



# **BlackBerry UEM**

## **Sécurisation des connexions réseau**

Administration

12.16



# Table des matières

<b>Gestion des connexions Wi-Fi, VPN, BlackBerry Secure Connect Plus et autres connexions professionnelles.....</b>	<b>5</b>
<b>Gestion des connexions professionnelles à l'aide des profils.....</b>	<b>6</b>
<b>Méthode recommandée : création de profils de connexions professionnelles.....</b>	<b>7</b>
<b>Configuration de réseaux Wi-Fi professionnels pour les terminaux.....</b>	<b>8</b>
Créer un profil Wi-Fi.....	8
Paramètres de profil Wi-Fi.....	9
Communs : paramètres de profil Wi-Fi.....	9
iOS et macOS : Paramètres de profil Wi-Fi.....	9
Android : paramètres de profil Wi-Fi.....	15
Windows : paramètres de profil Wi-Fi.....	20
<b>Configuration de réseaux VPN professionnels pour les terminaux.....</b>	<b>25</b>
Créer un profil VPN.....	25
Paramètres du profil VPN.....	26
iOS et macOS : Paramètres du profil VPN.....	26
Android : paramètres de profil VPN.....	40
Windows 10 : Paramètres du profil VPN.....	45
Activation d'un VPN par application.....	51
Comment BlackBerry UEM choisit les paramètres VPN par application à attribuer aux terminaux iOS.....	52
<b>Création de profils proxy pour les terminaux.....</b>	<b>53</b>
Créer un profil proxy.....	54
<b>Utilisation de BlackBerry Secure Connect Plus pour des connexions aux ressources professionnelles.....</b>	<b>56</b>
Étapes à suivre pour activer BlackBerry Secure Connect Plus.....	56
Exigences liées au serveur et au terminal pour BlackBerry Secure Connect Plus.....	57
Installation de composants BlackBerry Secure Connect Plus supplémentaires dans un environnement sur site.....	58
Installation ou mise à niveau du composant BlackBerry Secure Connect Plus dans un environnement Cloud.....	59
Activer BlackBerry Secure Connect Plus.....	59
Paramètres de profil de connectivité d'entreprise.....	60

Spécifier les paramètres DNS pour l'application BlackBerry Connectivity.....	63
Optimiser les connexions de tunnel sécurisées pour les terminaux Android qui utilisent des applications BlackBerry Dynamics.....	64
Résolution des problèmes BlackBerry Secure Connect Plus.....	64
L'adaptateur BlackBerry Secure Connect Plus passe à un état « Réseau non identifié » et cesse de fonctionner.....	64
BlackBerry Secure Connect Plus ne démarre pas.....	65
BlackBerry Secure Connect Plus cesse de fonctionner après une installation ou une mise à niveau BlackBerry UEM.....	65
Afficher les fichiers journaux pour BlackBerry Secure Connect Plus.....	66

## **Utilisation de BlackBerry 2FA pour les connexions sécurisées aux ressources essentielles.....67**

## **Configuration de l'authentification avec identification unique pour les terminaux.....68**

Créer un profil d'extension d'identification unique.....	68
--	----

## **Configuration des profils DNS pour les terminaux iOS et macOS.....71**

Créer un profil DNS.....	71
--------------------------	----

## **Gérer les domaines de messagerie et les domaines Web pour les terminaux iOS.....72**

Créer un profil de domaines gérés.....	72
--	----

## **Contrôle de l'utilisation du réseau pour les applications sur les terminaux iOS.....73**

Créer un profil d'utilisation du réseau.....	73
--	----

## **Filtrage de contenu Web sur les terminaux iOS.....74**

Créer un profil de filtre de contenu Web.....	74
---	----

## **Configuration des profils AirPrint et AirPlay pour les terminaux iOS.....76**

Créer un profil AirPrint.....	76
Créer un profil AirPlay.....	77

## **Configuration des noms de points d'accès pour les terminaux Android.....78**

Créer un profil de nom de point d'accès.....	78
Paramètres du profil de nom de point d'accès.....	78

## **Informations juridiques.....81**

# Gestion des connexions Wi-Fi, VPN, BlackBerry Secure Connect Plus et autres connexions professionnelles

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.

# Gestion des connexions professionnelles à l'aide des profils

Vous pouvez configurer la manière dont les terminaux se connectent aux ressources professionnelles à l'aide des profils suivants :

Profil	Description
Wi-Fi	Un profil Wi-Fi spécifie la manière dont les terminaux se connectent à un réseau Wi-Fi professionnel.
VPN	Un profil VPN spécifie la manière dont les terminaux se connectent à un VPN professionnel.
Proxy	Un profil proxy spécifie la manière dont les terminaux utilisent un serveur proxy pour accéder à des services Web sur Internet ou un réseau professionnel.
Connectivité d'entreprise	Le profil de connectivité d'entreprise détermine la manière dont les terminaux se connectent aux ressources de votre organisation via la connectivité d'entreprise et BlackBerry Secure Connect Plus.
BlackBerry 2FA	Un profil BlackBerry 2FA active l'authentification à deux facteurs pour les utilisateurs et spécifie la configuration de la préauthentification et les fonctionnalités de résolution autonome.
Extension d'identification unique	Un profil d'extension avec identification unique spécifie la manière dont les terminaux iOS et iPadOS s'authentifient automatiquement auprès des domaines sécurisés après que les utilisateurs se connectent pour la première fois.
Profil de connectivité BlackBerry Dynamics	Un profil de connectivité BlackBerry Dynamics définit 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.
E-mail	Un profil de messagerie spécifie la manière dont les terminaux se connectent à un serveur de messagerie professionnel et synchronisent les e-mails, les entrées de calendrier et les données de l'organiseur à l'aide de Exchange ActiveSync ou IBM Notes Traveler.
Messagerie IMAP/POP3	Un profil de messagerie IMAP/POP3 spécifie la manière dont les terminaux se connectent à un serveur de messagerie IMAP or POP3 et synchronisent les e-mails.

# Méthode recommandée : création de profils de connexions professionnelles

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.

Prenez en compte les recommandations suivantes :

- Déterminez les connexions professionnelles requises pour les terminaux de votre organisation.
- Créez des profils que vous pouvez associer à d'autres profils avant de créer les profils de connexions professionnelles qui les utilisent.
- Utilisez des variables, le cas échéant.

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 stockés sur le terminal 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.

### 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.

**Remarque :** Les terminaux Samsung Knox Workspace ne prennent pas en charge l'utilisation de certificats envoyés aux terminaux par BlackBerry UEM pour l'authentification Wi-Fi. Les utilisateurs doivent configurer manuellement l'authentification basée sur certificat sur les terminaux Samsung Knox Workspace.

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



## Paramètres de profil Wi-Fi

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. Les [profils Wi-Fi](#) sont pris en charge sur les types de terminaux suivants :

- iOS
- iPadOS
- macOS
- Android
- Windows

### Communs : paramètres de profil Wi-Fi

Commun : paramètre de profil Wi-Fi	Description
SSID	Ce paramètre spécifie le nom d'un réseau Wi-Fi et ses points d'accès sans fil. Le SSID est sensible à la casse et doit contenir des caractères alphanumériques. Les valeurs possibles sont limitées à 32 caractères.
Réseau masqué	Ce paramètre spécifie si le réseau Wi-Fi masque le SSID.

### iOS et macOS : Paramètres de profil Wi-Fi

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

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

iOS 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. Valeurs possibles : <ul style="list-style-type: none"><li>• Utilisateur</li><li>• Terminal</li></ul> Ce paramètre est valide uniquement pour macOS.
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. Ce paramètre s'applique uniquement aux terminaux exécutant iOS et iPadOS 14 ou version ultérieure.
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.

iOS et macOS : Paramètre de profil Wi-Fi	Description
Type de réseau	<p>Ce paramètre spécifie la configuration du réseau Wi-Fi.</p> <p>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.</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> <li>• Standard</li> <li>• Point d'accès hérité</li> <li>• Hotspot 2.0</li> </ul> <p>La valeur par défaut est Standard.</p>
Nom de l'opérateur affiché	<p>Ce paramètre spécifie le nom convivial de l'opérateur de points d'accès.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de réseau est défini sur Hotspot 2.0.</p>
Nom de domaine	<p>Ce paramètre spécifie le nom de domaine de l'opérateur de points d'accès.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de réseau est défini sur Hotspot 2.0.</p> <p>Le paramètre SSID n'est pas requis lorsque vous utilisez ce paramètre.</p>
Identifiants d'entreprise des consortiums d'itinérance	<p>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.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de réseau est défini sur Hotspot 2.0.</p>
Noms de domaine NAI	<p>Ce paramètre spécifie les noms de domaine de l'identifiant d'accès réseau capables d'authentifier un terminal.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de réseau est défini sur Hotspot 2.0.</p>
MCC/MNC	<p>Ce paramètre spécifie les combinaisons MCC et MNC qui identifient les opérateurs de réseaux mobiles. Chaque valeur doit contenir six chiffres.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de réseau est défini sur Hotspot 2.0.</p>
Autoriser la connexion aux réseaux des partenaires d'itinérance	<p>Ce paramètre spécifie si un terminal peut se connecter aux partenaires d'itinérance pour le point d'accès.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de réseau est défini sur Hotspot 2.0.</p>

iOS et macOS : Paramètre de profil Wi-Fi	Description
Type de sécurité	<p>Ce paramètre indique le type de sécurité utilisé par le réseau Wi-Fi.</p> <p>Si le paramètre Type de réseau est défini sur Hotspot 2.0, ce paramètre est défini sur WPA2-Enterprise.</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> <li>• Aucun</li> <li>• WEP personnel</li> <li>• WEP Enterprise</li> <li>• WPA-Personal</li> <li>• WPA-Enterprise</li> <li>• WPA2-Personal</li> <li>• WPA2-Enterprise</li> <li>• WPA3-Personal</li> <li>• WPA3-Enterprise</li> </ul> <p>La valeur par défaut est Aucune.</p>
Clé WEP	<p>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).</p> <p>Exemples de valeurs de clés hexadécimales : ABCDEF0123 ou ABCDEF0123456789ABCDEF0123. Exemples de valeurs de clés alphanumériques : abCD5 ou abCDefGHijKL1.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini sur WEP personnel.</p>
Clé pré-partagée	<p>Ce paramètre spécifie la clé pré-partagée du réseau Wi-Fi.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini sur WPA-Personal, WPA2-Personal ou WPA3-Personal.</p>
<b>Protocoles</b>	
Protocole d'authentification	<p>Ce paramètre spécifie la méthode EAP prise en charge par le réseau Wi-Fi. Vous pouvez sélectionner plusieurs méthodes EAP.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini sur WEP Enterprise, WPA-Enterprise, WPA2-Enterprise ou WPA3-Enterprise.</p> <p>Sélections possibles :</p> <ul style="list-style-type: none"> <li>• TLS</li> <li>• TTLS</li> <li>• LEAP</li> <li>• PEAP</li> <li>• EAP-FAST</li> <li>• EAP-SIM</li> <li>• EAP-AKA</li> </ul>

iOS et macOS : Paramètre de profil Wi-Fi	Description
Authentification interne	<p>Ce paramètre indique la méthode d'authentification interne à utiliser avec TTLS.</p> <p>Ce paramètre est valide uniquement si le paramètre Protocole d'authentification est défini sur TTLS.</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> <li>• Aucun</li> <li>• PAP</li> <li>• CHAP</li> <li>• MS-CHAP</li> <li>• MS-CHAPv2</li> <li>• EAP</li> </ul> <p>La valeur par défaut est MS-CHAPv2.</p>
Utiliser PAC	<p>Ce paramètre spécifie si la méthode EAP-FAST utilise des informations d'accès protégé (PAC).</p> <p>Ce paramètre est valide uniquement si le paramètre Protocole d'authentification est défini sur EAP-FAST.</p>
Déployer PAC	<p>Ce paramètre spécifie si la méthode EAP-FAST permet un déploiement PAC.</p> <p>Ce paramètre est valide uniquement si le paramètre Protocole d'authentification est défini sur EAP-FAST et si le paramètre Utiliser PAC est sélectionné.</p>
Déployer PAC anonymement	<p>Ce paramètre spécifie si la méthode EAP-FAST permet un déploiement PAC anonyme.</p> <p>Ce paramètre est valide uniquement si le paramètre Protocole d'authentification est défini sur Utiliser PAC et si le paramètre Déployer PAC est sélectionné.</p>
<b>Authentification</b>	
Identité externe pour TTLS, PEAP et EAP-FAST	<p>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).</p> <p>Ce paramètre est valide uniquement si le paramètre Protocole d'authentification est défini sur TTLS, PEAP ou EAP-FAST.</p>
Utiliser le mot de passe inclus dans le profil Wi-Fi	<p>Ce paramètre spécifie si le profil Wi-Fi inclut le mot de passe à des fins d'authentification.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini sur WEP Enterprise, WPA-Enterprise, WPA2-Enterprise ou WPA3-Enterprise.</p>

iOS et macOS : Paramètre de profil Wi-Fi	Description
Mot de passe	<p>Ce paramètre spécifie le mot de passe utilisé par un terminal pour s'authentifier auprès du réseau Wi-Fi.</p> <p>Ce paramètre est valide uniquement si le paramètre Utiliser le mot de passe inclus dans le profil Wi-Fi est sélectionné.</p>
nom d'utilisateur ;	<p>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%.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini sur WEP Enterprise, WPA-Enterprise, WPA2-Enterprise ou WPA3-Enterprise.</p>
Type d'authentification	<p>Ce paramètre spécifie le type d'authentification utilisé par un terminal pour se connecter au réseau Wi-Fi.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini sur WEP Enterprise, WPA-Enterprise, WPA2-Enterprise ou WPA3-Enterprise.</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> <li>• Aucun</li> <li>• Certificat partagé</li> <li>• SCEP</li> <li>• Informations d'identification de l'utilisateur</li> </ul> <p>La valeur par défaut est Aucune.</p>
Type de liaison de certificat	<p>Ce paramètre spécifie le type de liaison du certificat client associé au profil Wi-Fi.</p> <p>Ce paramètre est valide uniquement si le paramètre Type d'authentification est défini sur Certificat partagé.</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> <li>• Référence unique</li> <li>• Injection de variable</li> </ul> <p>La valeur par défaut est Référence unique.</p>
Profil de certificat partagé	<p>Ce paramètre spécifie le profil de certificat partagé avec le certificat client utilisé par un terminal pour s'authentifier auprès du réseau Wi-Fi.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de liaison de certificat est défini sur Référence unique.</p>
Nom du certificat client	<p>Ce paramètre spécifie le nom du certificat client utilisé par un terminal pour s'authentifier auprès du réseau Wi-Fi.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de liaison de certificat est défini sur Injection de variable.</p>

iOS et macOS : Paramètre de profil Wi-Fi	Description
Profil SCEP associé	<p>Ce paramètre spécifie le profil SCEP associé utilisé par un terminal pour obtenir un certificat client et s'authentifier auprès du réseau Wi-Fi.</p> <p>Ce paramètre est valide uniquement si le paramètre Type d'authentification est défini sur SCEP.</p>
Profil des informations d'identification de l'utilisateur associé	<p>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.</p> <p>Ce paramètre est valide uniquement si le paramètre Type d'authentification est défini sur Informations d'identification de l'utilisateur.</p>
<b>Se fier</b>	
Noms usuels de certificat attendus par le serveur d'authentification	<p>Ce paramètre spécifie les noms usuels du certificat envoyés par le serveur d'authentification au terminal (par exemple, *.exemple.com).</p> <p>Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini sur WEP Enterprise, WPA-Enterprise, WPA2-Enterprise ou WPA3-Enterprise.</p>
Type de liaison de certificat	<p>Ce paramètre spécifie le type de liaison des certificats client associés au profil Wi-Fi.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini sur WEP Enterprise, WPA-Enterprise, WPA2-Enterprise ou WPA3-Enterprise.</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> <li>• Référence unique</li> <li>• Injection de variable</li> </ul> <p>La valeur par défaut est Référence unique.</p>
Profils de certificat d'autorité de certification	<p>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.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de liaison de certificat est défini sur Référence unique.</p>
Noms de certificats approuvés	<p>Ce paramètre spécifie les noms des certificats approuvés utilisés par un terminal pour établir une connexion approuvée au réseau Wi-Fi.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de liaison de certificat est défini sur Injection de variable.</p>
Faire confiance aux décisions d'utilisateur	<p>Ce paramètre spécifie si un terminal doit inviter l'utilisateur à approuver un serveur lorsque la chaîne 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.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini sur WEP Enterprise, WPA-Enterprise, WPA2-Enterprise ou WPA3-Enterprise.</p>

<b>iOS et macOS : Paramètre de profil Wi-Fi</b>	<b>Description</b>
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**

<b>Android : paramètre de profil Wi-Fi</b>	<b>Description</b>
Profil proxy associé	<p>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.</p> <p>Les terminaux Android 8.0 et version ultérieure dotés des activations Contrôles MDM ou Confidentialité de l'utilisateur ne prennent pas en charge les profils Wi-Fi avec des paramètres de proxy. Si un terminal doté de l'un de ces types d'activation est mis à niveau vers Android 8.0, les profils Wi-Fi associés à un profil de proxy sont supprimés du terminal.</p>
BSSID	Ce paramètre spécifie l'adresse MAC du point d'accès sans fil du réseau Wi-Fi.
DNS primaire	<p>Ce paramètre spécifie le serveur DNS primaire au format décimal séparé par des points (par exemple, 192.0.2.0).</p> <p>Ce paramètre s'applique uniquement aux terminaux utilisant Samsung Knox lorsque l'adresse IP est attribuée de façon statique par le réseau de l'organisation.</p>
DNS secondaire	<p>Ce paramètre spécifie le serveur DNS secondaire au format décimal séparé par des points (par exemple, 192.0.2.0).</p> <p>Ce paramètre s'applique uniquement aux terminaux utilisant Samsung Knox lorsque l'adresse IP est attribuée de façon statique par le réseau de l'organisation.</p>

Android : paramètre de profil Wi-Fi	Description
Type de sécurité	<p>Ce paramètre indique le type de sécurité utilisé par le réseau Wi-Fi.</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> <li>• Aucun</li> <li>• Personnel</li> <li>• Entreprise</li> </ul> <p>La valeur par défaut est Aucune.</p>
Type de sécurité personnelle	<p>Ce paramètre indique le type de sécurité personnelle utilisé par le réseau Wi-Fi.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini sur Personnelle.</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> <li>• Aucun</li> <li>• WEP personnel</li> <li>• WPA-Personal/WPA2-Personal</li> </ul> <p>La valeur par défaut est Aucune.</p>
Clé WEP	<p>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).</p> <p>Exemples de valeurs de clés hexadécimales : ABCDEF0123 ou ABCDEF0123456789ABCDEF0123. Exemples de valeurs de clés alphanumériques : abCD5 ou abCDefGHijKL1.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de sécurité personnelle est défini sur WEP personnel.</p>
Clé pré-partagée	<p>Ce paramètre spécifie la clé pré-partagée du réseau Wi-Fi.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de sécurité personnelle est défini sur WPA-Personal/WPA2-Personal.</p>
Protocole d'authentification	<p>Ce paramètre spécifie la méthode EAP utilisée par le réseau Wi-Fi.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini sur Entreprise.</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> <li>• TLS</li> <li>• TTLS</li> <li>• PEAP</li> <li>• LEAP</li> </ul> <p>La valeur par défaut est TLS.</p> <p>Le protocole LEAP n'est pas pris en charge par les terminaux utilisant Samsung Knox.</p>



Android : paramètre de profil Wi-Fi	Description
Authentification interne	<p>Ce paramètre indique la méthode d'authentification interne à utiliser avec TTLS.</p> <p>Ce paramètre est valide uniquement si le paramètre Protocole d'authentification est défini sur TTLS.</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> <li>• Aucun</li> <li>• PAP</li> <li>• CHAP</li> <li>• MS-CHAP</li> <li>• MS-CHAPv2</li> <li>• GTC</li> </ul> <p>La valeur par défaut est MS-CHAPv2.</p> <p>Le protocole CHAP n'est pas pris en charge par les terminaux utilisant Samsung Knox.</p>
Identité Externe pour TTLS	<p>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).</p> <p>Ce paramètre est valide uniquement si le paramètre Protocole d'authentification est défini sur TTLS.</p>
Identité Externe pour PEAP	<p>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).</p> <p>Ce paramètre est valide uniquement si le paramètre Protocole d'authentification est défini sur PEAP.</p>
nom d'utilisateur ;	<p>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%.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini sur Entreprise.</p>
Utiliser le mot de passe inclus dans le profil Wi-Fi	<p>Ce paramètre spécifie si le profil Wi-Fi inclut le mot de passe à des fins d'authentification.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini sur Entreprise.</p>

Android : paramètre de profil Wi-Fi	Description
Mot de passe	<p>Ce paramètre spécifie le mot de passe utilisé par un terminal Android pour s'authentifier auprès du réseau Wi-Fi.</p> <p>Ce paramètre est valide uniquement si le paramètre Utiliser le mot de passe inclus dans le profil Wi-Fi est sélectionné.</p>
Type d'authentification	<p>Ce paramètre spécifie le type d'authentification utilisé par un terminal Android pour se connecter au réseau Wi-Fi.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini sur Entreprise.</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> <li>• Aucun</li> <li>• Certificat partagé</li> <li>• SCEP</li> <li>• Informations d'identification de l'utilisateur</li> </ul> <p>La valeur par défaut est Aucune.</p>
Type de liaison de certificat	<p>Ce paramètre spécifie le type de liaison du certificat client associé au profil Wi-Fi.</p> <p>Ce paramètre est valide uniquement si le paramètre Type d'authentification est défini sur Certificat partagé.</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> <li>• Référence unique</li> <li>• Injection de variable</li> </ul> <p>La valeur par défaut est Référence unique.</p>
Profil de certificat partagé	<p>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.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de liaison de certificat est défini sur Référence unique.</p> <p>Le nom du profil de certificat partagé doit contenir moins de 36 caractères pour les terminaux utilisant un Knox Workspace.</p>
Profil SCEP associé	<p>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.</p> <p>Ce paramètre est valide uniquement si le paramètre Type d'authentification est défini sur SCEP.</p> <p>Le nom du profil SCEP doit contenir moins de 36 caractères pour les terminaux utilisant un Knox Workspace.</p>

Android : paramètre de profil Wi-Fi	Description
Profil des informations d'identification de l'utilisateur associé	<p>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.</p> <p>Ce paramètre est valide uniquement si le paramètre Type d'authentification est défini sur Informations d'identification de l'utilisateur.</p> <p>Le nom du profil d'informations d'identification doit contenir moins de 36 caractères pour les terminaux utilisant un Knox Workspace.</p>
Nom du certificat client	<p>Ce paramètre spécifie le nom du certificat client utilisé par un terminal Android pour s'authentifier auprès du réseau Wi-Fi.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de liaison de certificat est défini sur Injection de variable.</p>
Noms usuels de certificat attendus par le serveur d'authentification	<p>Ce paramètre spécifie les noms usuels du certificat envoyés par le serveur d'authentification au terminal (par exemple, *.exemple.com).</p> <p>Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini sur Entreprise.</p>
Type de liaison de certificat	<p>Ce paramètre spécifie le type de liaison des certificats client associés au profil Wi-Fi.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini sur Entreprise.</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> <li>• Référence unique</li> <li>• Injection de variable</li> </ul> <p>La valeur par défaut est Référence unique.</p>
Profil du certificat d'autorité de certification	<p>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.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de liaison de certificat est défini sur Référence unique.</p>
Noms de certificats approuvés	<p>Ce paramètre spécifie les noms des certificats approuvés utilisés par un terminal Android pour établir une connexion approuvée au réseau Wi-Fi.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de liaison de certificat est défini sur Injection de variable.</p>

## 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	<p>Ce paramètre indique le type de sécurité utilisé par le réseau Wi-Fi.</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"><li>• Ouvert</li><li>• WPA-Enterprise</li><li>• WPA-Personal</li><li>• WPA2-Enterprise</li><li>• WPA2-Personal</li></ul> <p>La valeur par défaut est « Ouvert ».</p>
Type de cryptage	<p>Ce paramètre spécifie la méthode de cryptage utilisée par le réseau Wi-Fi.</p> <p>Le paramètre « Type de sécurité » détermine les types de cryptage pris en charge et la valeur par défaut de ce paramètre.</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"><li>• Aucun</li><li>• WEP</li><li>• TKIP</li><li>• AES</li></ul>
Clé WEP	<p>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).</p> <p>Exemples de valeurs de clés hexadécimales : ABCDEF0123 ou ABCDEF0123456789ABCDEF0123. Exemples de valeurs de clés alphanumériques : abCD5 ou abCDefGHijKL1.</p> <p>Ce paramètre est valide uniquement si le paramètre « Type de sécurité » est défini sur « Ouvert » et le paramètre « Type de cryptage » sur « WEP ».</p>
Index de clé	<p>Ce paramètre spécifie la position de la clé correspondante stockée sur le point d'accès sans fil.</p> <p>Ce paramètre est valide uniquement si le paramètre « Type de sécurité » est défini sur « Ouvert » et le paramètre « Type de cryptage » sur « WEP ».</p> <p>Les valeurs possibles sont comprises entre 1 et 4.</p> <p>La valeur par défaut est 2.</p>

Windows : paramètre de profil Wi-Fi	Description
Clé pré-partagée	<p>Ce paramètre spécifie la clé pré-partagée du réseau Wi-Fi.</p> <p>Ce paramètre est valide uniquement si le paramètre « Type de sécurité » est défini sur WPA-Personal.</p>
Activer l'identification unique	<p>Ce paramètre spécifie si le réseau Wi-Fi prend en charge l'authentification avec identification unique.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini WPA-Enterprise ou WPA2-Enterprise.</p>
Type d'identification unique	<p>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 l'instance Active Directory de votre organisation. 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 l'instance Active Directory de votre organisation.</p> <p>Ce paramètre est valide uniquement si le paramètre « Activer l'identification unique » est sélectionné.</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> <li>• Exécuter immédiatement avant la connexion d'utilisateur</li> <li>• Exécuter immédiatement après la connexion d'utilisateur</li> </ul> <p>La valeur par défaut est Exécuter immédiatement avant la connexion d'utilisateur.</p>
Délai de connectivité maximum	<p>Ce paramètre spécifie, en secondes, le délai maximum avant que la tentative de connexion avec identification unique échoue.</p> <p>Ce paramètre est valide uniquement si le paramètre « Activer l'identification unique » est sélectionné.</p> <p>Les valeurs possibles sont comprises entre 0 et 120 secondes.</p> <p>La valeur par défaut est de 10 secondes.</p>
Autoriser l'affichage de boîtes de dialogue supplémentaires lors de l'identification unique	<p>Ce paramètre indique si un terminal peut afficher des boîtes 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 boîte de dialogue.</p> <p>Ce paramètre est valide uniquement si le paramètre « Activer l'identification unique » est sélectionné.</p>
Ce réseau utilise des réseaux LAN virtuels pour l'authentification de l'ordinateur et de l'utilisateur	<p>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.</p> <p>Ce paramètre est valide uniquement si le paramètre « Activer l'identification unique » est sélectionné.</p>

Windows : paramètre de profil Wi-Fi	Description
Valider le certificat du serveur	<p>Ce paramètre spécifie si un terminal doit valider le certificat du serveur qui vérifie l'identité du point d'accès sans fil.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini WPA-Enterprise ou WPA2-Enterprise.</p>
Ne pas inviter l'utilisateur à autoriser de nouveaux serveurs ou des autorités de certification approuvées	<p>Ce paramètre spécifie si un utilisateur est invité à approuver le certificat du serveur.</p> <p>Ce paramètre est valide uniquement si le paramètre « Valider le certificat du serveur » est sélectionné.</p>
Profils de certificat d'autorité de certification	<p>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.</p> <p>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.</p> <p>Ce paramètre est valide uniquement si le paramètre « Valider le certificat du serveur » est sélectionné.</p>
Activer la reconnexion rapide	<p>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.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini WPA-Enterprise ou WPA2-Enterprise.</p>
Appliquer la protection NAP	<p>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.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de sécurité est défini WPA-Enterprise ou WPA2-Enterprise.</p>
Activer le mode FIPS	<p>Ce paramètre spécifie si le réseau Wi-Fi prend en charge la conformité avec la norme FIPS 140-2.</p> <p>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 ».</p>
Activer la mise en cache du PMK	<p>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.</p> <p>Ce paramètre est valide uniquement si le paramètre « Type de sécurité » est défini sur WPA2-Enterprise.</p>

Windows : paramètre de profil Wi-Fi	Description
Durée de vie du PMK	<p>Ce paramètre spécifie la durée, en minutes, pendant laquelle un terminal peut stocker le PMK dans le cache.</p> <p>Ce paramètre est valide uniquement si le paramètre « Activer la mise en cache du PMK » est sélectionné.</p> <p>Les valeurs possibles sont comprises entre 5 et 1 440 minutes.</p> <p>La valeur par défaut est 720 minutes.</p>
Nombre d'entrées du cache du PMK	<p>Ce paramètre spécifie le nombre maximum d'entrées du PMK qu'un terminal peut stocker dans le cache.</p> <p>Ce paramètre est valide uniquement si le paramètre « Activer la mise en cache du PMK » est sélectionné.</p> <p>Les valeurs possibles sont comprises entre 1 et 255.</p> <p>La valeur par défaut est 128.</p>
Ce réseau utilise la pré-authentification	<p>Ce paramètre spécifie si le point d'accès prend en charge la pré-authentification pour l'itinérance rapide WPA2.</p> <p>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.</p> <p>Ce paramètre est valide uniquement si le paramètre « Activer la mise en cache du PMK » est sélectionné.</p>
Tentatives de pré-authentification maximum	<p>Ce paramètre spécifie le nombre maximum de tentatives de pré-authentification autorisées.</p> <p>Ce paramètre est valide uniquement si le paramètre « Ce réseau utilise une pré-authentification » est sélectionné.</p> <p>Les valeurs possibles sont comprises entre 1 et 16.</p> <p>La valeur par défaut est 3.</p>
Type de proxy	<p>Ce paramètre spécifie le type de configuration proxy pour le profil Wi-Fi.</p> <p>Réglages possibles :</p> <ul style="list-style-type: none"> <li>• Aucun</li> <li>• Configuration PAC</li> <li>• Configuration manuelle</li> <li>• Web Proxy Autodiscovery</li> </ul> <p>La valeur par défaut est « Configuration manuelle ».</p> <p>Ce paramètre s'applique uniquement aux terminaux Windows 10 Mobile.</p>

Windows : paramètre de profil Wi-Fi	Description
URL du fichier PAC	<p>Ce paramètre spécifie l'URL du serveur Web qui héberge le fichier PAC et le nom du fichier PAC au format <code>http://&lt;web_server_URL&gt;/&lt;filename&gt;.pac</code>.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de proxy est défini sur Configuration PAC.</p>
Adresse	<p>Ce paramètre spécifie le nom du serveur et le port du proxy du réseau. Utilisez le format hôte:port (par exemple, <code>serveur01.example.com:123</code>). L'hôte doit être l'un des suivants :</p> <ul style="list-style-type: none"> <li>• un nom enregistré (ex. : nom de serveur), un nom de domaine complet ou un nom d'étiquette unique (par exemple, <code>serveur01</code> au lieu de <code>serveur01.exemple.com</code>)</li> <li>• une adresse IPv4 ou IPv6</li> </ul> <p>Ce paramètre est valide uniquement si le paramètre Type de proxy est défini sur Configuration manuelle.</p>
Web Proxy Autodiscovery	<p>Ce paramètre permet d'activer le Web Proxy Autodiscovery Protocol (WPAD) pour la recherche de proxy.</p> <p>Ce paramètre est valide uniquement si le paramètre « Type de proxy » est défini sur « Web Proxy Autodiscovery ».</p> <p>Par défaut, cette case n'est pas cochée.</p>
Désactiver les vérifications de la connectivité Internet	<p>Ce paramètre permet de désactiver les vérifications de la connectivité Internet.</p> <p>Par défaut, cette case n'est pas cochée.</p>
Profil SCEP associé	<p>Ce paramètre spécifie le profil SCEP associé utilisé par un terminal pour obtenir un certificat client et s'authentifier auprès du réseau Wi-Fi.</p>



# 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	<p>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.</p> <p>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.</p>
macOS	<p>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.</p>
Samsung Knox	<p>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.</p> <p>Vous pouvez activer un VPN par application afin de limiter ce dernier aux applications professionnelles que vous spécifiez.</p> <p>Une application client VPN prise en charge doit être installée sur le terminal. Cisco AnyConnect et Juniper sont pris en charge.</p> <p><b>Remarque :</b> L'application Juniper prend uniquement en charge SSL VPN.</p>
Windows 10	<p>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.</p>

## 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.

**Remarque :** certains terminaux peuvent ne pas être en mesure de stocker le mot de passe xAuth. Pour plus d'informations, rendez-vous sur le site [support.blackberry.com/community](http://support.blackberry.com/community) pour consulter l'article 30353.

#### 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 des certificats client aux terminaux, créez des informations d'identification de l'utilisateur, un SCEP ou un profil de certificat partagé 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. (Le serveur proxy pour les terminaux Windows 10 est configuré dans le 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. 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 VPN dans l'environnement de votre organisation. Si votre organisation requiert que les utilisateurs fournissent un nom d'utilisateur et un mot de passe pour se connecter au réseau VPN et que le profil correspond à plusieurs utilisateurs, dans le champ **Nom d'utilisateur**, saisissez %UserName%.
6. Répétez l'étape 5 pour chaque type de terminal de votre organisation.
7. Cliquez sur **Ajouter**.

## Paramètres du profil VPN

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. Les [profils VPN](#) sont pris en charge sur les types de terminaux suivants :

- iOS
- iPadOS
- macOS
- Samsung Knox
- Windows 10

### iOS et macOS : Paramètres du profil VPN

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

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

iOS et macOS : Paramètre du profil VPN	Description
Appliquer le profil à	<p>Ce paramètre indique si le profil VPN sur un terminal macOS est appliqué au compte d'utilisateur ou au terminal.</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> <li>• Utilisateur</li> <li>• Terminal</li> </ul> <p>Ce paramètre est valide uniquement pour les terminaux macOS.</p>
Type de connexion	<p>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.</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> <li>• L2TP</li> <li>• PPTP</li> <li>• IPsec</li> <li>• Cisco AnyConnect</li> <li>• Juniper</li> <li>• Pulse Secure</li> <li>• F5</li> <li>• SonicWALL Mobile Connect</li> <li>• Aruba VIA</li> <li>• Check Point Mobile</li> <li>• OpenVPN</li> <li>• Personnalisée</li> <li>• IKEv2</li> <li>• IKEv2 Always On</li> </ul> <p>La valeur par défaut est L2TP.</p> <p>Si vous sélectionnez IKEv2 Always On, de nombreux paramètres ont des valeurs distinctes pour les connexions cellulaires et Wi-Fi.</p> <p>Certaines valeurs ne sont pas valides pour les terminaux macOS.</p>
ID d'offre VPN	<p>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).</p> <p>Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur Personnalisée.</p>
Serveur	<p>Ce paramètre spécifie le FQDN ou l'adresse IP d'un serveur VPN.</p>
nom d'utilisateur ;	<p>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%.</p>

iOS et macOS : Paramètre du profil VPN	Description
Valeurs et clés personnalisées	<p>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.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur Personnalisée.</p>
Groupe de connexion ou domaine	<p>Ce paramètre spécifie le groupe de connexion ou le domaine utilisé par la passerelle VPN pour authentifier un terminal.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur SonicWALL Mobile Connect.</p>
Domaine	<p>Ce paramètre spécifie le nom de domaine d'authentification utilisé par la passerelle VPN pour authentifier un terminal.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur Juniper ou Pulse Secure.</p>
Rôle	<p>Ce paramètre spécifie le nom du rôle d'utilisateur utilisé par la passerelle VPN pour vérifier les ressources réseau auxquelles un terminal peut accéder.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur Juniper ou Pulse Secure.</p>
Type d'authentification	<p>Ce paramètre spécifie le type d'authentification de la passerelle VPN.</p> <p>Le paramètre Type de connexion détermine les types d'authentification pris en charge et la valeur par défaut de ce paramètre.</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> <li>• Mot de passe</li> <li>• RSA SecurID</li> <li>• Secret partagé</li> <li>• Secret partagé/Nom de groupe</li> <li>• Certificat partagé</li> <li>• SCEP</li> <li>• Informations d'identification de l'utilisateur</li> </ul>
Plug-ins EAP	<p>Ce paramètre spécifie les plug-ins d'authentification du VPN.</p> <p>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.</p>
Protocole d'authentification	<p>Ce paramètre spécifie les protocoles d'authentification du VPN.</p> <p>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.</p>

iOS et macOS : Paramètre du profil VPN	Description
Mot de passe	<p>Ce paramètre spécifie le mot de passe utilisé par un terminal pour s'authentifier auprès de la passerelle VPN.</p> <p>Ce paramètre est valide uniquement si le paramètre Type d'authentification est défini sur Mot de passe.</p>
Nom de groupe	<p>Ce paramètre spécifie le nom de groupe pour la passerelle VPN.</p> <p>Ce paramètre est valide uniquement dans les conditions suivantes :</p> <ul style="list-style-type: none"> <li>• Le paramètre Type de connexion est défini sur Cisco AnyConnect.</li> <li>• Le paramètre Type de connexion est défini sur IPsec et le paramètre Type d'authentification est défini sur Secret partagé/Nom de groupe.</li> </ul>
Secret partagé	<p>Ce paramètre spécifie le secret partagé à utiliser pour l'authentification VPN.</p> <p>Ce paramètre est valide uniquement dans les conditions suivantes :</p> <ul style="list-style-type: none"> <li>• Le paramètre Type de connexion est défini sur L2TP.</li> <li>• Le paramètre Type de connexion est défini sur IPsec et le paramètre Type d'authentification est défini sur Secret partagé/Nom de groupe.</li> <li>• Le paramètre Type de connexion est défini sur IKEv2 ou IKEv2 Always On et le paramètre Type d'authentification est défini sur Secret partagé.</li> </ul>
Profil de certificat partagé	<p>Ce paramètre spécifie le profil de certificat partagé avec le certificat client utilisé par un terminal pour s'authentifier auprès de la passerelle VPN.</p> <p>Ce paramètre est valide uniquement si le paramètre Type d'authentification est défini sur Certificat partagé.</p>
Profil SCEP associé	<p>Ce paramètre spécifie le profil SCEP associé utilisé par un terminal pour obtenir un certificat client et s'authentifier auprès du VPN.</p> <p>Ce paramètre est valide uniquement si le paramètre Type d'authentification est défini sur SCEP.</p>
Profil des informations d'identification de l'utilisateur associé	<p>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.</p> <p>Ce paramètre est valide uniquement si le paramètre Type d'authentification est défini sur Informations d'identification de l'utilisateur.</p>

iOS et macOS : Paramètre du profil VPN	Description
Niveau de cryptage	<p>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.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur PPTP.</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> <li>• Aucun</li> <li>• Automatique</li> <li>• Maximum</li> </ul> <p>La valeur par défaut est Aucune.</p>
Acheminer le trafic réseau via VPN	<p>Ce paramètre spécifie si vous souhaitez acheminer le trafic réseau via une connexion VPN.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur L2TP ou PPTP.</p>
Utiliser une authentification hybride	<p>Ce paramètre spécifie si vous souhaitez utiliser un certificat côté serveur pour l'authentification.</p> <p>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.</p>
Demander un mot de passe	<p>Ce paramètre spécifie si un terminal invite l'utilisateur à saisir un mot de passe.</p> <p>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.</p>
Demander un code PIN à l'utilisateur	<p>Ce paramètre spécifie si le terminal invite l'utilisateur à saisir un code PIN.</p> <p>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.</p>
Adresse distante	<p>Ce paramètre spécifie l'adresse IP ou le nom d'hôte du serveur VPN.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur IKEv2 ou IKEv2 Always On.</p>
ID local	<p>Ce paramètre spécifie l'identité du client IKEv2 dans l'un des formats suivants : FQDN, UserFQDN, Adresse et ASN1DN.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur IKEv2 ou IKEv2 Always On.</p>

iOS et macOS : Paramètre du profil VPN	Description
ID distant	<p>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.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur IKEv2 ou IKEv2 Always On.</p>
Activer VPN à la demande	<p>Ce paramètre spécifie si un terminal peut automatiquement établir une connexion VPN lorsqu'il accède à certains domaines.</p> <p>Pour les terminaux iOS et iPadOS, ce paramètre s'applique aux applications professionnelles.</p> <p>Ce paramètre est valide uniquement dans les conditions suivantes :</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• Le paramètre Type de connexion est défini sur IKEv2 et le paramètre Type d'authentification est défini sur Certificat partagé.</li> </ul>
Domaine ou noms d'hôte pouvant utiliser un VPN à la demande	<p>Ce paramètre spécifie les domaines et actions associées pour utiliser un VPN à la demande.</p> <p>Ce paramètre est valide uniquement si le paramètre Activer VPN à la demande est sélectionné.</p> <p>Valeurs possibles pour Action à la demande :</p> <ul style="list-style-type: none"> <li>• Toujours établir</li> <li>• Établir si nécessaire</li> <li>• Ne jamais établir</li> </ul>
Règles de VPN à la demande pour iOS 7.0 ou version ultérieure	<p>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.</p> <p>Ce paramètre remplace le paramètre Domaine ou noms d'hôte pouvant utiliser un VPN à la demande.</p> <p>Ce paramètre est valide uniquement si le paramètre Activer VPN à la demande est sélectionné.</p>
Déconnecter en mode veille	<p>Ce paramètre spécifie si la connexion VPN se déconnecte lorsqu'elle est en veille pendant une période donnée.</p> <p>Ce paramètre est valide uniquement si le paramètre Activer VPN à la demande est sélectionné.</p>

iOS et macOS : Paramètre du profil VPN	Description
Déconnecter en mode veille - Délai	<p>Ce paramètre spécifie le délai d'inactivité en secondes après lequel le VPN se déconnecte.</p> <p>La valeur par défaut est « 120 »</p> <p>Ce paramètre est valide uniquement si le paramètre Déconnecter en mode veille est sélectionné.</p>
Ne pas autoriser l'utilisateur à désactiver le VPN à la demande	<p>Ce paramètre spécifie si l'utilisateur peut désactiver le VPN à la demande.</p> <p>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.</p> <p>Ce paramètre s'applique uniquement aux terminaux exécutant iOS et iPadOS 14 et version ultérieure.</p>
Exclure le réseau local	<p>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. Ce paramètre s'applique uniquement aux terminaux exécutant iOS et iPadOS 13 et version ultérieure.</p>
Tous les routages autres que ceux par défaut sont prioritaires sur les routages définis localement	<p>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.</p> <p>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.</p> <p>Ce paramètre s'applique uniquement aux terminaux exécutant iOS et iPadOS 14.2 et version ultérieure.</p>
Inclure tous les réseaux	<p>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.</p>
Fournisseur désigné requis	<p>Ce paramètre spécifie un fournisseur VPN désigné. Si le fournisseur VPN est mis en œuvre en tant qu'extension système, ce paramètre est requis.</p> <p>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.</p>
Autoriser l'utilisateur à désactiver la connexion automatique	<p>Ce paramètre spécifie si les utilisateurs peuvent désactiver la connexion VPN.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur IKEv2 Always On.</p>



iOS et macOS : Paramètre du profil VPN	Description
Utiliser la même configuration de tunnel pour les réseaux cellulaires et Wi-Fi	<p>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.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur IKEv2 Always On.</p>
Activer xAuth	<p>Ce paramètre spécifie si le VPN prend en charge l'authentification étendue.</p> <p>Ce paramètre est valide uniquement si le paramètre « Type de connexion » est défini sur « IKEv2 » ou « IKEv2 Always On ».</p>
Version TLS minimale	<p>Ce paramètre spécifie la version TLS minimale utilisée par les terminaux pour l'authentification EAP-TLS.</p> <p>Ce paramètre est valide uniquement si le paramètre Activer xAuth est sélectionné et que le type d'authentification est défini sur Certificat.</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> <li>• 1.0</li> <li>• 1.1</li> <li>• 1.2</li> </ul> <p>Le paramètre par défaut est « 1.0 ».</p>
Version TLS maximale	<p>Ce paramètre spécifie la version TLS maximale utilisée par les terminaux pour l'authentification EAP-TLS.</p> <p>Ce paramètre est valide uniquement si le paramètre Activer xAuth est sélectionné et que le type d'authentification est défini sur Certificat.</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> <li>• 1.0</li> <li>• 1.1</li> <li>• 1.2</li> </ul> <p>Le paramètre par défaut est « 1.2 ».</p>
Type de certificat	<p>Ce paramètre spécifie le type de certificat utilisé pour l'authentification de la machine IKEv2.</p> <p>Ce paramètre est valide uniquement si le paramètre Activer xAuth est sélectionné et que le type d'authentification est défini sur Certificat.</p>
Nom commun de l'émetteur du certificat de serveur	<p>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.</p> <p>Ce paramètre est valide uniquement si le paramètre Activer xAuth est sélectionné et que le type d'authentification est défini sur Certificat.</p>

iOS et macOS : Paramètre du profil VPN	Description
Nom commun du certificat de serveur	<p>Ce paramètre spécifie le nom usuel du certificat de serveur que le serveur IKE envoie au terminal.</p> <p>Ce paramètre est valide uniquement si le paramètre Activer xAuth est sélectionné et que le type d'authentification est défini sur Certificat.</p>
Intervalle keepalive	<p>Ce paramètre spécifie la fréquence à laquelle un terminal envoie un paquet keepalive.</p> <p>Ce paramètre est valide uniquement si le paramètre « Type de connexion » est défini sur « IKEv2 » ou « IKEv2 Always On ».</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> <li>• Désactivé</li> <li>• 30 minutes</li> <li>• 10 minutes</li> <li>• 1 minute</li> </ul> <p>Le paramètre par défaut est 10 minutes.</p>
Désactiver MOBIKE	<p>Ce paramètre indique si le MOBIKE est désactivé.</p> <p>Ce paramètre est valide uniquement si le paramètre « Type de connexion » est défini sur « IKEv2 » ou « IKEv2 Always On ».</p>
Désactiver la redirection IKEv2	<p>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.</p> <p>Ce paramètre est valide uniquement si le paramètre « Type de connexion » est défini sur « IKEv2 » ou « IKEv2 Always On ».</p>
Activer Perfect Forward Secrecy (confidentialité totale des transferts)	<p>Ce paramètre spécifie si la passerelle VPN prend en charge le PFS.</p> <p>Ce paramètre est valide uniquement si le paramètre « Type de connexion » est défini sur « IKEv2 » ou « IKEv2 Always On ».</p>
Activer NAT keepalive	<p>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.</p> <p>Ce paramètre est valide uniquement si le paramètre « Type de connexion » est défini sur « IKEv2 » ou « IKEv2 Always On ».</p>
Intervalle NAT keepalive	<p>Ce paramètre spécifie la fréquence à laquelle un terminal envoie un paquet NAT keepalive (en secondes).</p> <p>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.</p> <p>La valeur minimale, également valeur par défaut, est de 20.</p>

iOS et macOS : Paramètre du profil VPN	Description
Utiliser les sous-réseaux internes IPv4 et IPv6 IKEv2	<p>Ce paramètre indique si le VPN peut utiliser l'attribut de configuration IKEv2 INTERNAL_IP4_SUBNET et INTERNAL_IP6_SUBNET.</p> <p>Ce paramètre est valide uniquement si le paramètre « Type de connexion » est défini sur « IKEv2 » ou « IKEv2 Always On ».</p>
Nom commun du certificat de serveur	<p>Ce paramètre spécifie le nom usuel du certificat envoyé par le serveur IKE au terminal.</p> <p>Ce paramètre est valide uniquement si le paramètre « Type de connexion » est défini sur « IKEv2 » ou « IKEv2 Always On ».</p>
Nom commun de l'émetteur du certificat de serveur	<p>Ce paramètre spécifie le nom usuel de l'émetteur du certificat dans le certificat envoyé par le serveur IKE au terminal.</p> <p>Ce paramètre est valide uniquement si le paramètre « Type de connexion » est défini sur « IKEv2 » ou « IKEv2 Always On ».</p>
Activer la vérification de révocation de certificat	<p>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.</p> <p>Ce paramètre est valide uniquement si le paramètre « Type de connexion » est défini sur « IKEv2 » ou « IKEv2 Always On ».</p>
Activer la fonction de secours	<p>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.</p> <p>Ce paramètre est valide uniquement si le paramètre « Type de connexion » est défini sur « IKEv2 » ou « IKEv2 Always On ».</p>
Appliquer les paramètres d'association de sécurité enfant	<p>Ce paramètre spécifie s'il faut appliquer les paramètres d'association de sécurité enfant.</p> <p>Ce paramètre est valide uniquement si le paramètre « Type de connexion » est défini sur « IKEv2 » ou « IKEv2 Always On ».</p>
Appliquer les paramètres d'association de sécurité IKE	<p>Ce paramètre spécifie s'il faut appliquer les paramètres d'association de sécurité IKE.</p> <p>Ce paramètre est valide uniquement si le paramètre « Type de connexion » est défini sur « IKEv2 » ou « IKEv2 Always On ».</p>
MTU	<p>Ce paramètre spécifie l'unité de transmission maximale en octets. Ce paramètre s'applique uniquement aux terminaux exécutant iOS et iPadOS 14 et version ultérieure.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de connexion est défini sur IKEv2 Always On.</p>

iOS et macOS : Paramètre du profil VPN	Description
Messagerie vocale	<p>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 s'applique uniquement aux terminaux exécutant iOS et iPadOS 13.4 et version ultérieure.</p> <p>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.</p>
AirPrint	<p>Ce paramètre spécifie si les connexions AirPrint AirPrint sont envoyées via le tunnel VPN, envoyées en dehors du tunnel VPN ou bloquées. Ce paramètre s'applique uniquement aux terminaux exécutant iOS et iPadOS 13.4 et version ultérieure.</p> <p>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.</p>
Autoriser le trafic d'une page Web captive en dehors du tunnel VPN	<p>Ce paramètre spécifie si le trafic des feuilles Web captives peut être envoyé en dehors du tunnel VPN.</p> <p>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.</p>
Autoriser le trafic des applications de réseaux sociaux captives en dehors du tunnel VPN	<p>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.</p> <p>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.</p>
Le trafic provenant de ces applications est autorisé en dehors du tunnel VPN	<p>Ce paramètre spécifie les applications de réseaux sociaux captives individuelles pour lesquelles le trafic peut être envoyé en dehors du tunnel.</p> <p>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.</p>
Autoriser le trafic des applications en dehors du tunnel VPN	<p>Ce paramètre spécifie les applications dont le trafic peut être envoyé en dehors du tunnel.</p> <p>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.</p>

iOS et macOS : Paramètre du profil VPN	Description
Groupe DH	<p>Ce paramètre spécifie le groupe DH utilisé par un terminal pour générer les clés.</p> <p>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.</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> <li>• 0</li> <li>• 1</li> <li>• 2</li> <li>• 5</li> <li>• 14</li> <li>• 15</li> <li>• 16</li> <li>• 17</li> <li>• 18</li> <li>• 19</li> <li>• 20</li> <li>• 21</li> <li>• 31</li> </ul> <p>Le paramètre par défaut est 2.</p>
Algorithme de cryptage	<p>Ce paramètre spécifie l'algorithme de cryptage IKE.</p> <p>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.</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> <li>• DES</li> <li>• 3DES</li> <li>• AES 128</li> <li>• AES 256</li> <li>• AES 128 GCM</li> <li>• AES 256 GCM</li> <li>• ChaCha20Poly1305</li> </ul> <p>Le paramètre par défaut est 3DES.</p>

iOS et macOS : Paramètre du profil VPN	Description
Algorithme d'intégrité	<p>Ce paramètre spécifie l'algorithme d'intégrité IKE.</p> <p>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.</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> <li>• SHA1 96</li> <li>• SHA1 160</li> <li>• SHA1 256</li> <li>• SHA2 384</li> <li>• SHA2 512</li> </ul> <p>La valeur par défaut est SHA1-96.</p>
Intervalle de renouvellement de clés	<p>Ce paramètre spécifie la durée de vie de la connexion IKE.</p> <p>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.</p> <p>Les valeurs possibles sont comprises entre 10 et 1 440 minutes.</p> <p>La valeur par défaut est 1 440.</p>
Activer un VPN par application	<p>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.</p> <p>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.</p>
Autoriser la connexion automatique des applications	<p>Ce paramètre spécifie si les applications associées au VPN par application peuvent établir automatiquement la connexion VPN.</p> <p>Ce paramètre est valide uniquement si le paramètre Activer VPN par application est sélectionné.</p>
Domaines Safari	<p>Ce paramètre spécifie les domaines pouvant établir la connexion VPN dans Safari.</p> <p>Ce paramètre est valide uniquement si le paramètre Activer VPN par application est sélectionné.</p>

iOS et macOS : Paramètre du profil VPN	Description
Domaines Calendrier	<p>Ce paramètre spécifie les domaines pouvant établir la connexion VPN dans Calendrier.</p> <p>Ce paramètre est valide uniquement si le paramètre Activer VPN par application est sélectionné. Ce paramètre s'applique uniquement aux terminaux iOS et iPadOS 13.0 et versions ultérieures.</p>
Domaines Contacts	<p>Ce paramètre spécifie les domaines pouvant établir la connexion VPN dans Contacts.</p> <p>Ce paramètre est valide uniquement si le paramètre Activer VPN par application est sélectionné. Ce paramètre s'applique uniquement aux terminaux iOS et iPadOS 13.0 et versions ultérieures.</p>
Domaines Messagerie	<p>Ce paramètre spécifie les domaines pouvant établir la connexion VPN dans Messagerie.</p> <p>Ce paramètre est valide uniquement si le paramètre Activer VPN par application est sélectionné. Ce paramètre s'applique uniquement aux terminaux iOS et iPadOS 13.0 et versions ultérieures.</p>
Domaines associés	<p>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.</p> <p>Ce paramètre est valide uniquement si le paramètre Activer VPN par application est sélectionné. Ce paramètre s'applique uniquement aux terminaux iOS et iPadOS 14.0 et versions ultérieures.</p>
Domaines exclus	<p>Ce paramètre spécifie les domaines ne pouvant pas établir de connexion VPN sur le terminal.</p> <p>Ce paramètre est valide uniquement si le paramètre Activer VPN par application est sélectionné. Ce paramètre s'applique uniquement aux terminaux iOS et iPadOS 14.0 et versions ultérieures.</p>
Tunnellisation du trafic	<p>Ce paramètre indique si le VPN achemine le trafic vers la couche d'application ou la couche IP.</p> <p>Ce paramètre est valide uniquement si le paramètre Activer VPN par application est sélectionné. Ce paramètre s'applique uniquement aux terminaux iOS et iPadOS 13.0 et versions ultérieures.</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> <li>• Couche d'application</li> <li>• Couche IP</li> </ul> <p>La valeur par défaut est Couche d'application.</p>
Profil proxy associé	<p>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.</p>

## Android : paramètres de profil VPN

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

Pour plus d'informations sur les paramètres de profil VPN pris en charge par les terminaux Samsung Knox Workspace, reportez-vous à la section [Samsung KnoxParamètres JSON d'un VPN](#).

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.  Valeurs possibles : <ul style="list-style-type: none"><li>• IPsec</li><li>• SSL</li></ul> La valeur par défaut est IPsec.  L'application Juniper VPN prend uniquement en charge 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 tunnellation fractionnée	Ce paramètre spécifie si un terminal peut utiliser la tunnellation fractionnée pour contourner la passerelle VPN (sous réserve de prise en charge par la passerelle VPN).  Valeurs possibles : <ul style="list-style-type: none"><li>• Désactivé</li><li>• Manuel</li><li>• Auto</li></ul> Si le paramètre Type de VPN est défini sur IPsec, ce paramètre doit être défini sur Désactivé.  La valeur par défaut est Désactivé.



Android : paramètre de profil VPN	Description
Itinéraires de transfert	<p>Ce paramètre spécifie le(s) cheminement(s) contournant la passerelle VPN. Vous pouvez spécifier une ou plusieurs adresses IP.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de VPN est défini sur SSL et le paramètre Type de tunnellation fractionnée sur Manuel.</p>
DPD	<p>Ce paramètre indique si le protocole DPD est activé.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de VPN est défini sur IPsec.</p>
Version IKE	<p>Ce paramètre spécifie la version du protocole IKE à utiliser avec la connexion VPN.</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> <li>• IKEv1</li> <li>• IKEv2</li> </ul> <p>La valeur par défaut est IKEv1.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de VPN est défini sur IPsec.</p>
Type d'authentification IPsec	<p>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.</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> <li>• Certificat</li> <li>• Clé pré-partagée</li> <li>• EAP MD5</li> <li>• EAP MSCHAPv2</li> <li>• Hybride RSA</li> <li>• Authentification CAC</li> </ul> <p>Ce paramètre est valide uniquement si le paramètre Type de VPN est défini sur IPsec.</p>

Android : paramètre de profil VPN	Description
Type d'ID de groupe IPsec	<p>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.</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> <li>• Par défaut</li> <li>• Adresse IPv4</li> <li>• Nom de domaine complet</li> <li>• FQDN de l'utilisateur</li> <li>• ID de clé IKE</li> </ul> <p>Si le paramètre Type d'authentification IPsec correspond à Certificat, ce paramètre est automatiquement défini sur Par défaut.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de VPN est défini sur IPsec.</p>
ID de groupe IPsec	<p>Ce paramètre spécifie l'ID de groupe IPsec de la connexion VPN.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de VPN est défini sur IPsec.</p>
Mode d'échange de clé de la phase 1 IKE	<p>Ce paramètre spécifie le mode d'échange de la connexion VPN.</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> <li>• Mode principal</li> <li>• Mode agressif</li> </ul> <p>La valeur par défaut est Mode principal.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de VPN est défini sur IPsec.</p>
Durée de vie IKE	<p>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.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de VPN est défini sur IPsec.</p>
Algorithme de cryptage IKE	<p>Ce paramètre spécifie l'algorithme de cryptage utilisé pour la connexion IKE.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de VPN est défini sur IPsec.</p>
Algorithme d'intégrité IKE	<p>Ce paramètre indique l'algorithme d'intégrité utilisé pour la connexion IKE.</p> <p>Ce paramètre est valide uniquement si le paramètre « Type de VPN » est défini sur « IPsec » et le paramètre « Version IKE » sur « IKEv2 ».</p>

Android : paramètre de profil VPN	Description
Groupe DH IPsec	<p>Ce paramètre spécifie le groupe DH utilisé par un terminal pour générer les clés. Les valeurs possibles sont 0, 1, 2, 5 et comprises entre 14 et 26.</p> <p>La valeur par défaut est 0.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de VPN est défini sur IPsec.</p>
Paramètre IPsec	<p>Ce réglage définit le paramètre IPsec utilisé pour la connexion VPN.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de VPN est défini sur IPsec.</p>
Perfect Forward Secrecy (confidentialité totale des transferts)	<p>Ce paramètre spécifie si la passerelle VPN prend en charge PFS.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de VPN est défini sur IPsec.</p>
Activer MOBIKE	<p>Ce paramètre spécifie si la passerelle VPN prend en charge MOBIKE.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de VPN est défini sur IPsec.</p>
Durée de vie IPsec	<p>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.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de VPN est défini sur IPsec.</p>
Algorithme de cryptage IPsec	<p>Ce paramètre spécifie l'algorithme de cryptage IPsec utilisé pour la connexion VPN.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de VPN est défini sur IPsec.</p>
Algorithme d'intégrité IPsec	<p>Ce paramètre indique l'algorithme d'intégrité IPsec utilisé pour la connexion VPN.</p> <p>Ce paramètre est valide uniquement si le paramètre « Type de VPN » est défini sur « IPsec » et le paramètre « Version IKE » sur « IKEv2 ».</p>
Type d'authentification	<p>Ce paramètre spécifie le type d'authentification de la passerelle VPN.</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> <li>• Aucun</li> <li>• Authentification basée sur certificat</li> <li>• Authentification CAC</li> </ul> <p>La valeur par défaut est Aucune.</p> <p>Ce paramètre est valide uniquement si le paramètre « Type de VPN » est défini sur « SSL ».</p>

Android : paramètre de profil VPN	Description
Algorithme SSL	<p>Ce paramètre spécifie l'algorithme de cryptage requis pour une connexion VPN SSL.</p> <p>Ce paramètre est valide uniquement si le paramètre « Type de VPN » est défini sur « SSL ».</p>
Ajouter des informations UID/PID	<p>Ce paramètre spécifie si les informations UID et PID sont ajoutées aux paquets envoyés au client VPN.</p> <p>Ce paramètre doit être sélectionné pour l'application VPN Cisco AnyConnect.</p>
Chainage de prise en charge	<p>Ce paramètre spécifie comment le chainage VPN est pris en charge.</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> <li>• Chainage de prise en charge</li> <li>• Tunnel extérieur</li> <li>• Tunnel intérieur</li> </ul> <p>La valeur par défaut est « Chainage de prise en charge ».</p>
Type de saisie de la chaîne fournisseur	<p>Ce paramètre spécifie les paires clé-valeur ou la chaîne JSON du VPN. Les informations de configuration sont spécifiques à l'application VPN du fournisseur.</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> <li>• Paires clé-valeur du fournisseur</li> <li>• Valeur JSON du fournisseur</li> </ul> <p>La valeur par défaut est Paires valeur-clé du fournisseur.</p>
Paires clé-valeur du fournisseur	<p>Ce paramètre spécifie les clés et les valeurs associées du VPN. Les informations de configuration sont spécifiques à l'application VPN du fournisseur.</p> <p>Ce paramètre est uniquement valide si le paramètre Type de saisie de la chaîne fournisseur est défini sur Paires valeur-clé du fournisseur.</p>
Valeur JSON du fournisseur	<p>Ce paramètre spécifie les informations de configuration propres à l'application VPN du fournisseur au format .json.</p> <p>Ce paramètre est uniquement valide si le paramètre Type de saisie de la chaîne fournisseur est défini sur Valeur JSON du fournisseur.</p>
ID du logiciel client VPN	<p>Ce paramètre spécifie l'ID de package de l'application VPN.</p>
Essayer automatiquement de se reconnecter après une erreur	<p>Ce paramètre spécifie si la connexion VPN doit être automatiquement redémarrée après que la connexion ait été perdue.</p>
Activer le mode FIPS	<p>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.</p>

Android : paramètre de profil VPN	Description
Connectivité d'entreprise pour les terminaux Android comprenant un espace Travail	<p>Ce paramètre indique si les terminaux Samsung Knox Workspace utilisent une connexion VPN pour toutes les applications dans l'espace Travail ou seulement pour les applications spécifiées.</p> <ul style="list-style-type: none"> <li>• « VPN à l'échelle du conteneur » utilise une connexion VPN pour toutes les applications dans l'espace Travail sur le terminal.</li> <li>• « VPN par application » utilise une connexion VPN uniquement pour les applications spécifiées.</li> </ul>
Applications autorisées à utiliser la connexion VPN	<p>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.</p> <p>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.</p>
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 du profil VPN

Windows : Paramètre du profil VPN	Description
Type de connexion	<p>Ce paramètre spécifie le type de connexion utilisé par un terminal Windows 10 pour un VPN.</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> <li>• Microsoft</li> <li>• Junos Pulse</li> <li>• SonicWALL Mobile Connect</li> <li>• F5</li> <li>• Check Point Mobile</li> <li>• Définition de la connexion manuelle</li> </ul> <p>La valeur par défaut est Microsoft.</p>
Serveur	<p>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.</p> <p>Ce paramètre est valide uniquement si le Type de connexion est défini sur Microsoft.</p>
Liste d'URL de serveur	<p>Ce paramètre spécifie une liste séparée par des virgules des serveurs au format URL, nom d'hôte ou format IP.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de connexion n'est pas défini sur Microsoft.</p>

Windows : Paramètre du profil VPN	Description
Type de stratégie de routage	<p>Ce paramètre spécifie le type de stratégie de routage.</p> <p>Ce paramètre est valide uniquement si le Type de connexion est défini sur Microsoft.</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> <li>• Tunnel fractionné</li> <li>• Appliquer le tunnel</li> </ul> <p>La valeur par défaut est Forcer le tunnel.</p>
Type de protocole natif	<p>Ce paramètre spécifie le type de stratégie de routage utilisé par le VPN.</p> <p>Ce paramètre est valide uniquement si le Type de connexion est défini sur Microsoft.</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> <li>• L2TP</li> <li>• PPTP</li> <li>• IKEv2</li> <li>• Automatique</li> </ul> <p>La valeur par défaut est Automatique.</p>
Authentification	<p>Ce paramètre indique la méthode d'authentification utilisée pour le VPN natif.</p> <p>Le paramètre Type de protocole natif détermine les méthodes d'authentification prises en charge et la valeur par défaut de ce paramètre.</p> <ul style="list-style-type: none"> <li>• Si vous sélectionnez L2TP ou PPTP, les valeurs possibles sont MS-CHAPv2 et EAP. La valeur par défaut est MS-CHAPv2.</li> <li>• Si vous sélectionnez IKEv2, les valeurs possibles sont Méthode utilisateur et Méthode machine. La valeur par défaut est Méthode utilisateur.</li> <li>• Si vous sélectionnez Automatique, la seule valeur possible est EAP.</li> </ul> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> <li>• EAP</li> <li>• MS-CHAPv2</li> <li>• Méthode utilisateur</li> <li>• Méthode machine</li> </ul>
Configuration EAP	<p>Ce paramètre spécifie le code XML de la configuration EAP.</p> <p>Pour plus d'informations sur la génération du code XML de la configuration EAP, rendez-vous sur <a href="https://docs.microsoft.com/en-us/windows/client-management/mdm/eap-configuration">https://docs.microsoft.com/en-us/windows/client-management/mdm/eap-configuration</a></p> <p>Ce paramètre est valide uniquement si le paramètre Authentification est défini sur EAP.</p>

Windows : Paramètre du profil VPN	Description
Méthode utilisateur	<p>Ce paramètre indique le type d'authentification de méthode utilisateur à utiliser.</p> <p>Ce paramètre est valide uniquement si le paramètre Authentification est défini sur Méthode utilisateur.</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> <li>• EAP</li> </ul>
Méthode machine	<p>Ce paramètre indique le type d'authentification de méthode machine à utiliser.</p> <p>Ce paramètre est valide uniquement si le paramètre Authentification est défini sur Méthode machine.</p> <p>Valeur possible :</p> <ul style="list-style-type: none"> <li>• Certificat</li> </ul>
Configuration personnalisée	<p>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.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de connexion n'est pas défini sur Microsoft.</p>
Nom de la famille de package de plug-ins	<p>Ce paramètre spécifie le nom de famille de package du VPN SSL personnalisé.</p> <p>Ce paramètre est valide uniquement si le Type de connexion est défini sur Définition de la connexion manuelle.</p>
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	<p>Ce paramètre identifie une application pour un VPN par application.</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> <li>• Nom de la famille de package. Pour trouver le nom de la famille de package, installez l'application et exécutez la commande Windows PowerShell, <code>Get-AppxPackage</code>. Pour plus d'informations, rendez-vous sur <a href="http://technet.microsoft.com/en-us/library/hh856044.aspx">http://technet.microsoft.com/en-us/library/hh856044.aspx</a></li> <li>• Emplacement d'installation de l'application. Par exemple, C:\Windows\System\notepad.exe.</li> </ul>
Liste des itinéraires	Ce paramètre spécifie une liste des itinéraires que le VPN peut emprunter. Si le VPN utilise la tunnellation 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.

Windows : Paramètre du profil VPN	Description
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.
Liste des filtres de trafic > ID d'application	<p>Ce paramètre identifie une application pour un filtre de trafic basé sur l'application.</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> <li>• Nom de la famille de package. Pour trouver le nom de la famille de package, installez l'application et exécutez la commande Windows PowerShell, <code>Get-AppxPackage</code>. Pour plus d'informations, rendez-vous sur <a href="http://technet.microsoft.com/en-us/library/hh856044.aspx">http://technet.microsoft.com/en-us/library/hh856044.aspx</a></li> <li>• Emplacement d'installation de l'application. Par exemple, <code>C:\Windows\System\notepad.exe</code>.</li> <li>• Tapez SYSTEM pour que les pilotes du noyau puissent envoyer le trafic par le biais du VPN (par exemple, PING ou SMB).</li> </ul>
Protocole	<p>Ce paramètre spécifie le protocole utilisé par le VPN.</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> <li>• Tout</li> <li>• TCP</li> <li>• UDP</li> </ul> <p>La valeur par défaut est Tout.</p>
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.



<b>Windows : Paramètre du profil VPN</b>	<b>Description</b>
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	<p>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.</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> <li>• Tunnel fractionné</li> <li>• Appliquer le tunnel</li> </ul> <p>Le paramètre par défaut est Forcer le tunnel.</p>
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	<p>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 :</p> <ul style="list-style-type: none"> <li>• Le terminal reste connecté au VPN. Il ne peut pas être déconnecté.</li> <li>• Le terminal doit être connecté à ce VPN pour disposer d'une connexion réseau.</li> <li>• Le terminal ne peut pas se connecter à, ou modifier, d'autres profils VPN.</li> </ul>
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 chaîne 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.
<b>Propriétés de la sécurité IP</b>	

Windows : Paramètre du profil VPN	Description
Constantes de transformation de l'authentification	<p>Valeurs possibles :</p> <ul style="list-style-type: none"> <li>• MD596</li> <li>• SHA196</li> <li>• SHA256128</li> <li>• GCMAES128</li> <li>• GCMAE192</li> <li>• GCMAES256</li> </ul> <p>Le paramètre par défaut est MD596.</p>
Constantes de transformation du chiffrement	<p>Valeurs possibles :</p> <ul style="list-style-type: none"> <li>• DES</li> <li>• DES3</li> <li>• AES 128</li> <li>• AES 192</li> <li>• AES256</li> <li>• GCMAES128</li> <li>• GCMAES192</li> <li>• GCMAES256</li> </ul> <p>Le paramètre par défaut est « DES ».</p>
Méthode de cryptage	<p>Valeurs possibles :</p> <ul style="list-style-type: none"> <li>• DES</li> <li>• DES3</li> <li>• AES 128</li> <li>• AES 192</li> <li>• AES256</li> </ul> <p>Le paramètre par défaut est « DES ».</p>
Méthode de vérification de l'intégrité	<p>Valeurs possibles :</p> <ul style="list-style-type: none"> <li>• MD5</li> <li>• SHA196</li> <li>• SHA256</li> <li>• SHA384</li> </ul> <p>Le paramètre par défaut est MD5.</p>

Windows : Paramètre du profil VPN	Description
Groupe Diffie-Hellman	<p>Valeurs possibles :</p> <ul style="list-style-type: none"> <li>• Groupe 1</li> <li>• Groupe 2</li> <li>• Groupe 14</li> <li>• ECP256</li> <li>• ECP384</li> <li>• Groupe 24</li> </ul> <p>Le paramètre par défaut est Group1.</p>
Groupe PFS	<p>Valeurs possibles :</p> <ul style="list-style-type: none"> <li>• PFS1</li> <li>• PFS2</li> <li>• PFS2048</li> <li>• ECP256</li> <li>• ECP384</li> <li>• PFSMM</li> <li>• PFS24</li> </ul> <p>La valeur par défaut est « PFS1 ».</p>
Type de proxy	<p>Ce paramètre spécifie le type de configuration proxy pour le VPN.</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> <li>• Aucun</li> <li>• Configuration PAC</li> <li>• Configuration manuelle</li> </ul> <p>La valeur par défaut est Aucune.</p>
URL du fichier PAC	<p>Ce paramètre spécifie l'URL du serveur Web qui héberge le fichier PAC, y compris le nom du fichier PAC. Par exemple, <a href="http://www.example.com/PACfile.pac">http://www.example.com/PACfile.pac</a>.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de proxy est défini sur Configuration PAC.</p>
Adresse	<p>Ce paramètre spécifie le FQDN ou l'adresse IP du serveur proxy.</p> <p>Ce paramètre est valide uniquement si le paramètre Type de proxy est défini sur Configuration manuelle.</p>
Profil SCEP associé	<p>Ce paramètre spécifie le profil SCEP associé utilisé par un terminal pour obtenir un certificat client et s'authentifier auprès du VPN.</p>

## Activation d'un VPN par application

Pour les terminaux iOS, iPadOS, Samsung Knox, et Windows 10, 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.

Pour les terminaux iOS et iPadOS, les applications sont associées à un profil VPN lorsque vous affectez l'application ou le groupe d'applications à un utilisateur, à un groupe d'utilisateurs ou à un groupe de terminaux.

Pour les terminaux Samsung Knox avec les activations Android Enterprise et Samsung Knox Workspace, les applications sont ajoutées au paramètre Applications autorisées à utiliser la connexion VPN dans le profil VPN.

Pour les terminaux Windows 10, les applications sont ajoutées à la « Liste d'applications de déclenchement » dans le profil VPN.

### **Comment BlackBerry UEM choisit les paramètres VPN par application à attribuer aux terminaux iOS**

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 :

- Les paramètres VPN d'application directement associés à une application sont prioritaires sur les paramètres VPN d'application indirectement associés via un groupe d'applications.
- Les paramètres VPN d'application directement associés à un utilisateur sont prioritaires sur les paramètres VPN d'application indirectement associés via un groupe d'utilisateurs.
- Les paramètres VPN d'application attribués à une application requise sont prioritaires sur les paramètres VPN d'application attribués à une instance facultative de la même application.
- Les paramètres VPN d'application associés au nom du groupe d'utilisateurs qui apparaît en premier dans la liste alphabétique sont prioritaires si les conditions suivantes sont remplies :
  - Une application est attribuée à plusieurs groupes d'utilisateurs
  - La même application apparaît 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 note contraire, les profils proxy prennent en charge les serveurs proxy utilisant l'authentification de base ou aucune authentification.

Terminal	Configuration du proxy
iOS et iPadOS	<p>Créez un profil proxy et associez-le aux profils utilisés par votre entreprise, notamment :</p> <ul style="list-style-type: none"><li>• Wi-Fi</li><li>• VPN</li></ul> <p>Vous pouvez attribuer un profil proxy à des comptes d'utilisateur, groupes d'utilisateurs ou groupes de terminaux.</p> <p><b>Remarque :</b> 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.</p>
macOS	<p>Créez un profil proxy et associez-le à un profil Wi-Fi ou VPN.</p> <p>macOS applique les profils aux terminaux ou comptes d'utilisateur. Les profils de proxy sont appliqués aux terminaux.</p>
Android	<p>Pour les terminaux Android Enterprise, créez un profil proxy et associez-le à un profil Wi-Fi.</p> <p>Les terminaux Android 8.0 et version ultérieure dotés des activations Contrôles MDM ou Confidentialité de l'utilisateur ne prennent pas en charge les profils Wi-Fi avec des paramètres de proxy.</p>

Terminal	Configuration du proxy
Samsung Knox	<p>Créer un profil proxy et associez-le avec les profils que votre entreprise utilise. Les conditions suivantes s'appliquent :</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> </ul> <p><b>Remarque :</b> Si vous souhaitez utiliser un proxy profil avec un profil de connectivité d'entreprise, BlackBerry Secure Connect Plus doit être activé.</p> <p>Vous pouvez attribuer un profil proxy à des comptes d'utilisateur, groupes d'utilisateurs ou groupes de terminaux. Les conditions suivantes s'appliquent :</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• Sur les terminaux Samsung Knox MDM, le profil configure les paramètres de proxy du navigateur sur le terminal.</li> </ul> <p><b>Remarque :</b> 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.</p>
Windows 10	<p>Créez un profil Wi-Fi ou VPN et spécifiez les informations du serveur proxy dans les paramètres du profil. Les conditions suivantes s'appliquent :</p> <ul style="list-style-type: none"> <li>• Le proxy Wi-Fi prend uniquement en charge la configuration manuelle et est uniquement pris en charge sur les terminaux Windows 10 Mobile.</li> <li>• Le proxy VPN prend en charge la configuration PARC ou manuelle.</li> </ul>

## Créer un profil proxy

Si votre organisation utilise un fichier PAC pour définir des règles de proxy, vous pouvez sélectionner la configuration PAC pour utiliser les paramètres du serveur proxy depuis le fichier PAC que vous spécifiez. Sinon, vous pouvez sélectionner la configuration manuelle et spécifier les paramètres du serveur proxy directement dans le profil.

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	<ol style="list-style-type: none"> <li>a. Dans la liste déroulante <b>Type</b>, vérifiez que le paramètre <b>Configuration PAC</b> est sélectionné.</li> <li>b. Dans le champ <b>URL du fichier PAC</b>, saisissez l'URL du serveur Web hébergeant le fichier PAC et indiquez le nom du fichier PAC (par exemple, <code>http://www.exemple.com/PACfile.pac</code>). Le fichier PAC ne doit pas être hébergé sur un serveur qui héberge BlackBerry UEM ou l'un de ses composants.</li> <li>c. Dans l'onglet <b>BlackBerry</b>, procédez comme suit : <ol style="list-style-type: none"> <li>1. Si votre entreprise 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 <b>Nom d'utilisateur</b>, saisissez <code>%UserName%</code>. Si le serveur proxy requiert le nom de domaine pour l'authentification, utilisez le format <code>&lt;domain&gt;\&lt;username&gt;</code>.</li> <li>2. Dans la liste déroulante <b>Modifiable par l'utilisateur</b>, cliquez sur les paramètres proxy que les utilisateurs de terminaux BlackBerry 10 peuvent modifier. La valeur par défaut est <b>Lecture seule</b>.</li> </ol> </li> </ol>
Définir les paramètres de configuration manuelle	<ol style="list-style-type: none"> <li>a. Dans la liste déroulante <b>Type</b>, cliquez sur <b>Configuration manuelle</b>.</li> <li>b. Dans le champ <b>Hôte</b>, saisissez le FQDN ou l'adresse IP du serveur proxy.</li> <li>c. Dans le champ <b>Port</b>, saisissez le numéro de port du serveur proxy.</li> <li>d. Si votre entreprise 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 <b>Nom d'utilisateur</b>, saisissez <code>%UserName%</code>. Si le serveur proxy requiert le nom de domaine pour l'authentification, utilisez le format <code>&lt;domain&gt;\&lt;username&gt;</code>.</li> <li>e. Dans l'onglet <b>BlackBerry</b>, procédez comme suit : <ol style="list-style-type: none"> <li>1. Dans la liste déroulante <b>Modifiable par l'utilisateur</b>, cliquez sur les paramètres proxy que les utilisateurs de terminaux BlackBerry 10 peuvent modifier. La valeur par défaut est <b>Lecture seule</b>.</li> <li>2. Vous pouvez également spécifier une liste d'adresses auxquelles les utilisateurs peuvent directement accéder à partir de leurs terminaux BlackBerry 10, sans utiliser le serveur proxy. Dans le champ <b>Liste d'exclusion</b>, saisissez les adresses (FQDN ou IP) et utilisez un point-virgule (;) pour séparer les valeurs de la liste. Vous pouvez utiliser le caractère générique (*) dans un nom FQDN ou IP (par exemple, <code>*.exemple.com</code> ou <code>192.0.2.*</code>).</li> </ol> </li> </ol>

7. Répétez les étapes 4 et 5 pour chaque type de terminal de votre organisation.

8. Cliquez sur **Ajouter**.

#### À la fin :

- Associez le profil proxy à un profil Wi-Fi, VPN ou de connectivité d'entreprise.
- Si nécessaire, classez les profils. 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.

# 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.

Pour les terminaux iOS et iPadOS, si vous configurez un VPN par application pour BlackBerry Secure Connect Plus, 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 BlackBerry 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 plus d'informations sur la méthode utilisée par BlackBerry Secure Connect Plus pour transférer des données depuis et vers les terminaux, reportez-vous [au contenu relatif à l'architecture sur site](#) ou [au contenu relatif à l'architecture Cloud](#).

## Étapes à suivre pour activer BlackBerry Secure Connect Plus

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.



Étape	Action
2	Si vous disposez de BlackBerry UEM Cloud, installez BlackBerry Connectivity Node ou mettez BlackBerry Connectivity Node à niveau vers la dernière version.
3	Activez BlackBerry Secure Connect Plus dans le profil de connectivité d'entreprise par défaut ou dans un profil personnalisé que vous créez.
4	Vous pouvez également spécifier les paramètres DNS pour l'application BlackBerry Connectivity.
5	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.
6	Attribuez le profil de connectivité aux comptes d'utilisateur ou aux groupes d'utilisateurs.

## 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 :

- Le pare-feu de votre entreprise doit autoriser les connexions sortantes sur le port 3101 vers `<région>.turnb.bbsecure.com` et `<région>.bbsecure.com`. Si vous configurez BlackBerry UEM pour qu'il utilise un serveur proxy, vérifiez que ce serveur proxy autorise les connexions sur le port 3101 vers ces sous-domaines. Pour connaître les domaines et les adresses IP à utiliser dans votre configuration de pare-feu, rendez-vous sur <http://support.blackberry.com/community> pour consulter l'article 36470.
- Dans chaque instance de BlackBerry 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 disposez de BlackBerry UEM Cloud, installez BlackBerry Connectivity Node ou le mettez à niveau vers la dernière version.

**Remarque :** Si votre environnement sur site inclut des terminaux Knox Workspace ou Android Enterprise dotés d'applications BlackBerry Dynamics, reportez-vous à la section [Optimiser les connexions de tunnel sécurisées pour les terminaux Android qui utilisent des applications BlackBerry Dynamics](#).

**Remarque :** 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. Pour plus d'informations sur BlackBerry Secure Gateway, reportez-vous à la section [Protection des données de la messagerie électronique à l'aide de BlackBerry Secure Gateway](#).

Pour les terminaux pris en charge :

Terminal	Configuration requise
iOS et iPadOS	<ul style="list-style-type: none"> <li>Les terminaux doivent être activés à l'aide de l'application BlackBerry UEM Client, disponible à partir de App Store</li> <li>Type d'activation Contrôles MDM</li> </ul>
Android Enterprise	<ul style="list-style-type: none"> <li>L'un des types d'activation suivants : <ul style="list-style-type: none"> <li>Espace Travail uniquement (Premium)</li> <li>Travail et Personnel - Contrôle total (Premium)</li> <li>Travail et Personnel - Confidentialité des données de l'utilisateur (Premium)</li> </ul> </li> </ul>
Samsung Knox Workspace	<ul style="list-style-type: none"> <li>Samsung Knox MDM version 5.0 ou ultérieure</li> <li>Samsung Knox version 2.3 ou ultérieure</li> <li>L'un des types d'activation suivants : <ul style="list-style-type: none"> <li>Espace Travail uniquement (Samsung Knox)</li> <li>Travail et Personnel - Contrôle total (Samsung Knox)</li> <li>Travail et Personnel - Confidentialité des données de l'utilisateur (Samsung Knox)</li> </ul> </li> </ul>

## Installation de composants BlackBerry Secure Connect Plus supplémentaires dans un environnement sur site

Vous pouvez installer une ou plusieurs instances de BlackBerry Connectivity Node pour ajouter des instances supplémentaires de composants de connectivité de terminal au domaine de votre organisation. Chaque BlackBerry Connectivity Node contient une instance active de BlackBerry Secure Connect Plus capable de traiter les données de terminal et d'établir des connexions sécurisées.

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

Si un domaine comprend plusieurs instances de BlackBerry UEM, le composant BlackBerry Secure Connect Plus de chaque instance est exécuté et traite les données. Les données sont équilibrées en termes de charges sur tous les composants BlackBerry Secure Connect Plus du domaine.

Le basculement de haute disponibilité est disponible pour BlackBerry Secure Connect Plus. Si un terminal utilise un tunnel sécurisé et que le composant BlackBerry Secure Connect Plus actuel devient indisponible, BlackBerry Infrastructure attribue le terminal à un composant BlackBerry Secure Connect Plus sur une autre instance de BlackBerry UEM. Le terminal utilise à nouveau le tunnel sécurisé sans interruption majeure.

Pour plus d'informations sur la planification et l'installation de BlackBerry Connectivity Node, [reportez-vous au contenu relatif à la planification](#) et [au contenu relatif à l'installation et à la mise à niveau](#).

## Installation ou mise à niveau du composant BlackBerry Secure Connect Plus dans un environnement Cloud

Lorsque vous installez BlackBerry Connectivity Node, le processus d'installation installe également le composant BlackBerry Secure Connect Plus sur le même ordinateur. Si vous mettez à niveau BlackBerry Connectivity Node vers la version la plus récente et que BlackBerry Secure Connect Plus n'est pas installé, le processus de mise à niveau installe BlackBerry Secure Connect Plus. Si BlackBerry Secure Connect Plus a été installé précédemment, le processus met BlackBerry Secure Connect Plus à niveau vers la dernière version.

Pour obtenir des instructions sur l'installation ou la mise à niveau de BlackBerry Connectivity Node, [reportez-vous à la section « Installation et mise à niveau de BlackBerry Connectivity Node » dans le contenu relatif à la configuration de BlackBerry UEM Cloud](#). Vous devez activer BlackBerry Connectivity Node avant de pouvoir activer BlackBerry Secure Connect Plus.

Vous avez la possibilité d'acheminer les données entre BlackBerry Secure Connect Plus et BlackBerry Infrastructure via BlackBerry Router ou un serveur proxy TCP (transparent ou SOCKS v5). Utilisez la console de gestion BlackBerry Connectivity Node (Paramètres généraux > Proxy) pour configurer les paramètres de proxy.

**Remarque :** Si vous spécifiez des informations de proxy non valides, BlackBerry Secure Connect Plus s'arrête et ne peut pas redémarrer. Si ce problème survient, corrigez les informations de proxy et redémarrez le service BlackBerry UEM - BlackBerry Secure Connect Plus dans les services Windows.

Vous pouvez installer une deuxième instance de BlackBerry Connectivity Node pour assurer la redondance. Les deux instances de BlackBerry Secure Connect Plus sont exécutées et traitent les données. La charge de données est équilibrée entre les deux instances. Si un terminal utilise un tunnel sécurisé et que le composant BlackBerry Secure Connect Plus actuel devient indisponible, BlackBerry Infrastructure attribue le terminal à l'autre instance. Le terminal utilise à nouveau le tunnel sécurisé sans interruption majeure.

## 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).

BlackBerry publie de nouvelles versions de l'application pour prendre en charge les nouvelles fonctionnalités et améliorations. Pour obtenir des instructions sur la mise à niveau de l'application, et pour en savoir plus sur les derniers problèmes connus et résolus, reportez-vous aux [Notes de version de BlackBerry Connectivity](#).

1. Sur la barre de menus de la console de gestion, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Réseaux et connexions > Connectivité d'entreprise**.
3. Cliquez sur **+**.
4. 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.

5. Configurez les valeurs appropriées pour les paramètres de profil pour chaque type de terminal. Pour plus d'informations sur les différents paramètres de profil, reportez-vous à [Paramètres de profil de connectivité d'entreprise](#).
6. Cliquez sur **Ajouter**.
7. Attribuez le profil aux groupes ou comptes d'utilisateur.
8. Si vous avez configuré un VPN par application pour les terminaux iOS et iPadOS procédez comme suit lorsque vous attribuez une application ou un groupe d'applications : associez cette application ou ce groupe d'applications au profil de connectivité d'entreprise qui convient.

**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 de terminaux iOS, iPadOS, Android Enterprise et Knox Workspace 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.
- 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.

**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.  Ce paramètre est valide uniquement si vous avez installé une ou plusieurs instances de BlackBerry Connectivity Node et configuré des groupes de serveurs.

**iOS : Paramètres de profil de connectivité d'entreprise**

Les paramètres de 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	<p>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.</p> <p>Sélectionnez ce paramètre pour spécifier des règles pour les connexions BlackBerry Secure Connect Plus.</p>
Règles de VPN à la demande pour iOS 9 ou version ultérieure	<p>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.</p> <p>Ce paramètre est valide uniquement si le paramètre Activer VPN à la demande est sélectionné.</p>
Activer un VPN par application	<p>Sélectionnez ce paramètre pour autoriser uniquement certaines applications à utiliser BlackBerry Secure Connect Plus.</p> <p><b>Remarque :</b> 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).</p>
Domaines Safari	<p>Cliquez sur  pour spécifier les domaines autorisés à lancer une connexion VPN dans Safari.</p>
Autoriser la connexion automatique des applications	<p>Spécifiez si les applications peuvent lancer la connexion VPN automatiquement.</p>
Profil de proxy	<p>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.</p> <p>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 <a href="#">Création de profils proxy pour les terminaux</a>.</p>

#### Android : Paramètres de profil de connectivité d'entreprise

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

Paramètre	Description
Connectivité d'entreprise pour les terminaux Android comprenant un espace Travail	<p>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.</p> <ul style="list-style-type: none"> <li>• « VPN à l'échelle du conteneur » utilise une connexion VPN pour toutes les applications dans l'espace Travail sur le terminal.</li> <li>• « VPN par application » utilise une connexion VPN uniquement pour les applications spécifiées.</li> </ul>
Applications non autorisées à utiliser BlackBerry Secure Connect Plus	<p>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.</p> <p>Cliquez sur <b>+</b> et saisissez un ID de package d'application. Si nécessaire, répétez l'opération pour restreindre d'autres applications.</p> <p>Par défaut, Google Play et les services sous-jacents (com.android.providers.media, com.android.vending, com.google.android.gms et com.google.android.apps.gcs) sont restreints car Google Play ne prend en charge aucun proxy. Il est recommandé de maintenir ces restrictions. Si vous supprimez l'une de ces restrictions, vous devez contacter l'assistance Google Play pour obtenir la configuration de pare-feu requise afin d'autoriser les connexions à Google Play à l'aide de BlackBerry Secure Connect Plus. Par défaut, les packages sont ajoutés au nouveau profil de connectivité d'entreprise, mais vous devez les ajouter à tous les profils existants.</p> <p>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 BlackBerry UEM Client de communiquer avec BlackBerry Infrastructure via BlackBerry UEM. Pour plus d'informations sur l'ouverture de ports dans le pare-feu lorsque les applications professionnelles utilisent BlackBerry Secure Connect Plus, rendez-vous sur le site Web <a href="http://support.blackberry.com/community">support.blackberry.com/community</a> pour consulter l'article 48330.</p> <p>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.</p> <p>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.</p>

Paramètre	Description
Applications autorisées à utiliser la connectivité d'entreprise	<p>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.</p> <p>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.</p>
Profil de proxy	<p>Si vous souhaitez acheminer le trafic du tunnel sécurisé depuis les terminaux Samsung Knox avec des activations Android Enterprise et Samsung Knox Workspace version 2.5 et ultérieure jusqu'au réseau professionnel via un serveur proxy, sélectionnez le profil de proxy adéquat.</p> <p>Cela ne s'applique pas aux terminaux Android Enterprise autres que Samsung Knox, ni aux terminaux exécutant Samsung Knox Workspace 2.4 et versions antérieures.</p>

## 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. Vous pouvez également spécifier des suffixes de recherche DNS. 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.

Si vous créez et configurez un ou plusieurs groupes de serveurs pour diriger les connexions BlackBerry Secure Connect Plus vers un chemin local spécifique à BlackBerry Infrastructure, vous pouvez définir des paramètres DNS spécifiques à chaque groupe de serveurs. Si vous le faites, les paramètres DNS pour un groupe de serveurs sont prioritaires sur les paramètres DNS mondiaux que vous spécifiez à l'aide de la procédure suivante. Pour plus d'informations sur la création et la configuration de groupes de serveurs, reportez-vous au [contenu relatif à l'installation et à la mise à niveau](#) ou au [contenu relatif à la configuration UEM Cloud](#).

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 sur des terminaux 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, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Réseaux et connexions > Connectivité BlackBerry Dynamics**.
3. Sélectionnez le profil assigné à Android Enterprise et Samsung Knox Workspace périphériques.
4. Cliquez sur .
5. Désactivez la case **Acheminer tout le trafic**.
6. 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.

### L'adaptateur BlackBerry Secure Connect Plus passe à un état « Réseau non identifié » et cesse de fonctionner

#### Cause

Ce problème peut survenir si vous redémarrez l'ordinateur qui héberge BlackBerry Secure Connect Plus.

#### Solution - Windows Server 2012

1. Dans le Gestionnaire de serveur, cliquez sur **Gérer > Ajouter des rôles et des fonctionnalités**. Cliquez sur **Suivant** jusqu'à accéder à l'écran **Fonctionnalités**. Développez **Outils d'administration de serveur distant > Outils d'administration de rôles** et sélectionnez **Outils de gestion des accès distants**. Exécutez l'Assistant pour installer les outils.
2. Cliquez sur **Outils > Gestion des accès distants**.
3. Sous **Configuration**, cliquez sur **DirectAccess et VPN**.
4. Sous **VPN**, cliquez sur **Ouvrir la gestion RRAS**.
5. Cliquez avec le bouton droit sur **Routage et Serveur d'accès à distance**, puis cliquez sur **Désactiver le routage et l'accès à distance**.
6. Cliquez avec le bouton droit sur **Routage et Serveur d'accès à distance**, puis cliquez sur **Configurer et activer l'accès à distance et le routage**.
7. Exécutez l'Assistant de configuration en sélectionnant les options suivantes :



- a. Sur l'écran **Configuration**, sélectionnez **Network Address Translation (NAT)**.
  - b. Sur l'écran **Connexion Internet NAT**, sélectionnez **Utiliser cette interface publique pour se connecter à Internet**. Vérifiez que BlackBerry Secure Connect Plus s'affiche dans la liste des interfaces réseau.
8. Ouvrez **Routage et accès à distance** > <nom\_serveur> > **IPv4** et cliquez sur **NAT**. Ouvrez les propriétés de **connexion au réseau local** et sélectionnez **Interface publique connectée à Internet** et **Activer NAT sur cette interface**. Cliquez sur **OK**.
  9. Ouvrez les propriétés **BlackBerry Secure Connect Plus** et sélectionnez **Interface privée connectée au réseau privé**. Cliquez sur **OK**.
  10. Cliquez avec le bouton droit sur **Routage et serveur d'accès à distance**, puis sur **Toutes les tâches** > **Redémarrer**.
  11. Dans les services Windows, redémarrez le service **BlackBerry UEM – BlackBerry Secure Connect Plus**.

Téléchargez et installez le correctif de l'article KB Windows [Échec de la fonctionnalité NAT sur un serveur RRAS basé sur Windows Server 2012](#).

## **BlackBerry Secure Connect Plus ne démarre pas.**

### **Cause possible**

Les paramètres TCP/IPv4 pour 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, entraînant l'échec de la configuration de routage/NAT lors de la mise à niveau. Ce problème peut également survenir après une nouvelle installation de BlackBerry 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**.

## Afficher les fichiers journaux pour BlackBerry Secure Connect Plus

Deux fichiers journaux, situés par défaut à l'emplacement `<lecteur>:\Program Files\BlackBerry\UEM\Logs\<aaaammjj>`, enregistrent les données concernant BlackBerry Secure Connect Plus :

- BSCP : consigne les données sur le composant serveur BlackBerry Secure Connect Plus
- BSCP-TS : consigne les données de connexion avec l'application BlackBerry Connectivity

Sur chaque ordinateur qui héberge une instance de BlackBerry Connectivity Node, les fichiers journaux de BlackBerry Secure Connect Plus se trouvent sous `<lecteur>:\Program Files\BlackBerry\BlackBerry Connectivity Node\Logs\<aaaammjj>`.

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](#).

# Configuration de l'authentification avec identification unique pour les terminaux

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.

Pour les terminaux exécutant iOS ou iPadOS 13 ou une version ultérieure, vous devez utiliser un profil d'extension avec identification unique pour leur permettre de s'authentifier automatiquement auprès des domaines et services Web du réseau de votre organisation. Les terminaux exécutant une version iOS antérieure à 13 utilisaient des profils d'identification unique.

- Kerberos
- NTLM
- Certificats SCEP pour les domaines approuvés spécifiés

Les applications BlackBerry Dynamics prennent également en charge l'authentification Kerberos. Pour plus d'informations, reportez-vous à la section [Configuration de Kerberos pour les applications BlackBerry Dynamics](#).

## Créer un profil d'extension d'identification unique

Les extensions d'identification unique sont prises en charge pour les terminaux exécutant iOS et iPadOS 13 ou version ultérieure. 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, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Réseaux et connexions** > **Extension d'identification unique**.
3. Cliquez sur **+**.
4. Saisissez le nom et la description du profil.
5. Dans la liste déroulante **Type d'extension d'identification unique**, indiquez si vous utilisez une extension personnalisée ou l'extension Kerberos fournie par Apple.

Tâche	Étapes
<p>Si vous sélectionnez <b>Extension personnalisée</b></p>	<ol style="list-style-type: none"> <li>a. Dans le champ <b>Identifiant d'extension</b>, saisissez l'identifiant de l'application qui exécute l'identification unique.</li> <li>b. Indiquez si le type d'identification est <b>Informations d'identification</b> ou <b>Rediriger</b></li> <li>c. Si vous avez sélectionné <b>Informations d'identification</b> comme type d'identification, procédez comme suit : <ol style="list-style-type: none"> <li>1. Dans le champ <b>Domaine</b>, saisissez le nom de domaine pour les informations d'identification.</li> <li>2. Dans la section <b>Domaines</b>, cliquez sur <b>+</b> pour ajouter un domaine.</li> <li>3. Dans le champ <b>Nom</b>, saisissez le domaine pour lequel l'extension d'application exécute l'identification unique.</li> <li>4. Ajoutez des domaines supplémentaires si nécessaire.</li> </ol> </li> <li>d. Si vous avez sélectionné <b>Rediriger</b> comme type d'identification, procédez comme suit : <ol style="list-style-type: none"> <li>1. Dans la section <b>URL</b>, cliquez sur <b>+</b> pour ajouter une URL.</li> <li>2. Dans le champ <b>Nom</b>, 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.</li> </ol> </li> <li>e. Dans le champ <b>Code de charge utile personnalisée</b>, saisissez le code de charge utile personnalisée pour l'extension d'application.</li> </ol>

Tâche	Étapes
<p>Si vous sélectionnez <b>Extension intégrée Kerberos</b></p>	<ul style="list-style-type: none"> <li>a. Dans la section <b>Domaines</b>, cliquez sur <b>+</b> pour ajouter un domaine.</li> <li>b. Dans le champ <b>Nom de domaine</b>, saisissez le nom de domaine pour les informations d'identification.</li> <li>c. Sélectionnez les <b>Données de l'extension pour l'authentification unique Kerberos Apple</b> 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.</li> <li>d. Définissez le <b>Nom principal</b> de la connexion.</li> <li>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 <b>Sélectionner le certificat PKINIT pour l'authentification</b>, puis sélectionnez le profil approprié.</li> <li>f. Si vous utilisez l'API GSS (Generic Security Service), spécifiez le <b>Nom GSS du cache Kerberos</b>.</li> <li>g. Dans la section <b>Identifiants de l'offre d'application</b>, cliquez sur <b>+</b> pour spécifier les ID d'offre autorisés à accéder au ticket d'émission de ticket.</li> <li>h. Dans la section <b>Centres de distribution clés préférés</b>, cliquez sur <b>+</b> 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.</li> <li>i. Dans le champ <b>Mappage domaine-domaine personnalisé</b>, saisissez tout mappage personnalisé requis des domaines aux noms de domaine au format de charge utile, par exemple <code>&lt;key&gt;exemple-domaine1&lt;/key&gt;&lt;array&gt;&lt;string&gt;org&lt;/string&gt;&lt;/array&gt;</code>.</li> <li>j. Dans le champ <b>Indication de connexion</b>, spécifiez le texte à afficher en bas de la fenêtre de connexion à Kerberos.</li> </ul>

6. Cliquez sur **Enregistrer**.

# Configuration des profils 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 peut vous aider à offrir une expérience de navigation Web plus rapide et plus sûre sur les terminaux exécutant iOS et iPadOS 14 et versions ultérieures, et macOS 11 et versions ultérieures.

## Créer un profil DNS

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Réseaux et connexions > DNS**.
3. Cliquez sur **+**.
4. Saisissez le nom et la description du profil.
5. Cliquez sur l'onglet correspondant à un type de terminal.
6. Sélectionnez le protocole DNS utilisé pour communiquer avec le serveur DNS.
7. 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).
8. Sélectionnez l'option **Ne pas autoriser l'utilisateur à désactiver les paramètres DNS** pour empêcher les utilisateurs de désactiver les paramètres. Cette option concerne uniquement les terminaux surveillés.
9. 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.
10. Dans le champ **Domaines**, indiquez la liste des chaînes de domaine qui seront utilisées pour déterminer les requêtes DNS qui utiliseront les serveurs DNS.
11. 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.
12. Cliquez sur **Enregistrer**.
13. Répétez les étapes 5 à 12 pour tout autre type de terminal.

# Gérer les domaines de messagerie et les 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.

## Créer un profil de domaines gérés

Les profils de domaines gérés s'appliquent uniquement aux terminaux iOS et iPadOS.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Réseaux et connexions > Domaines gérés**.
3. Cliquez sur **+**.
4. Saisissez le nom et la description du profil.
5. Dans le champ **Description**, tapez la description du profil.
6. Dans la section **Domaines de messagerie gérés**, cliquez sur **+**.
7. Dans le champ **Domaines de messagerie**, saisissez un nom de domaine de niveau supérieur (par exemple, `exemple.com` plutôt que `exemple.com/canada`).
8. Cliquez sur **Ajouter**.
9. 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 \(Domaines Web Safari gérés dans la Bibliothèque du développeur iOS\)](#).
10. Dans le champ **Domaines Web**, saisissez un nom de domaine.
11. 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.
12. Cliquez sur **Ajouter**.
13. Cliquez sur **Ajouter**.



# 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.

## Créer un profil d'utilisation du réseau

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 d'applications et attribuez-les aux groupes d'utilisateurs ou aux comptes d'utilisateurs.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Réseaux et connexions > Utilisation du réseau**.
3. Cliquez sur **+**.
4. Saisissez le nom et la description du profil.
5. Cliquez sur **+**.
6. Effectuez l'une des opérations suivantes :
  - Sélectionnez **Ajouter une application**, puis cliquez sur une application de la liste.
  - Sélectionnez **Spécifier l'ID du package d'applications** 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.\***).
7. 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**.
8. 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**.
9. Cliquez sur **Ajouter**.
10. Répétez les étapes 5 à 9 pour chacune des applications que vous souhaitez ajouter à la liste.

**À la fin** : Si nécessaire, classez les profils.

# Filtrage 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, 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	<p>Cette option permet d'accéder uniquement aux sites Web que vous spécifiez. Dans Safari, un signet est créé pour chaque site Web autorisé.</p> <p><b>Remarque :</b> 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 <a href="#">l'authentification moderne de Microsoft Office 365 pour les applications BlackBerry Dynamics</a>, le terminal doit pouvoir accéder au site Web des services de fédération Active Directory.</p>
Limiter le contenu pour adultes	<p>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 :</p> <ul style="list-style-type: none"><li>• 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.</li><li>• 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.</li></ul>

## Créer un profil de filtre de contenu Web

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).

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

Tâche	Étapes
Autoriser l'accès à des sites Web spécifiques uniquement	<ul style="list-style-type: none"> <li>a. Dans la liste déroulante <b>Sites Web autorisés</b>, vérifiez que le paramètre <b>Sites Web spécifiques uniquement</b> est sélectionné.</li> <li>b. Dans la section <b>Signets de sites Web spécifiques</b>, cliquez sur <b>+</b>.</li> <li>c. Procédez comme suit : <ul style="list-style-type: none"> <li>1. Dans le champ <b>URL</b>, saisissez l'adresse Web dont vous souhaitez autoriser l'accès.</li> <li>2. Dans le champ <b>Chemin du signet</b>, vous pouvez également saisir le nom d'un dossier de signets (par exemple, /Work/).</li> <li>3. Dans le champ <b>Titre</b>, saisissez le nom du site Web.</li> <li>4. Cliquez sur <b>Ajouter</b>.</li> </ul> </li> <li>d. Répétez les étapes 2 et 3 pour chaque site Web autorisé.</li> </ul>
Limiter le contenu pour adultes	<ul style="list-style-type: none"> <li>a. Dans la liste déroulante <b>Sites Web autorisés</b>, cliquez sur <b>Limiter le contenu pour adultes</b> pour activer le filtrage automatique.</li> <li>b. Vous pouvez également procéder comme suit : <ul style="list-style-type: none"> <li>1. Cliquez sur <b>+</b> en regard de <b>URL autorisées</b>.</li> <li>2. Saisissez l'adresse Web dont vous souhaitez autoriser l'accès.</li> <li>3. Répétez les étapes 2.a et 2.b pour chaque site Web autorisé.</li> </ul> </li> <li>c. Vous pouvez également procéder comme suit : <ul style="list-style-type: none"> <li>1. Cliquez sur <b>+</b> en regard de <b>URL non autorisées</b>.</li> <li>2. Saisissez l'adresse Web dont vous souhaitez refuser l'accès.</li> <li>3. Répétez les étapes 3.a et 3.b pour chaque site Web limité.</li> </ul> </li> </ul>

6. Cliquez sur **Ajouter**.

# Configuration des profils AirPrint et AirPlay pour 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 attribuer des profils AirPrint à des terminaux iOS et iPadOS afin que les utilisateurs n'aient pas à configurer les imprimantes manuellement.

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.

## Créer un profil AirPrint

Vous pouvez configurer les profils AirPrint et les attribuer aux terminaux iOS et iPadOS pour que les utilisateurs n'aient pas à configurer les imprimantes manuellement.

Pour plus d'informations sur la configuration requise des ports et du pare-feu, rendez-vous sur le protocole Bonjour et l'impression avec une application BlackBerry Dynamics, rendez-vous sur [support.blackberry.com/community](https://support.blackberry.com/community) pour consulter l'article 40030.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Réseaux et connexions > AirPrint**.
3. Cliquez sur **+**.
4. Saisissez le nom et la description du profil AirPrint.
5. Dans la section **Configuration d'AirPrint**, cliquez sur **+**.
6. Dans le champ **Adresse IP**, saisissez l'adresse IP de l'imprimante ou du serveur AirPrint.
7. 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 `_ipp.s.tcpBonjour`. Par exemple :
  - `printers/<gamme de l'imprimante>`
  - `printers/<modèle de l'imprimante>`
  - `ipp/print`
  - `IPP_Printer`
8. Si les connexions AirPrint sont sécurisées par TLS, vous pouvez également cocher la case **Forcer TLS**.

9. Si le port diffère de celui par défaut du protocole d'impression Internet, saisissez le numéro de port dans le champ **Port**.
10. Cliquez sur **Ajouter**.
11. Cliquez sur **Ajouter**.

## Créer un profil AirPlay

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Réseaux et connexions > AirPlay**.
3. Cliquez sur **+**.
4. Saisissez le nom et la description du profil AirPlay.
5. Cliquez sur **+** dans la section **Terminaux de destination autorisés**.
6. 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.
7. Dans le champ **Mot de passe**, saisissez un mot de passe.
8. Cliquez sur **Ajouter**.
9. Cliquez sur **+** dans la section **Terminaux de destination autorisés pour les terminaux supervisés**.
10. 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.
11. Cliquez sur **Ajouter**.

# Configuration des noms de points d'accès pour 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 Android 9 et versions ultérieures avec des activations Espace Travail uniquement et les terminaux Android 9 et 10 avec des activations 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, sélectionnez la règle de stratégie informatique « Forcer le terminal à utiliser les paramètres de profil de nom de point d'accès » dans les règles de stratégie informatique Android Global (tous les terminaux Android).

## Créer un profil de nom de point d'accès

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

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Réseaux et connexions > Nom du point d'accès**.
3. Cliquez sur **+**.
4. Saisissez le nom et la description du profil Nom de point d'accès. Cette information s'affiche sur les terminaux.
5. Saisissez le **Nom de point d'accès**.
6. 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](#).
7. Cliquez sur **Enregistrer**.

## 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 chaîne de texte.

Paramètre du profil de nom de point d'accès	Description
Masque binaire de type APN	<p>Ce paramètre spécifie les types de communication de données qui utilisent cette configuration APN. Différents types de communications peuvent utiliser des configurations différentes.</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> <li>• Trafic de données par défaut</li> <li>• Trafic MMS</li> <li>• GPS assisté par SUPL</li> <li>• Trafic DUN</li> <li>• Trafic prioritaire</li> <li>• Accès au portail FOTA de l'opérateur</li> <li>• IMS</li> <li>• CBS</li> <li>• APN de connexion initiale IA</li> <li>• NRP d'urgence</li> <li>• MCX (Mission Critical Service)</li> </ul>
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	<p>Ce paramètre spécifie le type d'authentification utilisé pour les communications.</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> <li>• NONE</li> <li>• PAP</li> <li>• CHAP</li> <li>• PAP ou CHAP</li> </ul>
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	<p>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.</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> <li>• IP</li> <li>• IPV6</li> <li>• IPV4V6</li> <li>• PPP</li> </ul>
Protocole d'itinérance	<p>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.</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> <li>• IP</li> <li>• IPV6</li> <li>• IPV4V6</li> <li>• PPP</li> </ul>
Opérateur activé	Ce paramètre indique si l'APN est activé pour l'opérateur.
Type MVNO	<p>Ce paramètre spécifie s'il faut restreindre l'utilisation de cet APN à certains MVNO (revendeurs de réseaux mobiles) ou comptes d'abonnés.</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> <li>• SP</li> <li>• IMSI</li> <li>• GID</li> <li>• ICCID</li> </ul>



# Informations juridiques

©2022 BlackBerry Limited. Les marques commerciales, notamment BLACKBERRY, BBM, BES, EMBLEM Design, ATHOC, CYLANCE et SECUSMART sont des marques commerciales ou des marques déposées de BlackBerry Limited, ses filiales et/ou sociétés affiliées, utilisées sous licence, et les droits exclusifs de ces marques commerciales sont expressément réservés. Toutes les autres marques commerciales appartiennent à leurs propriétaires respectifs.

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 COÛTS D'INDISPONIBILITÉ, LA PERTE D'UTILISATION DES PRODUITS OU SERVICES BLACKBERRY EN TOUT OU EN PARTIE, OU DE TOUT SERVICE DE COMMUNICATION, DU COÛT DE BIENS DE

SUBSTITUTION, DES FRAIS DE GARANTIE, DES ÉQUIPEMENTS OU SERVICES, DES COÛTS 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