, sélectionnez la connexion Entrust ou OpenTrust que vous avez configurée.
5. Dans la liste déroulante **Profil**, cliquez sur le profil qui convient.
6. Spécifiez les valeurs du profil.
7. 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.
8. Indiquez la **Période de renouvellement** du certificat. Cette période peut être comprise entre 1 et 120 jours.
9. 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 d'Android sont invités à saisir le mot de passe 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.

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 > Certificats > Informations d'identification de l'utilisateur**.
2. Cliquez sur +.
3. Saisissez le nom et la description du profil.
4. Dans la liste déroulante **Connexion à l'autorité de certification**, sélectionnez la connexion via les informations d'identification intelligentes Entrust que vous avez configurée.
5. 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.
6. 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 cochez la case **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.
7. Si les informations d'identification intelligentes sont envoyées à des applications BlackBerry Dynamics, sous l'onglet **BlackBerry Dynamics**, 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 iOS Android les terminaux et 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.

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

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 en double, cochez la case **Supprimer les certificats en double**.
10. Cliquez sur **Ajouter**.

À la fin :

- Pour autoriser les applications BlackBerry Dynamics à utiliser des certificats, cliquez sur l'option **Applications** de la barre de menus. Cliquez sur l'application BlackBerry Dynamics que vous souhaitez modifier, accédez à l'onglet **Paramètres > BlackBerry Dynamics**, puis cochez la case **Autoriser les applications BlackBerry Dynamics à utiliser les certificats utilisateur, les profils SCEP et les profils d'informations d'identification des utilisateurs**.
- 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 > Certificats > Informations d'identification de l'utilisateur**.
2. Cliquez sur +.
3. Saisissez le nom et la description du profil.
4. Dans la liste déroulante **Connexion à l'autorité de certification**, cliquez sur la connexion PKI BlackBerry Dynamics que vous avez configurée.
5. 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**.
6. 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.

7. Si vous souhaitez que le terminal supprime les certificats expirés, cochez la case **Supprimer un certificat expiré**.
8. Si vous souhaitez que le terminal supprime les certificats en double, cochez la case **Supprimer les certificats en double**.
9. Cliquez sur **Ajouter**.

À la fin :

- Pour autoriser les applications BlackBerry Dynamics à utiliser des certificats, cliquez sur l'option **Applications** de la barre de menus. Cliquez sur l'application BlackBerry Dynamics que vous souhaitez modifier, accédez à l'onglet **Paramètres > BlackBerry Dynamics**, puis cochez la case **Autoriser les applications BlackBerry Dynamics à utiliser les certificats utilisateur, les profils SCEP et les profils d'informations d'identification des utilisateurs**.
- 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.
- Si vous souhaitez renouveler les certificats inscrits via le connecteur PKI, cliquez sur **Actualiser les fonctionnalités PKI > Renouveler** pour indiquer à tous les terminaux BlackBerry Dynamics auxquels le profil est attribué de demander le renouvellement 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 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.

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 UEM Client pour **Délégation d'authentification d'application**.
2	Pour utiliser une solution PKI basée sur les applications avec des terminaux iOS, connectez-vous BlackBerry UEM à la solution PKI basée sur les applications de votre entreprise.

Étape	Action
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	Utilisez la solution PKI basée sur les applications avec les terminaux suivants : • Terminaux iOS : Créer un profil d'identification d'utilisateur pour utiliser des certificats d'application. • Terminaux Android : Créer un profil 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.

Avant de commencer : Configurer le BlackBerry UEM Client pour la prise en charge des certificats d'applications.

1. Sur la console de gestion UEM, dans la barre de menu, cliquez sur **Applications**.
2. Dans la liste des applications, sélectionnez BlackBerry UEM Client.
3. Dans la section **Configuration d'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**.

À la fin : Attribuez le 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.

Avant de commencer : Assurez-vous d'avoir effectué l'une des opérations suivantes :

- Si votre environnement utilise 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.

- 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.

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

Tâche	Étapes
Configurer BlackBerry Work lorsque votre organisation utilise BEMS	**a.** Sous l'onglet **Configuration de base**, dans la section **Paramètres de sécurité**, cochez la case **Utilise un certificat client plutôt qu'un identifiant/mot de passe**. **b.** Pour activer la détection automatique du serveur Microsoft Exchange sur lequel se trouvent les utilisateurs, dans la section **Paramètres client**, cochez la case **Utiliser BEMS pour effectuer la détection automatique du point de terminaison EAS/EWS pour l'utilisateur**. **c.** Sous l'onglet **Configuration avancée**, dans la section **Paramètres de certificat TLS**, saisissez le nom du profil d'informations d'identification de l'utilisateur pour le terminal.
Configurer BlackBerry Work lorsque votre entreprise n'utilise pas BEMS	**a.** Cliquez sur l'onglet **Configuration de base**. **b.** Si votre serveur utilise le format de connexion nom\identifiant utilisateur, dans le champ **Domaine par défaut** de la section **Paramètres Exchange ActiveSync**, spécifiez le domaine par défaut Windows NT auquel BlackBerry Work se connecte lorsque les utilisateurs ouvrent une session. **c.** Dans le champ **Active Sync Server**, spécifiez le serveur Exchange ActiveSync par défaut auquel BlackBerry Work se connectera lorsque les utilisateurs se connecteront à BlackBerry Work (par exemple, cas.mydomain.com). **d.** Dans le champ **URL de détection automatique**, spécifiez l'URL de détection automatique, si connue. Ceci accélère le processus de configuration de détection automatique (par exemple, https://autodiscover.mydomain.com). **e.** Dans le champ **Délai d'expiration de la détection automatique de connexion (iOS uniquement)**, 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** de la section **Paramètres de certificat TLS**, saisissez le nom du profil d'informations d'identification de l'utilisateur.

5. Cliquez sur **Enregistrer**.

À la fin : Créez une solution PKI basée sur les applications à utiliser avec les terminaux suivants :

- Terminaux iOS : Créer un profil d'identification d'utilisateur pour utiliser des certificats d'application.
- Terminaux Android : Créer un profil d'identification d'utilisateur pour utiliser des certificats du magasin de clés natif.

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

Avant de commencer :

- Configurer le BlackBerry UEM Client pour la prise en charge des certificats d'applications.
- Vérifiez que l'application PKI (par exemple, Purebred) est installée sur les terminaux des utilisateurs.

1. Sur la barre de menus, cliquez sur **Stratégies et profils > Certificats > Informations d'identification de l'utilisateur**.
2. Cliquez sur +.
3. Saisissez le nom et la description du profil.
4. Dans la liste déroulante **Connexion à l'autorité de certification**, cliquez sur 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.
5. 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
      ```
6. Si vous souhaitez que le terminal supprime les certificats ayant expiré, sélectionnez **Supprimer les certificats ayant expiré**.
7. Si vous souhaitez que le terminal supprime les certificats dupliqués, sélectionnez **Supprimer les certificats dupliqués**.
8. Cliquez sur **Ajouter**.

À la fin :

- Pour autoriser les applications BlackBerry Dynamics à utiliser des certificats, cliquez sur l'option **Applications** de la barre de menus. Cliquez sur l'application BlackBerry Dynamics que vous souhaitez modifier, puis sur l'onglet **Paramètres > BlackBerry Dynamics**, cochez la case **Autoriser les applications BlackBerry Dynamics à utiliser les certificats utilisateur, les profils SCEP et les profils d'informations d'identification des utilisateurs**.

- 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 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 > Certificats > SCEP**.
2. Cliquez sur +.
3. Saisissez le nom et la description du profil.
4. 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. Veuillez noter que 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.
5. 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.
6. Dans le champ **Nom de l'instance**, saisissez le nom de l'instance pour l'autorité de certification.
7. Vous pouvez également décocher la case correspondant aux types de terminaux pour lesquels vous ne souhaitez pas configurer le profil.

8. 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. Reportez-vous à :
      - Communs : paramètres de profil SCEP
      - iOS : paramètres de profil SCEP
      - macOS : paramètres de profil SCEP
      - Android : paramètres de profil SCEP
      - Windows 10 : paramètres de profil SCEP
      - BlackBerry Dynamics : paramètres de profil SCEP
9. Répétez l'étape 8 pour chaque type de terminal de votre organisation.
10. 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.

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.
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 UEM pour que 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. 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.
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 de profil SCEP

iOS : 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 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.

iOS : paramètre de 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.
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).
Nouvelles tentatives	Ce paramètre spécifie le nombre de nouvelles tentatives de connexion au service SCEP si la tentative de connexion échoue.
Délai de nouvelle tentative	Ce paramètre spécifie le délai d'attente, en secondes, avant une nouvelle tentative de connexion au service SCEP.
Taille de la clé	Ce paramètre spécifie la taille de la clé du certificat.
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.
Type SAN	Ce paramètre spécifie le type d'autre nom d'objet du certificat, si nécessaire.
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.

macOS : paramètres de profil SCEP

macOS : 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.
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.
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, par exemple : %UserDistinguishedName%.
Nouvelles tentatives	Ce paramètre spécifie le nombre de nouvelles tentatives de connexion au service SCEP si la tentative de connexion échoue.
Délai de nouvelle tentative	Ce paramètre spécifie le délai d'attente, en secondes, avant une nouvelle tentative de connexion au service SCEP.
Taille de la clé	Ce paramètre spécifie la taille de la clé du certificat.
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.
Type SAN	Ce paramètre spécifie le type d'autre nom d'objet du certificat, si nécessaire.
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.

macOS : paramètre de profil SCEP	Description
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 les terminaux associés aux types d'activation Android Management, reportez-vous à la section Considérations relatives aux types d'activation Android Management.

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 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 les utilisateurs d'Android Enterprise voient le certificat. 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 UEM Cloud.
Algorithme de cryptage	Ce paramètre spécifie l'algorithme de cryptage utilisé par les terminaux Android pour la demande d'inscription de certificat.
Fonction de hachage	Ce paramètre spécifie la fonction de hachage utilisée par les terminaux Android pour la demande d'inscription de certificat.
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.
Profils professionnels Android et 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.
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 pour générer la paire de clés client. Vous devez sélectionner un algorithme pris en charge par votre autorité de certification.
Puissance RSA	Ce paramètre spécifie la puissance RSA utilisée par les terminaux pour générer la paire de clés client. Vous devez saisir une force de clé prise en charge par votre autorité de certification. Ce paramètre n'est valide que si le paramètre Algorithme de clé est défini sur RSA.
Utilisation de la clé	Ce paramètre spécifie les opérations cryptographiques pouvant être effectuées à l'aide de la clé publique contenue dans le certificat.
Utilisation étendue de la clé	Ce paramètre spécifie l'objectif de la clé contenue dans le certificat.

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).
Type SAN	Ce paramètre spécifie le type d'autre nom d'objet du certificat, si nécessaire.

Windows 10 : paramètre de profil SCEP	Description
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.
Délai de nouvelle tentative	Ce paramètre spécifie le délai d'attente, en secondes, avant une nouvelle tentative de connexion au service SCEP.
Taille de la clé	Ce paramètre spécifie la taille de la clé du certificat.
Utilisation de la clé	Ce paramètre spécifie les opérations cryptographiques pouvant être effectuées à l'aide de la clé publique contenue dans le certificat.
Utilisation étendue de la clé	Ce paramètre spécifie l'objectif de la clé contenue dans le certificat.
Stockage de clés SCEP	Ce paramètre spécifie l'emplacement de stockage de la clé privée.
Fonction de hachage	Ce paramètre spécifie la fonction de hachage utilisée par un terminal Windows 10 pour la demande d'inscription de certificat.
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. La valeur maximale est de 365 jours.

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=<*common_name*>,O=<*domain_name*> ». 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.

BlackBerry Dynamics : paramètre de profil SCEP	Description
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 pour générer la paire de clés client. Vous devez sélectionner un algorithme pris en charge par votre autorité de certification.
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.
Algorithme de cryptage	Ce paramètre spécifie l'algorithme de chiffrement utilisé pour la demande d'inscription de certificat.
Fonction de hachage	Ce paramètre spécifie la fonction de hachage utilisée pour la demande d'inscription de certificat.
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.
Utilisation de la clé	Ce paramètre spécifie les opérations cryptographiques pouvant être effectuées à l'aide de la clé publique contenue dans le certificat.
Utilisation étendue de la clé	Ce paramètre spécifie l'objectif de la clé contenue dans le certificat.
Restrictions d'applications	Ce paramètre spécifie les applications BlackBerry Dynamics qui peuvent utiliser le certificat.
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.

BlackBerry Dynamics : paramètre de profil SCEP	Description
Supprimer les certificats expirés	Ce paramètre spécifie si le terminal supprime les certificats expirés.
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.

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 > Certificats > Certificat partagé**.
2. Cliquez sur +.
3. Saisissez le nom et la description du profil.
4. Dans le champ **Mot de passe**, indiquez un mot de passe pour le profil de certificat partagé.
5. Dans le champ **Fichier de certificat**, cliquez sur **Parcourir** pour localiser le fichier de certificat.
6. Si vous gérez des terminaux Android Enterprise et que vous souhaitez empêcher les utilisateurs de sélectionner le certificat pour l'utiliser à d'autres fins, sélectionnez **Masquer le certificat sur les terminaux Android Enterprise** dans l'onglet **Android**.
7. Si vous gérez des terminaux macOS, sous l'onglet **macOS**, accédez à la liste déroulante **Appliquer le profil à**, puis sélectionnez **Utilisateur** ou **Terminal**.
8. Cliquez sur **Ajouter**.

À la fin : Attribuez le profil de certificat partagé à des comptes d'utilisateur, groupes d'utilisateurs ou groupes de terminaux.

Spécification du certificat à utiliser par une application à l'aide d'un profil de mappage de certificats

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

Les profils de mappage de certificats vous permettent de spécifier les certificats à utiliser par les applications Android. 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.

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

1. Sur la barre de menus, cliquez sur **Stratégies et profils > Certificats > Mappage de certificats**.

2. Cliquez sur +.
3. Saisissez le nom et la description du profil.
4. Dans la table de mappage, cliquez sur +.
5. Sous **URI de la destination**, sélectionnez l'une des options suivantes :
   - Sélectionnez **Aucun(e)** afin que l'application n'utilise pas le certificat pour authentifier une connexion avec une ressource.
   - Sélectionnez **Toute** afin 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 afin que l'application utilise le certificat pour l'authentification avec une ressource spécifique.
6. 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** et cliquez sur 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.
   - Pour spécifier que l'application doit utiliser un certificat envoyé au terminal par un autre profil, sélectionnez **Certificat sélectionné** et cliquez sur le nom du profil dans la liste déroulante.
7. Sous **Applications autorisées pour l'URI de destination**, effectuez l'une des opérations 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.
8. Si nécessaire, répétez les étapes 5 à 8 pour ajouter d'autres mappages au profil.
9. Cliquez sur **Ajouter**.

À la fin :

- Attribuez le profil aux comptes d'utilisateur et groupes d'utilisateurs.
- Si vous créez plusieurs profils de mappage de certificats, classez-les (si nécessaire). Sélectionnez un profil et cliquez sur ↓↑ pour déplacer le profil vers le haut ou vers le bas du classement. Cliquez sur **Enregistrer**.

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 de connexion au réseau Wi-Fi, au VPN et au serveur de messagerie de votre entreprise, utilisez un profil d'informations d'identification de l'utilisateur, qui peut être associé à un profil Wi-Fi, VPN ou de messagerie.

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.

Ajout et gestion d'un certificat client pour un compte d'utilisateur

1. Sur la barre de menus de la console de gestion, cliquez sur **Utilisateurs > Terminaux gérés**.
2. Recherchez et cliquez sur un compte d'utilisateur.
3. Effectuez l'une des opérations suivantes :

Tâche	Étapes
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 certifications des utilisateurs individuels. Les profils d'informations d'identification de l'utilisateur peuvent être associés à un profil Wi-Fi, VPN ou de messagerie. **a.** Dans la section **Profils et stratégies informatiques**, cliquez sur +. **b.** Cliquez sur **Certificat utilisateur**. **c.** Saisissez la description du certificat. **d.** Dans la section **Appliquer le certificat à**, sélectionnez l'un des éléments suivants : 1. **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. 2. **Terminaux BlackBerry Dynamics activés** : choisissez cette option pour envoyer le certificat aux terminaux aux fins d'utilisation avec des applications BlackBerry Dynamics. **e.** Dans le champ **Fichier de certificat**, cliquez sur **Parcourir**. Accédez au fichier du certificat et sélectionnez-le. **f.** Si vous sélectionnez **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 si le terminal exécute la version la plus récente de UEM Client. Si vous ne définissez aucun mot de passe, l'utilisateur doit saisir le mot de passe du terminal. **g.** Cliquez sur **Ajouter**. **h.** Configurez la valeur TTL des certificats client. La valeur TTL par défaut avant suppression des certificats client est de 24 heures. 1. Dans la barre de menus, cliquez sur **Paramètres > Paramètres généraux > Certificats**. 2. Spécifiez la valeur TTL des certificats PKCS#12 sur le serveur.

Tâche	Étapes
Renouvellement ou suppression d'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'AC indiquant que le certificat n'est plus utilisé, mais le certificat n'est pas automatiquement révoqué. Effectuez l'une des opérations suivantes dans la section **Certificats utilisateur** : **a.** Cliquez sur ↻ pour demander le renouvellement du certificat à partir de l'autorité de certification. **b.** Cliquez sur ✕ pour supprimer le certificat des terminaux de l'utilisateur. 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 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. **a.** Dans la section **Stratégie informatique et profils**, en regard du profil d'informations d'identification de l'utilisateur, cliquez sur **Ajouter un certificat**. **b.** Cliquez sur **Parcourir**. Accédez au certificat et sélectionnez-le. **c.** 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 UEM si le terminal exécute la version la plus récente de UEM Client. Si vous ne spécifiez aucun mot de passe, l'utilisateur doit saisir le mot de passe du terminal. **d.** Cliquez sur **Ajouter**.

Tâche	Étapes
Modifier un certificat client pour un profil d'informations d'identification de l'utilisateur	Le nouveau certificat remplace le certificat existant sur le terminal. **a.** Dans la section **Stratégie informatique et profils**, en regard du profil d'informations d'identification de l'utilisateur, cliquez sur **Mettre à jour**. **b.** Cliquez sur **Parcourir** pour localiser le certificat. **c.** 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 UEM si le terminal exécute la version la plus récente de UEM Client. Si vous ne spécifiez aucun mot de passe, l'utilisateur doit saisir le mot de passe du terminal. **d.** Cliquez sur **Enregistrer**.

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