BlackBerry UEM

管理

ソース接続の管理

12.19

Contents

BlackBerry UEM を使用したセキュリティ保護された接続の管理

次の表は、このガイドで説明する管理タスクの概要を示しています。組織のニーズに基づいて完了すべきタスクを確認して決定します。

タスク	説明
Wi-Fi プロファイルの作成	Wi-Fi プロファイルを作成して、デバイスを仕事用の Wi-Fi ネットワークに接続する方法を指定できます。
VPN プロファイルの作成	VPN プロファイルを作成して、デバイスを仕事用の VPN に接続する方法を指定できます。
アプリごとの VPN プロファイルの作成	デバイス上のどのアプリが、データの転送に VPN を使用する必要があるかを指定することができます。
プロキシプロファイルの作成	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。
エンタープライズ接続プロファイルの作成	デバイスがエンタープライズ接続を使用して組織のリソースに接続する方法を指定し、BlackBerry Secure Connect Plus がアプリと組織のネットワーク間にセキュリティ保護された IP トンネルを提供する方法を指定できます。
BlackBerry 2FA プロファイルの作成	ユーザーのツーファクタ認証を有効にし、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拡張プロファイルの作成	iOS および iPadOS 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。
BlackBerry Dynamics 接続プロファイルの作成	BlackBerry Dynamics アプリを使用するときにデバイスが接続できるネットワーク接続、インターネットドメイン、IP アドレス範囲、およびアプリサーバーを定義できます。詳細については、管理関連の資料の「BlackBerry Dynamics アプリのネットワーク接続の設定」を参照してください。
DNS プロファイルの作成	指定されたドメインにアクセスするために iOS および macOS デバイスが使用する DNS サーバーを指定できます。
メールプロファイルの作成	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エントリ、オーガナイザデータを同期する方法を指定できます。詳細については、管理関連の資料で「メールプロファイルの作成」を参照してください。
IMAP/POP3 メールプロファイルを作成	デバイスの IMAP や POP3 メールサーバーへの接続方法とメールメッセージの同期方法を指定できます。詳細については、「IMAP/POP3 メールプロファイルの作成」を参照してください。

タスク	説明
ネットワーク使用プロファイルの作成	iOS および iPadOS アプリのネットワークモバイルネットワーク使用状況を管理できます。
Web コンテンツフィルタープロファイルの作成	ユーザーが監視対象の iOS または iPadOS デバイス上で、Safari または他のブラウザを使用して表示できる Web サイトを制限できます。
AirPrint プロファイルの作成	ユーザーがプリンタを見つけるのを助けることができます。
AirPlay プロファイルの作成	iOS および iPadOS のユーザーが接続できる AirPlay デバイスを指定できます。
アクセスポイント名プロファイルの作成	Android デバイスが通信事業者のネットワークと通信するために必要な情報を指定できます。
UEM の組織の PKI ソフトウェアへの接続	PKI サービスによって提供される証明書ベースの認証を UEM で管理するデバイスおよびアプリに拡張できます。たとえば、次の操作ができます。 • BlackBerry UEM と組織の Entrust ソフトウェアを接続する • BlackBerry UEM を組織の Entrust IdentityGuard サーバーに接続したスマート認証情報の使用 • BlackBerry UEM と組織の OpenTrust ソフトウェアを接続する • BlackBerry UEM から BlackBerry Dynamics PKI コネクターへの接続 • 組織のアプリベース PKI ソリューションへの BlackBerry UEM の接続
プロファイルを使用したデバイスおよびアプリへの証明書の送信	UEM プロファイルを使用してデバイスおよびアプリに証明書を送信できます。
ユーザーアカウント用クライアント証明書の管理	クライアント証明書は、個々のユーザーアカウントに直接追加することも、ユーザーアカウントに割り当てられたユーザー資格情報プロファイルに追加することもできます。

プロファイルを使用した仕事用接続の管理

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 など組織の環境内の仕事用リソースとデバイスの接続方法を設定します。同一のプロファイルで、iOS、macOS、Android、および Windows 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。

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。たとえば、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、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。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。

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、SCEP、共有証明書、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。
- 仕事用 Wi-Fi 接続にプロキシサーバーを使用する iOS、iPadOS、macOS、および Android Enterprise 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。

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. デバイスタイプのタブをクリックして、適切な設定を構成します。詳細については、iOS と macOS、Android、および Windows の Wi-Fi プロファイル設定を参照してください。

   Wi-Fi ネットワークへのアクセス時にユーザー名とパスワードを入力するように、組織がユーザーに要求している場合、［ユーザー名］フィールドに「`%UserName%`」と入力します。
8. 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。

終了したら： Wi-Fi 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ます。

iOS および macOS ：Wi-Fi プロファイル設定

iOS、iPadOS、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。
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。
MAC ランダム化を無効にする	この設定では、デバイスが Wi-Fi ネットワークに参加したときに MAC アドレスをランダム化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。
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、iPadOS、および macOS デバイスにのみ適用されます。Hotspot オプションのいずれかを選択した場合は、他のデバイスタイプの設定に同じ Wi-Fi プロファイルを使用しないでください。
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。

iOS、**iPadOS**、および **macOS** ：**Wi-Fi** プロファイル設定	説明
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、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。
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。
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、**iPadOS**、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。
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。
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。
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）。実際のユーザー名は、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。

iOS、iPadOS、および macOS ：Wi-Fi プロファイル設定	説明
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、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、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［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。
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てい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。
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。

iOS、iPadOS、および **macOS** ：**Wi-Fi** プロファイル設定	説明
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 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。
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。
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。
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てい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。
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。
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。

iOS、**iPadOS**、および **macOS** ：**Wi-Fi** プロファイル設定	説明
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に 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。 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 Android 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。
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。

Android ：**Wi-Fi** プロファイル設定	説明
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。
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。 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。 CHAP は、Samsung Knox を使用するデバイスではサポートされません。
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）。実際のユーザー名は、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。

Android ：**Wi-Fi** プロファイル設定	説明
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）。実際のユーザー名は、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。
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。
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てい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。
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。

Android : **Wi-Fi** プロファイル設定	説明
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。
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てい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。
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。
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。
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。
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。Active Directory 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。Active Directory 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。

Windows ：**Wi-Fi** プロファイル設定	説明
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。
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。
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を対象に 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。

Windows ：**Wi-Fi** プロファイル設定	説明
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。
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。
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。
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。

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。 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。
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。
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 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。

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、iPadOS、macOS、Samsung Knox、および Windows 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。

Samsung Knox 以外の Android デバイスの仕事用 VPN に接続するには、VPN アプリのアプリ構成設定を使用して 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
iOS および iPadOS	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。 KNOX SDK を使用するサポートされている VPN クライアントアプリをデバイスにインストールする必要があります。
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 プロファイルを作成する代わりに、CylanceGATEWAY の使用を選択して、デバイスが VPN プロバイダーとして認識するゼロトラストネットワークアクセス（ZTNA）プロファイルを作成できます。CylanceGATEWAY はデフォルトで何も設定されていません。詳細については、「BlackBerry UEM と CylanceGATEWAY の統合による ZTNA プロファイルの作成」を参照してください。

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。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 プロファイルを作成する代わりに、CylanceGATEWAY の使用を選択して、デバイスが VPN プロバイダーとして認識するゼロトラストネットワークアクセス（ZTNA）プロファイルを作成できます。CylanceGATEWAY はデフォルトで何も設定されていません。詳細については、「BlackBerry UEM と CylanceGATEWAY の統合による ZTNA プロファイルの作成」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、SCEP、共有証明書、またはユーザー資格情報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、iPadOS、macOS、および Samsung Knox 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。
- 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. デバイスタイプのタブをクリックして、適切な設定を構成します。詳細については、iOS と macOS、Android、および Windows の VPN プロファイル設定を参照してください。

   組織によって、VPN ネットワーク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いる場合は、［ユーザー名］フィールドに `%UserName%` と入力します。
6. ［追加］をクリックします。

終了したら： Wi-Fi 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ます。

iOS および macOS ：VPN プロファイル設定

iOS、iPadOS、 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。
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。 ［IKEv2 常時オン］を選択した場合、多くの設定にはセルラーと Wi-Fi 接続の値が個別に設定されます。
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。
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。

iOS、iPadOS、 および **macOS** ：**VPN** プロファイル設定	説明
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。
EAP プラグイン	この設定では、VPN の認証プラグインを指定します。 この設定は、［接続タイプ］が［L2TP］または［PPTP］に設定され、［認証の種類］が［RSA SecurID ］に設定されている場合にのみ有効です。
認証プロトコル	この設定では、VPN の認証プロトコルを指定します。 この設定は、［接続タイプ］が［L2TP］または［PPTP］に設定され、［認証の種類］が［RSA SecurID ］に設定されている場合にのみ有効です。
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、［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、iPadOS、 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］または［IKEv2 常時オン］に、［認証タイプ］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］が［共有証明書］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。 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 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］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。
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。
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。

iOS、iPadOS、 および **macOS** ：**VPN** プロファイル設定	説明
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］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。
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］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。
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］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。
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 および iPadOS 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、［認証タイプ］が［共有証明書］に設定されている場合。

iOS、**iPadOS**、および **macOS** ：**VPN** プロファイル設定	説明
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。
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。
アイドル状態のときに切断	この設定では、指定した時間アイドル状態になっているときに VPN 接続が切断するかどうかを指定します。 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。
アイドルタイマーで切断	この設定は、VPN が切断されるまでのアイドル時間を秒単位で指定します。 この設定は、［アイドル状態のときに切断］設定が選択されている場合のみ有効です。
ユーザーが必要に応じて VPN を無効にすることを許可しない	この設定は、ユーザーが必要に応じて VPN を無効に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［IPsec］、［Cisco AnyConnect ］、［Juniper ］、［Pulse Secure ］、［F5 ］、［SonicWALL Mobile Connect ］、［Aruba VIA ］、［Check Point Mobile ］、［OpenVPN ］、または［カスタム］に設定されている場合のみ有効です。
ローカルネットワークを除外	この設定では、VPN 接続の使用からローカルネットワークトラフィックを除外するかどうかを指定します。［すべてのネットワークを含める］設定も選択されている場合、ローカルネットワークトラフィックは VPN 経由でルーティングされません。
デフォルト以外のルートはすべて、ローカルに定義されたルートより優先されます	この設定では、VPN のデフォルト以外のルートがローカルに定義されたルートより優先されるかどうかを指定します。［すべてのネットワークを含める］設定も選択されている場合、この設定は無視されます。 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 ］、または［カスタム］に設定されている場合のみ有効です。

iOS、iPadOS、 および **macOS** ：**VPN** プロファイル設定	説明
すべてのネットワークを含める	この設定では、すべてのトラフィックを VPN 経由で送信するかどうかを指定します。［ローカルネットワークを除外］も選択されている場合、ローカルネットワークトラフィックは VPN 経由で送信されません。この設定は、iOS および iPadOS 13 以降を実行しているデバイスにのみ適用されます。
プロバイダー指定の要件	この設定は、指定された VPN プロバイダーを指定します。VPN プロバイダーがシステム拡張として実装されている場合は、この設定は必須です。 この設定は、［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］に設定されている場合のみ有効です。
ユーザーが自動接続を無効にできるようにする	この設定は、ユーザーが VPN 接続を無効にできるかどうかを指定します。 この設定は、［接続タイプ］が［IKEv2 常時オン］に設定されている場合のみ有効です。
携帯電話と Wi-Fi に同じトンネル設定を使用する	この設定は、デバイスが携帯電話ネットワークまたは Wi-Fi ネットワークのどちらを経由してデータを送信しているかに応じて、デバイスに個別の VPN 設定を行う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は、同じプロファイルで異なる携帯電話と Wi-Fi の設定を設定できます。 この設定は、［接続タイプ］が［IKEv2 常時オン］に設定されている場合のみ有効です。
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、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。
最大 TLS バージョン	この設定では、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。
証明書のタイプ	この設定では、IKEv2 マシン認証に使用される証明書のタイプを指定します。 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。

iOS、**iPadOS**、および **macOS** ：**VPN** プロファイル設定	説明
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サーバー証明書を発行した CA の共通名を指定します。証明書を使用して xAuth を有効にする場合は、この設定が必要です。 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。
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サーバー証明書の共通名を指定します。 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。
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］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。
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］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。
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］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。
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］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。
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］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。
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］または［IKEv2 常時オン］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。

iOS、iPadOS、 および **macOS** ：**VPN** プロファイル設定	説明
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］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。
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］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。
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］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。
証明書失効チェックを有効にする	この設定は、サーバー証明書の証明書失効チェックを試行するかどうかを指定します。応答がない場合、チェックは失敗しません。 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。
フォールバックを有効にする	この設定は、Wi-Fi Assist が有効な場合に、デバイスがモバイルネットワーク経由で VPN トンネルを確立できるかどうかを指定します。この設定は、iOS および iPadOS 13 以降を実行しているデバイスにのみ適用され、サーバーが個々のユーザーに対して複数のトンネルをサポートしている必要があります。 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。
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］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。
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］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。
MTU	この設定は、最大転送単位をバイト単位で指定します。 この設定は、［接続タイプ］が［IKEv2 常時オン］に設定されている場合のみ有効です。

iOS、iPadOS、 および **macOS** ：**VPN** プロファイル設定	説明
ボイスメール	この設定では、ボイスメールサービスへの接続が VPN トンネルを介して送信されるか、VPN トンネル外で送信されるか、ブロックされるかを指定します。 この設定は、［接続タイプ］が［IKEv2 常時オン］に設定されている場合のみ有効です。これは Wi-Fi 接続にのみ適用されます。
AirPrint	この設定では、AirPrint 接続を VPN トンネルを介して送信するか、VPN トンネル外で送信するか、ブロックするかを指定します。 この設定は、［接続タイプ］が［IKEv2 常時オン］に設定されている場合のみ有効です。これは Wi-Fi 接続にのみ適用されます。
VPN トンネル外のキャプティブ Web シートからのトラフィックを許可	この設定では、キャプティブ Web シートからのトラフィックを VPN トンネル外で送信できるかどうかを指定します。 この設定は、［接続タイプ］が［IKEv2 常時オン］に設定されている場合のみ有効です。これは Wi-Fi 接続にのみ適用されます。
VPN トンネル外のすべてのキャプティブネットワークアプリからのトラフィックを許可	この設定では、すべてのキャプティブネットワークアプリからのトラフィックを VPN トンネル外で送信でき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は、トラフィックをトンネル外で送信できる個々のアプリケーションを指定できます。 この設定は、［接続タイプ］が［IKEv2 常時オン］に設定されている場合のみ有効です。これは Wi-Fi 接続にのみ適用されます。
これらのアプリからのトラフィックは VPN トンネル外で許可	この設定では、トラフィックをトンネル外で送信できる個別のキャプティブネットワークアプリを指定します。 この設定は、［接続タイプ］が［IKEv2 常時オン］に設定されている場合のみ有効です。これは Wi-Fi 接続にのみ適用されます。
VPN トンネル外でアプリトラフィックを許可	この設定では、トラフィックをトンネル外で送信できるアプリを指定します。 この設定は、［接続タイプ］が［IKEv2 常時オン］に設定されている場合のみ有効です。これは Wi-Fi 接続にのみ適用されます。
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。
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。

iOS、iPadOS、 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。
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。
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］、［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。
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。
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。
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。
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。

iOS、**iPadOS**、 および **macOS** ：**VPN** プロファイル設定	説明
関連付けられたドメイン	この設定では、デバイス上で VPN 接続を開始できるドメインを指定します。ドメインは、apple-app-site-association ファイルにも含まれている必要があります。 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。
除外されたドメイン	この設定は、デバイスで VPN 接続の開始をブロックされ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。
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。
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。

Android ：**VPN** プロファイル設定

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

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。
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。 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。

Android : **VPN** プロファイル設定	説明
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。 ［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。
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。
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。 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。 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。 ［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。
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。 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 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。 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。
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。

Android ：**VPN** プロファイル設定	説明
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。 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。
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。
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 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。

Android ：**VPN** プロファイル設定	説明
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。
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。
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。
組み込み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。
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。 ［組み込み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。

Windows ：**VPN** プロファイル設定	説明
EAP 設定	この設定では、EAP 設定の XML を指定します。 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。
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。
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。 • 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。

Windows ：**VPN** プロファイル設定	説明
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。
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。 • アプリのインストール場所。例：`C:\Windows\System\Notepad.exe`。 • 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。
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。
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。

Windows ：**VPN** プロファイル設定	説明
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。
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	
認証変換定数	この設定では、VPN の認証レベルを指定します。この設定は、VPN サーバーの設定と一致する必要があります。
暗号変換定数	この設定は、VPN の暗号化レベルを指定します。この設定は、VPN サーバーの設定と一致する必要があります。
暗号化方式	この設定では、VPN のフェーズ 1 暗号化レベルを指定します。この設定は、VPN サーバーの設定と一致する必要があります。
整合性の確認方式	この設定では、VPN のフェーズ 1 認証レベルを指定します。この設定は、VPN サーバーの設定と一致する必要があります。

Windows ：VPN プロファイル設定	説明
Diffie-Hellman グループ	この設定は、VPN のキーグループを指定します。この設定は、VPN サーバーの設定と一致する必要があります。
PFS グループ	この設定では、VPN に使用される Perfect Forward Secrecy 暗号化プロトコルを指定します。この設定は、VPN サーバーの設定と一致する必要があります。
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。
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 UEM と CylanceGATEWAY の統合による ZTNA プロファイルの作成

VPN プロファイルを使用する代わりに、UEM と CylanceGATEWAY を統合できます。CylanceGATEWAY は、Cylance Endpoint Security テナントで有効にすることができる、クラウドネイティブの人工知能（AI）支援型ゼロトラストネットワークアクセス（ZTNA）ソリューションです。その後で、CylanceGATEWAY を Cylance 管理コンソールで設定できます。CylanceGATEWAY の設定方法の詳細については、Cylance Endpoint Security セットアップ関連の資料の「BlackBerry Gateway のセットアップ」を参照してください。CylanceGATEWAY がデバイスで有効になっているときに、デバイスが VPN プロバイダーとして認識する ZTNA プロファイルを作成します。CylanceGATEWAY はデフォルトでは何も信頼せず、誰も信頼しません。

CylanceGATEWAY は、デバイスがネットワークに接続されていない場合でも、デバイスに到達させないにインターネット宛先への接続をブロックできるようにすることで、ユーザーの iOS、Android、Windows 10 および 11、macOS デバイスを保護します。

デバイスの保護に加えて、CylanceGATEWAY は、ユーザーの使用パターンが想定内のものなのか異常な動作なのかを継続的に分析することで、組織のプライベートネットワークおよびクラウドベースのアプリケーションへのアクセスを保護します。異常イベントの割合が設定しきい値を超えた場合、CylanceGATEWAY はユーザーのネットワークアクセス制御ポリシーを動的に上書きしてネットワークアクセスをブロックし、続行する前にユーザーの認証を要求できます。

CylanceGATEWAY 管理者は、ユーザーがアクセスしたりアクセスをブロックしたりできるインターネットおよびプライベートネットワークの宛先を設定できます。

アプリごとの VPN 設定の有効化と割り当て

iOS、iPadOS、Samsung Knox、および Windows 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。

デバイス	アプリの設定
iOS および iPadOS	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 アクティベーションを備えた Samsung Knox デバイス	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	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。

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 および iPadOS デバイスのアプリに割り当てるかを決定します。

アプリごとの **VPN** 設定	優先順位
アプリに直接関連付けられている場合	アプリグループによって間接的に関連付けられたアプリごとの VPN 設定よりも優先されます。
ユーザーに直接関連付けられている場合	ユーザーグループによって間接的に関連付けられたアプリベース VPN 設定よりも優先されます。
必要なアプリに割り当てられている場合	同じアプリのオプションインスタンスに割り当てられたアプリごとの VPN 設定よりも優先されます。

アプリごとの **VPN** 設定	優先順位
アルファベット順リストの前に表示されたユーザーグループ名に関連付けられている場合	次の条件が満たされる場合、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、iPadOS、macOS、および Android の各デバイスでは、プロキシプロファイルを作成します。Windows 10 デバイスでは、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
iOS および iPadOS	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。 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ができます。 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、監視対象デバイスに対してのみグローバルプロキシとなり、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優先されます。監視対象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。

デバイス	プロキシ設定
Android	Android Enterprise デバイスでは、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。 アクティベーションが Android または MDM 制御 の ユーザーのプライバシー 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。
Samsung Knox	プロキシプロファイルを作成して、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。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か、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。 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ができます。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。 • 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て、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

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］をクリックします。 **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）。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。
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.** 組織によって、プロキシサーバー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%` 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要求する場合は、*<domain>**<username>* 形式を使用します。

7. 別のデバイスタイプについて、手順 4〜6 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。
- 複数のプロキシプロファイルを作成する場合は、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。プロファイルを選択し、⇅ をクリックしてプロファイルを上下に移動してランク付けします。［保存］をクリックします。

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 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を使用した 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 および iPadOS 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 と、サポートされているデバイスは、組織のネットワークに接続するの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、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 および iPadOS 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 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 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	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。
3	オプションで、BlackBerry Connectivity アプリの DNS 設定を指定します。
4	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。
5	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および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なければなりません。

BlackBerry UEM ドメインでは：

環境	要件
すべての UEM 環境	• 組織のファイアウォールは、ポート 3101 を介した *<region>*.turnb.bbsecure.com および *<region>*.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。プロキシサーバーを使用するように UEM を設定している場合は、ポート 3101 を経由して、これらのサブドメインに接続することをこのプロキシサーバーが許可していることを確認します。 • 個々の 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場合、BlackBerry Secure Connect Plus を使用した Google Play への接続を許可するために必要な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 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、BlackBerry Secure Connect Plus 向けに per-app VPN を設定することをお勧めします。
UEM オンプレミス	• お使いの環境に 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 • 必要に応じて、複数の BlackBerry Connectivity Node をインストールして、追加の BlackBerry Secure Connect Plus インスタンスをインストールできます。 • 必要に応じて、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サーバーグループを作成できます。
UEM Cloud	• 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。BlackBerry Connectivity Node をインストールまたはアップグレードすると、BlackBerry Secure Connect Plus もインストールまたはアップグレードされます。BlackBerry Secure Connect Plus を有効にする前に、BlackBerry Connectivity Node をアクティブ化する必要があります。 • TCP プロキシサーバー（透過型または SOCKS v5）経由で BlackBerry Secure Connect Plus と BlackBerry Infrastructure の間を移動するデータをルーティングする場合は、BlackBerry Connectivity Node 管理コンソールを使用してプロキシ設定を構成できます（［一般設定］ > ［プロキシ］）。

サポート対象のデバイスでは：

プロファイル	説明
iOS および iPadOS	• デバイスは、BlackBerry UEM Client を使用してアクティブ化する必要があります • MDM コントロールの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： • 仕事用領域専用（プレミアム） • 仕事用および個人用 - フルコントロール（プレミアム） • 仕事用と個人用 - ユーザープライバシ（プレミアム）

Samsung Knox Workspace	• サポートされる Samsung Knox のバージョン
	• 次のいずれかのアクティベーションタイプ：
	  • 仕事用領域専用（Samsung Knox）
	  • 仕事用および個人用 - フルコントロール（Samsung Knox）
	  • 仕事用および個人用 - ユーザープライバシ（Samsung Knox）

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 および iPadOS 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）。

作業を始める前に：組織の 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。

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］ > ［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。
2. 既存のエンタープライズ接続プロファイルを編集するか、新しいプロファイルを作成します。
3. 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および設定した場合、［**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。
4. 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。
5. ［追加］をクリックします。
6. 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。

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。デバイスユーザーは、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。プロファイルを選択し、⇵ をクリックしてプロファイルを上下に移動してランク付けします。［保存］をクリックします。
- iOS、iPadOS、Android Enterprise、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。
- オプションで、BlackBerry Connectivity アプリの DNS 設定を指定します。

BlackBerry Connectivity アプリの更新

最新の BlackBerry Connectivity アプリは、Google Play および BlackBerry myAccount ソフトウェアのダウンロードから入手できます。

- **Android** ユーザー：デバイスユーザーに、BlackBerry UEM Client と Google Play で使用可能な BlackBerry Connectivity アプリの最新バージョンに更新するよう指示します。Google Play にアクセスできないデバイスの場合は、Google Play にアクセスできない Samsung Knox Workspace および Android Enterprise デバイスの BlackBerry Connectivity アプリの更新 の指示に従います。
- **Samsung Knox Workspace** ユーザー：
  - Google Play アプリ管理が有効になっている Knox デバイスでは、デバイスユーザーに BlackBerry UEM Client および Google Play で使用可能な BlackBerry Connectivity アプリの最新バージョンに更新するように指示します。UEM 管理コンソールで、BlackBerry Connectivity アプリを「すべての Android デバイス」に送信するように設定し、適切なユーザーとグループに割り当てます。
  - Google Play アプリ管理が有効になっていない Knox デバイスの場合は、Google Play にアクセスできない Samsung Knox Workspace および Android Enterprise デバイスの BlackBerry Connectivity アプリの更新 の指示に従います。

メモ：CA 証明書プロファイルを使用して CA 証明書を Android または Knox Workspace デバイスに配布する場合は、アップロードした証明書が .der ファイル拡張子で DER エンコードされていること、または .pem ファイル拡張子で PEM エンコードされていることを確認します。これらの要件を満たさない CA 証明書は、BlackBerry Connectivity アプリの接続に問題を引き起こす可能性があります。

Google Play にアクセスできない Samsung Knox Workspace および Android Enterprise デバイスの BlackBerry Connectivity アプリの更新

以下の手順に従って、ユーザーのデバイス上の BlackBerry Connectivity アプリを最新バージョンに更新します。

最新のサーバー更新を利用するには、最新バージョンの BlackBerry UEM にアップグレードすることをお勧めします。

作業を始める前に：

- BlackBerry myAccount ソフトウェアのダウンロードにアクセスして、BlackBerry Connectivity アプリの最新バージョンをダウンロードします。UEM インスタンスをホストする各コンピュータでファイルを保存します。
- Knox Workspace デバイスユーザーに、BlackBerry UEM Client を Google Play で利用可能な最新バージョンに更新するように指示します。
- Knox Workspace アクティベーションの場合、BlackBerry Connectivity アプリの最新リリースが Google Play で利用できるため、ユーザーはアプリを自分で更新できます。アプリをサポートするように UEM を設定する場合にも、次の手順を完了する必要があります。

- Google Play が仕事用領域で有効になっている場合、Android Enterprise アクティベーションのために、ユーザーは Google Play から自分で BlackBerry Connectivity アプリの最新リリースに更新できます。アプリをサポートするように UEM を設定する場合にも、次の手順を完了する必要があります。
- UEM を設定して、BlackBerry Secure Connect Plus が必要なデバイスの BlackBerry Connectivity アプリをサポートするには：

1. UEM 管理コンソールのメニューバーで、［アプリ］をクリックします。
2. > ［内部アプリ］をクリックします。
3. ［参照］をクリックし、Android の最新 BlackBerry Connectivity アプリの .apk ファイルを選択します。
4. ［追加］をクリックします。
5. ［送信先］フィールドで、［すべての **Android** デバイス］を選択します。
6. ［**Google** ドメインでアプリを公開］の選択を解除します。
7. ［追加］をクリックします。
8. 前の手順で追加したアプリを、Google Play にアクセスできない Samsung Knox Workspace デバイスと Android Enterprise デバイスに割り当てます。アプリケーション種別は［必須］に設定する必要があります。

終了したら： UEM は、Knox Workspace デバイス上の UEM Client にポリシー更新通知を送信します。UEM Client は、アプリが必要なアプリとして割り当てられたときに BlackBerry Connectivity アプリを更新します。

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
- iPadOS
- Android

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。

iOS ：エンタープライズ接続プロファイル設定

iOS の設定は iPadOS デバイスにも適用されます。

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。

設定	説明
VPN をオンデマンドで有効にする	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）。
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	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。
Safari ドメイン	Safari でVPN接続を開始できるドメインを指定します。
カレンダードメイン	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。
連絡先ドメイン	連絡先内でVPN接続を開始できるドメインを指定します。
メールドメイン	メール内でVPN接続を開始できるドメインを指定します。
関連付けられたドメイン	関連付けられたドメインを指定します。
除外されたドメイン	除外された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。
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。
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。 ［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、UEM 経由で BlackBerry Infrastructure と通信することを UEM Client に許可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、KB 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、組織のファイアウォールで追加のポートを開いて、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ため、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。『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。 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 Connectivity アプリ DNS 設定を指定

BlackBerry Connectivity アプリにおいて、セキュリティで保護されたトンネル接続に使用する DNS サーバーを指定できます。DNS 設定を指定しなかった場合、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. 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. 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］ > ［ネットワークと接続］ > ［**BlackBerry Dynamics** 接続］をクリックします。
2. 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編集します。

3. ［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。
4. ［デフォルトの許可されたドメインルートタイプ］セクションで、［直接］を選択して、BlackBerry Proxy を介さずアプリからドメインにトラフィックを直接ルーティングします。
5. ［保存］をクリックします。

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 が開始しない

考えられる原因

BlackBerry Secure Connect Plus アダプタの 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、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 Services 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. `<drive>:\Program Files\BlackBerry\UEMSecureConnectPlus\config\blackberry\` に移動して **configureRRAS.bat** を 実行します
5. `<drive>:\Program Files\BlackBerry\UEMSecureConnectPlus\config\` に移動して **configure-network-interface.cmd** を実行します
6. Windows Services で、**BlackBerry UEM – BlackBerry Secure Connect Plus** サービスを開始します。

BlackBerry Secure Connect Plus のログファイルの表示

目的	ログファイル	例
BlackBerry Secure Connect Plus が BlackBerry Infrastructure に接続されていることを確認する	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 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。

iOS デバイスの自動認証の有効化

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またはシングルサインオン拡張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。

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します。カスタム拡張の設定を指定することも、Apple で提供されている Kerberos 拡張を使用することもできます。

作業を始める前に： 証明書ベースの認証を使用する場合は、必要な証明書プロファイルを作成します。

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］ > ［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。
2. ＋ をクリックします。
3. プロファイルの名前と説明を入力します。
4. ［シングルサインオン拡張タイプ］ドロップダウンリストで、Apple により提供される［カスタム拡張］または［**Kerberos** 組み込み拡張機能］をクリックします。

タスク	手順
［カスタム拡張機能］を選択した場合	**a.** ［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。 **b.** 適切なサインオンのタイプを選択します。 **c.** サインオンタイプとして［資格情報］を選択した場合は、次の手順を実行します。 **1.** ［領域］フィールドに、資格情報の領域名を入力します。 **2.** ［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。 **3.** ［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。 **4.** 必要に応じて追加のドメインを追加します。 **d.** サインオンタイプとして［リダイレクト］を選択した場合は、次の手順を実行します。 **1.** ［**URL**］セクションで、＋ をクリックして URL を追加します。 **2.** ［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。 **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
［**Kerberos** 組み込み拡張機能］を選択した場合	**a.** ［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。 **b.** ［領域名］フィールドに、資格情報の領域名を入力します。 **c.** 環境に適した［**Apple Kerberos SSO** 拡張データ］を選択します。デフォルトでは、自動ログインと Active Directory 自動検出が許可されています。また、デフォルトの領域を指定することも、管理対象アプリのみがシングルサインオンを使用できるようにすることも、ユーザーにアクセスの確認を要求することもできます。 **d.** 接続の［プリンシパル名］を設定します。 **e.** 証明書プロファイルを使用して認証用の PKINIT 証明書を提供する場合は、［認証用の **PKINIT** 証明書の選択］ドロップダウンリストからプロファイルタイプを選択し、適切なプロファイルを選択します。 **f.** Generic Security Service API を使用している場合は、［**Kerberos** キャッシュの **GSS** 名］を指定します。 **g.** ［アプリケーションバンドル **ID**］セクションで、＋をクリックして、チケット認可チケットへのアクセスを許可するバンドル ID を指定します。 **h.** ［優先キー配布センター］セクションで＋をクリックして、優先サーバーが DNS を使用して検出できない場合に指定します。各サーバーを krb5.conf ファイルで使用されているものと同じ形式で指定します。指定されたサーバーは接続性チェックに使用され、まず Kerberos トラフィックに対して試行されます。サーバーが応答しない場合、デバイスは DNS 検出を使用します。 **i.** ［カスタムドメイン領域マッピング］フィールドに、ドメインから領域名への必要なカスタムマッピングをペイロード形式で入力します（たとえば、`<key>sample-realm1</key><array><string>org</string></array>`）。 **j.** ［ログインヒント］フィールドで、Kerberos ログインウィンドウの下部に表示するテキストを指定します。

5. ［保存］をクリックします。

iOS および macOS デバイスの DNS サーバーの指定

特定のドメインへのアクセスに使用する DNS サーバーを指定できます。この設定は、より高速で安全な Web ブラウジング体験を提供するのに役立ちます。

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］ > ［ネットワークと接続］ > ［**DNS**］をクリックします。
2. ＋をクリックします。
3. プロファイルの名前と説明を入力します。
4. デバイスタイプのタブをクリックします。
5. DNS サーバーとの通信に使用する DNS プロトコルを選択します。
6. 次の操作のいずれかを実行します。
   a) ［**HTTPS**］を選択した場合は、https:// スキームを使用して、DNS-over-HTTPS サーバーの URI テンプレートを入力します。

b) ［**TLS**］を選択した場合は、DNS-over-TLS サーバーのホスト名を入力します。

7. ユーザーが設定を無効にできないようにするには、［ユーザーが **DNS** 設定を無効にすることを許可しない］チェックボックスをオンにします。このオプションは、監視対象デバイスにのみ影響します。
8. ［**DNS** アドレス］フィールドで、使用する DNS サーバーの IP アドレスのリストを指定します。これらは IPv4 アドレスと IPv6 アドレスを混在させることができます。
9. ［ドメイン］フィールドで、DNS サーバーを使用する DNS クエリを決定するために使用するドメイン文字列のリストを指定します。
10. ［**DNS** オンデマンドルール］フィールドで、サンプルペイロード形式を使用して DNS オンデマンドルールを指定します。
11. 各デバイスタイプについて、手順 5〜10 を繰り返します。
12. ［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 ドメインの指定

管理対象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「管理対象ドメイン」として定義できます。管理対象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 および iPadOS デバイスのみに適用されます。

管理対象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、管理対象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を受信者のメールアドレスとして追加した場合、デバイスではそのアドレスを赤く表示して受信者が組織外の人であることを警告します。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。
- 管理対象 Web ドメインのドキュメント、または管理対象 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。管理対象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。

1. メニューバーで、［ポリシーとプロファイル］ > ［ネットワークと接続］ > ［管理対象ドメイン］の順にクリックします。
2. ＋ をクリックします。
3. プロファイルの名前と説明を入力します。
4. ［説明］フィールドに、プロファイルの説明を入力します。
5. ［管理対象ドメイン］セクションで ＋ をクリックします。
6. ［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（たとえば、`example.com/canada` ではなく、`example.com`）。
7. ［追加］をクリックします。
8. ［管理対象 **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「管理対象の Safari Web ドメイン」を参照してください。
9. ［**Web** ドメイン］フィールドにドメイン名を入力します。
10. 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デバイスでのみサポートされます。
11. ［追加］をクリックし、もう一度［追加］をクリックします。

終了したら： 管理対象ドメイン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。

iOS デバイスでのアプリのネットワーク使用の制御

ネットワーク使用プロファイルを使用して、iOS および iPadOS 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、ユーザーおよびグループに割り当てます。

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］ > ［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。
2. ＋ をクリックします。
3. プロファイルの名前と説明を入力します。
4. ＋ をクリックします。
5. 次の操作のいずれかを実行します。
   - ［アプリを追加］をクリックして、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］オプションを選択し、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.***）。
6. デバイスのローミング中に、アプリがデータを使用するのを防止するには、［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。
7. 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、アプリがデータを使用するのを防止するには、［携帯データを許可］チェックボックスをオフにします。
8. ［追加］をクリックします。
9. 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： 複数のネットワーク使用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。プロファイルを選択し、⇅ をクリックしてプロファイルを上下に移動してランク付けします。［保存］をクリックします。

ネットワーク使用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ます。

iOS デバイスでの 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使用して、ユーザーが監視対象の iOS または iPadOS 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）。

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。 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する	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。

1. メニューバーで、［ポリシーとプロファイル］ > ［ネットワークと接続］ > ［**Web** コンテンツフィルター］の順にクリックします。
2. ＋ をクリックします。
3. 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。
4. 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 b と c 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.** その他の Web サイト追加するには、必要に応じてこの手順を繰り返します。 **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.** その他の Web サイト追加するには、必要に応じてこの手順を繰り返します。

5. ［追加］をクリックします。

終了したら： Web コンテンツフィルター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ます。

iOS デバイス用 AirPrint プロファイルの作成

AirPrint プロファイルを使用すると、AirPrint をサポートし、アクセス可能で、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します。AirPrint プロファイルを設定して iOS および iPadOS デバイスに割り当てることで、ユーザーがプリンタを手動で設定する必要がなくなります。

1. メニューバーで、［ポリシーとプロファイル］ **>** ［ネットワークと接続］ **>** ［**AirPrint**］の順にクリックします。
2. ＋ をクリックします。
3. プロファイルの名前と説明を入力します。
4. ［**AirPrint** の設定］セクションで ＋ をクリックします。
5. ［**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。

6. ［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
7. 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。
8. 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。
9. ［追加］をクリックし、もう一度［追加］をクリックします。

終了したら： AirPrint 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ます。

iOS デバイス用 AirPlay プロファイルの作成

AirPlay は、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ための機能です。

AirPlay プロファイルを使用すると、iOS および iPadOS のユーザーが接続できる AirPlay デバイスを指定できます。AirPlay プロファイルには、次の 2 つのオプションがあります。

- 組織の AirPlay デバイスがパスワードで保護されている場合、許可された宛先デバイスのパスワードを指定して、iOS および iPadOS デバイスユーザーがパスワードを知らなくても接続できるようにできます。
- 監視対象デバイスの場合は、監視対象デバイスに対して許可された AirPlay デバイスのリストを指定することで、ユーザーが接続できる AirPlay デバイスを制限できます。監視対象デバイスは、リストで指定された AirPlay デバイスにのみ接続できます。リストを作成しないと、監視対象デバイスはどの AirPlay デバイスにも接続できます。

1. メニューバーで、［ポリシーとプロファイル］ **>** ［ネットワークと接続］ **>** ［**AirPlay**］の順にクリックします。
2. ＋ をクリックします。
3. AirPlay プロファイルの名前と説明を入力します。
4. ［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。
5. ［デバイス名］フィールドに、パスワードを指定する 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 または iPadOS 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。
6. ［パスワード］フィールドにパスワードを入力します。
7. ［追加］をクリックします。
8. ［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。
9. ［デバイス **ID**］フィールドに、監視対象デバイスが接続できるようにする 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。監視対象デバイスは、リストの AirPlay デバイスにのみ接続できます。
10. ［追加］をクリックします。

終了したら： AirPlay 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ます。

Android デバイス用のアクセスポイント名プロファイルの作成

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。アクセスポイント名プロファイルは、仕事用領域のみ アクティベーションまたは 仕事用と個人用 - フルコントロール アクティベーションを使用するデバイスでサポートされます。

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、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］チェックボックスを選択します。

作業を始める前に： 必要なすべての APN 設定を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］ > ［ネットワークと接続］ > ［アクセスポイント名］の順にクリックします。
2. ＋ をクリックします。
3. 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。
4. ［アクセスポイント名］フィールドに、アクセスポイント名を入力します。
5. 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。
   詳細については、「アクセスポイント名プロファイルの設定」を参照してください。
6. ［保存］をクリックします。

終了したら： アクセスポイント名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ます。

アクセスポイント名プロファイルの設定

アクセスポイント名プロファイルの設定	説明
アクセスポイント名	この設定は、デバイスが通信事業者と通信するときに使用するアクセスポイント名（APN）を指定します。APN は短いテキストの文字列です。
APN タイプビットマスク	この設定は、この APN 設定を使用するデータ通信のタイプを指定します。通信の種類によって、使用する設定が異なる場合があります。
プロキシアドレス	この設定は、接続上のすべての Web トラフィックに使用する HTTP プロキシを指定します。この設定は、ほとんどの通信事業者には必要ありません。
プロキシポート	この設定は、接続上のすべての Web トラフィックに使用する HTTP プロキシポートを指定します。この設定は、ほとんどの通信事業者には必要ありません。
MMSC	この設定は、MMS メッセージの送受信に使用するマルチメディアメッセージングサービスセンター（MMSC）を指定します。

アクセスポイント名プロファイルの設定	説明
MMS プロキシアドレス	この設定は、MMSC と通信して MMS メッセージを送受信するための HTTP プロキシを指定します。
MMS プロキシポート	この設定は、MMSC と通信して MMS メッセージを送受信するための HTTP プロキシポートを指定します。
認証の種類	この設定では、通信に使用する認証の種類を指定します。
ユーザー名	［認証の種類］設定が［NONE］以外に設定されている場合、認証に必要な場合はユーザー名を指定します。
パスワード	［認証の種類］設定が［NONE］以外に設定されている場合、認証に必要な場合はパスワードを指定します。
Mobile Country Code（MCC）	この設定は、APN 設定を使用する通信事業者ネットワークの Mobile Country Code を指定します。
Mobile Network Code（MNC）	この設定は、APN 設定を使用する通信事業者ネットワークの Mobile Network Code を指定します。
プロトコル	この設定は、IPv6 ネットワークをサポートするデバイスのホームネットワークで IPv4、IPv6、またはその両方を有効にするかどうかを指定します。
ローミングプロトコル	この設定は、IPv6 ネットワークをサポートするデバイスのローミング中に IPv4、IPv6、またはその両方を有効にするかどうかを指定します。
有効にされた通信事業者	この設定は、APN がその通信事業者に対して有効であるかどうかを指定します。
MVNO タイプ	この設定は、この APN の使用を特定の MVNO（モバイルネットワークリセラー）または加入者アカウントに制限するかどうかを指定します。

デバイスまたはアプリでの PKI 証明書の使用

PKI 証明書は、認証局（CA）証明書サブジェクトの ID を確認し、その ID を公開鍵にバインドする CA によって発行されたデジタル文書です。各証明書には、証明書とは別に安全に保存された、対応する秘密鍵があります。公開鍵と秘密鍵は非対称キーペアを形成し、それをデータの暗号化および ID の認証に使用できます。CA は、CA を信頼するエンティティがその証明書も信頼できることを実証するために証明書に署名します。CA は、違反が発生した場合に、後で証明書の信頼を取り消すことができます。

デバイスおよびアプリでは、デバイスの機能とアクティベーションタイプに応じて、証明書を次の用途で使用できます。

- 仕事用メールサーバーを含む相互 TLS をサポートする Web サーバーに接続する場合に、SSL/TLS を使用して認証する
- 仕事用 Wi-Fi ネットワークまたは VPN で認証する
- S/MIME 保護を使用してメッセージを暗号化して署名する

デバイスでは、さまざまな目的に使用される複数の証明書を保存できます。BlackBerry UEM は、デバイス上の PKI 証明書の管理に役立つプロファイルを多数提供します。次に例を示します。

- CA サーバーの信頼性は、CA 証明書プロファイルを使用してデバイスおよびアプリに割り当てることができます。
- 証明書の自動登録は、SCEP およびユーザー資格情報プロファイルを使用して、デバイスおよびアプリに割り当てることができます。
- 公開暗号化証明書の取得は、証明書取得プロファイルを使用してデバイスおよびアプリに割り当てることができます。
- 証明書失効ステータスのチェックは、OCSP および CRL プロファイルを使用してデバイスおよびアプリに割り当てることができます。

デバイスで PKI 証明書を使用する場合は、次の操作を実行します。

手順	アクション
1	必要に応じて、BlackBerry UEM を組織の PKI ソフトウェアと統合します。
2	1 つ以上の CA 証明書プロファイルを作成して、デバイスとアプリに CA 証明書を送信します。
3	SCEP プロファイル、ユーザー資格情報プロファイル、共有証明書プロファイルを作成するか、特定ユーザーの証明書をアップロードして、クライアント証明書をデバイスとアプリに送信します。
4	必要に応じて、証明書プロファイルを Wi-Fi プロファイル、VPN プロファイル、またはメールプロファイルに関連付けます。
5	必要に応じて、証明書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ます。

手順	アクション
6	BlackBerry Dynamics アプリで証明書を使用する場合は、アプリ設定で、［BlackBerry Dynamics アプリで、ユーザー証明書、SCEP プロファイル、およびユーザー資格情報プロファイルを使用できるようにする］を選択します。

BlackBerry UEM と組織の PKI ソフトウェアとの統合

組織で PKI ソリューションを使用して証明書を発行する場合、BlackBerry UEM で管理するデバイスとアプリに、これらの PKI サービスで提供される証明書ベース認証を拡張できます。

Entrust 製品（Entrust IdentityGuard や Entrust Authority Administration Services など）と OpenTrust 製品（OpenTrust PKI や OpenTrust CMS など）は、クライアント証明書を発行する CA を提供します。所属組織の PKI ソフトウェアとの接続を設定し、複数のプロファイルを使って、CA 証明書やクライアント証明書をデバイスに送信することができます。

BlackBerry Dynamics 対応のデバイスの場合、BlackBerry Dynamics アプリの証明書を登録したり、Purebred などのアプリベースの証明書登録をサポートするアプリを使用するために、UEM と CA サーバー間の接続を作成する PKI コネクターを設定することもできます。

BlackBerry UEM と組織の Entrust ソフトウェアを接続する

組織の Entrust ソフトウェア（たとえば Entrust IdentityGuard や Entrust Authority Administration Services など）が発行した証明書を、BlackBerry UEM からデバイスや BlackBerry Dynamics アプリに送信できるようにするには、組織の Entrust ソフトウェアへの接続を UEM に追加します。

作業を始める前に： 所属組織の Entrust 管理者に連絡して、次の情報を取得します。

- Entrust MDM Web サービスの URL。
- UEM を Entrust ソフトウェアに接続する際に使用できる Entrust 管理者アカウントのログイン情報。
- 公開鍵（.der、.pem、または .cert）を含む Entrust CA 証明書。UEM はこの証明書を使用して Entrust サーバーへの SSL 接続を確立します。

1. 管理コンソールのメニューバーで、［設定］ > ［外部統合］ > ［認証局］の順にクリックします。
2. ［**Entrust** 接続を追加］をクリックします。
3. ［接続名］フィールドに、接続の名前を入力します。
4. ［**URL**］ フィールドに、Entrust MDM Web Service の URL を入力します。
5. ［ユーザー名］フィールドに、Entrust 管理者アカウントの名前を入力します。
6. ［パスワード］フィールドに、Entrust 管理者アカウントのパスワードを入力します。
7. CA 証明書をアップロードして、Entrust サーバーへの SSL 接続の確立を UEM に許可するには、［参照］をクリックします。CA 証明書に移動して選択します。
8. 接続をテストするには、［テスト接続］をクリックします。
9. ［保存］をクリックします。

終了したら： ユーザー資格情報プロファイルを作成して、PKI ソフトウェアからデバイスに証明書を送信します。

BlackBerry UEM を組織の Entrust IdentityGuard サーバーに接続したスマート認証情報の使用

Entrust IdentityGuard が管理する派生スマート認証情報を組織で使用する場合は、Android デバイスと、iOS および Android デバイスの BlackBerry Dynamics アプリの派生スマート認証情報を使用できます。

作業を始める前に： 所属組織の Entrust 管理者に連絡して、次の情報を取得します。

- Entrust IdentityGuard サーバーの URL
- Entrust IdentityGuard で指定されている、デバイスでアクティブ化されるスマート認証情報の名前
- デバイスに証明書を送信するための Entrust の CA 証明書

1. 管理コンソールのメニューバーで、［設定］ > ［外部統合］ > ［認証局］の順にクリックします。
2. ［外部統合］ > ［認証局］の順にクリックします。
3. ［**Entrust** スマート認証情報の接続を追加］をクリックします。
4. ［スマート認証情報名］フィールドに、Entrust IdentityGuard で指定したスマート認証情報の名前を入力します。
5. ［**Entrust URL**］フィールドに、Entrust IdentityGuard サーバーの URL を入力します。
6. ［追加］をクリックします。

終了したら：

- CA 証明書プロファイルの作成 Entrust の CA 証明書をデバイスに送信し、ユーザー資格情報プロファイルが割り当てられる同じユーザーまたはグループにプロファイルを割り当てます。
- デバイスで Entrust スマート認証情報を使用するためのユーザー資格情報プロファイルの作成。

BlackBerry UEM と組織の OpenTrust ソフトウェアを接続する

デバイスへの OpenTrust 証明書ベースの認証を拡張するには、組織の OpenTrust ソフトウェアへの接続を追加する必要があります。BlackBerry UEM は、OpenTrust PKI 4.8.0 以降と OpenTrust CMS 2.0.4 以降との統合をサポートします。この接続は BlackBerry Dynamics アプリではサポートされていません。

作業を始める前に： OpenTrust サーバーの URL、秘密鍵（.pfx または .p12 フォーマット）を含むクライアント側の証明書、および証明書のパスワードを取得するには、組織の OpenTrust 管理者にお問い合わせください。

1. メニューバーで、［設定］ > ［外部統合］ > ［認証局］の順にクリックします。
2. ［**OpenTrust** 接続を追加する］をクリックします。
3. ［接続名］フィールドに、接続の名前を入力します。
4. ［**URL**］ フィールドに、OpenTrust ソフトウェアの URL を入力します。
5. ［参照］をクリックします。OpenTrust サーバーへの接続を認証するために BlackBerry UEM で使用できるクライアント側の証明書に移動して選択します。
6. ［証明書のパスワード］フィールドに、OpenTrust サーバー証明書のパスワードを入力します。
7. 接続をテストするには、［テスト接続］をクリックします。
8. ［保存］をクリックします。

終了したら：

- ユーザー資格情報プロファイルを作成して、PKI ソフトウェアからデバイスに証明書を送信します。
- デバイスに証明書を配布するために OpenTrust ソフトウェアの UEM 接続を使用する場合、証明書が有効になるまで短い遅延が発生することがあります。この遅延が原因で、デバイスのアクティベーションプロセス中に、メール認証の問題が発生する可能性があります。この問題を解決するには、OpenTrust ソフトウェアで OpenTrust CA を設定し、［証明書のバックデート（秒）］を「180」に設定します。

BlackBerry UEM から BlackBerry Dynamics PKI コネクターへの接続

組織の PKI ソフトウェアを使用して BlackBerry Dynamics アプリの証明書を登録したい場合に、PKI ソフトウェアが BlackBerry UEM との直接接続をサポートしていなければ、BlackBerry Dynamics PKI コネクターが CA と通信して UEM を PKI コネクターにリンクするように設定することができます。BlackBerry UEM Cloud 環境では、UEM が BlackBerry Cloud Connector 経由で PKI コネクターと通信できるように、BlackBerry Connectivity Node をインストールする必要があります。

BlackBerry Dynamics PKI コネクタの設定の詳細については、『ユーザー証明書管理プロトコルおよび PKI コネクタ』マニュアルを参照してください。

作業を始める前に： BlackBerry Dynamics PKI コネクターを設定します。

1. 管理コンソールのメニューバーで、［設定］ > ［外部統合］ > ［認証局］の順にクリックします。
2. ［**BlackBerry Dynamics PKI** 接続を追加］をクリックします。
3. ［接続名］フィールドに、接続の名前を入力します。
4. ［**URL**］フィールドに、PKI コネクターの URL を入力します。
5. 次のオプションのいずれかを選択します。
   - ［ユーザー名とパスワードで認証する］：UEM がパスワードベースの認証を使用して BlackBerry Dynamics PKI コネクターで認証する場合は、このオプションを選択します。
   - ［クライアント証明書で認証する］：UEM が証明書ベースの認証を使用して BlackBerry Dynamics PKI コネクターで認証する場合は、このオプションを選択します。
6. ［ユーザー名とパスワードで認証する］を選択した場合は、［ユーザー名］フィールドと［パスワード］フィールドに、BlackBerry Dynamics PKI コネクターのユーザー名とパスワードを入力します。
7. ［クライアント証明書で認証する］を選択した場合は、［参照］をクリックして、BlackBerry Dynamics PKI コネクターが信頼する証明書を選択し、アップロードします。［クライアント証明書のパスワード］フィールドに、証明書のパスワードを入力します。
8. ［**PKI** コネクターの信頼済み証明書］セクションで、PKI コネクターへの信頼できる接続に UEM が使用する証明書を指定できます。次のいずれかのオプションを選択します。
   - **BlackBerry Control TrustStore** の **CA** 証明書
   - **CA** 証明書：このオプションを選択した場合は、［参照］をクリックし、組織の CA 証明書に移動して選択します。
   - **PKI Connector Server** 証明書：このオプションを選択した場合は、［参照］をクリックし、組織の PKI Connector Server 証明書に移動して選択します。
9. 接続をテストするには、［テスト接続］をクリックします。
10. ［保存］をクリックします。

終了したら： ユーザー資格情報プロファイルを作成して、PKI ソフトウェアからデバイスに証明書を送信します。

組織のアプリベース PKI ソリューションへの BlackBerry UEM の接続

Purebred などのアプリベースの PKI ソリューションには、CA と通信して証明書を登録し、デバイスに証明書を追加する、デバイスにインストールされたアプリなどがあります。アプリベースの PKI ソリューションを使用して、BlackBerry Dynamics アプリで使用する証明書を生成できます。

アプリベースの PKI ソリューションを iOS デバイスで使用するには、BlackBerry UEM と PKI プロバイダーとの間に接続を追加する必要があります。Android デバイスだけでアプリベースの PKI ソリューションを使用する場合はこのタスクは必要ありません。

CA から証明書を取得する PKI アプリが BlackBerry Dynamics アプリではない場合、BlackBerry UEM Client は PKI アプリと通信して証明書を取得し、その証明書を BlackBerry Dynamics アプリに提供します。

作業を始める前に： BlackBerry Dynamics アプリで使用するための証明書を取得するアプリが、UEM のアプリリストにあることを確認します。

1. 管理コンソールのメニューバーで、［設定］ > ［外部統合］ > ［認証局］の順にクリックします。
2. ［デバイスベースの証明書の接続を追加］をクリックします。
3. BlackBerry Dynamics アプリで使用するために PKI アプリから証明書を取得するアプリを選択します。Purebred を使用するには、UEM Client を選択します。
4. ［追加］をクリックします。

終了したら： 次の操作のいずれかを実行します。

- アプリベース証明書用のユーザー資格情報プロファイルを作成します。
- iOS デバイスでアプリベースの証明書を使用するためのユーザー資格情報プロファイルの作成。
- ユーザー資格情報プロファイルを作成して、ネイティブキーストアから証明書を使用する。

デバイスおよびアプリへのクライアント証明書の提供

クライアント証明書はいくつかの方法でデバイスとアプリへ送信できます。

証明書の追加	説明	サポートされるデバイス
デバイスのアクティベーション中	アクティベーションプロセス中に BlackBerry UEM が証明書をデバイスに送信します。デバイスはこれらの証明書を使用してデバイスと UEM の間にセキュリティ保護された接続を確立します。	すべて
SCEP プロファイル	デバイスが SCEP サービスを使用して組織の CA に接続し、この CA からクライアント証明書を取得するための SCEP プロファイルを作成できます。デバイスと BlackBerry Dynamics アプリは、これらの証明書を、証明書ベースの認証や、仕事用 Wi-Fi ネットワーク、仕事用 VPN、仕事用メールサーバーへの接続に使用できます。	iOS macOS Android Windows 10
組織の PKI ソリューションへの接続	組織で Entrust、OpenTrust ソフトウェア製品など、PKI ソリューションを使用して証明書を発行および管理している場合は、デバイスが組織の CA からクライアント証明書を取得する際に使用できるユーザー資格情報プロファイルを作成できます。BlackBerry Dynamics 対応のデバイスは、BlackBerry Dynamics アプリからの証明書ベース認証のために、これらの証明書を使用します。その他のデバイスは、これらの証明書を、ブラウザーからの証明書ベースの認証や、仕事用 Wi-Fi ネットワーク、仕事用 VPN、仕事用メールサーバーへの接続に使用します。	iOS macOS （BlackBerry Access 専用） Android Windows 10 （BlackBerry Access 専用）

証明書の追加	説明	サポートされるデバイス
共有証明書プロファイル	共有証明書プロファイルは、UEM が iOS、macOS、および Android デバイスに送信するクライアント証明書を指定します。UEM は、プロファイルが割り当てられている各ユーザーに同一のクライアント証明書を送信します。 管理者は、共有証明書プロファイルを作成するために、証明書と秘密鍵にアクセスする必要があります。	iOS macOS Android
クライアント証明書の個々のユーザーアカウントへの送信	ユーザーアカウントにクライアント証明書を追加できます。UEM は、証明書をユーザーの iOS および Android デバイスに送信できます。 証明書がユーザー資格情報プロファイルに関連付けられている場合、デバイスはこれらの証明書を使用して、仕事用 Wi-Fi ネットワーク、仕事用 VPN、および仕事用メールサーバーに接続できます。 管理者は、クライアント証明書をユーザーに送信するために、証明書と秘密鍵にアクセスする必要があります。	iOS Android
ユーザーによる UEM Self-Service へのアップロード	組織にオンプレミス UEM 環境がある場合、ユーザーは BlackBerry UEM Self-Service に証明書をアップロードできます。次に UEM は証明書をユーザーデバイスにプッシュします。 証明書がユーザー資格情報プロファイルに関連付けられている場合、デバイスと BlackBerry Dynamics アプリは、これらの証明書を証明書ベースの認証に使用して、仕事用 Wi-Fi ネットワーク、仕事用 VPN、および仕事用メールサーバーに接続できます。 この機能は UEM Cloud ではサポートされていません。	iOS Android
ユーザーインポート	ユーザーは BlackBerry Dynamics アプリで使用するためにデバイスのネイティブキーストアに証明書を追加できます。	Android

プロファイルを使用したデバイスおよびアプリへの証明書の送信

次のプロファイルを使用して、証明書をデバイスおよびアプリに送信できます。

プロファイル	説明
CA 証明書	CA 証明書プロファイルは、クライアントと関連付けられた ID、または CA によって署名されたサーバー証明書を信頼するためにデバイスおよび BlackBerry Dynamics アプリが利用できる CA 証明書を指定します。
ユーザー資格情報	ユーザー資格情報プロファイルは、次の方法でデバイスに証明書を送信します。 • 組織の PKI ソフトウェアへの接続を指定して、クライアント証明書をデバイスおよび BlackBerry Dynamics アプリに送信する。 • BlackBerry UEM で証明書を手動でアップロードし、オンプレミス環境では、ユーザーが BlackBerry UEM Self-Service を使用して証明書をアップロードできるようにする。 • Android デバイス上の BlackBerry Dynamics アプリと macOS および Windows 10 デバイス上の BlackBerry Access アプリが、デバイスのネイティブキーストアからの証明書を使用できるようにする。 • BlackBerry Dynamics アプリが、他のアプリベースの PKI ソリューション（Purebred など）から証明書をインポートできるようにする。
SCEP	SCEP プロファイルは、デバイスおよび BlackBerry Dynamics アプリが SCEP サービスを使用して組織の CA に接続し、この CA からクライアント証明書を取得する方法を指定します。
共有証明書	共有証明書プロファイルは、UEM が iOS および Android デバイスに送信するクライアント証明書を指定します。UEM は、プロファイルが割り当てられている各ユーザーに同一のクライアント証明書を送信します。

iOS および Android デバイスでは、証明書をユーザーアカウントに直接追加して、クライアント証明書をデバイスに送信することもできます。詳細については、「ユーザーアカウントへのクライアント証明書の追加および管理」を参照してください。

組織が S/MIME の証明書を使用している場合、iOS および Android デバイスでは、受信者の公開鍵を取得して証明書のステータスをチェックするように、プロファイルを使用してデバイスを設定することもできます。詳細については、「S/MIME を使用したメールセキュリティの強化」を参照してください。

BlackBerry Dynamics アプリの場合、プロファイルによって送信される証明書を使用するには、［アプリ］画面、［設定］ > ［**BlackBerry Dynamics**］で［ユーザー証明書、SCEP プロファイル、およびユーザー資格情報プロファイルの使用を BlackBerry Dynamics アプリに許可する］を選択する必要があります。

選択するプロファイルのタイプは、組織での証明書の使い方、およびその組織がサポートしているデバイスのタイプによって異なります。次のガイドラインを参考にしてください。

- SCEP プロファイルを使用するには、SCEP をサポートする CA を使用する必要があります。
- UEM と組織の PKI ソリューションの間で接続を設定した場合、ユーザー資格情報プロファイルを使用して証明書をデバイスに送信します。Entrust CA または OpenTrust CA に直接接続できます。また BlackBerry Dynamics PKI コネクターを使用して CA サーバーに接続し、BlackBerry Dynamics 対応デバイスの証明書を登録することもできます。
- BlackBerry Dynamics アプリで証明書を使用するには、ユーザー資格情報プロファイルを使用するか、個々のユーザーアカウントに証明書を追加する必要があります。

- 仕事用 Wi-Fi ネットワーク、仕事用 VPN、仕事用メールサーバーへの接続に使用する証明書を、ユーザーがアップロードできるようにするには、ユーザー資格情報プロファイルを使用します。
- Wi-Fi、VPN、およびメールサーバーの認証にクライアント証明書を使用するには、証明書プロファイルと Wi-Fi、VPN、またはメールプロファイルを関連付ける必要があります。
- Android Enterprise デバイスは、Wi-Fi 認証のために 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。
- 秘密鍵へのアクセスが必要になるため、ユーザーアカウントに追加されている共有証明書プロファイルおよび証明書で秘密鍵は秘密として保持されません。証明書の発行先デバイスのみに秘密鍵を送信するため、SCEP またはユーザー資格情報プロファイルを使用して CA に接続する方法は、安全性がより高くなります。

デバイスおよびアプリへの **CA** 証明書の送信

組織が S/MIME を使用している場合、またはデバイスや BlackBerry Dynamics アプリが証明書に基づく認証を使用して組織の環境内のネットワークまたはサーバーに接続している場合は、CA 証明書をデバイスに送信する必要が生じることがあります。

CA 証明書がデバイスに保存されると、デバイスとアプリは CA によって署名されたクライアント証明書またはサーバー証明書に関連付けられた ID を信頼します。組織のネットワーク証明書およびサーバー証明書に署名した CA の証明書がデバイスに保存されている場合、デバイスとアプリは、セキュリティ保護された接続を確立する際に、ネットワークとサーバーを信頼できます。組織の S/MIME 証明書に署名した CA 証明書がデバイスに保存されている場合、メールクライアントは、セキュリティ保護されたメールの受信時に送信者の証明書を信頼できます。

1 台のデバイスに、さまざまな目的で使用されている複数の CA 証明書を保存できます。CA 証明書プロファイルを使用すると、デバイスに CA 証明書を送信できます。

CA 証明書プロファイルの作成

作業を始める前に： PKI 管理者から CA 証明書ファイルを取得します。

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］ **>** ［証明書］ **>** ［**CA** 証明書］をクリックします。
2. ＋をクリックします。
3. プロファイルの名前と説明を入力します。各 CA 証明書プロファイルに固有の名前を付ける必要があります。いくつかの名前（たとえば、ca_1）は予約されています。
4. ［証明書ファイル］フィールドで、［参照］をクリックして証明書ファイルを見つけます。
5. CA 証明書が macOS デバイスに送信された場合、macOS タブの ［プロファイルを適用］ ドロップダウンリストで、［ユーザー］または［デバイス］を選択します。
6. ［追加］をクリックします。

終了したら： CA 証明書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ます。

ユーザー資格情報プロファイルを使用したデバイスおよびアプリへのクライアント証明書の送信

ユーザー資格情報プロファイルにより、デバイスは次の方法で取得されたクライアント証明書を使用できるようになります。

- 証明書を BlackBerry UEM 管理コンソールに手動でアップロードするか、オンプレミス環境で UEM にアップロードします。
- UEM と組織の Entrust CA または OpenTrust CA 間の確立された接続。
- Android デバイスの BlackBerry Dynamics アプリの場合、デバイスのネイティブのキーストアに保存された証明書。
- BlackBerry Dynamics アプリの場合、確立された BlackBerry Dynamics PKI コネクタ接続経由。
- BlackBerry Dynamics アプリの場合、Purebred のようなアプリベースの PKI ソリューションを使用

ユーザー資格情報プロファイルは、iOS および Android デバイスでサポートされます。アプリベースの PKI ソリューションは、iOS および Android デバイスの BlackBerry Dynamics アプリでサポートされています。証明書の手動アップロードは、iOS、Android Enterprise、および Samsung Knox Workspace でサポートされています。

代わりに、SCEP プロファイルを使用してデバイスにクライアント証明書を登録できます。また証明書をユーザーアカウントに直接アップロードすることもできます。選択するプロファイルのタイプは、所属組織による PKI ソフトウェアの使用方法、その組織がサポートしているデバイスのタイプ、および証明書の管理方法によって異なります。

手動で証明書をアップロードするためのユーザー資格情報プロファイルの作成

ユーザー資格情報プロファイルを使用すると、管理者またはユーザーは、ユーザーのデバイスに送信する証明書を手動でアップロードできます。

1. メニューバーで、［ポリシーとプロファイル］ > ［証明書］ > ［ユーザー資格情報］をクリックします。
2. ＋をクリックします。
3. プロファイルの名前と説明を入力します。各証明書プロファイルに固有の名前を付ける必要があります。
4. ［認証局との接続］ドロップダウンリストで、［手動でアップロードした証明書］を選択します。
5. Android Enterprise デバイスを管理している場合にユーザーが他の目的で証明書を使用することを選択できないようにするには、［**Android**］タブで［**Android Enterprise** デバイスの証明書を非表示］チェックボックスを選択します。
6. ［追加］をクリックします。

終了したら：

- デバイスがクライアント証明書を使用して、Wi-Fi ネットワーク、VPN、またはメールサーバーを認証する場合は、ユーザー資格情報プロファイルに Wi-Fi、VPN、またはメールプロファイルを関連付けます。
- 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。
- ユーザー資格情報プロファイルにクライアント証明書を追加するか、BlackBerry UEM Self-Service を使用して独自の証明書をアップロードするように指示します。

組織の **PKI** ソフトウェアに接続するためのユーザー資格情報プロファイルの作成

組織の PKI ソフトウェアに接続するユーザー資格情報プロファイルは、iOS および Android デバイスの証明書を登録できます。Entrust PKI ソフトウェアへの接続の場合、ユーザー資格情報プロファイルは BlackBerry Dynamics アプリの証明書を登録することもできます。

BlackBerry UEM は、BlackBerry Dynamics アプリに発行した証明書のキー履歴をサポートしていません。

作業を始める前に：

- 組織の Entrust または OpenTrust ソフトウェアに接続を設定します。
- 所属組織の Entrust または OpenTrust 管理者に問い合わせて、選択すべき PKI プロファイルを確認します。

- 提供する必要のあるプロファイル値については、Entrust または OpenTrust の管理者にお問い合わせください。
- 組織の OpenTrust システムが預託されたキーのみを返すように設定されている場合、OpenTrust 管理者は、OpenTrust システム内に各ユーザーの証明書が存在していることを確認する必要があります。UEM のユーザーにユーザー資格情報プロファイルを割り当てても、OpenTrust 内のユーザーに対して証明書が自動的に作成されることはありません。この場合、ユーザー資格情報プロファイルは、OpenTrust システム内で既存の証明書を持つユーザーにのみ証明書を配布できます。

1. メニューバーで、［ポリシーとプロファイル］ > ［証明書］ > ［ユーザー資格情報］をクリックします。
2. ＋をクリックします。
3. プロファイルの名前と説明を入力します。各証明書プロファイルに固有の名前を付ける必要があります。
4. ［認証局との接続］ドロップダウンリストで、設定した Entrust または OpenTrust 接続を選択します。
5. ［プロファイル］ドロップダウンリストで、適切なプロファイルをクリックします。
6. 目的のプロファイルの値を指定します。
7. 必要に応じて、Entrust クライアント証明書の SAN タイプおよび値を指定できます。
   a) ［SAN］表で、＋をクリックします。
   b) ［**SAN** の種類］ドロップダウンリストで、適切な種類をクリックします。
   c) ［**SAN** の値］フィールドに、SAN の値を入力します。

   SAN の種類を［RFC822 名］に設定した場合、値は有効なメールアドレスにする必要があります。［URI］に設定した場合、値はプロトコルと FQDN または IP アドレスを含む有効な URL にする必要があります。［NT プリンシパル名］に設定した場合、値は有効なプリンシパル名にする必要があります。［DNS 名］に設定した場合、値は有効な FQDN にする必要があります。
8. 証明書の［更新期間］を指定します。期間には 1～120 日を指定できます。
9. ［追加］をクリックします。

終了したら：

- デバイスがクライアント証明書を使用して、Wi-Fi ネットワーク、VPN、またはメールサーバーを認証する場合は、ユーザー資格情報プロファイルに Wi-Fi、VPN、またはメールプロファイルを関連付けます。
- 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。Android ユーザーには、画面に表示されるパスワードの入力を求めるプロンプトが表示されます。

デバイスで **Entrust** スマート認証情報を使用するためのユーザー資格情報プロファイルの作成

Entrust 派生したスマート認証情報は、次のアプリでサポートされています。

- iOS デバイス上の BlackBerry Dynamics アプリ
- Samsung Knox Workspace デバイス以外の Android デバイス上の BlackBerry Dynamics アプリ
- BlackBerry Hub やサポート対象の Web ブラウザーなど、署名、暗号化、および ID の認証に証明書を使用する Android Enterprise デバイスのアプリ
- Samsung ネイティブのメールクライアントやサポート対象の Web ブラウザーなど、署名、暗号化、および ID の認証に証明書を使用する Samsung Knox Workspace デバイスのアプリ

BlackBerry UEM は、派生したスマート認証情報のキー履歴をサポートしていません。

作業を始める前に：

- BlackBerry UEM を組織の Entrust IdentityGuard サーバーに接続したスマート認証情報の使用。
- CA 証明書プロファイルの作成 Entrust の CA 証明書をデバイスに送信し、このユーザー資格情報プロファイルが割り当てられる同じユーザーまたはグループにプロファイルを割り当てます。

1. メニューバーで、［ポリシーとプロファイル］ > ［証明書］ > ［ユーザー資格情報］をクリックします。
2. ＋をクリックします。
3. プロファイルの名前と説明を入力します。
4. ［認証局との接続］ドロップダウンリストで、設定した Entrust スマート認証情報の接続を選択します。
5. ［証明書の種類］ドロップダウンリストで、ID の認証、署名、または暗号化にスマート認証情報を使用するかどうかを指定します。

   複数の目的でアプリにスマート認証情報を送信する場合は、追加のユーザー資格情報プロファイルを作成します。
6. スマート認証情報が、Samsung Knox Workspace デバイスに送信される場合、または Android Enterprise デバイスの BlackBerry Dynamics アプリ以外のアプリに送信される場合は、［**Android**］タブをクリックして［ネイティブキーチェーンに配信］チェックボックスを選択します。

   この設定が選択されていない場合は、スマート認証情報は BlackBerry Dynamics アプリでのみ使用できます。
7. スマート認証情報が BlackBerry Dynamics アプリに送信される場合、［**BlackBerry Dynamics**］タブで、次の操作を実行します。
   a) ユーザーが証明書の登録を最初に行わず、後で完了できるようにするには、［オプションの証明書登録を許可する］を選択します。iOS および Android デバイスの場合、オプションの証明書登録は、特定のユーザー資格情報プロファイルタイプでサポートされます。サポート対象のタイプは、デバイス（アプリ）ベースプロバイダー、Entrust スマート資格情報、およびネイティブキーストアです。
   b) 重複した認証情報をデバイスで削除させる場合は、［重複した証明書を削除する］を選択します。デバイスは、開始日が最も早い認証情報を削除します。
   c) 有効期限が切れた認証情報をデバイスで削除するには、［有効期限が切れた証明書を削除する］を選択します。
   d) スマート認証情報の使用をすべての BlackBerry Dynamics アプリに許可するには、［証明書の使用をすべてのアプリに許可する］を選択します。
   e) スマート認証情報を使用する BlackBerry Dynamics アプリを指定するには、［証明書の使用を指定のアプリに許可する］を選択し、＋をクリックしてアプリを指定します。アプリのリストに BlackBerry UEM Client を含める必要があります。
8. ［追加］をクリックします。

終了したら：

- 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。
- デバイスがプロファイルを受信した後、ユーザーは Entrust IdentityGuard Self-Service Module にログインしてスマート認証情報を有効にし、UEM Client を使用して Entrust IdentityGuard Self-Service Module で示された QR コードをスキャンし、デバイスにスマート認証情報を追加する必要があります。
- Entrust スマート認証情報をデバイスから削除するには、プロファイルを割り当て解除するか、証明書を削除する前に、ユーザーが UEM Client でスマート認証情報を無効化する必要があります。

ユーザー資格情報プロファイルを作成して、ネイティブキーストアから証明書を使用する

次の状況で、ネイティブキーストアからの証明書を使用するようにユーザー資格情報プロファイルを設定できます。

- BlackBerry Dynamics アプリが Android デバイス上のネイティブキーストアからの証明書を使用できるようにする。
- BlackBerry Dynamics アプリがネイティブキーストアからの証明書を使用して、iOS デバイス上の PKI アプリから暗号化トークンにアクセスできるようにする。

- BlackBerry Access アプリが macOS または Windows 10 デバイス上のネイティブキーストアからの証明書を使用できるようにする。

キーストアに追加された任意の証明書をアプリで使用することも、アプリが選択できる証明書の制限を定義することもできます。たとえば、ネイティブキーストアに証明書を追加する Purebred など、アプリベースの PKI ソリューションを使用している場合は、Purebred PKI ソリューションによって発行された証明書をアプリに強制的に選択させ、アプリが指定された機能を持つ証明書を使用するように要求できます。

メモ：「ネイティブキーストア」とは、デバイス上のキーストアを指します。証明書の検出を開始する前に、ネイティブキーストアコネクターがあるすべてのユーザー資格情報プロファイルをユーザーに割り当てる必要があります。証明書が複数の UCP 要件を満たしている場合は、最適な一致が選択されます。

1. メニューバーで、［ポリシーとプロファイル］ > ［証明書］ > ［ユーザー資格情報］をクリックします。
2. ＋をクリックします。
3. プロファイルの名前と説明を入力します。各証明書プロファイルに固有の名前を付ける必要があります。
4. ［認証局との接続］ドロップダウンリストで、［ネイティブキーストア］を選択します。
5. ［サポートされるプラットフォーム］セクションで、このプロファイルでサポートするデバイス OS タイプを選択します。
6. Android ユーザーが証明書の登録を最初に行わず、後で完了できるようにするには、［証明書登録］セクションで［オプションの証明書登録を許可する］チェックボックスを選択します。
7. BlackBerry Dynamics アプリが使用する証明書を指定するには、次の操作を実行します。
   a) ［発行元］の横で、＋をクリックし、発行元名を入力します。

      BlackBerry Dynamics アプリは、指定された発行元が証明書で OpenSSL の短い形式の OID と一致する場合にのみ、証明書を使用します。この値は、発行元の証明書からコピーすることができます。等号（=）の前後にスペースを入れないでください。例：

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

   b) ［キー使用法］セクションで、証明書がサポートしている操作を選択します。

      BlackBerry Dynamics アプリは、少なくとも指定されたキー使用値が含まれている証明書のみを使用します。たとえば、暗号化証明書には、キー暗号化のキー使用値が含まれている場合があります。認証証明書には、デジタル署名のキー使用値が含まれている場合があります。署名証明書には、デジタル署名と否認防止の両方のキー使用値が含まれている場合があります。
   c) ［拡張キー使用法］セクションで、証明書が発行される対象の機能を選択します。

      BlackBerry Dynamics アプリは、選択したすべての拡張キー使用値が証明書に存在する場合にのみ、証明書を使用します。証明書には、追加の拡張キー使用値を含められます。
   d) メール、クライアント認証、スマートカードログイン以外の目的で証明書が発行された場合は、［追加オブジェクト **ID** の使用法］を選択し、＋をクリックして、キー使用法の OID を指定します。たとえば、証明書がサーバー認証に使用される場合、OID 1.3.6.1.5.5.7.3.1 がある可能性があります。
8. 有効期限が切れた証明書をデバイスで削除するには、［有効期限が切れた証明書を削除する］を選択します。
9. 重複した証明書をデバイスで削除するには、［重複した証明書を削除する］チェックボックスを選択します。
10. ［追加］をクリックします。

終了したら：

- BlackBerry Dynamics アプリで証明書を使用できるようにするには、メニューバーで［アプリ］をクリックします。変更する BlackBerry Dynamics アプリをクリックし、［設定］ > ［**BlackBerry Dynamics**］タブで、［**BlackBerry Dynamics** アプリで、ユーザー証明書、**SCEP** プロファイル、およびユーザー資格情報プロファイルを使用できるようにする］チェックボックスをオンにします。
- 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 Dynamics PKI コネクターに接続するためのユーザー資格情報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］ > ［証明書］ > ［ユーザー資格情報］をクリックします。
2. ＋をクリックします。
3. プロファイルの名前と説明を入力します。
4. ［認証局との接続］ドロップダウンリストで、設定した BlackBerry Dynamics PKI 接続をクリックします。
5. 証明書の要求時にユーザーにパスワードの入力を求める場合は、［ユーザー入力のパスワードまたは **OTP** を要求する］を選択します。
6. 現在の証明書が期限切れになる前に、新しい証明書をデバイスに自動的に要求させる場合は、［証明書の更新を有効にする］を選択し、新しい証明書をデバイスが要求するまでの期間を日数で指定します。
7. 有効期限が切れた証明書をデバイスで削除するには、［有効期限が切れた証明書を削除する］チェックボックスを選択します。
8. 重複した証明書をデバイスで削除するには、［重複した証明書を削除する］チェックボックスを選択します。
9. ［追加］をクリックします。

終了したら：

- BlackBerry Dynamics アプリで証明書を使用できるようにするには、メニューバーで［アプリ］をクリックします。BlackBerry Dynamics 変更するアプリをクリックし、［設定］ > ［**BlackBerry Dynamics**］タブで、［**BlackBerry Dynamics** アプリで、ユーザー証明書、**SCEP** プロファイル、およびユーザー資格情報プロファイルを使用できるようにする］チェックボックスをオンにします。
- 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。
- PKI コネクターを更新する場合は、［**PKI** 機能を更新］をクリックして、プロファイル用にサポートされている PKI 機能を更新します。
- PKI コネクター経由で登録されている証明書を更新する場合は、［**PKI** 機能を更新］ > ［更新］をクリックして、証明書の更新を要求するプロファイルが割り当てられているすべての BlackBerry Dynamics 対応デバイスにコマンドを実行します。

アプリベース証明書用のユーザー資格情報プロファイルの作成

Purebred などのアプリベースの PKI ソリューションには、CA と通信して証明書を登録し、デバイスに証明書を追加する、デバイスにインストールされたアプリなどがあります。アプリベースの PKI ソリューションを使用して、BlackBerry Dynamics アプリで使用する証明書を生成できます。

アプリベースの PKI ソリューションを iOS デバイスで使用するには、BlackBerry UEM と PKI プロバイダーとの間に接続を追加する必要があります。Android デバイスでアプリベースの PKI ソリューションを使用する場合はこのタスクは必要ありません。

CA から証明書を取得する PKI アプリが BlackBerry Dynamics アプリではない場合、BlackBerry UEM Client は PKI アプリと通信して証明書を取得し、その証明書を BlackBerry Dynamics アプリに提供します。

この方法を使用するデバイスに複数の証明書を送信する場合は、異なる種類の証明書を使用して各プロファイルに、複数のユーザー資格情報プロファイルを設定することを推奨します。複数の証明書に単一のプロファイルを

使用している場合、証明書が見つからないときに、その識別ができなくなります。たとえば、プロファイルに暗号証明書、署名証明書、認証証明書が個別に含まれていて、署名証明書と認証証明書だけがインポートされている場合、暗号化証明書がない場合でもインポートが成功したとデバイスに表示されます。しかし、3 つのユーザー資格情報プロファイルを個別に設定している場合に暗号化証明書が見つからないときは、問題は明らかにわかります。

組織のアプリベース PKI ソリューションを使用するための手順の一部は、iOS デバイスでソリューションを使用する場合にのみ必要です。

手順	アクション
1	アプリベース PKI ソリューションを iOS デバイスで使用するには、BlackBerry Dynamics プロファイルで、［**BlackBerry Dynamics** に登録する **UEM** クライアントを有効にする］を選択し、UEM Client に［アプリ認証委任］を指定します。
2	アプリベース PKI ソリューションを iOS デバイスで使用するには、BlackBerry UEM を組織のアプリベース PKI ソリューションに接続します。
3	PKI アプリが BlackBerry Dynamics アプリでない場合、アプリベース PKI ソリューションを iOS デバイスで使用するには、アプリベースの証明書をサポートするように BlackBerry UEM Client を設定します。
4	アプリベースの証明書を使用するために BlackBerry Dynamics アプリを設定します。
5	PKI アプリ（例：Purebred）がユーザーのデバイスにインストールされていることを確認します。
6	アプリベースの PKI ソリューションは、次のデバイスで使用します。 • iOS デバイス：アプリベースの証明書を使用するためにユーザー資格情報プロファイルを作成します。 • Android デバイス：ユーザー資格情報プロファイルを作成して、ネイティブキーストアから証明書を使用します。

アプリベースの証明書をサポートするための **BlackBerry UEM Client** の設定

このタスクは、組織のアプリベースの PKI ソリューションを iOS デバイスで使用し、PKI アプリが BlackBerry Dynamics アプリではない場合にのみ必要です。

作業を始める前に：アプリベースの証明書をサポートするための BlackBerry UEM Client の設定。

1. UEM 管理コンソールのメニューバーで、［アプリ］をクリックします。
2. アプリリストで BlackBerry UEM Client を選択します。
3. ［アプリ設定］セクションで をクリックします。
4. ［アプリ名］フィールドに、アプリの名前を入力します。
5. ［**UTI** スキーム］フィールドで、組織のアプリベースの PKI ソリューションの UTI スキームを指定します。たとえば、Purebred アプリを使用している場合は、スキーム `purebred.select.all-user`、`purebred.select.no-filter`、`purebred.zip.all-user`、`purebred.zip.no-filter` を使用します。

6. ［保存］をクリックします。

終了したら： 作成したアプリ設定を含む UEM Client を、アプリベースの PKI ソリューションを使用させるユーザーおよびデバイスに割り当てます。

アプリベースの証明書を使用するための **BlackBerry Dynamics** アプリの設定

BlackBerry Dynamics アプリは、証明書のキー使用法プロパティと拡張キー使用法プロパティに基づいて、S/MIME に使用する証明書と TLS 接続経由の認証に使用する証明書を自動的に選択します。同じ証明書のプロパティセットが 2 つ以上あると、アプリが TLS 認証に使用する証明書を解決できない場合があります。以下の手順に従って、アプリが使用する証明書を決定できます。

作業を始める前に： 次のいずれかを完了していることを確認します。

- 環境で、アプリベース PKI ソリューションを iOS デバイスで使用する場合、BlackBerry UEM を組織のアプリベース PKI ソリューションに接続します。
- 環境で、アプリベース PKI ソリューションを iOS デバイスで使用し、PKI アプリが BlackBerry Dynamics ではない場合は、アプリベースの証明書をサポートするように BlackBerry UEM Client を設定します。

1. UEM 管理コンソールのメニューバーで、［アプリ］をクリックします。
2. アプリリストで、アプリを選択します（BlackBerry Work や BlackBerry Access など）。
3. ［**BlackBerry Dynamics** アプリで、ユーザー証明書、**SCEP** プロファイル、およびユーザー資格情報プロファイルを使用できるようにする］チェックボックスを選択します。
4. BlackBerry Work を設定している場合、［アプリの設定］セクションで をクリックし、次のいずれかのタスクを実行します。

タスク	手順
組織で BEMS を使用しているときに BlackBerry Work を設定する	a. ［基本設定］タブの［セキュリティ設定］セクションで、［ログイン/パスワードの代わりにクライアント証明書を使用する］チェックボックスをオンにします。 b. ユーザーが使用している Microsoft Exchange サーバーの自動検出を有効にするには、［クライアント設定］セクションで、［**BEMS** を使用してユーザーの **EAS/EWS** の自動検出を実行する］チェックボックスを選択します。 c. ［詳細設定］タブの［**TLS** 証明書の設定］セクションで、デバイスのユーザー資格情報プロファイルの名前を入力します。

タスク	手順
組織で BEMS を使用していないときに BlackBerry Work を設定する	**a.** ［基本設定］タブをクリックします。 **b.** サーバーで、ドメイン名\ユーザーのログイン形式が使用されている場合は、［**Exchange ActiveSync** 設定］セクションの［デフォルトドメイン］フィールドで、ユーザーのログイン時に BlackBerry Work がデフォルトで接続する Windows NT ドメインを指定します。 **c.** ［**Active Sync** サーバー］フィールドで、ユーザーが BlackBerry Work にログインするときに BlackBerry Work が接続するデフォルトの Exchange ActiveSync サーバーを指定します（cas.mydomain.com など）。 **d.** わかっている場合は、［自動検出 **URL**］フィールドに自動検出 URL を指定します。これにより、自動検出セットアッププロセス（https://autodiscover.mydomain.com など）が高速になります。 **e.** ［秒単位の自動検出接続タイムアウト（**iOS** のみ）］フィールドで、自動検出接続のタイムアウトを秒単位で指定します。 **f.** ［**TLS** 証明書設定］セクションの、［ユーザー資格情報プロファイル名］フィールドに、ユーザー資格情報プロファイルの名前を入力します。

5. ［保存］をクリックします。

終了したら： アプリベースの PKI ソリューションを作成して、次のデバイスで使用します。

- iOS デバイス：アプリベースの証明書を使用するためにユーザー資格情報プロファイルを作成します。
- Android デバイス：ユーザー資格情報プロファイルを作成して、ネイティブキーストアから証明書を使用します。

iOS デバイスでアプリベースの証明書を使用するためのユーザー資格情報プロファイルの作成

作業を始める前に：

- アプリベースの証明書をサポートするための BlackBerry UEM Client の設定。
- PKI アプリ（例：Purebred）がユーザーのデバイスにインストールされていることを確認します。

1. メニューバーで、［ポリシーとプロファイル］ > ［証明書］ > ［ユーザー資格情報］をクリックします。
2. ＋をクリックします。
3. プロファイルの名前と説明を入力します。
4. ［認証局との接続］ドロップダウンリストで、BlackBerry UEM を PKI ソリューションに接続したときに指定したアプリの名前をクリックします。Purebred を使用している場合は、BlackBerry UEM Client を選択します。
5. BlackBerry Dynamics アプリが使用する証明書を指定するには、次の操作を実行します。
   a) ［キー使用法］セクションで、証明書がサポートしている操作を選択します。

      BlackBerry Dynamics アプリは、少なくとも指定されたキー使用値が含まれている証明書のみを使用します。たとえば、暗号化証明書には、キー暗号化のキー使用値が含まれている場合があります。認証証明書には、デジタル署名のキー使用値が含まれている場合があります。署名証明書には、デジタル署名と否認防止の両方のキー使用値が含まれている場合があります。
   b) ［拡張キー使用法］セクションで、証明書が発行される対象の機能を選択します。

      BlackBerry Dynamics アプリは、選択したすべての拡張キー使用値が証明書に存在する場合にのみ、証明書を使用します。証明書には、追加の拡張キー使用値を含められます。

c) メール、クライアント認証、スマートカードログイン以外の目的で証明書が発行された場合は、［追加オブジェクト **ID** の使用法］を選択し、＋をクリックして、キー使用法の OID を指定します。たとえば、証明書がサーバー認証に使用される場合、OID 1.3.6.1.5.5.7.3.1 がある可能性があります。

d) ［発行元］の横で、＋をクリックし、発行元名を入力します。

BlackBerry Dynamics アプリは、指定された発行元が証明書で OpenSSL の短い形式の OID と一致する場合にのみ、証明書を使用します。この値は、発行元の証明書からコピーすることができます。等号（=）の前後にスペースを入れないでください。例：

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

6. 有効期限が切れた証明書をデバイスで削除するには、［有効期限が切れた証明書を削除する］を選択します。
7. 重複した証明書をデバイスで削除するには、［重複した証明書を削除する］を選択します。
8. ［追加］をクリックします。

終了したら：

- BlackBerry Dynamics アプリで証明書を使用できるようにするには、メニューバーで［アプリ］をクリックします。BlackBerry Dynamics 変更するアプリをクリックし、［設定］ > ［**BlackBerry Dynamics**］タブで、［**BlackBerry Dynamics** アプリで、ユーザー証明書、**SCEP** プロファイル、およびユーザー資格情報プロファイルを使用できるようにする］チェックボックスをオンにします。
- 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。

SCEP を使用したデバイスおよびアプリへのクライアント証明書の送信

SCEP プロファイルを使用して、デバイスや BlackBerry Dynamics アプリが、SCEP サービスを通じて組織の CA からクライアント証明書を取得する方法を指定できます。SCEP は、各証明書の発行で管理者による入力や承認を要求することなく、多数のデバイスまたはアプリにクライアント証明書を登録するプロセスを簡略化する IETF プロトコルです。デバイスや BlackBerry Dynamics アプリは SCEP を使用して、組織で使用されている SCEP 準拠の CA に対してクライアント証明書を要求し、取得できます。

使用する CA は、チャレンジパスワードをサポートする必要があります。CA はチャレンジパスワードを使用して、証明書要求を送信する権限がデバイスまたはアプリにあることを確認します。

SCEP を BlackBerry UEM Cloud 環境で使用するには、BlackBerry Connectivity Node の最新バージョンをインストールして、UEM Cloud が会社のディレクトリにアクセスできるようにする必要があります。

組織で Entrust CA または OpenTrust CA を使用している場合、SCEP プロファイルは Windows 10 デバイスでサポートされません。

SCEP プロファイルの作成

必要なプロファイル設定は、組織の環境の SCEP サービス設定によって異なり、証明書が BlackBerry Dynamics アプリで使用されているか、または指定されたデバイスタイプで使用されているかによっても異なります。

実際の値を指定するのではなく、テキストフィールドに変数を使用して値を参照することができます。

メモ：SCEP プロファイルを使用して OpenTrust クライアント証明書をデバイスに配布する場合は、OpenTrust ソフトウェアにホットフィックスを適用する必要があります。詳細については、OpenTrust サポート担当者にお問い合わせ頂き、サポートケース「SUPPORT-798」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］ > ［証明書］ > ［**SCEP**］をクリックします。

2. ＋をクリックします。
3. プロファイルの名前と説明を入力します。
4. ［認証局との接続］ドロップダウンリストで、次の操作のいずれかを実行します。
   - 設定した Entrust 接続を使用するには、適切な接続をクリックします。［プロファイル］ドロップダウンリストで、特定のプロファイルをクリックします。目的のプロファイルの値を指定します。
   - 設定した OpenTrust 接続を使用するには、適切な接続をクリックします。［プロファイル］ドロップダウンリストで、特定のプロファイルをクリックします。目的のプロファイルの値を指定します。SCEP プロファイル内の鍵の使用量、鍵の使用量の拡張、サブジェクト、および SAN の各設定は OpenTrust クライアント証明書には適用されないことに注意してください。
   - ［汎用］をクリックして、別の CA を使用します。［**SCEP** チャレンジの種類］ドロップダウンリストで、［静的］または［動的］を選択してから、チャレンジの種類の必須設定を指定します。

     メモ：Windows デバイスでは、「静的」パスワードのみがサポートされています。
5. ［**URL**］ フィールドに、SCEP サービスの URL を入力します。URL には、プロトコル、FQDN、ポート番号、SCEP パスを含める必要があります。
6. ［インスタンス名］フィールドに CA のインスタンス名を入力します。
7. オプションで、プロファイルを設定しないデバイスタイプのチェックボックスをオフにします。
8. 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 SCEP サービス設定に一致する適切な値を設定します。以下を参照してください。
      - 共通：SCEP プロファイル設定
      - iOS ：SCEP プロファイル設定
      - macOS ：SCEP プロファイル設定
      - Android ：SCEP プロファイル設定
      - Windows 10 ：SCEP プロファイル設定
      - BlackBerry Dynamics ：SCEP プロファイル設定
9. 組織内のデバイスタイプごとに手順 8 を繰り返します。
10. ［追加］をクリックします。

終了したら： デバイスがクライアント証明書を使用して仕事用 Wi-Fi ネットワーク、仕事用 VPN、または仕事用メールサーバーを認証する場合は、SCEP プロファイルに Wi-Fi、VPN、またはメールプロファイルを関連付けます。

共通：**SCEP** プロファイル設定

共通：**SCEP** プロファイル設定	説明
認証局との接続	この設定では、CA が Entrust、OpenTrust、または別の CA であるかどうかを指定します。

共通：**SCEP** プロファイル設定	説明
URL	この設定では、SCEP サービスの URL を指定します。URL には、プロトコル、FQDN、ポート番号、および SCEP パス（SCEP 仕様で定義される CGI パス）を含める必要があります。デバイスを正常にアクティブ化するには、この設定に値を指定する必要があります。 SCEP HTTPS URL は iOS デバイスでサポートされています。
インスタンス名	この設定では、CA インスタンスの名前を指定します。 値には、SCEP サービスが理解できる任意の文字列を指定できます。たとえば、example.org などのドメイン名を指定できます。CA が複数の CA 証明書を保持している場合、このフィールドを使用して、必要な証明書を区別できます。
SCEP サーバー接続トラストチェーンの確認	この設定は、SCEP サーバーのルート CA が BlackBerry UEM 証明書ストアに保存されていることを UEM が確認するかどうかを指定します。このルート CA により、接続をテストする際、チャレンジパスワードの取得を実行する際、およびデバイスからの SCEP 要求のプロキシとして機能する際に、UEM が SCEP サーバーを信頼できるようになります。
SCEP チャレンジの種類	この設定では、SCEP チャレンジパスワードを動的に生成するか、または静的パスワードとして提供するかどうかを指定します。これを［静的］に設定すると、すべてのデバイスが同一のチャレンジパスワードを使用します。 Windows デバイスでは、「静的」パスワードのみがサポートされています。
チャレンジパスワード生成 URL	この設定では、デバイスが動的に生成されたチャレンジパスワードを SCEP サービスから取得するために使用する URL を指定します。URL には、プロトコル、ドメイン、ポート、および SCEP パス（SCEP 仕様で定義される CGI パス）を含める必要があります。 この設定は、［SCEP チャレンジの種類］が［動的］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 SCEP サービスに接続し、チャレンジパスワードを取得するために使用する認証の種類を指定します。 この設定は、［SCEP チャレンジの種類］が［動的］に設定されている場合のみ有効です。
ドメイン	この設定では、デバイスが SCEP サービスに接続し、チャレンジパスワードを取得するときに、NTLM 認証に使用されるドメインを指定します。 この設定は、［認証の種類］が［NTLM］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、SCEP サービスからチャレンジパスワードを取得するために必要なユーザー名を指定します。 この設定は、［SCEP チャレンジの種類］が［動的］に設定されている場合のみ有効です。

共通：**SCEP** プロファイル設定	説明
パスワード	この設定では、SCEP サービスからチャレンジパスワードを取得するために必要なパスワードを指定します この設定は、［SCEP チャレンジの種類］が［動的］に設定されている場合のみ有効です。
チャレンジパスワード	この設定では、デバイスが証明書の登録に使用するチャレンジパスワードを指定します。 この設定は、［SCEP チャレンジの種類］が［静的］に設定されている場合のみ有効です。

iOS ：**SCEP** プロファイル設定

iOS ：**SCEP** プロファイル設定	説明
SCEP 要求のプロキシとして BlackBerry UEM を使用	この設定では、デバイスからのすべての SCEP 要求を UEM 経由で送信するかどうかを指定します。CA がファイアウォールの内部にある場合は、この設定を使用して、CA をファイアウォールの外部にさらすことなく、クライアント証明書をデバイスに登録できます。
CA 接続に BlackBerry Connectivity Node を使用する	この設定は、SCEP 要求を BlackBerry Connectivity Node 経由でルーティングするかどうかを指定します。この設定は、BlackBerry UEM Cloud にのみ表示されます。
サブジェクト	この設定では、組織の SCEP 設定で必要な場合に、証明書のサブジェクトを指定します。サブジェクトは、「/CN=<*common_name*>/O=<*domain_name*>」の形式で入力します。プロファイルが複数のユーザーに対応している場合は、%UserDistinguishedName% などの変数を使用できます。
再試行	この設定では、SCEP サービスへの接続試行が失敗した場合に、接続を再試行する回数を指定します。
再試行遅延	この設定では、SCEP サービスへの接続を再試行する前に、待機する時間（秒単位）を指定します。
キーサイズ	この設定では、証明書のキーサイズを指定します。
指紋	この設定では、SCEP 証明書を登録するための指紋を指定します。CA が HTTPS ではなく HTTP を使用している場合、デバイスは指紋を使用して、登録プロセス中に CA の ID を確認します。指紋は隙間なく登録する必要があります。
SAN の種類	この設定では、必要な場合に、証明書のサブジェクトの別名のタイプを指定します。

iOS ：**SCEP** プロファイル設定	説明
SAN 値	この設定では、証明書のサブジェクトの代替表示を指定します。値は、メールアドレス、CA サーバーの DNS 名、またはサーバーの完全修飾 URL にする必要があります。 指定に適した値は、［SAN の種類］設定によって決まります。［RFC822 名］に設定した場合、値は有効なメールアドレスにする必要があります。［URI］に設定した場合、値はプロトコルと FQDN または IP アドレスを含む有効な URL にする必要があります。［NT プリンシパル名］に設定した場合、値は有効なプリンシパル名にする必要があります。［DNS 名］に設定した場合、値は有効な FQDN にする必要があります。
NT プリンシパル名	この設定では、証明書生成用の NT プリンシパル名を指定します。 この設定は、［SAN の種類］が［なし］以外に設定されている場合のみ有効です。
プロファイルの有効期限	証明書の発行後、CA の新しい証明書をデバイスが要求するまでの日数を指定します。 この値は、CA によって定義された証明書の有効期間より小さい値にする必要があります。

macOS ：**SCEP** プロファイル設定

macOS ：**SCEP** プロファイル設定	説明
SCEP 要求のプロキシとして BlackBerry UEM を使用	この設定では、デバイスからのすべての SCEP 要求を BlackBerry UEM 経由で送信するかどうかを指定します。CA がファイアウォールの内部にある場合は、この設定を使用して、CA をファイアウォールの外部にさらすことなく、クライアント証明書をデバイスに登録できます。
CA 接続に BlackBerry Connectivity Node を使用する	この設定は、SCEP 要求を BlackBerry Connectivity Node 経由でルーティングするかどうかを指定します。この設定は、BlackBerry UEM Cloud にのみ表示されます。
プロファイルを適用	この設定は、SCEP 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。
サブジェクト	この設定では、組織の SCEP 設定で必要な場合に、証明書のサブジェクトを指定します。件名を「/CN=<*common_name*>/O=<*domain_name*>」の形式で入力します。プロファイルが複数のユーザーに対応している場合は、%UserDistinguishedName% などの変数を使用できます。
再試行	この設定では、SCEP サービスへの接続試行が失敗した場合に、接続を再試行する回数を指定します。

macOS ：**SCEP** プロファイル設定	説明
再試行遅延	この設定では、SCEP サービスへの接続を再試行する前に、待機する時間（秒単位）を指定します。
キーサイズ	この設定では、証明書のキーサイズを指定します。
指紋	この設定では、SCEP 証明書を登録するための指紋を指定します。CA が HTTPS ではなく HTTP を使用している場合、デバイスは指紋を使用して、登録プロセス中に CA の ID を確認します。指紋は隙間なく登録する必要があります。
SAN の種類	この設定では、必要な場合に、証明書のサブジェクトの別名のタイプを指定します。
SAN 値	この設定では、証明書のサブジェクトの代替表示を指定します。値は、メールアドレス、CA サーバーの DNS 名、またはサーバーの完全修飾 URL にする必要があります。 指定に適した値は、［SAN の種類］設定によって決まります。［RFC822 名］に設定した場合、値は有効なメールアドレスにする必要があります。［URI］に設定した場合、値はプロトコルと FQDN または IP アドレスを含む有効な URL にする必要があります。［NT プリンシパル名］に設定した場合、値は有効なプリンシパル名にする必要があります。［DNS 名］に設定した場合、値は有効な FQDN にする必要があります。
NT プリンシパル名	この設定では、証明書生成用の NT プリンシパル名を指定します。 この設定は、［SAN の種類］が［なし］以外に設定されている場合のみ有効です。

Android ：**SCEP** プロファイル設定

Android Management アクティベーションタイプのデバイスについては、「Android Management のアクティベーションタイプに関する考慮事項」を参照してください。

Android ：**SCEP** プロファイル設定	説明
SCEP 要求のプロキシとして BlackBerry UEM を使用	この設定では、デバイスからのすべての SCEP 要求を UEM 経由で送信するかどうかを指定します。CA がファイアウォールの内部にある場合は、この設定を使用して、CA をファイアウォールの外部にさらすことなく、クライアント証明書をデバイスに登録できます。
Android Enterprise デバイスで証明書を非表示にする	この設定では、証明書が Android Enterprise のユーザーに表示されるかどうかを指定します。証明書が非表示の場合、ユーザーは証明書を選択して別の目的で使用することはできません。

Android ：**SCEP** プロファイル設定	説明
CA 接続に BlackBerry Connectivity Node を使用する	この設定は、SCEP 要求を BlackBerry Connectivity Node 経由でルーティングするかどうかを指定します。この設定は、UEM Cloud にのみ表示されます。
暗号化アルゴリズム	この設定では、Android デバイスが証明書登録要求に使用する暗号化アルゴリズムを指定します。
ハッシュ関数	この設定では、Android デバイスが証明書登録要求に使用するハッシュ関数を指定します。
証明書サムプリント	この設定では、CA のルート証明書の 16 進エンコードされたハッシュを指定します。サムプリントの指定には、アルゴリズム SHA-1、SHA-224、SHA-256、SHA-384、および SHA-512 を使用できます。Android Enterprise または Samsung Knox デバイスをアクティブ化するには、この設定に値を指定する必要があります。
自動更新	この設定では、証明書が期限切れになり、証明書の自動更新が実行されるまでの日数を指定します。
Android 仕事用プロファイルおよび **Samsung KNOX**	
サブジェクト	この設定では、組織の SCEP 設定で必要な場合に、証明書のサブジェクトを指定します。サブジェクトは、「/CN=<*common_name*>/O=<*domain_name*>」の形式で入力します。プロファイルが複数のユーザーに対応している場合は、%UserDistinguishedName% などの変数を使用できます。
SAN の種類	この設定では、必要な場合に、証明書のサブジェクトの別名のタイプを指定します。
SAN 値	この設定では、証明書のサブジェクトの代替表示を指定します。値には、メールアドレス、CA サーバーの DNS 名、サーバーの完全修飾 URL、またはプリンシパル名を指定する必要があります。 指定に適した値は、［SAN の種類］設定によって決まります。［RFC822 名］に設定した場合、値は有効なメールアドレスにする必要があります。［URI］に設定した場合、値はプロトコルと FQDN または IP アドレスを含む有効な URL にする必要があります。［NT プリンシパル名］に設定した場合、値は有効なプリンシパル名にする必要があります。［DNS 名］に設定した場合、値は有効な FQDN にする必要があります。
キーのアルゴリズム	この設定では、デバイスがクライアントキーペアの生成に使用するアルゴリズムを指定します。CA によってサポートされているアルゴリズムを選択する必要があります。

Android ：**SCEP** プロファイル設定	説明
RSA の強度	この設定では、デバイスがクライアントキーペアの生成に使用する RSA の強度を指定します。CA によってサポートされているキー強度を選択する必要があります。 この設定は、［キーアルゴリズム］が［RSA ］に設定されている場合のみ有効です。
キー使用法	この設定には、証明書に含まれるパブリックキーを使用して実行できる暗号化操作を指定します。
拡張キー使用法	この設定では、証明書に含まれるキーの目的を指定します。

Windows 10 ：**SCEP** プロファイル設定

Windows 10 ：**SCEP** プロファイル設定	説明
ユーザー証明書ストア	この設定は、証明書がデバイスのユーザー証明書の場所に保存されるかどうかを指定します。
サブジェクト	この設定では、組織の SCEP 設定で必要な場合に、証明書のサブジェクトを指定します。サブジェクトは、「/CN=*<common_name>*/O=*<domain_name>*」の形式で入力します。プロファイルが複数のユーザーに対応している場合は、%UserDistinguishedName% などの変数を使用できます。
SAN の種類	この設定では、必要な場合に、証明書のサブジェクトの別名のタイプを指定します。
SAN 値	この設定では、証明書のサブジェクトの代替表示を指定します。値は、メールアドレス、CA サーバーの DNS 名、またはサーバーの完全修飾 URL にする必要があります。 この設定に適した値は、［SAN の種類］設定で選択した値に応じて異なります。
再試行	この設定では、SCEP サービスへの接続試行が失敗した場合に、接続を再試行する回数を指定します。
再試行遅延	この設定では、SCEP サービスへの接続を再試行する前に、待機する時間（秒単位）を指定します。
キーサイズ	この設定では、証明書のキーサイズを指定します。
キー使用法	この設定には、証明書に含まれるパブリックキーを使用して実行できる暗号化操作を指定します。
拡張キー使用法	この設定では、証明書に含まれるキーの目的を指定します。

Windows 10 ：**SCEP** プロファイル設定	説明
SCEP キーストレージ	この設定は、秘密鍵の保存場所を指定します。
ハッシュ関数	この設定では、Windows 10 デバイスが証明書登録要求に使用するハッシュ関数を指定します。
証明書サムプリント	この設定では、CA のルート証明書の 16 進エンコードされたハッシュを指定します。サムプリントの指定には、アルゴリズム SHA-1、SHA-224、SHA-256、SHA-384、および SHA-512 を使用できます。
自動更新	この設定では、証明書が期限切れになり、証明書の自動更新が実行されるまでの日数を指定します。 最大値は 365 日です。

BlackBerry Dynamics ：**SCEP** プロファイル設定

これらの設定は、BlackBerry Dynamics および iOS デバイスの Android アプリで使用される SCEP 証明書に適用されます。

BlackBerry Dynamics ：**SCEP** プロファイル設定	説明
サブジェクト	この設定では、組織の SCEP 設定で必要な場合に、証明書のサブジェクトを指定します。サブジェクトは、「/CN=<*common_name*>,O=<*domain_name*>」の形式で入力します。プロファイルが複数のユーザーに対応している場合は、%UserDistinguishedName% などの変数を使用できます。
SAN の種類	この設定では、必要な場合に、証明書のサブジェクトの別名のタイプを指定します。
SAN 値	この設定では、証明書のサブジェクトの代替表示を指定します。値には、メールアドレス、CA サーバーの DNS 名、サーバーの完全修飾 URL、またはプリンシパル名を指定する必要があります。 指定に適した値は、［SAN の種類］設定によって決まります。［RFC822 名］に設定した場合、値は有効なメールアドレスにする必要があります。［URI］に設定した場合、値はプロトコルと FQDN または IP アドレスを含む有効な URL にする必要があります。［NT プリンシパル名］に設定した場合、値は有効なプリンシパル名にする必要があります。［DNS 名］に設定した場合、値は有効な FQDN にする必要があります。
キーのアルゴリズム	この設定では、クライアントキーペアを生成するために使用するアルゴリズムを指定します。CA によってサポートされているアルゴリズムを選択する必要があります。

BlackBerry Dynamics：SCEP プロファイル設定	説明
RSA の強度	この設定では、クライアントキーペアを生成するために使用する RSA の強度を指定します。CA によってサポートされているキー強度を選択する必要があります。 この設定は、［キーアルゴリズム］が［RSA ］に設定されている場合のみ有効です。
暗号化アルゴリズム	この設定では、証明書登録要求に使用する暗号化アルゴリズムを指定します。
ハッシュ関数	この設定では、証明書登録要求に使用するハッシュ関数を指定します。
証明書サムプリント	この設定では、CA のルート証明書の 16 進エンコードされたハッシュを指定します。サムプリントの指定には、アルゴリズム SHA-1、SHA-224、SHA-256、SHA-384、および SHA-512 のいずれかを使用できます。MD5 は、BlackBerry Dynamics プロファイルで［FIPS を有効にする］が選択されていない場合にのみサポートされます。
自動更新	この設定では、証明書が期限切れになり、証明書の自動更新が実行されるまでの日数を指定します。
キー使用法	この設定には、証明書に含まれるパブリックキーを使用して実行できる暗号化操作を指定します。
拡張キー使用法	この設定では、証明書に含まれるキーの目的を指定します。
アプリの制限	この設定は、証明書を使用できる BlackBerry Dynamics アプリを指定します。
SCEP の使用を許可されたアプリ	この設定は、SCEP 証明書を使用できる BlackBerry Dynamics アプリを指定します。 この設定は、［アプリの制限］設定が［証明書の使用を指定のアプリに許可する］に設定されている場合のみ有効です。
有効期限が切れた証明書を削除する	この設定では、デバイスが有効期限の切れた証明書を削除するかどうかを指定します。
重複する証明書を削除する	この設定では、デバイスが重複する証明書を削除するかどうかを指定します。デバイスは、開始日が最も早い証明書を削除します。

複数のデバイスへの同じクライアント証明書の送信

共有証明書プロファイルを使用すると、iOS、macOS、および Android デバイスにクライアント証明書を送信できます。

共有証明書プロファイルでは、そのプロファイルが割り当てられた全ユーザーに同じキーペアが送信されます。共有の証明書プロファイルは、複数のユーザーにクライアント証明書の共有を許可する場合にのみ、使用します。

作業を始める前に： デバイスに送信するクライアント証明書ファイルを取得する必要があります。証明書ファイルのファイル名拡張子は、pfx または .p12 にする必要があります。

1. メニューバーで、［ポリシーとプロファイル］ > ［証明書］ > ［共有の証明書］をクリックします。
2. ＋をクリックします。
3. プロファイルの名前と説明を入力します。
4. ［パスワード］フィールドに、共有の証明書プロファイルのパスワードを入力します。
5. ［証明書ファイル］フィールドで、［参照］をクリックして証明書ファイルを見つけます。
6. Android Enterprise デバイスを管理している場合にユーザーが他の目的で証明書を使用することを選択できないようにするには、［**Android**］タブで［**Android Enterprise** デバイスの証明書を非表示］を選択します。
7. macOS デバイスを管理している場合は、［**macOS**］タブの［プロファイルを適用］ドロップダウンリストで、［ユーザー］または［デバイス］を選択します。
8. ［追加］をクリックします。

終了したら： 共有の証明書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ます。

証明書マッピングプロファイルの使用によるアプリが使用する証明書の指定

Android デバイスでは、証明書マッピングプロファイルを使用して、アプリが使用するクライアント証明書を指定できます。証明書マッピングプロファイルは、BlackBerry Dynamics アプリではサポートされていません。

証明書マッピングプロファイルを使用すると、Android アプリが使用する証明書を指定できます。SCEP、ユーザー資格情報、または共有証明書プロファイルによってデバイスに送信された証明書を使用するように、アプリに要求できます。1 つ以上の指定されたアプリまたはすべての監視対象アプリで証明書を使用できます。また、アプリに証明書が必要なときにいつでも使用するか、特定の URI への接続にのみ使用するかを指定することもできます。

1 つのプロファイルで複数の証明書マッピングを指定できます。1 人のユーザーに割り当てることができる証明書マッピングプロファイルは 1 つのみです。

作業を始める前に： デバイスに証明書を送信するために必要な SCEP プロファイル、ユーザー資格情報プロファイル、共有証明書プロファイルを作成し、ユーザーまたはグループにそれらのプロファイルを割り当てます。

1. メニューバーで、［ポリシーとプロファイル］ > ［証明書］ > ［証明書マッピング］をクリックします。
2. ＋をクリックします。
3. プロファイルの名前と説明を入力します。
4. マッピングテーブルで、＋をクリックします。
5. ［宛先 **URI**］で、次のいずれかのオプションを選択します。
   - アプリでリソースとの接続の認証にその証明書を使用しない場合は、［なし］を選択します。
   - アプリであらゆるリソースとの接続の認証にその証明書を使用できる場合は、［すべて］を選択します。
   - アプリで特定のリソースとの認証にその証明書を使用できる場合は、［指定されたホスト：ポート］を選択し、ホストとポートを入力します。
6. ［アプリ証明書］で、次の操作のいずれかを実行します。
   - 別のプロファイルによってデバイスに送信された証明書をアプリで使用するように指定するには、［選択した証明書］を選択し、ドロップダウンリストからプロファイル名をクリックします。
   - サードパーティのソースによってデバイスに送信された証明書をアプリで使用するように指定するには、［証明書エイリアス］を選択し、証明書を表すエイリアスを入力します。

- 別のプロファイルによってデバイスに送信された証明書をアプリで使用するように指定するには、［選択した証明書］を選択し、ドロップダウンリストからプロファイル名をクリックします。

7. ［宛先 **URI** 用に許可されるアプリ］で、次の操作のいずれかを実行します。
   - あらゆる管理対象アプリが指定の証明書を要求できるようにするには、［仕事用領域内のすべてのアプリ］を選択します。
   - 指定されたアプリのみが証明書を要求できるようにするには、［指定されたアプリ］を選択し、＋をクリックして 1 つ以上のアプリを指定します。
8. 必要に応じて、手順 5〜8 を繰り返して、追加のマッピングをプロファイルに追加します。
9. ［追加］をクリックします。

終了したら：

- 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。
- 複数の証明書マッピングプロファイルを作成する場合は、必要に応じて、プロファイルをランク付けします。プロファイルを選択し、⇅をクリックしてプロファイルを上下に移動してランク付けします。［保存］をクリックします。

ユーザーアカウント用クライアント証明書の管理

クライアント証明書は、個々のユーザーアカウントに直接追加することも、ユーザーアカウントに割り当てられたユーザー資格情報プロファイルに追加することもできます。ユーザーアカウントに証明書を直接追加する方法は、BlackBerry Dynamics 対応デバイス、またはその他の監視対象 iOS デバイスと Android デバイスでサポートされています。証明書のユーザー資格情報プロファイルへのアップロードは、iOS デバイスおよび Android Enterprise デバイスでサポートされています。

仕事用 Wi-Fi ネットワーク、仕事用 VPN、仕事用メールサーバーへの接続に使用する証明書を、ユーザーがアップロードできるようにするには、Wi-Fi、VPN、またはメールプロファイルに関連付けできるユーザー資格情報プロファイルを使用します。

オンプレミス環境があって BlackBerry Dynamics アプリの証明書をユーザーアカウントにアップロードする場合は、ユーザー証明書の有効期間を設定する必要があります。有効期間が終了すると、証明書がサーバーから削除されます。

ユーザーアカウントへのクライアント証明書の追加および管理

1. 管理コンソールのメニューバーで、［ユーザー］ > ［管理対象デバイス］をクリックします。
2. ユーザーアカウントを検索してクリックします。
3. 次の操作のいずれかを実行します。

タスク	手順
ユーザーアカウントへのクライアント証明書の追加	クライアント証明書を個々のユーザーアカウントに追加し、その証明書を BlackBerry Dynamics 対応デバイスまたは他の管理対象の iOS および Android デバイスに送信できます。ユーザーデバイスが S/MIME またはクライアント認証で証明書を必要とし、ユーザー資格情報プロファイルまたは SCEP プロファイルを介して証明書をデバイスに送信できない場合に、クライアント証明書をユーザーアカウントに追加します。クライアント証明書のファイル名拡張子は、.pfx または .p12 にする必要があります。複数のクライアント証明書をデバイスに送信できます。ユーザー資格情報プロファイルを使用して、個々のユーザーの証明書をアップロードすることもできます。ユーザー資格情報プロファイルは、Wi-Fi、VPN、またはメールプロファイルに関連付けることができます。 **a.** ［**IT** ポリシーおよびプロファイル］セクションで ＋ をクリックします。 **b.** ［ユーザー証明書］をクリックします。 **c.** 証明書の説明を入力します。 **d.** ［証明書の適用先］セクションで、次のいずれかを選択します。 **1.** ［その他の管理対象デバイス］：BlackBerry Dynamics アプリ用以外のサポートされているすべての用途で iOS および Android デバイスに証明書を送信するには、このオプションを選択します。 **2.** ［**BlackBerry Dynamics** 対応デバイス］：BlackBerry Dynamics アプリで使用するために証明書をデバイスに送信するには、このオプションを選択します。 **e.** ［証明書ファイル］フィールドで、［参照］をクリックします。証明書ファイルに移動して選択します。 **f.** ［パスワード］フィールドで［その他の管理対象デバイス］を選択する場合は、証明書のパスワードを入力します。iOS デバイスでは、パスワードが必要です。Android デバイスでは、最新バージョンの UEM Client を実行している場合は、パスワードを入力する必要はありません。パスワードを設定しない場合、ユーザーはデバイスパスワードを入力する必要があります。 **g.** ［追加］をクリックします。 **h.** クライアント証明書の有効期間を設定します。クライアント証明書が削除されるまでのデフォルトの有効時間は 24 時間です。 **1.** メニューバーで［設定］**>**［一般設定］**>**［証明書］をクリックします。 **2.** サーバー上の PKCS#12 証明書の有効期間を指定します。

タスク	手順
ユーザーアカウントの BlackBerry Dynamics 証明書の更新または削除	CA から証明書の更新を要求するコマンドをユーザーのデバイスに送信できます。ユーザーのデバイスから、BlackBerry Dynamics 証明書を削除することもできます。証明書を削除すると、BlackBerry Dynamics PKI コネクターが、証明書が使用されなくなったという通知を CA に送信しますが、証明書は自動的には失効しません。 ［ユーザー証明書］セクションで、次の操作のいずれかを実行します。 **a.** CA から証明書の更新を要求するには、をクリックします。 **b.** ユーザーのデバイスから証明書を削除するには、✕をクリックします。 デバイスから Entrust スマート認証情報を削除するには、BlackBerry UEM Client でスマート認証情報を無効化する必要もあります。
オフプレミス環境におけるユーザー資格情報プロファイルへのクライアント証明書の追加	個々のユーザーの証明書をユーザー資格情報プロファイルにアップロードできます。ユーザーが、UEM Self-Service を使用して、自分の証明書をユーザー資格情報プロファイルにアップロードすることもできます。ユーザー資格情報プロファイルへの証明書のアップロードは、iOS デバイスおよび Android Enterprise デバイスでサポートされます。 クライアント証明書のファイル名拡張子は、.pfx または .p12 にする必要があります。管理者またはユーザーが新しい証明書をユーザー資格情報プロファイルにアップロードすると、ユーザーデバイス上の既存の証明書が置き換えられます 開始する前に： • 手動で証明書をアップロードするためのユーザー資格情報プロファイルの作成。 • ユーザー資格情報プロファイルをユーザーに割り当てます。 **a.** ［**IT** ポリシーおよびプロファイル］セクションで、ユーザー資格情報プロファイルの横にある［証明書を追加］をクリックします。 **b.** ［参照］をクリックします。証明書に移動して選択します。 **c.** 証明書のパスワードを入力します。iOS デバイスでは、パスワードが必要です。Android デバイスで、最新バージョンの UEM Client を実行している場合、UEM にパスワードを入力する必要はありません。パスワードを指定しない場合、ユーザーはデバイスパスワードを入力する必要があります。 **d.** ［追加］をクリックします。

タスク	手順
オフプレミス環境におけるユーザー資格情報プロファイルのクライアント証明書の変更	新しい証明書は、デバイス上の既存の証明書に置き換わります。 **a.** ［**IT** ポリシーおよびプロファイル］セクションで、ユーザー資格情報プロファイルの横にある［更新］をクリックします。 **b.** ［参照］をクリックして、証明書を探します。 **c.** 証明書のパスワードを入力します。iOS デバイスでは、パスワードが必要です。Android デバイスでは、最新バージョンの UEM Client を実行している場合は、UEM にパスワードを入力する必要はありません。パスワードを指定しない場合、ユーザーはデバイスパスワードを入力する必要があります。 **d.** ［保存］をクリックします。

商標などに関する情報

該当する特許は、次の場所で確認できます：www.blackberry.com/patents。

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