BlackBerry UEM

ネットワーク接続のセキュリティ保護

管理

12.12

目次

Wi-Fi、VPN、BlackBerry Secure Connect Plus、および他の仕事用接続の管理.....6

プロファイルを使用した仕事用接続の管理.....7

対策：仕事用接続プロファイルを作成.....8

デバイスの仕事用 **Wi-Fi** ネットワークの設定.....9

Wi-Fi プロファイルの作成.....9
Wi-Fi プロファイル設定.....10
共通：Wi-Fi プロファイル設定.....10
iOS および macOS ：Wi-Fi プロファイル設定.....10
Android ：Wi-Fi プロファイル設定.....17
Windows ：Wi-Fi プロファイル設定.....22
BlackBerry 10 ：Wi-Fi プロファイル設定.....27

デバイスの仕事用 **VPN** の設定.....33

VPN プロファイルの作成.....34
VPN プロファイル設定.....34
iOS および macOS ：VPN プロファイル設定.....35
Android ：VPN プロファイル設定.....44
Windows 10 ：VPN プロファイル設定.....50
BlackBerry 10 ：VPN プロファイル設定.....57
per-app VPN の有効化.....72
iOS デバイスに割り当てる per-app VPN 設定を BlackBerry UEM が選択する方法.....73

デバイスのプロキシプロファイルのセットアップ.....74

プロキシプロファイルの作成.....75

BlackBerry Secure Connect Plus を使用した仕事用リソースへの接続.....78

BlackBerry Secure Connect Plus を有効にする手順.....78
BlackBerry Secure Connect Plus のサーバーとデバイスの要件.....79
オンプレミス環境での追加 BlackBerry Secure Connect Plus コンポーネントのインストール.....80
クラウド環境での BlackBerry Secure Connect Plus コンポーネントのインストールまたはアップグレード.....81
BlackBerry Secure Connect Plus を有効化する.....82
エンタープライズ接続プロファイル設定.....82

BlackBerry Connectivity アプリ DNS 設定の指定 86
BlackBerry Dynamics アプリを使用する Android デバイスのためにセキュリティ保護されたトンネル接続を最適化する 87
Wi-Fi ネットワークが利用可能な場合に BlackBerry Secure Connect Plus 経由で BlackBerry 10 の仕事用領域トラフィックを直接実行する 87
BlackBerry Secure Connect Plus のトラブルシューティング 88
BlackBerry Secure Connect Plus Adapter が「識別されていないネットワーク」状態になり、動作を停止した 88
BlackBerry Secure Connect Plus が開始しない 89
BlackBerry UEM のインストールまたはアップグレード後、BlackBerry Secure Connect Plus が動作を停止する 89
BlackBerry Secure Connect Plus のログファイルを表示 90

BlackBerry 10 デバイスのエンタープライズ接続の使用 91
BlackBerry 10 デバイスのエンタープライズ接続を管理する 91

BlackBerry 2FA を使用した、重要なリソースへのセキュリティ保護された接続 92

デバイスでシングルサインオン認証を設定 93
前提条件：デバイスで Kerberos 認証を使用する 93
証明書ベースの iOS デバイス認証 94
シングルサインオンプロファイルの作成 94
シングルサインオン拡張プロファイルの作成 96

iOS デバイスのメールドメインと Web ドメインの管理 98
管理されているドメインプロファイルの作成 98

iOS デバイスのアプリのネットワーク使用を制御する 99
ネットワーク使用プロファイルの作成 99

iOS デバイス上での Web コンテンツのフィルター 100
Web コンテンツフィルタープロファイルの作成 100

iOS デバイス用 AirPrint プロファイルおよび AirPlay プロファイルの設定 102
AirPrint プロファイルの作成 102
AirPlay プロファイルの作成 103

Android デバイスのアクセスポイント名の設定 104
アクセスポイント名プロファイルの作成 104

商標などに関する情報..... 105

Wi-Fi、VPN、BlackBerry Secure Connect Plus、および他の仕事用接続の管理

プロファイルを使用して、組織内のデバイスの仕事用接続をセットアップし管理することができます。仕事用接続は、メールサーバーやプロキシサーバー、Wi-Fi ネットワーク、VPN など、組織環境内の仕事用リソースとデバイスの接続方法を定義します。同一のプロファイルで、iOS、macOS、Android、Windows、および BlackBerry 10 デバイスの設定を指定してから、そのプロファイルをユーザーアカウント、ユーザーグループ、またはデバイスグループに割り当てることができます。

プロファイルを使用した仕事用接続の管理

ポリシーおよびプロファイルライブラリで利用可能な次のプロファイルを使用して、デバイスが仕事用リソースに接続する方法を設定できます。

プロファイル	説明
Wi-Fi	Wi-Fi プロファイルは、デバイスが仕事用 Wi-Fi ネットワークに接続する方法を指定します。
VPN	VPN プロファイルは、デバイスが仕事用 VPN に接続する方法を指定します。
プロキシ	プロキシプロファイルは、デバイスがプロキシサーバーを使用してインターネットまたは仕事用ネットワーク上の Web サービスにアクセスする方法を指定します。
エンタープライズ接続	エンタープライズ接続プロファイルは、エンタープライズ接続および BlackBerry Secure Connect Plus を使用して、デバイスが組織のリソースに接続する方法を指定します。 iOS、Android Enterprise、Samsung Knox Workspace、および BlackBerry 10 デバイスは、BlackBerry Secure Connect Plus をファイアウォール内部の仕事用リソースへのセキュリティ接続に使用できます。
BlackBerry 2FA	BlackBerry 2FA プロファイルは、ユーザーのツーファクター認証を有効にし、事前認証および自己回復機能の設定を指定します。
シングルサインオン	シングルサインオンプロファイルは、ユーザーがユーザー名とパスワードを初めて入力した後に、デバイスがセキュリティ保護されたドメインでの認証を自動的に実行する方法を指定します。
BlackBerry Dynamics 接続プロファイル	BlackBerry Dynamics 接続プロファイルでは、ネットワーク接続、インターネットドメイン、IP アドレス範囲、および BlackBerry Dynamics アプリの使用時にデバイスが接続できるアプリサーバーを定義します。
メール	メールプロファイルは、デバイスを仕事用メールサーバーに接続し、Exchange ActiveSync や IBM Notes Traveler を使用してメールやカレンダーエントリ、オーガナイザーデータを同期する方法を指定します。
IMAP/POP3 メール	IMAP/POP3 メールプロファイルは、デバイスを IMAP または POP3 メールサーバーに接続して、メールを同期する方法を指定します。

対策：仕事用接続プロファイルを作成

一部の仕事用接続プロファイルには 1 つ以上の関連付けられたプロファイルを含めることができます。関連付けられたプロファイルを使用する場合は、既存のプロファイルを仕事用接続プロファイルにリンクします。デバイスは、仕事用接続プロファイルを使用する際に、関連付けられたプロファイルを使用する必要があります。

次のガイドラインを参考にしてください。

- 組織内のデバイスにどの仕事用接続が必要か決定します。
- 他のプロファイルに関連付けできるプロファイルを作成してから、それらを使用する仕事用接続プロファイルを作成します。
- 適切な場所で変数を使用します。

証明書プロファイルとプロキシプロファイルをさまざまな仕事用接続プロファイルと関連付けることができます。プロファイルは次の順番で作成する必要があります。

1. 証明書プロファイル
2. プロキシプロファイル
3. 仕事用接続プロファイル（メール、VPN、Wi-Fi など）

たとえば、Wi-Fi プロファイルを最初に作成する場合は、プロキシプロファイルの作成時に、それを Wi-Fi プロファイルに関連付けることはできません。プロキシプロファイルの作成後に、Wi-Fi プロファイルを変更してから、プロキシプロファイルをそれに関連付ける必要があります。

デバイスの仕事用 Wi-Fi ネットワークの設定

Wi-Fi プロファイルを使用して、ファイアウォール内部の仕事用 Wi-Fi ネットワークにデバイスを接続する方法を指定できます。Wi-Fi プロファイルは、ユーザーアカウント、ユーザーグループ、またはデバイスグループに割り当てることができます。

デフォルトでは、仕事用アプリと個人用アプリの両方とも、デバイスに保存された Wi-Fi プロファイルを使用して、組織のネットワークに接続できます。

Wi-Fi プロファイルの作成

必要となるプロファイルの設定は、各デバイスタイプと、選択する Wi-Fi セキュリティタイプおよび認証プロトコルに応じて異なります。

作業を始める前に：

- デバイスが仕事用 Wi-Fi 接続に対して証明書に基づく認証を使用している場合は、CA 証明書プロファイルを作成し、それをユーザーアカウント、ユーザーグループ、またはデバイスグループに割り当てます。デバイスにクライアント証明書を送信するには、SCEP プロファイル、共有証明書プロファイル、またはユーザー資格情報プロファイルを作成し、それを Wi-Fi プロファイルに関連付けます。
  メモ：Samsung Knox Workspace デバイスは、Wi-Fi 認証のために BlackBerry UEM によってデバイスに送信された証明書の使用をサポートしていません。ユーザーは、Samsung Knox Workspace デバイスで証明書ベースの認証を手動でセットアップする必要があります。
- 仕事用 Wi-Fi 接続にプロキシサーバーを使用する BlackBerry 10、iOS、macOS、Android Enterprise、および Samsung Knox デバイスの場合は、プロキシプロファイルを作成して Wi-Fi プロファイルに関連付けます。
- BlackBerry 10 デバイスが仕事用 Wi-Fi 接続で VPN を使用している場合は、VPN プロファイルを作成して Wi-Fi プロファイルに関連付けます。

1. メニューバーで［ポリシーとプロファイル］をクリックします。
2. ［ネットワークと接続］ > ［**Wi-Fi**］をクリックします。
3. ＋ をクリックします。
4. Wi-Fi プロファイルの名前と説明を入力します。この情報はデバイスに表示されます。
5. ［**SSID**］フィールドに Wi-Fi ネットワークのネットワーク名を入力します。
6. Wi-Fi ネットワークが SSID をブロードキャストしない場合は、［非表示のネットワーク］チェックボックスをオンにします。
7. 次の操作を実行します。
   a) デバイスタイプのタブをクリックします。
   b) 組織の環境内の Wi-Fi 設定と一致するように、各プロファイル設定に適切な値を設定します。組織により、Wi-Fi ネットワークに接続する際にユーザーがユーザー名とパスワードを入力することが義務付けられていて、かつプロファイルが複数のユーザーに対応している場合は、［ユーザー名］フィールドに「`%UserName%`」を入力します。
8. 組織内のデバイスタイプごとに手順 7 を繰り返します。
9. ［追加］をクリックします。

Wi-Fi プロファイル設定

実際の値を指定するのではなく、値を参照するためにテキストフィールドになっているプロファイル設定では、変数を使用できます。Wi-Fi プロファイルは、以下のデバイスタイプでサポートされています。

- iOS
- macOS
- Android
- Windows
- BlackBerry 10

共通：Wi-Fi プロファイル設定

共通：**Wi-Fi** プロファイル設定	説明
SSID	この設定は、Wi-Fi ネットワークのネットワーク名およびそのワイヤレスアクセスポイントを指定します。SSID は大文字と小文字を区別し、英数字を含んでいる必要があります。 使用できる値は 32 文字までに制限されています。
非表示のネットワーク	この設定では、Wi-Fi ネットワークで SSID を非表示にするかどうかを指定します。

iOS および macOS ：Wi-Fi プロファイル設定

macOS は、ユーザーアカウントまたはデバイスにプロファイルを適用します。どちらか一方に適用する Wi-Fi プロファイルを設定できます。

iOSおよび **macOS**：**Wi-Fi** プロファイル設定	説明
プロファイルを適用	この設定では、macOS デバイス上の Wi-Fi プロファイルをユーザーアカウントまたはデバイスに適用するかどうかを指定します。 使用できる値： • ユーザー • デバイス この設定は macOS に対してのみ有効です。
自動的にネットワークへ参加	この設定では、デバイスが Wi-Fi ネットワークに自動的に参加できるかどうかを指定します。
関連付けられているプロキシプロファイル	この設定では、デバイスが Wi-Fi ネットワークに接続されている場合に、プロキシサーバーへの接続で使用するために関連付けられるプロキシプロファイルを指定します。

iOSおよび **macOS**：**Wi-Fi** プロファイル設定	説明
ネットワークタイプ	この設定では、Wi-Fi ネットワークの設定を指定します。 Hotspot 設定は iOS および macOS デバイスにのみ適用されます。Android および BlackBerry 10 デバイスに Wi-Fi を設定するには、個別の Wi-Fi プロファイルを作成する必要があります。 使用できる値： • 標準 • レガシーホットスポット • Hotspot 2.0 デフォルト値は［標準］です。
表示される事業者名	この設定では、ホットスポット事業者のわかりやすい名前を指定します。 この設定は、［ネットワークタイプ］が［Hotspot 2.0］に設定されている場合のみ有効です。
ドメイン名	この設定では、ホットスポット事業者のドメイン名を指定します。 この設定は、［ネットワークタイプ］が［Hotspot 2.0］に設定されている場合のみ有効です。 この設定を使用する場合、［SSID］設定は必要ありません。
ローミングコンソーシアム OI	この設定では、ホットスポット経由でアクセス可能なローミングコンソーシアムと通信事業者の組織 ID を指定します。 この設定は、［ネットワークタイプ］が［Hotspot 2.0］に設定されている場合のみ有効です。
NAI 領域名	この設定では、iOS デバイスを認証できる NAI 領域名を指定します。 この設定は、［ネットワークタイプ］が［Hotspot 2.0］に設定されている場合のみ有効です。
MCC/MNC	この設定では、モバイルネットワークオペレーターを識別する MCC/MNC の組み合わせを指定します。各値には正確に 6 桁を含める必要があります。 この設定は、［ネットワークタイプ］が［Hotspot 2.0］に設定されている場合のみ有効です。
ローミングパートナーネットワークへの接続を許可する	この設定では、デバイスがホットスポットのローミングパートナーに接続できるかどうかを指定します。 この設定は、［ネットワークタイプ］が［Hotspot 2.0］に設定されている場合のみ有効です。

iOSおよび **macOS**：**Wi-Fi** プロファイル設定	説明
セキュリティの種類	この設定では、Wi-Fi ネットワークが使用するセキュリティの種類を指定します。 ［ネットワークタイプ］が［Hotpost 2.0］に設定されている場合は、この設定に［WPA2-Enterprise ］を指定します。 使用できる値： • None • WEP 個人 • WEP エンタープライズ • WPA-Personal • WPA-Enterprise • WPA2-Personal • WPA2-Enterprise • WPA3-Personal • WPA3-Enterprise デフォルト値は［なし］です。
WEP キー	この設定では、Wi-Fi ネットワークの WEP キーを指定します。WEP キーは 10 または 26 桁の 16 進数値（0〜9、A〜F）、もしくは 5 または 13 文字の英数字（0〜9、A〜Z）にする必要があります。 16 進数キー値の例は、ABCDEF0123 または ABCDEF0123456789ABCDEF0123 です。英数字キー値の例は、abCD5 または abCDefGHijKL1 です。 この設定は、［セキュリティの種類］が［WEP 個人］に設定されている場合のみ有効です。
事前共有キー	この設定では、Wi-Fi ネットワークの事前共有キーを指定します。 この設定は、［セキュリティの種類］が［WPA-Personal ］、［WPA2-Personal ］または［WPA3-Personal］に設定されている場合のみ有効です。
プロトコル	

iOSおよび **macOS**：**Wi-Fi** プロファイル設定	説明
認証プロトコル	この設定では、Wi-Fi ネットワークがサポートする EAP 方法を指定します。複数の EAP 方法を選択できます。 この設定は、［セキュリティの種類］が［WEP エンタープライズ］、［WPA-Enterprise ］、［WPA2-Enterprise ］または［WPA3-Enterprise］に設定されている場合のみ有効です。 次の中から選択します。 • TLS • TTLS • LEAP • PEAP • EAP-FAST • EAP-SIM
内部認証	この設定では、TTLS で使用する内部認証方式を指定します。 この設定は、［認証プロトコル］が［TTLS］に設定されている場合のみ有効です。 使用できる値： • None • PAP • CHAP • MS-CHAP • MS-CHAPv2 • EAP デフォルト値は［MS-CHAPv2］です。
PAC を使用	この設定では、EAP-FAST 方式が Protected Access の資格情報を使用するかどうかを指定します。 この設定は、［認証プロトコル］が［EAP-FAST］に設定されている場合のみ有効です。
PAC をプロビジョニング	この設定では、EAP-FAST 方式が PAC プロビジョニングを許可するかどうかを指定します。 この設定は、［認証プロトコル］が［EAP-FAST］に設定され、［PAC を使用］設定が選択されている場合のみ有効です。
匿名で PAC をプロビジョニング	この設定では、EAP-FAST 方式が匿名の PAC プロビジョニングを許可するかどうかを指定します。 この設定は、［認証プロトコル］が［EAP-FAST］に設定され、［PAC を使用］設定が選択され、さらに［PAC をプロビジョニング］設定が選択されている場合のみ有効です。

iOSおよび **macOS**：**Wi-Fi** プロファイル設定	説明
認証	
TTLS、PEAP、および EAP-FAST の外部 ID	この設定では、クリアテキストで送信されるユーザーの外部 ID を指定します。ユーザーの実際の ID を非表示にするために匿名のユーザー名を指定できます（たとえば、anonymous）。Wi-Fi ネットワークでの認証を受けるために、暗号化されたトンネルを使用して実際のユーザー名が送信されます。外部 ID に要求のルーティング先の領域名を含める場合は、ユーザーの実際の領域（たとえば、anonymous@example.com）にする必要があります。 この設定は、［認証プロトコル］が［TTLS］、［PEAP］、または［EAP-FAST］に設定されている場合のみ有効です。
Wi-Fi プロファイルに含まれるパスワードを使用	この設定では、Wi-Fi プロファイルに認証用のパスワードを含めるかどうかを指定します。 この設定は、［セキュリティの種類］が［WEP エンタープライズ］、［WPA-Enterprise ］、［WPA2-Enterprise ］または［WPA3-Enterprise］に設定されている場合のみ有効です。
パスワード	この設定では、iOS デバイスが Wi-Fi ネットワーク認証に使用するパスワードを指定します。 この設定は、［Wi-Fi プロファイルに含まれるパスワードを使用］設定が選択されている場合のみ有効です。
ユーザー名	この設定では、iOS デバイスが Wi-Fi ネットワーク認証に使用するユーザー名を指定します。プロファイルが複数のユーザーに対応している場合は、%UserName% 変数を指定できます。 この設定は、［セキュリティの種類］が［WEP エンタープライズ］、［WPA-Enterprise ］、［WPA2-Enterprise ］または［WPA3-Enterprise］に設定されている場合のみ有効です。
認証の種類	この設定では、デバイスが Wi-Fi ネットワークに接続する際に使用する認証タイプを指定します。 この設定は、［セキュリティの種類］が［WEP エンタープライズ］、［WPA-Enterprise ］、［WPA2-Enterprise ］または［WPA3-Enterprise］に設定されている場合のみ有効です。 使用できる値： • None • 共有証明書 • SCEP • ユーザー資格情報 デフォルト値は［なし］です。

iOSおよび **macOS**：**Wi-Fi** プロファイル設定	説明
証明書リンクの種類	この設定では、Wi-Fi プロファイルに関連付けられるクライアント証明書のリンクの種類を指定します。 この設定は、［認証の種類］が［共有証明書］に設定されている場合のみ有効です。 使用できる値： • 単一参照 • 可変インジェクション デフォルト値は［単一参照］です。
共有証明書プロファイル	この設定では、デバイスが Wi-Fi ネットワーク認証に使用するクライアント証明書を含む共有証明書プロファイルを指定します。 この設定は、［証明書リンクの種類］が［単一参照］に設定されている場合のみ有効です。
クライアント証明書名	この設定では、デバイスが Wi-Fi ネットワーク認証に使用するクライアント証明書の名前を指定します。 この設定は、［証明書リンクの種類］が［可変インジェクション］に設定されている場合のみ有効です。
関連付けられた SCEP プロファイル	この設定では、Wi-Fi ネットワークを認証するクライアント証明書を取得する際にデバイスが使用する、関連付けられた SCEP プロファイルを指定します。 この設定は、［認証の種類］が［SCEP］に設定されている場合のみ有効です。
関連付けられたユーザー資格情報プロファイル	この設定では、デバイスが Wi-Fi ネットワークで認証するクライアント証明書を取得する際にデバイスが使用する、関連付けられたユーザー資格情報プロファイルを指定します。 この設定は、［認証の種類］が［ユーザー資格情報］に設定されている場合のみ有効です。
信頼する	
認証サーバーが想定している証明書共通名	この設定では、認証サーバーがデバイスに送信する証明書の共通名を指定します（たとえば、*.example.com）。 この設定は、［セキュリティの種類］が［WEP エンタープライズ］、［WPA-Enterprise ］、［WPA2-Enterprise ］または［WPA3-Enterprise］に設定されている場合のみ有効です。

iOSおよび **macOS**：**Wi-Fi** プロファイル設定	説明
証明書リンクの種類	この設定では、Wi-Fi プロファイルに関連付けられる信頼済み証明書のリンクの種類を指定します。 この設定は、［セキュリティの種類］が［WEP エンタープライズ］、［WPA-Enterprise ］、［WPA2-Enterprise ］または［WPA3-Enterprise］に設定されている場合のみ有効です。 使用できる値： • 単一参照 • 可変インジェクション デフォルト値は［単一参照］です。
CA 証明書プロファイル	この設定では、デバイスが Wi-Fi ネットワークとの信頼を確立するために使用する、信頼済み証明書を備えた CA 証明書プロファイルを指定します。 この設定は、［証明書リンクの種類］が［単一参照］に設定されている場合のみ有効です。
信頼済み証明書名	この設定では、デバイスが Wi-Fi ネットワークとの信頼を確立する際に使用する、信頼済み証明書の名前を指定します。 この設定は、［証明書リンクの種類］が［可変インジェクション］に設定されている場合のみ有効です。
ユーザーの判断を信頼する	この設定では、デバイスが、信頼チェーンを確立できない場合に、ユーザーにサーバを信頼するよう要求するかどうかを指定します。この設定が選択されていない場合、指定した信頼済みサーバーへの接続のみが許可されます。 この設定は、［セキュリティの種類］が［WEP エンタープライズ］、［WPA-Enterprise ］、［WPA2-Enterprise ］または［WPA3-Enterprise］に設定されている場合のみ有効です。
キャプティブネットワークのバイパス	この設定では、デバイスがキャプティブネットワークをバイパスできるかどうかを指定します。
QoS マーキングプロファイルを有効にする	この設定では、Wi-Fi ネットワーク経由で送信されるトラフィックに対して、L2 および L3 マーキングを有効にできるかどうかを指定します。
FaceTime コールに QoS を使用する	この設定では、FaceTime コールの音声およびビデオトラフィックに L2 および L3 マーキングを使用できるかどうかを指定します。
QoS トラフィックには L2 マーキングのみを使用する	この設定では、Wi-Fi ネットワーク経由で送信されるトラフィックで、L2 マーキングのみを使用するかどうかを指定します。
選択したアプリに QoS マーキングを適用する	この設定では、L2 および L3 マーキングを使用できるアプリのバンドル ID を指定します。

Android ：Wi-Fi プロファイル設定

Android ：Wi-Fi プロファイル設定	説明
関連付けられているプロキシプロファイル	この設定では、Android デバイスが Wi-Fi ネットワークに接続されている場合に、プロキシサーバーに接続するために使用する関連付けられているプロキシプロファイルを指定します。 Android 8.0 以降のデバイスで、アクティベーションが MDM 制御 または ユーザーのプライバシー のデバイスは、プロキシ設定が含まれる Wi-Fi プロファイルをサポートしていません。これらのいずれかのアクティベーションタイプのデバイスを Android 8.0 にアップグレードすると、プロキシプロファイルが関連付けられている Wi-Fi プロファイルは、デバイスから削除されます。
BSSID	この設定では、Wi-Fi ネットワーク内のワイヤレスアクセスポイントの MAC アドレスを指定します。
プライマリ DNS	この設定では、ドット付き 10 進表記（たとえば、192.0.2.0）でプライマリ DNS サーバーを指定します。 この設定は、IP アドレスが組織のネットワークに静的に割り当てられている場合に、Samsung Knox を使用するデバイスのみに適用されます。
セカンダリ DNS	この設定では、ドット付き 10 進表記（たとえば、192.0.2.0）でセカンダリ DNS サーバーを指定します。 この設定は、IP アドレスが組織のネットワークに静的に割り当てられている場合に、Samsung Knox を使用するデバイスのみに適用されます。
セキュリティの種類	この設定では、Wi-Fi ネットワークが使用するセキュリティの種類を指定します。 使用できる値： • None • 個人 • エンタープライズ デフォルト値は［なし］です。
パーソナルセキュリティの種類	この設定では、Wi-Fi ネットワークが使用するパーソナルセキュリティの種類を指定します。 この設定は、［セキュリティの種類］が［個人］に設定されている場合のみ有効です。 使用できる値： • None • WEP 個人 • WPA-Personal/WPA2-Personal デフォルト値は［なし］です。

Android ：**Wi-Fi** プロファイル設定	説明
WEP キー	この設定では、Wi-Fi ネットワークの WEP キーを指定します。WEP キーは 10 または 26 桁の 16 進数値（0〜9、A〜F）、もしくは 5 または 13 文字の英数字（0〜9、A〜Z）にする必要があります。 16 進数キー値の例は、ABCDEF0123 または ABCDEF0123456789ABCDEF0123 です。英数字キー値の例は、abCD5 または abCDefGHijKL1 です。 この設定は、［パーソナルセキュリティの種類］が［WEP 個人］に設定されている場合のみ有効です。
事前共有キー	この設定では、Wi-Fi ネットワークの事前共有キーを指定します。 この設定は、［パーソナルセキュリティの種類］が［WPA-Personal/WPA2-Personal ］に設定されている場合のみ有効です。
認証プロトコル	この設定では、Wi-Fi ネットワークが使用する EAP 方法を指定します。 この設定は、［セキュリティの種類］が［エンタープライズ］に設定されている場合のみ有効です。 使用できる値： • TLS • TTLS • PEAP • LEAP デフォルト値は［TLS］です。 LEAP は、Samsung Knox を使用するデバイスではサポートされません。
内部認証	この設定では、TTLS で使用する内部認証方式を指定します。 この設定は、［認証プロトコル］が［TTLS］に設定されている場合のみ有効です。 使用できる値： • None • PAP • CHAP • MS-CHAP • MS-CHAPv2 • GTC デフォルト値は［MS-CHAPv2］です。 CHAP は、Samsung Knox を使用するデバイスではサポートされません。

Android ：**Wi-Fi** プロファイル設定	説明
TTLS の外部 ID	この設定では、クリアテキストで送信されるユーザーの外部 ID を指定します。ユーザーの実際の ID を非表示にするために匿名のユーザー名を指定できます（たとえば、anonymous）。Wi-Fi ネットワークでの認証を受けるために、暗号化されたトンネルを使用して実際のユーザー名が送信されます。外部 ID に要求のルーティング先の領域名を含める場合は、ユーザーの実際の領域（たとえば、anonymous@example.com）にする必要があります。 この設定は、［認証プロトコル］が［TTLS］に設定されている場合のみ有効です。
PEAP の外部 ID	この設定では、クリアテキストで送信されるユーザーの外部 ID を指定します。ユーザーの実際の ID を非表示にするために匿名のユーザー名を指定できます（たとえば、anonymous）。Wi-Fi ネットワークでの認証を受けるために、暗号化されたトンネルを使用して実際のユーザー名が送信されます。外部 ID に要求のルーティング先の領域名を含める場合は、ユーザーの実際の領域（たとえば、anonymous@example.com）にする必要があります。 この設定は、［認証プロトコル］が［PEAP］に設定されている場合のみ有効です。
ユーザー名	この設定では、Android デバイスが Wi-Fi ネットワーク認証に使用するユーザー名を指定します。プロファイルが複数のユーザーに対応している場合は、%UserName% 変数を指定できます。 この設定は、［セキュリティの種類］が［エンタープライズ］に設定されている場合のみ有効です。
Wi-Fi プロファイルに含まれるパスワードを使用	この設定では、Wi-Fi プロファイルに認証用のパスワードを含めるかどうかを指定します。 この設定は、［セキュリティの種類］が［エンタープライズ］に設定されている場合のみ有効です。
パスワード	この設定では、Android デバイスが Wi-Fi ネットワーク認証に使用するパスワードを指定します。 この設定は、［Wi-Fi プロファイルに含まれるパスワードを使用］設定が選択されている場合のみ有効です。

Android ：**Wi-Fi** プロファイル設定	説明
認証の種類	この設定では、Android デバイスが Wi-Fi ネットワークに接続するために使用する認証タイプを指定します。 この設定は、［セキュリティの種類］が［エンタープライズ］に設定されている場合のみ有効です。 使用できる値： • None • 共有証明書 • SCEP • ユーザー資格情報 デフォルト値は［なし］です。
証明書リンクの種類	この設定では、Wi-Fi プロファイルに関連付けられるクライアント証明書のリンクの種類を指定します。 この設定は、［認証の種類］が［共有証明書］に設定されている場合のみ有効です。 使用できる値： • 単一参照 • 可変インジェクション デフォルト値は［単一参照］です。
共有証明書プロファイル	この設定では、Android デバイスが Wi-Fi ネットワーク認証に使用するクライアント証明書を含む共有証明書プロファイルを指定します。 この設定は、［証明書リンクの種類］が［単一参照］に設定されている場合のみ有効です。 Knox Workspace を使用するデバイスの共有証明書プロファイル名は、36 文字未満である必要があります。
関連付けられた SCEP プロファイル	この設定では、Android デバイスが Wi-Fi ネットワーク認証に使用するクライアント証明書を取得するための関連付けられた SCEP プロファイルを指定します。 この設定は、［認証の種類］が［SCEP］に設定されている場合のみ有効です。 Knox Workspace を使用するデバイスの SCEP プロファイル名は、36 文字未満である必要があります。

Android ：**Wi-Fi** プロファイル設定	説明
関連付けられたユーザー資格情報プロファイル	この設定では、Android デバイスが Wi-Fi ネットワーク認証に使用するクライアント証明書を取得するための関連付けられたユーザー資格情報プロファイルを指定します。 この設定は、［認証の種類］が［ユーザー資格情報］に設定されている場合のみ有効です。 Knox Workspace を使用するデバイスのユーザー資格情報プロファイル名は、36 文字未満である必要があります。
クライアント証明書名	この設定では、Android デバイスが Wi-Fi ネットワーク認証に使用するクライアント証明書の名前を指定します。 この設定は、［証明書リンクの種類］が［可変インジェクション］に設定されている場合のみ有効です。
認証サーバーが想定している証明書共通名	この設定では、認証サーバーがデバイスに送信する証明書の共通名を指定します（たとえば、*.example.com）。 この設定は、［セキュリティの種類］が［エンタープライズ］に設定されている場合のみ有効です。
証明書リンクの種類	この設定では、Wi-Fi プロファイルに関連付けられる信頼済み証明書のリンクの種類を指定します。 この設定は、［セキュリティの種類］が［エンタープライズ］に設定されている場合のみ有効です。 使用できる値： • 単一参照 • 可変インジェクション デフォルト値は［単一参照］です。
CA 証明書プロファイル	この設定では、Android デバイスが Wi-Fi ネットワークとの信頼を確立するために使用する信頼済み証明書を備えた CA 証明書プロファイルを指定します。 この設定は、［証明書リンクの種類］が［単一参照］に設定されている場合のみ有効です。
信頼済み証明書名	この設定では、Android デバイスが Wi-Fi ネットワークとの信頼を確立するために使用する信頼済み証明書の名前を指定します。 この設定は、［証明書リンクの種類］が［可変インジェクション］に設定されている場合のみ有効です。

Windows ：Wi-Fi プロファイル設定

Windows ：Wi-Fi プロファイル設定	説明
このネットワークが範囲内の場合に自動的に接続する	この設定では、デバイスが Wi-Fi ネットワークに自動的に接続できるかどうかを指定します。
セキュリティの種類	この設定では、Wi-Fi ネットワークが使用するセキュリティの種類を指定します。 使用できる値： • オープン • WPA-Enterprise • WPA-Personal • WPA2-Enterprise • WPA2-Personal デフォルト値は［オープン］です。
暗号化の種類	この設定では、Wi-Fi ネットワークが使用する暗号化方式を指定します。 ［セキュリティタイプ］設定によって、サポートされる暗号化の種類と、この設定のデフォルト値が決定されます。 使用できる値： • None • WEP • TKIP • AES
WEP キー	この設定では、Wi-Fi ネットワークの WEP キーを指定します。WEP キーは 10 または 26 桁の 16 進数値（0〜9、A〜F）、もしくは 5 または 13 文字の英数字（0〜9、A〜Z）にする必要があります。 16 進数キー値の例は、ABCDEF0123 または ABCDEF0123456789ABCDEF0123 です。英数字キー値の例は、abCD5 または abCDefGHijKL1 です。 この設定は、［セキュリティタイプ］が［オープン］に設定され、［認証の種類］が［WEP］に設定されている場合にのみ有効です。
キーのインデックス	この設定では、ワイヤレスアクセスポイントに保存されている照合キーの場所を指定します。 この設定は、［セキュリティタイプ］が［オープン］に設定され、［認証の種類］が［WEP］に設定されている場合にのみ有効です。 使用できる値は 1〜4 です。 デフォルト値は、［2］です。

Windows ：Wi-Fi プロファイル設定	説明
事前共有キー	この設定では、Wi-Fi ネットワークの事前共有キーを指定します。 この設定は、［セキュリティタイプ］が［WPA-Personal ］に設定されている場合のみ有効です。
シングルサインオンを有効にする	この設定では、Wi-Fi ネットワークがシングルサインオン認証をサポートするかどうかを指定します。 この設定は、［セキュリティの種類］が［WPA-Enterprise ］または［WPA2-Enterprise ］に設定されている場合のみ有効です。
シングルサインオンのタイプ	この設定では、シングルサインオン認証を実行するタイミングを指定します。［ユーザーログインの直前に実行］に設定すると、ユーザーが組織の Active Directory にログインする前にシングルサインオンが実行されます。［ユーザーログインの直後に実行］に設定すると、ユーザーが組織の Active Directory にログインした後にシングルサインオンが実行されます。 この設定は、［シングルサインオンを有効にする］設定が選択されている場合のみ有効です。 使用できる値： • ユーザーログインの直前に実行 • ユーザーログインの直後に実行 デフォルト値は、［ユーザーログインの直前に実行］です。
接続の最大遅延	この設定では、シングルサインオンの接続試行が失敗するまでの遅延の最大時間（秒単位）を指定します。 この設定は、［シングルサインオンを有効にする］設定が選択されている場合のみ有効です。 使用できる値は、0〜120 秒です。 デフォルト値は［10 秒］です。
シングルサインオン時に追加のダイアログの表示を許可する	この設定では、デバイスがログイン画面の域を超えてダイアログボックスを表示できるかどうかを指定します。たとえば、EAP 認証が、認証時にサーバーから送信された証明書を確認するようにユーザーに要求する種類の場合、デバイスはダイアログボックスを表示できます。 この設定は、［シングルサインオンを有効にする］設定が選択されている場合のみ有効です。

Windows ：Wi-Fi プロファイル設定	説明
このネットワークではマシンとユーザーの認証用に個別の仮想 LAN を使用する	この設定では、デバイスが使用する VLAN をユーザーのログイン情報に基づいて変更するかどうかを指定します。たとえば、デバイスが起動時にある VLAN 上に存在し、その後、ユーザーのログイン後にユーザー権限に基づいて別の VLAN ネットワークに移行する場合があります。 この設定は、［シングルサインオンを有効にする］設定が選択されている場合のみ有効です。
サーバー証明書を検証	この設定では、デバイスが、ワイヤレスアクセスポイントの ID を実証するサーバー証明書を検証する必要があるかどうかを指定します。 この設定は、［セキュリティの種類］が［WPA-Enterprise ］または［WPA2-Enterprise ］に設定されている場合のみ有効です。
ユーザーに新しいサーバーまたは信頼済み認証局の承認を求めない	この設定では、ユーザーにサーバー証明書を信頼するように要求するかどうかを指定します。 この設定は、［サーバー証明書を検証］設定が選択されている場合のみ有効です。
CA 証明書プロファイル	この設定では、ワイヤレスアクセスポイントが使用するサーバー証明書の信頼の基点（Root of Trust）を提供する CA 証明書プロファイルを指定します。 この設定は、デバイスが信頼するルート CA を選択された CA に限定します。信頼済みルート CA を選択しない場合、デバイスは信頼済みルート認証局ストアに一覧されたすべてのルート CA を信頼します。 この設定は、［サーバー証明書を検証］設定が選択されている場合のみ有効です。
高速再接続を有効にする	この設定では、Wi-Fi ネットワークが、複数のワイヤレスアクセスポイントにわたる PEAP 認証のための高速再接続をサポートするかどうかを指定します。 この設定は、［セキュリティの種類］が［WPA-Enterprise ］または［WPA2-Enterprise ］に設定されている場合のみ有効です。
NAP を強制する	この設定では、ネットワークへの接続を許可する前に、デバイスがヘルス要件を満たしていることを確認するために、Wi-Fi ネットワークで NAP を使用してデバイスのシステムヘルスチェックを実行するかどうかを指定します。 この設定は、［セキュリティの種類］が［WPA-Enterprise ］または［WPA2-Enterprise ］に設定されている場合のみ有効です。
FIPS モードを有効にする	この設定は、Wi-Fi ネットワークが FIPS 140-2 標準へのコンプライアンスをサポートするかどうかを指定します。 この設定は、［セキュリティタイプ］が［WPA2 エンタープライズ］または［WPA2 パーソナル］に設定され、［暗号化の種類］が［AES］に設定されている場合にのみ有効です。

Windows ：Wi-Fi プロファイル設定	説明
PMK キャッシュを有効にする	この設定では、デバイスが WPA2 高速ローミングを有効にするために PMK をキャッシュできるかどうかを指定します。高速ローミングでは、デバイスが以前に認証したワイヤレスアクセスポイントでの 802.1X 設定をスキップします。 この設定は、［セキュリティタイプ］が［WPA2-Enterprise］に設定されている場合のみ有効です。
PMK の有効期間	この設定では、デバイスが PMK をキャッシュに保存できる期間（分数）を指定します。 この設定は、［PMK キャッシュを有効にする］設定が選択されている場合のみ有効です。 使用できる値は、5〜1440 分です。 デフォルト値は 720 分です。
PMK キャッシュのエントリ数	この設定では、デバイスがキャッシュに保存できる PMK エントリの最大数を指定します。 この設定は、［PMK キャッシュを有効にする］設定が選択されている場合のみ有効です。 使用できる値は 1〜255 です。 デフォルト値は、［128］です。
このネットワークでは事前認証を使用する	この設定では、アクセスポイントが WPA2 高速ローミングの事前認証をサポートするかどうかを指定します。 事前認証によって、1 つのワイヤレスアクセスポイントに接続しているデバイスが、その範囲内の他のワイヤレスアクセスポイントで 802.1X 設定を実行できます。事前認証では、PMK と関連付けられた情報が PMK キャッシュに保存されます。デバイスが事前認証済みのワイヤレスアクセスポイントに接続する場合は、キャッシュされた PMK 情報を使用して、認証と接続に要する時間を短縮できます。 この設定は、［PMK キャッシュを有効にする］設定が選択されている場合のみ有効です。
事前認証の最大試行回数	この設定では、許容される事前認証の最大試行回数を指定します。 この設定は、［このネットワークでは事前認証を使用する］設定が選択されている場合のみ有効です。 使用できる値は 1〜16 です。 デフォルト値は、［3］です。

Windows ：Wi-Fi プロファイル設定	説明
プロキシの種類	この設定では、Wi-Fi プロファイルのプロキシ設定のタイプを指定します。 使用できる設定： • None • PAC 設定 • 手動設定 • Web Proxy Autodiscovery デフォルト設定は、［手動設定］です。 この設定は Windows 10 Mobile デバイスにのみ適用されます。
PAC URL	この設定では、PAC ファイルをホストしている Web サーバーの URL と PAC ファイル名を、http://<Web サーバー URL>/<ファイル名>.pac の形式で指定します。 この設定は、［プロキシの種類］設定が［PAC 設定］に設定されている場合のみ有効です。
アドレス	この設定は、ネットワークプロキシのサーバー名とポートを指定します。「ホスト:ポート」の形式を使用します（例、server01.example.com:123）。ホストは次のいずれかの形式である必要があります。 • 登録済みの名前（サーバー名など）、FQDN、または単一ラベル名（server01.example.com ではなく、server01 など） • IPv4 または IPv6 アドレス この設定は、［プロキシの種類］設定が［手動設定］に設定されている場合のみ有効です。
Web Proxy Autodiscovery	この設定は、プロキシ検索に Web Proxy Autodiscovery Protocol（WPAD）を有効にするかどうかを指定します。 この設定は、［プロキシの種類］設定が［Web Proxy Autodiscover］に設定されている場合のみ有効です。 デフォルトでは、このチェックボックスはオフです。
インターネット接続のチェックをオフにする	この設定は、インターネット接続のチェックをオフにするかどうかを指定します。 デフォルトでは、このチェックボックスはオフです。
関連付けられた SCEP プロファイル	この設定では、Wi-Fi ネットワークを認証するクライアント証明書を取得する際にデバイスが使用する、関連付けられた SCEP プロファイルを指定します。

BlackBerry 10 ：Wi-Fi プロファイル設定

BlackBerry 10 ：Wi-Fi プロファイル設定	説明
セキュリティの種類	この設定では、Wi-Fi ネットワークが使用するセキュリティの種類を指定します。 使用できる値： • None • WEP 個人 • WPA-Personal • WPA-Enterprise • WPA2-Personal • WPA2-Enterprise デフォルト値は［なし］です。
WEP キー	この設定では、Wi-Fi ネットワークの WEP キーを指定します。WEP キーは 10 または 26 桁の 16 進数値（0〜9、A〜F）、もしくは 5 または 13 文字の英数字（0〜9、A〜Z）にする必要があります。 16 進数キー値の例は、ABCDEF0123 または ABCDEF0123456789ABCDEF0123 です。英数字キー値の例は、abCD5 または abCDefGHijKL1 です。 この設定は、［セキュリティの種類］が［WEP 個人］に設定されている場合のみ有効です。
事前共有キーの種類	この設定では、Wi-Fi ネットワークの事前共有キーの種類を指定します。 この設定は、［セキュリティの種類］が［WPA-Personal ］または［WPA2-Personal ］に設定されている場合のみ有効です。 使用できる値： • ASCII • HEX デフォルト値は［ASCII］です。
事前共有キー	この設定では、Wi-Fi ネットワークの事前共有キーを指定します。 この設定は、［セキュリティの種類］が［WPA-Personal ］または［WPA2-Personal ］に設定されている場合のみ有効です。 使用できる値は 64 文字までに制限されています。

BlackBerry 10 ：Wi-Fi プロファイル設定	説明
認証プロトコル	この設定では、Wi-Fi ネットワークが使用する EAP 方法を指定します。 この設定は、［セキュリティの種類］が［WPA-Enterprise ］または［WPA2-Enterprise ］に設定されている場合のみ有効です。 使用できる値： • PEAP • TTLS • EAP-FAST • TLS デフォルト値は［PEAP］です。
内部認証	この設定では、TLS トンネルで使用する内部認証方式を指定します。 内部認証に PAP を使用する場合は、この設定に［自動］を指定します。 この設定は、［認証プロトコル］が［PEAP］または［TTLS］に設定されている場合のみ有効です。 使用できる値： • 自動 • MS-CHAPv2 • GTC デフォルト値は［自動］です。
EAP-FAST プロビジョニング方式	この設定では、EAP-FAST 認証のプロビジョニング方式を指定します。 この設定は、［認証プロトコル］が［EAP-FAST］に設定されている場合のみ有効です。 使用できる値： • 匿名 • 認証済み デフォルト値は［匿名］です。
ユーザー名	この設定では、BlackBerry 10 デバイスが Wi-Fi ネットワーク認証に使用するユーザー名を指定します。プロファイルが複数のユーザーに対応している場合は、%UserName% 変数を指定できます。 この設定は、［認証プロトコル］が［PEAP］、［TTLS］、［EAP-FAST］、または［TLS］に設定されている場合のみ有効です。
パスワード	この設定では、BlackBerry 10 デバイスが Wi-Fi ネットワーク認証に使用するパスワードを指定します。 この設定は、［認証プロトコル］が［PEAP］、［TTLS］、または［EAP-FAST］に設定されている場合のみ有効です。

BlackBerry 10 ：Wi-Fi プロファイル設定	説明
バンドの種類	この設定では、Wi-Fi ネットワークが使用する周波数を指定します。 使用できる値： • デュアル • 2.4 GHz • 5.0 GHz デフォルト値は［デュアル］です。
DHCP を有効にする	この設定では、Wi-Fi ネットワークが DHCP を使用するかどうかを指定します。
IP アドレス	この設定では、Wi-Fi ネットワークのホストの IP アドレスを指定します。 この設定は、［DHCP を有効にする］設定が選択されていない場合のみ有効です。
サブネットマスク	この設定では、ドット付き 10 進表記（たとえば、192.0.2.0）でサブネットマスクを指定します。 この設定は、［DHCP を有効にする］設定が選択されていない場合のみ有効です。
プライマリ DNS	この設定では、ドット付き 10 進表記（たとえば、192.0.2.0）でプライマリ DNS サーバーを指定します。 この設定は、［DHCP を有効にする］設定が選択されていない場合のみ有効です。
セカンダリ DNS	この設定では、ドット付き 10 進表記（たとえば、192.0.2.0）でセカンダリ DNS サーバーを指定します。 この設定は、［DHCP を有効にする］設定が選択されていない場合のみ有効です。
デフォルトゲートウェイ	この設定では、ドット付き 10 進表記（たとえば、192.0.2.0）でデフォルトゲートウェイを指定します。 この設定は、［DHCP を有効にする］設定が選択されていない場合のみ有効です。
ドメインサフィックス	この設定では、DNS サフィックスの FQDN を指定します。 この設定は、［DHCP を有効にする］設定が選択されていない場合のみ有効です。
IPv6 を有効にする	この設定では、Wi-Fi ネットワークが IPv6 をサポートするかどうかを指定します。
アクセスポイントのハンドオーバーを有効にする	この設定は、BlackBerry 10 デバイスでワイヤレスアクセスポイント間の Wi-Fi ハンドオーバーを実行できるようにするかどうかを指定します。

BlackBerry 10 ：Wi-Fi プロファイル設定	説明
ユーザーが編集可能	この設定では、BlackBerry 10 デバイスユーザーが変更できる Wi-Fi 設定を指定します。これが［読み取り専用］に設定されている場合、ユーザーはどの設定も変更できません。これが［資格情報のみ］に設定されている場合、ユーザーはユーザー名とパスワードを変更できます。 使用できる値： • 読み取り専用 • 資格情報のみ デフォルト値は［読み取り専用］です。
データセキュリティレベル	この設定では、仕事用領域が高度な保存データ保護を使用している場合に、Wi-Fi プロファイルが保存される仕事用領域内のドメインを指定します。この設定は、［高度な保存データ保護を強制する］IT ポリシールールが選択されている場合にのみ有効です。これが［常時使用可能］に設定されている場合、プロファイルは起動（Startup）ドメインに保存され、仕事用領域がロックされている場合に使用できます。これが［認証後に使用可能］に設定されている場合、プロファイルは操作（Operational）ドメインに保存され、仕事用領域がロック解除された後、デバイスが再起動されるまで使用可能です。これが［仕事用領域がロック解除された場合のみ使用可能］に設定されている場合、プロファイルはロック（Lock）ドメインに保存され、仕事用領域がロック解除されている場合のみ Wi-Fi 接続用に使用できます。 使用できる値： • 常時使用可能 • 認証後に使用可能 • 仕事用領域がロック解除された場合のみ使用可能 デフォルト値は［常に使用可能］です。 最小要件は、BlackBerry 10 OS バージョン 10.3.1 です。
TLS 1.2を使用する	この設定は、BlackBerry 10 デバイスが Wi-Fi ネットワークを介した通信に TLS 1.2 を使用する必要があるかどうかを指定します。 使用できる値： • オフ • オン デフォルト値は［オフ］です。 最小要件は、BlackBerry 10 OS バージョン 10.3.3 です。
信頼する	

BlackBerry 10 ：Wi-Fi プロファイル設定	説明
クライアント証明書のソース	この設定では、BlackBerry 10 デバイスがクライアント証明書を取得可能な方法を指定します。デバイスがクライアント証明書を取得するための 4 つのオプションがあります。 • ［SCEP］を選択した場合は、デバイスがクライアント証明書をダウンロードするために使用できる、関連付けられた SCEP プロファイルも指定する必要があります。 • ［ユーザー資格情報］を選択した場合は、デバイスがクライアント証明書をダウンロードするために使用できる、ユーザー資格情報プロファイルも指定する必要があります。 • ［スマートカード］を選択した場合は、ユーザーはクライアント証明書を含むスマートカードとデバイスをペアリングする必要があります。 • ［その他］を選択した場合は、ユーザーが手動でクライアント証明書をデバイスに追加する必要があります。 スマートカードは、BlackBerry 10 OS バージョン 10.3.1 以降を実行しているデバイスでサポートされています。 使用できる値： • スマートカード • SCEP • ユーザー資格情報 • その他 デフォルト値は［その他］です。
関連付けられた SCEP プロファイル	この設定では、BlackBerry 10 デバイスが Wi-Fi ネットワーク認証に使用するクライアント証明書を登録するための関連付けられた SCEP プロファイルを指定します。 この設定は、［クライアント証明書のソース］が［SCEP］に設定されている場合のみ有効です。
関連付けられたユーザー資格情報プロファイル	この設定では、BlackBerry 10 デバイスが Wi-Fi ネットワーク認証に使用するクライアント証明書を登録するための関連付けられたユーザー資格情報プロファイルを指定します。 この設定は、［クライアント証明書のソース］が［ユーザー資格情報］に設定されている場合のみ有効です。 ユーザー資格情報を使用するための最小要件は、BlackBerry 10 OS バージョン 10.3.1 です。

BlackBerry 10 ：Wi-Fi プロファイル設定	説明
信頼済み証明書ソース	この設定では、信頼済み証明書のソースを指定します。これが［信頼済み証明書ストア］に設定されている場合、BlackBerry 10 デバイスは Wi-Fi 証明書ストアの証明書を使用している Wi-Fi ネットワークに接続できません。 使用できる値： • None • 信頼済み証明書ストア デフォルト値は［なし］です。
関連付けられたプロファイル	
仕事用データに BlackBerry Secure Connect Plus 接続とエンタープライズ接続プロファイルを使用します。	この設定では、BlackBerry 10 デバイスが仕事用 Wi-Fi ネットワークにアクセスできる場合を含め、すべての仕事用領域のトラフィックが BlackBerry Secure Connect Plus 経由で実行されるかどうかを指定します。この設定が未選択の場合、Wi-Fi プロファイルを設定して、BlackBerry 10 デバイスに割り当てた場合、デバイスは仕事用領域トラフィックに BlackBerry Secure Connect Plus よりも、仕事用 Wi-Fi ネットワークを優先します。 この機能を使用する場合は、BlackBerry 10 デバイスユーザーに割り当てられている IT ポリシーで、［仕事用アプリケーションにネットワークアクセス制御を強制する］IT ポリシールールが未選択になっていることを確認します。 この設定は、組織のデータ使用量とネットワークコストに影響を与える場合があります。この機能を使用する前に、組織で優先される設定になっていることを確認します。 最小要件は、BlackBerry 10 OS バージョン 10.3.2 です。
関連付けられている VPN プロファイル	この設定では、BlackBerry 10 デバイスが Wi-Fi ネットワークに接続されている場合に、VPN に接続するために使用する関連付けられている VPN プロファイルを指定します。
関連付けられているプロキシプロファイル	この設定では、BlackBerry 10 デバイスが Wi-Fi ネットワークに接続されている場合に、プロキシサーバーに接続するために使用する関連付けられているプロキシプロファイルを指定します。

デバイスの仕事用 VPN の設定

VPN プロファイルを使用して、iOS、macOS、Samsung Knox、Windows 10、および BlackBerry 10 デバイスを仕事用の VPN に接続する方法を指定できます。VPN プロファイルは、ユーザーアカウント、ユーザーグループ、またはデバイスグループに割り当てることができます。BlackBerry 10 デバイスの場合は、VPN プロファイルを Wi-Fi プロファイルに関連付けることもできます。

Samsung Knox 以外の Android デバイスの仕事用 VPN に接続するには、VPN アプリのアプリの設定を使用して VPN 設定を構成するか、ユーザーがデバイスで VPN 設定を手動で構成することができます。

デバイス	アプリとネットワーク接続
BlackBerry 10	デフォルトでは、仕事用アプリと個人用アプリの両方が、デバイスに保存された VPN プロファイルを使用して組織のネットワークに接続します。仕事用アプリは、BlackBerry Infrastructure を使用して組織のネットワークに接続することもできます。組織のセキュリティ基準が個人用アプリに組織のネットワークへのアクセスを許可していない場合、または仕事用アプリの接続オプションを制限したい場合は、接続オプションを制限できます。
iOS	仕事用アプリおよび個人用アプリはデバイスに保存された VPN プロファイルを使用して、組織のネットワークに接続できます。VPN プロファイルの per-app VPN を有効化して、このプロファイルを指定した仕事用アプリに制限することができます。 VPN をオンデマンドで有効にして、デバイスが特定ドメインの VPN に自動的に接続されるようにすることができます。たとえば、組織のドメインを指定して、ユーザーが VPN オンデマンドを使用してイントラネットのコンテンツにアクセスすることを許可できます。
macOS	アプリが組織のネットワークに接続できるように、VPN プロファイルを設定することができます。VPN をオンデマンドで有効にして、デバイスが特定ドメインの VPN に自動的に接続されるようにすることができます。たとえば、組織のドメインを指定して、ユーザーが VPN オンデマンドを使用してイントラネットのコンテンツにアクセスすることを許可できます。
Samsung Knox	Android Enterprise または Samsung Knox Workspace アクティベーションを備えた Samsung Knox デバイスでは、仕事用アプリはデバイスに保存された VPN プロファイルを使用して、組織のネットワークに接続できます。 per-app VPN を有効にして、このプロファイルを、指定した仕事用アプリに制限できます。 サポートされる VPN Client アプリをデバイスにインストールする必要があります。Cisco AnyConnect および Juniper がサポートされています。 メモ： Juniper アプリは SSL VPN のみをサポートしています。
Windows 10	アプリが組織のネットワークに接続できるように、VPN プロファイルを設定することができます。VPN プロファイルで、VPN を使用する必要があるアプリのリストを指定できます。

VPN プロファイルの作成

必要となるプロファイルの設定は、各デバイスタイプと選択する VPN 接続タイプおよび認証タイプに応じて異なります。

メモ：一部のデバイスでは、xAuth パスワードを保存できない場合があります。詳細については、support.blackberry.com/community にアクセスし、記事 30353 を参照してください。

作業を始める前に：

- デバイスが仕事用 VPN 接続に対して証明書に基づく認証を使用している場合は、CA 証明書プロファイルを作成して、それをユーザーアカウント、ユーザーグループ、またはデバイスグループに割り当てます。デバイスにクライアント証明書を送信するには、ユーザー資格情報、SCEP、または共有証明書プロファイルを作成し、それを VPN プロファイルに関連付けます。
- プロキシサーバーを使用する iOS、macOS、Samsung Knox、および BlackBerry 10 デバイスの場合、プロキシプロファイルを作成して、それを VPN プロファイルに関連付けます。（Windows 10 デバイスのプロキシサーバーは VPN プロファイルで設定されます。）
- Samsung Knox デバイスの場合、適切な VPN クライアントアプリをアプリリストに追加し、それらをユーザーアカウント、ユーザーグループ、またはデバイスグループに割り当てます。サポートされている VPN クライアントアプリは Cisco AnyConnect と Juniper です。

1. メニューバーで［ポリシーとプロファイル］をクリックします。
2. ［ネットワークと接続］ > ［**VPN**］をクリックします。
3. ＋ をクリックします。
4. VPN プロファイルの名前と説明を入力します。この情報はデバイスに表示されます。
5. 次の操作を実行します。
   a) デバイスタイプのタブをクリックします。
   b) 各プロファイル設定には、組織の環境内の VPN 設定に一致する適切な値をそれぞれ設定します。組織によって、VPN に接続するためにユーザーがユーザー名とパスワードを入力することが義務付けられており、プロファイルが複数のユーザーに対応している場合は、［ユーザー名］フィールドに `%UserName%` を入力します。
6. 組織内のデバイスタイプごとに手順 5 を繰り返します。
7. ［追加］をクリックします。

VPN プロファイル設定

実際の値を指定するのではなく、値を参照するためにテキストフィールドになっているプロファイル設定では、変数を使用できます。VPN プロファイルは、以下のデバイスタイプでサポートされています。

- iOS
- macOS
- Samsung Knox
- Windows 10
- BlackBerry 10

iOS および macOS ：VPN プロファイル設定

macOS は、ユーザーアカウントまたはデバイスにプロファイルを適用します。どちらか一方に適用する VPN プロファイルを設定することができます。

iOSおよび macOS：VPN プロファイル設定	説明
プロファイルを適用	この設定では、macOS デバイス上の VPN プロファイルをユーザーアカウントまたはデバイスに適用するかどうかを指定します。 使用できる値： • ユーザー • デバイス この設定は macOS デバイスに対してのみ有効です。
接続タイプ	この設定では、デバイスが VPN ゲートウェイ用に使用する接続タイプを指定します。一部の接続タイプでは、ユーザーが適切な VPN アプリをデバイスにインストールする必要もあります。 使用できる値： • L2TP • PPTP • IPSec • Cisco AnyConnect • Juniper • Pulse Secure • F5 • SonicWALL Mobile Connect • Aruba VIA • Check Point Mobile • OpenVPN • カスタム • IKEv2 • IKEv2 常時オン デフォルト値は［L2TP］です。 macOS デバイスでは、一部の値が有効ではありません。
VPN バンドル ID	この設定では、カスタム SSL VPN に対応する VPN アプリのバンドル ID を指定します。バンドル ID はリバース DNS 形式（たとえば、com.example.VPNapp）です。 この設定は、［接続タイプ］が［カスタム］に設定されている場合のみ有効です。
サーバー	この設定では、VPN サーバーの FQDN または IP アドレスを指定します。

iOSおよび **macOS**：**VPN** プロファイル設定	説明
ユーザー名	この設定では、デバイスが VPN ゲートウェイ認証に使用するユーザー名を指定します。プロファイルが複数のユーザーに対応している場合は、%UserName% 変数を指定できます。
カスタムのキーと値のペア	この設定では、カスタム SSL VPN 用のキーと関連付けられている値を指定します。設定情報は、ベンダーの VPN アプリに固有です。 この設定は、［接続タイプ］が［カスタム］に設定されている場合のみ有効です。
ログイングループまたはドメイン	この設定では、VPN ゲートウェイが iOS デバイスを認証するために使用するログイングループまたはドメインを指定します。 この設定は、［接続タイプ］が［SonicWALL Mobile Connect ］に設定されている場合のみ有効です。
領域	この設定では、VPN ゲートウェイが iOS デバイスを認証するために使用する認証領域の名前を指定します。 この設定は、［接続タイプ］が［Juniper ］または［Pulse Secure ］に設定されている場合のみ有効です。
ロール	この設定では、VPN ゲートウェイが iOS デバイスによるアクセスが可能なネットワークリソースを確認するために使用するユーザーロールの名前を指定します。 この設定は、［接続タイプ］が［Juniper ］または［Pulse Secure ］に設定されている場合のみ有効です。
認証の種類	この設定では、VPN ゲートウェイの認証の種類を指定します。 ［接続タイプ］によって、サポートされる認証の種類と、この設定のデフォルト値が決定されます。 使用できる値： • パスワード • RSA SecurID • 共有の秘密/グループ名 • 共有証明書 • SCEP • ユーザー資格情報
パスワード	この設定では、デバイスが VPN ゲートウェイ認証に使用するパスワードを指定します。 この設定は、［認証の種類］が［パスワード］に設定されている場合のみ有効です。

iOSおよび **macOS**：**VPN** プロファイル設定	説明
グループ名	この設定では、VPN ゲートウェイのグループ名を指定します。 この設定は、次の条件を満たしている場合にのみ有効になります。 • ［接続タイプ］設定が［Cisco AnyConnect ］に設定されている場合。 • ［接続タイプ］設定が［IPsec］に、［認証の種類］設定が［共有の秘密/グループ名］に設定されている場合。
共有の秘密	この設定では、VPN 認証に使用する共有の秘密を指定します。 この設定は、次の条件を満たしている場合にのみ有効になります。 • ［接続タイプ］設定が［L2TP］に設定されている場合。 • ［接続タイプ］設定が［IPsec］に、［認証の種類］設定が［共有の秘密/グループ名］に設定されている場合。 • ［接続タイプ］設定が［IKEv2］に、［認証方法］設定が［共有秘密］に設定されている場合。
共有証明書プロファイル	この設定では、デバイスが VPN ゲートウェイ認証に使用するクライアント証明書を含む共有証明書プロファイルを指定します。 この設定は、［認証の種類］または［認証方法］の設定が［共有証明書］に設定されている場合にのみ有効です。
関連付けられた SCEP プロファイル	この設定では、iOS デバイスが VPN 認証に使用するクライアント証明書を取得するために使用する関連付けられた SCEP プロファイルを指定します。 この設定は、［認証の種類］または［認証方法］の設定が［SCEP］に設定されている場合にのみ有効です。
関連付けられたユーザー資格情報プロファイル	この設定では、デバイスが VPN 認証に使用するクライアント証明書を取得するための関連付けられたユーザー資格情報プロファイルを指定します。 この設定は、［認証の種類］または［認証方法］の設定が［ユーザー資格情報］に設定されている場合にのみ有効です。
暗号化レベル	この設定では、VPN 接続のデータ暗号化レベルを指定します。これが［自動］に設定されている場合は、使用可能な暗号化強度がすべて許可されます。これが［最大］に設定されている場合は、最大の暗号化強度のみが許可されます。 この設定は、［接続タイプ］が［PPTP］に設定されている場合のみ有効です。 使用できる値： • None • 自動 • 最大 デフォルト値は［なし］です。

iOSおよび **macOS**：**VPN** プロファイル設定	説明
VPN 経由でネットワークトラフィックをルーティング	この設定では、すべてのネットワークトラフィックを VPN 接続経由で送信するかどうかを指定します。 この設定は、［接続タイプ］が［L2TP］または［PPTP］に設定されている場合のみ有効です。
ハイブリッド認証を使用する	この設定では、認証にサーバー側の証明書を使用するかどうかを指定します。 この設定は、［接続タイプ］が［IPsec］、［認証の種類］が［共有の秘密/グループ名］に設定されている場合にのみ有効です。
パスワードの入力を求める	この設定では、デバイスがユーザーにパスワードの入力を求めるプロンプトを表示するかどうかを指定します。 この設定は、［接続タイプ］が［IPsec］、［認証の種類］が［共有の秘密/グループ名］に設定されている場合にのみ有効です。
ユーザー PIN の入力を求める	この設定では、デバイスがユーザーに PIN の入力を求めるプロンプトを表示するかどうかを指定します。 この設定は、［接続タイプ］が［IPsec］、［認証の種類］が［共有証明書］、［SCEP］、または［ユーザー資格情報］に設定されている場合にのみ有効です。
リモートアドレス	この設定では、VPN サーバーの IP アドレスまたはホスト名を指定します。 この設定は、［接続タイプ］設定が［IKEv2］に設定されている場合のみ有効です。
ローカル ID	この設定では、IKEv2 クライアントの ID を、FQDN、UserFQDN、アドレス、ASN1DN のいずれかの形式で指定します。 この設定は、［接続タイプ］設定が［IKEv2］に設定されている場合のみ有効です。
リモート ID	この設定では、IKEv2 クライアントのリモート ID を、FQDN、ユーザー FQDN、アドレス、ASN1DN のいずれかの形式で指定します。 この設定は、［接続タイプ］設定が［IKEv2］に設定されている場合のみ有効です。

iOSおよび **macOS**：**VPN** プロファイル設定	説明
認証方法	この設定では、VPN の認証方法を指定します。 この設定は、［接続タイプ］設定が［IKEv2］に設定されている場合のみ有効です。 使用できる値： • 共有の秘密 • 共有証明書 • SCEP • ユーザー資格情報
VPN をオンデマンドで有効にする	この設定では、デバイスが特定のドメインにアクセスしたときに、VPN 接続を自動的に開始できるようにするかどうかを指定します。 iOS デバイスの場合、この設定は仕事用アプリに適用されます。 この設定は、次の条件を満たしている場合にのみ有効になります。 • ［接続タイプ］設定が［IPsec］、［Cisco AnyConnect ］、［Juniper ］、［Pulse Secure ］、［F5 ］、［SonicWALL Mobile Connect ］、［Aruba VIA ］、［Check Point Mobile ］、［OpenVPN ］、または［カスタム］に、［認証の種類］が［共有証明書］、［SCEP］、または［ユーザー資格情報］に設定されている場合。 • ［接続タイプ］設定が［IKEv2］に、［認証方法］が［共有証明書］に設定されている場合。
VPN オンデマンドを使用できるドメインまたはホスト名	この設定では、VPN オンデマンド対応のドメインおよび関連付けられているアクションを指定します。 この設定は、［VPN オンデマンドを有効にする］設定が選択されている場合のみ有効です。 ［オンデマンドアクション］に使用できる値： • 常に確立 • 必要に応じて確立 • 確立しない
iOS 7.0 以降の VPN オンデマンドルール	この設定では、VPN オンデマンドの接続要件を指定します。ペイロード形式の例の中から 1 つ以上のキーを使用する必要があります。 この設定は、［VPN オンデマンドを使用できるドメインまたはホスト名］の設定を無効にします。 この設定は、［VPN オンデマンドを有効にする］設定が選択されている場合のみ有効です。

iOSおよび **macOS**：**VPN** プロファイル設定	説明
xAuth を有効にする	この設定では、VPN が拡張認証をサポートするかどうかを指定します。 この設定は、［接続タイプ］が［IKEv2］または［IKEv2 常時オン］に設定されている場合のみ有効です。
最小 TLS バージョン	この設定では、iOS 11 以降を実行しているデバイスが EAP-TLS 認証に使用する最小 TLS バージョンを指定します。 この設定は、［xAuth を有効にする］設定が選択されていて、認証タイプが［証明書］である場合にのみ有効です。 使用できる値： • 1.0 • 1.1 • 1.2 デフォルト設定は［1.0］です。
最大 TLS バージョン	この設定では、iOS 11 以降を実行しているデバイスが EAP-TLS 認証に使用する最大 TLS バージョンを指定します。 この設定は、［xAuth を有効にする］設定が選択されていて、認証タイプが［証明書］である場合にのみ有効です。 使用できる値： • 1.0 • 1.1 • 1.2 デフォルト設定は［1.2］です。
キープアライブ間隔	この設定では、デバイスがキープアライブパケットを送信する頻度を指定します。 この設定は、［接続タイプ］設定が［IKEv2］に設定されている場合のみ有効です。 使用できる値： • 無効 • 30 分 • 10 分 • 1 分 デフォルト値は 10 分です。
MOBIKE を無効にする	この設定では、MOBIKE を無効にするかどうかを指定します。 この設定は、［接続タイプ］設定が［IKEv2］に設定されている場合のみ有効です。

iOSおよび **macOS**：**VPN** プロファイル設定	説明
IKEv2 リダイレクトを無効にする	この設定では、IKEv2 リダイレクトを無効にするかどうかを指定します。この設定が選択されていない場合、サーバーからリダイレクト要求を受け取ると、IKEv2 接続がリダイレクトされます。 この設定は、［接続タイプ］設定が［IKEv2］に設定されている場合のみ有効です。
Perfect Forward Secrecy を有効にする	この設定では、VPN が PFS をサポートするかどうかを指定します。 この設定は、［接続タイプ］設定が［IKEv2］に設定されている場合のみ有効です。
NAT キープアライブを有効にする	この設定では、VPN が NAT キープアライブパケットをサポートするかどうかを指定します。キープアライブパケットは、IKEv2 接続の NAT マッピングを維持するために使用されます。 この設定は、［接続タイプ］設定が［IKEv2］に設定されている場合のみ有効です。
NAT キープアライブ間隔	この設定では、デバイスが NAT キープアライブパケットを送信する頻度を秒単位で指定します。 この設定は、［接続タイプ］設定が［IKEv2］に設定され、［NAT キープアライブを有効にする］設定が選択されている場合のみ有効です。 最小値およびデフォルト値は 20 です。
IPv4 および IPv6 IKEv2 内部サブネットを使用する	この設定では、VPN で IKEv2 設定属性 INTERNAL_IP4_SUBNET および INTERNAL_IP6_SUBNET を使用できるかどうかを指定します。 この設定は、［接続タイプ］設定が［IKEv2］に設定されている場合のみ有効です。
サーバー証明書の共通名	この設定では、IKE サーバーがデバイスへ送信する証明書の共通名を指定します。 この設定は、［接続タイプ］設定が［IKEv2］に設定されている場合のみ有効です。
サーバー証明書発行者の共通名	この設定では、IKE サーバーがデバイスへ送信する証明書の証明書発行者の共通名を指定します。 この設定は、［接続タイプ］設定が［IKEv2］に設定されている場合のみ有効です。
子セキュリティ関連付けパラメーターを適用する	この設定では、子セキュリティ関連付けパラメーターを適用するかどうかを指定します。 この設定は、［接続タイプ］設定が［IKEv2］に設定されている場合のみ有効です。

iOSおよび **macOS**：**VPN** プロファイル設定	説明
IKE セキュリティ関連付けパラメーターを適用する	この設定では、IKE セキュリティ関連付けパラメーターを適用するかどうかを指定します。 この設定は、［接続タイプ］設定が［IKEv2］に設定されている場合のみ有効です。
DH グループ	この設定では、デバイスがキーマテリアルを生成するために使用する DH グループを指定します。 この設定は、［子セキュリティ関連付けパラメーターを適用する］または［IKE セキュリティ関連付けパラメーターを適用する］設定が選択されている場合にのみ有効です。 使用できる値： • 0 • 1 • 2 • 5 • 14 • 15 • 16 • 17 • 18 • 19 • 20 • 21 • 31 デフォルト設定は［2］です。
暗号化アルゴリズム	この設定では、IKE 暗号化アルゴリズムを指定します。 この設定は、［子セキュリティ関連付けパラメーターを適用する］または［IKE セキュリティ関連付けパラメーターを適用する］設定が選択されている場合にのみ有効です。 使用できる値： • DES • 3DES • AES 128 • AES 256 • AES 128 GCM • AES 256 GCM • ChaCha20Poly1305 デフォルト設定は［3DES］です。

iOSおよび **macOS**：**VPN** プロファイル設定	説明
整合性アルゴリズム	この設定では、IKE 整合性アルゴリズムを指定します。 この設定は、［子セキュリティ関連付けパラメーターを適用する］または［IKE セキュリティ関連付けパラメーターを適用する］設定が選択されている場合にのみ有効です。 使用できる値： • SHA1 96 • SHA1 160 • SHA1 256 • SHA2 384 • SHA2 512 デフォルト値は［SHA1-96］です。
Rekey 間隔	この設定では、IKE 接続のライフタイムを指定します。 この設定は、［子セキュリティ関連付けパラメーターを適用する］または［IKE セキュリティ関連付けパラメーターを適用する］設定が選択されている場合にのみ有効です。 使用できる値は、10～1440 分です。 デフォルト値は、［1440］です。
per-app VPN を有効にする	この設定では、VPN ゲートウェイが per-app VPN をサポートするかどうかを指定します。この機能は、組織の VPN の負荷を軽減するために役立ちます。たとえば、ファイアウォールの内部にあるアプリケーションサーバーや Web ページへのアクセスなど、特定の仕事用トラフィックのみが VPN を使用できるように指定できます。 この設定は、［接続タイプ］設定が［Cisco AnyConnect ］、［Juniper ］、［Pulse Secure ］、［F5 ］、［SonicWALL Mobile Connect ］、［Aruba VIA ］、［Check Point Mobile ］、［OpenVPN ］、［カスタム］、または［IKEv2］に設定されている場合のみ有効です。
アプリの自動接続を許可する	この設定では、per-app VPN に関連付けられたアプリが VPN 接続を自動的に開始できるようにするかどうかを指定します。 この設定は、［per-app VPN を有効にする］設定が選択されている場合のみ有効です。
Safari ドメイン	この設定では、Safari 内で VPN 接続を開始できるドメインを指定します。 この設定は、［per-app VPN を有効にする］設定が選択されている場合のみ有効です。

iOSおよび macOS：VPN プロファイル設定	説明
カレンダードメイン	この設定では、カレンダー内で VPN 接続を開始できるドメインを指定します。 この設定は、［per-app VPN を有効にする］設定が選択されている場合のみ有効です。この設定は、iOS 13.0 以降のデバイスにのみ適用されます。
連絡先ドメイン	この設定では、連絡先内で VPN 接続を開始できるドメインを指定します。 この設定は、［per-app VPN を有効にする］設定が選択されている場合のみ有効です。この設定は、iOS 13.0 以降のデバイスにのみ適用されます。
メールドメイン	この設定では、メール内で VPN 接続を開始できるドメインを指定します。 この設定は、［per-app VPN を有効にする］設定が選択されている場合のみ有効です。この設定は、iOS 13.0 以降のデバイスにのみ適用されます。
トラフィックトンネル	この設定では、VPN がトラフィックをアプリケーションレイヤーと IP レイヤーのどちらでトンネリングするかを指定します。 この設定は、［per-app VPN を有効にする］設定が選択されている場合のみ有効です。この設定は、iOS 13.0 以降のデバイスにのみ適用されます。 使用できる値： • アプリケーションレイヤー • IP レイヤー デフォルト設定は、［アプリケーションレイヤー］です。
関連付けられているプロキシプロファイル	この設定では、iOS デバイスが VPN に接続されている場合に、プロキシサーバーに接続するために使用する関連付けられているプロキシプロファイルを指定します。

Android ：VPN プロファイル設定

次の VPN プロファイル設定は Samsung Knox Workspace デバイスでのみサポートされています。

Samsung Knox Workspace デバイスでサポートされている VPN プロファイル設定の詳細については、「Samsung Knox VPN JSON パラメーター」を参照してください。

Android ：VPN プロファイル設定	説明
サーバーアドレス	この設定では、VPN サーバーの FQDN または IP アドレスを指定します。

Android ：VPN プロファイル設定	説明
VPN の種類	この設定では、デバイスによる VPN サーバーへの接続に IPsec と SSL のどちらを使用するかを指定します。 使用できる値： • IPSec • SSL デフォルト値は［IPsec］です。 Juniper VPN アプリは［SSL］のみをサポートしています。
必要なユーザー認証	この設定では、VPN サーバーに接続するためにデバイスユーザーがユーザー名とパスワードを指定する必要があるかどうかを指定します。
ユーザー名	この設定では、デバイスが VPN ゲートウェイ認証に使用するユーザー名を指定します。プロファイルが複数のユーザーに対応している場合は、%UserName% 変数を使用できます。 この設定は、［必要なユーザー認証］設定が選択されている場合のみ有効です。
パスワード	この設定では、デバイスが VPN ゲートウェイ認証に使用するパスワードを指定します。 この設定は、［必要なユーザー認証］設定が選択されている場合のみ有効です。
スプリットトンネルの種類	VPN ゲートウェイがスプリットトンネリングをサポートしている場合、デバイスがスプリットトンネリングを使用して VPN ゲートウェイをバイパスできるかどうかは、この設定により指定されます。 使用できる値： • 無効 • 手動 • 自動 ［VPN の種類］設定が［IPsec］に設定されている場合は、この設定を［無効］に設定する必要があります。 デフォルト値は［無効］です。
転送ルート	この設定は、VPN ゲートウェイをバイパスする 1 つ以上のルートを指定します。1 つ以上の IP アドレスを指定できます。 この設定は、［VPN の種類］設定が［SSL］に設定され、［スプリットトンネルの種類］設定が［手動］に設定されている場合にのみ有効です。
DPD	この設定では、DPD を有効にするかどうかを指定します。 この設定は、［VPN の種類］が［IPsec］に設定されている場合のみ有効です。

Android ：**VPN** プロファイル設定	説明
IKE のバージョン	この設定では、VPN 接続で使用する IKE プロトコルのバージョンを指定します。 使用できる値： • IKEv1 • IKEv2 デフォルト値は［IKEv1］です。 この設定は、［VPN の種類］が［IPsec］に設定されている場合のみ有効です。
IPsec 認証の種類	この設定では、IPsec VPN 接続の認証の種類を指定します。［IKE のバージョン］によって、サポートされる IPsec 認証の種類と、この設定のデフォルト値が決定されます。 使用できる値： • 証明書 • 事前共有キー • EAP MD5 • EAP MSCHAPv2 • ハイブリッド RSA • CAC ベース認証 この設定は、［VPN の種類］が［IPsec］に設定されている場合のみ有効です。
IPsec グループ ID の種類	この設定では、VPN 接続の IPsec グループ ID の種類を指定します。［IPsec 認証の種類］によって、サポートされる IPsec グループ ID の種類と、この設定のデフォルト値が決定されます。 使用できる値： • デフォルト • IPv4 アドレス • 完全修飾ドメイン名 • ユーザー FQDN • IKE キー ID ［IPsec 認証の種類］の設定が［証明書］に設定されている場合は、この設定は自動的に［デフォルト］に設定されます。 この設定は、［VPN の種類］が［IPsec］に設定されている場合のみ有効です。
IPsec グループ ID	この設定では、VPN 接続の IPsec グループ ID を指定します。 この設定は、［VPN の種類］が［IPsec］に設定されている場合のみ有効です。

Android ：**VPN** プロファイル設定	説明
IKE フェーズ 1 キー交換モード	この設定では、VPN 接続の交換モードを指定します。 使用できる値： • メインモード • アグレッシブモード デフォルト値は［メインモード］です。 この設定は、［VPN の種類］が［IPsec］に設定されている場合のみ有効です。
IKE ライフタイム	この設定では、IKE 接続のライフタイムを秒単位で指定します。サポートされていない値または Null 値に設定すると、デバイスのデフォルト値が使用されます。 この設定は、［VPN の種類］が［IPsec］に設定されている場合のみ有効です。
IKE 暗号化アルゴリズム	この設定では、IKE 接続に使用される暗号化アルゴリズムを指定します。 この設定は、［VPN の種類］が［IPsec］に設定されている場合のみ有効です。
IKE 整合性アルゴリズム	この設定では、IKE 接続に使用される整合性アルゴリズムを指定します。 この設定は、［VPN の種類］設定が［IPsec］に設定され、［IKE のバージョン］が［IKEv2］に設定されている場合にのみ有効です。
IPsec DH グループ	この設定では、デバイスがキーマテリアルを生成するために使用する DH グループを指定します。 使用できる値は、0、1、2、5、および 14〜26 です。 デフォルト値は、［0］です。 この設定は、［VPN の種類］が［IPsec］に設定されている場合のみ有効です。
IPsec パラメーター	この設定では、VPN 接続に使用される IPsec パラメーターを指定します。 この設定は、［VPN の種類］が［IPsec］に設定されている場合のみ有効です。
Perfect Forward Secrecy	この設定では、VPN ネットワークが PFS をサポートするかどうかを指定します。 この設定は、［VPN の種類］が［IPsec］に設定されている場合のみ有効です。
MOBIKE を有効にする	この設定では、VPN ゲートウェイが MOBIKE をサポートするかどうかを指定します。 この設定は、［VPN の種類］が［IPsec］に設定されている場合のみ有効です。

Android ：**VPN** プロファイル設定	説明
IPsec ライフタイム	この設定では、IPsec 接続のライフタイムを秒単位で指定します。サポートされていない値または Null 値に設定すると、デバイスのデフォルト値が使用されます。 この設定は、［VPN の種類］が［IPsec］に設定されている場合のみ有効です。
IPsec 暗号化アルゴリズム	この設定では、VPN 接続に使用される IPsec 暗号化アルゴリズムを指定します。 この設定は、［VPN の種類］が［IPsec］に設定されている場合のみ有効です。
IPsec 整合性アルゴリズム	この設定では、VPN 接続に使用される IPsec 整合性アルゴリズムを指定します。 この設定は、［VPN の種類］設定が［IPsec］に設定され、［IKE のバージョン］が［IKEv2］に設定されている場合にのみ有効です。
認証の種類	この設定では、VPN ゲートウェイの認証の種類を指定します。 使用できる値： • なし • 証明書に基づく認証 • CAC ベース認証 デフォルト値は［なし］です。 この設定は、［VPN の種類］が［SSL］に設定されている場合のみ有効です。
SSL アルゴリズム	この設定では、SSL VPN 接続に必要な暗号化アルゴリズムを指定します。 この設定は、［VPN の種類］が［SSL］に設定されている場合のみ有効です。
UID/PID 情報を追加する	この設定では、VPN クライアントアプリに送信されるパケットに UID および PID 情報を追加するかどうかを指定します。 この設定は、Cisco AnyConnect VPN アプリに対して選択する必要があります。
サポート連鎖	この設定では、VPN 連鎖のサポート方法を指定します。 使用できる値： • サポート連鎖 • 外部トンネル • 内部トンネル デフォルト値は［サポート連鎖］です。

Android ：**VPN** プロファイル設定	説明
ベンダー文字列入力タイプ	この設定では、VPN のために、キー値ペアまたは JSON 文字列を指定します。設定情報は、ベンダーの VPN アプリに固有です。 使用できる値： • ベンダーとキー値ペア • ベンダー JSON 値 デフォルト値は［ベンダーとキー値ペア］です。
ベンダーとキー値ペア	この設定では、VPN 用のキーと関連付けられている値を指定します。設定情報は、ベンダーの VPN アプリに固有です。 この設定は、［ベンダー文字列入力タイプ］設定が［ベンダーとキー値ペア］に設定されている場合にのみ有効です。
ベンダー JSON 値	この設定では、ベンダーの VPN アプリに固有の設定情報を JSON 形式で指定します。 この設定は、［ベンダー文字列入力タイプ］設定が［ベンダー JSON 値］に設定されている場合にのみ有効です。
VPN クライアントパッケージ ID	この設定では、VPN アプリのパッケージ ID を指定します。
エラー後に自動的に接続を再試行する	この設定では、接続が失われた後に、VPN 接続を自動的に再起動するかどうかを指定します。
FIPS モードを有効にする	この設定では、FIPS モードを有効にするかどうかを指定します。FIPS モードを有効にした場合、VPN 接続に FIPS 検証済みの暗号化アルゴリズムのみが使用されるようになります。
仕事用領域がある Android デバイスのエンタープライズ接続	この設定では、Samsung Knox Workspace デバイスで、仕事用領域の全アプリに VPN 接続を使用するか、あるいは、指定したアプリのみに使用するかを指定します。 • ［コンテナ単位の VPN］では、デバイスの仕事用領域にあるすべてのアプリに VPN 接続を使用します。 • ［per-app VPN］では、指定したアプリに対してのみ VPN 接続を使用します。
VPN 接続の使用を許可されたアプリ	この設定では、VPN 接続を使用できる仕事用領域内のアプリを指定します。利用可能なアプリのリストからアプリを選択するか、アプリパッケージ ID を指定できます。 この設定は、［仕事用領域がある Android デバイスのエンタープライズ接続］設定が［per-app VPN］に設定されている場合にのみ有効です。

Android ：VPN プロファイル設定	説明
関連付けられているプロキシプロファイル	この設定では、デバイスが VPN に接続されている場合に、プロキシサーバーに接続するために使用する関連付けられているプロキシプロファイルを指定します。

Windows 10 ：VPN プロファイル設定

Windows ：VPN プロファイル設定	説明
接続タイプ	この設定では、Windows 10 デバイスが VPN 用に使用する接続タイプを指定します。 使用できる値： • Microsoft • Junos Pulse • SonicWALL Mobile Connect • F5 • Check Point Mobile • 手動接続定義 デフォルト値は［Microsoft ］です。
サーバー	この設定では、VPN のパブリック IP アドレス、ルーティング可能な IP アドレス、または DNS 名を指定します。この設定では、VPN の外部 IP またはサーバーファームの仮想 IP を指定できます。 この設定は、［接続タイプ］が［Microsoft ］に設定されている場合のみ有効です。
サーバー URL リスト	この設定では、URL、ホスト名、または IP の形式で指定されたサーバーのカンマ区切りのリストを指定します。 この設定は、［接続タイプ］が［Microsoft ］に設定されていない場合のみ有効です。
ルーティングポリシーのタイプ	この設定では、ルーティングポリシーのタイプを指定します。 この設定は、［接続タイプ］が［Microsoft ］に設定されている場合のみ有効です。 使用できる値： • 分割トンネル • 強制トンネル デフォルト値は［強制トンネル］です。

Windows ：VPN プロファイル設定	説明
ネイティブプロトコルのタイプ	この設定では、VPN で使用されるルーティングポリシーのタイプを指定します。 この設定は、［接続タイプ］が［Microsoft ］に設定されている場合のみ有効です。 使用できる値： • L2TP • PPTP • IKEv2 • 自動 デフォルト値は［自動］です。
認証	この設定では、ネイティブ VPN に使用される認証方法を指定します。 ［ネイティブプロトコルのタイプ］設定によって、サポートされる認証方法と、この設定のデフォルト値が決定されます。 • ［L2TP］または［PPTP］を選択した場合は、［MS-CHAPv2］または［EAP］を指定できます。デフォルト値は［MS-CHAPv2］です。 • ［IKEv2］を選択した場合は、［ユーザー方式］または［機械方式］を指定できます。デフォルト値は［ユーザー方式］です。 • ［自動］を選択した場合、指定できるのは［EAP］のみです。 使用できる値： • EAP • MS-CHAPv2 • ユーザー方式 • 機械方式
EAP 設定	この設定では、EAP 設定の XML を指定します。 EAP 設定の XML を生成する方法の詳細については、次のサイトにアクセスしてください。 https://docs.microsoft.com/en-us/windows/client-management/mdm/eap-configuration この設定は、［認証］設定が［EAP］に設定されている場合のみ有効です。
ユーザー方式	この設定では、 使用するユーザー方式認証のタイプを指定します。 この設定は、［認証］設定が［ユーザー方式］に設定されている場合のみ有効です。 使用できる値： • EAP

Windows ：VPN プロファイル設定	説明
機械方式	この設定では、 使用する機械方式認証のタイプを指定します。 この設定は、［認証］設定が［機械方式］に設定されている場合のみ有効です。 使用できる値： • 証明書
カスタム設定	この設定では、SSL-VPN プラグイン固有の設定の、HTML でエンコードされた XML BLOB を指定します。これには、SSL-VPN プラグインで利用できるようにするためにデバイスに送信される認証情報が含まれます。 この設定は、［接続タイプ］が［Microsoft ］に設定されていない場合のみ有効です。
プラグインパッケージファミリー名	この設定では、カスタム SSL VPN のパッケージファミリー名を指定します。 この設定は、［接続タイプ］が［手動接続定義］に設定されている場合のみ有効です。
L2TP 事前共有キー	この設定では、L2TP 接続に使用される事前共有キーを指定します。
アプリトリガーリスト	この設定では、VPN 接続を開始するアプリのリストを指定します。
［アプリトリガーリスト］ > ［アプリ ID］	この設定では、per-app VPN 用のアプリを特定します。 使用できる値： • パッケージファミリー名。パッケージファミリー名を検索するには、アプリをインストールして Windows PowerShell コマンド `Get-AppxPackage` を実行します。詳細については、次のサイトにアクセスしてください。 http://technet.microsoft.com/en-us/library/hh856044.aspx • アプリのインストール場所。たとえば、C:\Windows\System\Notepad.exe と指定します。
ルートリスト	この設定では、VPN で使用されるルートのリストを指定します。VPN でスプリットトンネリングが使用されている場合は、ルートリストが必要です。
サブネットアドレス	この設定では、IPv4 または IPv6 アドレス形式を使用して、宛先プレフィックスの IP アドレスを指定します。
サブネットプレフィックス	この設定では、宛先プレフィックスのサブネットプレフィックスを指定します。
除外	この設定では、追加するルートが、ゲートウェイとしての VPN インターフェイスと物理インターフェイスのどちらをポイントする必要があるかを指定します。チェックボックスをオンにした場合、トラフィックは物理インターフェイスで転送されます。このチェックボックスをオフにした場合、トラフィックは VPN 経由で転送されます。

Windows ：VPN プロファイル設定	説明
ドメイン名リスト	この設定では、VPN の名前解決ポリシーテーブル（NRPT）ルールを指定します。
ドメイン名	この設定では、ドメインの FQDN またはサフィックスを指定します。
DNS サーバー	この設定では、DNS サーバーの IP アドレスのリストをカンマで区切って指定します。
Web プロキシサーバー	この設定では、Web プロキシサーバーの IP アドレスを指定します。
トリガー VPN	この設定では、このドメイン名ルールで VPN をトリガーするかどうかを指定します。
持続的	この設定では、VPN が接続されていないときにドメイン名ルールを適用するかどうかを指定します。
トラフィックフィルターリスト	この設定では、VPN 経由のトラフィックを許可するルールを指定します。
［トラフィックフィルターリスト］ > ［アプリ ID］	この設定では、アプリベースのトラフィックフィルター用のアプリを特定します。 使用できる値： • パッケージファミリー名。パッケージファミリー名を検索するには、アプリをインストールして Windows PowerShell コマンド `Get-AppxPackage` を実行します。詳細については、次のサイトにアクセスしてください。 http://technet.microsoft.com/en-us/library/hh856044.aspx • アプリのインストール場所。たとえば、`C:\Windows\System\Notepad.exe` と指定します。 • タイプ「SYSTEM」。カーネルドライバを有効にして、VPN 経由でトラフィックを送信できます（PING、SMB など）。
プロトコル	この設定では、VPN で使用するプロトコルを指定します。 使用できる値： • すべて • TCP • UDP デフォルト値は［すべて］です。
ローカルポートの範囲	この設定では、許可されているローカルポート範囲のリストをカンマで区切って指定します。たとえば、「100-120, 200, 300-320」のように指定します。
リモートポートの範囲	この設定では、許可されているリモートポート範囲のリストをカンマで区切って指定します。たとえば、「100-120, 200, 300-320」のように指定します。

Windows ：VPN プロファイル設定	説明
ローカルアドレスの範囲	この設定では、許可されているローカル IP アドレス範囲のリストをカンマで区切って指定します。
リモートアドレスの範囲	この設定では、許可されているリモート IP アドレス範囲のリストをカンマで区切って指定します。
ルーティングポリシーのタイプ	この設定では、トラフィックフィルターが使用するルーティングポリシーを指定します。［強制トンネル］に設定すると、すべてのトラフィックが VPN を経由します。［分割トンネル］に設定すると、トラフィックは VPN またはインターネットを経由します。 使用できる値： • 分割トンネル • 強制トンネル デフォルト設定は［強制トンネル］です。
資格情報を保存	この設定では、可能な場合に常に資格情報をキャッシュするかどうかを指定します。
常時オン	この設定は、サインイン時にデバイスを VPN に自動的に接続して、ユーザーが手動で VPN への接続を切断するまで接続を維持するかどうかを指定します。
ロックダウン	この設定では、デバイスがネットワークに接続するときにこの VPN 接続を使用する必要があるかどうかを指定します。この設定が有効になっている場合、次の条件が適用されます。 • デバイスの VPN 接続は維持されます。接続は切断できません。 • デバイスは、あらゆるネットワーク接続のために、この VPN への接続を維持する必要があります。 • デバイスは、他の VPN プロファイルに接続できません。また、プロファイルを変更することもできません。
DNS サフィックス	この設定では、1 つ以上の DNS サフィックスをカンマで区切って指定します。リストの最初の DNS サフィックスは、VPN へのプライマリ接続としても使用されます。このリストは、SuffixSearchList に追加されます。
信頼済みネットワークの検出	この設定では、カンマ区切りの文字列を指定して、信頼済みネットワークを特定します。ユーザーが組織の無線ネットワークに接続している場合は、VPN に自動的に接続されることはありません。
IP セキュリティのプロパティ	

Windows ：VPN プロファイル設定	説明
認証変換定数	使用できる値： • MD596 • SHA196 • SHA256128 • GCMAES128 • GCMAE192 • GCMAES256 デフォルト設定は［MD596］です。
暗号変換定数	使用できる値： • DES • DES3 • AES128 • AES192 • AES256 • GCMAES128 • GCMAES192 • GCMAES256 デフォルト設定は［DES］です。
暗号化方式	使用できる値： • DES • DES3 • AES128 • AES192 • AES256 デフォルト設定は［DES］です。
整合性の確認方式	使用できる値： • MD5 • SHA196 • SHA256 • SHA384 デフォルト設定は［MD5］です。

Windows ：VPN プロファイル設定	説明
Diffie-Hellman グループ	使用できる値： • Group1 • Group2 • Group14 • ECP256 • ECP384 • Group24 デフォルト設定は［Group1］です。
PFS グループ	使用できる値： • PFS1 • PFS2 • PFS2048 • ECP256 • ECP384 • PFSMM • PFS24 デフォルト値は［PFS1］です。
プロキシの種類	この設定では、VPN のプロキシ設定のタイプを指定します。 使用できる値： • なし • PAC 設定 • 手動設定 デフォルト値は［なし］です。
PAC URL	この設定では、PAC ファイルをホストしている Web サーバーの URL（PAC ファイル名を含む）を指定します。たとえば、http://www.example.com/PACfile.pac のように指定します。 この設定は、［プロキシの種類］設定が［PAC 設定］に設定されている場合のみ有効です。
アドレス	この設定では、プロキシサーバーの FQDN または IP アドレスを指定します。 この設定は、［プロキシの種類］設定が［手動設定］に設定されている場合のみ有効です。
関連付けられた SCEP プロファイル	この設定では、デバイスが VPN 認証のためのクライアント証明書を取得する際に使用する関連 SCEP プロファイルを指定します。

BlackBerry 10 ：VPN プロファイル設定

BlackBerry 10 ：VPN プロファイル設定	説明
VPN をオンデマンドで有効にする	この設定では、この VPN プロファイルに VPN オンデマンドを有効にするかどうかを指定します。この設定を選択する場合は、この VPN プロファイルを使用するアプリを指定します。このプロファイルで指定されるアプリのみが、このプロファイルの使用を許可されます。 VPN オンデマンドを使用する場合は、指定するアプリが VPN オンデマンドを使用できるように開発されており、アプリが BlackBerry 10 デバイスユーザーに割り当てられており、この VPN プロファイルがデバイスユーザーに割り当てられていることを確認します。 最小要件は、BlackBerry 10 OS バージョン 10.3.3 です。
サーバーアドレス	この設定では、VPN サーバーの FQDN または IP アドレスを指定します。
ゲートウェイの種類	この設定は、BlackBerry 10 デバイスの VPN クライアントがエミュレートする VPN クライアントの種類を指定します。 使用できる値： • Check Point VPN-1 • Cisco VPN 3000 Series Concentrator • Cisco Secure PIX Firewall • Cisco IOS Easy VPN • Cisco ASA Series • Cisco AnyConnect • Juniper SRX Series （IPsec VPN） • Juniper MAG Series または Juniper SA Series （SSL VPN） • Microsoft IKEv2 VPN サーバー • 汎用 IKEv2 VPN サーバー • NIAP 準拠の IKEv2 VPN サーバー デフォルト値は［Check Point VPN-1 ］です。
認証の種類	この設定では、VPN ゲートウェイの認証の種類を指定します。 ［ゲートウェイの種類］によって、サポートされる認証の種類と、この設定のデフォルト値が決定されます。 使用できる値： • PSK • PKI • XAUTH-PSK • XAUTH-PKI • EAP-TLS • EAP-MS-CHAPv2

BlackBerry 10 ：VPN プロファイル設定	説明
事前共有キーまたはグループパスワード	この設定では、VPN ゲートウェイの事前共有キーまたはグループパスワードを指定します。 この設定は、［認証の種類］が［PSK］または［XAUTH-PSK］に設定されている場合のみ有効です。
ユーザー名	この設定では、BlackBerry 10 デバイスが VPN ゲートウェイ認証に使用するユーザー名を指定します。プロファイルが複数のユーザーに対応している場合は、%UserName% 変数を使用できます。 この設定は、［ゲートウェイタイプ］が［Cisco AnyConnect ］に設定されているか、［認証の種類］が［XAUTH-PSK］または［XAUTH-PKI］に設定されている場合のみ有効です。
ハードウェアトークン	この設定では、ユーザーが VPN ゲートウェイでの認証を受けるためにハードウェアトークンを使用する必要があるかどうかを指定します。 この設定は、［認証の種類］が［XAUTH-PSK］または［XAUTH-PKI］に設定されている場合のみ有効です。
パスワード	この設定では、BlackBerry 10 デバイスが VPN ゲートウェイ認証に使用するパスワードを指定します。 この設定は、［ゲートウェイタイプ］が［Cisco AnyConnect ］に設定されているか、［認証の種類］が［XAUTH-PSK］または［XAUTH-PKI］に設定されており、［ハードウェアトークン］が未選択である場合のみ有効です。
EAP ID	この設定では、BlackBerry 10 デバイスが VPN ゲートウェイ認証に使用する EAP ID を指定します。 この設定は、［認証の種類］が［EAP-TLS］に設定されている場合のみ有効です。
EAP-TLS ゲートウェイ ID	この設定は、［ゲートウェイタイプ］設定が［NIAP 準拠の IKEv2 VPN サーバー］に設定され、［認証の種類］が［EAP-TLS］に設定されている場合にのみ有効です。 最小要件は、BlackBerry 10 OS バージョン 10.3.3 です。
MS-CHAPv2 EAP ID	この設定では、BlackBerry 10 デバイスが VPN ゲートウェイ認証に使用する MS-CHAPv2 EAP ID を指定します。 この設定は、［認証の種類］が［EAP-MS-CHAPv2］に設定されている場合のみ有効です。
MS-CHAPv2 ユーザー名	この設定では、BlackBerry 10 デバイスが VPN ゲートウェイ認証に使用する MS-CHAPv2 ユーザー名を指定します。 この設定は、［認証の種類］が［EAP-MS-CHAPv2］に設定されている場合のみ有効です。

BlackBerry 10 ：VPN プロファイル設定	説明
MS-CHAPv2 パスワード	この設定では、BlackBerry 10 デバイスが VPN ゲートウェイ認証に使用する MS-CHAPv2 パスワードを指定します。 この設定は、［認証の種類］が［EAP-MS-CHAPv2］に設定されている場合のみ有効です。
認証 ID の種類	この設定は、VPN ゲートウェイの認証 ID の種類を指定します。 この設定は、［ゲートウェイタイプ］設定が［Juniper MAG Series または Juniper SA Series （SSL VPN）］、［Microsoft IKEv2 VPN サーバー］、［汎用 IKEv2 VPN サーバー］、または［NIAP 準拠の IKEv2 VPN サーバー］に設定されている場合にのみ有効です。 ［ゲートウェイの種類］によって、サポートされる認証 ID の種類と、この設定のデフォルト値が決定されます。 使用できる値： • IPv4 • 完全修飾ドメイン名 • メールアドレス • ID 証明書の識別名 • ID 証明書の一般名 • キー ID
認証 ID またはグループユーザー名	この設定では、VPN ゲートウェイの認証 ID またはグループユーザー名を指定します。 この設定は、［ゲートウェイの種類］が［Juniper MAG Series または Juniper SA Series （SSL VPN）］、［Microsoft IKEv2 VPN サーバー］または［汎用 IKEv2 VPN サーバー］に設定されている場合、または［認証の種類］が［PSK］または［XAUTH-PSK］に設定されている場合のみ有効です。
ゲートウェイ認証の種類	この設定では、VPN ゲートウェイのゲートウェイ認証の種類を指定します。 この設定は、［ゲートウェイの種類］が［Juniper MAG Series または Juniper SA Series （SSL VPN）］、［Microsoft IKEv2 VPN サーバー］または［汎用 IKEv2 VPN サーバー］に設定されている場合にのみ有効です。 使用できる値： • None • PSK • PKI デフォルト値は［なし］です。

BlackBerry 10 ：VPN プロファイル設定	説明
VPN から受信する証明書で OCSP/CRL チェックを有効にする	この設定は、認証時に使用する証明書の証明書失効チェックを有効にします。 この設定は、［ゲートウェイタイプ］設定が［NIAP 準拠の IKEv2 VPN サーバー］に設定され、［認証の種類］設定が［PKI］または［EAP-TLS］に設定されている場合にのみ有効です。 最小要件は、BlackBerry 10 OS バージョン 10.3.3 です。
ゲートウェイの事前共有キー	この設定では、VPN ゲートウェイのゲートウェイ事前共有キーを指定します。 この設定は、［ゲートウェイ認証の種類］が［PSK］に設定されている場合のみ有効です。
ゲートウェイ認証 ID の種類	この設定では、VPN ゲートウェイのゲートウェイ認証 ID の種類を指定します。 この設定は、［ゲートウェイの種類］が［Juniper MAG Series または Juniper SA Series （SSL VPN）］、［Microsoft IKEv2 VPN サーバー］または［汎用 IKEv2 VPN サーバー］に設定されている場合にのみ有効です。 使用できる値： • IPv4 • 完全修飾ドメイン名 • メールアドレス • ID 証明書の識別名 • ID 証明書の一般名 • キー ID デフォルト値は［IPv4］です。
ゲートウェイ認証 ID	この設定では、VPN ゲートウェイのゲートウェイ認証 ID を指定します。 この設定は、［ゲートウェイ認証 ID の種類］が［完全修飾ドメイン名］または［メールアドレス］に設定されている場合のみ有効です。
IKEv2 プロトコルのメッセージ 1 で追加ゲートウェイリクエスト ID を送信する	デフォルト値は［無効］です。 この設定は、［ゲートウェイタイプ］設定が［NIAP 準拠の IKEv2 VPN サーバー］に設定されている場合のみ有効です。 最小要件は、BlackBerry 10 OS バージョン 10.3.3 です。

BlackBerry 10 ：VPN プロファイル設定	説明
要求されたゲートウェイ ID タイプ	この設定は、VPN のリクエストされたゲートウェイ ID タイプを指定します。 この設定は、［ゲートウェイタイプ］設定が［NIAP 準拠の IKEv2 VPN サーバー］に設定され、［IKEv2 プロトコルのメッセージ 1 で要求されたゲートウェイ ID を送信］設定が選択されている場合にのみ有効です。 使用できる値： • IPv4 • 完全修飾ドメイン名 • メールアドレス • ID 証明書の識別名 • ID 証明書の一般名 • キー ID デフォルト値は［IPv4］です。 最小要件は、BlackBerry 10 OS バージョン 10.3.3 です。
要求されたゲートウェイ ID	この設定では、VPN サーバーで複数の ID がサポートされている場合に、ログイン中の最初の IKE メッセージで特定のゲートウェイ ID を要求します。認証に使用するゲートウェイ ID とは異なる場合があります。 この設定は、［ゲートウェイタイプ］設定が［NIAP 準拠の IKEv2 VPN サーバー］に設定され、［IKEv2 プロトコルのメッセージ 1 で要求されたゲートウェイ ID を送信］設定が選択されている場合にのみ有効です。 最小要件は、BlackBerry 10 OS バージョン 10.3.3 です。
セカンダリユーザー名	この設定では、BlackBerry 10 デバイスが VPN ゲートウェイでセカンダリ認証を行うために使用するユーザー名を指定します。プロファイルが複数のユーザーに対応している場合は、%UserName% 変数を使用できます。 この設定は、［ゲートウェイタイプ］が［Cisco AnyConnect ］に設定されている場合のみ有効です。 最小要件は、BlackBerry 10 OS バージョン 10.3.1 です。
セカンダリパスワード	この設定では、BlackBerry 10 デバイスが VPN ゲートウェイでセカンダリ認証を行うために使用するパスワードを指定します。 この設定は、［ゲートウェイタイプ］が［Cisco AnyConnect ］に設定されている場合のみ有効です。 最小要件は、BlackBerry 10 OS バージョン 10.3.1 です。
グループ名	この設定では、VPN ゲートウェイのグループ名を指定します。 この設定は、［ゲートウェイタイプ］が［Cisco AnyConnect ］に設定されている場合のみ有効です。 最小要件は、BlackBerry 10 OS バージョン 10.3.1 です。

BlackBerry 10 ：VPN プロファイル設定	説明
自動クライアント証明書プロセスを有効にする	この設定では、VPN 接続が行われる場合に、クライアント証明書を自動的に選択するかどうかを指定します。 この設定は、［ゲートウェイタイプ］が［Cisco AnyConnect ］に設定されている場合のみ有効です。 最小要件は、BlackBerry 10 OS バージョン 10.3.1 です。
IPsec 認証を有効にする	この設定では、VPN ゲートウェイが IPsec 認証を使用するかどうかを指定します。 この設定は、［ゲートウェイタイプ］が［Cisco AnyConnect ］に設定されている場合のみ有効です。 最小要件は、BlackBerry 10 OS バージョン 10.3.1 です。
IPsec 認証の種類	この設定では、IPsec VPN 接続の認証の種類を指定します。 この設定は、［IPsec 認証を有効にする］設定が選択されている場合のみ有効です。 使用できる値： • EAP-MS-CHAPv2 • EAP-MD5 • EAP-GTC • EAP-AnyConnect • IKE-RSA デフォルト値は［EAP-MS-CHAPv2］です。 最小要件は、BlackBerry 10 OS バージョン 10.3.1 です。
EAP 認証 ID	この設定では、BlackBerry 10 デバイスが VPN ゲートウェイ認証に使用する EAP ID を指定します。 この設定は、［IPsec 認証の種類］が［EAP MSCHAPv2］、［EAP MD5］、または［EAP GTC］に設定されている場合のみ有効です。
サブネットを除外する	この設定では、VPN 接続の使用から指定されたサブネットを除外するかどうかを指定します。 この設定は、［ゲートウェイタイプ］が［Cisco AnyConnect ］に設定されている場合のみ有効です。 最小要件は、BlackBerry 10 OS バージョン 10.3.1 です。
除外サブネット	この設定では、VPN 接続を介して送信しないサブネットおよびサブネットマスクを指定します。 この設定は、［サブネットフラグを除外する］設定が選択されている場合のみ有効です。

BlackBerry 10 ：VPN プロファイル設定	説明
Cisco AnyConnect 設定ファイル（.xml）	この設定では、BlackBerry 10 デバイスに送信する Cisco AnyConnect 設定ファイルの場所を指定します。 この設定は、［ゲートウェイタイプ］が［Cisco AnyConnect ］に設定されている場合のみ有効です。 最小要件は、BlackBerry 10 OS バージョン 10.3.1 です。
仕事用ネットワークでの個人用アプリの使用を許可する	この設定では、BlackBerry 10 デバイス上の個人用アプリケーションが VPN 接続を使用できるようにするかどうかを指定します。 この設定は、［個人用アプリに仕事用ネットワークの使用を許可する］IT ポリシールールが選択されている場合にのみ有効です。 最小要件は、BlackBerry 10 OS バージョン 10.3.1 です。
信頼されない証明書アクション	この設定では、BlackBerry 10 デバイスが信頼されない証明書を受け入れるかどうかを設定します。［許可］に設定すると、デバイスは信頼されない証明書を自動的に受け入れます。［プロンプト］に設定すると、ユーザーは信頼されない証明書を受け入れるかどうかを選択できます。［許可しない］に設定すると、デバイスは信頼されない証明書を受け入れません。 ［ゲートウェイタイプ］の設定によって、サポートする信頼されない証明書アクションと、この設定のデフォルト値が決定されます。 使用できる値： • を許可する • 確認 • 許可しない 最小要件は、BlackBerry 10 OS バージョン 10.3.2 です。

BlackBerry 10 ：VPN プロファイル設定	説明
クライアント証明書のソース	この設定では、BlackBerry 10 デバイスがクライアント証明書を取得可能な方法を指定します。デバイスがクライアント証明書を取得するための 4 つのオプションがあります。 • ［スマートカード］を選択した場合、ユーザーはクライアント証明書を含むスマートカードとデバイスをペアリングする必要があります。 • ［SCEP］を選択した場合は、デバイスがクライアント証明書のダウンロードに使用できる、関連付けられた SCEP プロファイルも指定する必要があります。 • ［ユーザー資格情報］を選択した場合は、デバイスがクライアント証明書のダウンロードに使用できるユーザー資格情報プロファイルも指定する必要があります。 • ［その他］を選択した場合、ユーザーはクライアント証明書をデバイスに手動で追加する必要があります。 スマートカードは、BlackBerry 10 OS バージョン 10.3.1 以降を実行しているデバイスでサポートされています。 この設定は、［認証の種類］が［PKI］または［XAUTH-PKI］に設定されている場合のみ有効です。 使用できる値： • スマートカード • SCEP • ユーザー資格情報 • その他 デフォルト値は［その他］です。
関連付けられた SCEP プロファイル	この設定では、BlackBerry 10 デバイスが VPN 認証に使用するクライアント証明書を取得するための関連付けられた SCEP プロファイルを指定します。 この設定は、［クライアント証明書のソース］が［SCEP］に設定されている場合のみ有効です。
関連付けられたユーザー資格情報プロファイル	この設定では、BlackBerry 10 デバイスが VPN 認証に使用するクライアント証明書を取得するための関連付けられたユーザー資格情報プロファイルを指定します。 この設定は、［クライアント証明書のソース］が［ユーザー資格情報］に設定されている場合のみ有効です。 ユーザー資格情報を使用するための最小要件は、BlackBerry 10 OS バージョン 10.3.1 です。

BlackBerry 10 ：VPN プロファイル設定	説明
IKE ライフタイム	この設定では、IKE 接続のライフタイムを秒単位で指定します。サポートされていない値または Null 値に設定すると、BlackBerry 10 デバイスのデフォルト値が使用されます。 使用できる値は 1〜2,147,483,647 です。
IKE しきい値	この設定では、IKE 有効期間が何パーセントに達したときに VPN クライアントが新しい鍵の交換を開始するかを指定します。 0〜100% を設定できます。 デフォルト値は［90］です。 この設定は、［ゲートウェイタイプ］設定が［NIAP 準拠の IKEv2 VPN サーバー］に設定されている場合のみ有効です。 最小要件は、BlackBerry 10 OS バージョン 10.3.3 です。
IPsec ライフタイム	この設定では、IPsec 接続のライフタイムを秒単位で指定します。サポートされていない値または Null 値に設定すると、BlackBerry 10 デバイスのデフォルト値が使用されます。 使用できる値は 1〜2,147,483,647 です。
IPsec しきい値	この設定では、IPsec しきい値が何パーセントに達したときに VPN クライアントが新しい鍵の交換を開始するかを指定します。 0〜100% を設定できます。 デフォルト値は［90］です。 この設定は、［ゲートウェイタイプ］設定が［NIAP 準拠の IKEv2 VPN サーバー］に設定されている場合のみ有効です。 最小要件は、BlackBerry 10 OS バージョン 10.3.3 です。
VPN 拡張を許可する	この設定では、拡張を有効化または無効化することができます。 この設定は、［ゲートウェイタイプ］設定が［NIAP 準拠の IKEv2 VPN サーバー］に設定されている場合のみ有効です。 最小要件は、BlackBerry 10 OS バージョン 10.3.3 です。
VPN 拡張リスト	この設定を使用して、ベンダー ID ペイロードの生成に使用される拡張のリストを入力し、証明書の追加検証を行うことができます。 この設定は、［ゲートウェイタイプ］設定が［NIAP 準拠の IKEv2 VPN サーバー］に設定され、［VPN 拡張を許可する］設定が選択されている場合にのみ有効です。 最小要件は、BlackBerry 10 OS バージョン 10.3.3 です。

BlackBerry 10 ：VPN プロファイル設定	説明
ベンダー ID 拡張を必須にする	この設定では、ログイン中に管理者が VPN 拡張リストのいずれかの拡張を使用して、ベンダー ID ペイロードを生成する必要があることを示します。 この設定は、［ゲートウェイタイプ］設定が［NIAP 準拠の IKEv2 VPN サーバー］に設定され、［VPN 拡張を許可する］設定が選択されている場合にのみ有効です。 最小要件は、BlackBerry 10 OS バージョン 10.3.3 です。
証明書検証の拡張を要求	この設定は、管理者がいずれかの拡張を使用して、証明書の追加検証を実行する必要があることを示します。 この設定は、［ゲートウェイタイプ］設定が［NIAP 準拠の IKEv2 VPN サーバー］に設定され、［VPN 拡張を許可する］設定が選択されている場合にのみ有効です。 最小要件は、BlackBerry 10 OS バージョン 10.3.3 です。
セッション再開を有効化	この設定では、IKEv2 セッションの再開設定が有効に設定されます。VPN サーバーがこの機能をサポートしている場合、VPN クライアントは、接続を完全に切断してから再接続する代わりに、セッションを一時中断し、VPN 自動接続が有効になったと同時にセッションを再開します。 この設定は、［ゲートウェイタイプ］設定が［NIAP 準拠の IKEv2 VPN サーバー］に設定されている場合のみ有効です。 最小要件は、BlackBerry 10 OS バージョン 10.3.3 です。
チケットのしきい値	この設定は、チケットのしきい値の何パーセントに達したときにセッションを再開するかを指定します。 0〜100% を設定できます。 デフォルト値は［90］です。 この設定は、［ゲートウェイタイプ］設定が［NIAP 準拠の IKEv2 VPN サーバー］に設定され、［セッション再開を有効にする］設定が選択されている場合にのみ有効です。 最小要件は、BlackBerry 10 OS バージョン 10.3.3 です。
IKE 中にハッシュおよび URL 形式の証明書ペイロードを有効にする	この設定は、URL を使用して証明書を交換し、利用可能な場合に提供された HTTP URL から証明書を取得するために、VPN クライアントが IKEv2 の使用をサポートする VPN サーバーに通知するかどうかを指定します。 この設定は、［ゲートウェイタイプ］設定が［NIAP 準拠の IKEv2 VPN サーバー］に設定されている場合のみ有効です。 最小要件は、BlackBerry 10 OS バージョン 10.3.3 です。

BlackBerry 10 ：VPN プロファイル設定	説明
承認済みアルゴリズムを厳密に強制する	この設定は、NIAP 認定のアルゴリズムの使用が正確に実施されているかどうかを指定します。 この設定は、［ゲートウェイタイプ］設定が［NIAP 準拠の IKEv2 VPN サーバー］に設定されている場合のみ有効です。 最小要件は、BlackBerry 10 OS バージョン 10.3.3 です。
分割トンネル	この設定では、VPN ゲートウェイがスプリットトンネリングをサポートしている場合、BlackBerry 10 デバイスがスプリットトンネリングを使用して、VPN ゲートウェイをバイパスできるようにするかどうかを指定します。 ［ゲートウェイタイプ］設定が［NIAP 準拠の IKEv2 VPN サーバー］に設定されている場合は、この設定は有効ではありません。
バナーを無効にする	この設定では、BlackBerry 10 デバイスが VPN バナーをブロックするかどうかを指定します。 ［ゲートウェイタイプ］設定が［NIAP 準拠の IKEv2 VPN サーバー］に設定されている場合は、この設定は有効ではありません。
信頼済み証明書ソース	この設定では、信頼済み証明書のソースを指定します。これが［信頼済み証明書ストア］に設定されている場合、BlackBerry 10 デバイスは VPN 証明書ストアの証明書を使用している VPN に接続できます。 この設定は、［認証の種類］が［PKI］または［XAUTH-PKI］に設定されている場合のみ有効です。 使用できる値： • None • 信頼済み証明書ストア デフォルト値は［なし］です。
自動的に IP を決定	この設定では、BlackBerry 10 デバイスが VPN ゲートウェイの IP 設定を自動的に決定するかどうかを指定します。
プライベート IP	この設定では、VPN ゲートウェイのプライベート IP を指定します。 この設定は、［自動的に IP を決定］設定が選択されていない場合のみ有効です。
プライベート IP マスク	この設定では、VPN ゲートウェイのプライベート IP マスクを指定します。 この設定は、［自動的に IP を決定］設定が選択されていない場合のみ有効です。
サブネット	この設定では、VPN ゲートウェイのサブネットを指定します。 この設定は、［自動的に IP を決定］設定が選択されていない場合のみ有効です。

BlackBerry 10 ：VPN プロファイル設定	説明
サブネットマスク	この設定では、VPN ゲートウェイのサブネットマスクを指定します。 この設定は、［自動的に IP を決定］設定が選択されていない場合のみ有効です。
自動的に DNS を決定	この設定では、BlackBerry 10 デバイスが VPN ゲートウェイの DNS 設定を自動的に決定するかどうかを指定します。
プライマリ DNS	この設定では、ドット付き 10 進表記（たとえば、192.0.2.0）でプライマリ DNS サーバーを指定します。 この設定は、［自動的に DNS を決定］設定が選択されていない場合のみ有効です。
セカンダリ DNS	この設定では、ドット付き 10 進表記（たとえば、192.0.2.0）でセカンダリ DNS サーバーを指定します。 この設定は、［自動的に DNS を決定］設定が選択されていない場合のみ有効です。
ドメインサフィックス	この設定では、DNS サフィックスの FQDN を指定します。 この設定は、［自動的に DNS を決定］設定が選択されていない場合のみ有効です。
Perfect Forward Secrecy	この設定では、VPN ネットワークが PFS をサポートするかどうかを指定します。 この設定が選択されている場合は、［IPsec DH グループ］は 0 以外に設定する必要があります。
アルゴリズムを手動選択	この設定では、VPN ゲートウェイの暗号化アルゴリズムを設定する必要があるかどうかを指定します。
IKE DH グループ	この設定では、BlackBerry 10 デバイスがキーマテリアルを生成するために使用する DH グループを指定します。 この設定は、［アルゴリズムを手動選択］設定が選択されている場合のみ有効です。 使用できる値： • 1～26（3、4、6 を除く） • カスタム 1～カスタム 5 デフォルト値は［1］です。
カスタム IKE DH プロバイダー	この設定では、カスタム IKE DH のプロバイダーの名前を指定します。 この設定は、［IKE DH グループ］がカスタム値のいずれかに設定されている場合のみ有効です。

BlackBerry 10 ：VPN プロファイル設定	説明
MOBIKE を有効にする	この設定では、VPN ゲートウェイが MOBIKE をサポートするかどうかを指定します。 この設定は、［ゲートウェイタイプ］が［Microsoft IKEv2 VPN サーバー］または［汎用 IKEv2 VPN サーバー］に、［認証の種類］が［PKI］、［IKE DH グループ］がカスタム値のいずれかに設定されている場合のみ有効です。 最小要件は、BlackBerry 10 OS バージョン 10.3.1 です。
IKE 暗号	この設定では、BlackBerry 10 デバイスが共有の秘密鍵を生成するために使用するアルゴリズムを指定します。 この設定は、［アルゴリズムを手動選択］設定が選択されている場合のみ有効です。 使用できる値： • None • DES（56 ビットキー） • 3DES（168 ビットキー） • AES（128 ビットキー） • AES（192 ビットキー） • AES（256 ビットキー） デフォルト値は［なし］です。
IKE ハッシュ	この設定では、BlackBerry 10 デバイスが IKE とともに使用するハッシュ関数を指定します。 この設定は、［アルゴリズムを手動選択］設定が選択されている場合のみ有効です。 使用できる値： • None • MD5 • AES-XCBC • SHA-1 • SHA-256 • SHA-384 • SHA-512 デフォルト値は［なし］です。

BlackBerry 10 ：VPN プロファイル設定	説明
IKE PRF	この設定では、BlackBerry 10 デバイスが IKE とともに使用する PRF を指定します。 この設定は、［アルゴリズムを手動選択］設定が選択されている場合のみ有効です。 使用できる値： • None • HMAC • HMAC-MD5 • AES-XCBC • HMAC-SHA-1 • HMAC-SHA-256 • HMAC-SHA-384 • HMAC-SHA-512 デフォルト値は［なし］です。
IPsec DH グループ	この設定では、BlackBerry 10 デバイスが IPsec とともに使用する DH グループを指定します。 この設定は、［アルゴリズムを手動選択］設定が選択されている場合のみ有効です。 使用できる値は、0〜26（3、4、6 を除く）です。 デフォルト値は［0］です。
IPsec 暗号	この設定では、BlackBerry 10 デバイスが IPsec とともに使用するアルゴリズムを指定します。 この設定は、［アルゴリズムを手動選択］設定が選択されている場合のみ有効です。 使用できる値： • None • DES（56 ビットキー） • 3DES（168 ビットキー） • AES（128 ビットキー） • AES（192 ビットキー） • AES（256 ビットキー） デフォルト値は［なし］です。

BlackBerry 10 ：VPN プロファイル設定	説明
IPsec ハッシュ	この設定では、BlackBerry 10 デバイスが IPsec とともに使用するハッシュ関数を指定します。 この設定は、［アルゴリズムを手動選択］設定が選択されている場合のみ有効です。 使用できる値： • None • MD5 • AES-XCBC • SHA-1 • SHA-256 • SHA-384 • SHA-512 デフォルト値は［なし］です。
NAT キープアライブ	この設定では、デバイスが NAT キープアライブパケットを送信する頻度を指定します。サポートされていない値または Null 値に設定すると、BlackBerry 10 デバイスのデフォルト値が使用されます。 使用できる値は 1〜2,147,483,647 です。
DPD 実行頻度	この設定では、DPD の頻度を秒単位で指定します。BlackBerry 10 デバイスは最小値として 10 秒をサポートしています。サポートされていない値または Null 値に設定すると、デバイスのデフォルト値が使用されます。 使用できる値は 1〜2,147,483,647 です。
ユーザーが編集可能	この設定では、BlackBerry 10 デバイスユーザーが変更できる VPN 設定を指定します。これが［読み取り専用］に設定されている場合、ユーザーはどの設定も変更できません。これが［資格情報のみ］に設定されている場合、ユーザーはユーザー名とパスワードを変更できます。 使用できる値： • 読み取り専用 • 資格情報のみ デフォルト値は［読み取り専用］です。

BlackBerry 10 ：VPN プロファイル設定	説明
デバイスに VPN 情報を表示する	この設定では、BlackBerry 10 デバイスに VPN 情報を表示するかどうかを指定します。この設定が［表示可能］に設定されている場合、VPN プロファイル情報の大半がデバイスに表示されます。この設定が［非表示］に設定されている場合、プロファイル名のみがデバイスに表示されます。この設定が［資格情報のみ］に設定されている場合、プロファイル名と資格情報フィールドがデバイスに表示されます。 使用できる値： • 表示可能 • 非表示 • 資格情報のみ デフォルト値は［表示可能］です。
データセキュリティレベル	この設定では、仕事用領域が高度な保存データ保護を使用している場合に、VPN プロファイルが保存される仕事用領域内のドメインを指定します。この設定は、［高度な保存データ保護を強制する］IT ポリシールールが選択されている場合にのみ有効です。これが［常時使用可能］に設定されている場合、プロファイルは起動（Startup）ドメインに保存され、仕事用領域がロックされている場合に使用できます。これが［認証後に使用可能］に設定されている場合、プロファイルは操作（Operational）ドメインに保存され、仕事用領域がロック解除された後、デバイスが再起動されるまで使用可能です。これが［仕事用領域がロック解除された場合のみ使用可能］に設定されている場合、プロファイルはロック（Lock）ドメインに保存され、仕事用領域がロック解除されている場合のみ VPN 接続用に使用できます。 使用できる値： • 常時使用可能 • 認証後に使用可能 • 仕事用領域がロック解除された場合のみ使用可能 デフォルト値は［常に使用可能］です。 最小要件は、BlackBerry 10 OS バージョン 10.3.1 です。
関連付けられているプロキシプロファイル	この設定では、BlackBerry 10 デバイスが VPN に接続されている場合に、プロキシサーバーに接続するために使用する関連付けられているプロキシプロファイルを指定します。

per-app VPN の有効化

iOS、Samsung Knox、および Windows 10 デバイスの per-app VPN を設定して、デバイスで、どのアプリがデータ送信に VPN を使用する必要があるかを指定できます。per-app VPN は、特定の仕事用トラフィック（たとえば、ファイアウォール内のアプリケーションサーバーまたは Web ページへのアクセス）のみが VPN を使用できるようにすることで、組織の VPN の負荷の軽減を促進します。オンプレミス環境では、この機能でユーザーの

プライバシーもサポートし、VPN 経由で個人用トラフィックを送信しないため、個人用アプリの接続速度も高めます。

iOS デバイスでは、アプリまたはアプリグループをユーザー、ユーザーグループ、またはデバイスグループに割り当てるときに、アプリが VPN プロファイルに関連付けられます。

Android Enterprise および Samsung Knox Workspace でアクティベーションされた Samsung Knox デバイスでは、アプリは VPN プロファイルの［VPN 接続の使用を許可されたアプリ］設定に追加されます。

Windows 10 デバイスでは、アプリは VPN プロファイルの［アプリトリガーリスト］設定に追加されます。

iOS デバイスに割り当てる per-app VPN 設定を BlackBerry UEM が選択する方法

1 つの VPN プロファイルのみをアプリまたはアプリグループに割り当てることができます。BlackBerry UEM は、次のルールを使用して、どの per-app VPN 設定を iOS デバイスのアプリに割り当てるかを決定します。

- アプリに直接関連付けられた per-app VPN 設定は、アプリグループによって間接的に関連付けられた per-app VPN 設定より優先されます。
- ユーザーに直接関連付けられた per-app VPN 設定は、ユーザーグループによって間接的に関連付けられた per-app VPN 設定より優先されます。
- 必須のアプリに割り当てられた per-app VPN 設定は、同じアプリのオプションのインスタンスに割り当てられた per-app VPN 設定より優先されます。
- 次の条件が満たされる場合は、アルファベット順のリストで先に現れるユーザーグループ名に関連付けられた per-app VPN 設定が優先されます。
  - アプリが複数のユーザーグループに割り当てられている
  - 同じアプリがユーザーグループ内に表示される
  - アプリが同じ方法で割り当てられている（単一のアプリとして、またはアプリグループとして）
  - アプリがすべての割り当てで同じ種別である（必須またはオプション）

  たとえば、Cisco WebEx Meetings をオプションアプリとしてユーザーグループの Development および Marketing に割り当てます。ユーザーが両方のグループに属する場合、Development グループの per-app VPN 設定がそのユーザーの WebEx Meetings アプリに適用されます。

per-app VPN プロファイルがデバイスグループに割り当てられている場合は、デバイスグループに属するデバイスのユーザーアカウントに割り当てられている per-app VPN プロファイルより優先されます。

デバイスのプロキシプロファイルのセットアップ

デバイスがプロキシサーバーを使用してインターネットまたは仕事用ネットワーク上の Web サービスにアクセスする方法を指定できます。iOS、macOS、Android、および BlackBerry 10 の各デバイスの場合は、プロキシプロファイルを作成します。Windows 10 デバイスの場合は、プロキシ設定を Wi-Fi または VPN プロファイルに追加します。

特に明記されていない限り、プロキシプロファイルは、基本認証を使用しているか、認証を使用していないプロキシサーバーをサポートします。

デバイス	プロキシ設定
BlackBerry 10	プロキシプロファイルを作成して、所属組織が使用しているプロファイルに関連付けます。ファイルには次の情報を含めることができます。 • Wi-Fi • VPN • エンタープライズ接続
iOS	プロキシプロファイルを作成して、所属組織が使用しているプロファイルに関連付けます。ファイルには次の情報を含めることができます。 • Wi-Fi • VPN また、プロキシプロファイルは、ユーザーアカウント、ユーザーグループ、またはデバイスグループに割り当てることもできます。 メモ：ユーザーアカウント、ユーザーグループ、またはデバイスグループに割り当てられるプロキシプロファイルは、管理されたデバイスの場合に対してのみグローバルプロキシです。これは、Wi-Fi または VPN プロファイルに関連付けられたプロキシプロファイルよりも優先されます。管理されたデバイスはすべての HTTP 接続でグローバルプロキシ設定を使用します。
macOS	プロキシプロファイルを作成して、Wi-Fi または VPN プロファイルに関連付けます。 macOS は、ユーザーアカウントまたはデバイスにプロファイルを適用します。プロキシプロファイルはデバイスに適用されます。
Android	Android Enterprise デバイスでは、プロキシプロファイル作成して Wi-Fi プロファイルに関連付けます。 Android 8.0 以降のデバイスで、アクティベーションが MDM 制御 または ユーザーのプライバシー のデバイスは、プロキシ設定が含まれる Wi-Fi プロファイルをサポートしていません。これらのいずれかのアクティベーションタイプのデバイスを Android 8.0 にアップグレードすると、プロキシプロファイルが関連付けられている Wi-Fi プロファイルは、デバイスから削除されます。

デバイス	プロキシ設定
Samsung Knox	プロキシプロファイルを作成して、所属組織が使用しているプロファイルに関連付けます。次の条件が適用されます。 • Wi-Fi プロファイルの場合、Knox デバイスでは、手動設定が指定されたプロキシプロファイルのみがサポートされます。Wi-Fi プロファイルに関連付けられているプロキシプロファイルでは、基本認証または NTLM 認証を使用しているプロキシサーバー、および認証を使用していないプロキシサーバーがサポートされます。 • VPN およびエンタープライズ接続プロファイルの場合、Android Enterprise アクティベーションが行われた Samsung Knox デバイスおよび Knox 2.5 以降を使用する Samsung Knox Workspace デバイスでは、手動設定が指定されたプロキシプロファイルがサポートされます。Android Enterprise アクティベーションが行われた Samsung Knox デバイスおよび 2.5 よりも後のバージョンの Knox を使用する Knox Workspace デバイスでは、PAC 設定が指定されたプロキシプロファイルがサポートされます。 メモ： エンタープライズ接続プロファイルを含むプロキシプロファイルを使用するには、BlackBerry Secure Connect Plus を有効化する必要があります。 また、プロキシプロファイルは、ユーザーアカウント、ユーザーグループ、またはデバイスグループに割り当てることもできます。次の条件が適用されます。 • Knox Workspace デバイスおよび Android Enterprise アクティベーションが行われた Samsung Knox デバイスの場合、プロファイルは仕事用領域のブラウザープロキシ設定を設定します。 • Samsung Knox MDM デバイスの場合、プロファイルはデバイスのブラウザープロキシを設定します。 メモ： Knox 2.5 以前を使用する Knox Workspace デバイスと Knox MDM デバイスでは、PAC 設定はサポートされません。
Windows 10	Wi-Fi プロファイルまたは VPN プロファイルを作成し、プロファイル設定でプロキシサーバー情報を指定します。次の条件が適用されます。 • Wi-Fi プロキシでは手動設定のみがサポートされます。このプロキシは、Windows 10 Mobile デバイスでのみサポートされます。 • VPN プロキシでは、PAC 設定または手動設定がサポートされます。

プロキシプロファイルの作成

組織が PAC ファイルを使用してプロキシルールを定義している場合は、PAC 設定を選択して、指定した PAC ファイル内のプロキシサーバー設定を使用できます。それ以外の場合は、手動での設定を選択して、プロキシサーバー設定を直接プロファイルに指定できます。

1. メニューバーで［ポリシーとプロファイル］をクリックします。
2. ［ネットワークと接続］ > ［プロキシ］をクリックします。
3. ＋ をクリックします。
4. プロキシプロファイルの名前と説明を入力します。

5. デバイスタイプのタブをクリックします。
6. 次のタスクのいずれかを実行します。

タスク	手順
PAC 設定を指定する	**a.** ［種類］ドロップダウンリストで、［**PAC** 設定］オプションが選択されていることを確認します。 **b.** ［**PAC URL**］フィールドで、PAC ファイルをホストする Web サーバーの URL を、PAC ファイル名まで含めて入力します（たとえば、http://www.example.com/PACfile.pac）。BlackBerry UEM またはその任意のコンポーネントをホストしているサーバーでは、PAC ファイルをホストしないでください。 **c.** ［**BlackBerry**］タブで、次の操作を実行します。 **1.** 組織により、プロキシサーバーに接続する際にユーザーがユーザー名とパスワードを入力することが義務付けられていて、かつプロファイルが複数のユーザーに対応している場合は、［ユーザー名］フィールドに「`%UserName%`」と入力します。プロキシサーバーが認証用のドメイン名を必要とするる場合は、<ドメイン>\<ユーザー名> 形式を使用します。 **2.** ［ユーザーが編集可能］ドロップダウンリストで、BlackBerry 10 デバイスのユーザーが変更できるプロキシ設定をクリックします。デフォルト設定は、［読み取り専用］です。
手動設定を指定する	**a.** ［種類］ドロップダウンリストで、［手動設定］をクリックします。 **b.** ［ホスト］フィールドに、プロキシサーバーの FQDN または IP アドレスを入力します。 **c.** ［ポート］フィールドに、プロキシサーバーのポート番号を入力します。 **d.** 組織により、プロキシサーバーに接続する際にユーザーがユーザー名とパスワードを入力することが義務付けられていて、かつプロファイルが複数のユーザーに対応している場合は、［ユーザー名］フィールドに「`%UserName%`」と入力します。プロキシサーバーが認証用のドメイン名を必要とするる場合は、<ドメイン>\<ユーザー名> 形式を使用します。 **e.** ［**BlackBerry**］タブで、次の操作を実行します。 **1.** ［ユーザーが編集可能］ドロップダウンリストで、BlackBerry 10 デバイスのユーザーが変更できるプロキシ設定をクリックします。デフォルト設定は、［読み取り専用］です。 **2.** ユーザーがプロキシサーバーを使用せずに BlackBerry 10 デバイスから直接アクセスできるアドレスのリストを、オプションで指定できます。［除外リスト］フィールドでは、アドレス（FQDN または IP）を入力し、セミコロン（;）を使用してリスト内の値を区切ります。FQDN または IP でワイルドカード文字（*）を使用することができます（*.example.com、192.0.2.* など）。

7. 組織内のデバイスタイプごとに手順 4 と 5 を繰り返します。
8. ［追加］をクリックします。

終了したら：

- プロキシプロファイルを Wi-Fi、VPN、または エンタープライズ接続プロファイルに関連付けます。
- 必要に応じて、プロファイルをランク付けします。指定したランキングは、プロキシプロファイルをユーザーグループまたはデバイスグループに割り当てた場合のみ適用されます。

BlackBerry Secure Connect Plus を使用した仕事用リソースへの接続

BlackBerry Secure Connect Plus は、アプリと組織のネットワークとの間にセキュリティ保護された IP トンネルを提供する BlackBerry UEM コンポーネントです。

- Android Enterprise および BlackBerry 10 デバイスの場合、すべての仕事用アプリはセキュリティ保護されたトンネルを使用します。
- Samsung Knox Workspace デバイスおよび Android Enterprise アクティベーションが行われた Samsung Knox デバイスの場合、すべての仕事用領域アプリでトンネルを使用することも、per-app VPN を使用するアプリを指定することもできます。
- iOS デバイスの場合は、すべてのアプリでトンネルを使用することも、per-app VPN を使用するアプリを指定することもできます。

メモ： BlackBerry Secure Connect Plus を使用できない地域では、エンタープライズ接続プロファイル内で、Android デバイスに対して手動で無効にする必要があります。

セキュリティで保護された IP トンネルによって、ユーザーは、組織のファイアウォール内の仕事用リソースにアクセスするときに、標準のプロトコルとエンドツーエンドの暗号化を使用して、データのセキュリティを確保できます。

BlackBerry Secure Connect Plus およびサポートされているデバイスは、組織のネットワーク接続に最適なオプションである場合、セキュリティ保護された IP トンネルを確立します。デバイスに Wi-Fi プロファイルまたは VPN プロファイルが割り当てられていて、かつデバイスから仕事用の Wi-Fi ネットワークまたは VPN にアクセスできる場合、デバイスはこれらの方法を使用してネットワークに接続します。これらのオプションを使用できない場合（たとえば、ユーザーが仕事用 Wi-Fi ネットワークの範囲内にいない場合）、BlackBerry Secure Connect Plus とデバイスがセキュリティ保護された IP トンネルを確立します。

iOS デバイスで、BlackBerry Secure Connect Plus 用の per-app VPN を設定している場合、VPN プロファイルで指定された仕事用 Wi-Fi ネットワークまたは VPN に接続できる状況であっても、この設定が行われたアプリは常に BlackBerry Secure Connect Plus を介してセキュリティ保護されたトンネルを使用します。

サポートされているデバイスは、BlackBerry UEM と通信し、BlackBerry Infrastructure を介してセキュリティ保護されたトンネルを確立します。それぞれのデバイスに対して 1 つのトンネルが確立されます。トンネルは標準 IPv4 プロトコル（TCP と UDP）をサポートし、デバイスと BlackBerry UEM の間で送信される IP トラフィックは AES256 を使用してエンドツーエンドで暗号化されます。トンネルが開いている限り、アプリはネットワークリソースにアクセスできます。トンネルが不要になった場合（ユーザーが勤務先の Wi-Fi ネットワーク範囲内にいる場合など）は、接続が終了します。

BlackBerry Secure Connect Plus でデータをデバイスに、またはデバイスから転送する方法の詳細については、「オンプレミスアーキテクチャに関する資料」または「クラウドアーキテクチャに関する資料」を参照してください。

BlackBerry Secure Connect Plus を有効にする手順

BlackBerry Secure Connect Plus を有効にする場合は、次の操作を実行します。

手順	アクション
1	組織の BlackBerry UEM ドメインが、BlackBerry Secure Connect Plus を使用するための要件を満たしていることを確認します。
2	BlackBerry UEM Cloud がある場合は、BlackBerry Connectivity Node をインストールするか、BlackBerry Connectivity Node を最新バージョンにアップグレードします。
3	デフォルトのエンタープライズ接続プロファイルまたは作成したカスタムエンタープライズ接続プロファイルで、BlackBerry Secure Connect Plus を有効にします。
4	オプションで、BlackBerry Connectivity アプリの DNS 設定を指定します。
5	BlackBerry Dynamics が有効になっている Android Enterprise デバイスと Samsung Knox Workspace デバイスがオンプレミス環境にある場合は、セキュリティで保護されたトンネル接続を最適化します。
6	エンタープライズ接続プロファイルをユーザーアカウント、またはユーザーグループに割り当てます。

BlackBerry Secure Connect Plus のサーバーとデバイスの要件

BlackBerry Secure Connect Plus を使用するには、組織の環境が次の要件を満たしている必要があります。

BlackBerry UEM ドメインの要件：

- 組織のファイアウォールは、ポート 3101 を介した <リージョン>.turnb.bbsecure.com、および <リージョン>.bbsecure.com へのアウトバウンド接続を許可する必要があります。BlackBerry UEM でプロキシサーバーを使用する設定にしている場合は、これらのプロキシサーバーで、これらのサブドメインへのポート 3101 経由での接続が許可されていることを確認します。ファイアウォール設定で使用するドメインおよび IP アドレスの詳細については、http://support.blackberry.com/community にアクセスし、記事 36470 を参照してください。
- 個々の BlackBerry UEM インスタンスで、BlackBerry Secure Connect Plus コンポーネントを実行している必要があります。
- デフォルトでは、Android Enterprise デバイスは Google Play と基盤サービス（com.android.providers.media、com.android.vending、および com.google.android.apps.gcs）への接続に BlackBerry Secure Connect Plus を使用できないという制限があります。Google Play はプロキシをサポートしていません。Android Enterprise デバイスは、インターネット経由で Google Play に直接接続します。これらの制限は、デフォルトのエンタープライズ接続プロファイルおよび作成した新しいカスタムエンタープライズ接続プロファイルで設定されています。これらの制限はそのまま適用することをお勧めします。これらの制限を削除するには、BlackBerry Secure Connect Plus を使用した Google Play への接続を許可するファイアウォール設定について、Google Play サポートに問い合わせる必要があります。
- BlackBerry UEM Cloud がある場合は、BlackBerry Connectivity Node をインストールするか、最新バージョンにアップグレードする必要があります。

メモ： オンプレミス環境に BlackBerry Dynamics アプリを搭載した Knox Workspace または Android Enterprise デバイスが含まれている場合は、「BlackBerry Dynamics アプリを使用する Android デバイスのためにセキュリティ保護されたトンネル接続を最適化する」を参照してください。

メモ： BlackBerry Secure Gateway デバイスで iOS を有効にするためにメールプロファイルを使用する場合は、BlackBerry Secure Connect Plus 向けに per-app VPN を設定することをお勧めします。BlackBerry Secure Gateway の詳細については、「BlackBerry Secure Gateway を使用してメールデータを保護する」を参照してください。

サポート対象のデバイスでは：

デバイス	要件
iOS	• BlackBerry UEM Client から入手できる App Store を使用して、デバイスをアクティブ化する必要があります • MDM 制御 アクティベーションタイプ

Android Enterprise	• 次のいずれかのアクティベーションタイプ：
	  • 仕事用領域のみ（Premium）
	  • 仕事用と個人用 - フルコントロール（Premium）
	  • 仕事用と個人用 - ユーザーのプライバシー（Premium）

Samsung Knox Workspace	• Samsung Knox MDM 5.0 以降
	• Samsung Knox 2.3 以降
	• 次のいずれかのアクティベーションタイプ：
	  • 仕事用領域のみ（Samsung Knox）
	  • 仕事用と個人用 - フルコントロール（Samsung Knox）
	  • 仕事用と個人用 - ユーザーのプライバシー（Samsung Knox）

BlackBerry 10	• BlackBerry 10 OS バージョン 10.3.2 以降
	• 次のいずれかのアクティベーションタイプ：
	  • 仕事用と個人用 - 会社
	  • 仕事用領域のみ
	  • 仕事用と個人用 - 制限付き

オンプレミス環境での追加 BlackBerry Secure Connect Plus コンポーネントのインストール

BlackBerry Connectivity Node の 1 つ以上のインスタンスをインストールして、デバイス接続コンポーネントの追加インスタンスを組織のドメインに追加できます。それぞれの BlackBerry Connectivity Node には、デバイスデータを処理し、セキュアな接続を確立できる BlackBerry Secure Connect Plus のアクティブなインスタンスが含まれています。

サーバーグループを作成することもできます。サーバーグループには、BlackBerry Connectivity Node の インスタンスが 1 つ以上含まれています。サーバーグループを作成するときに、コンポーネントが BlackBerry Infrastructure に接続するために使用する地域データパスを指定します。たとえば、サーバーグループを作成し

て、BlackBerry Secure Connect Plus のデバイス接続と BlackBerry Secure Gateway に、BlackBerry Infrastructure への米国のパスを使用するように指示することができます。メールとエンタープライズ接続プロファイルをサーバーグループに関連付けることができます。これらのプロファイルが割り当てられているどのデバイスも、BlackBerry Infrastructure のいずれかのコンポーネントを使用するときには、そのサーバーグループの BlackBerry Connectivity Node への地域接続を使用します。

ドメインに複数の BlackBerry UEM インスタンスが含まれる場合は、それぞれのインスタンス内で BlackBerry Secure Connect Plus コンポーネントが実行され、データを処理します。データはドメイン内のすべての BlackBerry Secure Connect Plus コンポーネントに負荷分散されています。

高可用性フェールオーバーは、BlackBerry Secure Connect Plus で利用できます。デバイスがセキュリティ保護されたトンネルを使用しており、現在の BlackBerry Secure Connect Plus コンポーネントが利用不可能になった場合、BlackBerry Infrastructure はその他の BlackBerry UEM インスタンス上の BlackBerry Secure Connect Plus コンポーネントにデバイスを割り当てます。中断を最小限に抑え、デバイスはセキュリティ保護されたトンネルの使用を再開します。

BlackBerry Connectivity Node の計画およびインストールの詳細については、計画関連の資料とインストールおよびアップグレード関連の資料を参照してください。

クラウド環境での BlackBerry Secure Connect Plus コンポーネントのインストールまたはアップグレード

BlackBerry Connectivity Node をインストールする際に、セットアッププロセスは同じコンピューターに BlackBerry Secure Connect Plus コンポーネントもインストールします。BlackBerry Connectivity Node を最新バージョンにアップグレードする際に、BlackBerry Secure Connect Plus がインストールされていない場合、アップグレードプロセスは BlackBerry Secure Connect Plus をインストールします。BlackBerry Secure Connect Plus が以前にインストールされていた場合は、プロセスは BlackBerry Secure Connect Plus を最新バージョンにアップグレードします。

BlackBerry Connectivity Node のインストールまたはアップグレード手順については、BlackBerry UEM Cloud の設定関連の資料の「BlackBerry Connectivity Node のインストールまたはアップグレード」を参照してください。BlackBerry Secure Connect Plus を有効にするには、BlackBerry Connectivity Node をアクティブ化する必要があります。

オプションとして、BlackBerry Secure Connect Plus と BlackBerry Infrastructure の間で転送されるデータを、BlackBerry Router または TCP プロキシサーバー（透過型または SOCKS v5）を介してルーティングできます。BlackBerry Connectivity Node 管理コンソールを使用してプロキシ設定を設定できます（［一般設定］ > ［プロキシ］）。

メモ： 有効でないプロキシ情報を指定した場合、BlackBerry Secure Connect Plus は実行を停止し再起動されません。この問題が発生した場合は、プロキシ情報を修正し、Windows サービスで BlackBerry UEM - BlackBerry Secure Connect Plus サービスを再起動します。

冗長性を確保するために 2 つ目の BlackBerry Connectivity Node をインストールできます。BlackBerry Secure Connect Plus の両方のインスタンスが実行され、データを処理します。データは両インスタンス間で負荷分散されます。デバイスがセキュリティ保護されたトンネルを使用しており、現在の BlackBerry Secure Connect Plus インスタンスが利用不可能になった場合、BlackBerry Infrastructure はその他のインスタンスにデバイスを割り当てます。中断を最小限に抑え、デバイスはセキュリティ保護されたトンネルの使用を再開します。

BlackBerry Secure Connect Plus を有効化する

デバイスに BlackBerry Secure Connect Plus の使用を許可するには、エンタープライズ接続プロファイルで BlackBerry Secure Connect Plus を有効にし、プロファイルをユーザーおよびグループに割り当てる必要があります。

アクティベーション後に、このエンタープライズ接続プロファイルをデバイスに適用すると、BlackBerry UEM は BlackBerry Connectivity アプリをデバイスにインストールします（Android Enterprise デバイスの場合、アプリは自動的に Google Play からインストールされます。iOS デバイスの場合、アプリは自動的に App Store からインストールされます）。BlackBerry 10 デバイスでは、このアプリは非表示になっているので、ユーザーの介入は必要ありません。

BlackBerry は、新しい機能と拡張機能をサポートする新しいバージョンのアプリをリリースしました。アプリをアップグレードする手順と、最新の既知の問題および解決済みの問題については、BlackBerry Connectivity アプリのリリースノートを参照してください。

1. 管理コンソールのメニューバーで、［ポリシーとプロファイル］をクリックします。
2. ［ネットワークと接続］ > ［エンタープライズ接続］をクリックします。
3. ＋ をクリックします。
4. BlackBerry Infrastructure への特定の地域パスに BlackBerry Secure Connect Plus トラフィックを転送するために、1 つ以上のサーバーグループを作成して設定した場合は、［**BlackBerry Secure Connect Plus**］ドロップダウンリストで適切なサーバーグループをクリックします。
5. 各デバイスタイプのプロファイル設定に適切な値を設定します。各プロファイル設定の詳細については、「エンタープライズ接続プロファイル設定」を参照してください。
6. ［追加］をクリックします。
7. プロファイルをグループまたはユーザーアカウントに割り当てます。
8. iOS デバイス用に per-app VPN を設定した場合は、アプリまたはアプリグループを割り当てる際に、これを適切なエンタープライズ接続プロファイルに関連付けます。

終了したら：

- Android Enterprise および Samsung Knox Workspace デバイスでは、VPN としての実行、およびデバイスのプライベートキーへのアクセスを BlackBerry Connectivity アプリに許可することを求めるプロンプトがユーザーに向けて表示されます。この要求に同意するよう、ユーザーに指示してください。iOS、Android Enterprise、および Knox Workspace デバイスのユーザーは、このアプリを開いて接続ステータスを確認できます。ユーザーが他に何かする必要はありません。
- 複数のエンタープライズ接続プロファイルを作成した場合は、プロファイルをランク付けします。
- iOS、Android Enterprise、または Knox Workspace デバイスとの接続に関するトラブルシューティングを実行する場合に、ユーザーはアプリを使用して、管理者のメールアドレスにデバイスログを送信できます（ユーザーは提供する必要のあるメールアドレスを入力します）。ログは Winzip では表示できないことに注意してください。7-Zip などの別のユーティリティを使用することをお勧めします。
-

エンタープライズ接続プロファイル設定

エンタープライズ接続プロファイルは、以下のデバイスタイプでサポートされています。

- iOS
- Android
- BlackBerry 10

共通：エンタープライズ接続プロファイル設定

共通：コンプライアンスプロファイル設定	説明
BlackBerry Secure Connect Plus サーバーグループ	この設定は、BlackBerry Secure Connect Plus が特定の地域パスにトラフィックを向けるために使用するサーバーグループを指定します。 この設定は、BlackBerry Connectivity Node の 1 つ以上のインスタンスをインストールしていて、かつサーバーグループを設定している場合にのみ有効です。

iOS ：エンタープライズ接続プロファイル設定

設定	説明
BlackBerry Secure Connect Plus を有効化する	この設定では、デバイスとネットワークの間で仕事用データを送信するために、仕事用アプリで BlackBerry Secure Connect Plus を使用するかどうかを指定します。
VPN をオンデマンドで有効にする	この設定は、仕事用アプリが仕事用リソースにアクセスするときに、BlackBerry Secure Connect Plus を使用して VPN 接続を自動的に開始できるかどうかを指定します。 この設定を選択して、BlackBerry Secure Connect Plus 接続のルールを指定します。
iOS 9 以降の VPN オンデマンドルール	この設定では、BlackBerry Secure Connect Plus を使用して、VPN オンデマンドの接続要件を指定します。ペイロード形式の例の中から 1 つ以上のキーを使用する必要があります。 この設定は、［VPN オンデマンドを有効にする］設定が選択されている場合のみ有効です。
per-app VPN を有効にする	BlackBerry Secure Connect Plus の使用を特定のアプリに制限するには、この設定を選択します。 メモ： このオプションを選択した場合、ユーザーは、BlackBerry Secure Connect Plus を使用するために、デバイス上で VPN 接続を手動でオンにする必要があります。VPN 接続がオンになっている限り、デバイスは仕事用ネットワークへの接続に BlackBerry Secure Connect Plus を使用します。仕事用 Wi-Fi ネットワークなどの別の接続を使用する場合は、ユーザーは VPN 接続をオフにする必要があります。場合によっては、VPN 接続のオンとオフを切り替えるようにユーザーに指示します（たとえば、ユーザーが仕事用 Wi-Fi ネットワークの範囲内にいないときに VPN 接続をオンにするよう指示できます）。
Safari ドメイン	＋ をクリックして、Safari での VPN 接続の開始を許可されているドメインを指定します。
アプリの自動接続を許可する	アプリが VPN 接続を自動的に開始できるようにするかどうかを指定します。

設定	説明
プロキシプロファイル	この設定は、プロキシサーバーを介して、セキュリティ保護されたトンネルトラフィックをデバイスから仕事用ネットワークにルーティングする場合に、関連付けられているプロキシプロファイルを指定します。 プロキシプロファイルでは、IP アドレスを使用した手動設定を使用する必要があります。PAC 設定はサポートされていません。詳細については、「デバイスのプロキシプロファイルのセットアップ」を参照してください。

Android ：エンタープライズ接続プロファイル設定

設定	説明
BlackBerry Secure Connect Plus を有効化する	この設定では、デバイスとネットワークの間で仕事用データを送信するために、仕事用アプリで BlackBerry Secure Connect Plus を使用するかどうかを指定します。
仕事用領域がある Android デバイスのエンタープライズ接続	この設定では、Android Enterprise デバイスと Samsung Knox Workspace デバイスで、仕事用領域の全アプリに BlackBerry Secure Connect Plus を使用するか、指定したアプリのみに使用するかを指定します。 • ［コンテナ単位の VPN］では、デバイスの仕事用領域にあるすべてのアプリに VPN 接続を使用します。 • ［per-app VPN］では、指定したアプリに対してのみ VPN 接続を使用します。

設定	説明
BlackBerry Secure Connect Plus の使用を制限されるアプリ	この設定では、Android Enterprise デバイスで、BlackBerry Secure Connect Plus を使用できない仕事用領域内のアプリを指定します。 + をクリックして、アプリパッケージ ID を入力します。その他のアプリを制限するには、必要に応じてこの手順を繰り返します。 Google Play にはプロキシのサポートがないので、Google Play および基盤となるサービス（com.android.providers.media、com.android.vending、com.google.android.gms、com.google はデフォルトで制限されます。これらの制限はそのまま適用することをお勧めします。これらの制限を解除するには、BlackBerry Secure Connect Plus を使用して Google Play に接続できるようにファイアウォールを設定する必要があるので、Google Play サポートに連絡する必要があります。 ［仕事用アプリに VPN の使用のみを強制する］IT ポリシールールがデバイスに適用されている場合、この設定は無視され、BlackBerry UEM Client および Google Play を含め、仕事用アプリは、BlackBerry Secure Connect Plus の利用を制限されません。この場合、ファイアウォールでポートを開いて、BlackBerry UEM Client が BlackBerry UEM 経由で BlackBerry Infrastructure と通信できるようにする必要があります。仕事用アプリで BlackBerry Secure Connect Plus を使用するためにファイアウォールでポートを開く方法の詳細については、support.blackberry.com/community にアクセスし、記事 48330 を参照してください。 組織で BlackBerry Dynamics アプリを使用している場合は、アプリに対して BlackBerry Secure Connect Plus の使用を制限することをお勧めします。制限しない場合は、組織のファイアウォールで追加のポートを開き、アプリが BlackBerry Dynamics NOC にデータを送信できるようにする必要があります。また、データが BlackBerry Infrastructure と BlackBerry Dynamics NOC の両方にルーティングされるので、アプリからのネットワークアクティビティが遅くなる可能性があります。 この設定は、［仕事用領域がある Android デバイスのエンタープライズ接続］設定が［コンテナ単位の VPN］に設定されている場合にのみ有効です。
エンタープライズ接続の使用を許可されたアプリ	この設定では、Android Enterprise デバイスおよび Samsung Knox Workspace デバイスで、BlackBerry Secure Connect Plus を使用できる仕事用領域内のアプリを指定します。利用可能なアプリのリストからアプリを選択するか、アプリパッケージ ID を指定できます。 この設定は、［仕事用領域がある Android デバイスのエンタープライズ接続］設定が［per-app VPN］に設定されている場合にのみ有効です。

設定	説明
プロキシプロファイル	セキュリティ保護されたトンネルのトラフィックを Android Enterprise アクティベーションおよび Samsung Knox Workspace 2.5 以降のデバイスを含む Samsung Knox デバイスからプロキシサーバーを介して仕事用ネットワークにルーティングする場合は、適切なプロキシプロファイルを選択します。 この設定は、Samsung Knox デバイス以外の Android Enterprise デバイスまたは Samsung Knox Workspace バージョン 2.4 以前を搭載したデバイスには適用されません。

BlackBerry 10 ：エンタープライズ接続プロファイル設定

設定	説明
エンタープライズ接続	BlackBerry 10 デバイスでは、エンタープライズ接続は常に有効です。この設定を変更することはできません。詳細については、「BlackBerry 10 デバイスのエンタープライズ接続を管理する」を参照してください。
プロキシプロファイル	この設定は、プロキシサーバーを介して、セキュリティ保護されたトンネルトラフィックをデバイスから仕事用ネットワークにルーティングする場合に、関連付けられているプロキシプロファイルを指定します。
BlackBerry Secure Connect Plus を有効化する	この設定では、デバイスとネットワークの間で仕事用データを送信するために、仕事用アプリで BlackBerry Secure Connect Plus を使用するかどうかを指定します。

BlackBerry Connectivity アプリ DNS 設定の指定

セキュリティ保護されたトンネル接続で、BlackBerry Connectivity アプリが使用する DNS サーバーを指定できます。また、DNS 検索サフィックスも指定できます。DNS 設定を指定しない場合、アプリは BlackBerry Secure Connect Plus コンポーネントをホストしているコンピューターから DNS アドレスを取得し、デフォルトの検索サフィックスはそのコンピューターの DNS ドメインになります。

1 つ以上のサーバーグループを作成して設定し、BlackBerry Secure Connect Plus 接続を BlackBerry Infrastructure への特定の地域パスに向けると、各サーバーグループに固有の DNS 設定を指定できます。指定した場合、サーバーグループの DNS 設定は、次の手順を使用して指定したグローバル DNS 設定よりも優先されます。サーバーグループの作成と設定の詳細については、「オンプレミスインストールおよびアップグレード関連の資料」または「UEM Cloud 設定関連の資料」を参照してください。

1. 次の操作のいずれかを実行します。
   - オンプレミス環境では、UEM 管理コンソールのメニューバーで、［設定］ > ［インフラストラクチャ］ > ［**BlackBerry Secure Connect Plus**］をクリックします。
   - クラウド環境では、BlackBerry Connectivity Node コンソール（http:/localhost:8088）の左ペインで、［一般設定］ > ［**BlackBerry Secure Connect Plus**］をクリックします。
2. ［**DNS** サーバーを手動設定］チェックボックスをオンにし、＋ をクリックします。
3. ドット付き 10 進法（例：192.0.2.0）で DNS サーバーアドレスを指定します。［追加］をクリックします。

4. 必要に応じて、手順 2〜3 を繰り返して、さらに DNS サーバーを追加します。［**DNS** サーバー］の表で、［ランキング］列の矢印をクリックし、DNS サーバーの優先度を設定します。
5. DNS 検索サフィックスを指定する場合は、次の手順に従って操作します。
   a) ［**DNS** 検索サフィックスの手動管理］チェックボックスをオンにし、＋をクリックします。
   b) DNS 検索サフィックス（例：domain.com）を入力します。［追加］をクリックします。
6. 必要に応じて、手順 5 を繰り返して、さらに DNS 検索サフィックスを追加します。［**DNS** 検索サフィックス］の表で、［ランキング］列の矢印をクリックし、DNS サーバーの優先度を設定します。
7. ［保存］をクリックします。

BlackBerry Dynamics アプリを使用する Android デバイスのためにセキュリティ保護されたトンネル接続を最適化する

BlackBerry Secure Connect Plus を有効化していて、かつ Android Enterprise デバイスまたは Samsung Knox Workspace デバイスに BlackBerry Dynamics アプリがインストールされているオンプレミス環境がある場合、BlackBerry Dynamics 接続プロファイルを設定してこれらのデバイスに割り当て、BlackBerry Proxy を無効化にすることをお勧めします。BlackBerry Proxy と BlackBerry Secure Connect Plus の両方を使用すると、データが両方のネットワークコンポーネントにルーティングされるため、アプリからのネットワークアクティビティに遅延が生じる可能性があります。

1. メニューバーで［ポリシーとプロファイル］をクリックします。
2. ［ネットワークと接続］ > ［**BlackBerrry Dynamics** の接続］をクリックします。
3. Android Enterprise および Samsung Knox Workspace デバイスに割り当てられているプロファイルを選択します。
4. ✎ をクリックします。
5. ［すべてのトラフィックをルーティングする］チェックボックスをオフにします。
6. ［保存］をクリックします。

Wi-Fi ネットワークが利用可能な場合に BlackBerry Secure Connect Plus 経由で BlackBerry 10 の仕事用領域トラフィックを直接実行する

BlackBerry UEM を使用して Wi-Fi プロファイルを設定し、BlackBerry 10 デバイスに割り当てると、BlackBerry Secure Connect Plus よりも仕事用 Wi-Fi ネットワークが優先されます。仕事用 Wi-Fi ネットワークが利用できず、かつデバイスに VPN プロファイルが割り当てられていないかデバイスが VPN にアクセスできないとき、デバイスは BlackBerry Secure Connect Plus を使用します。デバイスが仕事用 Wi-Fi ネットワークにアクセスできる場合でも、BlackBerry Secure Connect Plus 経由ですべての仕事用領域トラフィックを直接実行するオプションもあります。組織のセキュリティ標準によって、Wi-Fi ネットワークを経由した仕事用リソースへのデバイス接続が妨げられている場合に、このオプションを使用できます。

メモ：この機能を有効にすると、通常仕事用 Wi-Fi ネットワークを使用する仕事用領域トラフィックはすべて、セキュリティで保護された接続を通じて BlackBerry Infrastructure に送信されます。この設定は、組織のデータ使用量とネットワークコストに影響を与える場合があります。この機能が組織が優先する設定であることを、有効にする前に確認します。

作業を始める前に： オンプレミス環境では、BlackBerry 10 デバイスユーザーに割り当てられている IT ポリシーで、［仕事用アプリのネットワークアクセス制御を強制する］IT ポリシールールが選択されていないことを確認します。

1. メニューバーで［ポリシーとプロファイル］をクリックします。
2. ［ネットワークと接続］ > ［**Wi-Fi**］をクリックします。
3. BlackBerry 10 デバイスユーザーに割り当てられた Wi-Fi プロファイルをクリックします。
4. ✎ をクリックします。
5. ［**BlackBerry**］タブの［関連付けられたプロファイル］セクションで、［仕事用データに **BlackBerry Secure Connect Plus** 接続とエンタープライズ接続プロファイルを使用します。］チェックボックスをオンにします。
6. ［保存］をクリックします。

終了したら： 複数の Wi-Fi プロファイルを作成および割り当てている場合は、必要に応じてこのタスクを繰り返します。

BlackBerry Secure Connect Plus のトラブルシューティング

BlackBerry Secure Connect Plus の設定で問題が発生した場合は、次の問題を考慮してください。

BlackBerry Secure Connect Plus Adapter が「識別されていないネットワーク」状態になり、動作を停止した

原因

この問題は、BlackBerry Secure Connect Plus をホストするコンピューターを再起動したときに発生することがあります。

解決策 - **Windows Server 2012**

1. Server Manager で、［管理］ > ［役割と機能の追加］をクリックします。［機能］画面が表示されるまで［次へ］をクリックします。［リモートサーバー管理ツール］ > ［役割管理ツール］の順に展開し、［リモートアクセス管理ツール］を選択します。ウィザードを実行して、ツールをインストールします。
2. ［ツール］ > ［リモートアクセス管理］の順にクリックします。
3. ［設定］の［**DirectAccess** と **VPN**］をクリックします。
4. ［**VPN**］の［**RRAS** 管理を開く］をクリックします。
5. ［ルーティングとリモートアクセスサーバー］を右クリックし、［ルーティングとリモートアクセスの無効化］をクリックします。
6. ［ルーティングとリモートアクセスサーバー］を右クリックし、［ルーティングとリモートアクセスの構成と有効化］をクリックします。
7. 次のオプションを選択して、セットアップウィザードを完了します。
   a. ［設定］画面で、［ネットワークアドレス変換（**NAT**）］を選択します。
   b. ［**NAT** インターネット接続］画面で、［インターネットへの接続にパブリックインターフェイスを使用する］を選択します。ネットワークインターフェイスのリストに BlackBerry Secure Connect Plus が表示されていることを確認します。

8. ［ルーティングとリモートアクセス］ > <サーバー名> > ［**IPV4**］を開き、［**NAT**］をクリックします。［ローカルエリア接続］プロパティを開き、［インターネットに接続されるパブリックインターフェイス］と［このインターフェイスで **NAT** を有効にする］をオンにします。［**OK**］をクリックします。
9. ［**BlackBerry Secure Connect Plus**］プロパティを開き、［プライベートネットワークに接続されるプライベートインターフェイス］をオンにします。［**OK**］をクリックします。
10. ［ルーティングとリモートアクセスサーバー］を右クリックし、［すべてのタスク］ > ［再起動］をクリックします。
11. Windows Services で、［**BlackBerry UEM – BlackBerry Secure Connect Plus**］サービスを再起動します。

Windows KB 記事「NAT functionality fails on a Windows Server 2012-based RRAS server」のホットフィックスをダウンロードし、インストールします。

BlackBerry Secure Connect Plus が開始しない

考えられる原因

BlackBerry Secure Connect Plus アダプターの TCP/IPv4 設定が正しくない可能性があります。

解決策

［ネットワーク接続］ > ［**BlackBerry Secure Connect Plus** アダプター］ > ［プロパティ］ > ［インターネットプロトコルバージョン **4**（**TCP/IPv4**）］ > ［プロパティ］で、［次の **IP** アドレスを使用］が選択され、次のデフォルト値になっていることを確認します。

- IP アドレス：172.16.0.1
- サブネットマスク：255.255.0.0

必要に応じて、これらの設定を修正し、サーバーを再起動します。

BlackBerry UEM のインストールまたはアップグレード後、BlackBerry Secure Connect Plus が動作を停止する

原因

この問題は、BlackBerry UEM がオンプレミス環境でアップグレードされる前に、RRAS 更新中にサーバーが再起動されなかったことが原因で、アップグレード中に NAT/ルーティング設定が失敗した場合に発生することがあります。この問題は、BlackBerry UEM の新規インストール後にも発生する可能性があります。

解決策

1. サーバーを再起動します。
2. Windows の［サービス］で、**BlackBerry UEM - BlackBerry Secure Connect Plus** サービスを停止します。
3. 管理者として、Windows PowerShell （64 ビット）を起動するか、コマンドプロンプトを開きます。
4. <ドライブ>`:\Program Files\BlackBerry\UEMSecureConnectPlus\config\blackberry\` に移動し、**configureRRAS.bat** を実行します。
5. <ドライブ>`:\Program Files\BlackBerry\UEMSecureConnectPlus\config\` に移動し、**configure-network-interface.cmd** を実行します。
6. Windows の［サービス］で、**BlackBerry UEM - BlackBerry Secure Connect Plus** サービスを開始します。

BlackBerry Secure Connect Plus のログファイルを表示

デフォルトで <ドライブ>:\Program Files\BlackBerry\UEM\Logs\<*yyyymmdd*> にある 2 つのログファイルは、BlackBerry Secure Connect Plus に関するデータを記録します。

- BSCP：BlackBerry Secure Connect Plus サーバーコンポーネントに関するデータを記録します
- BSCP-TS：BlackBerry Connectivity アプリとの接続に必要なデータを記録します

BlackBerry Connectivity Node インスタンスをホストする各コンピュータで、BlackBerry Secure Connect Plus のログファイルは、<ドライブ>:\Program Files\BlackBerry\BlackBerry Connectivity Node\Logs\<*yyyymmdd*> に置かれています。

目的	ログファイル	例
BlackBerry Secure Connect Plus が BlackBerry Infrastructure に接続されているかどうかを確認する	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]
BlackBerry Secure Connect Plus がデバイスの BlackBerry Connectivity アプリからコールを受信する準備ができていることを確認する	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
デバイスがセキュリティ保護されたトンネルを使用していることを確認する	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
BlackBerry Secure Connect Plus がカスタムトランスコーダー設定を使用していることを確認する	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" }]]
デバイスがカスタムトランスコーダーを使用していることを確認する	BSCP-TS	37: [13:41:39.800371][][3][BlackBerry_1.0.0.1-25B212A5] Connected

BlackBerry 10 デバイスのエンタープライズ接続の使用

エンタープライズ接続は BlackBerry 10 デバイスと組織のネットワーク間で送信されたすべての仕事用データを、BlackBerry Infrastructure を通じて BlackBerry UEM に送信します。エンタープライズ接続は、BlackBerry UEM がオンプレミス環境にインストールされている場合にのみサポートされます。この機能を使用すると、BlackBerry 10 デバイス管理や、メールサーバー、内部 CA、およびその他の Web サーバーまたはコンテンツサーバーに接続するアプリに対し、組織のファイアウォールを経由してインターネットに直接接続できなくすることができます。エンタープライズ接続は、BlackBerry Secure Connect Plus を使用していない場合でも、BlackBerry 10 デバイスで常に有効になっています。BlackBerry 10 デバイスは、ネットワークの可用性に基づいて、仕事用リソースに接続するための最も効率的なパスを選択します。

プロキシプロファイルをエンタープライズ接続プロファイルに関連付けて、プロキシサーバー経由でデータを送信できます。

エンタープライズ接続を使用して、BlackBerry 10 デバイスが組織のネットワークとの間でデータを転送する方法の詳細については、「オンプレミスアーキテクチャに関する資料」を参照してください。

BlackBerry 10 デバイスのエンタープライズ接続を管理する

エンタープライズ接続プロファイルを使用して BlackBerry Secure Connect Plus を設定する場合は、このタスクの代わりに「BlackBerry Secure Connect Plus を有効化する」を参照してください。

デフォルトでは、BlackBerry UEM はデフォルトのエンタープライズ接続プロファイルをすべてのユーザーに割り当てます。デフォルトのプロファイルを編集したり、新しいエンタープライズ接続プロファイルを作成したりできます。

BlackBerry 10 デバイスでは、エンタープライズ接続が常に有効になっています。エンタープライズ接続プロファイルを使用してプロキシプロファイルを関連付け、プロキシサーバー経由でデータを送信できます。

作業を始める前に： 必要に応じて、プロキシプロファイルを作成します。

1. メニューバーで［ポリシーとプロファイル］をクリックします。
2. ［ネットワークと接続］ > ［エンタープライズ接続］をクリックします。
3. ＋ をクリックします。
4. プロファイルの名前と説明を入力します。エンタープライズ接続プロファイルごとに固有の名前が必要です。
5. ［**BlackBerry**］タブをクリックします。
6. プロキシサーバーを使用する場合、プロキシプロファイルを選択します。
7. ［追加］をクリックします。

終了したら： 必要に応じて、プロファイルをランク付けします。

BlackBerry 2FA を使用した、重要なリソースへのセキュリティ保護された接続

BlackBerry 2FA は、ツーファクター認証で、組織の重要なリソースへのアクセスを保護します。BlackBerry 2FA は、ユーザーがリソースにアクセスしようとするたびに、ユーザーが入力したパスワードとセキュリティ保護されたプロンプトをモバイルデバイスで使用します。

BlackBerry UEM 管理コンソールから、BlackBerry 2FA を管理します。このコンソールでは、BlackBerry 2FA プロファイルを使用して、ユーザーに対してツーファクター認証を有効にできます。BlackBerry 2FA の最新バージョンと、事前認証や自己回復などの関連機能を使用するには、BlackBerry 2FA プロファイルがユーザーに割り当てられている必要があります。詳細については、BlackBerry 2FA 関連の資料を参照してください。

デバイスでシングルサインオン認証を設定

シングルサインオンプロファイルを使用して、BlackBerry 10 デバイスと特定の iOS デバイスを有効にして、組織のネットワーク内のドメインおよび Web サービスでの認証を自動的に実行できます。シングルサインオンプロファイルを割り当てると、ユーザーは、指定したセキュリティ保護されたドメインに初めてアクセスを試行したときに、ユーザー名とパスワードの入力が求められます。ログイン情報はユーザーのデバイスに保存され、ユーザーがプロファイルに指定されたセキュリティ保護されたドメインにアクセスを試行すると自動的に使用されます。ユーザーがパスワードを変更した場合は、セキュリティ保護されたドメインへの次回アクセス試行時に、パスワードの入力が求められます。

iOS（または iPadOS）13 以降を実行しているデバイスでは、シングルサインオン拡張プロファイルを使用して、組織のネットワーク内のドメインおよび Web サービスでデバイスが自動的に認証されるようにする必要があります。

SCEP プロファイルを使用して BlackBerry 10 デバイスに送信する証明書に信頼済みドメインを指定するために、シングルサインオンプロファイルを使用することもできます。信頼済みドメインを指定しておくと、BlackBerry 10 ユーザーは信頼済みドメインにアクセスするときに、必要な証明書を選択できるようになります。

シングルサインオンプロファイルは、次の認証の種類をサポートしています。

認証の種類	デバイス **OS**	対象
• Kerberos	iOS	• ブラウザーとアプリ • どのアプリがプロファイルを使用できるかを制限できる
	BlackBerry 10	• 仕事用領域内のブラウザーとアプリ
• NTLM • SCEP 証明書の信頼済みドメインを指定	BlackBerry 10	• 仕事用領域内のブラウザーとアプリ

BlackBerry Dynamics アプリは Kerberos 認証もサポートしています。詳細については、「BlackBerry Dynamics アプリの Kerberos の設定」を参照してください。

前提条件：デバイスで **Kerberos** 認証を使用する

デバイスで Kerberos を使用していて、デバイスで有効な TGT が利用可能な場合、ユーザーが仕事用領域内のブラウザーやアプリから組織の内部リソースにアクセスするときにログイン情報を求めるプロンプトは表示されません。

特定のドメインに対して Kerberos 認証を設定するために、組織の Kerberos 設定ファイル（krb5.conf）をアップロードできます。BlackBerry UEM は、Kerberos の Heimdal 実装をサポートします。

設定ファイルが次の要件を満たしていることを確認します。

- Kerberos 設定はデフォルトでは、UDP ではなく TCP を使用する必要があります。KDC ホストのプレフィックス tcp/ を使用します。
- 組織が VPN を使用している場合は、VPN ゲートウェイで KDC へのトラフィックを許可する必要があります。

BlackBerry Dynamics アプリの Kerberos 認証の設定方法の詳細については、「BlackBerry Dynamics アプリでの Kerberos 設定」を参照してください。

証明書ベースの iOS デバイス認証

iOS デバイスの場合、証明書を使用して、組織のネットワーク内のドメインおよび Web サービスに対してデバイスを認証できます。既存の共有の証明書プロファイル、SCEP プロファイル、またはユーザー資格情報プロファイルをシングルサインオンプロファイルに追加できます。iOS デバイス上のブラウザーまたはアプリが証明書に基づくシングルサインオンを使用すると、ユーザーは自動的に認証されます（証明書が有効な場合）。指定されているセキュリティ保護されたドメインにアクセスする際には、ログイン情報を入力する必要はありません。

シングルサインオンプロファイルの作成

シングルサインオンプロファイルは、BlackBerry 10 および iOS デバイスでサポートされています。BlackBerry Dynamics アプリのシングルサインオン認証を設定するには、「BlackBerry Dynamics アプリでの Kerberos 設定」「」を参照してください。

作業を始める前に：

- BlackBerry 10 デバイスの Kerberos 認証を設定する場合は、組織の Kerberos 設定ファイル（krb5.conf）を検索します。
- iOS デバイスに対して証明書に基づく認証を使用する場合は、必須の共有証明書プロファイルまたは SCEP プロファイルを作成します。

1. メニューバーで［ポリシーとプロファイル］をクリックします。
2. ［ネットワークと接続］ > ［シングルサインオン］をクリックします。
3. ＋ をクリックします。
4. プロファイルの名前と説明を入力します。
5. 次のタスクを実行します。

タスク	手順
Kerberos デバイスの iOS 認証を設定する	**a.** ［**iOS**］タブをクリックします。 **b.** ［**Kerberos**］の下の ＋ をクリックします。 **c.** ［名前］フィールドに、設定の名前を入力します。 **d.** ［プリンシパル名］フィールドで、<プライマリ>/<インスタンス>@<領域> の形式で、Kerberos プリンシパルの名前を入力します（たとえば、`user/admin@blackberry.example.com`）。 **e.** ［領域］フィールドで、Kerberos 領域を大文字で入力します（たとえば、**EXAMPLE.COM**）。 **f.** ［**URL** プレフィックス］フィールドで、デバイスでの認証を実行するサイトの URL プレフィックスを入力します。プレフィックスは、http:// または https:// で始める必要があり、ワイルドカード値（*）を含めることができます（たとえば、**https://www.blackberry.example.com/***）。 **g.** さらに URL プレフィックスを指定するには、＋ をクリックして、フィールドを追加します。 **h.** 設定を特定のアプリに制限する場合は、＋ の横の ［アプリ **ID**］ をクリックします。アプリバンドル ID を入力します。ID を複数のアプリと一致させるために、ワイルドカード値（*）を使用できます（たとえば、**com.company.***）。 **i.** さらにアプリ識別子を指定するには、＋ をクリックして、フィールドを追加します。 **j.** iOS デバイスで証明書に基づく認証を使用する場合は、［資格情報］ドロップダウンリストで、［証明書］、［**SCEP**］、または［ユーザー資格情報］をクリックします。証明書のドロップダウンリストで、使用する証明書プロファイルをクリックします。 **k.** ［追加］をクリックします。 **l.** 必要に応じて、手順 2〜11 を繰り返して、別の Kerberos 設定を追加します。
Kerberos デバイスの BlackBerry 10 認証を設定する	**a.** ［**BlackBerry**］タブをクリックします。 **b.** ［参照］をクリックします。組織の Kerberos 設定ファイル（krb5.conf）に移動して、選択します。

タスク	手順
BlackBerry 10 デバイス用 SCEP 証明書での NTLM 認証または信頼済みドメインを設定する	**a.** ［**BlackBerry**］タブをクリックします。 **b.** ［信頼済みドメイン］の下の ＋ をクリックします。 **c.** ［名前］フィールドに、設定の名前を入力します。 **d.** ［ドメイン］フィールドに、信頼済みサブドメイン、または自動的に認証するためにドメイン資格情報を使用できる個々のホストを入力します。サーバー名を、FQDN、ホスト名、エイリアス、または IP アドレスとして入力します。DNS 名には、ワイルドカード（*）を含めることができます。 **e.** さらにサブドメインを指定するには、＋ をクリックして、フィールドを追加します。 **f.** ［追加］をクリックします。 **g.** 必要に応じて、手順 2〜6 を繰り返して、別の信頼済みドメインを追加します。

6. ［追加］をクリックします。

終了したら： 必要に応じて、プロファイルをランク付けします。

シングルサインオン拡張プロファイルの作成

シングルサインオン拡張機能は、iOS または iPadOS 13 以降を実行しているデバイスでサポートされています。

1. メニューバーで［ポリシーとプロファイル］をクリックします。
2. ［ネットワークと接続］ > ［シングルサインオン拡張］をクリックします。
3. ＋ をクリックします。
4. プロファイルの名前と説明を入力します。
5. ［拡張識別子］フィールドに、シングルサインオンを実行するアプリの識別子を入力します。
6. サインオンのタイプを選択します。

タスク	手順
［資格情報］を選択した場合	**a.** ［領域］フィールドに、資格情報の領域名を入力します。 **b.** ［ドメイン］セクションで、＋ をクリックしてドメインを追加します。 **c.** ［名前］フィールドに、アプリ拡張機能がシングルサインオンを実行するドメインを入力します。 **d.** 必要に応じて追加のドメインを追加します。 **e.** ［カスタムペイロードコード］フィールドに、アプリ拡張機能のカスタムペイロードコードを入力します。

タスク	手順
［リダイレクト］を選択した場合	**a.** ［**URL**］セクションで、＋をクリックして URL を追加します。 **b.** ［名前］フィールドに、アプリ拡張機能がシングルサインオンを実行する ID プロバイダーの URL プレフィックスを入力します。必要に応じて追加の URL を追加します。 **c.** ［カスタムペイロードコード］フィールドに、アプリ拡張機能のカスタムペイロードコードを入力します。

7. ［保存］をクリックします。

iOS デバイスのメールドメインと Web ドメインの管理

管理ドメインプロファイルを使用して、特定のメールドメインおよび Web ドメインを、組織の内部にある「監視対象ドメイン」として定義できます。管理ドメインプロファイルは、MDM 制御 アクティベーションタイプの iOS デバイスのみに適用されます。

管理ドメインプロファイルを割り当てた後：

- ユーザーがメールメッセージを作成し、追加した受信者のメールアドレスが、管理ドメインプロファイルに指定されていないドメインのアドレスであった場合、受信者が組織外の人であることを警告するために、デバイス上ではそのアドレスが赤く表示されます。デバイスは、ユーザーが外部受信者へメールを送信するのを阻止しません。
- 管理された Web ドメインのドキュメント、または管理された Web ドメインからダウンロードされたドキュメントを表示する場合、ユーザーは、BlackBerry UEM によって管理されているアプリを使用する必要があります。デバイスは、ユーザーが他の Web ドメインからのドキュメントにアクセスしたり、それを表示したりするのを阻止しません。管理ドメインプロファイルは、Safari ブラウザーにのみ適用されます。

管理されているドメインプロファイルの作成

管理対象のドメインプロファイルは、iOS デバイスのみに適用されます。

1. メニューバーで［ポリシーとプロファイル］をクリックします。
2. ［ネットワークと接続］ > ［管理されているドメイン］をクリックします。
3. ＋ をクリックします。
4. プロファイルの名前と説明を入力します。
5. オプションで、［説明］フィールドに、プロファイルの説明を入力します。
6. ［管理されているメールドメイン］セクションで ＋ をクリックします。
7. ［メールドメイン］フィールドに、最上位のドメイン名を入力します（例えば、`example.com/canada` ではなく、`example.com`）。
8. ［追加］をクリックします。
9. ［管理されている **Web** ドメイン］セクションで ＋ をクリックします。Web ドメインの指定形式の例については、『iOS 開発者ライブラリ』の「管理されている Safari の Web ドメイン」を参照してください。
10. ［**Web** ドメイン］フィールドにドメイン名を入力します。
11. 指定した Web ドメインで、パスワードの自動入力を有効にする場合は、［パスワードの自動入力を許可する］チェックボックスをオンにします。このオプションは監視対象 iOS デバイスでのみサポートされます。
12. ［追加］をクリックします。
13. ［追加］をクリックします。

iOS デバイスのアプリのネットワーク使用を制御する

ネットワーク使用プロファイルを使用して、iOS デバイスのアプリがモバイルネットワークをどのように使用するかを制御することができます。

ネットワーク使用を管理するために、デバイスがモバイルネットワークに接続されている間、またはデバイスのローミング中に、指定したアプリがデータを転送しないようにすることができます。ネットワーク使用プロファイルには、1 つのアプリ用または複数のアプリ用のルールを格納することができます。

ネットワーク使用プロファイルの作成

ネットワーク使用プロファイル内のルールは、仕事用アプリにのみ適用されます。アプリをユーザーまたはグループに割り当てていない場合、ネットワーク使用プロファイルを使用しても効果はありません。

作業を始める前に： アプリをアプリリストに追加して、ユーザーグループまたはユーザーアカウントに割り当てます。

1. メニューバーで［ポリシーとプロファイル］をクリックします。
2. ［ネットワークと接続］ **>** ［ネットワーク使用］をクリックします。
3. ＋ をクリックします。
4. プロファイルの名前と説明を入力します。
5. ＋ をクリックします。
6. 次の操作のいずれかを実行します。
   - ［アプリを追加］をタップして、リスト内のアプリをクリックします。
   - ［アプリパッケージ **ID** を指定］を選択し、ID を入力します。アプリパッケージ ID は、バンドル ID とも呼ばれています。アプリパッケージ ID を確認するには、アプリリストでアプリをクリックします。ワイルドカード値（*）を使用して、複数のアプリの ID を検索できます。（たとえば、**com.company.***）。
7. デバイスのローミング中に、アプリによるデータ使用を防止するには、［データローミングを許可］チェックボックスをオフにします。
8. デバイスがモバイルネットワークに接続しているときに、アプリによるデータ使用を防止するには、［携帯データを許可］チェックボックスをオフにします。
9. ［追加］をクリックします。
10. リストに追加する各アプリについて、ステップ 5〜9 を繰り返します。

終了したら： 必要に応じて、プロファイルをランク付けします。

iOS デバイス上での Web コンテンツのフィルター

Web コンテンツフィルタープロファイルを使用して、ユーザーが監視対象の iOS デバイス上で、Safari または他のブラウザーアプリを使用して表示できる Web サイトを制限できます。Web コンテンツフィルタープロファイルはユーザーアカウント、ユーザーグループ、またはデバイスグループに割り当てることができます。

Web コンテンツフィルタープロファイルを作成する場合、モバイルデバイスを使用するための組織の標準をサポートする［許可された Web サイト］オプションを選択できます。

許可された **Web** サイト	説明
特定の Web サイトのみ	このオプションは、指定した Web サイトのみへのアクセスを許可します。許可された Web サイトごとに、Safari にブックマークが作成されます。 メモ：特定の Web サイトへのアクセスのみを許可する場合は、デバイスがアクセスする必要があるすべての Web サイトが、許可された Web サイトのリストに指定されていることを確認する必要があります。たとえば、BlackBerry Dynamics アプリ用に Microsoft Office 365 モダン認証を設定する場合、デバイスは Active Directory フェデレーションサービスの Web サイトにアクセスできる必要があります。
アダルトコンテンツを制限	このオプションは、不適切なコンテンツを特定しブロックするための自動フィルターを有効にします。また、次の設定を使用して、特定の Web サイトを含めることもできます。 • 許可された URL：1 つ以上の URL を追加して、特定の Web サイトへのアクセスを許可することができます。ユーザーは、自動フィルターがアクセスをブロックするかどうかに関係なく、このリスト内の Web サイトを表示できます。 • ブラックリストに登録された URL：1 つ以上の URL を追加して、特定の Web サイトへのアクセスを拒否することができます。ユーザーは、自動フィルターがアクセスを許可するかどうかに関係なく、このリスト内の Web サイトは表示できません。

Web コンテンツフィルタープロファイルの作成

Web コンテンツフィルタープロファイルを作成する場合は、指定する各 URL を http:// または https:// で始める必要があります。必要に応じて、同じ URL の http:// および https:// バージョンに個別のエントリを追加します。DNS 解決は実行されないため、限定された Web サイトは引き続きアクセス可能です（たとえば、http://www.example.com と指定すると、ユーザーは IP アドレスを使用して Web サイトにアクセスできる場合があります）。

1. メニューバーで［ポリシーとプロファイル］をクリックします。
2. ［ネットワークと接続］ > ［**Web** コンテンツフィルター］をクリックします。
3. ＋ をクリックします。
4. Web コンテンツフィルタープロファイルの名前と説明を入力します。
5. 次のタスクのいずれかを実行します。

タスク	手順
特定の Web サイトのみへのアクセスを許可する	**a.** ［許可された **Web** サイト］ドロップダウンリストで、［特定の **Web** サイトのみ］が選択されていることを確認します。 **b.** ［特定の **Web** サイトのブックマーク］セクションで ＋ をクリックします。 **c.** 次の操作を実行します。 **1.** ［**URL**］フィールドでは、アクセスを許可する Web アドレスを入力します。 **2.** オプションで、［ブックマークのパス］フィールドに、ブックマークフォルダーの名前（たとえば、/Work/）を入力します。 **3.** ［タイトル］フィールドに、Web サイトの名前を入力します。 **4.** ［追加］をクリックします。 **d.** 許可する Web サイトごとに手順 2 と 3 を繰り返します。
アダルトコンテンツを制限する	**a.** ［許可された **Web** サイト］ドロップダウンリストで、［アダルトコンテンツを制限］をクリックして自動フィルターを有効にします。 **b.** オプションで、次の操作を実行します。 **1.** ［許可された **URL**］の横の ＋ をクリックします。 **2.** アクセスを許可する Web アドレスを入力します。 **3.** 許可する Web サイトごとに手順 2.a と 2.b を繰り返します。 **c.** オプションで、次の操作を実行します。 **1.** ［ブラックリストに登録された **URL**］の横の ＋ をクリックします。 **2.** アクセスを拒否する Web アドレスを入力します。 **3.** 制限する Web サイトごとに手順 3.a と 3.b を繰り返します。

6. ［追加］をクリックします。

iOS デバイス用 AirPrint プロファイルおよび AirPlay プロファイルの設定

ユーザーは、AirPrint プロファイルを使用することで、AirPrint をサポートし、アクセス可能で、自身が必要な権限を持つプリンターを簡単に探すことができます。Bonjour などのプロトコルが別のサブネットワーク上で AirPrint 対応プリンタを検出できない場合、AirPrint プロファイルはリソースの場所を指定するのに役立ちます。AirPrint プロファイルを iOS デバイスに割り当てることで、ユーザーがプリンターを手動で設定する必要がなくなります。

AirPlay は iOS の機能です。この機能を使用して、Apple TV、AirPort Express、AirPlay 対応スピーカーなどの互換性のある AirPlay デバイスで、写真を表示したり、音楽やビデオをストリーミングしたりすることができます。

AirPlay プロファイルを使用して、特定の AirPlay デバイスのパスワードを設定し、承認されているユーザーだけがそのデバイスにアクセスできるようにすることができます。また、許可されている出力先デバイスのリストを作成して、監視された iOS デバイスが、指定された AirPlay デバイスだけに接続するように設定することもできます。AirPlay プロファイルは、ユーザーアカウント、ユーザーグループ、またはデバイスグループに割り当てることができます。

例：**AirPlay** デバイスのパスワードを設定する

特定の AirPlay デバイスへのアクセスを制限する場合は、デバイスの名前を追加してパスワードを設定します。その AirPlay プロファイルを持つ iOS デバイスのユーザーは、AirPlay デバイスにアクセスする際に、パスワードを入力する必要があります。AirPlay プロファイルでのみパスワードが必要です。AirPlay デバイス自体に、パスワードは必要ありません。その AirPlay プロファイルを持たない iOS デバイスのユーザーは、パスワードを入力しなくても AirPlay デバイスにアクセスできます。

例：監視されている **iOS** デバイス用の **AirPlay** デバイスのリストを作成する

監視されている iOS デバイスで、特定のデバイスにのみコンテンツをストリーミングできるようにするには、デバイス ID を追加します。監視されているデバイスは、指定したデバイスにのみコンテンツをストリーミングすることができます。監視されていないデバイスは、このリストの影響を受けません。

AirPrint プロファイルの作成

AirPrint プロファイルを設定して iOS デバイスに割り当てることができます。このようにすると、ユーザーはプリンターを手動で設定する必要がなくなります。

Bonjour プロトコルおよび BlackBerry Dynamics アプリでの印刷の詳細については、support.blackberry.com/community にアクセスして、記事 40030 を参照してください。

1. メニューバーで［ポリシーとプロファイル］をクリックします。
2. ［ネットワークと接続］ > ［**AirPrint**］をクリックします。
3. ＋ をクリックします。
4. AirPrint プロファイルの名前と説明を入力します。
5. ［**AirPrint** の設定］セクションで ＋ をクリックします。
6. ［**IP** アドレス］フィールドに、プリンターまたは AirPrint サーバーの IP アドレスを入力します。

7. ［リソースパス］フィールドに、プリンターのリソースパスを入力します。
   プリンターのリソースパスは、`_ipps.tcp` Bonjour レコードの `rp` パラメーターに対応します。例：
   - printers/<プリンターシリーズ>
   - printers/<プリンターの機種>
   - ipp/print
   - IPP_Printer
8. オプションで、AirPrint 接続が TLS で保護されている場合、［**TLS** を使用する］チェックボックスをオンにします。このオプションは、iOS 11.0 以降でサポートされています。
9. オプションで、ポートがインターネットプリンティングプロトコルのデフォルトと異なる場合は、［ポート］フィールドにポート番号を入力します。このオプションは、iOS 11.0 以降でサポートされています。
10. ［追加］をクリックします。
11. ［追加］をクリックします。

AirPlay プロファイルの作成

1. メニューバーで［ポリシーとプロファイル］をクリックします。
2. ［ネットワークと接続］ **>** ［**AirPlay**］をクリックします。
3. ＋ をクリックします。
4. AirPlay プロファイルの名前と説明を入力します。
5. ［許可された保存先デバイス］セクションの ＋ をクリックします。
6. ［デバイス名］フィールドに、追加する AirPlay デバイスの名前を入力します。AirPlay デバイスの名前はデバイス設定で確認できます。また、デバイスの名前を参照するには、iOS デバイスのコントロールセンターにある［**AirPlay**］をタップして、近くにある利用可能な AirPlay デバイスのリストを表示します。
7. ［パスワード］フィールドにパスワードを入力します。
8. ［追加］をクリックします。
9. ［監視されたデバイス用に許可された保存先デバイス］セクションの ＋ をクリックします。
10. ［デバイス **ID**］フィールドに、追加する AirPlay デバイスのデバイス ID を入力します。AirPlay デバイスのデバイス ID は、デバイス設定で確認できます。デバイス ID の検索方法の詳細については、Apple 製品に関するドキュメントを参照してください。
11. ［追加］をクリックします。

Android デバイスのアクセスポイント名の設定

APN は、モバイルデバイスが通信事業者のネットワークに接続するために必要な情報を指定します。1 つまたは複数のアクセスポイント名プロファイルを使用して、通信事業者用の APN をユーザーの Android デバイスに送信できます。

デバイスには通常、共通の通信事業者用に APN がプリセットされています。ユーザーは、新しい APN をデバイスに追加することもできます。アクセスポイント名プロファイルによってデバイスに送信された APN をデバイスに強制的に使用させる場合は、Android グローバル（すべての Android デバイス）IT ポリシールールで［デバイスにアクセスポイント名プロファイル設定の使用を強制する］IT ポリシールールを選択します。

アクセスポイント名プロファイルの作成

作業を始める前に： 必要な APN 設定をすべて通信事業者から取得します。

1. メニューバーで［ポリシーとプロファイル］をクリックします。
2. ［ネットワークと接続］ > ［アクセスポイント名］をクリックします。
3. ＋ をクリックします。
4. アクセスポイント名プロファイルの名前と説明を入力します。この情報はデバイスに表示されます。
5. ［アクセスポイント名］を入力します。
6. 各プロファイル設定の通信事業者の仕様に一致する値を指定します。
7. ［保存］をクリックします。

商標などに関する情報

©2020 BlackBerry Limited. BLACKBERRY、BBM、BES、EMBLEM Design、ATHOC、CYLANCE、SECUSMART などの商標（ただし、これらに限定されるとは限らない）は BlackBerry Limited、その子会社および関連会社の商標または登録商標であり、ライセンスに基づいて使用され、当該の商標に対する独占権は明確に留保されています。その他すべての商標は各社の所有物です。

本書は、参照用として本書で取り上げるすべての文書（提供される文書または BlackBerry の Web サイトで参照可能な文書）を含めて「現状のまま」または「参照可能な形で」提供されるか、またはアクセスすることができ、BlackBerry Limited およびその関連会社（「BlackBerry」）はいかなる条件付け、承認、表明、または保証もしないものとし、BlackBerry は本書の誤記、技術的な誤りまたはその他の誤り、エラー、遺漏について何ら責任を負いません。BlackBerry の所有権、機密情報および/または企業秘密を保護するため、本書では一部の BlackBerry テクノロジの側面を一般化された用語で記述している場合があります。BlackBerry は、本書に含まれる情報を定期的に変更する権利を留保します。ただし、BlackBerry には、本書への変更、更新、拡張、または他の追加を適時ユーザーに提供する義務はないものとします。

本書は、第三者をソースとする情報、ハードウェアまたはソフトウェア、製品またはサービス（コンポーネントや、著作権保護されたコンテンツなど）、および/または第三者の Web サイト（これらをまとめて「サードパーティ製品およびサービス」という）への参照を含んでいる可能性があります。BlackBerry は、サードパーティ製品およびサービスの内容、正確性、著作権遵守、互換性、性能、信頼性、適法性、品格、リンク、他の側面などに限定することなく、サードパーティ製品およびサービスを一切管理することはなく、責任も負いません。本書においてサードパーティ製品およびサービスを参照することは、BlackBerry がサードパーティ製品およびサービスまたは第三者を保証することを意味するものではありません。

該当する司法管轄地域の適用法で明確に禁じられている場合を除き、本書で参照されているソフトウェア、ハードウェア、サービス、またはサードパーティ製品およびサービスについて、耐久性、特定の目的または使用に対する適合、商品性、適性品質、権利侵害の不存在、品質満足度、権原、または制定法、慣習法、取引過程、商慣習から生じる、本書またはその使用に関する、または性能または性能の不履行に関する条件付け、承認、表明、保証などに限定することなく、明示的または黙示的に、いかなる条件付け、承認、表明、または保証も除外されます。ユーザーは、国や地域によって異なる他の権利を有する場合もあります。一部の司法管轄地域では、黙示的な保証および条件の除外事項または限定事項は禁止されています。法律で認められている範囲で、本書に関連する黙示的な保証または条件は、上記に定めるように除外できないが限定できる場合、ユーザーが本書または該当する対象物を初めて入手してから 90 日間に限定されます。

該当する司法管轄地域の適用法で認められている最大限の範囲で、本書またはその使用に関連して、または本書で参照されているソフトウェア、ハードウェア、サービス、またはサードパーティ製品およびサービスの性能または性能の不履行に関連して、直接的、必然的、典型的、偶発的、間接的、特殊的、懲罰的、または加重的損害、金銭的損失による損害（利益または収益の損失、予想される貯蓄の未達成、事業の中断、ビジネス情報の消失、ビジネス機会の喪失、データの破損または消失、データの送受信の失敗、BlackBerry 製品またはサービスと併用したアプリケーションに関連する問題、ダウンタイムコスト、BlackBerry 製品またはサービスあるいはその一部の使用機会や通信サービスの使用機会の喪失、代替品コスト、保険料、設備費、保守費、資本コストなど）に限定することなく、損害を予想できたかどうかを問わず、BlackBerry が損害の可能性について勧告を受けていた場合を含め、いかなる場合においても、BlackBerry はいかなる損害の責任も負わないものとします。

該当する司法管轄地域の適用法で認められている最大限の範囲で、契約、不法行為、またはユーザーに対する過失責任または厳格責任について、BlackBerry は他のいかなる義務、責務、または責任も負わないものとします。

本書の限定事項、除外事項、および免責事項は、（A）訴訟原因、請求、またはユーザーによる行為（契約違反、過失、不法行為、厳格責任、その他の法理論など）の性質に関係なく、この契約の基本目的または本書に記載されている救済策の根本的違反または不履行を免れるため、（B）BlackBerry およびその関連会社、その後継

者、譲受人、代理業者、納入業者（通信事業者を含む）、認可された BlackBerry 販売業者（通信事業者を含む）およびその取締役、従業員、および請負業者に適用されます。

上記に定める限定事項および除外事項に加えて、いかなる場合においても、BlackBerry の取締役、従業員、代理業者、販売業者、納入業者、請負業者または BlackBerry の関連会社は、本書に起因または関連する責任を負わないものとします。

ユーザーは、サードパーティ製品およびサービスの加入、インストール、または使用前に、通信事業者がサードパーティ製品およびサービスのすべての機能をサポートすることに同意していることを確認する責任を負います。一部の通信事業者は、BlackBerry® Internet Service への加入によるインターネット閲覧機能を提供しない場合があります。サービスの利用、ローミング、サービスプラン、その他の機能については、通信事業者に問い合わせてください。BlackBerry 製品およびサービスにおけるサードパーティ製品およびサービスのインストールまたは使用には、第三者の権利を侵害または妨害しないように、特許、商標、著作権、または他のライセンスが必要になる場合があります。ユーザーは、サードパーティ製品およびサービスを使用するかどうかを決定し、使用するためにサードパーティライセンスが必要かどうかを確認する責任を負います。必要な場合、ユーザーはライセンスを取得する責任を負います。ユーザーは、必要なライセンスをすべて取得するまで、サードパーティ製品およびサービスをインストールまたは使用してはなりません。BlackBerry 製品およびサービスで提供されるサードパーティ製品およびサービスは、ユーザーの便宜のために「現状のまま」提供され、BlackBerry は明示的にも黙示的にもいかなる条件付け、承認、表明、または保証もしないものとし、BlackBerry はそれに関連するいかなる責任も負わないものとします。ユーザーによるサードパーティ製品およびサービスの使用は、ライセンスまたは BlackBerry との他の契約で明示的に対象になっている場合を除き、個別のライセンスおよび第三者との他の該当契約の条件に従うものとし、その制約を受けるものとします。

BlackBerry 製品またはサービスの使用条件は、個別のライセンスまたは BlackBerry との他の該当契約に定められています。本書の内容は、本書以外に BlackBerry 製品またはサービスの一部に対して BlackBerry が提供した文書による明示的な契約または保証を破棄するものではありません。

BlackBerry Enterprise Software には、特定のサードパーティ製ソフトウェアが組み込まれています。このソフトウェアに関連するライセンスおよび著作権情報は、http://worldwide.blackberry.com/legal/thirdpartysoftware.jsp でご確認いただけます。

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

BlackBerry UK Limited
Ground Floor, The Pearce Building, West Street,
Maidenhead, Berkshire SL6 1RL
United Kingdom

Published in Canada