# BlackBerry UEM

## 設定ガイド

12.10

# 目次

# このガイドについて

BlackBerry UEM は、組織で BlackBerry 10、BlackBerry OS（バージョン 5.0～7.1）、iOS、macOS、Android、および Windows の各デバイスを管理するのに役立ちます。このガイドには、BlackBerry UEM を設定して組織のニーズに対応する方法が記載されています。

このガイドは、製品のセットアップと導入を担当するシニア IT プロフェッショナルを対象としています。このガイドのタスクを完了するには、事前に製品をインストールしてライセンスを取得する必要があります。インストール手順の詳細については、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。ライセンスの取得の詳細については、ライセンス関連の資料を参照してください。

このガイドのタスクを完了した後は、管理関連の資料を参照して、BlackBerry UEM の管理方法について学習します。

# はじめに

## 初めて BlackBerry UEM を設定する

次の表は、このガイドで説明する設定タスクの概要を示しています。タスクは、組織のニーズに応じて選択します。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、デバイスの制御のセットアップ、ユーザーおよびグループの作成、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 | 必須またはオプション | 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 | オプション | BlackBerry UEM コンソールが使用するデフォルトの SSL 証明書と BlackBerry UEM が iOS デバイスの MDM プロファイルの署名に使用するデフォルトの証明書を、信頼済みの証明書に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 | オプション | 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 | オプション | 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 | オプション | 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 | オプション | 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。 |
| BlackBerry UEM 管理者のシングルサインオンの設定 | オプション | BlackBerry UEM を Microsoft Active Directory に接続する場合は、シングルサインオン認証を設定すると、管理者またはユーザーがログイン Web ページをバイパスし、管理コンソールまたは BlackBerry UEM Self-Service に直接アクセスできるようになります。 |

| タスク | 必須またはオプション | 説明 |
| --- | --- | --- |
| APNS 証明書を取得して登録する | オプション | 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 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。 |
| Exchange ActiveSync にアクセス可能なデバイスの制御 | オプション | 許可リストに追加されていないデバイスが仕事用メールやオーガナイザーデータにアクセスしないように Microsoft Exchange を設定している場合は、BlackBerry UEM で Microsoft Exchange 設定を作成する必要があります。 |
| 仕事用プロファイルのある Android デバイスをサポートするように BlackBerry UEM を設定する | オプション | 仕事用プロファイルのある Android 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。 |
| Samsung KNOX デバイスの認証の管理 | オプション | 認証をオンにすると、BlackBerry UEM は、Samsung KNOX デバイスの完全性と整合性をテストするためのチャレンジを送信します。 |
| Apple の Device Enrollment Program 用 BlackBerry UEM の設定 | オプション | 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。 |
| BlackBerry UEM Self-Service をセットアップする | オプション | ユーザーにパスワードの変更などの特定の管理タスクの実行を許可するために、BlackBerry UEM Self-Service Web アプリケーションをセットアップして配布できます。 |
| BlackBerry Enterprise Identity を有効化する | オプション | BlackBerry Enterprise Identity を有効にして、Box、Concur、Dropbox、Salesforce、Workspaces などのサービスプロバイダーへのシングルサインオンアクセスを提供することができます。 |
| 高可用性を設定する | オプション | ユーザーのためにサービスの中断を最小限に抑えるために、複数のアクティブな BlackBerry UEM インスタンスをインストールできます。 |
| データベースミラーリングを設定する | オプション | 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。 |

| タスク | 必須またはオプション | 説明 |
| --- | --- | --- |
| Exchange ActiveSync への TLS/SSL 接続を確立するように BlackBerry UEM を設定する | オプション | BlackBerry Secure Gateway を有効にして、メールサーバーと MDM 制御 アクティベーションタイプの iOS デバイスの間でセキュリティ保護された接続を提供する場合は、Exchange ActiveSync サーバー証明書を BlackBerry UEM に追加する必要がある場合があります。 |
| 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 | オプション | 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。 |
| BlackBerry UEM を Microsoft Azure に接続する | オプション | 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。 |
| BES10 または から、ユーザー、グループ、およびその他のデータを移行する BlackBerry UEM | オプション | 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 BES10 または BlackBerry UEM から移行できます。 |
| BlackBerry Dynamics の設定 | オプション | 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 Dynamics アプリの証明書の設定 | オプション | ユーザーのデバイス上の BlackBerry Dynamics アプリがクライアント証明書を使用できるようにする場合は、個々のユーザーアカウントに証明書をアップロードするか、BlackBerry UEM が CA からのクライアント証明書を自動的に登録してデバイスに送信するように PKI コネクターを設定することができます。 |
| BlackBerry UEM と Cisco ISE を統合する | オプション | 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。 |
| SNMP 監視を設定する | オプション | サードパーティ SNMP ツールを使用して、BlackBerry UEM コンポーネントのアクティビティを監視できます。 |

# BlackBerry OS デバイスを管理するためのタスクを設定する

組織の BlackBerry UEM ドメインが BlackBerry OS（バージョン 5.0～7.1）デバイスをサポートする場合、BlackBerry OS デバイスの管理をカスタマイズできます。BES5 から BlackBerry UEM にアップグレードした場合、アップグレード前に実行された BES5 コンポーネントの設定はアップグレード後も元の状態を保つため、追加の設定タスクを実行する必要はありません。

表内の各タスクの手順の詳細については、help.blackberry.com/detectLang/category/enterprise-services にアクセスし、『*BlackBerry Enterprise Server 5* インストールおよび設定ガイド』または『*BlackBerry Enterprise Server 5* 管理ガイド』を参照してください。

| 目的 | リソース |
| --- | --- |
| カレンダーデータを管理するサービスを指定する<br>デフォルトでは、BlackBerry OS デバイスのカレンダーデータは Microsoft Exchange Web Services が管理します。ユーザーにこのサービスを使用する権限がない場合、ユーザーのカレンダーデータは、MAPI ライブラリおよび CDO ライブラリを使用して管理されます。Microsoft Exchange Web Services にのみ管理されるまたは MAPI ライブラリおよび CDO ライブラリにのみ管理されるカレンダーデータを選択できます。 | インストールおよび設定ガイド<br>• インストール後のタスク：BlackBerry Enterprise Server を設定して Microsoft Exchange Web Services を使用する |
| SNMP サービスを使用して、BlackBerry OS デバイスを管理するコンポーネントを監視する | インストールおよび設定ガイド<br>• インストール後のタスク：監視のためのコンピューターを設定する |
| エンタープライズサービスポリシーを使用して、BlackBerry UEM にアクセスできる BlackBerry OS デバイスを制御します。 | 管理ガイド<br>• セキュリティオプションを設定する：デバイスの BlackBerry Enterprise Server へのアクセスを管理する |
| BlackBerry MDS Connection Service、BlackBerry Collaboration Service、および BlackBerry Administration Service 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 | 管理ガイド<br>• BlackBerry Enterprise Server 環境の設定 |
| BlackBerry OS デバイスを管理するコンポーネントを高可用性に設定する | 管理ガイド<br>• BlackBerry Enterprise Server の高可用性の設定<br>• BlackBerry Enterprise Server コンポーネントの高可用性の設定<br>• BlackBerry Configuration Database の高可用性の設定 |
| BlackBerry OS デバイスの BlackBerry MDS Connection Service がプッシュデータを管理してユーザーに Web コンテンツへのアクセスを許可する方法を変更する | 管理ガイド<br>• エンタープライズアプリケーションおよび Web コンテンツへのユーザーのアクセス方法の設定<br>• エンタープライズアプリケーションおよび Web コンテンツへのユーザーのアクセス方法の管理 |

| 目的 | リソース |
| --- | --- |
| 拡張プラグインを使用して BlackBerry OS デバイスのメールや添付ファイルを処理および変更します。 | 管理ガイド<br>• メッセージ環境のセットアップ：メッセージを処理するための拡張プラグイン |
| BlackBerry OS デバイスに証明書の登録を許可し、アプリケーションやネットワークでの認証を実行できるようにします。 | 管理ガイド<br>• ワイヤレスネットワーク経由で証明書を登録するための BlackBerry デバイスの設定 |
| BlackBerry OS デバイスユーザーに、BlackBerry Web Desktop Manager を使用したセルフサービスタスクの実行を許可する | 管理ガイド<br>• ユーザーが BlackBerry Web Desktop Manager を使用できるようにする方法<br>• BlackBerry Web Desktop Manager の設定 |
| アプリ、OS の更新、設定が BlackBerry OS デバイスに送信される方法を変更する | 管理ガイド<br>• デバイスへの BlackBerry Java Application、BlackBerry Device Software、および BlackBerry デバイス設定の配信管理 |
| BlackBerry OS デバイスユーザーのオーガナイザーデータ同期の変更 | 管理ガイド<br>• オーガナイザーデータ同期の管理 |
| BlackBerry OS デバイスを管理するコンポーネントのメール設定と添付文書のサポートを変更する | 管理ガイド<br>• 組織のメッセージング環境および添付ファイルサポートの管理 |
| 場所、詳細レベル、最大サイズなどの様々なログファイル設定を変更する | 管理ガイド<br>• BlackBerry Enterprise Server ログファイル |
| BlackBerry OS デバイスが管理するコンポーネントが使用するポートを確認し、必要に応じて変更する | 管理ガイド<br>• BlackBerry Enterprise Solution の接続タイプとポート番号 |

# 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 Enterprise Mobility Suite サービス

BlackBerry UEM によって提供されるセキュリティおよび生産性機能に加え、BlackBerry は、BlackBerry UEM ドメインの価値を高めて組織固有のニーズを満たすことができる、複数のサービスを提供しています。次のサービスを追加し、BlackBerry UEM 管理コンソールから管理できます。

| サービスの種類 | サービス名と説明 |
| --- | --- |
| エンタープライズサービス | • BlackBerry Workspaces は、Windows および Mac OS のタブレットやコンピューター、または Android、iOS、BlackBerry 10 デバイスから、ユーザーがファイルやフォルダーに安全にアクセスし、これらを編集および共有できるようにします。BlackBerry Workspaces は、組織外のユーザーとファイルを共有した後でも、アクセスを制限する DRM コントロールを適用することで、ファイルを保護します。<br>• BlackBerry Enterprise Identity は、BlackBerry Workspaces、Box、Workday、WebEx、Salesforce などのサービスプロバイダーにユーザーがシングルサインオンでアクセスできるようにします。カスタム SaaS サービスのサポートを追加することもできます。<br>• BlackBerry 2FA は、ツーファクター認証で、組織の重要なリソースへのアクセスを保護します。BlackBerry 2FA は、ユーザがリソースにアクセスしようとするたびに、Android、iOS、または BlackBerry 10 デバイスで、ユーザーが入力したパスワードとセキュリティで保護されたプロンプトを使用します。<br>• BlackBerry UEM Notifications は、管理者が SMS、電話、およびメールで UEM コンソールから直接ユーザーにメッセージを送信できるようにします。このアドオンにより、追加のメッセージングソリューションが不要になるので、エンドユーザーとユーザーグループへの通信が簡素化されます。 |

| サービスの種類 | サービス名と説明 |
| --- | --- |
| BlackBerry Dynamics プラットフォーム | • BlackBerry Enterprise Mobility Server（BEMS）は、BlackBerry Dynamics アプリに追加サービスを提供します。BEMS は、BlackBerry メール、BlackBerry Connect、BlackBerry Presence、BlackBerry Docs などのサービスを統合します。これらのサービスが統合されていれば、ユーザーはセキュリティで保護されたインスタントメッセージを使用して相互に通信し、BlackBerry Dynamics アプリでユーザーのリアルタイムのプレゼンスを表示し、仕事用ファイルサーバーや Microsoft SharePoint ドキュメントにアクセスしてこれらを同期および共有できます。<br>• BlackBerry Dynamics SDK を使用すると、開発者は Android および iOS デバイスと Mac OS および Windows コンピューター用のセキュリティ保護されたアプリを作成できます。これは BlackBerry Dynamics プラットフォームのクライアント側です。 |
| BlackBerry Dynamics 生産性向上アプリ | • BlackBerry Work は、メール、カレンダー、連絡先（Microsoft Exchange と完全に同期）など、ユーザーが安全に自身の仕事をモバイル化するために必要なすべてを提供します。このアプリはまた、高度なドキュメントコラボレーションも提供します。BlackBerry Work は、仕事用データと個人用データを分離し、デバイス上で MDM プロファイルを使用せずに他の仕事用アプリとシームレスに統合します。<br>• BlackBerry Access を使用すると、ユーザーは選択したモバイルデバイスで組織のイントラネットに安全にアクセスできるようになります。<br>• BlackBerry Connect は、ユーザーのデバイス上で使いやすいインターフェイスを提供し、セキュリティ保護されたインスタントメッセージングを使用した通信とコラボレーション、企業ディレクトリの検索、およびユーザープレゼンスをすべて強化します。<br>• BlackBerry Tasks を使用すると、ユーザーは Microsoft Exchange と同期されるメモを Android および iOS デバイスで作成、編集、および管理できます。<br>• BlackBerry Notes を使用すると、ユーザーは Microsoft Exchange と同期されるメモを選択したモバイルデバイスで作成、編集、および管理できます。 |

さまざまな BlackBerry Enterprise Mobility Suite ライセンスおよびライセンスの取得方法の詳細については、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。<br>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。<br>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。<br>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。<br>BlackBerry UEM Core または BlackBerry Connectivity Node の追加のインスタンスの名前が、この証明書のサブジェクトの別名に追加されていることを確認します。 |

| 証明書 | 説明 |
| --- | --- |
| 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。<br>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。<br>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。<br>BlackBerry UEM Core または BlackBerry Connectivity Node の追加のインスタンスの名前が、この証明書のサブジェクトの別名に追加されていることを確認します。 |
| 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。<br>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。<br>BlackBerry UEM Core または BlackBerry Connectivity Node の追加のインスタンスの名前が、この証明書のサブジェクトの別名に追加されていることを確認します。 |

# 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

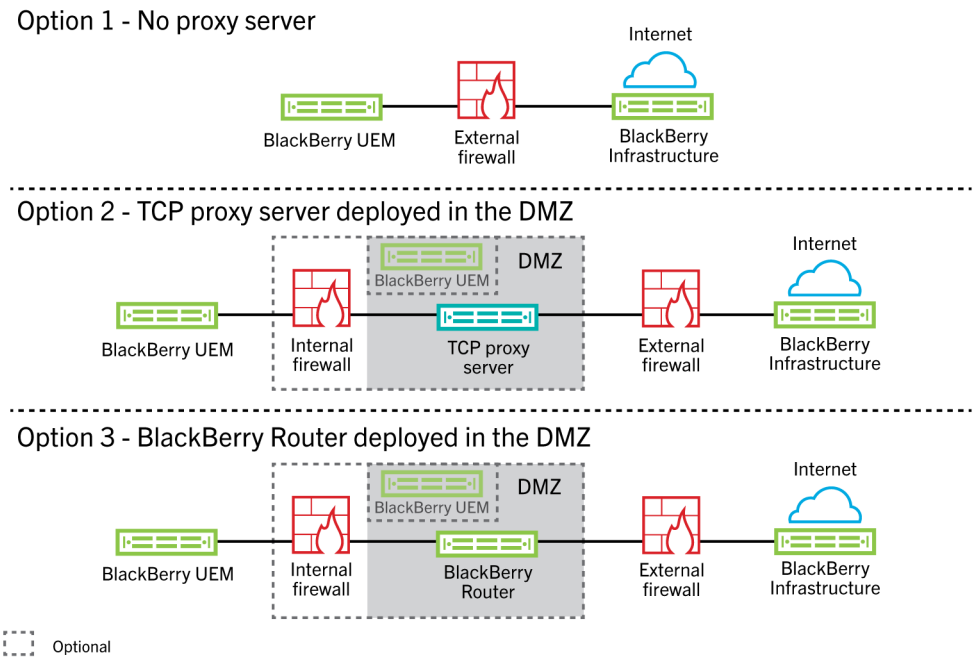
BlackBerry Infrastructure に到達する前に、TCP プロキシサーバーまたは BlackBerry Router のインスタンスを介してデータを送信するように BlackBerry UEM を設定することができます。

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。

BlackBerry OS（バージョン 5.0～7.1）デバイスの場合、BlackBerry Router は、仕事用 Wi-Fi ネットワークまたは BlackBerry Device Manager を備えたコンピューターに接続されたデバイスとの間でデータを直接送信したり、受信したりします。

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。<br>• クライアントブラウザーの設定が必要ありません。<br>• 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。<br>• 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。<br>• 許容可能な使用ポリシーの強制によく使用されます。<br>• 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。<br>• 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。<br>• 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。<br>• 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。<br>• 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。<br>• 任意の IP アドレスへのプロキシ TCP 接続です。<br>• 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、http://support.blackberry.com/kb にアクセスして、記事「KB36385」を参照してください。

### BlackBerry Router 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： 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。

# HTTP プロキシを介してデータを BlackBerry Dynamics NOC に送信する

BlackBerry UEM と BlackBerry Dynamics NOC の間で HTTP プロキシを使用してデータを送信するように BlackBerry UEM を設定できます。

メモ： プロキシは BlackBerry Dynamics NOC へのポート 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。

### HTTP プロキシ設定の設定

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. ［**HTTP** プロキシを有効にする］を選択します。
3. 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
4. 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。
5. ［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。
6. ［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。
7. プロキシサーバー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 BlackBerry UEM が認証に使用するドメインを指定します。

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。<br>環境にリソースフォレストが含まれている場合、「リソースフォレストを含む環境での 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。 |

# リソースフォレストを含む環境での Microsoft Active Directory 認証の設定

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。

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 BlackBerry UEM をインストールする必要があります。リソースフォレストでは、ユーザーアカウントごとにメールボックスを作成し、メール

ボックスをユーザーアカウントと関連付けます。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 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。

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 アカウントの名前を入力します。
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。

    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. 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場合、［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、「BlackBerry UEM のシングルサインオンの設定」を参照してください。
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。

関連タスク

Microsoft Active Directory アカウントがシングルサインオンをサポートするための制約付き委任の設定

関連資料

ブラウザー要件：シングルサインオン

# 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を確認します。
- 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. ［デバイスの所有］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、管理関連の資料の「ディレクトリにリンクされたグループの作成」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、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

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. ［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、ユーザーアカウントが 2 つの連続した同期サイクルにオンボーディングディレクトリグループに存在しない場合を除き、ユーザーが BlackBerry UEM から削除されないことを意味します。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。

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、＋アイコンをクリックします。
4. ［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。<br>b. 同期の時間フレームを指定します。<br>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。<br>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。<br>b. 同期を開始する日を選択します。 |

5. ［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。

# BlackBerry UEM のシングルサインオンの設定

BlackBerry UEM を Microsoft Active Directory に接続する場合は、シングルサインオン認証を設定すると、管理者またはユーザーがログイン Web ページをバイパスし、管理コンソールまたは BlackBerry UEM Self-Service に直接アクセスできるようになります。管理者またはユーザーが Windows にログインした場合、ブラウザーは資格情報を使用して、BlackBerry UEM で自動的に認証を行います。Windows のログイン情報は、Microsoft Active Directory の資格情報または派生した資格情報を含めることができます（たとえば、CAC リーダーやデジタルトークンから）。

Microsoft Active Directory 接続用に BlackBerry UEM へのシングルサインオンを有効にする前に、ディレクトリ接続に BlackBerry UEM が使用する Microsoft Active Directory アカウント用に、制約付き委任を設定する必要があります。

メモ：シングルサインオンを有効にする場合、Microsoft Active Directory アカウントに行うすべての変更に対して、BlackBerry UEM インスタンスをホストするそれぞれのコンピューターで BlackBerry UEM サービスを再起動する必要があります。管理者およびユーザーはコンピューターからログアウトし、再度ログインして、BlackBerry UEM のシングルサインオンを使用する必要があります。

BlackBerry UEM のシングルサインオンを設定するには、次の操作を実行します。

| 手順 | アクション |
| --- | --- |
| 1 | Microsoft Active Directory アカウントがシングルサインオンをサポートするための制約付き委任の設定。 |
| 2 | Microsoft Active Directory 接続用シングルサインオンを有効にします。 |
| 3 | シングルサインオンのブラウザー要件を確認します。 |

# Microsoft Active Directory アカウントがシングルサインオンをサポートするための制約付き委任の設定

BlackBerry UEM 用にシングルサインオンをサポートするには、ディレクトリ接続に Microsoft Active Directory が使用する BlackBerry UEM アカウント用に、制約付き委任を設定する必要があります。制約付き委任を設定すると、管理者またはユーザーが管理コンソールまたは BlackBerry UEM にアクセスする場合に、ブラウザーが BlackBerry UEM Self-Service での認証を代理で行うことができます。

1. Windows Server の ADSI Edit ツールまたは setspn コマンドラインツールを使用して、BlackBerry UEM の次の SPN を Microsoft Active Directory アカウントに追加します。
   - HTTP/*<host_FQDN_or_pool_name>*（HTTP/domain123.example.com など）
   - BASPLUGIN111/*<host_FQDN_or_pool_name>*（BASPLUGIN111/domain123.example.com など）

   BlackBerry UEM ドメインで管理コンソールに高可用性を設定した場合は、プール名を指定します。または、管理コンソールをホストするコンピューターの FQDN を指定します。

メモ：Microsoft Active Directory フォレスト内の他のアカウントが同じ SPN を持っていないことを確認します。

2. Microsoft Active Directory Users and Computers を開きます。
3. Microsoft Active Directory アカウントプロパティの［委任］タブで、次のオプションを選択します。
   - 指定されたサービスへの委任でのみこのユーザーを信頼する
   - Kerberos のみを使う
4. 手順 1 の SPN をサービスリストに追加します。

関連概念

管理コンソールの高可用性の設定

# BlackBerry UEM のシングルサインオンの設定

BlackBerry UEM にログインする管理者およびユーザーのシングルサインオンを設定する場合、管理コンソールと BlackBerry UEM Self-Service 用に設定します。

作業を始める前に：

- Microsoft Active Directory がディレクトリ接続に使用する BlackBerry UEM アカウントの制約付き委任を設定します。
- 複数の Microsoft Active Directory 接続用にシングルサインオンを有効にする場合は、Microsoft Active Directory フォレスト間に信頼関係がないことを確認します。

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. ［設定されたディレクトリ接続］セクションで、Microsoft Active Directory 接続の名前をクリックします。
3. ［認証］タブで、［**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。
4. ［保存］をクリックします。
5. ［保存］をクリックします。
   BlackBerry UEM によって、Microsoft Active Directory 認証情報が検証されます。情報が有効でない場合、BlackBerry UEM は正しい情報を入力するよう要求します。
6. ［閉じる］をクリックします。

終了したら：

- 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。
- 管理者および BlackBerry UEM Self-Service ユーザーに、BlackBerry UEM のシングルサインオンをサポートするようにブラウザーを設定するよう指示します。

関連タスク

Microsoft Active Directory アカウントがシングルサインオンをサポートするための制約付き委任の設定

## シングルサインオン用コンソール **URL**

BlackBerry UEM 用シングルサインオンを設定する場合、次の URL を使って、管理者は管理コンソールに、ユーザーは BlackBerry UEM Self-Service にアクセスするよう指示する必要があります。

| コンソール | シングルサインオン認証用 **URL** |
| --- | --- |
| BlackBerry UEM 管理コンソール | https://<*host_FQDN_or_pool_name*>:<*port*>/admin |
| BlackBerry UEM Self-Service | https://<*host_FQDN_or_pool_name*>:<*port*>/mydevice |

シングルサインオン認証は、管理者による管理コンソールへのログインと、ユーザーによる BlackBerry UEM Self-Service へのログインを許可するその他の認証方法より優先されます。組織のセキュリティ基準により、管理者またはユーザーがその他の認証方法を使用することが必要とされる場合は、次の URL を使用して管理コンソールまたは BlackBerry UEM Self-Service にアクセスするよう指示する必要があります。

| コンソール | その他の認証方法用 **URL** |
| --- | --- |
| BlackBerry UEM 管理コンソール | https://<*host_FQDN_or_pool_name*>:<*port*>/admin?sso=n |
| BlackBerry UEM Self-Service | https://<*host_FQDN_or_pool_name*>:<*port*>/mydevice?sso=n |

メモ：BlackBerry UEM をインストールする場合、デフォルトでは、セットアップアプリケーションは、ポート 8000 を BlackBerry UEM Self-Service に割り当て、ポート 443 を管理コンソールに割り当てようとします。ポート 443 が利用できない場合は、セットアップアプリケーションはポート 8008 を使用しようとします。デフォルトのポートが使用できない場合、セットアップアプリケーションはポート値を 12000～12999 の範囲で割り当てます。BlackBerry UEM Self-Service および管理コンソールに割り当てられているポートを確認するには、インストールおよびアップグレード関連の資料の「BlackBerry UEM セットアップアプリケーションによって割り当てられているポート値の確認」を参照してください。

## ブラウザー要件：シングルサインオン

BlackBerry UEM のシングルサインオンを設定する場合は、管理者および BlackBerry UEM Self-Service ユーザーが使用するブラウザーに次の要件が適用されます。

| 項目 | 要件 |
| --- | --- |
| ブラウザー | 次のいずれか：<br>• Internet Explorer<br>• Microsoft Edge<br>• Mozilla Firefox<br>• Google Chrome<br>サポートされるバージョンの詳細については、「互換性一覧表」を参照してください。 |

| 項目 | 要件 |
| --- | --- |
| ブラウザー設定 | 次の設定の Internet Explorer ：<br>• 管理コンソールおよび BlackBerry UEM Self-Service の URL は、ローカルイントラネットゾーンに割り当てられる（［インターネットオプション］ > ［セキュリティ］）。<br>• ［統合 Windows 認証を使用する］が選択されていること（［インターネットオプション］ > ［詳細設定］）。<br>次の設定の Firefox ：<br>• about:config リストで、https://, *<host_FQDN_or_pool_name>* が「network.negotiate-auth.trusted-uris」設定に追加されている。詳細については、kb.mozillazine.org/about:config にアクセスしてください。<br>Google Chrome は、Internet Explorer からローカルイントラネットゾーンを使用します。管理コンソールおよび BlackBerry UEM Self-Service の URL は、ローカルイントラネットゾーンに割り当てられる必要があります（［インターネットオプション］ > ［セキュリティ］）。 |

# 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。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。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

APNs 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. ［**APNs** 証明書を取得］をクリックします。
   現在の APNs 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. ［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。

終了したら： Apple 発行の APNs 証明書を要求する方法。

# Apple 発行の APNs 証明書を要求する方法

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。

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 証明書を要求する方法。

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 証明書のステータスと有効期限を表示するには、［設定］ > ［外部統合］ > ［**iOS** 管理］をクリックします。APNs 証明書を更新する方法の詳細については、『APNs 証明書を更新する』を参照してください。

# 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。

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. ［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. 元の APNs 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。
4. 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。
5. 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。
6. ［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。
7. ［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 証明書のステータスと有効期限を表示するには、［設定］ **>** ［外部統合］ **>** ［**iOS** 管理］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

http://support.blackberry.com/kb にアクセスし、記事 KB37266 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。

# Exchange ActiveSync にアクセス可能なデバイスの制御

デバイスが明示的に許可リストに追加される場合を除き、未許可のデバイスによる Exchange ActiveSync の使用をブロックできます。許可リストにないデバイスは、仕事用メールやオーガナイザーデータにアクセスできません。BlackBerry Gatekeeping Service を使用すると、デバイスを許可リストに簡単に追加できます。

BlackBerry Gatekeeping Service を使用するには、Microsoft Exchange Server または Microsoft Office 365 のゲートキーピング設定を作成し、ゲートキーピングプロファイルと、自動ゲートキーピングサーバーが選択されたメールプロファイル（またはアプリ設定を持つメールアプリ）をユーザーに割り当てる必要があります。

ゲートキーピングを設定し、ゲートキーピングプロファイルとメールプロファイル（またはアプリ設定を持つメールアプリ）をユーザーに割り当てた後、ユーザーのデバイスが許可リストに自動的に追加されます。ゲートキーピングプロファイル、メールプロファイル、またはメールアプリがユーザーから削除される場合、ユーザーのデバイスは許可リストから削除され、他の手段（Windows PowerShell など）を使用して許可されないかぎり、Microsoft Exchange に接続できなくなります。

BlackBerry Connectivity Node の 1 つ以上のインスタンスをインストールして、デバイス接続コンポーネントの追加インスタンスを組織のドメインに追加できます。各 BlackBerry Connectivity Node には、BlackBerry Gatekeeping Service のインスタンスが含まれています。各インスタンスは、組織のゲートキーピングサーバーにアクセスできる必要があります。プライマリ BlackBerry UEM コンポーネントとともにインストールされる BlackBerry Gatekeeping Service によってのみ、ゲートキーピングデータを管理する場合、それぞれの BlackBerry Connectivity Node で BlackBerry Gatekeeping Service を無効にするようにデフォルト設定を変更できます。BlackBerry Connectivity Node のインストールと設定の詳細については、計画関連の資料とインストールおよびアップグレード関連の資料を参照してください。

デバイス接続トラフィックを、BlackBerry Infrastructure への特定の地域接続に向けるように、サーバーグループを設定できます。ゲートキーピングプロファイルをサーバーグループに関連付けると、そのゲートキーピングプロファイルが割り当てられているすべてのユーザーは、そのサーバーグループの BlackBerry Gatekeeping Service のアクティブなインスタンスを使用します。サーバーグループを設定する場合、グループ内の BlackBerry Gatekeeping Service のインスタンスを無効にすることができます。

次の詳細については、管理関連の資料を参照してください。

- ゲートキーピングプロファイルへの自動ゲートキーピングサーバーの追加
- 許可リストに自動的に追加されないデバイスの許可またはブロック

# Exchange ActiveSync および BlackBerry Gatekeeping Service を設定する手順

BlackBerry Gatekeeping Service 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 | ゲートキーピングのための権限の設定。 |

| 手順 | アクション |
| --- | --- |
| 2 | 承認されているデバイスのみに Exchange ActiveSync へのアクセスを許可。 |
| 3 | ゲートキーピングのための Microsoft IIS 権限を設定する。 |
| 4 | ゲートキーピング設定の作成。 |
| 5 | ゲートキーピングプロファイルを作成し、それをユーザーアカウント、ユーザーグループ、またはデバイスグループに割り当てます。手順については、管理関連資料の「ゲートキーピングプロファイルの作成」を参照してください。。 |

# ゲートキーピングのための権限の設定

Exchange ActiveSync ゲートキーピングを使用するには、Microsoft Exchange Server または Microsoft Office 365 でユーザーアカウントを作成し、ゲートキーピングのために必要な権限を与える必要があります。

Microsoft Office 365 を使用している場合、Microsoft Office 365 ユーザーアカウントを作成し、メール受信者と組織のクライアントアクセスのロールを割り当てます。

Microsoft Exchange Server 2010 以降を使用している場合、次の手順に従って、Exchange ActiveSync のメールボックスとクライアントアクセスを管理するための適切な権限を持つ管理ロールを設定します。このタスクを実行するには、適切な権限を保持する Microsoft Exchange 管理者として、管理ロールの作成および変更する必要があります。

作業を始める前に：

- Microsoft Exchange をホストするコンピューターで、BlackBerry UEM のゲートキーピングを管理するためのアカウントとメールボックスを作成します（例：BUEMAdmin）。Exchange ActiveSync を作成するときに、このアカウントのログイン情報を指定する必要があります。このアカウントの名前をメモして、以下のタスクの最後に指定します。
- WinRM は、ゲートキーピングを設定する Microsoft Exchange Server をホストするコンピューターのデフォルト設定になっています。管理者としてコマンドプロンプトからコマンド「`Winrm quickconfig`」を実行する必要があります。ツールで「変更しますか`[y/n]`」と表示されたら「`y`」と入力します。コマンドが成功すると、次のメッセージが表示されます。

```
WinRM はリモート管理用に更新されました。


WinRM サービスの種類が遅延自動開始に変更されました。

WinRM サービスが開始されました。

このコンピュータ上のあらゆる IP への WS-Man 要求を受け付けるため、HTTP://* 上に WinRM リス

ナー

 を作成しました。
```

1. Microsoft Exchange Management Shell を開きます。

2. 「New-ManagementRole -Name "<*name_new_role_mail_recipients*>" -Parent "Mail Recipients"」と入力します。Enter キーを押します。
3. 「New-ManagementRole -Name "<*name_new_role_org_ca*>" -Parent "Organization Client Access"」と入力します。Enter キーを押します。
4. 「New-ManagementRole -Name "<*name_new_role_exchange_servers*>" -Parent "Exchange Servers"」と入力します。Enter キーを押します。
5. 「Get-ManagementRoleEntry "<*name_new_role_mail_recipients*>*" | Where {$_.Name -ne "Get-ADServerSettings"} | Remove-ManagementRoleEntry」と入力します。Enter キーを押します。
6. 「Get-ManagementRoleEntry "<*name_new_role_org_ca*>*" | Where {$_.Name -ne "Get-CasMailbox"} | Remove-ManagementRoleEntry」と入力します。Enter キーを押します。
7. 「Get-ManagementRoleEntry "<*name_new_role_exchange_servers*>*" | Where {$_.Name -ne "Get-ExchangeServer"} | Remove-ManagementRoleEntry」と入力します。Enter キーを押します。
8. 「Add-ManagementRoleEntry "<*name_new_role_mail_recipients*>\Get-ActiveSyncDeviceStatistics" -Parameters Mailbox」と入力します。Enter キーを押します。
9. 「Add-ManagementRoleEntry "<*name_new_role_mail_recipients*>\Get-ActiveSyncDevice" -Parameters Identity」と入力します。Enter キーを押します。
10. Microsoft Exchange 2013 を使用している場合のみ、この手順を実行します。「Add-ManagementRoleEntry “<*name_new_role_mail_recipients*>\Get-MobileDeviceStatistics” –Parameters Mailbox」と入力します。Enter キーを押します。
11. Microsoft Exchange 2013 を使用している場合のみ、この手順を実行します。「Add-ManagementRoleEntry “<*name_new_role_mail_recipients*>\Get-MobileDevice” –Parameters Mailbox」と入力します。Enter キーを押します。
12. 「Add-ManagementRoleEntry "<*name_new_role_org_ca*>\Set-CasMailbox" -Parameters Identity, ActiveSyncBlockedDeviceIDs, ActiveSyncAllowedDeviceIDs」と入力します。Enter キーを押します。
13. 「New-RoleGroup "<*name_new_group*>" -Roles "<*name_new_role_mail_recipients*>", "<*name_new_role_org_ca*>", "<*name_new_role_exchange_servers*>"」と入力します。Enter キーを押します。
14. 「Add-RoleGroupMember -Identity "<*name_new_group*>" -Member "BUEMAdmin"」と入力します。Enter キーを押します。
15. 「Add-ManagementRoleEntry "<*name_new_role_mail_recipients*>\Set-AdServerSettings"」と入力します。 Enter キーを押します。
16. 「Add-ManagementRoleEntry "<*name_new_role_mail_recipients*>\Remove-ActiveSyncDevice" -Parameters Identity,Confirm」と入力します。Enter キーを押します。
17. Microsoft Exchange 2013 を使用している場合のみ、この手順を実行します。種類 「Add-ManagementRoleEntry 「<*name_new_role_mail_recipients*>\Remove-MobileDevice" -Parameters Identity,Confirm」と入力します。Enter キーを押します。

終了したら： 承認されているデバイスのみに Exchange ActiveSync へのアクセスを許可。

# 承認されているデバイスのみに Exchange ActiveSync へのアクセスを許可

所属組織が Microsoft Exchange Server 2010 以降を使用している場合は、「Microsoft Exchange を設定して承認されているデバイスのみに Exchange ActiveSync へのアクセスを許可」を参照してください。

所属組織が Microsoft Office 365 を使用している場合は、「Microsoft Office 365 でのモバイルデバイスアクセスポリシーの設定」を参照してください。

## Microsoft Exchange を設定して承認されているデバイスのみに Exchange ActiveSync へのアクセスを許可

承認されているデバイスのみに Microsoft Exchange Server へのアクセスを許可するには、Exchange ActiveSync 2010 以降を設定する必要があります。Microsoft Exchange で許可リストに明示的に追加されていない既存ユーザーのデバイスは、BlackBerry UEM による許可が得られるまで検疫されます。

このタスクを実行するには、適切な権限を保持する Microsoft Exchange 管理者として、Set-ActiveSyncOrganizationSettings を設定する必要があります。承認されているデバイスのみに Exchange ActiveSync へのアクセスを許可する方法の詳細については、https://technet.microsoft.com にアクセスし、「*Exchange ActiveSync* のデバイスを有効にする」を参照してください。

作業を始める前に：

- ゲートキーピングのための権限の設定。
- 現在 Microsoft Exchange を使用しているユーザーがいるかどうかを Exchange ActiveSync 管理者に確認してください。

組織の Exchange ActiveSync のデフォルトアクセスレベルが［許可］に設定されており、ユーザーがデバイスを正常にセットアップおよび同期している場合には、デフォルトアクセスレベルを［検疫］に設定する前に、これらのユーザーが個人的例外またはユーザーアカウントに関連付けられているデバイスルールを持っていることを確認します。持っていない場合、これらのユーザーは検疫され、BlackBerry UEM により許可されるまでデバイスは同期されません。

Exchange ActiveSync のデフォルトアクセスレベルを設定して検疫する方法の詳細については、http://support.blackberry.com/kb にアクセスし、記事「KB33531」を参照してください。

1. Microsoft Exchange Management Shell をホストするコンピューターで、Microsoft Exchange Management Shell を開きます。
2. 「`Set-ActiveSyncOrganizationSettings -DefaultAccessLevel Quarantine`」と入力します。Enter キーを押します。

終了したら： ゲートキーピングのための Microsoft IIS 権限を設定する。

## Microsoft Office 365 でのモバイルデバイスアクセスポリシーの設定

BlackBerry Gatekeeping Service で Microsoft Office 365 を使用するには、Microsoft Office 365 でモバイルデバイスポリシーを設定して、デフォルトでデバイスを検疫する必要があります。

作業を始める前に： ゲートキーピングのための権限の設定。

組織の Exchange ActiveSync のデフォルトアクセスレベルが［許可］に設定されており、ユーザーがデバイスを正常にセットアップおよび同期している場合には、デフォルトアクセスレベルを［検疫］に設定する前に、これらのユーザーが個人的例外またはユーザーアカウントに関連付けられているデバイスルールを持っていることを

確認します。持っていない場合、これらのユーザーは検疫され、BlackBerry UEM により許可されるまでデバイスは同期されません。

Exchange ActiveSync のデフォルトアクセスレベルを設定して検疫する方法の詳細については、http://support.blackberry.com/kb にアクセスし、記事「KB33531」を参照してください。

1. Microsoft Office 365 管理ポータルにログインします。
2. サイドメニューで、［管理者］をクリックします。
3. ［**Exchange**］をクリックします。
4. ［モバイル］セクションで、［モバイルデバイスアクセス］をクリックします。
5. ［編集］をクリックします。
6. ［検疫 - ブロックまたは許可の判断を後で行う］をクリックします。

終了したら： ゲートキーピングのための Microsoft IIS 権限を設定する。

# ゲートキーピングのための Microsoft IIS 権限を設定する

BlackBerry UEM は Windows PowerShell コマンドを使用して、許可されたデバイスのリストを管理します。BlackBerry Gatekeeping Service を使用するには、Microsoft IIS 権限を設定する必要があります。Microsoft クライアントアクセスサーバーロールをホストするコンピューターで、次の操作を実行します。

作業を始める前に： 承認されているデバイスのみに Exchange ActiveSync へのアクセスを許可。

1. Microsoft Internet Information Services （IIS）マネージャーを開きます。
2. 左ペインで、サーバーを展開します。
3. ［サイト］ > ［デフォルトの **Web** サイト］を展開します。
4. ［PowerShell］フォルダーを右クリックします。［権限を編集］をクリックします。
5. ［セキュリティ］タブをクリックします。［編集］をクリックします。
6. ［追加］をクリックし、ゲートキーピングのための Microsoft Exchange 権限を設定したときに作成された <new_group> を入力します。
7. ［**OK**］をクリックします。
8. ［読み込んで実行］、［フォルダーの内容を一覧表示］、および［読み込み］が選択されていることを確認します。［**OK**］をクリックします。
9. ［**PowerShell**］フォルダーを選択します。認証アイコンをダブルクリックします。
10. ［**Windows** 認証］を選択します。［有効］をクリックします。
11. Microsoft Internet Information Services （IIS）マネージャーを閉じます。

終了したら： ゲートキーピング設定の作成。

# ゲートキーピング設定の作成

ゲートキーピング設定を作成し、組織のセキュリティポリシーに準拠するデバイスが Microsoft Exchange Server または Microsoft Office 365 に接続できるようにできます。

作業を始める前に：

- ゲートキーピングのための権限の設定。

- 承認されているデバイスのみに Exchange ActiveSync へのアクセスを許可。
- ゲートキーピングのための Microsoft IIS 権限を設定する。

1. メニューバーで、［設定］ > ［外部統合］ > ［**Microsoft Exchange** ゲートキーピング］をクリックします。
2. Microsoft Exchange Server リストセクションで、＋をクリックします。
3. ［サーバー名］フィールドに、アクセスを管理する Microsoft Exchange Server または Microsoft Office 365 環境の名前を入力します。
4. Exchange ActiveSync ゲートキーピングを管理するために作成したアカウントのユーザー名とパスワードを入力します。
5. ［認証の種類］ドロップダウンリストで、Microsoft Exchange Server または Microsoft Office 365 で使用する認証の種類を選択します。
6. BlackBerry UEM と Microsoft Exchange Server または Microsoft Office 365 の間で SSL 認証を有効にするには、［**SSL**を使用］チェックボックスをオンにします。オプションで、追加の証明書確認を選択します。
7. ［プロキシのタイプ］ドロップダウンリストで、BlackBerry UEM と Microsoft Exchange Server または Microsoft Office 365 の間で使用するプロキシ設定の種類を選択します（存在する場合）。
8. 以前の手順でプロキシ設定を選択した場合は、プロキシサーバーで使用される認証の種類を選択します。
9. 必要に応じて［認証が必須］を選択し、ユーザー名とパスワードを入力します。
10. ［テスト接続］をクリックし、接続が成功していることを確認します。
11. ［保存］をクリックします。
12. ［**Android for Work** メールクライアントリスト］セクションで、＋をクリックします。

メモ： BlackBerry Hub + サービスはデフォルトでリストに追加されます。

13. メールアプリを選択し、［次へ］をクリックします。
14. ［デバイス **ID**］ドロップダウンリストで、デバイス ID にマップするアプリ設定からのフィールドを選択します。
15. ［メールアドレス］ドロップダウンリストで、ユーザーのメールアドレスにマップするアプリ設定からのフィールドを選択します。

終了したら：

- ゲートキーピングプロファイルを作成し、それをユーザーアカウント、ユーザーグループ、またはデバイスグループに割り当てます。管理関連資料の「ゲートキーピングプロファイルの作成」を参照してください。。
- 1 つまたは複数の BlackBerry Gatekeeping Service のアクティブなインスタンスを持つサーバーグループを設定した場合は、ゲートキーピングプロファイルを適切なサーバーグループに関連付けます。そのゲートキーピングプロファイルを割り当てられているすべてのユーザーは、そのサーバーグループの BlackBerry Gatekeeping Service の任意のアクティブなインスタンスを使用できます。

# 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。

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

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** トークンのエンドポイント値をコピーし、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、［新しいアプリケーションの登録］を選択します。
6. アプリの次の情報を入力します。

| フィールド | 設定 |
| --- | --- |
| 名前 | <アプリケーションの名前> |
| アプリケーションのタイプ | Web app/API |
| サインオン URL | 有効な URL<br>メモ： 登録されたドメインがない場合は、http://localhost/ を使用できます。 |

7. ［作成］をクリックします。
8. 作成したアプリをクリックします。
9. 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。

10. Microsoft Intune を使用するアプリケーションを作成する場合、［設定］メニューの［必要な権限］をクリックします。次のタスクを実行します。
    a) ［追加］をクリックします。
    b) ［**API** を選択する］をクリックします。
    c) ［**Microsoft Graph**］を選択します。
    d) ［選択］をクリックします。
    e) 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 アプリの読み込みと書き込み（プレビュー）
       - すべてのユーザーの基本プロファイルの読み込み
       - すべてのグループの読み込み
    f) ［選択］をクリックします。
    g) ［完了］をクリックします。
    h) ［必要な権限］ペインで［アクセス許可の付与］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。
    i) 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。
11. ［設定］メニューの［キー］を選択します。次のタスクを実行します。
    a) キーの名前を入力します。
    b) キーの期間を選択します。
    c) ［保存］をクリックします。
    d) キー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 を設定して Microsoft Intune と同期する または BlackBerry UEM を設定して Windows Store for Business と同期します。。

# BlackBerry UEM を設定して Microsoft Intune と同期する

Microsoft Intune は、MDM と MAM の両方の機能を備えたクラウドベースの EMM サービスです。Intune MAM は、アプリ（Office 365 アプリなど）にセキュリティ機能を提供しており、アプリ内でデータを保護します。例えば、Intune では、アプリ内でのデータ暗号化を要求したり、コピー、貼り付け、印刷、［名前を付けて保存］コマンドの使用を禁止したりできます。

BlackBerry UEM を Microsoft Intune に接続した後で、UEM 管理コンソールを使用し、管理関連の資料の説明に従って Microsoft Intune アプリ保護プロファイルを作成することができます。

Microsoft Intune と同期するように BlackBerry UEM を設定する前に、BlackBerry UEM を Microsoft Azure に接続する必要があります。

### BlackBerry UEM を設定して Microsoft Intune と同期する

作業を始める前に： Azure でのエンタープライズエンドポイントの作成

1. BlackBerry UEM 管理コンソールにログインします。
2. ［設定］ > ［外部統合］ > ［**Microsoft Intune**］に移動します。
3. Azure でエンタープライズアプリケーションを作成したときに Azure ポータルからコピーした情報を入力します。
   - クライアント **ID**：Azure アプリケーションの登録によって生成されたアプリケーション ID
   - クライアント キー：Azure アプリケーションの登録によって生成されたクライアントシークレット
   - **OAUTH 2.0** トークンエンドポイント：認証トークンを要求するためのテナント固有の OAuth エンドポイントの URL
   - ユーザー名：Intune にアクセスするために BlackBerry UEM が使用する管理者アカウント。Intune 管理者アカウントに必要な権限の詳細については、https://support.blackberry.com/kb にアクセスして記事 50341 をご覧ください。
   - パスワード：Intune 管理者アカウントのパスワード
4. ［次へ］をクリックします。

終了したら： Microsoft Intune アプリ保護プロファイルの作成

# BlackBerry UEM を設定して Windows Store for Business と同期する

Windows 10 アプリを管理する場合は、Windows 10 アプリをアプリリストに追加する前に、BlackBerry UEM を Windows Store for Business と同期するように設定する必要があります。

後で Windows Store for Business の接続を削除する場合、BlackBerry UEM と同期されているすべての Windows 10 アプリが削除され、アプリはユーザーとグループから割り当て解除されます。

BlackBerry UEM を設定して Windows Store for Business と同期するには、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 Windows Store for Business と同期します。。 |
| 5 | Windows Store for Business の管理者の作成。 |

## BlackBerry UEM を設定して Windows Store for Business と同期します。

作業を始める前に： Microsoft Azure アカウントの作成。

1. BlackBerry UEM 管理コンソールにログインします。
2. ［設定］ > ［アプリ管理］ > ［**Windows 10** アプリ］に移動します。
3. Azure でエンタープライズアプリケーションを作成したときに Azure ポータルからコピーした情報を入力します。
   - クライアント **ID**：Azure アプリケーションの登録によって生成されたアプリケーション ID
   - クライアント キー：Azure アプリケーションの登録によって生成されたクライアントシークレット
   - **OAUTH 2.0** トークンエンドポイント：認証トークンを要求するためのテナント固有の OAuth エンドポイントの URL
   - ユーザー名：Intune にアクセスするための BlackBerry UEM の管理者のユーザー名。
   - パスワード：ユーザー名のパスワード
4. ［次へ］をクリックします。

終了したら： Windows Store for Business の管理者の作成。

## Windows Store for Business の管理者の作成

デバイス上の Windows 10 アプリを管理するには、Windows Store for Business でアプリカタログを作成し、アプリを BlackBerry UEM と同期する必要があります。Windows Store for Business でカタログを作成するには、ストアにログインするために 1 つ以上の管理者アカウントを作成する必要があります。

作業を始める前に：

- Microsoft Azure アカウントの作成。
- Azure でのエンタープライズエンドポイントの作成。
- BlackBerry UEM を設定して Windows Store for Business と同期します。。

1. Microsoft Azure ポータルで、［**Microsoft Azure**］ > ［**Azure Active Directory**］ > ［ユーザーとグループ ］ > ［すべてのユーザー］に移動します。
2. ［ユーザーを追加］をクリックします。
3. 画面で、必要なユーザー情報を入力します。
4. ［ディレクトリの役割］の横の矢印をクリックし、［グローバル管理］を選択して、［**OK**］をクリックします。
5. パスワードを作成するか、［パスワードの表示］を選択し、生成されたパスワードをコピーします。
6. ［作成］をクリックします。
7. ［**Azure Active Directory**］ > ［エンタープライズアプリケーション］ > ［すべてのアプリケーション］をクリックし、作成したエンタープライズアプリケーションを選択します。
8. 作成したグローバル管理者アカウントを、アプリケーションのユーザーとして追加します。

## Windows Store for Business でアプリを有効にする

作業を始める前に：

- BlackBerry UEM を設定して Windows Store for Business と同期します。。
- Windows Store for Business の管理者の作成

1. 作成したグローバル管理アカウントを使用して、Windows Store for Business にログインします。

2. ［設定］ > ［管理ツール］をクリックします。
3. Windows Store for Business と同期したい MDM ツールになるように作成したアプリを選択します。
4. ［アクティブにする］をクリックします。

# 仕事用プロファイルのある Android デバイスをサポートするように BlackBerry UEM を設定する

仕事用プロファイルのある Android 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。仕事用プロファイルのある Android 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。

メモ：アプリケーションポリシーを使用し、Gmail アプリを設定することができます。ただし、デバイスをアクティブにするには、MDM アクティベーションタイプではなく、仕事用および個人用または仕事専用のアクティベーションタイプを使用する必要があります。

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 で、仕事用プロファイルアカウントのある Android デバイス（管理 Google Play アカウントと呼ばれる）を管理できます。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、仕事用プロファイルがある Android 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。

| 仕事用プロファイルのある **Android** 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。<br>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。<br>Google Play では、アプリ管理をサポートします。 |

| 仕事用プロファイルのある **Android** 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 で、仕事用プロファイルアカウントのある Android デバイス（管理 Google Play アカウントと呼ばれる）を管理できます。 | • 組織に Google ドメインがない<br>• 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、仕事用プロファイルのある Android デバイスを 2 つ目の BlackBerry UEM ドメインで使用したい。 | 仕事用プロファイルアカウントのある Android デバイス | Google Play では、アプリ管理をサポートします。<br>Google サービスはサポートされていません。 |

# 仕事用プロファイルのある **Android** デバイスをサポートするように **BlackBerry UEM** を設定する

作業を始める前に：

- BlackBerry UEM は、Android 5.1 以降を実行している仕事用プロファイルのある Android デバイスをサポートしています。
- 管理された Google Play アカウントオプションを使用する仕事用プロファイルがある Android デバイスをサポートするように BlackBerry UEM を設定した場合、「仕事用領域のみ」アクティベーションタイプのデバイスのアクティブ化は、Android 6.0 以降を実行しているデバイス上でのみサポートされます。
- 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 Android 仕事用プロファイルの接続の削除』を参照してください。

1. メニューバーで、［設定］ > ［外部統合］ > ［**Google** ドメイン接続］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 |
| --- | --- |
| Google ドメインの使用 | a. ［**BlackBerry UEM** を既存の **Google** ドメインに接続する］を選択します。<br>b. ［次へ］をクリックします。<br>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、http://support.blackberry.com/kb にアクセスして、記事 000037748 を読んでください。 |

| タスク | 手順 |
| --- | --- |
| 仕事用プロファイルアカウントのある Android デバイスの使用 | **a.** ［**BlackBerry UEM** での **Android** 仕事用アカウントの管理を許可する］を選択します。<br>**b.** ［次へ］をクリックします。<br>**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。<br>**d.** ［開始］をクリックします。<br>**e.** 組織の名前を入力します。［確認］をクリックします。<br>**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。 |

3. 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
4. ［完了］をクリックします。

終了したら： 仕事用プロファイルのある Android デバイスをアクティブ化する手順を実行します。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「デバイスの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 Android 仕事用プロファイルの接続の削除

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、Android 作業プロファイルの接続を削除します。

- BlackBerry UEM インスタンスをアンインストールする
- Android 作業プロファイルの接続を確立する前に作成した仮想マシンのスナップショットに戻す
- 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

Android 作業プロファイル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。Android 作業プロファイルの接続を BlackBerry UEM で削除した場合、Android 作業プロファイ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すべてのデバイスも無効になります。

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

仕事用プロファイルのある Android デバイスをサポートするように BlackBerry UEM を設定する場合、Google で接続を削除することができます。

1. 仕事用プロファイルのある Android 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］の順にクリックします。
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、作業プロファイルが含まれる Android 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。
   - 仕事用プロファイルを持つ Android 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。

# E-FOTA ライセンスの追加

Enterprise Firmware Over The Air（E-FOTA）を使用し、Samsung からのファームウェアの更新を Samsung KNOX デバイスにインストールするタイミングを制御することができます。ファームウェアバージョンを制御することにより、ユーザーのデバイスで使用されるファームウェアバージョンが、アプリでサポートされ、組織のポリシーを準拠しているものになります。

ファームウェアのバージョンを制御するためのデバイス SR 要件プロファイルを作成する前に、UEM で E-FOTA ライセンスを追加する必要があります。

1. メニューバーで［ライセンス］>［ライセンスの概要］をクリックします。
2. ［**E-FOTA**］セクションで［ライセンスを追加］をクリックします。
3. ［**E-FOTA** ライセンスの追加］ダイアログボックスで、名前、クライアント ID、クライアントシークレット、顧客 ID、およびライセンスキーを入力します。
4. ［保存］をクリックします。

終了したら： Android デバイス用のデバイス SR 要件プロファイルを作成します。

# Samsung KNOX デバイスの認証の管理

認証をオンにすると、BlackBerry UEM は、次のアクティベーションタイプでアクティブ化された Samsung KNOX デバイスの完全性と整合性をテストするためのチャレンジを送信します。

- 仕事用と個人用 - フルコントロール （Samsung KNOX）
- 仕事用領域のみ （Samsung KNOX）
- 仕事用と個人用 - ユーザーのプライバシー （Samsung KNOX）

1. メニューバーで［設定］ > ［一般設定］ > ［認証］をクリックします。
2. Samsung KNOX デバイスの認証をオンにするには、［**KNOX Workspace** デバイスの定期的な認証チャレンジを有効にする］を選択します。
3. ［チャレンジの頻度］セクションで、デバイスが認証応答を BlackBerry UEM に返す必要がある頻度を日数または時間数で指定します。
4. ［猶予期間］セクションで、猶予期間を時間数または日数で指定します。認証応答が得られずに猶予期間が終了すると、デバイスが準拠していないと見なされ、そのデバイスは、ユーザーに割り当てられているコンプライアンスプロファイルに指定された条件を適用されます。また、ユーザーのデバイスが通信範囲外にある場合、電源がオフになっている場合、またはバッテリーが切れている場合、BlackBerry UEM が送信する認証チャレンジに応答できず、BlackBerry UEM が非準拠であると判断されることも考慮してください。コンプライアンス違反時にデバイスを削除するように組織のコンプライアンスポリシーが設定されている場合、猶予期間が満了する前にデバイスが応答しないと、デバイス上のデータは削除されます。
5. ［保存］をクリックします。

終了したら： デバイスがルートと見なされるときに実行される操作を指定するコンプライアンスプロファイルを作成します。手順については、BlackBerry UEM 管理関連資料の「デバイスのコンプライアンスルールの強制」を参照してください。

# SafetyNet を使用した Android デバイスおよび BlackBerry Dynamics アプリの認証の管理

Android SafetyNet 認証を使用する場合、BlackBerry UEM は、組織の環境内の Android デバイスと BlackBerry Dynamics アプリの完全性と整合性をテストするためのチャレンジを送信します。SafetyNet は、組織のアプリを実行する環境のセキュリティと互換性を評価するのに役立ちます。BlackBerry の既存のルートおよび悪用検出に加えて、SafetyNet 認証を使用できます。SafetyNet の詳細については、Google の情報を参照してください。

次の製品は、SafetyNet 認証をサポートしています。

- BlackBerry UEM
- Android 用 BlackBerry UEM Client
- Android 用 BlackBerry Dynamics アプリ

## SafetyNet 認証の設定に関する考慮事項

- Google SafetyNet 認証失敗オプションは、Android デバイスおよび BlackBerry Dynamics アプリ用のコンプライアンスプロファイル設定であり、デバイスまたはアプリが SafetyNet 認証に不合格になった場合に発生するアクションを指定できます。このオプションを設定するには、［ポリシーとプロファイル］ > ［コンプライアンス］ > ［**Android**］タブに移動します。
- ［Google SafetyNet 認証失敗］コンプライアンスルールを有効にしていない場合、既にアクティブ化されているアプリにはコンプライアンスアクションが強制されません。
- SafetyNet を有効にすると、アクティベーション中の認証が実行されます。ポリシーを使用してアクティベーション中の認証を強制することはできません。
- BlackBerry UEM Client は、SafetyNet 認証を有効にするのに必須ではありません。
- BlackBerry UEM Client は、SafetyNet 認証用に設定できる BlackBerry Dynamics アプリのリストには表示されません。BlackBerry UEM は、認証チャレンジを BlackBerry UEM Client に送信し、そこから応答を受信します。
- BlackBerry UEM は、認証チャレンジを、設定者が設定したそれぞれの BlackBerry Dynamics アプリに送信します。
- BlackBerry UEM は、古いバージョンのアプリを信頼しません。たとえば、BlackBerry Work に対して認証チャレンジを有効にする場合は、組織のデバイス上の BlackBerry Work のバージョンが最新バージョンであることを確認する必要があります。最新バージョンでない場合、新しいアクティベーションは失敗します。既存のアクティブ化されたユーザーが古いバージョンのアプリを使用していても、組織のコンプライアンスプロファイルで［Google SafetyNet 認証失敗］オプションを有効にするまで、アプリまたはデバイスに対して障害となるアクションは実行されません。
- BlackBerry UEM では、アクティベーション認証および定期的な認証に加えて、新しい REST API を使用しており、これによって設定者はカスタムサーバーワークフローを作成できます。たとえば、アプリが特定のセキュリティ保護されたリモートアイテムにアクセスする必要がある場合、アクセスを許可する前に、アプリサーバーが BlackBerry UEM と通信してアプリまたはデバイス上で SafetyNet 認証を強制します。
- ユーザーのデバイスは、通信可能範囲にないか、電源オフにされているか、バッテリー切れである場合、BlackBerry UEM から送信された認証チャレンジに応答できないため、BlackBerry UEM は、そのデバイスを非準拠であると見なします。準拠から外れているデバイスを消去するように組織のコンプライアンスポリシーが設定されている場合、猶予期間が終了する前にそのデバイスが応答しなければ、そのデバイスがワイヤレスネットワークに接続したときにそのデバイス上のデータが削除されます。

- ［アプリの猶予期間］フィールドに時間を設定した場合、設定したその時間枠内に応答しないアプリに対してのみアクションが実行されます。たとえば、［アプリの猶予期間］の値を 7 日間に設定し、ユーザーが BlackBerry Work を毎日使用しているが、BlackBerry Tasks を 7 日以内に使用しなかった場合、BlackBerry Tasks に対してのみアクションが実行されます。
- 新しいアプリを BlackBerry UEM に追加し、そのアプリがアクティベーション中の認証に失敗した場合、組織のコンプライアンスプロファイルの［Google SafetyNet 認証失敗］セクションでどのオプションを設定しているかに関係なく、そのアプリはアクティブ化されません。アプリは、既にアクティブ化されている場合、コンプライアンスプロファイルで指定したルールの対象となります。
- 組織のユーザーは、最新バージョンの Google Play サービスをインストールしている必要があります。
- デバイスが認証に失敗しても、［管理対象デバイス］ページの［OS 侵害］列には失敗の表示はありません。
- Android デバイス用の BlackBerry Dynamics アプリの開発については、開発者関連の資料を参照してください。

# SafetyNET 認証の設定に関する考慮事項 - アプリのバージョン

- 組織の Android デバイスに対して SafetyNet 認証を有効にする前に、デバイスユーザーがデバイス上の UEM Client をバージョン 12.9 MR1 以降にアップグレードしていることを確認してください。アップグレードしていない場合、デバイス上で猶予期間コンプライアンスアクションが強制されます。
- 組織の BlackBerry UEM インスタンスに対して認証を有効にし、BlackBerry UEM Client バージョン 12.10 をインストールしている場合、Android デバイスのアクティベーション中にデバイスの完全性と整合性が確認されます。BlackBerry UEM Client バージョン 12.9 MR1 がインストールされている場合は、アクティベーション後にデバイスレベルの SafetyNet 認証が実行されます。この機能を有効にする前に、Android 用 BlackBerry UEM Client バージョン 12.9 MR1 以降が組織の Android デバイスにインストールされていることを確認してください。

| **BlackBerry UEM** のバージョン | **SafetyNet** 認証が実行されるタイミング |
|---|---|
| 12.9 MR1 | デバイスのアクティベーション後 |
| 12.10 | • BlackBerry UEM Client がインストールされている場合はデバイスのアクティベーション後<br>• BlackBerry UEM Client がインストールされている場合はデバイスのアクティベーション中<br>• BlackBerry Dynamics アプリのアクティベーション中<br>• BlackBerry Dynamics アプリのアプリアクティベーション後<br>• REST API を使用してオンデマンドで<br>• BlackBerry UEM Client がアクティブ化されている場合はデバイスの再起動時 |

- BlackBerry UEM 12.9 MR1 を組織の環境にインストールし、SafetyNet 認証を有効にした場合、BlackBerry UEM 12.10 にアップグレードするときは、組織のコンプライアンスプロファイルで［Google SafetyNet 認証失敗］オプションを選択して、組織の Android デバイスが SafetyNet 認証強制アクションの対象にならないようにする必要があります。

# SafetyNet を使用した Android デバイスの認証の管理

Android SafetyNet 認証を使用する場合、BlackBerry UEM は、組織の環境内の Android デバイスとアプリの完全性と整合性をテストするためのチャレンジを送信します。SafetyNet は、組織のアプリを実行する環境のセキュリティと互換性を評価するのに役立ちます。SafetyNet の詳細については、Google の情報を参照してください。注：この機能を使用する前に、Android MR1 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。

この機能を使用する前に、Android MR1 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る点に注意してください。

1. メニューバーで［設定］**>**［一般設定］**>**［認証］をクリックします。
2. Android デバイスの認証をオンにするには、［**SafetyNet** を使用した定期的な認証チャレンジを有効にする］を選択します
3. Google の Compatibility Test Suite をオンにする場合は、［**CTS** プロファイルの一致を有効にする］を選択します。CTS の詳細については、Google の情報を参照してください。
4. ［チャレンジの頻度］セクションで、デバイスが認証応答を BlackBerry UEM に返す必要がある頻度を日数または時間数で指定します。
5. ［猶予期間］セクションで、猶予期間を時間数または日数で指定します。認証応答が得られずに猶予期間が終了すると、デバイスが準拠していないと見なされ、そのデバイスは、ユーザーに割り当てられているコンプライアンスプロファイルに指定された条件を適用されます。また、ユーザーのデバイスが通信範囲外にある場合、電源がオフになっている場合、またはバッテリーが切れている場合、BlackBerry UEM が送信する認証チャレンジに応答できず、BlackBerry UEM がデバイスは非準拠であると判断することも考慮してください。コンプライアンス違反時にデバイスを削除するように組織のコンプライアンスポリシーが設定されている場合、猶予期間が満了する前にデバイスが応答しないと、デバイス上のデータは削除されます。
6. ［保存］をクリックします。

# Windows 10 デバイスの認証の管理

認証をオンにすると、BlackBerry UEM は、Windows 10 デバイスの完全性と整合性をテストするためのチャレンジを送信します。デバイスは Microsoft Health Attestation Service と通信し、組織のコンプライアンスプロファイルで設定した設定に基づいてコンプライアンスを確認します。

1. メニューバーで［設定］ > ［一般設定］ > ［認証］をクリックします。
2. Windows 10 デバイスの認証をオンにするには、［**Windows 10** デバイスの定期的な認証チャレンジを有効にする］を選択します。
3. ［チャレンジの頻度］セクションで、デバイスが認証応答を BlackBerry UEM に返す必要がある頻度を日数または時間数で指定します。
4. ［猶予期間］セクションで、猶予期間を時間数または日数で指定します。認証応答が得られずに猶予期間が終了すると、デバイスが準拠していないと見なされ、そのデバイスは、ユーザーに割り当てられているコンプライアンスプロファイルに指定された条件を適用されます。また、ユーザーのデバイスが通信範囲外にある場合、電源がオフになっている場合、またはバッテリーが切れている場合、BlackBerry UEM が送信する認証チャレンジに応答できず、BlackBerry UEM がデバイスは非準拠であると判断することも考慮してください。コンプライアンス違反時にデバイスを削除するように組織のコンプライアンスポリシーが設定されている場合、猶予期間が満了する前にデバイスが応答しないと、デバイス上のデータは削除されます。
5. ［保存］をクリックします。

デバイスの詳細ページには、コンプライアンス違反を表示することができます。

終了したら：

デバイスがルートと見なされるときに実行される操作を指定するコンプライアンスプロファイルを作成します。手順については、BlackBerry UEM 管理関連資料の「デバイスのコンプライアンスルールの強制」を参照してください。

# 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 と DEP を同期できます。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。
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、http://support.blackberry.com/kb 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 で登録されている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。

# ユーザーのための BlackBerry UEM Self-Service のセットアップ

BlackBerry UEM Self-Service は、ユーザーがアクティベーションパスワードの作成、デバイスのリモートからのロック、デバイスからのデータの削除などの管理タスクを実行できるように、管理者がユーザーに対して使用可能にする Web ベースのアプリケーションです。ユーザーは、BlackBerry UEM Self-Service を使用するためにコンピューターにソフトウェアをインストールする必要はありません。管理者は、ユーザーに Web アドレスとログイン情報を提供する必要があります。

管理者は、ユーザーが BlackBerry UEM Self-Service にログインする前に、強制的にログイン通知を読んで、同意するように設定できます。注意事項通知の詳細については、管理関連資料の「コンソールのログイン通知の作成」を参照してください。

## BlackBerry UEM Self-Service をセットアップする

ユーザーがログインしていくつかのセルフサービスタスクを実行できるように、BlackBerry UEM Self-Service をセットアップします。

1. メニューバーで［設定］>［セルフサービス］をクリックします。
2. ［セルフサービス設定］をクリックします。
3. ［セルフサービスコンソールへのアクセスをユーザーに許可する］が選択されていることを確認します。
4. アクティベーションパスワードが期限切れになるまでに、デバイスをアクティブ化できる分数、時間数、日数を指定します。
5. アクティベーションパスワードに必要な最小文字数を指定します。
6. ［最低限のパスワードの複雑さ］ドロップダウンリストで、アクティベーションパスワードに必要な複雑さのレベルを選択します。
7. BlackBerry UEM Self-Service でアクティベーションパスワードを作成したときにアクティベーションメールをユーザーに自動的に送信するには、［アクティベーションメールを送信］チェックボックスをオンにします。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か、ドロップダウンリストから別のテンプレートを選択することができます。
8. BlackBerry UEM Self-Service にログインしたユーザーにログイン通知メールを送信するには、［セルフサービスログイン通知を送信］チェックボックスをオンにします。
9. ［保存］をクリックします。

終了したら： ユーザーに BlackBerry UEM Self-Service の Web アドレスとログイン情報を提供します。

# BlackBerry UEM ドメインで高可用性を設定する

BlackBerry UEM は有効/有効の高可用性モデルを使用し、デバイスユーザーのためにサービスの中断を最小限に抑えます。高可用性を設定するには、BlackBerry UEM の複数のインスタンスをそれぞれ個別のコンピューターにインストールします。各インスタンスは BlackBerry UEM データベースに接続し、ユーザーアカウントとデバイスを能動的に管理します。

BlackBerry UEM の高可用性には次の機能が含まれます。

| 機能 | 説明 |
| --- | --- |
| BlackBerry 10 デバイスを正常な BlackBerry UEM インスタンスに自動的に移動する | BlackBerry UEM インスタンスの BlackBerry 10 デバイスがエンタープライズ接続を使用して仕事用リソースに接続できない場合、これらのデバイスは健全な BlackBerry UEM インスタンスに再割り当てされます。BlackBerry 10 デバイスはエンタープライズ接続を使用してメールやカレンダーのデータ、仕事用ブラウザー、組織のネットワークにアクセスできます。エンタープライズ接続は、ほとんどの管理タスク（例：プロファイルの割り当て）を正常に完了するために必要です。 |
| iOS、Android、および Windows デバイスは任意の BlackBerry UEM インスタンスに接続可能 | 1 つ以上の BlackBerry UEM インスタンスが正常でない場合、iOS、Android、および Windows デバイスは、いずれか 1 つの正常なインスタンスに接続します。結果として、デバイスサービスは中断することなく継続されます。 |
| BlackBerry Affinity Manager フェールオーバー | BlackBerry Affinity Manager は、BlackBerry 10 デバイスを BlackBerry UEM インスタンスに割り当て、各インスタンスのエンタープライズ接続を監視し、エンタープライズ接続に問題がある場合には BlackBerry 10 ユーザーを移動します。BlackBerry Affinity Manager は iOS、Android、または Windows デバイスを特定の BlackBerry UEM インスタンスに割り当てることはできません。<br><br>BlackBerry Affinity Manager は 1 つだけアクティブで、その他の BlackBerry Affinity Manager インスタンスはスタンバイ状態です。アクティブな BlackBerry Affinity Manager に問題がある場合は、各スタンバイインスタンスがアクティブになるための選択プロセスを開始します。選択プロセスを最初に完了したインスタンスがアクティブな BlackBerry Affinity Manager になります。 |
| 任意の BlackBerry UEM インスタンスからデバイスを管理する | 管理コンソールまたは BlackBerry UEM インスタンスの BlackBerry UEM Core に問題がある場合、いずれかの正常なインスタンスの管理コンソールと BlackBerry UEM Core を使用してすべてのデバイス（BlackBerry 10、iOS、Android、および Windows デバイス）の管理を続行できます。 |
| 管理コンソールのラウンドロビン DNS プール | サードパーティソフトウェアを使用し、各 BlackBerry UEM インスタンスで管理コンソールに接続するラウンドロビン DNS プールを設定することができます。コンソールに問題がある場合、プールは機能しているコンソールに管理者が接続していることを確認します。 |

| 機能 | 説明 |
| --- | --- |
| BlackBerry Connectivity Node | BlackBerry Connectivity Node の 1 つ以上のインスタンスをインストールして、デバイス接続コンポーネントの追加インスタンスを組織のドメインに追加できます。また、サーバーグループを作成して、セキュリティ保護された接続のための地域データパスを指定し、BlackBerry Connectivity Node のコンポーネントの高可用性を設定することもできます。詳細については、「高可用性と BlackBerry Connectivity Node」を参照してください。 |

BlackBerry UEM が復元操作を完了すると、影響を受けるユーザーへのサービスは短時間中断されます。中断時間は、BlackBerry 10 デバイスの数および BlackBerry UEM インスタンスの数などの様々な要素に応じて変化します。BlackBerry 10 ユーザーが別のインスタンスに再割り当てされる場合、中断時間は平均で 3 分です。BlackBerry Affinity Manager フェールオーバーが発生する場合、中断時間は平均で 10 分です。

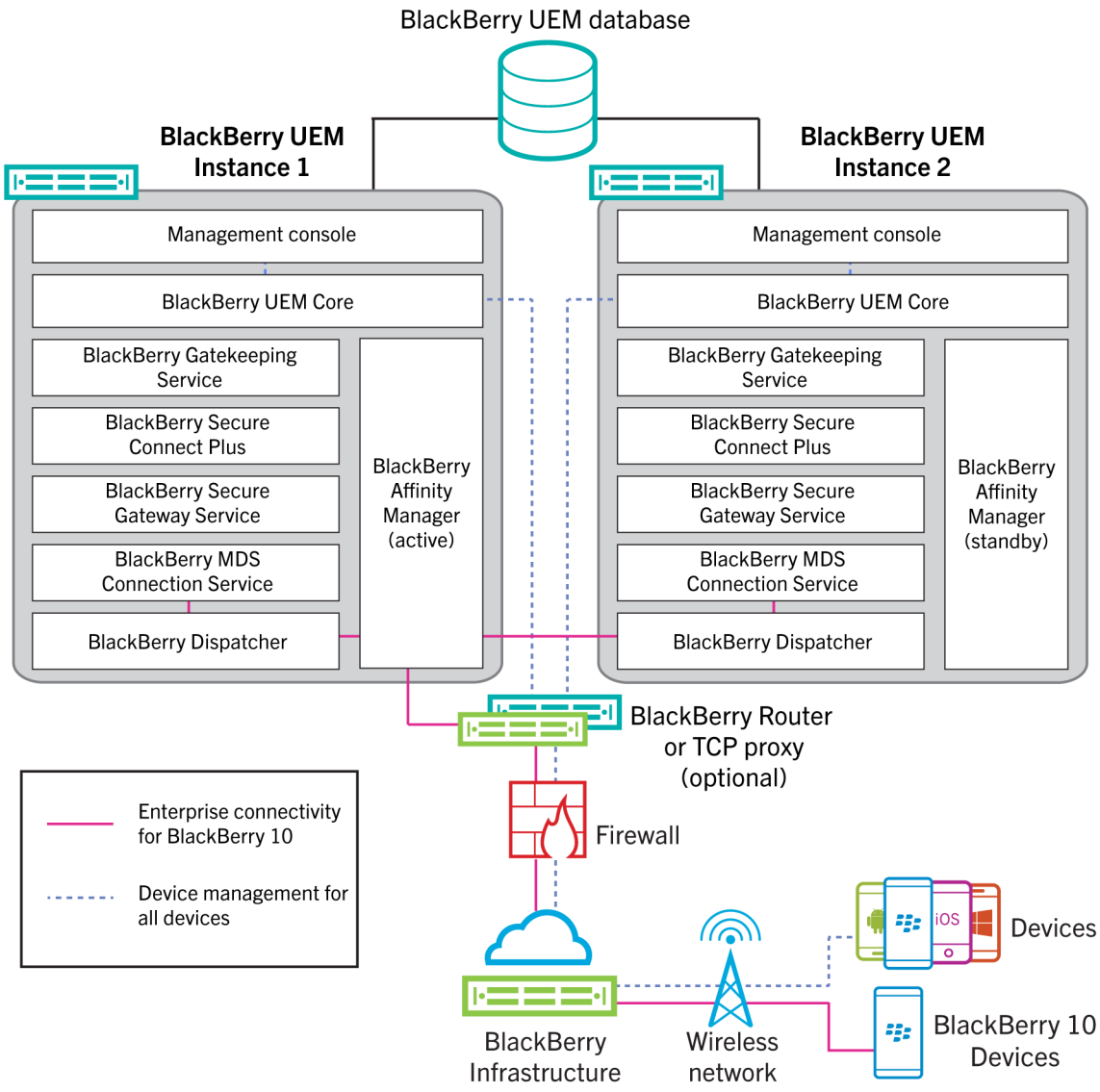
# BlackBerry OS デバイスを管理するコンポーネントの高可用性

BES5 から BlackBerry UEM にアップグレードする前に BES5 を高可用性に設定した場合、設定はアップグレードの完了後に予想通りに機能します。高可用性設定は BlackBerry OS デバイスを管理するコンポーネントのみに適用されます。

BlackBerry OS デバイスを管理するコンポーネントを高可用性に設定する方法の詳細については、help.blackberry.com/detectLang/category/enterprise-services にアクセスし、『*BlackBerry Enterprise Server 5* 管理ガイド』を参照してください。

# アーキテクチャ：BlackBerry UEM の高可用性

次の図は、2 つの BlackBerry UEM インスタンスを持つ高可用性ドメインを示しています。任意の数の BlackBerry UEM インスタンスをインストールできます。このトピックでは、特定のコンポーネントが高可用性設定にどのように関わるかを説明します。BlackBerry UEM のアーキテクチャおよびコンポーネントの詳細については、アーキテクチャ関連の資料を参照してください。




| コンポーネント | 説明 |
| --- | --- |
| BlackBerry UEM データベース | 各 BlackBerry UEM インスタンスは、BlackBerry UEM データベースに接続してユーザーやデバイスのデータにアクセスします。 |

| コンポーネント | 説明 |
| --- | --- |
| 管理コンソールと BlackBerry UEM Core | 任意の管理コンソールを使用して、ドメインのユーザーアカウントとデバイスを管理できます。コンソールに関連付けられた BlackBerry UEM Core は、管理タスクを事項します。<br>各コンソールに接続するラウンドロビン DNS プールを設定することができます。コンソールに問題がある場合、プールは機能しているコンソールに接続します。<br>それぞれのインスタンスは、BlackBerry 10 により割り当てられた BlackBerry Affinity Manager デバイスのエンタープライズ接続を管理します。いずれかの正常なインスタンスが、すべてのデバイスタイプのデバイス管理タスクを処理できます。 |
| BlackBerry MDS Connection Service および BlackBerry Dispatcher | これらのコンポーネントにより、BlackBerry 10 デバイスは仕事用リソースにアクセスしてこれを使用できます。 |
| BlackBerry Affinity Manager | BlackBerry Affinity Manager は次の操作を担当します。<br>• BlackBerry 10 デバイスを BlackBerry UEM インスタンスに割り当てる<br>• BlackBerry Infrastructure との接続を維持する<br>• アクティブな BlackBerry Work Connect Notification Service を設定して開始する<br>• 各インスタンスの BlackBerry MDS Connection Service および BlackBerry Dispatcher の健全性を確認し、エンタープライズ接続を監視する<br>BlackBerry Affinity Manager は 1 つだけアクティブです（他はスタンバイ状態です）。エンタープライズ接続の問題を検出したアクティブなインスタンスは、BlackBerry 10 ユーザーを健全な BlackBerry UEM インスタンスに再割り当てします。<br>各スタンバイ BlackBerry Affinity Manager は、アクティブな BlackBerry Affinity Manager を監視します。アクティブな BlackBerry Affinity Manager に問題がある場合は、フェールオーバーが発生し、スタンバイインスタンスの 1 つがアクティブになります。 |

# BlackBerry 10 デバイスのデータの負荷分散

BlackBerry UEM のインスタンスを同じドメインに複数インストールすると、BlackBerry 10 デバイスのデータはすべての健全な実行中のインスタンスでほぼ均等に負荷分散されます。たとえば、BlackBerry UEM の 3 つのインスタンスをインストールし、ドメインに 3000 台の BlackBerry 10 デバイスが含まれる場合、BlackBerry UEM は実行中の 3 つの各インスタンスにデバイス約 1000 台を割り当てます。

特定のサーバー上のデバイスの数が、サーバーごとの平均デバイス数よりも 500 以上多い場合、BlackBerry UEM は、負荷分散を実行します。

BlackBerry 10 デバイスを特定のインスタンスに手動で割り当てることはできません。BlackBerry Affinity Manager は、BlackBerry 10 デバイスを管理するインスタンスを判別します

インスタンスが一時的に使用できない場合、他のインスタンスがユーザーとデバイスのデータを管理します。

各 BlackBerry UEM インスタンスは同じ SRP ID を使用し、同じ BlackBerry UEM データベースに接続します。各インスタンスのすべてのコンポーネントは、BlackBerry Affinity Manager および BlackBerry Work Connect Notification Service.を除くあらゆる種類のデバイスで稼働し、データを能動的に管理します。BlackBerry Affinity Manager および BlackBerry Work Connect Notification Service ではインスタンス 1 つのみがアクティブです。

各インスタンスのステータスは、管理コンソールで表示できます。

# 高可用性と BlackBerry Connectivity Node

BlackBerry Connectivity Node の 1 つ以上のインスタンスをインストールして、デバイス接続コンポーネントの追加インスタンスを組織のドメインに追加できます。各 BlackBerry Connectivity Node は、BlackBerry Secure Connect Plus、BlackBerry Gatekeeping Service、BlackBerry Secure Gateway、BlackBerry Proxy、BlackBerry Cloud Connector という BlackBerry UEM コンポーネントを含んでいます。

各 BlackBerry Connectivity Node は、これらのコンポーネントの別のアクティブなインスタンスをセキュリティ保護されたデバイス接続を処理および管理できる BlackBerry UEM ドメインに提供します。BlackBerry Connectivity Node の計画およびインストールの詳細については、計画関連の資料とインストールおよびアップグレード関連の資料を参照してください。

サーバーグループを作成することもできます。サーバーグループには、BlackBerry Connectivity Node の 1 つ以上のインスタンスが含まれています。サーバーグループを作成するときに、コンポーネントが BlackBerry Infrastructure に接続するために使用する地域データパスを指定します。たとえば、サーバーグループを作成して、BlackBerry Secure Connect Plus のデバイス接続と BlackBerry Secure Gateway に、BlackBerry Infrastructure への米国のパスを使用するように指示することができます。メールとエンタープライズ接続プロファイルをサーバーグループに関連付けることができます。これらのプロファイルが割り当てられているどのデバイスも、BlackBerry Connectivity Node のいずれかのコンポーネントを使用するときには、そのサーバーグループの BlackBerry Infrastructure への地域接続を使用します。

サーバーグループに BlackBerry Connectivity Node の複数のインスタンスが含まれている場合、デバイスは実行中のどのインスタンスでも使用できます。デバイス接続は、グループ内の使用可能なインスタンス間で負荷分散されます。インスタンスを使用できない場合、デバイスは、セキュリティ保護された接続にこれらのコンポーネントを使用できません。少なくとも 1 つのインスタンスを使用できる必要があります。

# BlackBerry UEM がコンポーネントの健全性を評価する方法

次の BlackBerry UEM コンポーネントには、復元操作が必要かどうかを判別するための健全性スコアがあります。

| コンポーネント | 健全性の監視 | 健全性スコアの要素 | 健全性がしきい値を下回った場合の処理 |
| --- | --- | --- | --- |
| BlackBerry MDS Connection Service および BlackBerry Dispatcher（健全性スコアを合計します） | アクティブな BlackBerry Affinity Manager | • コンポーネントが稼働しているかどうか<br>• アクティブな BlackBerry Affinity Manager に接続できるかどうか<br>• BlackBerry 10 デバイスに接続できるかどうか<br>• データベースに接続できるかどうか | BlackBerry Affinity Manager が不健全な BlackBerry UEM インスタンスから健全なインスタンスに BlackBerry 10 デバイスを移動します。 |
| アクティブな BlackBerry Affinity Manager | 各スタンバイ BlackBerry Affinity Manager | • BlackBerry Affinity Manager のステータス（アクティブ、スタンバイ、またはアクティブになるための選択プロセス中）<br>• BlackBerry Dispatcher に接続できるかどうか<br>• BlackBerry UEM Core および各スタンバイ BlackBerry Affinity Manager からコールを受信できるかどうか<br>• BlackBerry Infrastructure に接続できるかどうか<br>• データベースに接続して設定をロードできるかどうか | スタンバイインスタンスがフェールオーバーを開始し、1 つがアクティブな BlackBerry Affinity Manager になります。 |

# 追加の BlackBerry UEM インスタンスをインストールする

高可用性ドメインを作成するために追加の BlackBerry UEM インスタンスをインストールするには、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。コンピューターが BlackBerry UEM インスタンスのインストールのためのシステム要件を満たしていることを確認し、インストールの前後に必要なタスクを完了します。互換性の詳細については、「互換性一覧表」を参照してください。

追加の BlackBerry UEM インスタンをインストールするときは次の操作を実行します。

- 各インスタンスを別のコンピューターにインストールします。
- セットアップアプリケーションの［セットアップの種類］画面で、［既存のドメインを使用する］を選択します。
- ［データベース情報］画面で、元の BlackBerry UEM のインストール時に作成した BlackBerry UEM データベースの情報を指定します。

追加の BlackBerry UEM インスタンスをインストールしてインストール後に必要なタスクを完了すると、有効/有効の高可用性設定がドメインで使用できるようになります。ユーザーとデバイスのデータは、BlackBerry UEM インスタンスで均等に負荷分散され、アクティブな BlackBerry Affinity Manager は各インスタンスのエンタープライズ接続を監視し、スタンバイ状態の BlackBerry Affinity Manager インスタンスはアクティブなインスタンスを監視してフェールオーバーが必要かどうかを判別します。

# 管理コンソールの高可用性の設定

BlackBerry UEM 管理コンソールを高可用性に設定するために、組織のハードウェア負荷分散装置または DNS サーバーを使用して、ドメイン内の各管理コンソールに接続するラウンドロビンプールを設定できます。管理コンソールが使用できない場合、負荷分散装置または DNS サーバーは使用可能な他のコンソールの 1 つに接続します。

ラウンドロビンプールのセットアップの詳細については、組織のハードウェア負荷分散装置または DNS サーバーに関するドキュメントを参照してください。

ラウンドロビンプールを設定した後は、管理コンソールの %AdminPortalURL% 変数および %UserSelfServicePortalURL% 変数（［設定］ > ［一般設定］ > ［デフォルトの変数］）をプール名で更新することをお勧めします。この操作により、管理コンソールと BlackBerry UEM Self-Service へのリンクにこれらの変数を使用するメールは、ラウンドロビンプールを使用できます。

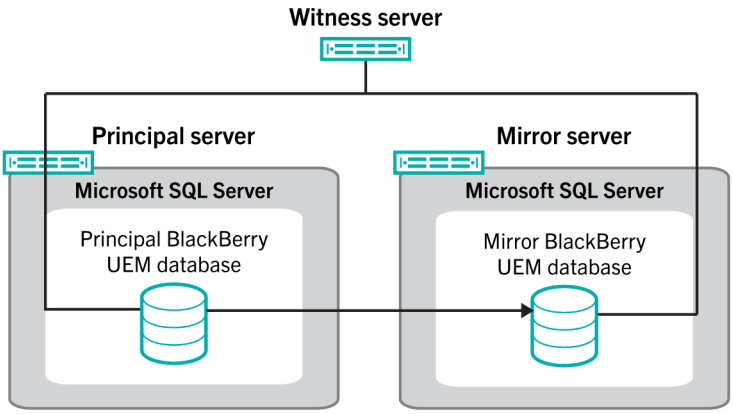
シングルサインオンを有効にした場合、そのプール名が付いた Microsoft Active Directory アカウント用の SPN を更新し、BlackBerry UEM インスタンスをホストするそれぞれのコンピューターで BlackBerry UEM サービスを再起動する必要があります。

DNS サーバーがインスタンスに異なる IP アドレスを割り当てる場合は、ラウンドロビンプールの BlackBerry UEM 管理コンソールインスタンスは BlackBerry UEM ドメインから切断できます。新しい IP アドレスがユーザーのログイン情報を認識しないため、インスタンスは切断されます。このような場合は、ユーザーはいったんログアウトし、再度ログインする必要があります。

関連タスク

Microsoft Active Directory アカウントがシングルサインオンをサポートするための制約付き委任の設定

# データベースミラーリングを使用して高可用性データベースを設定する




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。

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 の使い方の詳細については、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。AlwaysOn 機能は、BES5 から BlackBerry UEM にアップグレード（BES5 データベースを BlackBerry UEM データベースにアップグレード）した場合使用できないため、ご注意ください。AlwaysOn は、BlackBerry OS デバイスを管理するコンポーネントではサポートされていません。

データベースミラーリングを設定する場合は、プリンシパル BlackBerry UEM データベース（インストール時に作成されたデータベース）をバックアップし、バックアップファイルを使用してべつのコンピューターにミラーデータベースを作成します。その後、2 つのデータベースの間にミラーリング関係を設定し、ミラーデータベースが同じ処理を実行して同じデータを保存するようにします。

自動フェールオーバーを有効にするには、ウィットネスサーバーをセットアップしてプリンシパルデータベースを監視します。プリンシパルデータベースが応答を停止した場合、ウィットネスサーバーは自動フェールオーバーを開始してデータベースをミラーリングします。BlackBerry UEM コンポーネントはデータベースをミラーリングし、デバイスサービスは中断することなく継続されます。ロールスイッチが発生すると、ミラーデータベースはプリンシパルデータベースになり、元のプリンシパルデータベースはミラーデータベースになります。このロールスイッチは、ミラーリングセッション中に発生する可能性があります。

このセクションでは、ミラーデータベースの作成方法と BlackBerry UEM コンポーネントを設定してデータベースミラーリングをサポートする方法を説明します。BlackBerry OS デバイスを管理するコンポーネントにデータベースミラーリングを設定するオプションも使用できます。詳細については、「BlackBerry OS デバイスを管理するコンポーネントのための高可用性データベース」を参照してください。

データベースミラーリングの詳細については、technet.microsoft.com/sqlserver にアクセスし、『データベースミラーリング - SQL サーバー 2012』または『データベースミラーリング - SQL サーバー 2014』を参照してください。

# BlackBerry OS デバイスを管理するコンポーネントのための高可用性データベース

BlackBerry 10、iOS、Android、および Windows の各デバイスを管理する BlackBerry UEM コンポーネントは、BlackBerry OS デバイスを管理するコンポーネントと同じデータベースを使用します。BlackBerry OS デバイスを管理するコンポーネントは、別の方法を使用してミラーデータベースに接続します。BlackBerry OS デバイスを管理するコンポーネントのためのデータベースミラーリングを設定する場合は、このセクションの完了後に追加の手順を実行できます。

help.blackberry.com/detectLang/category/enterprise-services にアクセスし、『*BlackBerry Enterprise Server 5* 管理ガイド』の「BlackBerry Configuration Database の高可用性の設定」を参照してください。この章には、BlackBerry OS デバイスを管理するコンポーネントをミラーデータベースに接続する手順が記載されています。

メモ：「BlackBerry Configuration Database の高可用性の設定」には、Microsoft SQL Server 2005 の説明が含まれます。このバージョンの Microsoft SQL Server のサポートは終了しています。

BES5 から BlackBerry UEM にアップグレードする前に BES5 のデータベースミラーリングを設定した場合、設定はアップグレードの完了後に予想通りに機能します。設定は BlackBerry OS デバイスを管理するコンポーネントのみに適用されます。

## 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 | BlackBerry UEM ドメインがシステム要件や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。 |

## システム要件：データベースミラーリング

| 項目 | 要件 |
| --- | --- |
| Microsoft SQL Server | BlackBerry UEM は、次のいずれかを使用したデータベースミラーリングをサポートしています。<br>• Microsoft SQL Server 2012<br>• Microsoft SQL Server 2014 |

| 項目 | 要件 |
| --- | --- |
| SQL Server Native Client | SQL Server 2012 Native Client は、BlackBerry UEM インスタンスをホストする各コンピューターにインストールされている必要があります。BlackBerry UEM セットアップアプリケーションは SQL Server 2012 Native Client をインストールします。 |
| バージョンパリティ | ミラーデータベースをホストする Microsoft SQL Server は、プリンシパルデータベースをホストする Microsoft SQL Server と同じバージョンおよびエディションであることが必要です。 |
| シングルデータセンター | プリンシパルデータベースおよびミラーデータベースは、同じデータベースセンターに配置されていることが必要です。 |
| データベースの場所 | プリンシパルデータベースと別のコンピューターにミラーデータベースを作成します。 |
| 操作モード | 自動フェールオーバーを備えた高度に安全なモードでデータベースミラーリングを設定します。 |
| ウィットネス | ウィットネスサーバーは自動フェールオーバーに必要です。ウィットネスサーバーは、プリンシパルサーバーやミラーサーバーと別のサーバーであることが必要です。<br>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。 |

# 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、http://support.blackberry.com/kb にアクセスし、記事 KB34373 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 サーバー 2012』または『データベースミラーリング - SQL サーバー 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します。。

# BlackBerry UEM をミラーデータベースに接続します。

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、http://support.blackberry.com/kb 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）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します。 を繰り返します。

必要に応じて、BlackBerry OS デバイスを管理するコンポーネントを設定し、新しいミラーサーバーに接続します（BlackBerry OS デバイスを管理するコンポーネントのための高可用性データベース を参照）。

# BlackBerry Secure Gateway を有効にする場合の Exchange ActiveSync への TLS/SSL 接続の設定

BlackBerry Secure Gateway を有効にして、BlackBerry UEM を介した、組織のメールサーバーと MDM 制御 アクティベーションタイプの iOS デバイスの間のセキュリティで保護された接続を提供する場合は、BlackBerry UEM を設定して、Exchange ActiveSync への TLS/SSL 接続を作成する必要がある場合があります。BlackBerry Secure Gateway の有効化の詳細については、管理関連の資料の「BlackBerry Secure Gateway を使用してメールデータを保護する」を参照してください。

Exchange ActiveSync サーバーが TLS 接続を必要とするように構成されている場合、Exchange ActiveSync サーバー証明書（またはそのルート証明書）を BlackBerry UEM に追加する必要があります。BlackBerry Secure Gateway は、TLS/SSL 接続を確立するときに、Exchange ActiveSync サーバーを信頼するための証明書を必要とします。

Exchange ActiveSync サーバーのセキュリティ要件に応じて、BlackBerry Secure Gateway が Exchange ActiveSync との認証に使用できる TLS バージョンと暗号のリストを更新する必要があります。

## Exchange ActiveSync サーバー証明書を信頼するように BlackBerry UEM を設定する

作業を始める前に： Exchange ActiveSync サーバーから X.509 形式（*.cer、*.der）で証明書をエクスポートし、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保存します。

1. 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。
2. ［**Exchange ActiveSync** サーバー信頼］の横にある＋をクリックします。
3. ［参照］をクリックします。
4. 使用する証明書ファイルを選択します。
5. ［開く］をクリックします。
6. 証明書の説明を入力します。
7. ［追加］をクリックします。

## Exchange ActiveSync がサポートする TLS バージョンと暗号を使用するように BlackBerry UEM を設定します。

1. メニューバーで、［設定］ > ［外部統合］ > ［**BlackBerry Secure Gateway**］をクリックします。
2. 変更するテーブルの＋をクリックします。
3. ［選択］リストで追加または削除する TLS バージョンまたは暗号をクリックします。
4. 矢印をクリックして、目的のリストに項目を移動します。
5. ［割り当て］をクリックします。

# Windows 10 アクティベーションの簡易化

Java から検出サービスとして BlackBerry 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 | 自動検出プロキシツールをダウンロードするには、BlackBerry UEM ツールを参照します。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。

```
C:\Program Files (x86)\Java\jre1.8.0_60\bin>keytool -genkey -alias tomcat -
keyalg RSA -keysize 2048
C:\Program Files (x86)\Java\jre1.8.0_60\bin> keytool -certreq -alias tomcat -
keyalg RSA -file <filename>.csr
```

```
C:\Program Files (x86)\Java\jre1.8.0_60\bin>keytool -genkey -alias tomcat -
keyalg RSA -keysize 2048
Enter keystore password: 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. 自動検出プロキシツールをダウンロードするには、BlackBerry UEM ツールを参照します。.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。

# 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 12.8 または 12.9 に移行してから BlackBerry UEM バージョン 12.10 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 12.10 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/kb にアクセスして記事 KB 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/kb 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<br>• データの移行元となる BlackBerry UEM インスタンスは、バージョン 12.8 以降である必要があります。<br>• 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。<br>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（BES10 および BlackBerry UEM）のデフラグ | 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。<br>• 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。<br>• 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。<br>• 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。<br>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/kb にアクセスし、記事 KB47626 を参照してください。 |

# 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。 |
| | 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。 |

| 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<br>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<br>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<br>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。<br>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、ソフトウェア設定割り当て、および BlackBerry OS 属性は移行されません。

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、BES12 または 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 BES12 または 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。<br>• ポリシーセットの各アプリの設定<br>• セキュリティポリシー<br>• 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。<br>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。<br>• 移行先サーバーに既に存在するアプリの使用状況<br>• BlackBerry Dynamics 以外のアプリ<br>• 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<br>。 |
| 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。<br>2. ユーザーアカウントを検索します。<br>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。<br>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。<br>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。<br>2. アクセスキーを生成するユーザーを選択します。<br>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。<br>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。<br>• Wi-Fi<br>• VPN<br>• プロキシ<br>• メール<br>• Web アイコン<br>• 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。<br>［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。<br>［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。<br>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。<br>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。<br>• 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。<br>• 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。<br>• 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。<br>• 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 つ以上割り当てるか、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。<br>• 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。 |
| iOS ソース上の BlackBerry UEM 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。<br>• 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）<br>• 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。<br>• 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。 |

| 項目 | 考慮事項 |
| --- | --- |
| Good Control デバイス（スタンドアロン Good Control から） | **BlackBerry Dynamics** アプリ<br>• 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。<br>• 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。<br>• ［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。<br>• 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。<br>• 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。<br>• 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/kb にアクセスし、記事 KB47626 を参照してください。<br>デバイス認証<br>• 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。<br>• 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。<br>デバイス管理<br>• 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。<br>オペレーティングシステム<br>• 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。<br>チャットセッション<br>• 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。<br>• 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。<br>ユーザー<br>• 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。 |

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の種類/構成 | 移行 |
|---|---|---|
| BlackBerry 10 | 次の条件のいずれか | サポート |
| Android | • MDM 制御<br>• BlackBerry 2FA | サポート |
| 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<br>• BlackBerry 2FA 専用のデバイス登録<br>• BlackBerry UEM Client がインストール済みの DEP デバイス | サポート |
| iOS | • 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 クラスターを作成します。 | **a.** ＋をクリックします。<br>**b.** クラスターの名前を入力します。<br>**c.** ［保存］をクリックします。 |
| BlackBerry Proxy クラスターの名前を変更します。 | **a.** クラスター名をクリックします。<br>**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。<br>**c.** ［保存］をクリックします。 |
| BlackBerry Proxy インスタンスを別の BlackBerry Proxy クラスターに移動します。 | **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。<br>**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。<br>**c.** ［保存］をクリックします。 |
| 空の BlackBerry Proxy クラスターを削除します。 | **a.** そのクラスターの✕をクリックします。<br>**b.** ［削除］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に BlackBerry Proxy を有効にします。 | 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。 |

# BlackBerry Proxy 接続用の Direct Connect または Web プロキシの設定

デフォルトでは、ユーザーのデバイス上の BlackBerry Dynamics アプリは、BlackBerry Dynamics NOC にデータを送信します。デバイスと BlackBerry Dynamics NOC の物理的な距離に応じて、接続にはネットワーク遅延が発生する可能性があります。

これらの問題を軽減するために、BlackBerry Dynamics Direct Connect を有効にすることができます。Direct Connect は、BlackBerry Dynamics アプリが NOC への接続をバイパスして組織のファイアウォールの背後にある BlackBerry Proxy インスタンスに直接接続できるようにします。デバイスが BlackBerry Dynamics NOC よりもドメイン内の BlackBerry Proxy インスタンスに物理的に近い場合、Direct Connect はネットワークの遅延を削減できます。

BlackBerry Dynamics アプリが、BlackBerry Proxy インスタンスに接続するときに、DMZ 内の Web プロキシサーバーを介してデータを送信するようにアプリを設定することもできます。

作業を始める前に：

- BlackBerry Dynamics アプリからの接続を Web プロキシサーバーを介してルーティングする場合は、プロキシサーバーが HTTP Connect コマンドをサポートしている必要があり、認証を要求しないようにする必要があります。組織の内部ファイアウォールでは、ポート 17533 経由の接続を許可する必要があります。
- BlackBerry Proxy インスタンスの Web プロキシサーバーを設定しない場合は、組織の内部および外部のファイアウォールがポート 17533 経由の接続を許可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. ［**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。

   ホスト名を変更した場合、BlackBerry Proxy インスタンスはクライアント接続用の新しい証明書を生成し、証明書への署名を求める要求を BlackBerry Dynamics CA に送信します。
5. Web プロキシを設定するには、［**Web** プロキシを使用］チェックボックスをオンにします。完全修飾ホスト名とポート番号を指定します。
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、および BlackBerry Proxy プロパティ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、http://support.blackberry.com/kb 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）。<br>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。<br>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 |

| プロパティ | 説明 | デフォルト | 再起動 |
| --- | --- | --- | --- |
| 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。<br>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。<br>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。<br>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.max.write.throughput | コンテナ管理の同時書き込み操作の最大数。<br>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 |

| プロパティ | 説明 | デフォルト | 再起動 |
| --- | --- | --- | --- |
| 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 |
| --- | --- | --- | --- |
| 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 |

| プロパティ | 説明 | デフォルト | 再起動 |
| --- | --- | --- | --- |
| 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<br>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。 | 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）。<br>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。 | 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 | — |
| 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。<br>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。<br>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 |
| gp.eacp.command.service.nslo | 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.<br>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。<br>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 | — |
| gp.proxy.auth.username | 外部 Web プロキシサーバーに接続するためのユーザー名 | 設定なし | いいえ |

| プロパティ | 説明 | デフォルト | 再起動 |
| --- | --- | --- | --- |
| gp.proxy.auth.domain | 外部 Web プロキシサーバーへの認証ログインのための Active Directory ドメイン | 設定なし | いいえ |
| gp.proxy.auth.password | 外部 Web プロキシサーバーに認証するためのパスワード | 設定なし | いいえ |
| gp.proxy.https.host | 外部 Web プロキシサーバーの名前 | 設定なし | いいえ |
| gp.proxy.https.port | 外部 Web プロキシサーバーへの HTTPS 接続のポート番号 | 設定なし | いいえ |
| GP プロキシ URL 制御 | 次のオプションのいずれかを入力します。<br>1. NOC URL（qp.proxy.urls は無視されます）<br>2. Route All（qp.proxy.urls は無視されます）<br>3. Custom URLs List（qp.proxy.urls に URL を入力します。リストに NOC URL を含める必要があります）。 | 1 | いいえ |
| gp.proxy.urls | プロキシする必要がある URL | 設定なし | はい |
| gp.proxy.use | 外部 Web プロキシサーバーを使用します | オフ | いいえ |

# 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、TLSv1、v1.1、および v1.2 が許可され、SSLv3 は許可されません。プロトコルを 1 つ以上選択する必要があります。

注意： SSLv3 のみを選択しないでください。これにより、クライアントへのすべての接続が切断される可能性があります。

1. 管理コンソールのメニューバーで、［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。

# BlackBerry Dynamics アプリの証明書の設定

ユーザーのデバイス上の BlackBerry Dynamics アプリがクライアント証明書を使用できるようにする場合は、個々のユーザーアカウントに証明書をアップロードするか、BlackBerry UEM が CA からのクライアント証明書を自動的に登録してデバイスに送信するように PKI コネクターを設定することができます。

ユーザーアカウントに証明書をアップロードする場合は、ユーザー証明書の有効期間を設定する必要があります。有効期間が終了すると、証明書がサーバーから削除されます。

CA によって発行された証明書を BlackBerry Dynamics アプリに自動的に登録する場合は、PKI コネクターを設定する必要があります。

Purebred などのアプリベースの PKI ソリューションを使用して、BlackBerry Dynamics アプリの証明書を登録することもできます。詳細については、管理関連の資料を参照してください。

## クライアント証明書の有効期間の設定

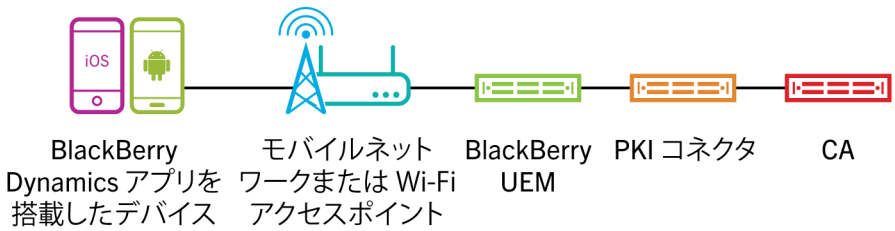
BlackBerry Dynamics アプリの個々のユーザーアカウントに証明書をアップロードする場合は、クライアント証明書の有効期間を設定する必要があります。有効期間が終了すると、証明書がサーバーから削除されます。これにより、クライアント証明書がデバイスにプッシュされた後も、長期間サーバー上に残ることを防止します。デフォルトの有効期間は 24 時間です。

1. メニューバーで［設定］ > ［一般設定］ > ［証明書］をクリックします。
2. サーバー上の PKCS#12 証明書の有効期間を指定します。

終了したら： クライアント証明書をユーザーアカウントに追加します（まだ行っていない場合）。

## BlackBerry Dynamics アプリの PKI 接続の設定

エンタープライズ CA によって発行された証明書を BlackBerry Dynamics アプリに自動的に登録するには、PKI コネクターを介して CA と通信する必要があります。PKI コネクターは、バックエンドサーバー上の Java プログラムと Web サービスのセットであり、BlackBerry UEM が証明書要求を送信し、CA から応答を受信できるようにします。




BlackBerry UEM は、BlackBerry Dynamics ユーザー証明書管理プロトコルを使用して、PKI コネクターと通信します。このプロトコルは HTTPS を介して実行され、JSON 形式のメッセージを定義します。

PKI コネクターは、ユーザー証明書管理プロトコルを実装しています。PKI コネクターの実装の例については、「PKI Cert Creation via Good Control: Reference Implementation」（Good Control を使用した PKI 証明書の作成：参照の実装）を参照してください。このドキュメントの PKI コネクターを構築および展開する例は、BlackBerry UEM にも適用されます。ただし、管理関連の資料の説明に従って、BlackBerry UEM 管理コンソールで BlackBerry UEM と PKI コネクターの間の接続を設定する必要があります。

### PKI コネクターの相互作用

BlackBerry UEM は、HTTP POST メソッドを使用して、PKI コネクターへの API コールを実行します。PKI コネクターは、パスワード認証および証明書ベースの認証をサポートしています。

#### GetInfo API

この API は、PKI コネクターが実装しているコマンドを検出します。このコマンドは、BlackBerry UEM で提供される認証資格情報の検証、および BlackBerry UEM と PKI コネクターとの間の接続のテストにも使用されます。

このコマンドが実装されていない場合、BlackBerry UEM は、有効な PKI コネクターではないと想定します。

送信された URI のパスコンポーネントは次のとおりです。`customerSpecifiedPrefix/pki?operation=getInfo`

`customerSpecifiedPrefix` はオプションです。デフォルトのパスでホストされていないときに、サービスがホストされているサーバー上の場所を指定します。

HTTP 本文で予期される JSON 形式の応答は、次のようになります。

| 要素またはキー | 種類 | 必須 | 応答 |
|---|---|---|---|
| 操作 | 文字列の配列 | Y | PKI コネクターによって実装されたすべてのコマンドを一覧表示した配列 |

要求/応答の例

BlackBerry UEM 管理コンソールで、PKI コネクターの URL が https://cert.example.com のように設定されていると仮定します。

```
GET /pki?operation=getInfo HTTP/1.0
Host: cert.example.com
Content-Type: application/json
Content-Length: 0

応答

HTTP/1.0 200 OK Host: cert.example.com
Content-Type: application/json
Content-Length: XYZ

{
      “operations” : [“getInfo”, “getUserKeyPair”]
}
```

#### キーペアの要求 API

この API は、キーペアが作成されたときにユーザー証明書を取得するために使用されます。この要求は、最初の証明書要求に使用される可能性があります。

送信される URI のパスコンポーネントは次のとおりです。`customerSpecifiedPrefix/pki?operation=getUserKeyPair`

`customerSpecifiedPrefix` はオプションです。デフォルトのパスでホストされていないときに、サービスがホストされているサーバー上の場所を指定します。

HTTP 本文で送信される JSON 形式の入力は、次のとおりです。

| 要素またはキー | 種類 | 必須 | コメント |
|---|---|---|---|
| mType | 文字列 | Y | {"initialCert"] |
| user | 文字列 | Y | ユーザーのメールアドレスまたはその他の識別子<br>発行者によって作成される証明書のサブジェクト |
| authToken | 文字列 | N | OTP またはパスワード（initialCert の場合） |
| reqId | 文字列 | Y | 送信者による応答との照合を支援するため |

HTTP 本文の JSON 形式の応答の暗号化される場合がある PKCS #12 ペイロードは次のようになります。

| 要素/キー | 種類 | 必須 | コメント |
|---|---|---|---|
| status | 文字列 | Y | {success, failure} |
| failureInfo | 文字列 | N | 下の失敗の理由を参照してください |
| payloadType | 文字列 | N | =pkcs12 |
| payload | Base64 エンコード | N | ユーザーの秘密鍵と公開証明書を含む pkcs12。暗号化される場合とされない場合があります。 |
| decryptionPassword | Base64 エンコード | N | 暗号化パスワードがユーザーが提供する OTP と同じである場合は、descryptionPassword を提供する必要はありません。<br>pkcs12 がパスワードで暗号化され、OTP が使用されなかった場合、decryptionPassword でパスワードが返されます。 |
| reqId | 文字列 | Y | リクエストで受信した reqID |

要求/応答の例

BlackBerry UEM 管理コンソールで、PKI コネクターの URL が https://cert.example.com のように設定されていると仮定します。

要求：SSL 接続を介して、サーバー cert.example.com に次のペイロードが送信されます。

```
POST /pki?operation=getUserKeyPair HTTP/1.0
Host: cert.example.com
Content-Type: application/json
Content-Length: XYZ
{
      "mType": "initialCert",
      "user": "joe.foo@example.com",
      "authToken": "56ht12d0",
      "reqId": "12487"
}
```

サーバー URL が https://cert.example.com/foo に設定されている場合、要求は次のようになります。

```
POST /foo/pki?operation=getUserKeyPair HTTP/1.0
Host: cert.example.com
Content-Type: application/json
Content-Length: XYZ
```

応答：

```
HTTP/1.0 200 OK
Host: cert.example.com
Content-Type: application/json
Content-Length: XYZ
 {
      "status":"success",
      "reqId": "12487",
      "payloadType":"pkcs12",
      "decryptionPassword":"NTZodDEyZDA=",
      "payload":"BASE64 Encoded PKCS#12"
}
```

障害の理由

以下のエラーは、CA によって返されます。

| 失敗 | 説明 |
| --- | --- |
| unknownUser | ユーザーが存在しないか、許可されていません |
| badRequest | 要求の形式が正しくありません |
| unknownRequest | 要求されたアクションはサポートされていません |
| authFailure | OTP またはパスワードが有効期限切れまたは不正です |
| badAlg | サポートされていないまたは認識されないアルゴリズムが使用されました |
| unknownCert | 操作で使用または参照されている証明書が見つかりません |
| badMessageCheck | 署名または整合性チェックに失敗しました |
| badTime | 署名の時間が十分ではありませんでした |
| unknown | 不明なエラーとして処理されたその他のエラー |

# 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、デバイスがルーティング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）。<br>• BlackBerry 10 OS バージョン 10.3.2 以前（10.3.3 以降が必要）<br>• Android 6.0（Marshmallow）<br>• BlackBerry OS（バージョン 7.1 以前）<br>• デスクトップ向け Windows 10<br>Cisco ISE は、「iOS 」アクティベーションタイプの 仕事用と個人用 - ユーザーのプライバシー デバイスのデータを取得できません。 |
| 待機ポート | Cisco ISE は、BlackBerry Web Services 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 UEM 待機ポート 18084 を使用します。<br>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。

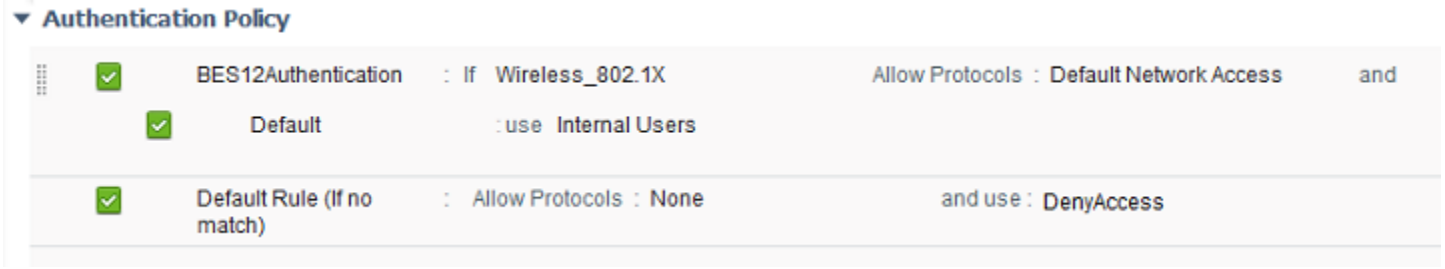
接続が確立した後、［**Policy**］ > ［**Policy Elements**］ > ［**Dictionaries**］ > ［**System**］ > ［**MDM**］ > ［**Dictionary Attributes**］で、BlackBerry UEM の辞書の属性を表示できます。Cisco ISE のポーリングのログエントリは、BlackBerry UEM Core （CORE）ログファイルに記録されます。

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）。

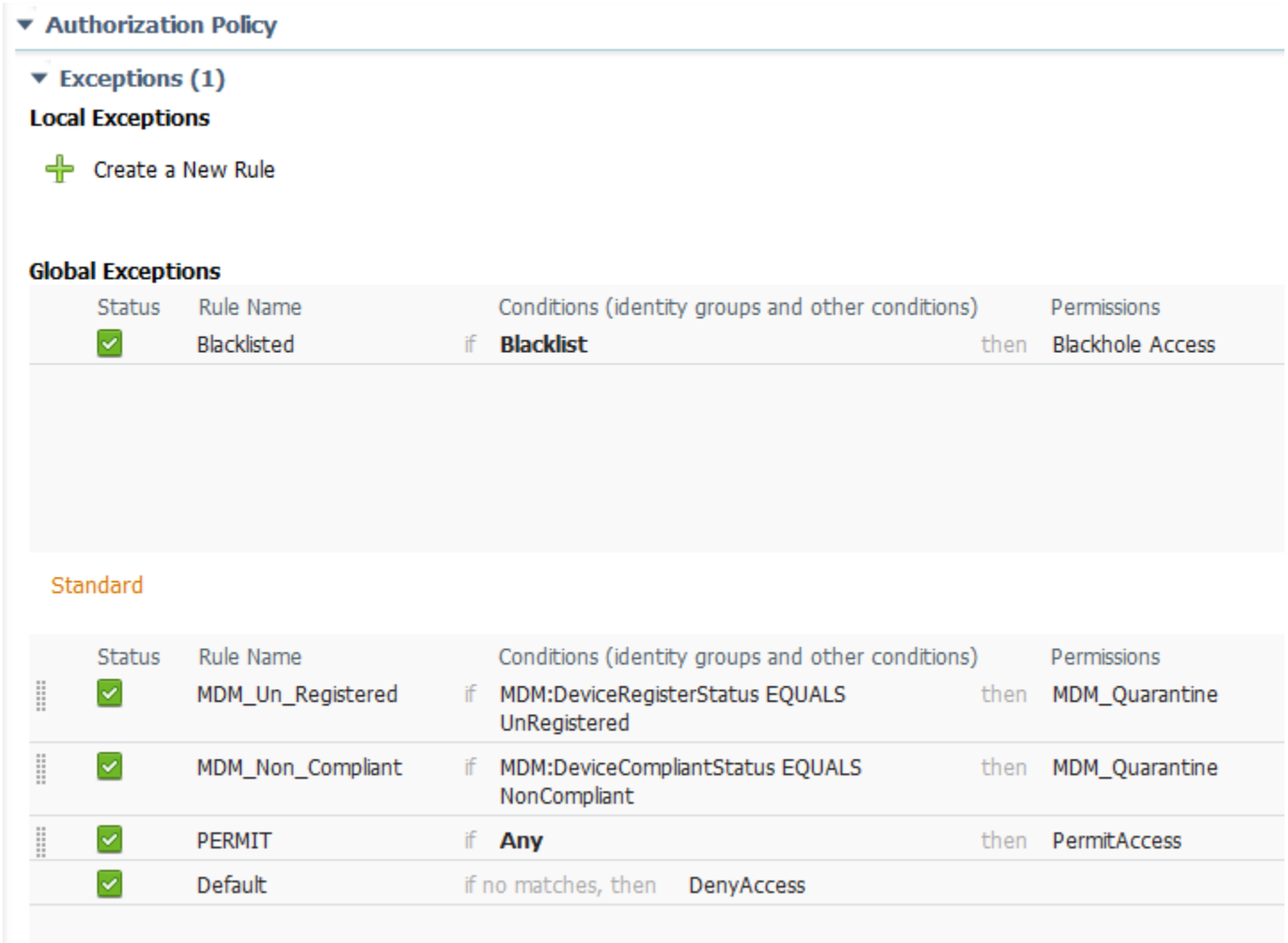
- ワイヤレス LAN コントローラーで ACL を設定します。
- BlackBerry UEM でアクティブ化されていないデバイスをリダイレクトする、認証プロファイルを設定します。詳細については、「BlackBerry UEM でアクティブ化されていないデバイスのリダイレクト」を参照してください。
- BlackBerry UEM でアクティブ化されていないか BlackBerry UEM に準拠していないデバイスを、Cisco ISE が処理する方法を決定する、認証ポリシールールを設定します。［**Policy**］ > ［**Policy Sets**］で、ポリシーを作成します。ポリシ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




認可ポリシー



# 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。<br>• MAC アドレス：デバイス固有の MAC アドレス<br>• 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<br>• 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<br>• 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<br>• 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<br>• 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<br>• 製造元<br>• 機種<br>• シリアル番号<br>• 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。<br>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。<br>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。<br>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 にログインしてデバイスをアクティブ化するには、BlackBerry UEM Self-Service のユーザーアカウントが必要です。BlackBerry UEM 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 Cisco ISE 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。

# SNMP ツールを使用した BlackBerry UEM の監視

サードパーティ SNMP ツールを使用して、いくつかの BlackBerry UEM コンポーネントのアクティビティを監視できます。SNMP 監視には、SNMP サービスと SNMP 管理ツールが必要です。BlackBerry UEM をホストするコンピューターで、SNMP サービスを実行します。Windows Services に配置された SNMP サービスには、BlackBerry UEM コンポーネントからデータを収集する SNMP エージェントが含まれます。

また、SNMP 管理ツール（MIB ブラウザーなど）を使用して、エージェントから受信したデータの表示と分析を実行します。通常、管理ツールには、エージェントからのトラップメッセージの取得と解釈に使用される SNMP トラップ管理ツールが含まれます。管理ツールは、BlackBerry UEM をホストするコンピューターまたは別のコンピューターにインストールできます。

SNMP を設定する場所は、2 か所あります。

- BlackBerry UEM Core、BlackBerry Secure Connect Plus、BlackBerry Secure Gateway、および BlackBerry Cloud Connector を監視するには、管理コンソールの SNMP を設定します。「SNMP を設定してコンポーネントを監視する」を参照してください。
- BlackBerry UEM エンタープライズ接続コンポーネントを監視するには、SNMP サービスを設定します。

デフォルトでは、管理ツールは条件の OID を表示します。これは、クラス階層内のクラス値を識別する一連の整数です。BlackBerry UEM の SNMP OID および SNMP トラップはすべて、クラス値が 1.3.6.1.4.1.3530.8 で始まります。サフィックス（たとえば、25.1.1）は、各 OID 値を一意に識別します。

MIB は、SNMP エージェントが監視する条件を指定します。MIB は、BlackBerry UEM コンポーネントの変数と管理データを定義および説明するデータベースで、各 SNMP トラップ値の意味を含みます。MIB は、コンポーネントについて SNMP サービスが収集できるデータの種類を決定します。SNMP モニタリングを設定するとき、管理者は管理ツールを使用して MIB をコンパイルします。

SNMP のネットワークセキュリティの詳細については、support.microsoft.com を参照してください。

## サポートされる SNMP 操作

SNMP 操作を使用して、BlackBerry UEM がインストールされたコンピューター上で実行されている SNMP エージェントからデータを収集できます。BlackBerry UEM は次の SNMP 操作をサポートしています。

| 操作 | 説明 |
| --- | --- |
| ゲット | 特定の MIB 項目の値を取得します。 |
| 次をゲット | MIB ファイル内の順序で項目の値および OID を取得します。 |
| トラップ | SNMP エージェントからの SNMP トラップメッセージを SNMP トラップ管理ツールに送信します。SNMP トラップメッセージには、BlackBerry UEM コンポーネントが実行する特定の操作に関するデータが含まれています。 |

# システム要件：SNMP 監視

| 項目 | 要件 |
| --- | --- |
| サポートされる BlackBerry UEM コンポーネント | 次の BlackBerry UEM コンポーネントに、SNMP 監視を設定できます。<br>• BlackBerry Affinity Manager<br>• BlackBerry Cloud Connector<br>• BlackBerry Dispatcher<br>• BlackBerry MDS Connection Service<br>• BlackBerry Router<br>• BlackBerry Secure Connect Plus<br>• BlackBerry Secure Gateway<br>• BlackBerry UEM Core<br>他の BlackBerry UEM コンポーネントは、SNMP モニタリングをサポートしません。 |
| SNMP 管理ツール | 管理ツールに MIB コンパイラが含まれない場合、管理ツールをホストするコンピューターに MIB コンパイラをインストールします。<br>SNMP サービスでサーバーアクティビティのレポートにトラップメッセージを送信する場合は、管理ツールに SNMP トラップ管理ツールが含まれていることを確認します。代わりに、BlackBerry UEM をホストするコンピューターまたは別のコンピューター上にスタンドアロンの SNMP トラップ管理ツールをインストールできます。 |
| ネットワークアクセス | SNMP 管理ツールをホストするコンピューターまたはスタンドアロンの SNMP トラップ管理ツールは、BlackBerry UEM がインストールされたコンピューターにアクセスしてデータを受信できることが必要です。 |
| SNMP サービス | BlackBerry UEM がインストールされているコンピューターでは、SNMP エージェントと SNMP サービスを含む SNMP サービスをインストールします。<br>SNMP サービスは、Windows のほとんどのバージョンで利用可能です。詳細については、support.microsoft.com にアクセスしてください。 |
| SNMP サービス設定 | BlackBerry UEM がインストールされているコンピューターの Windows Services で、次の SNMP サービス設定を実行します。<br>• 有効な SNMP コミュニティ名<br>• SNMP コミュニティの最低限の読み取り専用権限<br>• SNMP サービスが SNMP データを受け付けることができるコンピューター名の IP アドレス |

# BlackBerry UEM の MIB

デフォルトでは、BlackBerry UEM の MIB は、BlackBerry UEM がインストールされたコンピューターの *<drive>*\Program Files\BlackBerry\UEM\Monitoring\bin\mib にあります。

BlackBerry UEM には次の MIB が含まれている場合があり、BlackBerry UEM コンポーネントのデータ分析に使用できます。

| MIB ファイル | 説明 |
| --- | --- |
| BES-BCCMIB-SMIV2 | BlackBerry Cloud Connector の SNMP インターフェイスの OID ツリールートの定義が含まれます。 |
| BES-BCCMonitoringMIB-SMIV2 | SNMP 管理ツールを使用してアクセスおよび取得可能な管理対象 BlackBerry Cloud Connector オブジェクトの定義が含まれます。 |
| BES-BSCPMIB-SMIV2 | BlackBerry Secure Connect Plus の SNMP インターフェイスの OID ツリールートの定義が含まれます。 |
| BES-BSCPMonitoringMIB-SMIV2 | SNMP 管理ツールを使用してアクセスおよび取得可能な管理対象 BlackBerry Secure Connect Plus オブジェクトの定義が含まれます。 |
| BES-BSGMIB-SMIV2 | BlackBerry Secure Gateway の SNMP インターフェイスの OID ツリールートの定義が含まれます。 |
| BES-BSGMonitoringMIB-SMIV2 | SNMP 管理ツールを使用してアクセスおよび取得可能な管理対象 BlackBerry Secure Gateway オブジェクトの定義が含まれます。 |
| BES-CoreEventingMIB-SMIV2 | BlackBerry UEM Core が発行するトラップと通知の定義が含まれます。 |
| BES-CoreMIB-SMIV2 | BlackBerry UEM Core の SNMP インターフェイスの OID ツリールートの定義が含まれます。 |
| BES-CoreMonitoringMIB-SMIV2 | SNMP 管理ツールを使用してアクセスおよび取得可能な管理対象オブジェクトの定義が含まれます。 |
| BES-EC-MIB-SMIV2 | 次の BlackBerry UEM のエンタープライズ接続コンポーネントが発行する管理対象オブジェクト、トラップ、および通知の定義が含まれます。<br>• BlackBerry Affinity Manager<br>• BlackBerry Dispatcher<br>• BlackBerry MDS Connection Service<br>• BlackBerry Router |

# MIB をコンパイルして SNMP 管理ツールを設定する

組織の SNMP 監視ソフトウェアを有効化して BlackBerry UEM コンポーネントを監視するには、SNMP 管理ツールを使用して BlackBerry UEM の MIB ファイルをコンパイルする必要があります。ツールに MIB コンパイラが含まれない場合、ツールをホストするコンピューターに MIB コンパイラをインストールします。

作業を始める前に： SNMP 管理ツールに関するドキュメントを読み、MIB をコンパイルするツールを使用する方法を確認します。

1. BlackBerry UEM をホストするコンピューターで、*<drive>*\Program Files\BlackBerry\UEM\Monitoring\bin\mib を参照します。
2. SNMP 管理ツール（または個別にインストールした MIB コンパイラ）を使用して .mib ファイルをコンパイルします。

# SNMP を使用したコンポーネントの監視

SNMP を使用して次のコンポーネントを監視するには、BlackBerry UEM 管理コンソールの設定を実行する必要があります。

- BlackBerry UEM Core
- BlackBerry Secure Connect Plus
- BlackBerry Secure Gateway

BlackBerry UEM Core は、デバイス管理を担当する複数のサブコンポーネントで構成されています。BlackBerry Secure Connect Plus は、BlackBerry 10 の仕事用領域アプリ、KNOX Workspace、および仕事用プロファイルを含む Android デバイスと、組織のネットワークの間にセキュリティ保護された IP トンネルを提供します。BlackBerry Secure Gateway は、BlackBerry Infrastructure を介して組織のメールサーバーに iOS デバイスを安全に接続できるようにします。

## SNMP を設定してコンポーネントを監視する

SNMP を使用して BlackBerry UEM Core、BlackBerry Secure Connect Plus、BlackBerry Secure Gateway、または BlackBerry Cloud Connector を監視するには、管理コンソールの設定を実行する必要があります。

1. メニューバーで、［設定］ > ［インフラストラクチャ］ > ［**SNMP**］をクリックします。
2. ［グローバル設定］を展開し、［**SNMP** の監視を有効化］チェックボックスをオンにします。
3. ［コミュニティ］フィールドに新しいコミュニティ名を入力してデフォルト値を置き換えます。
4. ［IP アドレス］フィールドで、トラップ管理ツールがインストールされているサーバーの IPv4 UDP アドレスを入力します。
5. ［ポート］フィールドに、トラップ管理ツールのポート番号を入力します。デフォルトでは、このポート番号は 1620 です。
6. ［保存］をクリックします。
7. 各 BlackBerry UEM インスタンス名を展開します。必要に応じて BlackBerry UEM で SNMP データ要求を待ち受けるために使用するポート番号を変更することができます。次のポート番号はデフォルトで割り当てられています。
   - BlackBerry UEM Core ：1610
   - BlackBerry Secure Connect Plus ：1611
   - BlackBerry Secure Gateway ：1612
   - BlackBerry Cloud Connector ：1613

   メモ： BlackBerry Cloud Connector のポート番号を変更するには、BlackBerry UEM データベースで、`com.rim.platform.dm.ic.ed.snmp.monitoring.udpport` の値を編集する必要があります。
8. ［保存］をクリックします。

終了したら： 次のタスクのいずれかを実行します。

- BlackBerry UEM Core の監視を有効にする場合は、Windows Services で **BlackBerry UEM - UEM Core** サービスを再起動します。
- BlackBerry Secure Connect Plus の監視を有効にする場合は、Windows Services で **BlackBerry UEM - BlackBerry Secure Connect Plus** サービスを再起動します。
- BlackBerry Secure Gateway の監視を有効にする場合は、Windows Services で **BlackBerry UEM - BlackBerry Secure Gateway** サービスを再起動します。
- BlackBerry Cloud Connector の監視を有効にする場合は、Windows Services で **BlackBerry UEM - BlackBerry Cloud Connector** サービスを再起動します。

# 用語集

| | |
|---|---|
| **ADSI** | Active Directory Service Interfaces（アクティブディレクトリサービスインターフェイス） |
| **APN** | Apple Push Notification service（Apple プッシュ通知サービス） |
| **BES5** | BlackBerry Enterprise Server 5 |
| **BES10** | BlackBerry Enterprise Service 10 |
| **BlackBerry UEM instance** | A BlackBerry UEM instance refers to one installation of the BlackBerry UEM Core and all associated BlackBerry UEM components that communicate with it. The components can be installed on the same server or multiple servers. There can be more than one BlackBerry UEM instance in a BlackBerry UEM domain. |
| **BlackBerry UEM domain** | A BlackBerry UEM domain consists of a BlackBerry UEM database and a BlackBerry Control database and any BlackBerry UEM instances that connect to them. |
| **BES12** | BlackBerry Enterprise Service 12 |
| **BES12** インスタンス | BES12 インスタンスとは、個別にインストールされるオプションのコンポーネントである BlackBerry Router を除き、1 台のコンピューター上にインストールされているすべての BES12 コンポーネントを指しています。 BES12 インスタンスは、「unit of scale（スケールユニット）」と呼ばれることもあります。 |
| **CAS** | Client Access Server（クライアントアクセスサーバー） |
| **CSR** | Certificate Signing Request（証明書署名要求） |
| **DEP** | Device Enrollment Program |
| **DNS** | Domain Name System（ドメインネームシステム） |
| **FQDN** | Fully Qualified Domain Name（完全修飾ドメイン名） |
| **HTTPS** | Hypertext Transfer Protocol over Secure Sockets Layer（HTTP に SSL によるデータ暗号化機能が付加されたプロトコル） |

| | |
|---|---|
| **IIS** | Internet Information Services（インターネットインフォメーションサービス） |
| **LDAP** | Lightweight Directory Access Protocol（TCP/IPネットワークで、ディレクトリデータベースにアクセスするためのプロトコル） |
| **MIB** | Management Information Base |
| **MMC** | Microsoft Management Console |
| **OID** | Object Identifier（オブジェクト識別子） |
| **PAC** | Proxy Auto-Configuration（プロキシ自動設定） |
| **PAP** | Push Access Protocol（プッシュアクセスプロトコル） |
| **SCEP** | Simple Certificate Enrollment Protocol |
| **SMTP** | Simple Mail Transfer Protocol（SMTP）は POP または IMAP でインターネットなどのネットワークを経由してメールを送受信するために使用される TCP/IP プロトコルです。 |
| **SNMP** | Simple Network Management Protocol（TCP/IPネットワークにおいて、ネットワークに接続された通信機器をネットワーク経由で監視/制御するためのプロトコル） |
| **SPN** | Service Principal Name（SPN）は、Microsoft Active Directory 内のユーザーまたはグループの属性で、Kerberos 対応サービスのクライアントと Kerberos 対応サービス間の相互認証をサポートします。Microsoft Active Directory アカウントには、1 つ以上の SPN を含めることができます。 |
| **SRP** | Server Routing Protocol（サーバールーティングプロトコル） |
| **SSL** | Secure Sockets Layer（セキュアソケットレイヤー） |
| **TCP** | Transmission Control Protocol（伝送制御プロトコル） |
| **TCP/IP** | Transmission Control Protocol/Internet Protocol（TCP/IP）。インターネットなどのネットワークを経由したデータの送受信に使用される通信プロトコル一式です。 |

| | |
|---|---|
| **TLS** | Transport Layer Security（トランスポートレイヤーセキュリティ） |

# 商標などに関する情報

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。

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、以下に適用されます。（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、および（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。

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、使用するために第三者の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
200 Bath Road
Slough, Berkshire SL1 3XE
United Kingdom

Published in Canada