BlackBerry UEM

PKI を使用した接続のセキュリティ保護

管理

12.17

目次

証明書と PKI 5

証明書を使用する手順 6

BlackBerry UEM と組織の PKI ソフトウェアとの統合 7

BlackBerry UEM と組織の Entrust ソフトウェアの接続 7
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 8
BlackBerry UEM と組織の OpenTrust ソフトウェアの接続 8
BlackBerry UEM から BlackBerry Dynamics PKI コネクターへの接続 9
組織のアプリベース PKI ソリューションへの BlackBerry UEM の接続 10

デバイスおよびアプリへのクライアント証明書の提供 11

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 13

プロファイル選択によるクライアント証明書のデバイスおよびアプリへの送信 14
デバイスおよびアプリへの CA 証明書の送信 14
CA 証明書プロファイルの作成 14
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 15
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 15
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 16
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 17
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 18
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 19
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 20
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 23
SCEP プロファイルの作成 24
SCEP プロファイル設定 24
複数のデバイスへの同じクライアント証明書の送信 39
共有の証明書プロファイルの作成 39
アプリで使用する証明書を指定する 40
証明書マッピングプロファイルの作成 40

ユーザーアカウント用クライアント証明書の管理 42

ユーザーアカウントへのクライアント証明書の追加 42
ユーザーアカウントのクライアント証明書の変更 43
ユーザーアカウントの BlackBerry Dynamics 証明書の更新または削除 43
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 43
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 44

クライアント証明書の有効期間の設定.....44

商標などに関する情報..... 46

証明書と PKI

PKI 証明書は、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。

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。

- HTTPS を使用する Web ページに接続するときに、SSL/TLS を使用して認証する
- 仕事用メールサーバーで認証する
- 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の暗号化と署名を行う

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。

証明書を使用する手順

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 ソフトウェアに接続します。
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。
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、BlackBerry 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 ソフトウェアの接続

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 BlackBerry 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
- BlackBerry 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。BlackBerry 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. メニューバーで［設定］をクリックします。
2. ［外部統合］ > ［認証局］の順にクリックします。
3. ［**Entrust** 接続を追加］をクリックします。
4. ［接続名］フィールドに、接続の名前を入力します。
5. ［**URL**］フィールドに、Entrust MDM Web Service の URL を入力します。
6. ［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。
7. ［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。
8. Entrust サーバーへの SSL 接続の確立を BlackBerry UEM に許可するために CA 証明書をアップロードするには、［参照］をクリックします。CA 証明書に移動して選択します。
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。

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 管理者に問い合わせて、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ベート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. メニューバーで［設定］をクリックします。
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 ソフトウェアの接続

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 形式）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］をクリックします。
2. ［外部統合］ > ［認証局］の順にクリックします。
3. ［**OpenTrust** 接続を追加する］をクリックします。
4. ［接続名］フィールドに、接続の名前を入力します。
5. ［**URL**］ フィールドに、OpenTrust ソフトウェアの URL を入力します。
6. ［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証明書に移動して選択します。
7. ［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。
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。
- デバイスに証明書を配布するために OpenTrust ソフトウェアの BlackBerry 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 BlackBerry 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。

メモ：BlackBerry UEM Cloud 環境では、BlackBerry 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。

PKI コネクターは、バックエンドサーバー上の Java プログラムと Web サービスのセットであり、BlackBerry UEM が証明書要求を送信し、CA から応答を受信できるようにします。BlackBerry UEM は、BlackBerry Dynamics ユーザー証明書管理プロトコルを使用して、PKI コネクターと通信します。このプロトコルは HTTPS を介して実行され、JSON 形式のメッセージを定義します。BlackBerry Dynamics PKI コネクター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 コネクター』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. 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］：BlackBerry 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］：BlackBerry 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 BlackBerry 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する必要があります。
   - **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する必要があります。

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、BlackBerry UEM のアプリリストにあることを確認します。

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. ［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 アプリで使用する証明書を PKI アプリから取得するアプリを選択します。Purebred を使用するには、BlackBerry UEM Client を選択します。
4. ［追加］をクリックします。

終了したら：

- 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。
- 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 BlackBerry 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）
共有証明書プロファイル	共有証明書プロファイルは、BlackBerry 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。BlackBerry 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

証明書の追加	説明	サポートされるデバイス
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。BlackBerry 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 BlackBerry 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 BlackBerry 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 BlackBerry 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	BlackBerry 10 デバイスでは、ユーザーは［システム設定］の［セキュリティおよびプライバシー］に移動し、デバイスの証明書ストアにクライアント証明書をインポートできます。仕事用ブラウザーでの使用や仕事用メールアカウントからの S/MIME 保護されたメッセージの送信のための証明書は、デバイスのファイルシステムから、または仕事用領域からアクセスできるネットワーク上の場所からインポートできます。 Android デバイスでは、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

ポリシーおよびプロファイルライブラリで利用可能な次のプロファイルを使用して、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 アプリに送信できるようにする。 • BlackBerry UEM で証明書を手動でアップロードできるようにし、オンプレミス環境では BlackBerry UEM Self-Service を使用した証明書のアップロードをユーザーができるようにする。 • 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、BlackBerry 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。BlackBerry 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」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、アプリの設定で［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。

プロファイル選択によるクライアント証明書のデバイスおよびアプリへの送信

さまざまなタイプのプロファイルを使用して、デバイスおよび BlackBerry Dynamics アプリにクライアント証明書を送信できます。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。
- BlackBerry 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。

  メモ：Android Enterprise デバイスは、Wi-Fi 認証のために BlackBerry UEM によってデバイスに送信された証明書の使用をサポートしていません。
- 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. 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. ［証明書］ > ［CA 証明書］をクリックします。

3. ＋をクリックします。
4. プロファイルの名前と説明を入力します。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。
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. CA 証明書を BlackBerry 10 デバイスに送信する場合は、［BlackBerry ］タブで、証明書をデバイスに送信するために次の証明書ストアを 1 つ以上指定します。
   - ブラウザー証明書ストア
   - VPN 証明書ストア
   - Wi-Fi 証明書ストア
   - エンタープライズ証明書ストア
7. 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。
8. ［追加］をクリックします。

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 BlackBerry UEM Self-Service にアップロード
- BlackBerry UEM と組織の Entrust CA または OpenTrust CA 間の確立された接続経由
- 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 コネクター接続経由
- 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

UEM Self-Service で証明書を手動でアップロードする場合、管理コンソールのユーザーページで証明書を確認できます。また証明書を削除、あるいは置換することもできます。この機能は BlackBerry UEM Cloud ではサポートされていません。

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。

組織の PKI ソフトウェアに BlackBerry UEM を接続する方法の詳細については、「BlackBerry UEM と組織の PKI ソフトウェアとの統合」を参照してください。

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］をクリックします。
2. ［証明書］ > ［ユーザー資格情報］をクリックします。
3. ＋をクリックします。
4. プロファイルの名前と説明を入力します。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。
5. ［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。
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。このオプションは、Android 9.0 以降のデバイスにのみ適用されます。
7. ［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へのクライアント証明書の追加 または、BlackBerry UEM Self-Service を使用して自分の証明書をアップロードするようにユーザーに指示します。

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。

メモ：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。BlackBerry UEM は、PKI ソフトウェアからプロファイルのリストを取得します。
- 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。たとえば、デバイスの種類（devicetype）、Entrust IdentityGuard グループ（iggroup）、Entrust IdentityGuard username（igusername）などが必要です。
- 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。BlackBerry 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］をクリックします。
2. ［証明書］ > ［ユーザー資格情報］をクリックします。
3. ＋をクリックします。
4. プロファイルの名前と説明を入力します。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。
5. ［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。
6. ［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。
7. 目的のプロファイルの値を指定します。
8. 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。

9. 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。
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、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 ユーザーは、プロファイルを受信したときに、パスワードの入力を求められます（パスワードは画面上に表示されます）。

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 デバイスでの 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

メモ：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］をクリックします。
2. ［証明書］ **>** ［ユーザー資格情報］をクリックします。
3. ＋をクリックします。
4. プロファイルの名前と説明を入力します。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。
5. ［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。
6. ［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。
7. 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］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。
8. スマート認証情報が BlackBerry Dynamics アプリに送信される場合、［**BlackBerry Dynamics**］タブをクリックして、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。

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。
- 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、BlackBerry 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 BlackBerry 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］をクリックします。
2. ［証明書］ > ［ユーザー資格情報］をクリックします。
3. ＋をクリックします。
4. プロファイルの名前と説明を入力します。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。
5. ［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。

6. ［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。
7. 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］を選択します。

   これは、Android デバイス専用です。
8. 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。
9. 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。

   S/MIME に使用される有効期限が切れた暗号化証明書は、証明書の有効期限が切れる前に暗号化されたメッセージをユーザーが確認できるように、デバイス上に保持しておく必要があります。
10. 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。デバイスは、開始日が最も早い証明書を削除します。
11. ［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］をクリックします。
2. ［証明書］ > ［ユーザー資格情報］をクリックします。
3. ＋をクリックします。
4. プロファイルの名前と説明を入力します。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。
5. ［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 接続を選択します。
6. 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。

7. 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。
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］を選択します。デバイスは、開始日が最も早い証明書を削除します。
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。

BlackBerry Dynamics PKI コネクター経由で登録された証明書の更新

すべての BlackBerry Dynamics ユーザーのユーザー証明書を更新する必要がある場合、ユーザー資格情報プロファイルが割り当てられている全デバイスに、証明書の更新を要求するコマンドを送信できます。

1. メニューバーで［ポリシーとプロファイル］をクリックします。
2. ［証明書］ > ［ユーザー資格情報］をクリックします。
3. 変更するプロファイルの名前をクリックします。
4. ［**PKI** 機能を更新］をクリックすると、PKI コネクターの最新の詳細情報が確実に BlackBerry UEM に反映されます。
5. ［更新］をクリックして、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、証明書を更新するように指示します。

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。

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。

アプリベースの証明書を使用する手順

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 Client** を有効にする］を選択し、BlackBerry UEM Client を［アプリ認証委任］に指定します。
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 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使用するユーザー資格情報プロファイルを作成します。
7	アプリベース PKI ソリューションを Android デバイスで使用するには、ネイティブキーストアからの証明書を使用するユーザー資格情報プロファイルを作成します。

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。

1. BlackBerry 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。
7. 作成したアプリ設定を含む BlackBerry 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。

1. BlackBerry 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. ［ユーザー証明書と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］オプションを選択します。
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.** ［設定］タブで ［クライアントには、**GC** にアップロードされた個々のログイン証明書（**SSL**）が必要］を選択します。 **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、［**BEMS** を使用してユーザーの **EAS/EWS** の自動検出を実行する］を選択します。 **c.** ［**Exchange** 設定］タブの［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。
組織で BEMS を使用していないときに BlackBerry Work を設定する	**a.** ［**Exchange** 設定］タブを選択します。 **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、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、［デフォルトドメイン］フィールドに指定します。 **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（cas.mydomain.com など）を指定します。 **d.** 自動検出 URL がわかっている場合は、［自動検出 **URL**］フィールドに指定します。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.** ［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。

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

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. ［証明書］ **>** ［ユーザー資格情報］をクリックします。
3. ＋をクリックします。
4. プロファイルの名前と説明を入力します。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。

5. ［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選択します。Purebred を使用している場合は、BlackBerry UEM Client を選択します。
6. 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
      ```
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］を選択します。

   S/MIME に使用される有効期限が切れた暗号化証明書は、証明書の有効期限が切れる前に暗号化されたメッセージをユーザーが確認できるように、デバイス上に保持しておく必要があります。
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］を選択します。デバイスは、開始日が最も早い証明書を削除します。
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、BlackBerry 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］をクリックします。
2. ［証明書］ > ［**SCEP**］をクリックします。
3. ＋をクリックします。
4. プロファイルの名前と説明を入力します。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。
5. ［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ません。
   - ［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。
6. ［**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。
7. ［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。
8. 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。
9. 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。
10. 組織内のデバイスタイプごとに手順 8 を繰り返します。
11. ［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。

SCEP プロファイル設定

SCEP プロファイルは、以下のデバイスタイプでサポートされています。

- iOS
- macOS
- Android
- Windows 10

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。組織の Entrust ソフトウェアまたは OpenTrust ソフトウェアに 1 つ以上の接続を設定した場合は、ドロップダウンリストでその接続のうちのいずれかを選択できます。その他の CA を使用している場合は、［汎用］を選択します。 Entrust または OpenTrust 接続を選択する場合は、適切な PKI プロファイルを選択し、必要な値を指定する必要があります。利用可能なプロファイルは、Entrust または OpenTrust 管理者が PKI ソフトウェアで設定した内容によって異なります。 デフォルト値は［汎用］です。
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 BlackBerry 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、BlackBerry UEM が SCEP サーバーを信頼できるようになります。

共通：**SCEP** プロファイル設定	説明
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。これを［動的］に設定すると、すべてのデバイスが固有のチャレンジパスワードを受信します。 使用できる値： • 静的 • 動的 デフォルト値は［動的］です。 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。 使用できる値： • 基本 • NTLM デフォルト値は［基本］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。
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。

共通：**SCEP** プロファイル設定	説明
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 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。
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=<共通名>,O=<ドメイン名>」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、変数を使用できます（%UserDistinguishedName%など）。
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。 使用できる値は 1～999 です。 デフォルト値は［3］です。
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。 使用できる値は 1～999 です。 デフォルト値は［10 秒］です。
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。 使用できる値： • 1024 • 2048 • 4096 デフォルト値は、［1024］です。

iOS ：**SCEP** プロファイル設定	説明
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。 使用できる値： • None • RFC822 名 • DNS 名 • 統一資源識別子 デフォルト値は［なし］です。
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。
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。最大値は 1825 日です。

macOS ：**SCEP** プロファイル設定

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

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。 使用できる値： • ユーザー • デバイス
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=<共通名>,O=<ドメイン名>」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、変数を使用できます（%UserDistinguishedName%など）。
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。 使用できる値は 1～999 です。 デフォルト値は［3］です。
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。 使用できる値は 1～999 です。 デフォルト値は［10 秒］です。
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。 使用できる値： • 1024 • 2048 デフォルト値は［1024］です。
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。

macOS ：**SCEP** プロファイル設定	説明
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。 使用できる値： • None • RFC822 名 • DNS 名 • 統一資源識別子 デフォルト値は［なし］です。
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 デバイスの SCEP プロファイルの例を確認するには、support.blackberry.com/community にアクセスして、記事 38248 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 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。
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 9.0 以降の 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。
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。

Android：**SCEP** プロファイル設定	説明
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。 使用できる値： • なし • 3DES • AES（128 ビット） • AES（196 ビット） • AES（256 ビット） デフォルト値は［Triple DES］です。
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。 使用できる値： • なし • SHA-1 • SHA-224 • SHA-256 • SHA-384 • SHA-512 デフォルト値は［SHA-1］です。
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。 使用できる値は 1〜365 です。 デフォルト値は［30］です。
Android Enterprise/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=<共通名>/O=<ドメイン名>」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。

Android：**SCEP** プロファイル設定	説明
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。 使用できる値： • RFC 822 名 • 統一資源識別子 • NT プリンシパル名 • DNS 名 デフォルト値は［RFC 822 名］です。
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、Android Enterprise および Samsung Knox 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。 使用できる値： • なし • RSA • ECC デフォルト値は［RSA］です。
RSA の強度	この設定では、Android Enterprise および Samsung Knox 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。 使用できる値： • 1024 • 2048 • 4096 • 8192 • 16384 デフォルト値は［1024］です。

Android：**SCEP** プロファイル設定	説明
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。 次の中から選択します。 • デジタル署名 • 否認防止 • キー暗号化 • データ暗号化 • キーの合意 • キー証明書の署名 • CRL 署名 • 暗号化のみ • 解読のみ デフォルトの選択は、［デジタル署名］、［キー暗号化］、および［キーの合意］です。
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。 次の中から選択します。 • サーバー認証 • クライアント認証 • コード署名 • メール保護 • タイムスタンプ • OCSP 署名 • Secure Shell クライアント • Secure Shell サーバー デフォルト選択は［クライアント認証］です。

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=<共通名>/O=<ドメイン名>」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。

Windows 10：SCEP プロファイル設定	説明
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。 使用できる値： • None • RFC 822 名 • DNS 名 • 統一資源識別子 デフォルト値は［なし］です。
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。 使用できる値は 1～999 です。 デフォルト値は［3］です。
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。 使用できる値は 1～999 です。 デフォルト値は［10 秒］です。
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。 使用できる値： • 1024 • 2048 • 4096 • 8192 • 16384 デフォルト値は［1024］です。

Windows 10：SCEP プロファイル設定	説明
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。 • デジタル署名 • 否認防止 • キー暗号化 • データ暗号化 • キーの合意 • キー証明書の署名 • CRL 署名 • 暗号化のみ デフォルトの選択肢は［キー証明書の署名］と［暗号化のみ］です。
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。 • サーバー認証 • クライアント認証 • コード署名 • メール保護 • タイムスタンプ • OCSP 署名 • Secure Shell クライアント • Secure Shell サーバー デフォルト選択は［クライアント認証］です。
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。 使用できる値： • TPM • TPM（サポートされている場合） • KSP デフォルト値は［KSP］です。
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。 使用できる値： • SHA-1 • SHA-224 • SHA-256 • SHA-384 • SHA-512 デフォルト値は［SHA-1］です。

Windows 10：**SCEP** プロファイル設定	説明
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。 使用できる値は 1～365 です。 デフォルト値は［30］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=<共通名>,O=<ドメイン名>」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。 使用できる値： • RFC 822 名 • 統一資源識別子 • NT プリンシパル名 • DNS 名 デフォルト値は［RFC 822 名］です。
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。

BlackBerry Dynamics：SCEP プロファイル設定	説明
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。 使用できる値： • RSA
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。 使用できる値： • 2048 • 4096 デフォルト値は［2048］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。 使用できる値： • 3DES • AES（128 ビット） • AES（196 ビット） • AES（256 ビット） デフォルト値は［Triple DES］です。
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。 使用できる値： • SHA-256 • SHA-384 • SHA-512 デフォルト値は［SHA-256］です。
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。

BlackBerry Dynamics：SCEP プロファイル設定	説明
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。 使用できる値は 1～365 です。 デフォルト値は［30］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。 次の中から選択します。 ・ デジタル署名 ・ 否認防止 ・ キー暗号化 ・ データ暗号化 ・ キーの合意 ・ キー証明書の署名 ・ CRL 署名 ・ 暗号化のみ ・ 解読のみ デフォルトの選択は、［デジタル署名］、［キー暗号化］、および［キーの合意］です。
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。 次の中から選択します。 ・ サーバー認証 ・ クライアント認証 ・ コード署名 ・ メール保護 ・ タイムスタンプ ・ OCSP 署名 ・ Secure Shell クライアント ・ Secure Shell サーバー デフォルト選択は［クライアント認証］です。
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。 使用できる値： ・ 証明書の使用をすべてのアプリに許可する ・ 証明書の使用を指定のアプリに許可する デフォルトでは、［証明書の使用をすべてのアプリに許可する］が選択されています。

BlackBerry Dynamics：SCEP プロファイル設定	説明
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。

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

共有の証明書プロファイルの作成

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］をクリックします。
2. ［証明書］**>**［共有の証明書］をクリックします。
3. ＋をクリックします。
4. プロファイルの名前と説明を入力します。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。いくつかの名前（たとえば、ca_1）は予約されています。
5. ［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。
6. ［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。
7. 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。このオプションは、Android 9.0 以降にのみ適用されます。
8. 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。
9. ［追加］をクリックします。

アプリで使用する証明書を指定する

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。

証明書マッピングプロファイルの作成

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］をクリックします。
2. ［証明書］ > ［証明書マッピング］をクリックします。
3. ＋をクリックします。
4. プロファイルの名前と説明を入力します。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。
5. マッピングテーブルで、＋をクリックします。
6. ［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。
7. ［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選択します。
   - 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。エイリアスが不明である場合は、証明書プロバイダーに関するドキュメントを参照するか、証明書プロバイダーの管理者に問い合わせてください。
   - 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選択します。
8. ［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。
9. 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。
10. ［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。
- 必要に応じて、プロファイルをランク付けします。

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

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。

1. メニューバーで、［ユーザー］ > ［管理されているデバイス］をクリックします。
2. ユーザーアカウントを検索します。
3. 検索結果で、ユーザーアカウントの名前をクリックします。
4. ［**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。
5. ［ユーザー証明書］をクリックします。
6. 証明書の説明を入力します。
7. ［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。
   - ［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。
   - ［**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。
8. ［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。
9. ［その他の管理対象デバイス］を選択した場合、［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。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 BlackBerry UEM Client を実行している場合は、BlackBerry 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。

10. ［追加］をクリックします。
    証明書は、［ユーザーの概要］ページの［ユーザー証明書］表に記されています。

終了したら：

- BlackBerry Dynamics 対応デバイスの場合、アップロードした証明書がサーバーから自動的に削除されるまでにBlackBerry UEM サーバー上に残っている時間を設定します。デフォルト設定は 24 時間です。

ユーザーアカウントのクライアント証明書の変更

1. メニューバーで、［ユーザー］ > ［管理されているデバイス］をクリックします。
2. ユーザーアカウントを検索します。
3. 検索結果で、ユーザーアカウントの名前をクリックします。
4. ［IT ポリシーおよびプロファイル］セクションで、変更するユーザー証明書をクリックします。
5. をクリックします。
6. 必要な変更を行います。証明書が適用されるデバイスを変更することはできません。
7. ［保存］をクリックします。

終了したら： 管理者またはユーザーが、デバイスから削除した BlackBerry Dynamics ユーザー証明書を変更すると、その証明書はデバイスに再送信されます。

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。

1. メニューバーで、［ユーザー］ > ［管理されているデバイス］をクリックします。
2. ユーザーアカウントを検索します。
3. 検索結果で、ユーザーアカウントの名前をクリックします。
4. ［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。
   - CA から証明書の更新を要求するには、をクリックします。
   - 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。

   メモ： 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。

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、BlackBerry 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

作業を始める前に：

- 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。

1. 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ます。
3. 検索結果で、ユーザーアカウントの名前をクリックします。
4. ［**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。
5. ［参照］をクリックして、証明書ファイルを探します。
6. 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 BlackBerry UEM Client を実行している場合は、BlackBerry 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。
7. ［追加］をクリックします。

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

管理者またはユーザーがユーザー資格情報プロファイルに追加した証明書を変更できます。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。

1. メニューバーで、［ユーザー］ > ［管理されているデバイス］をクリックします。
2. ユーザーアカウントを検索します。
3. 検索結果で、ユーザーアカウントの名前をクリックします。
4. ［**IT** ポリシーおよびプロファイル］セクションのユーザー資格情報プロファイルの行で、［更新］をクリックします。
5. ［参照］をクリックして、証明書ファイルを探します。
6. 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 BlackBerry UEM Client を実行している場合、BlackBerry 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。
7. ［保存］をクリックします。

クライアント証明書の有効期間の設定

BlackBerry Dynamics アプリの個々のユーザーアカウントに証明書をアップロードする場合は、クライアント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。これにより、クライアント証明書がデバイスにプッシュされた後も、長期間サーバー上に残ることを防止します。デフォルトの有効期間は 24 時間です。

この機能は BlackBerry UEM Cloud ではサポートされていません。

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。

終了したら： 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（まだ行っていない場合）。

商標などに関する情報

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