BlackBerry UEM

設定ガイド

12.12

目次

初めて **BlackBerry UEM** を設定する.....7
BlackBerry UEM の設定に必要な管理者権限.....8
ライセンスを取得してアクティブ化する.....8

BlackBerry UEM 証明書の変更.....9
BlackBerry Dynamics 証明書の変更に関する考慮事項.....10
BlackBerry UEM 証明書の変更.....11

BlackBerry UEM を設定してプロキシサーバーを介してデータを送信する.....13
TCP プロキシサーバーを介してデータを BlackBerry Infrastructure に送信する.....13
TCP を比較する.....14
透過型 TCP プロキシサーバーを使用するように BlackBerry UEM を設定する方法.....14
TCP プロキシサーバーで SOCKS v5 を有効にする.....15
BlackBerry Router から BlackBerry Infrastructure にデータを送信する.....15
BlackBerry Router を使用するための BlackBerry UEM の設定.....16

内部プロキシサーバーによる接続の設定.....17
サーバー側のプロキシ設定の指定.....17

会社のディレクトリに接続する.....18
Exchange にリンクされたメールボックスを含む環境での Microsoft Active Directory 認証の設定.....18
Microsoft Active Directory インスタンスに接続する.....19
LDAP ディレクトリに接続する.....20
ディレクトリにリンクされたグループを有効にする.....22
オンボーディングを有効にする.....23
オンボーディングおよびオフボーディングの有効化と設定.....24
会社のディレクトリ接続を同期する.....25
同期レポートのプレビュー.....25
同期レポートの表示.....25
同期スケジュールを追加する.....26

SMTP サーバーに接続してメール通知を送信する.....27
SMTP サーバーに接続してメール通知を送信する.....27

データベースミラーリングの設定.....28
データベースミラーリングを設定する手順.....28
前提条件：データベースミラーリングを設定する.....28

ミラーデータベースを作成して設定する....29
BlackBerry UEM をミラーデータベースに接続する....29
新しいミラーデータベースを設定する....30

BlackBerry UEM の Microsoft Azure への接続....31
Microsoft Azure アカウントの作成....31
Microsoft Active Directory と Microsoft Azure の同期....31
Azure でのエンタープライズエンドポイントの作成....32

BlackBerry Infrastructure 経由での BlackBerry Web Services へのアクセスを有効にする....34

APNs 証明書を取得して iOS および macOS デバイスを管理する....35
BlackBerry 発行の署名付き CSR を取得する....35
Apple 発行の APNs 証明書を要求する....36
APNs 証明書を登録する....36
APNs 証明書を更新する....36
APNs のトラブルシューティング....37
［APNs 証明書が CSR と一致しません。適切な APNs ファイル（.pem）を指定するか新しい CSR を送信してください］....37
署名された CSR を取得しようとすると、「システムでエラーが発生しました」と表示される....37
iOS または macOS デバイスをアクティベーションできない....38

DEP 用に BlackBerry UEM を設定....39
DEP アカウントの作成....39
パブリックキーのダウンロード....39
サーバートークンの生成....40
サーバートークンを BlackBerry UEM に登録....40
最初の登録設定の追加....40
サーバートークンの更新....41
DEP 接続の削除....42

Android Enterprise デバイスをサポートするための BlackBerry UEM の設定....43
Android Enterprise デバイスをサポートするための BlackBerry UEM の設定....44
Google ドメインへの接続の削除....45
Google アカウントを使用して Google ドメイン接続を削除する....46
Google ドメイン接続の編集またはテスト....46

Windows 10 アクティベーションの簡易化....47
Windows 10 アクティベーションを簡易化するために検出サービスを導入する....47
UEM と Azure Active Directory 参加の統合....49
UEM と Azure Active Directory 参加の統合....50
Microsoft Azure での Windows Autopilot の設定....51

Azure での Windows Autopilot 導入プロファイルの作成 51
Windows Autopilot デバイスを Azure にインポートする..... 51

ソースサーバーからのユーザー、デバイス、グループ、およびその他のデータの移行..... 53
前提条件：ソースサーバーからのユーザー、デバイス、グループ、およびその他のデータの移行..... 53
ソースサーバーへの接続..... 55
Good Control サーバー用の自己署名ルート証明書をエクスポートします。..... 57
考慮事項：ソースサーバーから IT ポリシー、プロファイル、およびグループを移行する..... 58
ソースサーバーから IT ポリシー、プロファイル、およびグループを移行する..... 60
Good Control から BlackBerry UEM への完全なポリシーとプロファイルの移行..... 61
BlackBerry UEM の Good Control の機能..... 61
考慮事項：ソースサーバーからのユーザーの移行..... 63
ソースサーバーからのユーザーの移行..... 64
考慮事項：ソースサーバーからのデバイスの移行..... 65
デバイスの移行のクイックリファレンス..... 68
ソースサーバーからのデバイスの移行..... 68
DEP デバイスの移行..... 69
BlackBerry UEM Client がインストール済みの DEP デバイスの移行..... 69
BlackBerry UEM Client がインストールされていない DEP デバイスの移行..... 70

BlackBerry Dynamics アプリをサポートするための BlackBerry UEM の設定... 71
BlackBerry Proxy クラスターの管理..... 71
ポート転送を使用した Direct Connect の設定..... 72
BlackBerry Dynamics プロパティの設定..... 73
BlackBerry Dynamics グローバルプロパティ..... 73
BlackBerry Dynamics プロパティ..... 77
BlackBerry Proxy プロパティ..... 78
BlackBerry Dynamics アプリの通信設定..... 80
HTTP プロキシを介した BlackBerry Dynamics アプリデータの送信..... 80
PAC ファイルの考慮事項 80
の BlackBerry Dynamics アプリプロキシ設定の設定..... 81
BlackBerry Dynamics アプリの Kerberos の設定..... 82
ドメイン、レルム、フォレスト..... 83
前提条件..... 84
Kerberos 制約付き委任の設定..... 85
トラブルシューティングと診断..... 88
Kerberos PKINIT の設定..... 88

BlackBerry UEM と Cisco ISE を統合..... 90
要件：BlackBerry UEM と Cisco ISE の統合..... 90
Cisco ISE が使用できる管理者アカウントを作成する..... 91
BlackBerry Web Services 証明書を Cisco ISE 証明書ストアに追加します。..... 92
BlackBerry UEM を Cisco ISE に接続する..... 93
例：BlackBerry UEM の認証ポリシールール..... 94
Cisco ISE を使用したネットワークアクセスとデバイス制御の管理..... 95

BlackBerry UEM でアクティブ化されていないデバイスのリダイレクト.....96

商標などに関する情報..... 97

初めて BlackBerry UEM を設定する

次の表は、このガイドで説明する初期設定タスクの概要を示しています。この表を使用して、どの設定を実行する必要があるかを判別してください。適切なタスクを完了すると、管理者のセットアップ、ユーザーとグループの作成と管理、デバイスの制御のセットアップ、およびデバイスのアクティブ化を実行できるようになります。

タスク	説明
デフォルトの証明書を信頼済みの証明書と置き換える	さまざまな UEM コンポーネントとデバイス間の通信を認証するために BlackBerry UEM で使用されるデフォルトの自己署名証明書を置き換えることができます。
BlackBerry UEM を設定してプロキシサーバーを介してデータを送信する	BlackBerry Infrastructure に到達する前に、TCP プロキシサーバーまたは BlackBerry Router のインスタンスを介してデータを送信するように BlackBerry UEM を設定することができます。BlackBerry Dynamics NOC に到達する前に HTTP プロキシを介してデータを送信するように BlackBerry UEM を設定することもできます。
内部プロキシサーバーによる接続の構成	組織で、ネットワーク内のサーバー間の接続にプロキシサーバーを使用する場合は、サーバー側のプロキシ設定を構成し、BlackBerry UEM Core が管理コンソールのリモートインスタンスと通信できるようにする必要があります。
BlackBerry UEM を会社のディレクトリに接続する	BlackBerry UEM を 1 つ以上の会社のディレクトリ（Microsoft Active Directory や LDAP ディレクトリなど）に接続し、BlackBerry UEM がユーザーデータにアクセスしてユーザーアカウントを作成できるようにできます。
BlackBerry UEM を SMTP サーバーに接続する	BlackBerry UEM でアクティベーションメールやその他の通知をユーザーに送信するには、BlackBerry UEM が使用できる SMTP サーバー設定を指定する必要があります。
データベースミラーリングを設定する	BlackBerry UEM データベースで問題が発生した場合にデータベースサービスとデータの整合性を維持するために、プリンシパルデータベースのバックアップとして機能するフェールオーバーデータベースをインストールして設定できます。
BlackBerry UEM を Microsoft Azure に接続する	BlackBerry UEM を使用して、Microsoft Intune によって管理される iOS および Android アプリを導入する場合、または Windows 10 アプリを BlackBerry UEM で管理する場合、BlackBerry UEM を Microsoft Azure に接続します。
APNS 証明書を取得して登録する	データを管理して iOS または macOS デバイスに送信するには、BlackBerry 発行の署名付き CSR を取得し、同 CSR を使用して Apple 発行の APNs 証明書を取得し、BlackBerry UEM ドメインに APNs 証明書を登録する必要があります。
Apple の Device Enrollment Program 用 BlackBerry UEM の設定	BlackBerry UEM 管理コンソールを使って、組織が DEP 用に Apple から購入した iOS デバイスを管理したい場合は、この機能を設定する必要があります。

タスク	説明
Android Enterprise デバイスをサポートするための BlackBerry UEM の設定	Android Enterprise デバイスをサポートするには、G Suite ドメインまたは Google Cloud ドメインを設定して、サードパーティのモバイルデバイス管理プロバイダーをサポートし、G Suite ドメインまたは Google Cloud ドメインと通信するために、BlackBerry UEM を設定する必要があります。
Windows 10 アクティベーションを簡易化するためにネットワークを設定する	ユーザーがサーバーアドレスを入力しないで済むようにネットワークの設定を変更して、Windows 10 デバイスのアクティベーションプロセスを簡易化できます。
ソースサーバーからのユーザー、デバイス、グループ、およびその他のデータの移行	管理コンソールを使用して、ユーザー、デバイス、グループ、およびその他のデータをオンプレミスのソース BlackBerry UEM または Good Control （スタンドアロン）から移行できます。
BlackBerry Dynamics の設定	BlackBerry Proxy および BlackBerry Dynamics アプリに固有の設定を構成することができます。
BlackBerry UEM と Cisco ISE を統合する	Cisco ISE および BlackBerry UEM の間の接続を作成できるように、Cisco ISE は BlackBerry UEM からデバイスデータを取得し、ネットワークアクセス制御ポリシーを適用することができます。

BlackBerry UEM の設定に必要な管理者権限

このガイドの設定タスクを実行するときは、BlackBerry UEM のインストール時に作成した管理者アカウントを使用して管理コンソールにログインします。設定タスクを完了するのに複数の人員が必要な場合は、追加の管理者アカウントを作成できます。管理者アカウントの作成の詳細については、管理関連の資料を参照してください。

BlackBerry UEM を設定する管理者アカウントを作成した場合、アカウントにセキュリティ管理者ロールを割り当てる必要があります。デフォルトのセキュリティ管理者ロールは、すべての設定タスクを完了するのに必要な権限を保持しています。

ライセンスを取得してアクティブ化する

デバイスをアクティベーションするには、必要なライセンスを取得する必要があります。ライセンスの取得は、このガイドの設定手順を実行する前、さらにユーザーアカウントを追加する前に実行する必要があります。

ライセンスオプションの詳細、および各種ライセンスタイプでサポートされている機能および製品の詳細については、ライセンス関連の資料を参照してください。

BlackBerry UEM 証明書の変更

BlackBerry UEM をインストールすると、セットアップアプリケーションでさまざまな自己署名証明書が生成され、さまざまな UEM コンポーネントとデバイスの間の通信を認証するために使用されます。組織のセキュリティポリシーで組織の CA によって証明書が署名される必要がある場合、またはデバイスとブラウザーが既に信頼している CA によって発行された証明書を使用したい場合は、証明書を変更できます。

メモ： 証明書を変更するときに問題が発生した場合、UEM コンポーネント間の通信、および UEM とデバイスの間の通信が中断されます。証明書の変更を選択した場合は、変更を慎重に計画してテストします。

次の証明書を変更できます。

証明書	説明
コンソールと BlackBerry Web サービスの SSL 証明書	BlackBerry UEM 管理コンソールおよび BlackBerry UEM Self-Service がブラウザーを認証するために使用する SSL 証明書。 高可用性を設定する場合、証明書に BlackBerry UEM ドメインの名前が付いている必要があります。BlackBerry UEM ドメインの名前は、管理コンソールの［設定］>［インフラストラクチャ］>［インスタンス］で確認できます。
BlackBerry Web Services 用の SSL 証明書。	BlackBerry Web Services が、BlackBerry Web Services API を使用して BlackBerry UEM を管理するアプリケーションを認証するために使用する SSL 証明書。 高可用性を設定する場合、証明書に BlackBerry UEM ドメインの名前が付いている必要があります。BlackBerry UEM ドメインの名前は、管理コンソールの［設定］>［インフラストラクチャ］>［インスタンス］で確認できます。
Apple プロファイル署名証明書	BlackBerry UEM が、ユーザーが iOS デバイスをアクティブ化するときに受け入れる必要がある MDM プロファイルへの署名に使用する証明書。 CA によって署名された証明書を使用している場合は、アクティブ化の前に、CA のルート証明書が、ユーザーの iOS デバイスにインストールされていることを確認します。
BlackBerry Dynamics アプリ用の SSL 証明書	BlackBerry Dynamics Launcher が BlackBerry UEM とのセキュリティで保護された通信チャネルの確立に使用する SSL 証明書。統合された BlackBerry Dynamics Launcher を含む BlackBerry Dynamics アプリは、サーバーと認証するために、証明書を BlackBerry UEM に提示できます。
BlackBerry Dynamics サーバーの証明書	BlackBerry UEM と BlackBerry Proxy の間の接続を認証する SSL 証明書。
アプリケーション管理用の証明書	BlackBerry UEM と BlackBerry Dynamics アプリの認証に使用される SSL 証明書。 この証明書のルート CA 証明書は、デバイス上の信頼済み CA 証明書のリストに保存されます。サーバーがデバイスで認証されると、サーバーはこの証明書を検証のためにデバイスに提示します。 この証明書を変更し、BlackBerry UEM が証明書をすべての BlackBerry Dynamics アプリにプッシュする前に、変更が有効になる場合、証明書を受信しなかったすべてのアプリを再びアクティブ化する必要があります。

証明書	説明
Direct Connect の証明書	BlackBerry Dynamics Direct Connect と他のコンポーネントの間の認証に使用される SSL 証明書。 この証明書を変更し、BlackBerry UEM が証明書をすべての BlackBerry Dynamics アプリにプッシュする前に、変更が有効になる場合、証明書を受信しなかったすべてのアプリを再びアクティブ化する必要があります。 Direct Connect の設定方法の詳細については、「BlackBerry UEM を使用した Direct Connect の設定」を参照してください。

BlackBerry Dynamics 証明書の変更に関する考慮事項

BlackBerry Dynamics SSL 証明書のいずれかを変更する場合は、次の考慮事項に留意してください。証明書を変更するときに問題が発生した場合、BlackBerry UEM コンポーネント間の通信、および BlackBerry UEM と BlackBerry Dynamics アプリの間の通信が中断されます。証明書の変更を慎重に計画してテストします。

すべての周辺機器への新しい証明書の追加

任意の BlackBerry Dynamics 証明書をネットワーク上の周辺機器に追加した場合、BlackBerry UEM に証明書を追加する前に周辺機器に新しい証明書を追加します。

BlackBerry Dynamics アプリの更新

アプリケーション管理または Direct Connect のために BlackBerry Dynamics 証明書を置き換える場合は、証明書を置き換える前にユーザーの BlackBerry Dynamics アプリが最新のバージョンに更新されていることを確認してください。

組織で開発された BlackBerry Dynamics アプリは、BlackBerry Dynamics SDK のバージョン 3.2 以降で構築する必要があります。古いアプリは BlackBerry UEM から新しい証明書を受信できません。

証明書を受信するには、**BlackBerry Dynamics** アプリを開く必要がある

アプリが BlackBerry UEM から証明書を受信するためには、ユーザーが BlackBerry Dynamics アプリを開く必要があります。アプリケーション管理または Direct Connect のために BlackBerry Dynamics 証明書を置き換える場合に、BlackBerry UEM が証明書をすべての BlackBerry Dynamics アプリにプッシュする前に変更が有効になる場合、証明書を受信しなかったすべてのアプリを再びアクティブ化する必要があります。アプリが iOS デバイスで一時停止されているときまたは Android デバイスが Doze モードになっているときには、アプリは証明書を受信しません。

BlackBerry Connectivity Node にアクセス可能であることを確認する

BlackBerry Dynamics 証明書が置換えられるときに、BlackBerry UEM がいずれかの BlackBerry Proxy インスタンスに到達できない場合には、BlackBerry Dynamics アプリは、証明書の交換の後にこれらのインスタンスに接続することはできません。

証明書の変更を適切にスケジュールする

BlackBerry Dynamics サーバーの証明書を交換する場合は、アクティビティが少ない時間帯を選択してサーバーを再起動してください。

新しい証明書を BlackBerry Proxy および BlackBerry Dynamics アプリに伝達するために十分な時間を与えます。BlackBerry Dynamics サーバーの証明書のみを交換する場合は、サーバーを再起動する前に、少なくとも 10 分間待ってください。

アプリケーション管理または Direct Connect のために BlackBerry Dynamics 証明書を交換する場合は、有効な日付までの時間が、コンプライアンスプロファイルの接続検証の「最後の接続時刻」の設定よりも長い時間になるようにすることをお勧めします。

アプリケーション管理と Direct Connect の BlackBerry Dynamics 証明書の両方を交換する場合は、有効な時刻を 30 分以上離して設定してください。多数のユーザーと BlackBerry Dynamics アプリがある場合は、各証明書間で 30 分以上待つ必要があります。

BlackBerry UEM 証明書の変更

作業を始める前に：

- 信頼済みの CA によって署名された証明書を取得します。証明書はキーストア形式（.pfx、pkcs12）であることが必要です。
- アプリケーション管理または Direct Connect のために BlackBerry Dynamics 証明書を置き換える場合は、最初にユーザーの BlackBerry Dynamics アプリが最新のバージョンに更新されていることを確認してください。

1. メニューバーで、［設定］ > ［インフラストラクチャ］ > ［サーバー証明書］をクリックします。
2. 置き換える証明書のセクションで、［詳細を表示］をクリックします。
3. ［証明書を置換］をクリックします。
4. 証明書ファイルを参照して選択します。
5. 証明書の暗号化パスワードを入力します。
6. BlackBerry Dynamics サーバーの証明書を置き換える場合は、変更を有効にするために BlackBerry UEM を再起動するタイミングを指定します。

   サーバーを再起動するには、アクティビティが少ない時間帯を選択することをお勧めします。
7. アプリケーション管理または Direct Connect 用の BlackBerry Dynamics 証明書を置き換える場合は、証明書の変更の有効な日付を指定します。

   有効な日付は、コンプライアンスプロファイルの接続検証の「最後の接続時刻」の設定よりもかなり後の日付にすることをお勧めします。複数の証明書を変更する場合は、有効な時刻を 30 分以上離す必要があります。
8. ［置換］をクリックします。

終了したら：

- ［サーバー証明書］タブの証明書を置き換えた場合は、すべてのサーバーで BlackBerry UEM Core サービスを再起動します。サーバーを再起動するには、アクティビティが少ない時間帯を選択することをお勧めします。
- BlackBerry Dynamics 証明書タブの証明書の場合、［デフォルトに戻す］をクリックして、自己署名証明書の使用に戻すことができます。

- 自己署名証明書をそれ以上信頼する必要がない場合は、BlackBerry Dynamics 証明書タブで、［**BlackBerry UEM CA** を信頼する］および［**BlackBerry Dynamics CA** を信頼する］チェックボックスをオフにすることができます。BlackBerry Dynamics 証明書タブのすべての証明書を置き換えた場合にのみ、［**BlackBerry Dynamics CA** を信頼する］チェックボックスをオフにすることができます。
- 証明書を変更した後に BlackBerry Dynamics アプリが通信を停止した場合は、アプリが最新であることを確認してから、ユーザーにアプリの再アクティベーションを指示します。

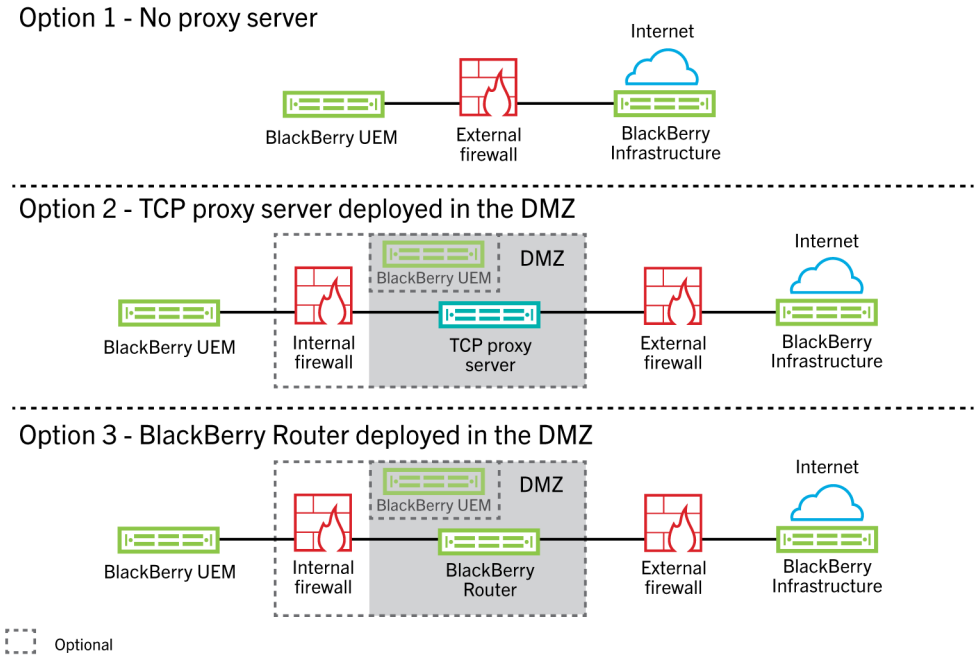
BlackBerry UEM を設定してプロキシサーバーを介してデータを送信する

BlackBerry Infrastructure に到達する前に、TCP プロキシサーバーまたは BlackBerry Router のインスタンスを介してデータを送信するように BlackBerry UEM を設定することができます。

デフォルトでは、BlackBerry UEM はポート 3101 を使用して BlackBerry Infrastructure へ直接接続します。組織のセキュリティポリシーによって、内部システムがインターネットへ直接接続できないようにすることが要求される場合は、BlackBerry Router または TCP プロキシサーバーをインストールできます。BlackBerry Router または TCP プロキシサーバーは、BlackBerry UEM と BlackBerry Infrastructure の間の仲介として動作します。

DMZ で組織のファイアウォールの外側に BlackBerry Router またはプロキシサーバーをインストールできます。DMZ に BlackBerry Router または TCP プロキシサーバーをインストールすると、BlackBerry UEM のセキュリティレベルを一段引き上げることができます。BlackBerry Router またはプロキシサーバーのみがファイアウォールの外側から BlackBerry UEM に接続します。BlackBerry Infrastructure とデバイスの間の BlackBerry UEM へのすべての接続は、BlackBerry Router またはプロキシサーバーを通過します。

この画像は、プロキシサーバーを介してデータを BlackBerry Infrastructure に送信するための、プロキシサーバーなし、TCP プロキシサーバーの DMZ への展開、および BlackBerry Router の DMZ への展開の各オプションを示しています。



TCP プロキシサーバーを介してデータを BlackBerry Infrastructure に送信する

透過型 TCP プロキシサーバーを BlackBerry UEM Core サービスに設定して、別の透過型 TCP プロキシサーバーを BlackBerry Affinity Manager サービスに設定することができます。これらのサービスにはアウトバウンド接続

が必要で、別のポートが設定されている可能性があります。サービスごとに複数の透過型 TCP プロキシサーバーをインストールまたは設定することはできません。

認証を行わずに SOCKS v5 で設定された複数の TCP プロキシサーバーを設定し、BlackBerry UEM に接続できます。認証を行わずに SOCKS v5 で設定された複数の TCP プロキシサーバーは、アクティブなプロキシサーバーの 1 つが正常に機能していない場合にサポートを提供できます。

すべての SOCKS v5 サービスインスタンスが待機する必要があるシングルポートのみを設定できます。複数の TCP プロキシサーバーを SOCKS v5 で設定している場合、各サーバーは、プロキシの待機ポートを共有する必要があります。

TCP を比較する

プロキシ	説明
透過型 TCP プロキシ	• 特別なクライアント設定を要求することなく、ネットワークレイヤーで通常の通信を検出します。 • クライアントブラウザーの設定が必要ありません。 • 通常、クライアントとインターネットの間に配置されます。 • ゲートウェイまたはルーターの機能の一部を実行します。 • 許容可能な使用ポリシーの強制によく使用されます。 • 一部の国では一般に ISP によって使用され、アップストリーム帯域を保存し、キャッシングを介して顧客の応答時間を改善します。
SOCKS v5 プロキシ	• プロキシサーバーを介してインターネットトラフィックを処理するインターネットプロトコルです。 • ブラウザーや SOCKS をサポートする FTP クライアントなど、ほぼすべての TCP/UDP アプリケーションで扱うことができます。 • インターネットで匿名性とセキュリティを確保するのに適したソリューションとなります。 • クライアントとサーバーの間でプロキシサーバーを経由してネットワークパケットをルーティングします。 • 認証されたユーザーのみにアクセスが許可されるように、認証を提供できます。 • 任意の IP アドレスへのプロキシ TCP 接続です。 • HTTP のように UDP プロトコルや TCP プロトコルを匿名化できます。

透過型 TCP プロキシサーバーを使用するように BlackBerry UEM を設定する方法

作業を始める前に： 互換性のある透過型 TCP プロキシサーバーを BlackBerry UEM ドメインにインストールします。

1. メニューバーで、［設定］ > ［インフラストラクチャ］ > ［**BlackBerry Router** とプロキシ］をクリックします。
2. ［プロキシサーバー］オプションを選択します。
3. 次のタスクを実行します。

タスク	手順
TCP プロキシサーバー経由での TCP データのルーティング	［**BlackBerry UEM Core**］、［**BlackBerry Secure Gateway Service**］フィールドに、プロキシサーバーの FQDN または IP アドレスおよびポート番号を入力します。各フィールドには 1 つの値が必要です。
TCP プロキシサーバー経由での SRP トラフィックのルーティング	［**Affinity Manager**］フィールドに、プロキシサーバーの FQDN または IP アドレスおよびポート番号を入力します。各フィールドには 1 つの値が必要です。
TCP プロキシサーバー経由での BlackBerry Secure Connect Plus トラフィックのルーティング	［**BlackBerry Secure Connect Plus**］フィールドに、プロキシサーバーの FQDN または IP アドレスおよびポート番号を入力します。各フィールドには 1 つの値が必要です。

4. ［保存］をクリックします。

TCP プロキシサーバーで SOCKS v5 を有効にする

作業を始める前に： SOCKS v5（認証なし）と互換性のある TCP プロキシサーバーを BlackBerry UEM ドメインにインストールします。

1. メニューバーで、［設定］ > ［インフラストラクチャ］ > ［**BlackBerry Router** とプロキシ］をクリックします。
2. ［プロキシサーバー］オプションを選択します。
3. ［**SOCKS v5** を有効にする］チェックボックスをオンにします。
4. ＋ をクリックします。
5. ［サーバーアドレス］フィールドに、SOCKS v5 プロキシサーバーの IP アドレスまたはホスト名を入力します。
6. ［追加］をクリックします。
7. 設定する SOCKS v5 プロキシサーバーそれぞれに対して手順 1～6 を繰り返します。
8. ［ポート］フィールドにポート番号を入力します。
9. ［保存］をクリックします。

BlackBerry Router から BlackBerry Infrastructure にデータを送信する

可用性を高めるために複数の BlackBerry Router インスタンスを設定できます。BlackBerry Router インスタンスに待機用のポートを 1 つだけ設定します。

BlackBerry UEM は、BlackBerry Router で元々使用されていた BES5 インスタンスをサポートしていません。

デフォルトでは、BlackBerry UEM は、ポート 3102 を使用して BlackBerry Router に接続して BlackBerry UEM サービスに接続し、ポート 3101 を使用して BES5 サービスに接続します。BlackBerry Router は、BlackBerry UEM Core および BlackBerry Affinity Manager からのすべての発信トラフィックをサポートしています。

メモ： BlackBerry Router でデフォルト以外のポートを使用する場合は、support.blackberry.com/community にアクセスして、記事 36385 を参照してください。

BlackBerry Router を使用するための BlackBerry UEM の設定

作業を始める前に： BlackBerry UEM ドメインに BlackBerry Router をインストールします。BlackBerry Router のインストールの詳細については、インストールおよびアップグレード関連の資料を参照してください。

1. メニューバーで、［設定］ > ［インフラストラクチャ］ > ［**BlackBerry Router** とプロキシ］をクリックします。
2. ［**BlackBerry Router**］オプションを選択します。
3. ＋ をクリックします。
4. BlackBerry UEM に接続する BlackBerry Router インスタンスの IP アドレスまたはホスト名を入力します。
5. ［追加］をクリックします。
6. 設定する BlackBerry Router インスタンスそれぞれに対して手順 1～5 を繰り返します。
7. ［ポート］フィールドに、すべての BlackBerry Router インスタンスが待機するポート番号を入力します。デフォルト値は 3102 です。
8. ［保存］をクリックします。

内部プロキシサーバーによる接続の設定

組織で、ネットワーク内のサーバー間の接続にプロキシサーバーを使用する場合は、サーバー側のプロキシ設定を構成し、BlackBerry UEM Core が BlackBerry UEM 管理コンソールと通信できるようにする必要があります（別のコンピューターにインストールされている場合）。また、場合によっては、認証機関や、データを BlackBerry MDS Connection Service にプッシュするプッシュアプリケーションをホストしているサーバーなどの他の内部サービスと BlackBerry UEM が通信できるように、サーバー側のプロキシを設定する必要があります。

サーバー側のプロキシ設定は、アウトバウンド接続には適用されません。BlackBerry UEM で TCP プロキシサーバーを使用するための設定の詳細については、「BlackBerry UEM を設定してプロキシサーバーを介してデータを送信する」を参照してください。

サーバー側のプロキシ設定の指定

作業を始める前に： PAC URL またはホスト名とポート番号、およびプロキシサーバーに接続するために必要なその他の設定を確認してください。

1. メニューバーで、［設定］ > ［インフラストラクチャ］ > ［サーバー側のプロキシ］をクリックします。
2. BlackBerry UEM インストールの一部である多くのサーバーまたはすべてのサーバーがプロキシサーバーに接続する必要がある場合は、次の操作を実行して、グローバルサーバー側のプロキシ設定を設定します。
   a) ［グローバルサーバー側のプロキシ設定］の［タイプ］リストで［**PAC** 設定］または［手動設定］を選択します。
   b) プロキシサーバーで必要な設定を指定し、［保存］をクリックします。
3. 1 つまたは複数のサーバーにグローバル設定と異なるプロキシ設定が必要な場合は、次の操作を実行して、サーバーのプロキシ設定を設定します。
   a) サーバー名の［タイプ］リストで、［なし］、［**PAC** 設定］、または［手動設定］を選択します。
   b) ［**PAC** 設定］または［手動設定］を選択した場合は、プロキシサーバーに必要な設定を指定します。
   c) ［保存］をクリックします。

会社のディレクトリに接続する

BlackBerry UEM を会社のディレクトリに接続すると、組織のユーザーのリストにアクセスできるようにできます。BlackBerry UEM を複数のディレクトリに接続できます。ディレクトリは、Microsoft Active Directory と LDAP の両方の組み合わせにすることができます。

会社のディレクトリが接続されている場合は、次の機能を利用することができます。

- ディレクトリからユーザーデータを使用して BlackBerry UEM にユーザーアカウントを作成でき、BlackBerry UEM は管理コンソールの管理者と BlackBerry UEM Self-Service のユーザーを認証できます。
- 会社のディレクトリグループを BlackBerry UEM グループにリンクして、会社のディレクトリと同じ編成方法で、BlackBerry UEM のユーザーを編成することができます。「ディレクトリにリンクされたグループを有効にする」を参照してください。
- 会社のディレクトリで特定のグループのオンボーディングを有効にし、BlackBerry UEM ユーザーを自動的に作成することができます。オンボーディングを有効にすると、ユーザーが会社のディレクトリのグループから削除されたときに、デバイスデータまたはユーザーアカウントを削除するようにオフボーディングを設定することもできます。「オンボーディングを有効にする」を参照してください。

BlackBerry UEM を会社のディレクトリに接続しない場合は、手動でローカルユーザーアカウントを作成し、デフォルト認証を使用して管理者を認証できます。

BlackBerry UEM を会社のディレクトリに接続するには、次の操作を実行します。

手順	アクション
1	Microsoft Active Directory インスタンスまたは LDAP ディレクトリに対して接続を作成します。 環境にリソースフォレストが含まれている場合、「Exchange にリンクされたメールボックスを含む環境での Microsoft Active Directory 認証の設定」を参照してください。
2	オプションで、ディレクトリにリンクされたグループを有効にします。
3	オプションで、オンボーディングを有効にします。
4	オプションで、同期スケジュールを追加します。

Exchange にリンクされたメールボックスを含む環境での Microsoft Active Directory 認証の設定

リソースフォレストモデルでは、Microsoft Exchange サーバーは 1 つのフォレスト（リソースフォレスト）に配置され、個々のユーザーアカウントはアカウントフォレストに配置されます。Microsoft Exchange のみを実行しているリソースフォレストを含む組織の環境では、信頼済みのアカウントフォレスト内にあるユーザーアカウントの Microsoft Active Directory 認証を設定できます。

Exchange リソースフォレストが組織の環境に存在する場合は、そのリソースフォレストに接続するように BlackBerry UEM を設定する必要があります。各ユーザーアカウントのリソースフォレストにメールボックスを作成し、これらのメールボックスをユーザーアカウントに関連付ける必要があります。リソースフォレストのメールボックスとアカウントフォレストのユーザーアカウントを関連付けると、ユーザーアカウントはメールボックスにフルアクセスが可能となり、アカウントフォレストのユーザーアカウントは Microsoft Exchange サーバーに接続されます。BlackBerry UEM は、メールボックスを使用して、個々のドメインのユーザアカウントを検索します。

BlackBerry UEM にログインするユーザーを認証するには、BlackBerry UEM リソースフォレストの一部であるグローバルカタログサーバーに保存されるユーザー情報を読む必要があります。リソースフォレストの一部である Windows ドメインに置かれている BlackBerry UEM の Microsoft Active Directory アカウントを作成する必要があります。ディレクトリ接続を作成するときには、Microsoft Active Directory アカウントの Windows ドメイン、ユーザー名、およびパスワード、そして必要に応じて BlackBerry UEM が使用できるグローバルカタログサーバーの名前を提供します。

詳細については、technet.microsoft.com にアクセスして「リンクされたメールボックスの管理」を参照してください。

Microsoft Active Directory インスタンスに接続する

作業を始める前に： BlackBerry UEM が使用できる Microsoft Active Directory アカウントを作成します。アカウントは、以下の要件を満たす必要があります。

- Microsoft Exchange フォレストの一部である Windows ドメインに配置されていることが必要です。
- ユーザーコンテナにアクセスし、Microsoft Exchange フォレストのグローバルカタログサーバーのユーザーオブジェクトを読み取る権限を持つ必要があります。
- パスワードは、有効期限が切れないように設定し、次回のログイン時に変更する必要がないようにする必要があります。
- シングルサインオンを有効にする場合は、アカウントに制約付き委任を設定する必要があります。
- UEM サーバーも Active Directory ドメインに参加している必要があります。

1. メニューバーで、［設定］ > ［外部統合］ > ［会社のディレクトリ］をクリックします。
2. ［**Microsoft Active Director** 接続を追加］をクリックします。
3. ［ディレクトリ接続名］フィールドに、ディレクトリ接続の名前を入力します。
4. ［ユーザー名］フィールドに、Microsoft Active Directory アカウントのユーザー名を入力します。
5. ［ドメイン］フィールドに、Microsoft Exchange フォレストの一部である Windows ドメインの名前を DNS 形式（たとえば、example.com）で入力します。
6. ［パスワード］フィールドにアカウントのパスワードを入力します。
7. ［**Kerberos** キー配布センターの選択］ドロップダウンリストで、次のいずれかの操作を実行します。
   - BlackBerry UEM でキー配布センター（KDC）を自動的に検出することを許可するには、［自動］をクリックします。
   - BlackBerry UEM で認証に使用する KDC のリストを指定するには、［手動］をクリックします。［サーバー名］フィールドに、DNS 形式で KDC ドメインコントローラーの名前を入力します（例：kdc01.example.com）。必要に応じて、ドメインコントローラーが使用するポート番号（例：kdc01.example.com:88）を入力します。＋ をクリックし、BlackBerry UEM で使用する追加の KDC ドメインコントローラーを指定します。
8. ［グローバルカタログの選択］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。

- BlackBerry UEM でグローバルカタログサーバーを自動的に検出する場合、［自動］をクリックします。
- BlackBerry UEM で使用するグローバルカタログサーバーのリストを指定するには、［手動］をクリックします。［サーバー名］フィールドで、BlackBerry UEM がアクセスするグローバルカタログサーバーの DNS 名を入力します（例：globalcatalog01.example.com）。必要に応じて、グローバルカタログサーバーが使用するポート番号 （例：globalcatalog01.com:3268）を入力します。＋ をクリックして、追加のサーバーを指定します。

9. ［続行］をクリックします。
10. ［グローバルカタログ検索ベース］フィールドで、次の操作のいずれかを実行します。
    - BlackBerry UEM でグローバルカタログ全体の検索を許可するには、フィールドを空白にしておきます。
    - BlackBerry UEM が認証することのできるユーザーアカウントを制御するには、ユーザーコンテナ（例：OU=sales,DC=example,DC=com）の識別名を入力します。
11. グローバルグループのサポートを有効にする場合は、［グローバルグループのサポート］ドロップダウンリストで［はい］をクリックします。

    オンボーディングにグローバルグループを使用する場合は、［はい］を選択する必要があります。グローバルグループドメインを設定するには、［グローバルグループドメインのリスト］セクションで、＋ をクリックします。［ドメイン］フィールドで、追加するドメインを選択します。［ユーザー名とパスワードを指定しますか］フィールドのデフォルトの選択は「いいえ」です。このデフォルトを選択すると、フォレスト接続のユーザー名とパスワードが使用されます。［はい］を選択した場合は、選択したドメインの Microsoft Active Directory アカウントの有効な資格情報を入力する必要があります。［**KDC** の選択］フィールドで、［自動］を選択して、BlackBerry UEM でキー配布センターを自動的に検出するか、または［手動］を選択して、BlackBerry UEM で認証に使用する KDC のリストを指定することができます。［追加］をクリックします。
12. 環境に Microsoft Exchange リソースフォレストが含まれている場合、リンクされている Microsoft Exchange メールボックスのサポートを有効にするには、［リンクされた **Microsoft Exchange** メールボックスのサポート］ドロップダウンリストで、［はい］をクリックします。

    BlackBerry UEM でアクセスするフォレストごとに Microsoft Active Directory アカウントを設定するには、［アカウントフォレストのリスト］セクションで ＋ をクリックします。ユーザーのドメイン名（ユーザーはアカウントフォレスト内のドメインに属している場合があります）とユーザー名とパスワードを指定します。必要に応じて、BlackBerry UEM で検索する KDC を指定します。必要に応じて、BlackBerry UEM でアクセスするグローバルカタログサーバーを指定します。［追加］をクリックします。
13. シングルサインオンを有効にするには、［**Windows** シングルサインオンを有効にする］チェックボックスをオンにします。シングルサインオンの詳細については、「管理関連の資料」を参照してください。シングルサインオンは、オンプレミス環境でのみサポートされます。
14. 会社のディレクトリからユーザーの詳細情報を同期するには、［追加のユーザーの詳細を同期］チェックボックスをオンにします。追加の詳細には、会社名とオフィスの電話番号が含まれます。
15. ［保存］をクリックします。
16. ［閉じる］をクリックします。

終了したら： ディレクトリ同期スケジュールを追加する場合は、「同期スケジュールを追加する」を参照してください。

LDAP ディレクトリに接続する

作業を始める前に：

- 関連する LDAP ディレクトリに配置された BlackBerry UEM の LDAP アカウントを作成します。アカウントは、以下の要件を満たす必要があります。
  - アカウントが、ディレクトリ内のすべてのユーザーを読み取る権限を持つ。
  - アカウントのパスワードが期限切れにならず、次回のログインでユーザーがパスワードの変更を求められない。
- LDAP 接続が SSL 暗号化されている場合は、LDAP 接続のサーバー証明書があること、および LDAP サーバーが TLS 1.2 をサポートしていることを確認します。SSL が有効な場合、BlackBerry UEM への LDAP 接続は TLS 1.2 を使用する必要があります。
- 組織で使用する LDAP 属性値を確認します（以下の手順では、一般的な属性値の例を示します）。手順 11 以降で LDAP 属性値を指定する必要があります。

1. メニューバーで、［設定］ > ［外部統合］ > ［会社のディレクトリ］をクリックします。
2. ［**LDAP** 接続を追加］をクリックします。
3. ［ディレクトリ接続名］フィールドに、ディレクトリ接続の名前を入力します。
4. ［**LDAP** サーバー検出］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。
   - 自動的に LDAP サーバーを検出するには、［自動］をクリックします。［**DNS** ドメイン名］フィールドで、会社のディレクトリをホストするサーバーのドメイン名を入力します。
   - LDAP サーバーのリストを指定するには、［以下のリストからサーバーを選択］をクリックします。［**LDAP** サーバー］フィールドで、LDAP サーバーの名前を入力します。LDAP サーバーを追加するには、＋ をクリックします。
5. ［**SSL** を有効にする］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。
   - LDAP 接続が SSL 暗号化されている場合は、［はい］をクリックします。［**LDAP** サーバーの **SSL** 証明書］フィールドの横にある［参照］をクリックし、LDAP サーバーの証明書を選択します。
   - LDAP 接続が SSL 暗号化されていない場合は、［いいえ］をクリックします。
6. ［**LDAP** ポート］フィールドに、通信の TCP ポート番号を入力します。デフォルト値は、SSL が有効な場合は 636、SSL が無効な場合は 389 です。
7. ［認証が必須］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。
   - 接続に認証が必要な場合は、［はい］をクリックします。［ログイン］フィールドで、LDAP へのログインが認証されているユーザーの DN を入力します（例：an=admin,o=Org1）。［パスワード］フィールドにパスワードを入力します。
   - 接続に認証が必要ない場合、［いいえ］をクリックします。
8. ［ユーザー検索ベース］フィールドに、ユーザー情報の検索でベース DN として使用する値を入力します。
9. ［**LDAP** ユーザー検索フィルター］フィールドに、組織のディレクトリサーバーでユーザーオブジェクトを検索するのに必要な LDAP 検索フィルターを入力します。たとえば、IBM Domino Directory の場合、`(objectClass=Person)` を入力します。

   メモ：検索結果から無効なユーザーアカウントを除外するには、`(&(objectclass=user)(logindisabled=false))` を入力します。
10. ［**LDAP** ユーザー検索範囲］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。
    - ベースオブジェクトに続くすべてのオブジェクトを検索するには、［すべてのレベル］をクリックします。これがデフォルト設定です。
    - ベース DN から直接続く 1 レベルのオブジェクトを検索するには、［**1** レベル］をクリックします。
11. ［固有 **ID**］フィールドに、組織の LDAP ディレクトリの各ユーザーを個別に識別する属性名を入力します（不変でグローバルに一意な文字列であることが必要です）。たとえば、IBM Domino LDAP 7 以降では、`dominoUNID` です。

12. ［名］フィールドに、各ユーザーの名の属性を入力します（たとえば、givenName）。
13. ［姓］フィールドに、各ユーザーの姓の属性を入力します（たとえば、sn）。
14. ［ログイン属性］フィールドに、認証のためのユーザーのログイン属性を入力します（たとえば、uid）。
15. ［メールアドレス］フィールドに、各ユーザーのメールアドレスの属性を入力します（たとえば、mail）。値を設定しない場合、デフォルト値が使用されます。
16. ［表示名］フィールドに、各ユーザーの表示名の属性を入力します（たとえば、displayName）。値を設定しない場合、デフォルト値が使用されます。
17. ［メールプロファイルのアカウント名］フィールドに、各ユーザーのメールプロファイルのアカウント名の属性を入力します（たとえば、mail）。
18. ［ユーザープリンシパル名］フィールドに、SCEP のユーザープリンシパル名を入力します（たとえば、mail）。
19. ディレクトリ接続のディレクトリにリンクされたグループを有効にするには、［ディレクトリにリンクされたグループを有効にする］チェックボックスをオンにします。

    以下の情報を指定します。

    - ［グループ検索ベース］フィールドに、グループ情報の検索でベース DN として使用する値を入力します。
    - ［**LDAP** グループ検索フィルター］フィールドに、会社のディレクトリでグループオブジェクトを検索するのに必要な LDAP 検索フィルターを入力します。たとえば、IBM Domino Directory の場合、(objectClass=dominoGroup) を入力します。
    - ［グループ固有 **ID**］フィールドに、各グループの固有 ID の属性を入力します。この属性は、不変でグローバルに一意であることが必要です（たとえば、cn を入力）。
    - ［グループの表示名］フィールドに、各グループの表示名の属性を入力します（たとえば、cn を入力）。
    - ［グループメンバーシップの属性］フィールドに、各グループのメンバーシップ ID の属性を入力します。この属性は、不変でグローバルに一意であることが必要です（たとえば、member を入力）。
    - ［テストグループ名］フィールドに、指定したグループ属性を検証するための既存のグループ名を入力します。
20. ［保存］をクリックします。
21. ［閉じる］をクリックします。

終了したら： ディレクトリ同期スケジュールを追加する場合は、「同期スケジュールを追加する」を参照してください。

ディレクトリにリンクされたグループを有効にする

作業を始める前に： 会社のディレクトリの同期が進行中でないことを確認します。会社のディレクトリ接続に加えた変更は、同期が完了するまで保存できません。

1. メニューバーで、［設定］ > ［外部統合］ > ［会社のディレクトリ］をクリックします。
2. 編集する会社のディレクトリ名をクリックします。
3. ［同期設定］タブで［ディレクトリにリンクされたグループを有効にする］チェックボックスをオンにします。
4. 会社のディレクトリグループの同期を強制するには、［同期を強制する］チェックボックスをオンにします。

   選択した場合、グループが会社のディレクトリから削除されたときに、そのグループへのリンクが、ディレクトリにリンクされているグループおよびオンボーディングディレクトリグループから削除されます。ディ

レクトリにリンクされているグループに関連付けられているすべての会社のディレクトリグループが削除された場合、ディレクトリにリンクされているグループはローカルグループに変換されます。選択されていない場合で会社のディレクトリグループが見つからない場合、同期プロセスがキャンセルされます。

5. ［同期制限］フィールドで、各同期プロセスで許可する変更の最大数を入力します。

   デフォルト設定は 5 です。同期する変更の数が同期制限を超えている場合は、同期プロセスが実行されないようにすることができます。変更は、グループに追加するユーザー、グループから削除するユーザー、オンボーディングされるユーザー、オフボーディングされるユーザーを加算することで計算されます。

6. ［ディレクトリグループの最大ネストレベル］フィールドに、会社のディレクトリグループの同期するネストレベルの数を入力します。
7. ［保存］をクリックします。

終了したら： ディレクトリにリンクされたグループを作成します。詳細については、管理関連の資料を参照してください。

オンボーディングを有効にする

オンボーディングにより、ユニバーサルまたはグローバルな会社のディレクトリグループのユーザーメンバーシップに基づいて BlackBerry UEM に自動的にユーザーアカウントを追加できます。ユーザーアカウントは同期処理中に BlackBerry UEM に追加されます。

また、オンボーディングされたユーザーに、メールメッセージとアクティベーションパスワードまたは BlackBerry Dynamics アプリのアクセスキーを自動的に送信するように選択することもできます。

オフボーディング

オンボーディングを有効にする場合は、オフボーディングを設定することもできます。ユーザーがオンボードディレクトリグループですべての会社ディレクトリグループから削除された場合、BlackBerry UEM は、次のいずれかの方法でユーザーを自動的にオフボーディングすることができます。

- ユーザーのデバイスから作業データまたはすべてのデータを削除する
- BlackBerry UEM からユーザーアカウントを削除する

オフボーディング保護を使用すると、1 つの同期サイクル分だけデバイスデータまたはユーザーアカウントの削除を遅延させ、ディレクトリレプリケーションの遅延のための予期しない削除を回避できます。同期の間隔にかかわらず、オフボーディング保護の遅延には最低 2 時間が必要です。

メモ： オフボーディング設定は、BlackBerry UEM の既存のディレクトリユーザーにも適用されます。プレビューアイコンをクリックして、ディレクトリ同期レポートを生成し、変更内容を確認することをお勧めします。

同期

オフボーディングを有効にした後は、次の同期の実行中に、オフボーディングがオンになる前に管理コンソールで手動で追加したユーザーでかつオンボーディングディレクトリにリンクされているグループのメンバーになっていないすべてのユーザーにオフボーディングルールが適用されます。

オンボーディングを有効にした後で、ユーザーがディレクトリにリンクされているグループに既に存在している場合でも、ユーザーを手動で BlackBerry UEM に追加することができます。オフボーディングが有効になっている場合、BlackBerry UEM に手動で追加したユーザーについては、ユーザーが同期のときにオンボーディング同

期グループのメンバーになっていない場合、次の同期が発生したときにユーザーのデバイスにオフボーディングルールが適用されます。

オンボーディングおよびオフボーディングの有効化と設定

ユニバーサルグループおよびグローバルグループのメンバーであるユーザーを自動的にオンボーディングできます。ドメインローカルグループでは、オンボーディングはサポートされていません。

作業を始める前に：

- 会社のディレクトリの同期が進行中でないことを確認します。会社のディレクトリ接続に加えた変更は、同期が完了するまで保存できません。
- グローバルグループのメンバーをオンボードするには、Microsoft Active Directory 接続設定でグローバルグループのサポートを有効にする必要があります。

1. メニューバーで、［設定］ > ［外部統合］ > ［会社のディレクトリ］をクリックします。
2. 編集する会社のディレクトリ名をクリックします。
3. ［同期設定］タブで［ディレクトリにリンクされたグループを有効にする］チェックボックスをオンにします。
4. ［オンボーディングを有効にする］チェックボックスをオンにします。
5. デバイスアクティベーションオプションを使用してオンボーディングを設定するグループごとに、次のアクションを実行します。
   a) ＋ をクリックします。
   b) 会社のディレクトリグループの名前を入力します。🔍 をクリックします。
   c) グループを選択します。［追加］をクリックします。
   d) 必要な場合は、［ネストされたグループをリンク］を選択します。
   e) ［デバイスのアクティベーション］セクションで、ユーザーが自動生成されたアクティベーションパスワードを受け取るか、またはアクティベーションパスワードを受け取らないかを選択します。自動生成されたパスワードのオプションを選択した場合は、アクティベーション期間を設定し、アクティベーションメールテンプレートを選択します。
6. BlackBerry Dynamics でユーザーをオンボードするには、［**BlackBerry Dynamics** アプリのみを使用してユーザーをオンボードする］チェックボックスをオンにします。
7. BlackBerry Dynamics アプリのみのアクティベーションを使用してオンボードする各グループに対して次の操作を実行します。
   a) ＋ をクリックします。
   b) 会社のディレクトリグループの名前を入力します。🔍 をクリックします。
   c) グループを選択します。［追加］をクリックします。
   d) 必要な場合は、［ネストされたグループをリンク］を選択します。
   e) 追加するユーザーごとに生成するアクセスキーの数、アクセスキーの有効期限、およびメールテンプレートを選択します。
8. ユーザーがオフボードされた場合にデバイスデータを削除するには、［ユーザーがすべてのオンボーディングディレクトリグループから削除されたらデバイスデータを削除する］チェックボックスをオンにします。次のオプションのいずれかを選択します。
   - 仕事用データのみを削除
   - すべてのデバイスデータを削除
   - 会社所有の全デバイスデータを削除/個人所有の仕事用データのみを削除

9. ユーザーがすべてのオンボーディンググループから削除されたときに BlackBerry UEM からユーザーアカウントを削除するには、［ユーザーがすべてのオンボーディングディレクトリグループから削除されたらユーザーを削除する］を選択します。ユーザーアカウントがすべてのオンボーディングディレクトリグループから削除された後に初めて同期サイクルが発生したときに、ユーザーアカウントが BlackBerry UEM から削除されます。
10. ユーザーアカウントまたはデバイスデータが BlackBerry UEM から予期せず削除されないようにするには、［オフボーディング保護］を選択します。

    オフボーディング保護とは、次の同期サイクルの 2 時間後までユーザーが BlackBerry UEM から削除されないことを意味します。
11. 会社のディレクトリグループの同期を強制するには、［同期を強制する］チェックボックスをオンにします。

    選択した場合、グループが会社のディレクトリから削除されたときに、そのグループへのリンクが、オンボーディングディレクトリグループおよびディレクトリにリンクされているグループから削除されます。選択されていない場合で会社のディレクトリグループが見つからない場合、同期プロセスがキャンセルされます。
12. ［同期制限］フィールドで、各同期プロセスで許可する変更の最大数を入力します。デフォルトの設定は 5 です。

    同期する変更の数が同期制限を超えている場合は、同期プロセスが実行されないようにすることができます。変更は、グループに追加するユーザー、グループから削除するユーザー、オンボーディングされるユーザー、オフボーディングされるユーザーを加算することで計算されます。
13. ［ディレクトリグループの最大ネストレベル］フィールドに、会社のディレクトリグループの同期するネストレベルの数を入力します。
14. ［保存］をクリックします。

会社のディレクトリ接続を同期する

作業を始める前に： 同期レポートのプレビュー

1. メニューバーで、［設定］ > ［外部統合］ > ［会社のディレクトリ］をクリックします。
2. ［同期］列で、をクリックします。

終了したら： 同期レポートの表示

同期レポートのプレビュー

同期レポートをプレビューすると、同期化が行われる前に予定されている更新が、予想される更新であることを確認できます。

1. メニューバーで、［設定］ > ［外部統合］ > ［会社のディレクトリ］をクリックします。
2. ［プレビュー］列で をクリックします。
3. ［今すぐプレビュー］をクリックします。
4. レポートの処理が終了したら、［最終レポート］列の日付をクリックします。
5. 以前に生成された同期レポートを表示するには、ドロップダウンメニューをクリックします。

同期レポートの表示

1. メニューバーで、［設定］ > ［外部統合］ > ［会社のディレクトリ］をクリックします。

2. ［最終レポート］列で、日付をクリックします。
3. 以前に生成された同期レポートを表示するには、ドロップダウンメニューをクリックします。

同期スケジュールを追加する

同期スケジュールを追加して、BlackBerry UEM を組織の会社のディレクトリと自動的に同期することができます。同期スケジュールには、次の 3 種類があります。

- 間隔：各同期の間隔の長さ、時間フレーム、およびそれが発生する日を指定します。
- 1 日 1 回：同期が開始される時刻と、それが発生する日を指定します。
- 繰り返しなし：1 度限りの同期の日時を指定します。

［会社のディレクトリ］画面では、いつでも手動で BlackBerry UEM と会社のディレクトリを同期できます。

1. メニューバーで、［設定］ > ［外部統合］ > ［会社のディレクトリ］をクリックします。
2. 編集する会社のディレクトリグループをクリックします。
3. ［同期スケジュール］タブで、＋ をクリックします。
4. 同期する情報の量を減らすには、［同期タイプ］ドロップダウンリストで、次のいずれかのオプションを選択します。
   - ［すべてのグループとユーザー］：これはデフォルト設定です。このオプションを選択すると、ユーザーは同期中にオンボーディングおよびオフボーディングされ、適切なディレクトリにリンクされたグループにリンクされます。オンボーディングまたはオフボーディングされていないが、ディレクトリにリンクされたグループを変更したユーザーと、属性に変更があったユーザーは同期されます。
   - ［オンボーディンググループ］：このオプションを選択すると、ユーザーは同期中にオンボーディングおよびオフボーディングされ、適切なディレクトリにリンクされたグループにリンクされます。属性に変更があったユーザーは同期されます。オンボーディングまたはオフボーディングされていないが、ディレクトリにリンクされたグループを変更したユーザーは同期されません。
   - ［ディレクトリにリンクされたグループ］：このオプションを選択すると、ユーザーは同期中にオンボーディングおよびオフボーディングされません。ディレクトリにリンクされたグループに変更があったユーザーは適切にリンクされます。属性に変更があったユーザーは同期されます。
   - ［ユーザー属性］：このオプションを選択すると、ユーザーは同期中にオンボーディングおよびオフボーディングされません。ディレクトリにリンクされたグループに変更があったユーザーは同期されません。属性に変更があったユーザーは同期されます。
5. ［繰り返し］ドロップダウンリストで、次のいずれかのオプションを選択します。

オプション	手順
間隔	**a.** ［間隔］フィールドに、同期の間隔を分単位で入力します。 **b.** 同期の時間フレームを指定します。 **c.** 同期を実行する曜日を選択します。
1日1回	**a.** 同期を開始する時刻を指定します。 **b.** 同期を実行する曜日を選択します。
繰り返しなし	**a.** 同期を開始する時刻を指定します。 **b.** 同期を開始する日を選択します。

6. ［追加］をクリックします。

SMTP サーバーに接続してメール通知を送信する

BlackBerry UEM にメール通知の送信を許可するには、BlackBerry UEM を SMTP サーバーに接続する必要があります。

BlackBerry UEM はメール通知を使用してアクティベーションの手順をユーザーに送信します。管理者は、BlackBerry UEM を設定して BlackBerry UEM Self-Service のパスワードとデバイスコンプライアンスの警告を送信し、個別にメールを送信することもできます。

BlackBerry UEM SMTP サーバーに接続しない場合、BlackBerry UEM はパスワード、アクティベーションメッセージ、またはメールを送信できません。管理者は BlackBerry UEM コンプライアンス警告をデバイスに直接送信できます。

アクティベーションメッセージ、デバイスコンプライアンスの警告、およびメールの個別送信の詳細については、管理関連の資料を参照してください。

SMTP サーバーに接続してメール通知を送信する

1. メニューバーで、［設定］ > ［外部統合］ > ［**SMTP** サーバー］をクリックします。
2. ✎ をクリックします。
3. ［送信者の表示名］フィールドに、BlackBerry UEM メール通知で使用する名前を入力します。たとえば、`donotreply` や `BUEM Admin` などです。
4. ［送信者アドレス］フィールドに、メール通知の送信で BlackBerry UEM が使用するメールアドレスを入力します。
5. ［**SMTP** サーバー］フィールドに、SMTP サーバーの FQDN を入力します。たとえば、`mail.example.com` などです。
6. ［**SMTP** サーバーポート］フィールドに、SMTP サーバーのポート番号を入力します。デフォルトのポート番号は 25 です。
7. ［サポートされている暗号化の種類］ドロップダウンメニューで、メール通知適用する暗号化の種類を選択します。
8. SMTP サーバーが認証を要求する場合、［ユーザー名］フィールドに SMTP サーバーのログイン名を入力します。［パスワード］フィールドに SMTP サーバーのパスワードを入力します。
9. 必要に応じて SMTP CA 証明書をインポートします。
   a) 組織の SMTP サーバーの SSL 証明書ファイルを使用しているコンピューターにコピーします。
   b) ［参照］をクリックします。
   c) SSL 証明書ファイルを参照し、［アップロード］をクリックします。
10. ［保存］をクリックします。

終了したら： SMTP サーバーへの接続をテストする場合は［テスト接続］をクリックし、テストメールを送信します。BlackBerry UEM が、［送信者アドレス］フィールドに指定したメールアドレスにメッセージを送信します。

データベースミラーリングの設定

データベースミラーリングを使用して、BlackBerry UEM データベースで高可用性を実現することができます。データベースミラーリングは、BlackBerry UEM データベースで問題が発生した場合にデータベースサービスとデータの整合性を維持できる Microsoft SQL Server 機能です。データベースミラーリングを使用する方法の詳細については、計画関連の資料を参照してください。

メモ：Microsoft は、Microsoft SQL Server の将来のバージョンでデータベースミラーリングを廃止する予定であるため、AlwaysOn 機能を使用して高可用性データベースを設定することを推奨しています。AlwaysOn を使用するには、設定手順を実行してから BlackBerry UEM をインストールする必要があります。AlwaysOn を使用する方法の詳細については、計画関連の資料を参照してください。

データベースミラーリングを設定する手順

データベースミラーリングを設定するには、次の操作を実行します。

手順	アクション
1	計画関連の資料の要件を確認し、BlackBerry UEM ドメインが前提条件を満たしていることを確認します。
2	ミラーデータベースを作成してミラーリングセッションを開始し、ウィットネスサーバーをセットアップします。
3	各 BlackBerry UEM インスタンスを設定してミラーデータベースに接続します。

前提条件：データベースミラーリングを設定する

- プリンシパルサーバーを設定してサーバーをミラーリングし、リモートコンピューターからのアクセスを許可します。
- プリンシパルサーバーを設定してサーバーをミラーリングし、権限を同じにします。
- プリンシパルサーバーを監視するのに使用するウィットネスサーバーをセットアップします。
- Microsoft SQL Server Agent を設定し、BlackBerry UEM サービスを実行している Windows アカウントと同じ権限に設定されたローカル管理権限を持つドメインユーザーアカウントを使用します。
- ドメインユーザーアカウントにプリンシパルサーバーとミラーサーバーの両方の権限があることを確認します。
- DNS サーバーが稼動していることを確認します。
- BlackBerry UEM データベースインスタンスをホストする各コンピューターの SQL Server 2012 Native Client で、［名前付きパイプ］オプションをオフにします。［名前付きパイプ］オプションをオフにしない場合は、https://support.blackberry.com/community にアクセスし、記事 34373 を参照してください。
- 組織の Microsoft SQL Server のバージョンの追加前提条件については、technet.microsoft.com/sqlserver にアクセスし、「データベース ミラーリング (SQL Server 2012)」または「データベース ミラーリング (SQL Server 2014)」を参照してください。

- ミラーデータベースがデフォルトのインスタンスを使用する場合は、BlackBerry UEM コンポーネントはカスタム静的ポートではなく、デフォルトポートの 1433 のみを使用してミラーデータベースに接続できます。これは、Microsoft SQL Server 2005 以降の制限によるものです。この問題の詳細については、「SQL 2005 JDBC ドライバーおよびデータベースミラーリング」を参照してください。

ミラーデータベースを作成して設定する

作業を始める前に： ミラーデータベースを作成して設定する際にデータベースの整合性を維持するには、BlackBerry UEM インスタンスをホストするすべてのコンピューターで BlackBerry UEM サービスを停止します。

1. Microsoft SQL Server Management Studio で、プリンシパルデータベースを参照します。
2. ［復旧モデル］プロパティを［**FULL**］に変更します。
3. クエリエディターで、**-- ALTER DATABASE** *<BUEM_db>* **SET TRUSTWORTHY ON** クエリを実行します。*<BUEM_db>* は、プリンシパルデータベースの名前です。
4. プリンシパルデータベースのバックアップを作成します。［バックアップの種類］オプションを［完全］に変更します。
5. バックアップファイルをミラーサーバーにコピーします。
6. ミラーサーバーで、データベースを復元してミラーデータベースを作成します。データベースを復元する際は、［復旧なし］オプションを選択します。
7. ミラーデータベースの名前が、プリンシパルデータベースの名前と一致することを確認します。
8. Microsoft SQL Server Management Studio のプリンシパルサーバーで、プリンシパルデータベースを右クリックし、［ミラー］タスクを選択します。［ミラーリング］ページで、［セキュリティの構成］をクリックして［データベースミラーリングセキュリティの構成］ウィザードを起動します。
9. ミラーリング処理を開始します。詳細については、『データベースミラーリングのセットアップ – SQL サーバー 2012』または『データベースミラーリングのセットアップ – SQL サーバー 2014』を参照してください。
10. 自動フェールオーバーを有効化するには、ミラーリングセッションにウィットネスを追加します。詳細については、『データベースミラーリングウィットネス – SQL サーバー 2012』または『データベースミラーリングウィットネス – SQL サーバー 2014』を参照してください。

終了したら：

- フェールオーバーが適切に機能することを確認するには、サービスを手動でミラーデータベースにフェールオーバーさせ、プリンシパルデータベースに戻します。
- BlackBerry UEM インスタンスをホストする各コンピューターで、BlackBerry UEM サービスを再起動します。BlackBerry UEM - BlackBerry Work Connect Notification Service を停止してから再度開始しないでください。このサービスは BlackBerry UEM - BlackBerry Affinity Manager サービスの再起動時に、自動的に再起動されます。
- BlackBerry UEM をミラーデータベースに接続する。

BlackBerry UEM をミラーデータベースに接続する

このタスクは、BlackBerry UEM インスタンスをホストするすべてのコンピューターで繰り返します。コンピューターで BlackBerry UEM コンポーネントのみが BlackBerry Router の場合、同コンピューターでこのタスクを実行する必要はありません。

作業を始める前に：

- ミラーデータベースを作成して設定する。
- ミラーサーバーが稼動していることを確認します。
- このタスクを完了するには、BlackBerry UEM 設定ツールを使用するか、以下の手順を使用してデータベースのプロパティファイルを手動で更新することができます。BlackBerry UEM 設定ツールを使用する場合は、support.blackberry.com/community にアクセスして、記事 KB36443 を参照してください。「BlackBerry UEM データベースのプロパティの更新」セクションで、指示に従って SQL ミラーリングを有効にし、ミラーサーバーの FQDN を提供します。

1. BlackBerry UEM インスタンスをホストするコンピューターで、*<drive>*:\Program Files\BlackBerry\UEM\common-settings に移動します。
2. テキストエディターで **DB.properties** を開きます。
3. ［フェールオーバーを使用するためのオプション設定］セクションで、**configuration.database.ng.failover.server=** の後にミラーサーバーの FQDN を入力します（例：`configuration.database.ng.failover.server=mirror_server.domain.net`）。
4. 必要に応じて、次の操作のいずれかを実行します。
   - インストール時にプリンシパルデータベースに名前付きインスタンスを指定した状態で、ミラーデータベースがデフォルトのインスタンスを使用する場合は、**configuration.database.ng.failover.instance=** の後の値を削除します。
   - プリンシパルデータベースがデフォルトのインスタンスを使用し、ミラーデータベースが名前付きインスタンスを使用する場合は、**configuration.database.ng.failover.instance=** の後に名前付きインスタンスを入力します。
5. 保存して **DB.properties** を閉じます。

終了したら：

- BlackBerry UEM サービスを再起動します。BlackBerry UEM - BlackBerry Work Connect Notification Service を停止してから再度開始しないでください。このサービスは BlackBerry UEM - BlackBerry Affinity Manager サービスの再起動時に、自動的に再起動されます。
- BlackBerry UEM インスタンスをホストする各コンピューターでこのタスクを繰り返します。
- BlackBerry UEM インスタンスをホストする各コンピューターがサーバーの省略名を使用してミラーサーバーに接続できることを確認します。

新しいミラーデータベースを設定する

ロールスイッチが発生した（BlackBerry UEM コンポーネントが既存のミラーデータベースにフェールオーバーし、既存のミラーデータベースがプリンシパルデータベースになった）後に新しいミラーデータベースを作成して設定する場合は、BlackBerry UEM インスタンスをホストする各コンピューターで BlackBerry UEM をミラーデータベースに接続する を繰り返します。

BlackBerry UEM の Microsoft Azure への接続

Microsoft Azure は、アプリケーションとサービスの導入および管理に使用する Microsoft クラウドコンピューティングサービスです。BlackBerry UEM を使用して、Microsoft Intune によって管理される iOS および Android アプリを導入する場合、または Windows 10 アプリを BlackBerry UEM で管理する場合、BlackBerry UEM を Azure に接続する必要があります。

BlackBerry UEM は、1 つの Azure テナントのみの構成をサポートします。BlackBerry UEM を Azure に接続するには、次の操作を実行します。

手順	アクション
1	Microsoft Azure アカウントの作成.
2	Microsoft Active Directory と Microsoft Azure の同期.
3	Azure でのエンタープライズエンドポイントの作成.
4	BlackBerry UEM を設定して、Microsoft Intune および Windows Store for Business と同期します。

Microsoft Azure アカウントの作成

Microsoft Intune によって保護されているアプリを iOS および Android デバイスに導入するか、Windows 10 アプリを BlackBerry UEM で管理するには、Microsoft Azure アカウントを所有し、Azure で BlackBerry UEM に認証する必要があります。

組織に Microsoft Azure アカウントがない場合は、このタスクを完了してください。

メモ： Microsoft Intune の正しいライセンスとアカウント権限を取得していることを確認するには、support.blackberry.com/community にアクセスし、記事 50341 を参照してください。

1. https://azure.microsoft.com にアクセスし、［無料アカウント］をクリックして、画面の指示に従ってアカウントを作成します。

   アカウントを作成するには、クレジットカード情報を提供する必要があります。
2. https://portal.azure.com の Azure 管理ポータルにサインインし、サインアップしたときに作成したユーザー名とパスワードでログインします。

終了したら： Microsoft Active Directory と Microsoft Azure の同期.

Microsoft Active Directory と Microsoft Azure の同期

Windows 10 ユーザーがオンラインアプリをインストールしたり、Microsoft Intune で保護されているアプリを iOS および Android デバイスに送信できるようにするには、ユーザーが Microsoft Azure Active Directory

に存在している必要があります。ユーザーがオンプレミスの Active Directory と Azure Active Directory の間で、Microsoft Azure Active Directory Connect を使用してユーザーとグループを同期する必要があります。詳細については、https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect にアクセスしてください。

作業を始める前に： Microsoft Azure アカウントの作成

1. Azure AD Connect を http://www.microsoft.com/en-us/download/details.aspx?id=47594 からダウンロードします。
2. Azure AD Connect ソフトウェアをインストールします。
3. オンプレミスの Active Directory と Azure Active Directory に接続するように、Azure AD Connect を設定します。

終了したら： Azure でのエンタープライズエンドポイントの作成

Azure でのエンタープライズエンドポイントの作成

Microsoft Azure への BlackBerry UEM アクセスを提供するには、Azure 内にエンタープライズエンドポイントを作成する必要があります。エンタープライズエンドポイントを使用して、BlackBerry UEM が Microsoft Azure に認証できます。詳細については、https://docs.microsoft.com/en-us/azure/active-directory/active-directory-app-registration を参照してください。

BlackBerry UEM を Microsoft Intune と Windows Store for Business の両方に接続している場合は、権限の違いと将来の変更の可能性があるため、それぞれの目的に別のエンタープライズアプリケーションを使用してください。

作業を始める前に：

- Microsoft Active Directory と Microsoft Azure の同期
- モダン認証を使用する場合は、返信 URL があることを確認してください。モダン認証用に返信 URL を取得する手順については、「BlackBerry UEM を設定し Microsoft Intune と同期する」を参照してください。

1. Azure ポータルにログインします。
2. ［**Microsoft Azure**］ > ［**Azure Active Directory**］ > ［アプリの登録］に移動します。
3. ［エンドポイント］をクリックします。
4. ［**OAuth 2.0** トークンエンドポイント（**v1**）］値をコピーし、テキストファイルに貼り付けます。

   これは、BlackBerry UEM で必要な **OAuth 2.0** トークンエンドポイントです。
5. ［エンドポイント］のリストを閉じ、［新しい登録］をクリックします。
6. ［名前］フィールドに、アプリの名前を入力します。
7. アプリケーションを使用するか、API にアクセスできるアカウントタイプを選択します。
8. ［リダイレクト **URI**］セクションのドロップダウンリストで、［**Web**］を選択し、有効な URL を入力します。URL の形式は、https://<*FQDN_of_the_BlackBerry_UEM_server*>:<*port*>/admin/intuneauth です。
   - クライアント資格情報認証を使用するか、登録されたドメインがない場合は、`http://localhost/` を使用できます。
   - モダン認証を使用する場合は、BlackBerry UEM から返信 URL を入力します。手順については、「BlackBerry UEM を設定し Microsoft Intune と同期する」を参照してください。
9. ［登録］をクリックします。
10. アプリケーションのアプリケーション **ID** をコピーし、テキストファイルに貼り付けます。

これは、BlackBerry UEM で必要なクライアント **ID** です。

11. Microsoft Intune を使用するアプリケーションを作成する場合、［管理］セクションの［**API** のアクセス許可］をクリックします。次のタスクを実行します。
    a) ［アクセス許可の追加］をクリックします。
    b) ［**Microsoft Graph**］を選択します。
    c) ［デリゲートされたアクセス許可］を選択します。
    d) アクセス許可リストを下にスクロールし、［委任されたアクセス許可］の下で、Microsoft Intune の次の権限を設定します。
        - Microsoft Intune アプリの読み取りと書き込み（［**DeviceManagementApps**］ **>** ［**DeviceManagementApps.ReadWrite.All**］）
        - すべてのグループの読み取り（［グループ］ **>** ［**Group.Read.All**］）
        - すべてのユーザーの基本プロファイルの読み取り（［ユーザー］ **>** ［**User.ReadBasic.All**］）
    e) ［アクセス許可の追加］をクリックします。
    f) ［同意する］で、［管理者の同意の付与］をクリックします。

        メモ：権限を付与するには、グローバル管理者になっている必要があります。
    g) メッセージが表示されたら、［はい］をクリックして、現在のディレクトリのすべてのアカウントの権限を付与します。

    Windows Store for Business に接続するアプリを作成する場合は、デフォルトの権限を使用することができます。
12. ［管理］セクションの［証明書およびシークレット］をクリックします。次の操作を実行します。
    a) ［クライアントシークレット］で、［新しいクライアントシークレット］をクリックします。
    b) クライアントシークレットの説明を入力します。
    c) クライアントシークレットの期間を選択します。
    d) ［追加］をクリックします。
    e) 新しいクライアントシークレットの値をコピーします。

        これは、BlackBerry UEM で必要なクライアントキーです。

        警告：この時点でキーの値をコピーしない場合は、この画面を終了した後に値が表示されないため、新しいキーを作成する必要があります。

終了したら： BlackBerry UEM を設定し Microsoft Intune と同期する
または、BlackBerry UEM を設定し Windows Store for Business と同期する

BlackBerry Infrastructure 経由での BlackBerry Web Services へのアクセスを有効にする

組織で組織のファイアウォールの外側にある Web サービスクライアントを使用していて、クライアントが BlackBerry Web Services API（REST またはレガシー SOAP）へのアクセスを必要とする場合、クライアントは BlackBerry Infrastructure 経由で API に安全に接続できます。クライアントアプリでこのアクセスを有効にする方法の詳細については、BlackBerry Web Services REST API リファレンスの「はじめに」セクションを参照してください。

Web サービスクライアントは、管理コンソールでこのアクセスを有効にした場合にのみ BlackBerry Infrastructure を使用して BlackBerry Web Services API にアクセスできます。デフォルトでは、このアクセスは有効になっていません。

1. メニューバーで［設定］ > ［一般設定］ > ［**BlackBerry Web Services** アクセス］をクリックします。
2. ［有効］をクリックします。
3. ［保存］をクリックします。

APNs 証明書を取得して iOS および macOS デバイスを管理する

APNs は、Apple プッシュ通知サービスです。BlackBerry UEM を使用して iOS または macOS デバイスを管理するには、APNs 証明書を取得して登録する必要があります。複数の BlackBerry UEM ドメインを設定する場合、各ドメインで APNs 証明書が必要になります。

APNs 証明書の取得と登録は、初回ログインウィザードで実行するか、管理コンソールの［外部統合］セクションで実行することができます。

メモ： 各 APNs 証明書は 1 年間有効です。管理コンソールは、有効期限を表示します。期限が切れる前に、証明書の取得時に使用したものと同じ Apple ID を使用して、APNs 証明書を更新する必要があります。管理コンソールで Apple ID を確認できます。期限切れの 30 日前に証明書の更新を通知するように、メールイベント通知を作成することもできます。証明書の期限が切れると、デバイスは BlackBerry UEM からデータを受信しなくなります。新しい APNs 証明書を登録した場合、デバイスユーザーはデバイスを再度アクティブ化してデータを受信する必要があります。

詳細については、https://developer.apple.com にアクセスし、記事 TN2265 の『*Issues with Sending Push Notifications*』を参照してください。

Google Chrome ブラウザーまたは Safari ブラウザーを使用して、管理コンソールと Apple プッシュ証明書ポータルにアクセスすることをお勧めします。これらのブラウザーでは、APNs 証明書の要求と登録に最適なサポートが用意されています。

APNs 証明書を取得および登録するには、次の操作を実行します。

手順	アクション
1	BlackBerry 発行の署名付き CSR を取得します。
2	署名付き CSR を使用して Apple 発行の APNs 証明書を要求します。
3	APNs 証明書を登録します。

BlackBerry 発行の署名付き CSR を取得する

APN 証明書を取得するには、先に BlackBerry 発行の署名付き CSR を取得する必要があります。

1. メニューバーで、［設定］ > ［外部統合］ > ［**Apple** プッシュ通知］をクリックします。
2. APN 証明書がまだない場合、［手順 **1/3 - BlackBerry** 発行の署名付き **CSR** 証明書をダウンロード］セクションで、［証明書をダウンロード］をクリックします。

   現在の APN 証明書を更新する場合は、代わりに［証明書を更新］をクリックします。
3. ［保存］をクリックして署名付き CSR ファイル（.scsr）をコンピューターに保存します。

終了したら： Apple 発行の APNs 証明書を要求する.

Apple 発行の APNs 証明書を要求する

作業を始める前に： BlackBerry 発行の署名付き CSR を取得する.

1. メニューバーで、［設定］ > ［外部統合］ > ［**Apple** プッシュ通知］をクリックします。
2. ［手順 **2/3 - Apple** 発行の **APNs** 証明書を要求］セクションで、［**Apple** プッシュ証明書ポータル］をクリックします。Apple プッシュ証明書ポータルが表示されます。
3. 有効な Apple ID を使用して、Apple プッシュ証明書ポータルにサインインします。
4. 指示に従って署名付き CSR（.scsr）をアップロードします。
5. コンピューターに APNs 証明書をダウンロードおよび保存します。
6. （オプション） をクリックして［メモ］ウィンドウを表示します。
7. ［メモ］ウィンドウで、APNs 証明書を要求するために使用した Apple ID を入力します。

   証明書を更新するには、同じ Apple ID を使用する必要があります。
8. ［メモ］ウィンドウの外側をクリックして閉じます。

終了したら： APNs 証明書を登録する.

APNs 証明書を登録する

作業を始める前に： Apple 発行の APNs 証明書を要求する.

1. メニューバーで、［設定］ > ［外部統合］ > ［**Apple** プッシュ通知］をクリックします。
2. ［手順 **3/3 - APNs** 証明書を登録］セクションで、［参照］をクリックします。移動して APNs 証明書（.pem）を選択します。
3. ［送信］をクリックします。

終了したら： BlackBerry UEM と APN サーバー間の接続をテストするには、［**APN** 証明書をテスト］をクリックします。

APNs 証明書を更新する

APNs 証明書は 1 年間有効です。管理者は、有効期限が切れる前に APNs 証明書を更新する必要があります。証明書は、元の APN 証明書を取得するために使用したものと同じ Apple ID を使用して更新する必要があります。

期限切れの 30 日前に証明書の更新を通知するように、メールイベント通知を作成することができます。

作業を始める前に： BlackBerry 発行の署名付き CSR を取得する.

1. メニューバーで、［設定］ > ［外部統合］ > ［**Apple** プッシュ通知］をクリックします。
2. ［証明書を更新］をクリックします。
3. ［手順 **1/3 - BlackBerry** 発行の署名付き **CSR** 証明書をダウンロード］セクションで、［証明書をダウンロード］をクリックします。
4. ［保存］をクリックして署名付き CSR ファイル（.scsr）をコンピューターに保存します。
5. ［手順 **2/3 - Apple** 発行の **APNs** 証明書を要求］セクションで、［**Apple** プッシュ証明書ポータル］をクリックします。Apple プッシュ証明書ポータルが表示されます。

6. 元の APN 証明書の取得時に使用したものと同じ Apple ID を使用して Apple プッシュ証明書ポータルにサインインします。
7. 指示に従って APNs 証明書（.pem）を取得します。新しい署名付き CSR をアップロードする必要があります。
8. 更新された APNs 証明書をコンピューターにダウンロードおよび保存します。
9. ［手順 **3/3 - APNs** 証明書を登録］セクションで、［参照］をクリックします。移動して更新された APNs 証明書を選択します。
10. ［送信］をクリックします。

終了したら： BlackBerry UEM と APN サーバー間の接続をテストするには、［**APN** 証明書をテスト］をクリックします。

APNs のトラブルシューティング

このセクションは、APNs の問題をトラブルシューティングするために役立ちます。

［APNs 証明書が CSR と一致しません。適切な APNs ファイル（.pem）を指定するか新しい CSR を送信してください］

説明

BlackBerry 発行の最新の署名付き CSR ファイルを Apple プッシュ認証ポータルにアップロードしなかった場合、APNs 証明書を登録する際にエラーメッセージを受信することがあります。

解決策

BlackBerry 発行の CSR ファイルを複数ダウンロードした場合、最後にダウンロードした CSR のみが有効です。どの CSR が最新のものかわかっている場合は、Apple プッシュ証明書ポータルに戻って同 CSR をアップロードします。どの CSR が最新のものかわかっていない場合は、BlackBerry から新しい CSR を取得し、Apple プッシュ証明書ポータルに戻って同 CSR をアップロードします。

署名された CSR を取得しようとすると、「システムでエラーが発生しました」と表示される

説明

署名された CSR を取得しようとすると、以下のエラーが発生します。「システムでエラーが発生しました。やり直してください」

解決策

https://support.blackberry.com/community/s/article/37266 にアクセスして、記事 37266 を参照してください。

iOS または macOS デバイスをアクティベーションできない

考えられる原因

iOS または macOS デバイスをアクティベーションできない場合、APN 証明書が正しく登録されていない可能性があります。

解決策

次の操作を 1 つ以上実行します。

- 管理コンソールのメニューバーで、［設定］ > ［外部統合］ > ［**Apple** プッシュ通知］をクリックします。APN 証明書のステータスが［インストール済み］であることを確認します。ステータスが正しくない場合は、APN 証明書の再登録を試みます。
- ［**APNs** 証明書をテスト］をクリックし、BlackBerry UEM と APNs サーバーの間の接続をテストします。
- 必要に応じて、BlackBerry 発行の新しい署名付き CSR と新しい APNs 証明書を取得します。

DEP 用に BlackBerry UEM を設定

BlackBerry UEM を Apple の Device Enrollment Program と同期する前に、DEP を使用できるように BlackBerry UEM を設定する必要があります。BlackBerry UEM を設定すると、BlackBerry UEM 管理コンソールを使用して、組織が DEP 用に購入した iOS デバイスのアクティベーションを管理できます。

Apple Business Manager アカウントを使用して BlackBerry UEM を DEP と同期できます。Apple Business Manager は Web ベースのポータルで、 DEP で iOS デバイスを登録および管理したり、 Apple Vpp アカウントを管理したりできます。組織で DEP または VPP を使用している場合は、Apple Business Manager にアップグレードできます。

BlackBerry UEM の Device Enrollment Program 用に Apple を設定するには、次の操作を実行します。

手順	アクション
1	DEP アカウントの作成.
2	パブリックキーのダウンロード.
3	サーバートークンの生成.
4	サーバートークンを BlackBerry UEM に登録.
5	最初の登録設定の追加.

DEP アカウントの作成

1. メニューバーで、［設定］ > ［外部統合］ > ［**Apple Device Enrollment Program**］をクリックします。
2. ＋ をクリックします。
3. ［名前］フィールドに、アカウントの名前を入力します。
4. ［手順 **1/4**：**Apple DEP** アカウントを作成］で、［**Apple DEP** アカウントを追加］をクリックします。
5. フィールドを入力し、プロンプトに従ってアカウントを作成します。

終了したら： パブリックキーのダウンロード.

パブリックキーのダウンロード

作業を始める前に： DEP アカウントの作成.

1. メニューバーで、［設定］ > ［外部統合］ > ［**Apple Device Enrollment Program**］をクリックします。
2. ＋ をクリックします。

3. ［手順 **2/4**：パブリックキーをダウンロード］で、［パブリックキーをダウンロード］をクリックします。
4. ［保存］をクリックします。

終了したら： サーバートークンの生成.

サーバートークンの生成

作業を始める前に： パブリックキーのダウンロード.

1. メニューバーで、［設定］ > ［外部統合］ > ［**Apple Device Enrollment Program**］をクリックします。
2. ＋ をクリックします。
3. ［手順 **3/4**：**Apple DEP** アカウントからサーバートークンを生成］で、［**Apple DEP** ポータルを開く］をクリックします。
4. DEP アカウントにサインインします。
5. プロンプトに従って、サーバートークンを生成します。

終了したら： サーバートークンを BlackBerry UEM に登録.

サーバートークンを BlackBerry UEM に登録

BlackBerry UEM は、Apple の Device Enrollment Program と通信する際に、認証にサーバートークンを使用します。

作業を始める前に： サーバートークンの生成.

1. メニューバーで、［設定］ > ［外部統合］ > ［**Apple Device Enrollment Program**］をクリックします。
2. ＋ をクリックします。
3. ［手順 **4/4**：サーバートークンを **BlackBerry UEM** に登録］で、［参照］をクリックします。
4. **.p7m** サーバートークンファイルを選択します。
5. ［開く］をクリックします。
6. ［次へ］をクリックします。

終了したら： 最初の登録設定の追加.

最初の登録設定の追加

作業を始める前に： サーバートークンを BlackBerry UEM に登録 最初の登録設定を追加する前に実行します。

サーバートークンを登録後、最初の登録設定を追加するウィンドウが自動的に BlackBerry UEM に表示されます。

1. 設定の名前を入力します。
2. 次のタスクのいずれかを実行します。
   - 登録設定を Apple のデバイス登録プログラムで登録するときに、BlackBerry UEM で登録設定をデバイスに自動的に割り当てる場合は、［すべての新しいデバイスをこの設定に自動的に割り当てる］チェックボックスをオンにします。

- BlackBerry UEM コンソールを使用して、登録設定を特定のデバイスに手動で割り当てる場合は、［すべての新しいデバイスをこの設定に自動的に割り当てる］チェックボックスをオフにします。

3. セットアップ時には、オプションでデバイスに表示する部門名とサポート電話番号を入力します。
4. ［デバイス設定］セクションで、次のチェックボックスを選択します。
   - ペアリングを許可する：オンの場合、ユーザーはデバイスとコンピューターをペアリングできます。
   - 管理モードを有効にする：オンの場合、デバイスは管理モードで有効になります。少なくとも［管理モードを有効にする］と［MDM プロファイルの削除を許可］のどちらか一方を選択する必要があります。
   - 必須 - 選択した場合、ユーザーは、会社のディレクトリのユーザー名とパスワードを使用してデバイスをアクティブにすることができます。
   - MDM プロファイルの削除を許可：オンの場合、ユーザーはデバイスを無効にできます。少なくとも［管理モードを有効にする］と［MDM プロファイルの削除を許可］のどちらか一方を選択する必要があります。
   - デバイスが設定されるまで待機する：オンの場合、BlackBerry UEM でのアクティベーションが完了するまでデバイスのセットアップをキャンセルできません。この設定は、［管理モードを有効にする］を選択した場合のみ有効です。
5. ［セットアップ時にスキップ］セクションでは、デバイスのセットアップに含めない項目を選択します。
   - パスコード - オンの場合、デバイスのパスコード作成を求めるプロンプトは表示されません。
   - 位置情報サービス - オンの場合、デバイスで位置情報サービスが無効になります。
   - 復元 - オンの場合、ユーザーはバックアップファイルからデータを復元できません。
   - Android から移動 - 選択した場合、Android デバイスからデータを復元することはできません。
   - Apple ID - オンの場合、ユーザーは Apple ID と iCloud にサインインできません。
   - 使用条件 - オンの場合、ユーザーには iOS の使用条件が表示されません。
   - Siri - 選択した場合、Siri はデバイスで無効になっています。
   - 診断 - オンの場合、診断情報はセットアップ時にデバイスから自動的に送信されません。
   - バイオメトリック - 選択した場合、ユーザーはタッチ ID を設定できません。
   - 支払い - オンの場合、ユーザーは Apple Pay を設定できません。
   - ズーム - 選択した場合、ユーザーはズームを設定できません。
   - ホームボタンのセットアップ - オンの場合、ユーザーはホームボタンのクリックを調整できません。
   - 画面時間 - 選択した場合、DEP の登録時に画面時間をセットアップするオプションがスキップされます。
   - ソフトウェア更新 - 選択した場合、必須のソフトウェア更新画面がデバイスに表示されません。
   - iMessage と Face Time - 選択した場合、iMessage と Face Time 画面がデバイスに表示されません。
6. ［保存］をクリックします。

   メッセージ「エラーが発生しました。サーバーのトークンファイルを復号化できませんでした」が表示された場合、support.blackberry.com/community にアクセスして、記事 37282 を参照してください。
7. ［新しいデバイスをこの設定に自動的に割り当てる］を選択した場合は、［はい］をクリックします。

終了したら： iOS デバイスをアクティベーションします。DEP に登録されているデバイスのアクティブ化の詳細については、「管理関連の資料」を参照してください。

サーバートークンの更新

サーバートークンは 1 年間有効です。管理者は有効期限が切れる前に、トークンを更新する必要があります。トークンのステータスを確認するには、［Apple Device Enrollment Program］ウィンドウで［有効期限の日付］を確認します。

作業を始める前に： パブリックキーが変更された場合は、新しいパブリックキーをダウンロードします。

1. メニューバーで、［設定］ > ［外部統合］ > ［**Apple Device Enrollment Program**］をクリックします。
2. DEP アカウントの名前をクリックします。
3. ［有効期限の日付］セクションで、［サーバートークンを更新］をクリックします。
4. ［手順 **1/2**：**Apple DEP** アカウントからサーバートークンを生成］で、［**Apple DEP** ポータルを開く］をクリックします。
5. DEP のアカウントにサインインします。
6. プロンプトに従って、サーバートークンを生成します。
7. ［手順 **2/2**：サーバートークンを **BlackBerry UEM** に登録］で、［参照］をクリックします。
8. **.p7m** サーバートークンファイルを選択します。
9. ［開く］をクリックします。
10. ［保存］をクリックします。

DEP 接続の削除

注意： すべての DEP 接続を削除する場合は、Apple の Device Enrollment Program で新しい iOS デバイスをアクティベーションできません。登録設定をデバイスに割り当て済みで、設定が適用されていない場合は、BlackBerry UEM はデバイスに割り当てられた登録設定を削除します。接続を削除しても、BlackBerry UEM でアクティブになっているデバイスには影響がありません。

組織が DEP を使用する iOS デバイスの導入をやめた場合は、DEP への BlackBerry UEM 接続を削除できます。

1. メニューバーで、［設定］ > ［外部統合］ > ［**Apple Device Enrollment Program**］をクリックします。
2. DEP アカウントの名前をクリックします。
3. ［**DEP** 接続を削除］ をクリックします。
4. ［削除］をクリックします。
5. ［**OK**］をクリックします。

Android Enterprise デバイスをサポートするための BlackBerry UEM の設定

Android Enterprise デバイスは、Android デバイスを管理することを望む組織に、強化されたセキュリティを提供します。Android Enterprise デバイスの詳細については、https://support.google.com/work/android/ を参照してください。

Android Enterprise デバイスをサポートするための BlackBerry UEM の設定の詳細な手順については、support.blackberry.com/community にアクセスし、記事 37748 を参照してください。

Android Enterprise デバイスをサポートするように BlackBerry UEM を設定する方法は 2 つあります。

1. Google Cloud ドメインまたは G Suite ドメインへ BlackBerry UEM を接続します。

   メモ：1 つの BlackBerry UEM ドメインのみを Google ドメインに接続できます。
2. BlackBerry UEM が管理 Google Play アカウントを持つ Android Enterprise デバイスを管理することを許可します。このオプションを使用するために、Google ドメインは必要ありません。詳細については、https://support.google.com/googleplay/work/ を参照してください。

次の表に、Android Enterprise デバイスを設定するためのさまざまなオプションをまとめています。

Android Enterprise デバイスをサポートするように **BlackBerry UEM** を設定する方法	この方法を選択する状況	ユーザーアカウントタイプ	サポートされる **Google** サービス
BlackBerry UEM ドメインへ G Suite を接続する	組織に G Suite ドメインがある	G Suite アカウント（組織用）	Gmail、Google Calendar、Drive などのすべての G Suite サービスをサポートします。 Google Play では、アプリ管理をサポートします。
BlackBerry UEM ドメインへ Google Cloud を接続する	組織に Google Cloud ドメインがある	Google Cloud アカウント（管理 Google アカウントとも呼ばれます）（組織用）	G Suite と同様ですが、Gmail、Google Calendar、Drive などの有料製品にはアクセスできません。 Google Play では、アプリ管理をサポートします。

Android Enterprise デバイスをサポートするように **BlackBerry UEM** を設定する方法	この方法を選択する状況	ユーザーアカウントタイプ	サポートされる **Google** サービス
BlackBerry UEM が管理 Google Play アカウントとして Android Enterprise デバイスを管理することを許可する	組織に Google ドメインがない または 1 つの BlackBerry UEM ドメインに接続されている Google ドメインがあり、Android Enterprise デバイスを 2 つ目の BlackBerry UEM ドメインで使用したい。	管理 Google Play アカウントを持つ Android Enterprise デバイス	Google Play では、アプリ管理をサポートします。 Google サービスはサポートされていません。

Android Enterprise デバイスをサポートするための BlackBerry UEM の設定

1 つの BlackBerry UEM ドメインのみを Google ドメインに接続できます。別の BlackBerry UEM ドメインに接続する前に、既存の接続を削除する必要があります。「Google ドメインへの接続の削除」を参照してください。

1. メニューバーで、［設定］ > ［外部統合］ > ［**Android** エンタープライズ］をクリックします。
2. 次のタスクのいずれかを実行します。

タスク	手順
管理 Google Play アカウントを持つ Android Enterprise デバイスを使用する	**a.** ［**BlackBerry UEM** での **Google Play** アカウントの管理を許可する］を選択します。 **b.** ［次へ］をクリックします。 **c.** ［**Android** で作業する］ウィンドウで、Google アカウントを使用してサインインします。任意の Google または Gmail アカウントを使用することができます。使用するアカウントは［**Android** で作業する］サービスの管理者アカウントになります。 **d.** ［開始］をクリックします。 **e.** 組織の名前を入力します。［確認］をクリックします。 **f.** ［登録を完了］をクリックします。BlackBerry UEM 管理コンソールに戻ります。

タスク	手順
Google ドメインを使用する	**a.** ［**BlackBerry UEM** を既存の **Google** ドメインに接続する］を選択します。 **b.** ［次へ］をクリックします。 **c.** サービスアカウントを作成するためのフィールドに入力し、［次へ］をクリックします。手順については、support.blackberry.com/community にアクセスして、記事 37748 を参照してください。

3. デバイスにアプリの設定を送信する方法を指定します。アプリ設定に追加した情報は、BlackBerry Infrastructureを使用して提供することも、Google インフラストラクチャを使用して提供することもできます。次の操作のいずれかを実行します。
   - アプリ設定の詳細を BlackBerry Infrastructureを使用して送信するには、［**UEM Client** を使用してアプリ設定を送信する］を選択します。
   - アプリ設定の詳細を Google インフラストラクチャを使用して送信するには、［**Google Play** を使用してアプリ設定を送信する］を選択します。
4. メッセージが表示されたら、［承諾］をクリックして、次のアプリの一部またはすべてに設定された権限を受け入れます。
   - Google Chrome
   - BlackBerry Connectivity
   - BlackBerry Hub + サービス
   - BlackBerry Hub
   - BlackBerry カレンダー
   - BlackBerry 連絡先
   - BlackBerry メモ
   - BlackBerry タスク
5. ［完了］をクリックします。

終了したら： Android Enterprise デバイスをアクティブ化する手順を完了します。デバイスのアクティベーションの詳細については、管理関連の資料の「デバイスアクティベーション」を参照してください。

Google ドメインへの接続の削除

Google Cloud ドメインまたは G Suite ドメインに接続できるのは、1 つの BlackBerry UEM ドメインのみです。別の BlackBerry UEM ドメインに接続する前に、既存の接続を削除する必要があります。

次の作業を完了する前に、Google ドメインへの接続を削除します。

- BlackBerry UEM ドメインを廃棄する
- 別の BlackBerry UEM インスタンスを Google Cloud または G Suite ドメインに接続する

Google ドメインへの接続を削除しないと、Google Cloud または G Suite ドメインを新しい BlackBerry UEM インスタンスに接続できなくなることがあります。BlackBerry UEM の接続を削除した場合、Android Enterprise アクティベーションタイプでアクティブ化されたすべてのデバイスが非アクティブ化されます。

1. メニューバーで、［設定］ > ［外部統合］をクリックします。
2. ［**Google** ドメイン接続］をクリックします。

3. ［接続を削除］をクリックします。
4. ［削除］をクリックします。

Google アカウントを使用して Google ドメイン接続を削除する

Android Enterprise デバイスをサポートするように BlackBerry UEM を設定した場合、Google で接続を削除することができます。

1. Android Enterprise デバイスの設定に使用した Google アカウントを使用して、https://play.google.com/work にログインします。
2. ［管理設定］をクリックします。
3. ［組織情報］セクションで、⋮ をクリックします。
4. ［組織を削除］をクリックします。
5. ［削除］をクリックします。
6. BlackBerry UEM コンソールのメニューバーで、［設定］ > ［外部統合］をクリックします。
7. ［**Google** ドメイン接続］をクリックします。
8. ［テスト接続］をクリックします。
9. ［接続を削除］をクリックします。
10. ［削除］をクリックします。

Google ドメイン接続の編集またはテスト

BlackBerry UEM で Google ドメイン接続を編集し、Android Enterprise デバイスを管理するために使用する Google ドメインのタイプを変更したり、Google ドメイン接続をテストしたりすることができます。接続を編集またはテストするときには、既に有効になっているデバイスは影響を受けません。

1. メニューバーで、［設定］ > ［外部統合］をクリックします。
2. ［**Google** ドメイン接続］をクリックします。
3. ✎ をクリックします。
4. 次のタスクのいずれかを実行します。
   - ［テスト接続］をクリックして、接続の現在のステータスを確認します。
   - Android Enterprise デバイスを管理するドメインのタイプを選択し、［保存］をクリックします。

Windows 10 アクティベーションの簡易化

BlackBerry から検出サービスとして Java Web アプリケーションを使用して、Windows 10 デバイスのユーザーのために、アクティベーションプロセスを簡易化することができます。検出サービスを使用する場合、ユーザーはアクティベーションプロセスでサーバーアドレスを入力する必要はありません。この Web アプリケーションを導入しない場合でも、メッセージが表示されたときにサーバーアドレスを入力することで、ユーザーは Windows 10 デバイスをアクティベーションできます。

異なるオペレーティングシステムと Web アプリケーションツールを使用して、検出サービス Web アプリケーションを導入できます。このトピックでは、高レベルの手順について説明します。一般的なオペレーティングシステムとツールを使用する手順の詳細については、「Windows 10 アクティベーションを簡易化するために検出サービスを導入する」の例を参照してください。

検出サービス Web アプリケーションを導入する場合、次の操作を実行します。

手順	アクション
1	Java アプリケーションサーバー用に、静的な DNS Host A レコードを作成します。このレコードでは、`enterpriseenrollment.<email_domain>` を指定する必要があります。*<email_domain>* はユーザーのメールアドレスに対応します。
2	ユーザーが組織ネットワークの外部にいる場合でも、ユーザーがデバイスをアクティベーションできるようにするには、ポート 443 で外部からの通信を待機するように検出サービスのホストコンピューターを設定します。
3	証明書の作成とインストールを実行して、Windows 10 デバイスと検出サービス間の TLS 接続をセキュリティで保護します。
4	*my*Account にログインして、自動検出プロキシツールをダウンロードします。このファイルを実行して .war ファイルを抽出し、Java アプリケーションサーバーのルートに導入します。
5	検出サービス Web アプリケーションの wdp.properties ファイルを更新して、組織の SRP ID のリストを含めます。

Windows 10 アクティベーションを簡易化するために検出サービスを導入する

次の手順では、検出サービス Web アプリケーションを以下の環境に導入する方法について説明します。

作業を始める前に： 次のソフトウェアが環境にインストールされ、実行されていることを確認します。

- Windows Server 2012 R2
- Java JRE 1.8 以降
- Apache Tomcat 8 バージョン 8.0 以降

1. 検出サービスをホストするコンピューターの静的 IP アドレスを設定します。

メモ：ユーザーが組織ネットワークの外部にいる場合でも、ユーザーがデバイスをアクティベーションできるようにするには、外部からこの IP アドレスにポート 443 でアクセスできるようにする必要があります。

2. 手順 1 で設定した静的 IP アドレスを指し示す名前 **enterpriseenrollment.<*email_domain*>** のために、DNS Host A レコードを作成します。
3. Apache Tomcat をインストールしたディレクトリで、server.xml ファイルを検索して **8080** を見つけ、以下の例に示すようにコメントタグを適用します。

```
<!--
    <Connector port="8080" protocol="HTTP/1.1"
    connectionTimeout="20000"
    redirectPort="8443" />
    -->
```

4. **server.xml** を検索して見つかった **8443** をすべて **443** に変更します。
5. **<Connector port="443"** セクションを検索して、上下のコメントタグを削除し、以下の例に示すように変更します。

```
<Connector port="443" protocol="org.apache.coyote.http11.Http11NioProtocol"
    maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
    clientAuth="false" sslProtocol="TLS" keystoreFile="C:\Users\<account _name>
\.keystore" />
```

6. 上記の例で指定したアカウントでログインしているときに、以下の例に示すように 2 つのコマンドを実行して証明書を生成します。姓名の入力を求められたら、以下の手順の例に示すように `enterpriseenrollment.<email _domain>` を入力します。

```
filename>.csr
```

```
changeit
    What is your first and last name?
      [Unknown]:  enterpriseenrollment.example.com
    What is the name of your organizational unit?
      [Unknown]:  IT Department
    What is the name of your organization?
      [Unknown]:  Manufacturing Co.
    What is the name of your City or Locality?
      [Unknown]:  Waterloo
    What is the name of your State or Province?
      [Unknown]:  Ontario
    What is the two-letter country code for this unit?
      [Unknown]:  CA
    Is CN=enterpriseenrollment.example.com, OU=Business Unit, O=Example
 Company, L=Waterloo, ST=Ontario, C=CA correct?
      [no]:  yes

    C:\Program Files (x86)\Java\jre1.8.0_60\bin>keytool -certreq -alias tomcat
 -keyalg RSA -file <enterpriseenrollment.example.com>.csr
    Enter key password for <enterpriseenrollment.example.com>
            (RETURN if same as keystore password):
```

7. 証明書署名要求の認証局への送信。認証局は .p7b ファイルを送り返します。上記の例では、認証局はファイル `enterpriseenrollment.example.com.p7b` を返します。
   - 証明書署名リクエストを主要な外部認証局に送信する場合は、アクティベーションプロセスの実行時に、この証明書を信頼するための追加操作をユーザーが行う必要はありません。

- 証明書署名リクエストを内部の認証局に送信する場合は、アクティベーションプロセスを開始する前に、ユーザーは CA 証明書をデバイスにインストールする必要があります。

8. 以下の例に示すコマンドを使用して証明書をインストールします。

```
C:\Program Files (x86)\Java\jre1.8.0_60\bin>keytool -import -trustcacerts -
alias tomcat -file <filename>.p7b
```

9. Apache Tomcat を停止します。
10. myAccount にアクセスして、自動検出プロキシツールをダウンロードします。.zip ファイルを解凍し、**W10AutoDiscovery-<*version*>.exe** を実行します。
    .exe ファイルは、ファイル `W10AutoDiscovery-<version>.war` を `C:\BlackBerry` に抽出します。
11. Apache Tomcat をインストールしたディレクトリで、フォルダー `\webapps\ROOT` をチェックします。既に存在している場合、`\ROOT` フォルダーを削除します。
12. `W10AutoDiscovery-<version>.war` の名前を `ROOT.war` に変更します。これを、Apache Tomcat のインストールディレクトリにあるフォルダー `\webapps` に移動します。
13. Apache Tomcat を開始します。
    Apache Tomcat は新しい Web アプリを導入して `\webapp\ROOT` フォルダーを作成します。
14. 管理者として notepad.exe を実行します。Apache Tomcat をインストールしたディレクトリで `\webapps\ROOT\WEB-INF\classes\config\wdp.properties` を開きます。
15. 以下の例に示すように、BlackBerry UEM ドメインのホスト ID を行 `wdp.whitelisted.srpid` に追加します。BlackBerry UEM 管理コンソールで、BlackBerry UEM ドメインのホスト ID を確認できます。複数の BlackBerry UEM ドメインがある場合は、それぞれのホスト ID を指定します。次の操作を実行します。
    a) メニューバーで［設定］**>**［ライセンス］**>**［ライセンスの概要］をクリックします。
    b) ［ライセンスをアクティブ化］をクリックします。
    c) ［ライセンスのアクティベーション方法］ドロップダウンリストで、［ホスト **ID**］をクリックします。

```
wdp.whitelisted.srpid=<Host ID>, <Host ID>, <Host ID>
```

16. Apache Tomcat を再起動します。

UEM と Azure Active Directory 参加の統合

Windows 10 デバイスの登録プロセスを簡素化するために、BlackBerry UEM と Azure Active Directory 参加を統合できます。これが設定されている場合、ユーザーは、Azure Active Directory のユーザー名とパスワードを使用して、デバイスを UEM に登録することができます。Azure Active Directory 参加は、Windows 10 の初期設定中に Windows 10 デバイスを UEM で自動的にアクティブ化することを可能にする Windows Autopilot をサポートするためにも必要です。

Azure Active Directory 参加を UEM と統合するには、次の操作を実行します。

手順	説明
1	UEM の %ClientlessActivationURL% デフォルト変数の値を使用して、UEM を Azure Active Directory 参加と統合できるように次の URL を決定します。たとえば、デフォルトのアクティベーションメールテンプレートを使用するユーザーの詳細画面で、［アクティベーションメールを表示］をクリックすると、Windows 10 サーバー名フィールドに%ClientlessActivationURL% の値が表示されます。 1. MDM 使用条件 URL を決定します。この URL では、次の構造が使用されます。 *%ClientlessActivationURL%*/azure/termsofuse たとえば、%ClientlessActivationURL% 変数が `https://enrol.example.net/S123456789/win/mdm` に解決される場合は、`https://enrol.example.net/S123456789/win/mdm/azure/termsofuse` を使用します。 2. MDM 探索 URL を決定します。この URL では、次の構造が使用されます。 *%ClientlessActivationURL%*/azure/discovery たとえば、%ClientlessActivationURL% 変数が `https://enrol.example.net/S123456789/win/mdm` に解決される場合は、`https://enrol.example.net/S123456789/win/mdm/azure/discovery` を使用します。 3. %ClientlessActivationURL% デフォルト変数のホスト名のみを使用して、アプリ ID URI を決定します。 たとえば、%ClientlessActivationURL% 変数が `https://enrol.example.net/S123456789/win/mdm` に解決される場合は、`https://enrol.example.net` を使用します。
2	UEM と Azure Active Directory 参加の統合.

UEM と Azure Active Directory 参加の統合

作業を始める前に： MDM 使用条件 URL、MDM 探索 URL、およびアプリ ID URI を決定します。詳細については、「UEM と Azure Active Directory 参加の統合」を参照してください。

1. Microsoft Azure 管理ポータル（https://portal.azure.com）にサインインします。
2. ［モビリティ（**MDM** および **MAM**）］に移動します。
3. ［アプリケーションを追加］をクリックします。
4. ［オンプレミス **MDM** アプリケーション］をクリックします。フレンドリ名を入力します（例：`BlackBerry UEM`）。
5. ［追加］をクリックします。
6. 前の手順で追加したアプリケーションをクリックして、設定を構成します。
7. ユーザースコープ（［一部］または［すべて］）を指定します。該当する場合は、グループを選択します。
8. ［**MDM** 使用条件 **URL**］フィールドで、URL を指定します。
9. ［**MDM** 探索 **URL**］フィールドで、URL を指定します。
10. ［保存］をクリックします。
11. ［オンプレミスの **MDM** アプリケーション設定］ > ［プロパティ］をクリックします。

12. ［アプリケーション **ID/URI**］フィールドで、URL を指定します。
13. ［保存］をクリックします。

Microsoft Azure での Windows Autopilot の設定

Windows Autopilot デバイスのアクティベーションをサポートするには、次の操作を実行します。

手順	説明
1	UEM と Azure Active Directory 参加の統合.
2	Azure での Windows Autopilot 導入プロファイルの作成 次に、これを Azure のユーザーグループに割り当てます。
3	Windows Autopilot デバイスを Azure にインポートする.

Azure での Windows Autopilot 導入プロファイルの作成

ユーザーが Windows Autopilot を使用して自分のデバイスをアクティブ化できるようにするには、Azure で適切なユーザーグループに Windows Autopilot 導入プロファイルを割り当てる必要があります。

1. Microsoft Azure 管理ポータル（https://portal.azure.com）にサインインします。
2. ［デバイスの登録］ > ［**Windows** の登録］ > ［**Windows AutoPilot Deployment** プロファイル］に進みます。
3. Windows Autopilot 導入プロファイルを作成します。
4. プロファイルの名前と説明を入力します。
5. Out-of-Box Experience 設定を構成します。
6. プロファイルを適切なユーザーグループに割り当てます。
7. ［保存］をクリックします。

Windows Autopilot デバイスを Azure にインポートする

Windows Autopilot でアクティブ化することを許可する各 Windows 10 デバイスをインポートするには、次の手順を実行します。

1. Windows 10 デバイスをオンにして、デバイスの初期設定をロードします。
2. インターネット接続を使用して Wi-Fi ネットワークに接続します。
3. キーボードで、**Ctrl + Shift + F3** キーまたは **Ctrl + Fn + Shift + F3** キーを押します。デバイスが再起動し、監査モードに入ります。
4. 管理者として **Windows PowerShell** を実行します。
5. `Save-Script -Name Get-WindowsAutoPilotInfo -Path C:\Windows\Temp` を実行して、Windows PowerShell スクリプトを確認します。
6. `Install-Script -Name Get-WindowsAutoPilotInfo` を実行して、スクリプトをインストールします。

7. `Get-WindowsAutoPilotInfo.ps1 -OutputFile C:\Windows\Temp\MyComputer.csv` を実行して、デバイス情報を .csv ファイルに保存します。
8. .csv ファイルを Microsoft Azure にインポートするには、次の操作を実行します。
   a) Azure ポータルで、［デバイスの登録］ **>** ［**Windows** の登録］ **>** ［**Windows AutoPilot** デバイス］に移動します。
   b) ［インポート］をクリックします。
   c) .csv ファイルを選択します。
9. ［システム準備ツール］ダイアログで、次の操作を実行します。
   a) ［システムクリーンアップアクション］フィールドで、［システムの **OOBE**（**Out-of-Box Experience**）に入る］を選択し、［一般化する］を選択解除します。
   b) ［シャットダウンオプション］フィールドで、［再起動］を選択します。

ソースサーバーからのユーザー、デバイス、グループ、およびその他のデータの移行

BlackBerry UEM 管理コンソールを使用して、ユーザー、デバイス、グループ、およびその他のデータを次のソースサーバーから移行できます。

- BlackBerry UEM （オンプレミス）
- Good Control （スタンドアロン）

メモ： ユーザー、デバイス、グループ、およびその他のデータを BES10 ソースサーバーから移行する場合は、BlackBerry UEM バージョン 12.9 に移行してから BlackBerry UEM バージョン 12.11 にアップグレードして、バージョン 12.12 にアップグレードする必要があります。BES10 から BlackBerry UEM バージョン 12.11 および 12.12 への直接移行はサポートされていません。

メモ： Good Control のみのユーザーを BES12 バージョン 12.5 と統合されている Good Control サーバーから移行する場合は、support.blackberry.com/community にアクセスして記事 48870 をご覧ください。

メモ： .csv ファイルを使用して BlackBerry Dynamics ユーザーとデバイスを一括して移行する方法については、support.blackberry.com/community を参照して、記事 49442 をお読みください。

ユーザー、デバイス、グループ、およびその他のデータを移行するには、次の手順を実行します。

手順	アクション
1	移行の前提条件を確認します。
2	ソースサーバーへの接続.
3	オプションで、IT ポリシー、プロファイル、およびグループを移行します。
4	Good Control ソースサーバーからの移行の場合は、Good Control から BlackBerry UEM にポリシーとプロファイルを移行します。
5	ユーザーを移行します。
6	デバイスを移行します。

前提条件：ソースサーバーからのユーザー、デバイス、グループ、およびその他のデータの移行

移行を始める前に次の前提条件を満たしてください。

前提条件	詳細
ログイン	セキュリティ管理者として BlackBerry UEM にログインします。
ソフトウェアバージョンのチェック	データを BlackBerry UEM に移行するには • データの移行元となる BlackBerry UEM インスタンスは、バージョン 12.10 以降である必要があります。 • データの移行元となる Good Control （スタンドアロン）インスタンスは、バージョン 5.0 以降である必要があります。
BlackBerry UEM の同期	移行を開始する前に、どのような方法でも Good Control ソースサーバーと BlackBerry UEM を統合しないでください。
BlackBerry UEM の会社ディレクトリ接続の設定	移行先である BlackBerry UEM の会社のディレクトリ接続を、ソースでの設定と同じ方法で設定します。たとえば、ソースが Active Directory 統合用に設定されていて、example.com ドメインに接続されている場合は、移行先の BlackBerry UEM を Active Directory 統合用に設定して、example.com ドメインに接続します。 重要： 移行先サーバー上の会社のディレクトリがソースサーバー上の会社のディレクトリと一致していない場合、移行は機能しません。
データベースのデフラグ（BlackBerry UEM）	移行を開始する前に、 ソースデータベースおよび移行先の BlackBerry UEM データベース（存在する場合）をデフラグします。多数のユーザーを移行する場合は、ユーザーの各セットを移行した後に移行先の BlackBerry UEM データベースをデフラグする必要があります。Microsoft SQL Server データベースのデフラグの詳細については、www.technet.microsoft.com にアクセスし、記事『インデックスの再編成および再構築』を参照してください。
BlackBerry Dynamics アプリのステータスの確認	移行するすべての BlackBerry Dynamics アプリのバージョンを確認します。これには、ファーストパーティのアプリ、BlackBerry Dynamics アプリ、サードパーティの ISV アプリ、および内部のカスタムアプリが含まれます。すべてのアプリは BlackBerry Dynamics SDK バージョン 4.0.0 以降である必要があります。移行するアプリに使用されている SDK のバージョンを確認するには、Good Control でコンテナアクティビティレポートを実行します。移行でサポートされていない **BlackBerry Dynamics** アプリは、管理者が移行を開始すると、デバイスから消去されます。

前提条件	詳細
BlackBerry Dynamics アプリの権利のステータスの確認	次のことを確認します。 • 移行先 BlackBerry UEM に、ソース Good Control サーバーと同じ BlackBerry Dynamics アプリの権利のリストがある。 • 移行されたすべてのユーザーアカウントに移行先 BlackBerry UEM 上で、ソース Good Control サーバー上と同じ BlackBerry Dynamics アプリの権利のリストが割り当てられている。 • 認証委任が、ソース Good Control サーバーと移行先 BlackBerry UEM で同じである。移行後に認証委任を変更することができます。 権利が不足していると、移行後に BlackBerry Dynamics アプリが無効になります。
Good Control 組織 ID の確認	カスタムアプリは、ソースサーバーと移行先のサーバーが同じ Good Control 組織 ID の場合にのみ移行します。2 つの組織を結合することができます。詳細については、support.blackberry.com/community にアクセスし、記事 47626 を参照してください。
必須ポートがファイアウォールでブロックされていないことを確認	BlackBerry Connectivity Node でポート 8887（TCP）がブロック解除されていることを確認します。 Microsoft SQL Server でポート 1433（TCP）およびポート 1434（UDP）がブロック解除されていることを確認します。

ソースサーバーへの接続

BlackBerry UEM をデータの移行元になるソースサーバーに接続する必要があります。複数のソースを追加できますが、アクティブなソースにできるのは 1 度に 1 つのソースだけです。

メモ：データベースへのログインに使用する資格情報に関連付けられたデータベースアカウントに、書き込み権限があることを確認してください。

メモ：最後に移行を実行してからソース BlackBerry UEM サーバーをアップグレードした場合は、別の移行を実行する前にソースサーバーの設定を再作成する必要があります。

1. メニューバーで、［設定］ > ［移行］ > ［設定］をクリックします。
2. ＋ をクリックします。
3. ［ソースの種類］ドロップダウンリストで、ソースサーバーの種類を選択します。
4. 選択したソースサーバーの種類に応じて、次のようにフィールドに入力します。

ソースサーバーの種類	フィールド	コンテンツ
BlackBerry UEM	表示名	ソースサーバーのわかりやすい名前を入力します。

ソースサーバーの種類	フィールド	コンテンツ
	データベースサーバー	動的ポートは <host>\<instance> の形式、静的ポートは <host>:<port> の形式を使用して、ソースデータベースをホストするコンピューターの名前を入力します。
	データベース認証の種類	ソースデータベースへの接続で使用する認証の種類を選択します。
	SQL ユーザー名 SQL パスワード	SQL 認証を選択した場合は、［SQL ユーザー名］フィールドと［SQL パスワード］フィールドに、ソースデータベースに接続するためのログイン情報を入力します。
	データベース名	ソースデータベースの名前を入力します。
	ソース UEM の認証の種類	ソース BlackBerry UEM の管理コンソールへのログインに使用される認証の種類を選択します。
	ユーザー名 パスワード	ソース管理コンソールにログインするためのログイン情報を入力します。
	ドメイン	Microsoft Active Directory 認証を選択した場合は、ソース管理コンソールが配置されているドメイン名を入力します。
Good Control（スタンドアロン）	表示名	ソースサーバーのわかりやすい名前を入力します。
	ソース Good Control （スタンドアロン）ホスト名	Good Control 管理コンソールの FQDN を入力します。
	ソース Good Control （スタンドアロン）証明書	Good Control CA ルート証明書をアップロードして、SSL 接続を確立します。設定ファイルは CER 形式である必要があります。手順については、「Good Control サーバー用の自己署名ルート証明書のエクスポート」を参照してください。

ソースサーバーの種類	フィールド	コンテンツ
	ユーザー名 パスワード	ソース管理コンソールの管理者アカウントにログインするためのログイン情報を入力します。 メモ：これらの資格情報は、アクセス権 MANAGE_CONTAINERS と MANAGE_USERS_AND_GROUPS を持つ Good Control 管理者に対応している必要があります。アカウントには、Good Control サービスアカウントまたは通常の管理者アカウントを使用できます。ただし、アカウントに関連付けられているパスワードが管理コンソールにアクセスできる必要があります。ハードウェアトークンを持ち、パスワードを持たない Active Directory ユーザーアカウントを使用することはできません。
	ドメイン	ソース管理コンソールの管理者アカウントが置かれているドメインの名前を入力します。管理者がドメインを持たないローカルユーザーである場合は、このフィールドを空白のままにすることができます。

5. ［保存］をクリックします。
6. ソースと移行先の間の接続をテストするには、［テスト接続］をクリックします。
7. ［保存］をクリックします。

終了したら：

- IT ポリシー、プロファイル、およびグループを移行する場合は、ベストプラクティスを確認し、ソースサーバーから IT ポリシー、プロファイル、およびグループを移行するを参照してください。
- ユーザーを移行する場合は、考慮事項を確認し、ソースサーバーからのユーザーの移行を参照してください。
- ユーザーを移行した後で、ソースサーバーからのデバイスの移行を参照してください。

Good Control サーバー用の自己署名ルート証明書をエクスポートします。

Good Control 証明書がサードパーティの証明書と置き換えられていない場合は、次のタスクを完了します。BlackBerry UEM は、サードパーティが提供する証明書を基本的に信頼するため、Good Control サーバーから証明書をエクスポートして、BlackBerry UEM にインポートする必要はありません。

メモ：次のタスクはブラウザー固有ではありません。固有の手順については、使用しているブラウザーのドキュメントを参照してください。

1. ブラウザーで、いずれかの Good Control サーバーのログイン画面に移動します。証明書に署名した CA が Good Control で、ブラウザーはその CA を既知の CA として認識しないために、証明書エラーメッセージが表示されることがあります。
2. ［証明書］ダイアログを開くには、［URL］フィールドで証明書のアイコンをクリックします。
3. ［証明書を表示］または［証明書情報］をクリックして、証明書管理メニューを開きます。
4. ［証明書のパス］タブをクリックします。

5. ルート証明書を選択します。ルート証明書は、証明書の階層の最初の項目です（例：GD12345678 CA）。
6. ［証明書を表示］をクリックします。
7. ［詳細］タブをクリックします。
8. ［ファイルにコピー］または［エクスポート］をクリックします。
9. ［**DER encoded binary X.509 (.CER)**］または［**Base-64 encoded X.509 (.CER)**］形式を選択します。
10. 証明書の場所とファイル名を入力します。
11. ［次へ］または［保存］をクリックします。
12. ［完了］をクリックします。

考慮事項：ソースサーバーから IT ポリシー、プロファイル、およびグループを移行する

BlackBerry UEM ソースの移行では、次の項目が移行先データベースにコピーされます。

- 選択した IT ポリシー
- メールプロファイル
- Wi-Fi プロファイル
- VPN プロファイル
- プロキシプロファイル
- BlackBerry Dynamics プロファイル
- CA 証明書プロファイル
- 共有証明書プロファイル
- SCEP プロファイル
- ユーザー資格情報プロファイル
- 認証局設定
- 選択したポリシーおよびプロファイルと関連付けられたポリシーおよびプロファイル

メモ： BlackBerry UEM からのグループの場合、ユーザー、ロール、およびソフトウェア設定割り当ては移行されません。

Good Control （スタンドアロン）ソースからの移行では、次の項目が移行先データベースにコピーされます。

- ポリシーセット
- 接続プロファイル
- アプリグループ
- アプリの使用状況（証明書用）
- 証明書

BlackBerry UEM

BlackBerry UEM IT ポリシー、プロファイル、およびグループを別のドメインに移行する場合は、次のガイドラインを参考にしてください。

項目	考慮事項
IT ポリシーパスワード	Android デバイス用に選択したソース IT ポリシーのいずれかに最小文字数が 4 文字未満または 16 文字を超えるパスワードが含まれている場合、BlackBerry UEM IT ポリシーまたはプロファイルは移行できません。ソース IT ポリシーを選択解除または更新して、移行を再開します。
プロファイル名	移行後、すべての SCEP、ユーザー資格情報、共有の証明書、または CA 証明書のプロファイルに一意の名前が付けられていることを確認する必要があります。同じタイプの 2 つのプロファイルに同じ名前が付いている場合は、どちらかのプロファイル名を編集する必要があります。
ディレクトリグループ	ディレクトリグループを移行する場合、設定されたディレクトリがソースと移行先のデータベースでそれぞれ 1 個だけであることが必要です。このディレクトリは、ソースと移行先の両方のデータベースで、同様に設定する必要があります。ディレクトリが同様にセットアップされていない場合、ディレクトリグループは移行されません。
ネストされたグループ	ソースデータベースと移行先データベースが BES5 と統合されている BlackBerry UEM データベースの場合は、ネストされたユーザーグループを移行することはできませんネストされたグループを移行しようとした場合、他のグループ、プロファイル、および PKI 設定情報は移行されません。

Good Control （スタンドアロン）

Good Control （スタンドアロン）セキュリティポリシーセット、接続プロファイル、アプリグループ、および証明書を BlackBerry UEM に移行する場合は、次のガイドラインを考慮してください。

項目	考慮事項
ポリシーセット	移行後に、各 Good Control ポリシーセットが BlackBerry UEM に次の項目として表示されます。 • ポリシーセットの各アプリの設定 • セキュリティポリシー • コンプライアンスポリシー
接続プロファイル	BlackBerry Dynamics 接続プロファイルが Good Control （スタンドアロン）から BlackBerry UEM に移行されるときには、アプリの［サーバー］タブの値は移行されません。これらの値は、UEM で新しい BlackBerry Dynamics 接続プロファイルを手動で作成する場合と同じように、移行先 UEM サーバーのデフォルト値を使用して設定されます。 BlackBerry Dynamics 接続プロファイルが Good Control （スタンドアロン）から BlackBerry UEM に移行されるときには、［インフラストラクチャ］タブの一部の値は移行されません。管理者は、移行された各プロファイルを手動で編集し、プライマリ BlackBerry Proxy クラスターとセカンダリ BlackBerry Proxy クラスターの値を設定する必要があります。

項目	考慮事項
アプリグループ	Everyone グループは移行されますが、そのグループにはユーザーが割り当てられず、移行先 BlackBerry UEM の All Users グループに関連付けられていません。管理者は、必要に応じてユーザーに手動で割り当てる必要があります。
アプリ	ソースサーバーからのアプリの権利が移行先サーバーに存在しない場合、そのアプリの割り当ては移行されません。アプリグループが移行されます。
アプリの使用状況（証明書用）	アプリの使用状況は、以下を除き、移行されます。 • 移行先サーバーに既に存在するアプリの使用状況 • BlackBerry Dynamics 以外のアプリ • 他の Good Control 組織からのカスタムアプリ

ソースサーバーから IT ポリシー、プロファイル、およびグループを移行する

オプションで、ソースサーバーから IT ポリシー、プロファイル、およびグループを移行できます。

1. メニューバーで［設定］をクリックします。
2. 複数のソースを設定している場合は、左ペインで［移行］ **>** ［設定］をクリックした後、データの移行元となるソースサーバーの名前の横のラジオボタンを選択します。
3. ［移行］ > ［**IT** ポリシー、プロファイル、グループ］をクリックします。
4. ［次へ］をクリックします。
5. 移行するアイテムのチェックボックスをオンにします。

   移行先への移行時に、それぞれのポリシー名およびプロファイル名にソースサーバーの名前が追加されます。
6. ［プレビュー］をクリックして、選択したポリシーおよびプロファイルをレビューします。
7. ［移行］をクリックします。
8. IT ポリシー、プロファイル、およびグループを設定するには、［**IT** ポリシーとプロファイルを設定］をクリックして［ポリシーとプロファイル］画面に移動します。

終了したら： 移行先サーバーで、デバイスを移行する前に、移行できなかったポリシーとプロファイルを作成し、それらをユーザーに割り当てます。Good Control ソースサーバーから移行するときに実行する手順に関する具体的な情報については、「Good Control から BlackBerry UEM への完全なポリシーとプロファイルの移行」を参照してください。

Good Control から BlackBerry UEM への完全なポリシーとプロファイルの移行

ユーザー、デバイス、グループ、およびその他のデータを Good Control から BlackBerry UEM に移行した後で、移行先の BlackBerry UEM で次のタスクを実行する必要があります。BlackBerry UEM で Good Control の機能を見つける場所については、「BlackBerry UEM の Good Control の機能」を参照してください。

アプリ、ポリシー、およびユーザー間の関係を再構築します。

- アプリの設定をグループ内の BlackBerry Dynamics アプリに割り当てます。
- 接続プロファイルをグループに割り当てます。
- 移行された BlackBerry Dynamics ポリシーおよびコンプライアンスポリシーをユーザーに割り当てます。
- 上書きプロファイル（BlackBerry Dynamics プロファイルおよびコンプライアンスプロファイル）を設定します。

.json ファイルの設定を Good Control から BlackBerry UEM に移動します。

移行された接続プロファイルを完了します。

- アプリサーバーの情報を入力します。
- ［インフラストラクチャ］タブで、BlackBerry Proxy クラスターを設定します。

BlackBerry UEM の Good Control の機能

次の表は、Good Control の機能と同様のタスクを BlackBerry UEM で実行できる場所を示しています。

Good Control の機能	BlackBerry UEM で見つかる場所
ユーザーおよびグループ	［ユーザー］をクリックします。
管理者	［設定］ > ［管理者］をクリックします。
BlackBerry Dynamics アプリと権利の管理	アプリと管理するアプリをクリックします 。
BlackBerry Dynamics アプリのログの消去、ロック解除、ロック、および管理	**1.** メニューバーで［ユーザー］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.** 管理するアプリがインストールされているデバイスの［デバイス］タブを選択します。 **5.** ［**BlackBerry Dynamics** アプリ］のセクションで、管理するアプリの横にあるコマンドを選択します。
アクセスキーの生成	**1.** ［ユーザー］をクリックします。 **2.** アクセスキーを生成するユーザーを選択します。 **3.** ［アクティベーションパスワードの設定］をクリックします。 **4.** ［**BlackBerry Dynamics** アクセスキーの生成］オプションを選択します。

Good Control の機能	BlackBerry UEM で見つかる場所
サービスの管理	［設定］ > ［**BlackBerry Dynamics**］ > ［アプリサービス］をクリックします。
アプリグループ	［グループ］ > ［ユーザー］をクリックします。
セキュリティポリシー	［ポリシーとプロファイル］ > ［**BlackBerry Dynamics**］をクリックします。
コンプライアンスポリシー	［ポリシーとプロファイル］ > ［コンプライアンス（**BlackBerry Dynamics**）］をクリックします。
プロビジョニングプロファイル	［設定］ > ［アクティベーションのデフォルト］をクリックします。
アプリ固有のポリシー	［アプリ］をクリックして管理する BlackBerry Dynamics アプリをクリックします。
アプリサーバーを追加	［ポリシーとプロファイル］ > ［接続（**BlackBerry Dynamics**）］をクリックします。
接続プロファイル	［ポリシーとプロファイル］ > ［**BlackBerry Dynamics** の接続］をクリックします。
デバイスポリシー	［ポリシーとプロファイル］ > ［ポリシー］ > ［**IT** ポリシー］をクリックします。
デバイス設定	［ポリシーとプロファイル］ > ［ネットワークと接続］をクリックし、次のプロファイルを選択します。 • Wi-Fi • VPN • プロキシ • メール • Web アイコン • カスタムペイロード
Apple DEP	［設定］ > ［外部統合］ > ［**Apple Device Enrollment Program**］をクリックします。
APNS 管理	［設定］ > ［外部統合］ > ［**Apple** プッシュ通知］をクリックします。
ユーザーセルフサービスの管理	［設定］ > ［セルフサービス］をクリックします。
Direct Connect 設定	［設定］ > ［**BlackBerry Dynamics**］ > ［**Direct Connect**］をクリックします。
サーバーのプロパティ	［設定］ > ［**BlackBerry Dynamics**］ > ［プロパティ］をクリックします。

Good Control の機能	**BlackBerry UEM** で見つかる場所
Good Proxy クラスター構成	［設定］ > ［**BlackBerry Dynamics**］ > ［クラスター］をクリックします。
信頼済み認証局	［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。 ［設定］ > ［外部統合］ > ［認証局］をクリックします。
証明書の定義	［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。 ［設定］ > ［外部統合］ > ［認証局］をクリックします。
ユーザーのアップロード済み証明書	［ユーザー］ > ［すべてのユーザー］ > ［ユーザーの詳細］ > ［概要］ > ［**IT** ポリシーおよびプロファイル］をクリックします。
アプリケーションの使用状況	対応するアプリケーションの詳細ページで、**BlackBerry Dynamics** アプリにユーザーの資格情報およびユーザー資格情報プロファイルの使用を許可します。
レポート作成	［設定］ > ［**BlackBerry Dynamics**］ > ［レポート］をクリックします。
サーバージョブ	［設定］ > ［**BlackBerry Dynamics**］ > ［ジョブ］をクリックします。

考慮事項：ソースサーバーからのユーザーの移行

ユーザーを移行先の BlackBerry UEM に移行する場合は、次の点に留意する必要があります。

項目	考慮事項
移行の最大数	ソースから一度に移行できるユーザーは、最大 1000 人です。移行先が BES5 データベースからアップグレードされた BlackBerry UEM データベースである場合は、一度に移行できるユーザーは、最大 300 人です。 最大値を超えるユーザー数を選択した場合、最大値のユーザーのみが移行先の BlackBerry UEM に移行されます。残りのユーザーはスキップされます。ソースサーバーからすべてのユーザーを移行するには、移行プロセスを必要な回数繰り返します。 メモ： 1000 ユーザーの移行中に BlackBerry UEM がタイムアウトする場合は、少ないユーザー数で移行をお試しください。

項目	考慮事項
メールアドレス	• ユーザーは、移行される前にメールアドレスを所有している必要があります。 • 既に移行先の BlackBerry UEM で同じメールアドレスを使用しているユーザーは移行できません。これらのユーザーは、移行するユーザーのリストには表示されません。 • ソースの 2 人のユーザーが同じメールアドレスを所有している場合は、［ユーザーを移行］画面に 1 人のユーザーだけが表示されます。 • ソースの 2 人のユーザーが同じメールアドレスを所有している場合は、［デバイスを移行］画面のユーザー情報は 2 人のうちどちらかの情報である可能性があります。
デバイス	• ソースのユーザーが BlackBerry 10 デバイスと iOS または Android デバイスの両方を所有していて、デバイスが別のユーザー名で同じメールアドレスを使用している場合、一部のデバイスは移行されません。 • 移行後、ユーザーが BlackBerry 10 デバイスと、iOS、Android、Windows、または macOS デバイスを所有している場合、ユーザーは移行前に BES10 Self-Service、BES12 Self-Service、または BlackBerry UEM Self-Service で使用していたのと同じログイン情報を BlackBerry UEM Self-Service でも使用する必要があります。
パスワード	移行後、ローカルユーザーは BlackBerry UEM Self-Service に初めてにログインした後にパスワードを変更する必要があります。移行前に BES12 Self-Service または BlackBerry UEM Self-Service にアクセスする権限を持っていなかったユーザーは、移行後に自動的に権限を付与されません。
グループ	グループが割り当てられていないユーザーをフィルタリングして、それらのユーザーを移行に含めることができます。
Good Dynamics	Good Dynamics プロファイルが割り当てられているユーザーを移行することができます。

ソースサーバーからのユーザーの移行

ソースサーバーから移行先の BlackBerry UEM にユーザーを移行できます。ユーザーは移行の完了後、ソースと移行先の両方に維持されます。

1. メニューバーで、［設定］ > ［移行］ > ［ユーザー］をクリックします。
2. ［ユーザーを移行］画面で、ソースが Good Control （スタンドアロン）構成の場合は、［キャッシュを更新］をクリックします。

   キャッシュでは、1000 人のユーザーを入力するごとに約 10 分かかります。

   BlackBerry UEM はユーザーデータをキャッシュして検索機能を高速化しますが、ユーザーデータはソースから直接移行されます。キャッシュの更新は、最初のユーザーのセットの移行の場合のみ必須であり、その後はオプションです。
3. ［次へ］をクリックします。
4. 移行するユーザーを選択します。

Good Control の移行の場合、最初の 20,000 人のユーザーのみが表示されます。最初の 20,000 人に入っていない特定のユーザーを見つけるには、ユーザー名またはメールアドレスを検索します。すべてを選択すると、最初のページのユーザーのみが選択されます。選択したいユーザーの数に合わせてページサイズを設定します。

Good Control の移行の場合、キャッシュが更新された後にソースで変更が行われた場合、これらの変更は表示されるキャッシュデータに反映されません。移行中にソースサーバーに変更を加えないようにする必要がありますが、変更した場合は、キャッシュを定期的に更新してください。

5. ［次へ］をクリックします。
6. 選択したユーザーにグループを 1 つ以上割り当て、IT ポリシーと 1 つ以上のプロファイルを割り当てます。

   詳細については、管理関連の資料を参照してください。
7. ［プレビュー］をクリックします。
8. ［移行］をクリックします。

終了したら： ソースサーバーからのデバイスの移行.

考慮事項：ソースサーバーからのデバイスの移行

デバイスを移行先の BlackBerry UEM に移行する場合は、次の点に留意する必要があります。

項目	考慮事項
ベストプラクティス	残りのデバイスを移行する前に移行先のサーバーが正しく設定されていることを確認するために、固有の設定ごとに（たとえば、別のグループ、ポリシー、アプリの構成など）1 つのデバイスを移行することがベストプラクティスです。
移行の最大数	ソースサーバーから一度に移行できるデバイスは、最大 2000 です。
移行先の BlackBerry UEM	デバイスを移行する前に BlackBerry UEM がそのデバイスタイプと OS をサポートすることを確認します。
ユーザー	• ユーザーが移行先の BlackBerry UEM ドメインに存在している必要があります。 • BlackBerry UEM から移行する場合、ユーザー 1 人につき 6 台以上のデバイスを同時に移行することはできません。
BlackBerry UEM ソース上の iOS デバイス	• iOS デバイスに最新バージョンの BlackBerry UEM Client がインストールされている必要があります。 • すべての iOS デバイスが信頼済みになっている必要があります（信頼されていない iOS デバイスは移行できません） • BlackBerry UEM Client を移行のために開くことができないため、アプリロックプロファイルを割り当てられている iOS デバイスは移行できません。
BlackBerry UEM ソース上の Android デバイス	• Android デバイスに最新バージョンの BlackBerry UEM Client がインストールされている必要があります。 • 仕事用プロファイルのある Android デバイスは移行できません。

項目	考慮事項
Windows デバイス	Windows デバイスを移行することはできません。
macOS デバイス	macOS デバイスを移行することはできません。
MDM 制御 （BlackBerry UEM）	MDM 制御 によりアクティベーションされたデバイスは、移行が始まるとメールへのアクセスを一時的に失います。メールサービスは、移行が完了すると復元されます。
Good Control デバイス（スタンドアロン Good Control から）	**BlackBerry Dynamics** アプリ • 移行と互換性のあるすべての BlackBerry Dynamics アプリが移行されます。移行と互換性がない **BlackBerry Dynamics** アプリは、管理者が移行を開始すると、デバイスから消去されます。これらのアプリは、移行先の BlackBerry UEM で再度アクティベーションする必要があります。 • 互換性のないアプリは、BlackBerry Dynamics SDK バージョン 4.0.0 より前のバージョンで構築されているアプリです。移行の前に、コンテナアクティビティレポートを実行して、アプリの SDK のバージョンを確認することができます。 • ［デバイスを移行］画面では、互換性のないコンテナの列に、移行できない各デバイスの BlackBerry Dynamics アプリの数と、各デバイスの BlackBerry Dynamics アプリの合計数が表示されます。数字をクリックすると、移行と互換性がない BlackBerry Dynamics アプリが表示されます。 • ユーザーが、移行先 BlackBerry UEM 上のアプリの権利を持っていることを確認します。アプリの権利を持っていない場合は、移行後、ユーザーは、アプリがブロックされているというメッセージを受信します。 • 移行先 BlackBerry UEM にそのユーザーのアプリが既に登録されている場合、BlackBerry Dynamics アプリは移行されません。 • BlackBerry Access for Windows 10 および BlackBerry Access for macOS では、移行はサポートされていません。移行が完了した後、ユーザーはこれらのアプリを UEM に再登録する必要があります。 • カスタムアプリは、ソースサーバーと移行先のサーバーが同じ Good Control 組織 ID の場合にのみ移行します。2 つの組織を結合することができます。詳細については、support.blackberry.com/community にアクセスし、記事 47626 を参照してください。 デバイス認証 • Good for Enterprise のデバイス認証委任があるデバイスは移行されません。認証委任としての Good for Enterprise を削除した後、移行を続行する前にキャッシュを更新します。BlackBerry UEM 上でソースサーバー上と同じ認証委任がユーザーに割り当てられていることを確認することがベストプラクティスです。 • 認証委任は、ソース Good Control サーバーと移行先 BlackBerry UEM で同じである必要があります。移行後に認証委任を変更することができます。

項目	考慮事項
	デバイス管理 • Good Dynamics MDM の登録は移行されません。ユーザーは MDM から登録を解除する必要があります。移行先 BlackBerry UEM が MDM を必要とする場合、ユーザーは古い MDM プロファイルを手動で削除し、BlackBerry UEM Client をアクティベーションして、デバイスを MDM に再登録する必要があります。 オペレーティングシステム • 不明なオペレーティングシステムがあるデバイスは移行されません。 チャットセッション • ソース BEMS サーバーは、古い Connect チャットセッションを最大 24 時間開いたまま保持しているため、ユーザーが一時的に 2 つのデバイスからチャットにログインするように表示されることがあります。 • 未読の Connect チャットメッセージは、移行中に削除されます。ユーザーは移行前に Connect からログアウトする必要があります。 ユーザー • ユーザーが BlackBerry Dynamics アプリがある複数のデバイスを使用している場合は、すべてのデバイスが自動的に選択されて移行されます。 • 複数の Good Control ソースサーバーから同じユーザーのデバイスを移行することはできません。複数の Good Control のソースからデバイスを移行することができますが、ユーザーが BlackBerry Dynamics デバイスを移行先 BlackBerry UEM に既に持っていることはありません。 キーのロック解除 • 移行が開始された後にユーザーが BlackBerry Dynamics アプリのパスワードを忘れた場合でも、コンテナが移行を完了する前であれば、ロック解除アクセスキーを Good Control ソースから取得する必要があります。移行が完了したら、キーを移行先 BlackBerry UEM から取得する必要があります。 アクセスキー • 移行後 Good Control ソースサーバー上でアクセスキーを生成できなくなります。 移行後 • 移行を開始するには、Android ユーザーがデバイスを再起動し、BlackBerry Dynamics アプリを強制的にコールドスタートする必要があります。2 回目の再起動が必要な場合があります。 • iOS デバイスのユーザーは、アプリを閉じるには、上にスワイプする必要があります。 • 移行を開始するには、最初に認証委任として設定されているアプリを開くことをお勧めします。 • 移行が完了するまでは、一部のアプリがランチャーに表示されません。 • 移行後、ランチャーのアプリアイコンの配置がデフォルトにリセットされます。 • デバイスは、VIP ルール、ブックマーク、およびユーザー証明書を新しいサーバーにアップロードします。 **.json** 設定 • .json 設定はグローバルであるため、それらを移行すると、移行先デバイスの .json 設定が上書きされる可能性があります。したがって、.json 設定は移

デバイスの移行のクイックリファレンス

デバイスタイプ	アクティベーションタイプ/構成	移行
BlackBerry 10	次の条件のいずれか	サポート
Android	• MDM 制御 • BlackBerry 2FA	サポート
Android	• BlackBerry Dynamics （UEM から UEM）	サポートされていません
仕事用プロファイルのある Android デバイス	次の条件のいずれか	サポートされていません
Android Samsung Knox Workspace デバイス	次の条件のいずれか	サポート
iOS	• MDM 制御 • BlackBerry 2FA 専用のデバイス登録 • BlackBerry UEM Client がインストール済みの DEP デバイス	サポート
iOS	• BlackBerry Dynamics （UEM から UEM） • BlackBerry UEM Client がインストールされていない DEP デバイス	サポートされていません
Windows	次の条件のいずれか	サポートされていません
macOS	次の条件のいずれか	サポートされていません

ソースサーバーからのデバイスの移行

ソースサーバーから移行先の BlackBerry UEM にユーザーを移行すると、同ユーザーのデバイスを移行できるようになります。デバイスはソースサーバーから移行先の BlackBerry UEM に移動し、移行後はソースから消去されます。

作業を始める前に：

- デバイスを移行する前に、移行したユーザーに適切なポリシーと権利が割り当てられていることを確認します。
- BlackBerry UEMおよび BES10 の移行の場合、iOS デバイスのユーザーに、BlackBerry UEM Client を開いて BlackBerry UEM への移行を開始する必要があること、また移行が完了するまで BlackBerry UEM Client を開いたままにしておく必要があることを通知します。

1. メニューバーで、［設定］ > ［移行］ > ［デバイス］をクリックします。
2. ［デバイスを移行］画面で、ソースが Good Control （スタンドアロン）構成の場合は、［キャッシュを更新］をクリックします。

   キャッシュでは、1000 のデバイスを入力するごとに約 10 分かかります。

   BlackBerry UEM はデバイスデータをキャッシュして検索機能を高速化しますが、デバイスデータはソースから直接移行されます。キャッシュの更新は、最初のデバイスのセットの移行の場合のみ必須であり、その後はオプションです。
3. ［次へ］をクリックします。
4. 移行するデバイスを選択します。

   Good Control の移行の場合、最初の 20,000 のデバイスのみが表示されます。最初の 20,000 人に入っていない特定のユーザーを見つけるには、ユーザー名またはメールアドレスを検索します。すべてを選択すると、最初のページのデバイスのみが選択されます。選択したいデバイスの数に合わせてページサイズを設定します。

   メモ： キャッシュはユーザー別に表示され、一部のユーザーが複数のデバイスを持つ場合があるため、デバイスの数よりも少ない行数が表示されます。

   Good Control の移行の場合、キャッシュが更新された後にソースで変更が行われた場合、これらの変更は表示されるキャッシュデータに反映されません。移行中にソースサーバーに変更を加えないようにする必要がありますが、変更した場合は、キャッシュを定期的に更新してください。
5. ［プレビュー］をクリックします。
6. ［移行］をクリックします。
7. 移行中のデバイスのステータスを表示するには、［移行］ > ［ステータス］をクリックします。

   移行された BlackBerry Dynamics アプリを確認するには、Good Control でコンテナアクティビティレポートを実行します。

   すべてのデバイスが移行される場合でも、すべてのユーザーの認証委任アプリが移行を完了するまで、Good Control 設定が実行されていることを確認します。

DEP デバイスの移行

Apple の Device Enrollment Program（DEP）に登録している iOS デバイスをソース BES12 または BlackBerry UEM データベースから別の BlackBerry UEM データベースに移行できます。

BlackBerry UEM Client がインストール済みの DEP デバイスの移行

iOS の Device Enrollment Program（DEP）に登録しており、「Apple 」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タイプでアクティベーションされた MDM 制御 デバイスを移行できます。

作業を始める前に： BlackBerry UEM Client のアプリ設定で、［**BlackBerry UEM** からデバイスが削除されたらアプリをデバイスから削除する］チェックボックスをオフにします。

1. DEP ポータルで、新しい仮想 MDM サーバーを作成します。
2. 移行先の BlackBerry UEM インスタンスを新しい仮想 MDM サーバーに接続します。詳細については、「DEP 用に BlackBerry UEM を設定」を参照してください。

   移行先の BlackBerry UEM インスタンスの DEP プロファイルが、ソースの BES12 または BlackBerry UEM インスタンスの DEP プロファイルと一致することを確認してください。
3. DEP デバイスをソースの仮想 MDM サーバーから新しい仮想 MDM サーバーに移動します。

4. BlackBerry UEM 管理コンソールで、ソースのインスタンスから移行先の BlackBerry UEM インスタンスに DEP デバイスを移行します。

BlackBerry UEM Client がインストールされていない DEP デバイスの移行

iOS の Device Enrollment Program（DEP）に登録されており、Apple がインストールされていない BlackBerry UEM Client デバイスは、移行をサポートしていないデバイスリストに表示されます。

1. DEP ポータルで、新しい仮想 MDM サーバーを作成します。
2. 移行先の BlackBerry UEM インスタンスを新しい仮想 MDM サーバーに接続します。詳細については、「DEP 用に BlackBerry UEM を設定」を参照してください。

   移行先の BlackBerry UEM インスタンスがソースのインスタンスと同じ DEP プロファイルを持っていることを確認してください。
3. DEP デバイスをソースの仮想 MDM サーバーから新しい仮想 MDM サーバーに移動します。
4. それぞれの DEP デバイスを工場出荷時の状態にリセットします。
5. それぞれの DEP デバイスを再度アクティベーションします。

BlackBerry Dynamics アプリをサポートするための BlackBerry UEM の設定

このセクションの指示に従って、BlackBerry Proxy および BlackBerry Dynamics アプリに固有の BlackBerry UEM 設定を設定します。

BlackBerry Proxy クラスターの管理

BlackBerry Proxy の最初のインスタンスをインストールするときには、BlackBerry UEM によって「First」という名前の BlackBerry Proxy クラスターが作成されます。1 つのクラスターのみが存在する場合は、BlackBerry Proxy の追加のインスタンスがデフォルトでクラスターに追加されます。追加のクラスターを作成し、BlackBerry Proxy インスタンスを使用可能なクラスター間で移動することができます。複数の BlackBerry Proxy クラスターが使用可能な場合、新しいインスタンスはデフォルトでクラスターに追加されません。新しいクラスターは割り当てられていないと見なされ、使用可能ないずれかのクラスターに手動で追加する必要があります。

1. 管理コンソールのメニューバーで、［設定］ > ［**BlackBerry Dynamics**］をクリックします。
2. ［クラスター］をクリックします。
3. 次のタスクを実行します。

タスク	手順
新しい BlackBerry Proxy クラスターを作成する	**a.** ＋ をクリックします。 **b.** クラスターの名前を入力します。 **c.** ［保存］をクリックします。
BlackBerry Proxy クラスターの名前を変更する	**a.** クラスター名をクリックします。 **b.** クラスター名を変更します。クラスターごとに固有の名前が必要です。 **c.** ［保存］をクリックします。
BlackBerry Proxy インスタンスを別の BlackBerry Proxy クラスターに移動する	**a.** ［サーバー］列で、BlackBerry Proxy インスタンスの名前をクリックします。 **b.** BlackBerry Proxy［クラスター］ドロップダウンリストで、インスタンスを追加するクラスターを選択します。 **c.** ［保存］をクリックします。
空の BlackBerry Proxy クラスターを削除する	**a.** そのクラスターの✕をクリックします。 **b.** ［削除］をクリックします。

タスク	手順
クラスターのアプリプロキシ設定を設定する	**a.** ［設定］ > ［**BlackBerry Dynamics**］ > ［クラスター］をクリックします。 **b.** クラスター名をクリックします。 **c.** ［グローバル設定を上書き］をクリックします。 詳細については、「BlackBerry Dynamics アプリプロキシ設定の設定」を参照してください。
すべてのクラスターの PAC ファイルの更新をダウンロードする	• ［**PAC** キャッシュを更新］をクリックします。
信頼されたルート証明書を指定して、サーバーから PAC ファイルをダウンロードする	**a.** 管理コンソールからアクセスできるネットワークの場所に X.509 形式（*.cer、*.der）で証明書が保存されていることを確認してください。 **b.** メニューバーで、［設定］ > ［外部統合］ > ［信頼済み証明書］をクリックします。 **c.** ［**PAC** サーバー信頼］の横にある＋をクリックします。 **d.** ［参照］をクリックします。 **e.** 使用する証明書ファイルを選択します。 **f.** ［開く］をクリックします。 **g.** 証明書の説明を入力します。 **h.** ［追加］をクリックします。
アクティベーションのために使用できるよう BlackBerry Proxy を有効にする	アクティベーションのために使用する BlackBerry Proxy インスタンスの［アクティベーションのための有効化］オプションを選択します。少なくとも 1 つのインスタンスを選択する必要があります。

ポート転送を使用した Direct Connect の設定

作業を始める前に：

- BlackBerry Connectivity Node サーバーごとにパブリック DNS エントリを設定します（たとえば、bp01.mydomain.com、bp02.mydomain.com など）。
- 外部ファイアウォールを設定して、ポート 17533 でのインバウンド接続を許可し、そのポートを各 BlackBerry Connectivity Node サーバーに転送します。
- BlackBerry Connectivity Node インスタンスが DMZ にインストールされている場合は、各 BlackBerry Connectivity Node と BlackBerry Dynamics アプリがアクセスする必要があるアプリケーションサーバー（たとえば、Microsoft Exchange、内部 Web サーバー、および BlackBerry UEM Core）との間で適切なポートが開い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、［設定］ > ［**BlackBerry Dynamics**］をクリックします。
2. ［**Direct Connect**］をクリックします。
3. BlackBerry Proxy インスタンスをクリックします。

4. Direct Connect をオンにするには、［**Direct Connect** をオンにする］チェックボックスをオンにします。［**BlackBerry Proxy** ホスト名］フィールドで、ホスト名が正しいことを確認します。作成したパブリック DNS エントリがサーバーの FQDN と異なる場合は、代わりに外部 FQDN を指定します。
5. クラスタ内のすべての BlackBerry Proxy インスタンスについて、手順 3 と 4 を繰り返します。

   Direct Connect の一部の BlackBerry Proxy インスタンスのみを有効にするには、新しい BlackBerry Proxy クラスターを作成します。クラスター内のすべてのサーバーは、同じ設定である必要があります。詳細については、管理関係の資料で「BlackBerry Proxy クラスターの管理」を参照してください。
6. ［保存］をクリックします。

BlackBerry Dynamics プロパティの設定

組織内の BlackBerry Dynamics アプリを使用するように、プロパティを設定することができます。各プロパティの詳細およびデフォルト設定の変更の影響については「BlackBerry Dynamics グローバルプロパティ」、「BlackBerry Dynamics プロパティ」、「BlackBerry Proxy プロパティ」、および「 の BlackBerry Dynamics アプリプロキシ設定の設定」を参照してください。BlackBerry Proxy プロパティの設定のベストプラクティスの詳細については、support.blackberry.com/community にアクセスして、記事 47875 をご覧ください。

1. 管理コンソールのメニューバーで、［設定］ > ［**BlackBerry Dynamics**］をクリックします。
2. 次の操作のいずれかを実行します。
   - グローバルプロパティを設定するには、［グローバルプロパティ］をクリックします。
   - 特定の BlackBerry UEM のインスタンスのプロパティを設定するには、［プロパティ］をクリックします。［サーバータイプ］ドロップダウンリストで、［**BlackBerry Control** サーバー］をクリックし、設定する BlackBerry UEM サーバーを選択します。
   - 特定の BlackBerry Proxy のインスタンスのプロパティを設定するには、［プロパティ］をクリックします。［サーバータイプ］ドロップダウンリストで、［**BlackBerry Proxy** サーバー］をクリックし、設定する BlackBerry Proxy サーバーを選択します。
3. 必要に応じてプロパティを設定します。
4. ［保存］をクリックします。

BlackBerry Dynamics グローバルプロパティ

次の表に、設定可能な BlackBerry Dynamics グローバルプロパティを示します。

「再起動」列は、プロパティを変更したときに、BlackBerry UEM の再起動が必要かどうかを示します。

メモ： プロパティが管理コンソールに表示されていても、ここに記載されていない場合、それは使用されなくなった推奨されていないプロパティです。

証明書の管理

プロパティ	説明	デフォルト	再起動
個々のエンドユーザーの PKCS12 証明書のキーストアの有効期間を秒単位で指定します。	デバイスユーザーがメールメッセージに署名するためおよびクライアント認証のためにアップロードできる PKCS12 証明書のキーストアの有効期間（秒）。 メモ： このプロパティは読み取り専用です。変更することはできません。	86400	—

Communication

プロパティ	説明	デフォルト	再起動
cntmgmt.internal.port	コンテナ管理サービスの内部ポート。	Null（デフォルトは 17317 です）	はい
cntmgmt.max.conns.above.limi	cntmgmt.max.conns.persec プロパティで設定されている制限を超過して許可される接続の最大数。 メモ： BlackBerry テクニカルサポートに相談せずにこの設定を変更しないでください。	3	はい
cntmgmt.max.conns.persec	コンテナ管理のための 1 秒あたりの最大接続数。 メモ： BlackBerry テクニカルサポートに相談せずにこの設定を変更しないでください。	30	はい
cntmgmt.max.active.sessions	コンテナ管理のアクティブなセッションの最大数。	10000	はい
cntmgmt.max.idle.count	コンテナ管理に許可されているアイドル接続の最大数。 メモ： BlackBerry テクニカルサポートに相談せずにこの設定を変更しないでください。	0	はい
cntmgmt.max.read.throughput	コンテナ管理の同時読み取り操作の最大数。 メモ： BlackBerry テクニカルサポートに相談せずにこの設定を変更しないでください。	500	はい

プロパティ	説明	デフォルト	再起動
cntmgmt.max.write.throughput	コンテナ管理の同時書き込み操作の最大数。 メモ： BlackBerry テクニカルサポートに相談せずにこの設定を変更しないでください。	500	はい
cntmgmt.ssl.external.enable	外部コンテナ管理で SSL を有効にするかどうかを制御します。	オン	はい
cntmgmt.ssl.internal.enable	内部コンテナ管理で SSL を有効にするかどうかを制御します。	オン	はい

コンテナの複製

BlackBerry UEM がデバイス上で重複しているコンテナを識別した場合、それらを削除するためのバッチジョブをスケジュールします。重複したコンテナは、同じデバイス上の別のコンテナと同じユーザー ID と権利 ID（BlackBerry Dynamics アプリ ID とも呼ばれます）を持っています。重複したコンテナが削除されると、BlackBerry UEM ログファイルに記録されます。

プロパティ	説明	デフォルト	再起動
プロビジョニング後、ユーザーの同じデバイス上の古い重複するコンテナを自動的に削除する	新しいバージョンのアプリがプロビジョニングされたときに、BlackBerry UEM で重複するコンテナを自動的に削除するかどうかを指定します。この設定を選択している場合は、他の重複するコンテナのプロパティよりも優先されます。	オン	いいえ
重複するコンテナを自動的に削除するジョブを有効にする（オン/オフ）	BlackBerry UEM で重複するコンテナを識別してデバイスから削除するジョブを自動的にスケジュールするかどうかを指定します。	オン	いいえ
重複するコンテナが削除されるまでの非アクティブタイムアウト時間（秒）	BlackBerry UEM が重複するコンテナを削除するジョブをスケジュールする前に、重複するコンテナが非アクティブになっている必要がある時間（秒）。	259200	いいえ
重複するコンテナを削除するジョブが実行される頻度（秒）	BlackBerry UEM で重複するコンテナを識別して削除するジョブを実行する間隔（秒）。	86400	いいえ
1 つのジョブで削除するコンテナの最大数	1 つのジョブでデバイスから削除できる非アクティブなコンテナの最大数。	100	いいえ

Kerberos 制約付き委任

プロパティ	説明	デフォルト	再起動
明示的な UPN を使用	Microsoft Active Directory または Office 365 の Exchange ActiveSync と統合されたサービスへの認証時に BlackBerry Dynamics アプリが明示的な UPN または暗黙的な UPN を使用するかどうかを指定します。組織の Active Directory は、環境に応じて、両方のオプションをサポートするか、いずれか 1 つのオプションのみをサポートする場合があります。	オフ	いいえ
KCD を有効にする（gc.krb5.enabled）	BlackBerry UEM が BlackBerry Dynamics アプリの Kerberos 制約付き委任をサポートするかどうかを指定します。	オフ	はい

その他

プロパティ	説明	デフォルト	再起動
config.command.expiry	未応答のメッセージを再送信するまでに、BlackBerry UEM が待機する時間（秒）。	60	はい
config.command.retry	BlackBerry UEM で未応答のメッセージを識別して再送信するタスクを実行する間隔（秒）。0 に設定されている場合、BlackBerry UEM はタスクを実行しません。	900	はい
gc.entgw.report.userinfo	ユーザーの表示名が BlackBerry Dynamics NOC に報告されるかどうかを指定します。	オフ	いいえ
policy.compliance.interval	BlackBerry UEM がすべてのポリシーセットのコンプライアンスポリシーを BlackBerry Dynamics から取得する頻度（分）。	1440	はい

非アクティブなコンテナの消去

BlackBerry UEM がデバイス上で非アクティブなコンテナを識別した場合、それらを削除するためのバッチジョブをスケジュールします。BlackBerry UEM は、コンテナがデフォルトの 90 日間 BlackBerry UEM に接続されていない場合、コンテナを非アクティブと見なします。非アクティブなコンテナが削除されると、BlackBerry UEM ログファイルに記録されます。

プロパティ	説明	デフォルト	再起動
非アクティブなコンテナを自動的に削除するジョブを有効にする（オン/オフ）	BlackBerry UEM で非アクティブなコンテナを識別してデバイスから削除するジョブを自動的にスケジュールするかどうかを指定します。	オフ	いいえ
コンテナの非アクティブ間隔（秒）	BlackBerry UEM コンテナが非アクティブと見なされるまでの時間（秒）。	7776000	いいえ
非アクティブなコンテナを削除するジョブが実行される頻度（秒）	BlackBerry UEM で非アクティブなコンテナを識別して削除するジョブを実行する間隔（秒）。	86400	いいえ
1 つのジョブで削除するコンテナの最大数	1 つのジョブでデバイスから削除できる非アクティブなコンテナの最大数。	100	いいえ

レポート作成

プロパティ	説明	デフォルト	再起動
メモリ不足を防止するためにエクスポート可能なレポートで返されるレコードの制限を設定します。	レポートに含めることができる行の最大数。入力できる最大値は 1000000 です。	5000	いいえ

データ保持ポリシー

プロパティ	説明	デフォルト	再起動
データベースでの読み取り操作のログ記録	BlackBerry Control が BlackBerry Control データベースでの読み取り操作をログに記録するかどうかを指定します。	オン	はい
サーバージョブの消去	BlackBerry UEM が一定の間隔でサーバージョブを自動的に消去するかどうかを指定します。	オン	はい
サーバージョブの消去間隔（日数）	［サーバージョブの消去］がオンになっている場合に、BlackBerry UEM がサーバージョブを消去する間隔（日数）を指定します。	30	はい

BlackBerry Dynamics プロパティ

次の表に、各組織の BlackBerry UEM Core インスタンスに設定できるプロパティを示します。

Kerberos 制約付き委任

プロパティ	説明	デフォルト	再起動
GC サーバー上の krb5.config ファイル（gc.krb5.config.file）の場所	複数の Kerberos のドメインとの CAPATH 信頼関係がある場合に領域間の認証に使用される krb5.conf ファイル	設定なし	はい
KCD デバッグモードの有効化（gc.bkr5.debug）	BlackBerry UEM がデバッグレベルのデータをログに記録するかどうか。	オフ	はい
KDC の完全修飾名（gc.krb5.kdc）	Kerberos キー配布センター（KDC）サービスをホストするサーバーの FQDN。	設定なし	はい
Keytab ファイルの場所（gc.krb5.keytab.file）	Kerberos をホストしているコンピューター上の BlackBerry UEM keytab ファイルの場所。	設定なし	はい
KCD サービスが実行されているサービスアカウント名（gc.krb5.principal.name）	Kerberos アカウントのユーザー名。ドメインまたは領域を含めないでください。	設定なし	はい
領域 - Active Directory（gc.krb5.realm）	Kerberos アカウントの領域。	設定なし	はい

BlackBerry Proxy プロパティ

次の表に、各組織の BlackBerry Proxy インスタンスに設定できるプロパティを示します。

プロパティ	説明	デフォルト	再起動
gp.gps.max.sessions	アクティブなセッションの最大数	15000	—
gp.gps.dns.server.ttl.ms	DNS サーバーの応答を待機する時間（ミリ秒）。	1800000	—
gp.gps.server.flowcontrol	サーバーでフロー制御が有効になっているかどうかを指定します。	オフ	—
gp.gps.tcp.keepalive	サーバーで TCP キープアライブが有効になっているかどうかを指定します。	オフ	—

プロパティ	説明	デフォルト	再起動
gp.gps.unalias.hostname	アプリサーバーの DNS ルックアップには、IP アドレスまたはホスト名を使用します。 このオプションを選択した場合、BlackBerry Proxy は、アプリサーバーの IP アドレスを使用したリバース DNS 参照を使用します。 このオプションを選択しない場合、BlackBerry Proxy は、DNS 参照にアプリサーバーのホスト名を使用します。	オフ	はい
gps.directconnect.suppo	BlackBerry Direct Connect を介して行われたブリッジングと通信を暗号化する暗号スイートを追加または変更します。 独自のプロキシサーバーを Direct Connect 用に設定し、クライアントデバイスと BlackBerry Proxy サーバーとの間に配置することもできます。独自のプロキシサーバーを追加した場合は、BlackBerry Proxy サーバーの暗号が独自のプロキシサーバーで必要な暗号と対応していることを確認してください。 メモ：すべての暗号は、Java でサポートされている必要があります。	TLS_ECDHE_RSA_WI	はい _CBC_SHA3
gp.directconnect.supported.protocols	システムの直接接続ブリッジでサポートする暗号化プロトコルを追加または変更します。	TLSv1、TLSv1.1、TLSv1.2	はい
gp.eacp.command.servic	Active Directory サーバーに対して TCP を介した LDAP を有効にします。Active Directory サーバーは、TCP プロトコルを使用した LDAP サービスを提供しているので、クライアントは、_ldap._tcp 形式の DNS レコードを紹介することによって LDAP サーバーを見つけます。DnsDomainName. このオプションを選択した場合、BlackBerry Proxy は、指定されたサービスホスト名の nslookup に LDAP を使用します。 このオプションを選択しない場合、BlackBerry Proxy は、指定したサービスホスト名を使用して、リバース DNS 参照を直接使用します。	オフ	はい
gc.mdc.hb.timeout	ハートビートタイムアウトを指定します。	0	–

プロパティ	説明	デフォルト	再起動
gp.server.secure.ciphers	BlackBerry Proxy サーバーを介して行われた通信を暗号化する暗号スイートを追加または変更します。 メモ：すべての暗号は、Java でサポートされている必要があります。	TLS_ECDHE_RSA_WI	ー
gp.server.secure.protocols	BlackBerry Proxy サーバーでサポートする暗号化プロトコルを追加または変更します。	TLSv1、TLSv1.1、TLSv1.2	

BlackBerry Dynamics アプリの通信設定

組織のドメインの BlackBerry Dynamics アプリの通信設定を実行できます。通信設定を使用すると、選択したプロトコルを使用してネットワーク内でセキュリティ保護された通信を提供できます。デフォルトでは、TLS v1.2 のみが許可されます。また、TLSv1 および v1.1 を許可することもできます。プロトコルを 1 つ以上選択する必要があります。

1. 管理コンソールのメニューバーで、［設定］ > ［**BlackBerry Dynamics**］をクリックします。
2. ［通信設定］をクリックします。
3. 必要に応じて設定します。
4. ［保存］をクリックします。

HTTP プロキシを介した BlackBerry Dynamics アプリデータの送信

BlackBerry Proxy とアプリケーションサーバーとの間で HTTP プロキシを介して BlackBerry Dynamics アプリデータを送信するように BlackBerry UEM を設定できます。BlackBerry Dynamics アプリは、手動プロキシ設定とアプリケーションサーバーへの接続用の PAC ファイルの両方をサポートしています。PAC ファイルを使用するには、アプリを BlackBerry Dynamics SDK 7.0 以降で開発する必要があります。手動設定と PAC ファイル設定の両方を設定する場合、PAC ファイルはそれをサポートするアプリに対して優先されます。旧バージョンの BlackBerry Dynamics SDK を使用して開発されたアプリは、手動設定を使用します。

BlackBerry Access は、BlackBerry Access を使用した閲覧にのみ適用される手動プロキシ設定および PAC ファイルアプリ設定もサポートしています。BlackBerry Access のプロキシ設定、または別のプロキシ設定を持つ他のアプリは、BlackBerry UEM プロキシ設定を上書きします。詳細については、『BlackBerry Access 管理ガイド』を参照してください。

メモ：BlackBerry Dynamics NOC への接続には、手動プロキシ設定も使用されます。プロキシはポート 443 にアクセスできる必要があります。ポートの要件の詳細については、BlackBerry Dynamics NOC への BlackBerry UEM 発信接続を参照してください。

PAC ファイルの考慮事項

BlackBerry Proxy で PAC ファイルを使用する場合は、次のサポート上の考慮事項に注意してください。

BlackBerry UEM は、次の PAC ファイルディレクティブをサポートしています。

- DIRECT
- PROXY（HTTPS プロキシとして処理 - HTTP CONNECT を使用して確立された接続）
- HTTPS（HTTP CONNECT を使用して確立された接続）

BlackBerry UEM は、次の PAC ファイルディレクティブをサポートしていません。

- BLOCK（DIRECT として処理）
- SOCKS（接続エラーが発生）
- SOCKS4（接続エラーが発生）
- SOCKS5（接続エラーが発生）
- HTTP（接続エラーが発生）
- BlackBerry Access によって定義されたカスタム「NATIVE」ディレクティブ（接続エラーが発生）

BlackBerry UEM には、PAC ファイルに関する次の追加の制限があります。

- dnsDomainIs 関数には、「_」および「*」の文字を含めることはできません。
- shExpMatch 関数には、「[0-9]」、「?」、「/^d」、または「d+」の表現を含めることはできません。
- URI からパスとクエリーを削除するオプションはサポートされていません。

の BlackBerry Dynamics アプリプロキシ設定の設定

グローバル BlackBerry Dynamics アプリプロキシ設定は、手動で設定することも、PAC ファイルを使用して設定することもできます。BlackBerry Proxy クラスターおよび個々のサーバーのグローバル設定を上書きすることができます。ただし、個々のサーバーの設定を上書きする複雑さのレベルは通常必須ではなく、推奨されません。

1. 次の操作のいずれかを実行します。

タスク	手順
グローバルアプリプロキシ設定を設定する	**a.** ［設定］ **>** ［インフラストラクチャ］ **>** ［**BlackBerry Router** とプロキシ］をクリックします。 **b.** ［グローバル設定］をクリックします。
クラスターのアプリプロキシ設定を設定する	**a.** ［設定］ **>** ［**BlackBerry Dynamics**］ **>** ［クラスター］をクリックします。 **b.** クラスター名をクリックします。 **c.** ［グローバル設定を上書き］をクリックします。
サーバーの手動アプリプロキシ設定を設定する	**a.** ［設定］ **>** ［インフラストラクチャ］ **>** ［**BlackBerry Router** とプロキシ］をクリックします。 **b.** ［グローバル設定を上書き］をクリックします。 メモ： サーバーのグローバルプロキシ設定を上書きする場合、PAC ファイルはサポートされません。

2. 次のオプションのいずれかを選択します。
   - 手動 **HTTP** プロキシを有効にする
   - **PAC** を有効にする

PAC ファイルは、アプリケーションサーバーへの接続でのみサポートされています。両方のオプションを設定すると、アプリケーションサーバーへの接続には PAC 設定が優先されます。PAC ファイルは、BlackBerry Dynamics SDK 7.0 以降で開発されたアプリでのみサポートされています。

3. ［手動 **HTTP** プロキシを有効にする］を選択した場合は、次の手順を実行します。
   a) 次のオプションのいずれかを選択します。
      - プロキシを使用して **BlackBerry Dynamics NOC** サーバーにのみ接続する
      - プロキシを使用してすべてのサーバーに接続する
      - プロキシを使用して指定されたサーバーにのみ接続する
   b) プロキシを使用して指定されたサーバーに接続する場合、＋をクリックして、追加のサーバーを指定します。
   c) ［アドレス］フィールドに、プロキシサーバーのアドレスを入力します。
   d) ［ポート］フィールドに、プロキシサーバーが待機するポート番号を入力します。
   e) PAC ファイルで指定されたプロキシが認証を必要とする場合、［認証を使用］を選択し、［ユーザー名］と［パスワード］を指定し、必要な場合はアプリが認証に使用する［ドメイン］を指定します。
4. ［**PAC** を有効にする］を選択した場合は、次の手順を実行します。
   a) ［**PAC URL**］フィールドに、PAC ファイルの URL を入力します。
   b) プロキシサーバーが認証を必要とする場合、［プロキシ認証をサポート］を選択し、［ユーザー名］と［パスワード］を指定し、必要な場合はアプリが認証に使用する［ドメイン］を指定します。

      プロキシ認証では、エンドユーザー認証資格情報はサポートされていません。
5. ［保存］をクリックします。

BlackBerry Dynamics アプリの Kerberos の設定

BlackBerry Dynamics アプリは、Kerberos 制約付き委任と Kerberos PKINIT の両方をサポートします。Kerberos 制約付き委任（KCD）と Kerberos PKINIT は Kerberos の別個の実装です。BlackBerry Dynamics アプリではどちらか一方をサポートできますが、両方はサポートできません。

Kerberos 制約付き委任（KCD）を使用すると、ユーザーはネットワーク資格情報を入力しなくても、企業リソースにアクセスできます。KCD では、ユーザーの資格情報を含まないキーで暗号化および復号化されるサービスチケットを使用します。

委任が設定されている場合、BlackBerry Dynamics アプリは BlackBerry UEM に認証を委任し、その代理として仕事用リソースへのアクセスを要求してもらいます。KCD はアクセスされるリソースを制約します。管理者はアクセス可能なネットワークリソースを制限できます。これを行うには、委任（BlackBerry UEM）が特定のサービスに対してのみ信頼できるアカウントとして実行されるように設定します。

たとえば、KCD が設定されておらず、アプリが mypage.mydomain.com などのリソースを要求した場合、アプリはユーザーに資格情報の入力を求めます。KCD を設定すると、BlackBerry Dynamics インフラストラクチャが認証を処理し、ユーザーはリソースの資格情報を入力するように求められません。

Kerberosは、Microsoft Active Directory の一部です。BlackBerry UEM で Kerberos 制約付き委任を設定する前に、Kerberos 環境が正しく機能していること、および内部リソースの制約付き委任の設定に関連する影響を理解していることを確認してください。Kerberos の一般または制約付き委任に関する情報が必要な場合は、適切な Microsoft ドキュメントを参照してください。

Kerberos PKINIT 認証は、BlackBerry Dynamics アプリと Windows KDC の間で信頼を直接確立します。ユーザー認証は、Microsoft Active Directory 証明書サービスによって発行された証明書に基づきます。PKINIT を使用するには、Kerberos 制約付き委任を BlackBerry UEM のアプリ設定で有効にしないでください。

このセクションの情報はガイドラインです。Kerberos および BlackBerry UEM の詳細について必要な場合は、BlackBerry テクニカルサポートにお問い合わせください。

ドメイン、レルム、フォレスト

単一レルム Kerberos 環境での BlackBerry UEM 動作は、1 つのコアまたは同じ設定の複数のコアで構成されます。複数レルム Kerberos環境での BlackBerry UEM 動作は、個別に設定された複数のコアで構成されます。

レルムは、ユーザーレルムまたはリソースレルムのいずれかであるエンティティのコレクションです。リソースレルムは、ユーザーレルム以外のレルムです。Kerberos では、レルム名は常に大文字で入力する必要があります。

ドメインはディレクトリサービスドメインで、最も頻繁に Active Directory から取得されます。

レルムとドメインという用語は、KCD 内では互換性があります。

単一レルム **Kerberos** 環境

1. BlackBerry Dynamics アプリは、内部サーバーまたはサービス（ターゲット）に要求を送信します。

   ターゲットには、ホスト名（サーバー名）または Kerberos と BlackBerry Dynamics で保護されるアカウントのいずれかを指定できます。たとえば、IIS がネットワークサービスとしてサーバー上で実行されている場合、ターゲットは IIS をネットワークとして実行しているサーバーです。一方、IIS がユーザー（IISSrvUser など）として実行されている場合、ターゲットはそのユーザー名 IISSrvUser になります。
2. ターゲットは、BlackBerry Dynamics がインターセプトする認証チャレンジで応答します。
3. BlackBerry Dynamics SDK は、ターゲットにアクセスするためのサービスチケットの要求を BlackBerry UEM に送信します。
4. BlackBerry UEM は、（内部 BlackBerry Dynamics プロトコルを介して）ユーザーまたはアプリを認証し、ターゲット上のサービスのユーザー（委任）に代わってサービスチケットを要求します。
5. Active Directory はローカルポリシーを確認します。ユーザーがターゲット上のリソースにアクセスする権限を持っていて、ターゲット上のリソースが許可（制約）されている場合、Active Directory はそのリソースのサービスチケットを BlackBerry UEM に返します。
6. BlackBerry UEM は、返されたサービスチケットから必要な情報を BlackBerry Dynamics SDK に送信します。
7. BlackBerry Dynamics アプリは、BlackBerry UEM からの情報を使用して、ターゲットへの認証を完了します。

複数レルム **Kerberos** 環境、単一フォレスト設定

複数レルム KCD 環境では、BlackBerry Dynamics クライアントはターゲットサーバーの DNS ドメインに基づいて KCD 要求を処理するために BlackBerry UEM Core を選択します。ターゲットが KCD ターゲットであると判定されると、BlackBerry Dynamics クライアントはターゲットと同じ DNS ドメイン内にある BlackBerry UEM Core サーバーのリストを決定し、要求を処理するためにこのリストから（優先度に基づいて）BlackBerry UEM Core をランダムに選択します。

そのような DNS が一致しない場合（ターゲットと同じ DNS ドメイン内に BlackBerry UEM Core サーバーがない場合）、クライアントはすべての BlackBerry UEM Core サーバーのリストからランダムに選択します。

メモ：リソース（Microsoft Exchange など）の FQDN 名が、リソースが存在する Kerberos レルムを正確に反映していない場合、BlackBerry UEM はリソースを正しく認証できない場合があります。たとえば、リソースの DNS プール名が cas.domain.com で、その DNS プール名の内部にある実際のサーバーが server1.alternatedomain.domain.com と server2.alternatedomain.domain.com の場合、SDK は正しいレルム内の BlackBerry UEM Core サーバーを見つけることができません。

SDK は、ターゲットホストの DNS ドメインをすべての BlackBerry UEM Core サーバーの DNS ドメインと比較することにより、Kerberos 要求が発生するとすぐに、追加のフェッチなしで、デバイス上で比較をオフラインで実行できます。ターゲットと同じ DNS ドメイン内の Core サーバーのリストが空の場合、SDK はサーバーの完全なリストを返します。それ以外の場合は、以前に生成されたリストが使用されます。リストはランダム化され、優先順位（第 1 位がプライマリ）も満たすように、さらにソートされます。SDK は上位 2 つのエントリを選択し、最上位の Core サーバーに KCD 要求を開始します。この要求が失敗すると、SDK は要求を 2 番目の Core サーバーに送信します。

詳細については、support.blackberry.com/community にアクセスし、記事 49304 を参照してください。

別のドメインの **BlackBerry UEM** および **BlackBerry Connectivity Node** の **DNS**

BlackBerry UEM サーバーと BlackBerry Connectivity Node サーバーは、多くの場合、同じ Kerberos ドメインにインストールされますが、同じドメインにインストールする必要はありません。BlackBerry Connectivity Node を DMZ または「犠牲」ワークグループにインストールできます。この設定を選択する場合は、次に示すように、必要なネットワーク設定をいくつか設定する必要があります。

BlackBerry Dynamics は、通常の Kerberos （または Kerberos 認証）と Kerberos 制約付き委任（KCD）との間で動作が異なり、ネットワーク設定に影響します。

- KCD では、BlackBerry UEM Core サービスはクライアントアプリの代わりにチケット発行サーバー（ドメインコントローラー）に認証チケットを要求します。
- 制約付き委任を使用しない Kerberos では、クライアントアプリがチケット発行の要求を行い、その要求は BlackBerry Proxy を通過します。つまり、BlackBerry Proxy が Kerberos ドメインコントローラー（サーバー）の名前の検出をできるようにする必要があります。ドメインネームシステム（DNS）では、この検出を有効にする Kerberos サービスを指定する SRV レコードを追加する必要があります。この SRV レコードは、CNAME レコードではなく、A レコードまたは AAAA レコードに関連付ける必要があります。次の構文は、example.com という名前のインターネットドメイン内の Kerberos ドメインコントローラー用です。

  ```
  _kerberos._tcp.example.com. 86400 IN SRV 0 5 88 kerberos.example.com
  ```

  これは、Kerberos 要求を TCP ポート 88 で待機する kerberos.example.com という名前のサーバーを指します。優先度は 0、重みは 5 です。

前提条件

- Active Directory サービスのポート 88 は、すべての BlackBerry UEM サーバーからアクセスできる必要があります。
- Kerberos 環境には、次のコンポーネントが含まれている必要があります。
  - Microsoft Active Directory サーバー：Windows ネットワークに関連付けられているすべてのユーザーとコンピューターを認証および承認するディレクトリサービス
  - Kerberos キー配布センター（KDC）：Active Directory ドメイン内のユーザーとコンピューターにセッションチケットとキーを提供する Active Directory サーバー上の認証サービス

- すべての HTTP サービス（BlackBerry Enterprise Mobility Server およびその他のサービスを含む）のサービスプリンシパル名（SPN）を作成します。デバイスがアクセスできるようにするターゲットリソースごとに SPN を設定する必要があります。例：

  ```
  setspn -S HTTP/SPHOST.FQDN:PORT domain\AppPoolUser
  ```

  SPN の作成および変更方法の詳細については、docs.microsoft.com を参照して、「Kerberos 接続のサービスプリンシパル名の登録」を参照してください。SPN は、アプリサーバーまたは Active Directory サーバーの所有者が設定する必要があります。

複数レルム Kerberos 環境の場合：

- 各 Kerberos レルムには少なくとも 1 つの BlackBerry UEM Core サーバーをインストールする必要があります。レルム間のリソース委任はサポートされていないため、BlackBerry UEM はリソースと同じ Kerberos レルム内に存在する必要があります。
- 複数レルム KCD を設定する前に、単一レルム KCD が動作していることを確認します。
- すべての信頼は、双方向で推移的なフォレストの信頼である必要があります。

  重要：BlackBerry UEM Core サーバーと Microsoft SQL Server データベースの間には、最大 5 ミリ秒の遅延時間を確保してください。詳細については、「BlackBerry UEM のハードウェア要件」を参照してください。

Kerberos 制約付き委任の設定

複数レルム設定の場合は、常に最初に単一レルムを設定してテストしてから、他のレルムまたはフォレストの追加に進みます。

メモ：BlackBerry Docs 用に KCD を設定する場合は、「Docs サービスの Kerberos 制約付き委任の設定」を参照してください。

メモ：keytab ファイルの詳細については、support.blackberry.com にアクセスし、記事 42712 を参照してください。

1. Kerberos サービスアカウントをサービスプリンシパル名（SPN）にマッピングします。Active Directory サーバーで管理者コマンドプロンプトを開き、`setspn -s GCSvc/UEM_Core_host_machine DOMAIN\Kerberos_service_account` と入力します。

   ホストサーバー名、ドメイン、およびサービスアカウントの変数を環境に適した値に置き換えます。

   例：

   ```
   setspn -s GCSvc/uem1.example.com example.com\kcdadmin
   ```

   メモ：Kerberos サービスアカウントは、BlackBerry UEMで KCD サービスを設定するサービスアカウント名（gc.krb5.principal.name）です。このアカウントは、BlackBerry UEM サービスアカウントと同じである必要はありませんが、同じでもかまいません。

2. Kerberos keytab ファイルを作成します。Kerberos アカウントパスワードを変更するときは、新しい keytab ファイルを生成して BlackBerry UEM サーバーにコピーする必要があります。

   Kerberos keytab ファイルを作成すると、Kerberos アカウントパスワードも設定されます。このコマンドで設定されたパスワードにより、コマンドで指定したアカウントのパスワードが設定されます。すでにパスワードが与えられている場合は、必ず同じパスワードを使用してください。異なるパスワードを使用すると、パスワードがリセットされます。UEM サービスアカウントを使用して keytab ファイルを作成する場合、このパスワードには BlackBerry UEM サービスアカウントのパスワードも含まれます。keytab ファイルを作成するには、次の操作を実行します。

   a) KDC サーバー上でコマンドプロンプトウィンドウを開きます。

b) ktpass コマンドを使用します。ktpass コマンドの詳細については、docs.microsoft.com を参照してください。

```
ktpass -out outfilename.keytab -mapuser kerberos_account@REALM_IN_ALL_CAPS
-princ kerberos_account@REALM_IN_UPPERCASE/ptype KRB5_NT_PRINCIPAL -pass
kerberos_account_password
```

outfilename	これは出力ファイルの名前です。
kerberos_account	これは Kerberos アカウントの名前です。
REALM_IN_UPPERCASE	これは Kerberos レルムです。名前には大文字のみを使用する必要があります。
-pass kerberos_account_password	これは、再利用された Kerberos アカウントの既存のパスワードです。kerberos_account_password に ^ などの特殊文字が含まれている場合は、二重引用符で囲みます。

例：

```
ktpass -out outfilename.keytab -mapuser kerberos_account@REALM_IN_UPPERCASE
 -princ kerberos_account@REALM_IN_UPPERCASE /ptype KRB5_NT_PRINCIPAL -pass
 kerberos_account_password
```

または

```
ktpass /out outfilename.keytab /mapuser kerberos_account@REALM_IN_UPPERCASE /
princ kerberos_account@REALM_IN_UPPERCASE /ptype KRB5_NT_PRINCIPAL /pass
 kerberos_account_password
```

c) このディレクトリに保存されている新しい keytab ファイル（例では kcdadmin.keytab）を BlackBerry UEM サーバーにコピーします。重要：同じ KCD 管理者アカウントを使用するように設定されている BlackBerry UEM Core サーバーが複数ある場合は、すべての BlackBerry UEM サーバーに keytab ファイルをコピーする必要があります。

keytab ファイルは、c:\keytab など、サーバー上の任意の場所にコピーできます。この場所は後で参照するので、メモしておきます。

3. AD ユーザーオブジェクトグループメンバーシップの列挙を有効にします。詳細については、docs.microsoft.com にアクセスして「Active Directory の特権アカウントとグループ」を参照してください。
4. BlackBerry UEM サーバーで、ユーザー資格情報を Kerberos システムに送信できるように BlackBerry UEM サービスアカウントの権限を設定します。これは、関連付けられているサービスプリンシパル名（SPN）を持つアカウントと同じです。権限を設定するには、次の操作を実行します。
   a) Windows コンソールで［ローカルセキュリティポリシー］ペインを開きます。
   b) ［ローカルポリシー］で、［ユーザー権限の割り当て］ を選択し、右側のパネルで［オペレーティングシステムの一部として機能］を右クリックし、［プロパティ］を選択します。
   c) ［プロパティ］ウィンドウで、［ユーザーまたはグループの追加］をクリックし、サービスアカウントの名前を入力して、［**OK**］をクリックします。
5. BlackBerry UEM で Kerberos 関連のプロパティを設定します。

各 BlackBerry UEM Core サーバーの BlackBerry UEM 設定では、KDC（ドメインコントローラー）を 1 つだけ指定できます。つまり、ドメインコントローラーへの KCD 関連のすべてのコールは、常にその 1 つの KCD に移動します。これは、その 1 つの KDC がダウンした場合、すべての KCD コールが失敗することを意味します。

- UEM で KCD を有効にするには、［設定］ > ［BlackBerry Dynamics］ > ［グローバルプロパティ］で、次の設定を行う必要があります。

プロパティ	説明
明示的な UPN を使用	このプロパティを有効にすると、ユーザーのエイリアスとドメインを組み合わせて生成される暗黙的な UPN ではなく、Active Directory に保存された明示的な UPN を使用して、BlackBerry UEM に認証を強制的に実行させることができます。
KCD を有効にする（gc.krb5.enabled）	KCD を有効にするには、このチェックボックスをオンにします。

- UEM で KCD を有効にするには、［設定］ > ［BlackBerry Dynamics］ > ［プロパティ］（サーバー名をクリック）で、次の設定を行う必要があります。

プロパティ	例	説明
gc.krb5.kdc=<kdc_host_name>	UEM1.EXAMPLE.COM	KDC の完全修飾名。通常、Active Directory ドメインコントローラーの FQDN に対応します。
gc.krb5.keytab.file=<keytab_file_location>	c:/keytab/kcdadmin.keytab	keytab ファイルの場所。パス名には、バックスラッシュではなく、スラッシュを使用してください。
gc.krb5.principal.name=<kcd_service_account>	kcdadmin@EXAMPLE.COM	KCD サービスで使用されるサービスアカウントの名前。
gc.krb5.realm=<REALM>	EXAMPLE.COM	Active Directory レルムの名前。値はすべて大文字にする必要があります。

6. （オプション）krb5.conf ファイルを作成します。これは、CAPATH 信頼がある場合にのみ必要です。このファイルを作成する必要がある場合は、Active Directory チームに問い合わせてください。

   複数の Kerberos ドメインの CAPATH 信頼関係を確立するには krb5.conf ファイルが必要です。BlackBerry UEM サーバー上の krb5.conf ファイルの場所は、サーバープロパティ gc.krb5.config.file で指定する必要があります。

   krb5.conf ファイルの例：

```
[libdefaults] default_realm = NA.POD1.COM [realms] NA.POD1.COM = { kdc
 = pod1-na-ad.na.pod1.com } [ capaths] NA.POD1.COM = { APAC.POD2.COM =
 POD2.COM POD2.COM = POD1.COM POD1.COM = . } POD2.COM = { NA.POD1.COM =
```

```
POD1.COM POD1.COM = . } APAC.POD2.COM = { NA.POD1.COM = POD1.COM POD1.COM =
POD2POD2.COM POD2.COM = .}
```

トラブルシューティングと診断

ログファイルを使用して、システム管理者が修正または調査および解決のために BlackBerry テクニカルサポートに送信できる問題を検出するのに役立ちします。また、BlackBerry ナレッジベースで情報を検索することもできます。

ログを表示するには、デバッグログを有効にします。

Kerberos および KCD ログファイルのエラーコード

BlackBerry UEM サーバーログに記録された情報は、Kerberos 認証や KCD の問題やエラーの説明に役立つことがよくあります。Kerberos エラーログの例を次に示します。

```
2019-06-26T13:23:19.424-0500 - CORE {ContainerMgmtServerThread#1}
 none|none [{{externalTenantId,S12345678}}] - ERROR KRB u=
 B32F95DF-4338-499A-A06D-7EAC36852A21 while requesting KRB ServiceTicket
 for serviceClass= HTTP server= uem1.example.com port= 443 serviceName=
 httpcom.rim.platform.mdm.dynamics.kerberos.KerberosException: Failed to
 impersonate userPrincipal KCDADMIN@UEM1.EXAMPLE.COM;
             krbErrCode: 63;
             krbErrText: Fail to create credential.
```

エラーメッセージで最も重要なパラメータは、krbErrCode と krbErrText の 2 つです。これらのパラメータは、検出された考えられるエラー状態の説明を提供します。

Kerberos エラーメッセージの完全なリストについては、docs.microsoft.com にアクセスして「Kerberos および LDAP エラーメッセージ」を参照してください。

Kerberos PKINIT の設定

BlackBerry UEM は、PKI 証明書を使用した BlackBerry Dynamics ユーザー認証に Kerberos PKINIT をサポートしています。

BlackBerry Dynamics アプリで Kerberos PKINIT を使用する場合、組織で次の要件を満たす必要があります。

重要なポイント

- Kerberos 制約付き委任を無効にする必要があります。
- KDC ホストは BlackBerry Dynamics 接続プロファイルの［許可ドメイン］リストに追加する必要があります。
- KDC ホストは、TCP ポート 88（Kerberos デフォルトポート）で待機する必要があります。
- BlackBerry Dynamics は、UDP を介した KDC をサポートしていません。
- KDC は、DNS に A レコード（IPv4）または AAAA レコード（IPv6）を必要とします。
- BlackBerry Dynamics は、正しい KDC の検索に、Kerberos 設定ファイル（`Krb5.conf` など）を使用しません。
- KDC は、クライアントに別の KDC ホストを参照させることができます。BlackBerry Dynamics は、参照される KDC ホストが BlackBerry Dynamics 接続プロファイルの［許可ドメイン］リストに追加されている限り、照会に従います。
- KDC は、別の KDC ホストから BlackBerry Dynamics へ TGT を透過的に取得できます。

サーバー証明書

- Active Directory 証明書サービスで発行された Windows KDC サーバー証明書は、以下の Windows Server バージョンだけからのものである必要があります。これ以外のサーバーバージョンはサポートされていません。
  - Windows Server 2008 R2 を含んだインターネット情報サーバー
  - Windows Server 2012 R2 を含んだインターネット情報サーバー
- 有効な KDC サービス証明書が、BlackBerry Dynamics 証明書ストアまたはデバイス証明書ストアのいずれかに置かれている必要があります。

クライアント証明書

- 証明書の最小キー長は 2,048 バイトにする必要があります。
- クライアント証明書は、https://support.microsoft.com/en-us/kb/287547 で Microsoft が指定しているように、オブジェクト ID szOID_NT_PRINCIPAL_NAME 1.3.6.1.4.1.311.20.2.3 のサブジェクトの別名に、ユーザープリンシパル名（user@domain.com など）を含めている必要があります。
- ユーザープリンシパル名のドメインは、Windows KDC サービスの領域の名前と一致している必要があります。
- 証明書の拡張キー使用法プロパティは Microsoft スマートカードログオン（1.3.6.1.4.1.311.20.2.2）である必要があります。
- 証明書が有効である必要があります。上記のサーバーに照らして確認してください。

BlackBerry UEM と Cisco ISE を統合

Cisco Identity Services Engine （ISE）は、デバイスが組織の仕事用ネットワークにアクセスできるかどうかを制御する機能を提供する、ネットワーク管理ソフトウェアです（たとえば、Wi-Fi の許可または拒否、VPN 接続など）。Cisco ISE 管理者は、許可されたデバイスのみが仕事用ネットワークにアクセスできることを確実に行うための、アクセスポリシーを作成し適用できます。

Cisco ISE および BlackBerry UEM の間の接続を作成できるので、Cisco ISE は BlackBerry UEM 上でアクティベーションされたデバイスに関するデータを取得できます。Cisco ISE はデバイスデータを確認し、デバイスがアクセスポリシーに準拠しているかどうかを判断します。例：

- Cisco ISE は、ユーザーのデバイスが BlackBerry UEM 上でアクティベーションされているかどうかを確認します。デバイスがアクティベーションされていない場合、アクセスポリシーにより、デバイスの仕事用 Wi-Fi または VPN アクセスポイントへの接続を阻止できます。
- Cisco ISE は、ユーザーのデバイスが BlackBerry UEM に準拠しているかどうかを確認します。デバイスが準拠していない場合（たとえば、デバイスがルート化や脱獄をしているなど）、アクセスポリシーにより、デバイスの仕事用 Wi-Fi または VPN アクセスポイントへの接続を阻止できます。

Cisco ISE 管理者は、Cisco ISE 管理コンソール内のデバイスに関するデータを、表示、ソート、フィルタリングできます。管理者はまた、デバイスのロック、デバイスからの仕事用データの削除、またはデバイスからのすべてのデータの削除などのデバイス管理タスクを実行できます。

BlackBerry UEM と Cisco ISE を統合するには、次の操作を実行します。

手順	アクション
1	所属組織の環境が BlackBerry UEM と Cisco ISE を統合するための要件を満たしていることを確認します。
2	Cisco ISE がデバイスに関するデータを取得するのに使用できる、BlackBerry UEM 管理者アカウントを作成します。
3	BlackBerry Web Services 証明書を Cisco ISE 証明書ストアに追加します。
4	BlackBerry UEM を Cisco ISE に接続し、認証プロファイルとアクセスポリシーを設定します。

要件：BlackBerry UEM と Cisco ISE の統合

項目	要件
Cisco ISE のバージョン	BlackBerry UEM は、Cisco ISE バージョン 1.2 以降との統合をサポートします。

項目	要件
サポートされる OS	次を除く、BlackBerry UEM がサポートするすべてのオペレーティングシステム（「互換性一覧表」を参照してください）。 • BlackBerry 10 OS バージョン 10.3.2 以前（10.3.3 以降が必要） • BlackBerry OS（バージョン 7.1 以前） • デスクトップ向け Windows 10
待機ポート	Cisco ISE は、BlackBerry UEM からデバイスに関するデータを取得するために、デフォルトの BlackBerry Web Services 待機ポート 18084 を使用します。 BlackBerry UEM のインストール時にポート 18084 が使用不可だった場合、セットアップアプリケーションはこの目的のために別の有効なポートを選択します。正しいポート値を確認するには、BlackBerry UEM Core ログファイル（CORE）で `(^/ciscoise/.*)` を検索し、このテキストのすぐ前に表示されているポート番号を記録します。
ファイアウォール	ファイアウォールが BlackBerry UEM と Cisco ISE の間に存在する場合は、両システム間の HTTPS セッションを許可するようにファイアウォールを設定します。

Cisco ISE が使用できる管理者アカウントを作成する

Cisco Identity Services Engine （ISE）は、デバイスに関するデータの取得に使用できる、専用の BlackBerry UEM 管理者アカウントを必要とします。既存の管理者アカウントを使用するか、新しい管理者アカウントを作成します。この管理者アカウントは、ディレクトリユーザーではなく、ローカル管理者アカウントである必要があります。この管理者アカウントは、次の権限を持つロールを必要とします。

- ユーザーとアクティブ化されたデバイスを表示
- デバイスの管理
- デバイスをロックしてメッセージを設定
- 仕事用データのみを削除
- すべてのデバイスデータを削除

デフォルトのセキュリティ管理者とエンタープライズ管理者のロールに、これらの権限があります。カスタムロールを持つ管理者アカウントを新規作成するには、セキュリティ管理者ロールを持つ管理者アカウントを使用して、次の手順を実行します。

作業を始める前に： 管理者アカウントのカスタムロールを作成するには、BlackBerry UEM 管理コンソールで、［設定］ > ［管理者］ > ［ロール］ > をクリックします。必要な権限を選択します。［保存］をクリックします。

1. BlackBerry UEM 管理コンソールのメニューバーで、［ユーザー］をクリックします。
2. ［ユーザーを追加］をクリックします。
3. ［ローカル］タブをクリックします。
4. 名、姓、表示名、ユーザー名、およびメールアドレスを指定します。
5. ［コンソールのパスワード］フィールドに、管理者アカウントのパスワードを入力します。
6. ［デバイスアクティベーションパスワードを設定しない］オプションを選択します。

7. ［保存］をクリックします。
8. メニューバーで［設定］をクリックします。
9. ［管理者］ > ［ユーザー］をクリックします。
10. をクリックします。
11. 作成したユーザーアカウントを検索してクリックします。
12. ［ロール］ドロップダウンリストで、作成したカスタムロール、デフォルトのセキュリティ管理者ロール、またはデフォルトのエンタープライズ管理者ロールをクリックします。
13. ［保存］をクリックします。

終了したら： BlackBerry Web Services 証明書を Cisco ISE 証明書ストアに追加します。

BlackBerry Web Services 証明書を Cisco ISE 証明書ストアに追加します。

Cisco Identity Services Engine と接続するために BlackBerry UEM （ISE）を有効にするには、BlackBerry Web Services 証明書をエクスポートして、その証明書を Cisco ISE 証明書ストアにインポートする必要があります。所属組織の BlackBerry UEM ドメインに複数の BlackBerry UEM のインスタンスがある場合、1 つのインスタンスから証明書をエクスポートするだけで済みます。

Cisco ISE 管理者アカウントを所有していない場合は、これらの手順を Cisco ISE 管理者に送付してください。

メモ： 手順 3 以降は、Cisco ISE バージョン 1.4 に基づきます。最新の Cisco ISE ドキュメントについては、Cisco ISE の設定ガイドの『*Cisco Identity Services Engine* 管理者ガイド』を参照してください。

作業を始める前に： Cisco ISE が使用できる管理者アカウントを作成する。

1. ブラウザーで **https://*<server_name>*:*<BlackBerry_Web_Services_port>*/enterprise/admin/util/ws?wsdl** に移動します。ここで *<server_name>* は BlackBerry UEM Core コンポーネントをホストするコンピューターの FQDN です。*<BlackBerry_Web_Services_port>* のデフォルト値は 18084 です。
2. BlackBerry Web Services 証明書をエクスポートし、デスクトップに保存します。手順については、使用しているブラウザーのドキュメントを参照してください。

   例：Google Chrome では、URL の横の鍵アイコンをクリックします。［接続］タブで、［証明書情報］をクリックします。［詳細］タブで［ファイルにコピー］をクリックし、画面上の手順に従います。
3. Cisco ISE 管理コンソールにログインします。
4. メニューバーで、［**Administration**］ > ［**System**］ > ［**Certificates**］をクリックします。
5. 左ペインで、［**Trusted Certificates**］をクリックします。
6. ［インポート］をクリックします。BlackBerry Web Services 証明書を参照し選択します。
7. ［**Trust for client authentication and Syslog**］チェックボックスをオンにします。
8. ［**Trust for authentication of Cisco Services**］チェックボックスをオンにします。
9. ［送信］をクリックします。

終了したら： BlackBerry UEM を Cisco ISE に接続する。

BlackBerry UEM を Cisco ISE に接続する

Cisco Identity Services Engine （ISE）管理者アカウントを所有していない場合は、BlackBerry UEM および BlackBerry UEM 管理者アカウントに関する必要な情報とともに、これらの手順を Cisco ISE 管理者に送付してください。

メモ： 次の手順は、Cisco ISE バージョン 1.4 に基づいています。最新の Cisco ISE ドキュメントについては、Cisco ISE の設定ガイドの『*Cisco Identity Services Engine* 管理者ガイド』を参照してください。

作業を始める前に： BlackBerry Web Services 証明書を Cisco ISE 証明書ストアに追加します。。

1. Cisco ISE 管理コンソールにログインします。
2. メニューバーで、［**Administration**］ > ［**Network Resources**］ > ［**External MDM**］をクリックします。
3. ［追加］をクリックします。
4. ［**Name**］フィールドに、接続のわかりやすい名前を入力します。
5. ［**Hostname or IP address**］フィールドに、BlackBerry UEM ドメインの FQDN または IP アドレスを入力します。
6. ［**Port**］フィールドに「`18084`」と入力します。

   BlackBerry UEM のインストール時にポート 18084 が使用不可だった場合、セットアップアプリケーションはこの目的のために別の有効なポートを選択します。正しいポート値を確認するには、BlackBerry UEM Core ログファイル（CORE）で (`^/ciscoise/.*`) を検索し、このテキストのすぐ前に表示されているポート番号を記録します。
7. ［**User Name**］フィールドに、BlackBerry UEM 管理者アカウントのユーザー名を入力します。
8. ［**Password**］フィールドに、BlackBerry UEM 管理者アカウントのパスワードを入力します。
9. ［**Polling Interval**］フィールドで、デバイスデータのために Cisco ISE が BlackBerry UEM をポーリングする間隔を分単位で指定します。デフォルト値の 240 分を使用することをお勧めします。

   メモ： この値を 60 分以下に設定した場合、組織の環境に重大なパフォーマンスの影響を与える可能性があります。この値を 0 に設定した場合、Cisco ISE は BlackBerry UEM をポーリングしません。
10. ［**Enable**］チェックボックスをオンにします。
11. ［**Test Connection**］をクリックし、Cisco ISE が BlackBerry UEM に接続できることを確認します。
12. ［送信］をクリックします。

接続が確立した後、［**Policy**］ > ［**Policy Elements**］ > ［**Dictionaries**］ > ［**System**］ > ［**MDM**］ > ［**Dictionary Attributes**］で、BlackBerry UEM の辞書の属性を表示できます。Cisco ISE のポーリングのログエントリは、BlackBerry UEM Core （CORE）ログファイルに記録されます。

終了したら： Cisco ISE 管理コンソールで、次の設定タスクを実行します。最新の手順については、Cisco ISE の設定ガイドの『*Cisco Identity Services Engine* 管理者ガイド』を参照してください（「Set Up MDM Servers With Cisco ISE」を参照）。

- ワイヤレス LAN コントローラーで ACL を設定します。
- BlackBerry UEM でアクティブ化されていないデバイスをリダイレクトする、認証プロファイルを設定します。詳細については、「BlackBerry UEM でアクティブ化されていないデバイスのリダイレクト」を参照してください。
- BlackBerry UEM でアクティブ化されていないか BlackBerry UEM に準拠していないデバイスを、Cisco ISE が処理する方法を決定する、認証ポリシールールを設定します。［**Policy**］ > ［**Policy Sets**］で、ポリシーを作成します。ポリシーの例については、「例：BlackBerry UEM の認証ポリシールール」を参照してください。

例：BlackBerry UEM の認証ポリシールール

認証ポリシー

Authentication Policy

BES12Authentication	: If	Wireless_802.1X	Allow Protocols : Default Network Access	and	
Default	: use	Internal Users			
Default Rule (If no match)	:	Allow Protocols : None	and use : DenyAccess		

認可ポリシー

Authorization Policy

Exceptions (1)

Local Exceptions

Create a New Rule

Global Exceptions

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
	Blacklisted	if	**Blacklist**	then	Blackhole Access

Standard

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
	MDM_Un_Registered	if	MDM:DeviceRegisterStatus EQUALS UnRegistered	then	MDM_Quarantine
	MDM_Non_Compliant	if	MDM:DeviceCompliantStatus EQUALS NonCompliant	then	MDM_Quarantine
	PERMIT	if	**Any**	then	PermitAccess
	Default	if no matches, then	DenyAccess		

Cisco ISE を使用したネットワークアクセスとデバイス制御の管理

Cisco Identity Services Engine （ISE）管理者は次の操作を実行できます。手順については、『*Cisco Identity Services Engine* 管理者ガイド』の「Set Up MDM Servers With Cisco ISE」を参照してください。

アクション	説明
デバイスデータを表示する	BlackBerry UEM に関連付けられたデバイスに関する情報を表示できます。次の情報が表示されます。 • MAC アドレス：デバイス固有の MAC アドレス • コンプライアンス：デバイスが BlackBerry UEM に準拠しているかどうか • ディスクの暗号化：デバイスデータが暗号化されているかどうか • 登録：デバイスが BlackBerry UEM でアクティブ化されているかどうか • 脱獄：デバイスがルート化または脱獄されているかどうか • PIN ロック：デバイスがパスワードを使用しているかどうか • 製造元 • 機種 • シリアル番号 • OS バージョン
NAC ポリシーを設定する	デバイスが仕事用 Wi-Fi または VPN アクセスポイントに接続できるかどうかを制御する、アクセスポリシーを設定します。たとえば、BlackBerry UEM に準拠していないデバイスが、仕事用ネットワークにアクセスするのを防ぐアクセスポリシーを設定できます。
デバイスをロックする	ユーザーの、iOS、Android、または Windows デバイスをロックします（BlackBerry 10 デバイスではこの機能はサポートされません）。この機能は、ユーザーのデバイスが一時的に置き忘れられた場合に役立ちます。BlackBerry UEM は、IT 管理コマンドを使用してデバイスをロックします。ユーザーは、ロックを解除するために、デバイスパスワードを入力する必要があります。 デバイスユーザーが My Device portal を使用してこの操作を実行することもできます。
仕事用データを削除する	デバイスから、ユーザーの個人用データやアプリをそのまま残して、仕事用データのみと仕事用アプリを削除します。この機能は、ユーザーがデバイスを紛失したり、ユーザーが退職した場合に役立ちます。BlackBerry UEM は、IT 管理コマンドを使用して仕事用データを削除します。 デバイスユーザーが My Device portal を使用してこの操作を実行することもできます。

アクション	説明
すべてのデータを削除する	デバイスからすべてのデータとアプリを削除し、デバイスを工場出荷時のデフォルト設定に戻します。この機能は、ユーザーのデバイスが紛失または盗難されたり、デバイスが別のユーザーに渡った場合に役立ちます。BlackBerry UEM は、IT 管理コマンドを使用してすべてのデバイスデータを削除します。 デバイスユーザーが My Device portal を使用してこの操作を実行することもできます。

IT 管理コマンドの詳細、およびロック、仕事用データの削除、すべてのデータの削除のコマンドをサポートするアクティベーションタイプの詳細については、管理関連の資料を参照してください。

BlackBerry UEM でアクティブ化されていないデバイスのリダイレクト

Cisco Identity Services Engine （ISE）が仕事用ネットワーク（Wi-Fi または VPN）にアクセスしようとしているデバイスを識別し、そのデバイスが BlackBerry UEM でアクティブ化されていない場合、Cisco ISE はデバイスのブラウザーで、ユーザーを BlackBerry UEM Self-Service コンソールにリダイレクトする登録ページを開きます。

ユーザーが BlackBerry UEM Self-Service にログインしてデバイスをアクティブ化するには、BlackBerry UEM のユーザーアカウントが必要です。Cisco ISE による登録ページへのリダイレクトが表示された場合は BlackBerry UEM 管理者に問い合わせるようユーザーに指示してください。

ユーザーアカウントの追加およびアクティブ化に関する詳細については、管理関連の資料を参照してください。

メモ： ユーザーのデバイスが以前 BlackBerry UEM でアクティブ化され、その後無効化された場合、ユーザーがデバイスから仕事用ネットワークにアクセスしようとしても BlackBerry UEM Self-Service にリダイレクトされません。この問題を解決するには、BlackBerry UEM からデバイスを削除するときに、そのデバイスのデータを Cisco ISE から削除します。

商標などに関する情報

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Published in Canada