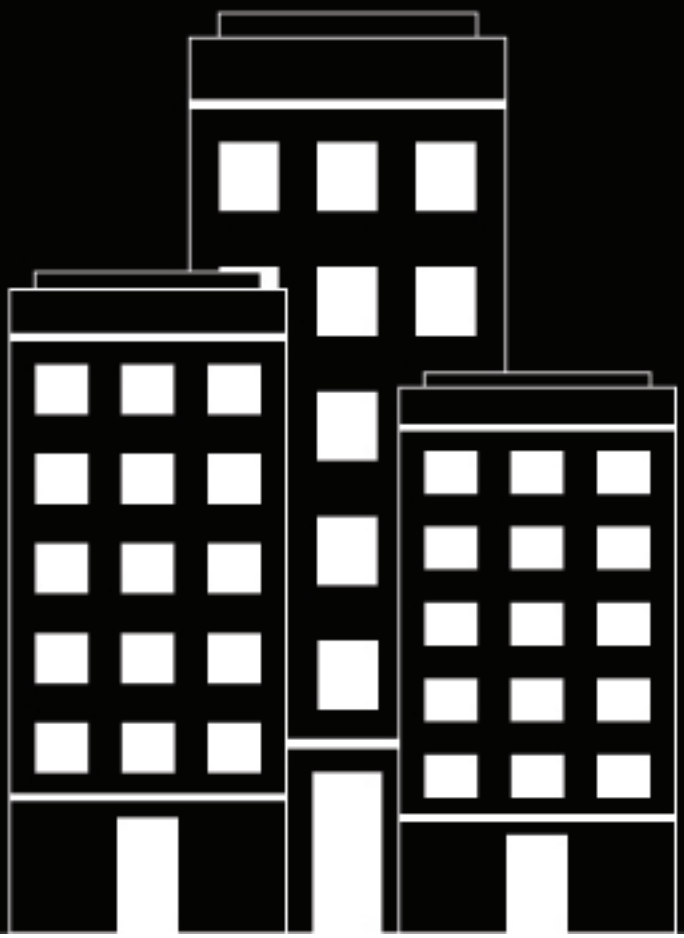

BlackBerry UEM

設定ガイド

12.19

Contents

BlackBerry UEM の設定

次の表は、このガイドで説明する初期設定タスクの概要を示しています。これらを確認して、組織のニーズに基づいて完了すべきタスクを決定します。適切なタスクを完了すると、管理者のセットアップ、ユーザーとグループの作成と管理、デバイスの制御のセットアップ、およびデバイスのアクティブ化を実行できるようになります。

このガイドの設定タスクを実行するときは、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ます。UEM を設定するために追加の管理者アカウントを作成する場合は、適切な権限レベルが付与されるように、セキュリティ管理者ロールをアカウントに割り当てる必要があります。

タスク	オンプレミス	Cloud	説明
UEM が認証に使用するデフォルトの証明書を変更	√		コンポーネントとデバイス間の通信を認証するために UEM で使用されるデフォルトの自己署名証明書を置き換えることができます。
BlackBerry Connectivity Node をインストール		√	BlackBerry Connectivity Node を UEM Cloud 環境にインストールして設定すると、オンプレミスの会社のディレクトリにアクセスし、セキュアな接続機能を有効にできます。
プロキシサーバーを介してデータを送信するよう UEM を設定	√	√	BlackBerry Infrastructure に到達する前に、プロキシサーバーを介してデータを送信するように UEM を設定できます。UEM Cloud 環境では、スタンドアロンの BlackBerry Router をインストールしてプロキシサーバーとして機能させることができます。
内部プロキシサーバーによる接続の構成	√		組織で、ネットワーク内のサーバー間の接続にプロキシサーバーを使用する場合は、サーバー側のプロキシ設定を構成し、UEM コンポーネント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。
SMTP サーバーに接続してメール通知を送信する	√		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、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。
UEM を会社のディレクトリへ接続	√	√	UEM を会社のディレクトリに接続して、ユーザーアカウントの作成、ディレクトリリンクグループの有効化、ユーザーのオンボーディングとディレクトリ同期を設定します。
UEM を Microsoft Entra ID に接続	√	√	UEM を Entra に接続して、UEM でディレクトリユーザーアカウントを作成し、Microsoft Intune によって管理される iOS および Android のアプリを展開し、Entra ID の条件付きアクセスをサポートするように UEM を設定します。

タスク	オンプレミス	Cloud	説明
APN 証明書を登録して iOS および macOS デバイスを管理	√	√	iOS および macOS のデバイスでデータを管理し、データを送信する場合は、APN 証明書を取得して登録します。
Apple Device Enrollment Program 用に UEM を設定	√	√	UEM 管理コンソールを使用して、組織が DEP 用に Apple から購入した iOS デバイスを管理できます。
Android Enterprise デバイスをサポートするように UEM を設定	√	√	Android Enterprise デバイスをサポートするには、Google Workspace 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、Google Workspace ドメインまたは Google Cloud ドメインと通信するよう UEM を設定する必要があります。
Android Management のデバイスをサポートするように UEM を設定	√	√	Android Management デバイスをサポートするには、Google Cloud コンソールで Android Management を設定し、UEM で Android Management 接続を追加します。
Chrome OS デバイスを管理するように UEM を設定	√	√	特定の Chrome OS 管理機能をサポートするように UEM を設定できます。
Windows 10 ライセンス認証を簡素化	√	√	ユーザーがサーバーアドレスを指定しないで済むように Windows 10 デバイスのアクティベーションプロセスを簡素化できます。
ソースサーバーからのユーザー、デバイス、グループ、およびその他のデータの移行	√	√	サポートされている BlackBerry サーバーからユーザー、デバイス、グループ、およびその他のデータを移行できます。
BlackBerry Dynamics アプリのネットワーク通信とプロパティを設定	√	√	BlackBerry Dynamics アプリのネットワーク通信およびその他のプロパティを設定できます。
UEM を Cisco ISE と統合	√		Cisco ISE との接続を確立し、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できます。
ダークサイト環境の UEM に対する Knox StrongSwan を使用した VPN の設定	√		UEM のダークサイト環境では、Samsung Knox デバイスが社内のサーバーおよびリソースにアクセスできるように VPN アクセスを設定する必要があります。

BlackBerry UEM が認証に使用する証明書の変更

オンプレミスの 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複数の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すでに信頼している 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。

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
Apple プロファイル署名証明書	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のある MDM プロファイルへの署名に、UEM が使用する証明書です。 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。
コンソールと BlackBerry Web サービスの SSL 証明書	管理コンソールおよび UEM Self-Service がブラウザーを認証するために使用する SSL 証明書です。 高可用性を設定する場合、証明書に UEM ドメインの名前が付いている必要があります。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 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 証明書です。 高可用性を設定する場合、証明書に UEM ドメインの名前が付いている必要があります。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 Dynamics アプリ用の SSL 証明書	BlackBerry Dynamics Launcher が UEM とのセキュリティ保護された通信チャネルを確立するのに使用する SSL 証明書です。統合された BlackBerry Dynamics Launcher を含む BlackBerry Dynamics アプリは、証明書を UEM に提示してサーバーで認証を受けることができます。
アプリケーション管理用の証明書	UEM と BlackBerry Dynamics アプリの認証に使用される SSL 証明書です。 このルート CA 証明書は、デバイス上の信頼済み CA 証明書のリストに保存されます。サーバーがデバイスで認証されると、サーバーはこの証明書を検証のためにデバイスに提示します。この証明書を変更し、UEM が証明書をすべての BlackBerry Dynamics アプリにプッシュする前に、変更が有効になる場合、証明書を受信しなかったすべてのアプリを再びアクティブ化する必要があります。

証明書	説明
Direct Connect の証明書	BlackBerry Dynamics Direct Connect 用に設定された BlackBerry Proxy サーバーとデバイス上の BlackBerry Dynamics アプリ間の認証に使用される SSL 証明書です。 この証明書を更新すると、新しいバージョンは常に非 BlackBerry Dynamics Direct Connect 接続経由でデバイスに送信されます。変更時にオンラインになっていないデバイスまたはコンテナは、オンラインに戻ったときに更新を受け取ります。この証明書の更新は、UEM サーバーと、適用可能なネットワークアプライアンスで同時に行う必要があります。 Direct Connect の設定の詳細については、「BlackBerry UEM での Direct Connect の設定」を参照してください。
BlackBerry Dynamics サーバーの証明書	UEM と BlackBerry Proxy の間の接続を認証する SSL 証明書です。

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、次の考慮事項を確認してください。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 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。

注意事項	詳細
周辺機器に新しい証明書を追加する	BlackBerry Dynamics 証明書をネットワーク上の周辺機器に追加している場合、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 アプリの最新バージョンを使用する	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、その前にユーザーが BlackBerry Dynamics アプリの最新バージョンを使用していることを確認します。
証明書を受信するには、BlackBerry Dynamics アプリを開く必要がある	アプリで UEM から証明書を受信するには、ユーザーがデバイスで 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、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 が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、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。

注意事項	詳細
証明書の変更をスケジュールする	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。

BlackBerry UEM 証明書の変更

作業を始める前に：

- BlackBerry Dynamics 証明書の変更に関する考慮事項 を確認します。
- 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）である必要があり、TripleDES-SHA1 暗号化タイプで暗号化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］ > ［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. ［サーバー証明書］タブまたは［**BlackBerry Dynamics** 証明書］タブの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. ［参照］をクリックします。証明書ファイルに移動して選択します。
5. ［暗号化パスワード］または［パスワード］フィールドに新しいパスワードを入力します。
6. ［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 UEM Core サービスを再起動します。
- 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。
- 信頼する必要がない自己署名証明書は、BlackBerry Dynamics 証明書タブで、［**BlackBerry UEM CA** を信頼する］チェックボックスおよび［**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 Connectivity Node のインストールと組織のファイアウォール内にあるリソースへの接続

BlackBerry Connectivity Node は、専用コンピューターにインストールして BlackBerry UEM Cloud の追加的な機能を有効にできるコンポーネントのコレクションです。BlackBerry Connectivity Node には、次のコンポーネントが含まれています。

コンポーネント	目的
BlackBerry Cloud Connector	BlackBerry Cloud Connector を使用すると、UEM Cloud はオンプレミス環境にある会社のディレクトリにアクセスできるようになります。会社のディレクトリを検索して、ユーザーデータをインポートすることで、UEM にディレクトリユーザーアカウントを作成できます。ユーザーデータは、設定したスケジュールでディレクトリと同期されます。 SCEP を使用する場合、UEM Cloud は会社のディレクトリにアクセスできる必要があります。 ディレクトリユーザーは、ディレクトリの資格情報を使用して BlackBerry UEM Self-Service にアクセスできます。ディレクトリユーザーに管理ロールを割り当てた場合、ユーザーはディレクトリの資格情報を使用して管理コンソールにログインすることもできます。 また、BlackBerry Cloud Connector により、PKI コネクタは BlackBerry Dynamics アプリに証明書を送信することもできます。
BlackBerry Proxy	BlackBerry Proxy は組織と BlackBerry Dynamics NOC の間で接続を維持します。この接続により、BlackBerry Dynamics アプリは、ファイアウォール内にある組織のリソースと安全に通信できます。また BlackBerry Dynamics Direct Connect もサポートされているため、アプリデータの転送で BlackBerry Dynamics NOC をバイパスすることができます。詳細については、「BlackBerry Dynamics アプリのネットワーク通信とプロパティの設定」を参照してください。
BlackBerry Secure Connect Plus	BlackBerry Secure Connect Plus では、組織のファイアウォール内の仕事用リソースにアクセスするときに、標準のプロトコルとエンドツーエンドの暗号化を使用して、データのセキュリティを確保できます。詳細については、「仕事用リソースへの接続のための BlackBerry Secure Connect Plus の使用」を参照してください。
BlackBerry Secure Gateway	BlackBerry Secure Gateway は、MDM 制御 アクティベーションタイプを使用している iOS デバイスに、組織のメールサーバーへのセキュリティ保護された接続を BlackBerry Infrastructure 経由で提供します。詳細については、「BlackBerry Secure Gateway を使用して iOS デバイスに送信されたメールデータを保護する」を参照してください。

コンポーネント	目的
BlackBerry Gatekeeping Service	BlackBerry Gatekeeping Service では、Exchange ActiveSync にアクセス可能なデバイスを簡単に制御できます。詳細については、「Exchange ActiveSync にアクセス可能なデバイスの制御」を参照してください。

BlackBerry Connectivity Node のインストールファイルおよびアクティベーションファイルは、UEM 管理コンソールで入手できます。これらのファイルを使用して、BlackBerry Connectivity Node の新しいインスタンスをインストールしたり、既存のインスタンスをアップグレードしたりできます。

BlackBerry Connectivity Node をインストールしてアクティブ化する手順

BlackBerry Connectivity Node のインスタンスは、1 つインストールすることも、冗長性を持たせるために複数インストールすることもできます。

手順	アクション
1	BlackBerry Connectivity Node をインストールするための要件と考慮事項を確認します。
2	BlackBerry Connectivity Node のインストールおよび設定。
3	オプションで、地域接続を管理するサーバーグループの作成。
4	BlackBerry Secure Connect Plus、BlackBerry Secure Gateway、BlackBerry GateKeeping Service、および BlackBerry Dynamics アプリの追加設定を実行します。

要件：**BlackBerry Connectivity Node**

項目	要件または考慮事項
ハードウェア	日常業務に使用されているコンピューターではなく、技術的な目的で確保されている専用コンピューターに BlackBerry Connectivity Node をインストールします。コンピューターは、インターネットと会社のディレクトリにアクセスできる必要があります。すでにオンプレミスの BlackBerry UEM インスタンスをホストしているコンピューターには、BlackBerry Connectivity Node をインストールできません。 BlackBerry Connectivity Node のインスタンスは、1 つインストールすることも、冗長性を持たせるために複数インストールすることもできます。インスタンスはそれぞれ専用のコンピューターにインストールする必要があります。 BlackBerry Connectivity Node をホストするコンピューターは、次の要件を満たす必要があります。 • 6 プロセッサコア、E5-2670（2.6 GHz）、E5-2683 v4（2.1 GHz）、または同等 • 12 GB の利用可能なメモリ • 64 GB のディスク領域
シングルサービスパフォーマンスモード	必要に応じて、サーバーグループ内の各 BlackBerry Connectivity Node を指定して、単一の接続タイプ（BlackBerry Secure Connect Plus のみ、BlackBerry Secure Gateway のみ、または BlackBerry Proxy のみ）を処理できます。これにより、リソースが解放され、同じ数のユーザーまたはコンテナに必要なサーバーの数を減らすことができます。シングルサービスパフォーマンスモードが有効になっている各 BlackBerry Connectivity Node は、最大 10,000 台のデバイスをサポートできます。 BlackBerry Connectivity Node のシングルサービスパフォーマンスモードを有効にする場合は、上記のハードウェア要件は次のように調整されます。 • BlackBerry Secure Connect Plus のみ：4 プロセッサコア、E5-2670（2.6 GHz）、E5-2683 v4（2.1 GHz）、または同等 • BlackBerry Secure Gateway のみ：8 プロセッサコア、E5-2670（2.6 GHz）、E5-2683 v4（2.1 GHz）、または同等 • BlackBerry Proxy のみ：変更はありません。
拡張性と高可用性	各 BlackBerry Connectivity Node は最大 5,000 台のデバイスをサポートできます。インスタンスを追加でインストールすると、最大 50,000 台のデバイスをサポートできます。 サーバーグループに複数の BlackBerry Connectivity Node を導入すると、高可用性とロードバランシングを実現できます。

項目	要件または考慮事項
ソフトウェア	BlackBerry Connectivity Node インスタンスをホストするコンピューターは、次の要件を満たす必要があります。 • サポートされる OS • Windows PowerShell 2.0 以降が、BlackBerry Secure Connect Plus および BlackBerry Gatekeeping Service の RRAS をインストールするセットアップアプリケーションに必要です。 • 必要なバージョンの JRE をインストールし、BB_JAVA_HOME 変数を設定します。詳細については、「Java の場所の環境変数の設定」を参照してください。
ディレクトリ接続	サポートされているディレクトリサービスを使用していることを確認します。 1 つ以上のディレクトリ接続を設定できますが、複数の BlackBerry Connectivity Node インスタンスがある場合は、すべてのディレクトリ接続を同じように設定する必要があります。1 つのディレクトリ接続が見つからないか、または正しく設定されていない場合、BlackBerry Connectivity Node は管理コンソールに無効と表示されます。
ポート	BlackBerry Connectivity Node コンポーネントおよび関連するプロキシサーバーが BlackBerry Infrastructure と通信できるように、次のアウトバウンドポートが組織のファイアウォールで開いていることを確認します。 • BlackBerry Connectivity Node をアクティブ化する場合は 443（HTTPS） • その他のすべてのアウトバウンド接続の場合は 3101（TCP）
管理者アカウント	BlackBerry Connectivity Node をインストールして設定する場合は、次の要件を満たす管理者アカウントを使用します。 • コンピューターでソフトウェアをインストールして設定する権限がある Windows アカウントを使用します。 • 設定するディレクトリ接続ごとに、読み取り権限を持つディレクトリアカウントを選択します。 • BlackBerry Connectivity Node のインストールファイルおよびアクティベーションファイルをダウンロードする権限を持つ UEM Cloud 管理者アカウント（セキュリティ管理者など）を使用します。

BlackBerry Connectivity Node のインストールおよび設定

作業を始める前に：

- BlackBerry Connectivity Node をインストールするための要件と考慮事項を確認します。
- 管理コンソールのメニューバーで、［設定］ > ［外部統合］ > ［**BlackBerry Connectivity Node** のセットアップ］をクリックします。 をクリックし、BlackBerry Connectivity Node のセットアップアプリケーションをダウンロードします。BlackBerry Connectivity Node インスタンスをアクティブにするときに、既存のサーバーグループに追加する場合は、［サーバーグループ］ドロップダウンリストで、適切なサーバーグループ

をクリックします。アクティベーションファイルを生成して保存します。アクティベーションファイルは 60 分間有効です。

- BlackBerry Connectivity Node インスタンスをホストするコンピューターにセットアップアプリケーションとアクティベーションファイルを転送します。そのコンピューターで以下の手順を完了します。

1. BlackBerry Connectivity Node セットアップアプリケーションを実行します。
2. 言語を選択します。［**OK**］をクリックします。
3. ［次へ］をクリックします。
4. 国または地域を選択します。使用許諾契約書を読んで、承諾します。［次へ］をクリックします。
5. インストールプログラムは、コンピューターがインストール要件を満たしていることを確認します。［次へ］をクリックします。
6. インストールのファイルパスを変更するには、［**...**］をクリックして、使用するファイルパスに移動します。［インストール］をクリックします。
7. インストールが完了したら、［次へ］をクリックします。

   BlackBerry Connectivity Node コンソールのアドレスが表示されます（http:/localhost:8088）。リンクをクリックし、サイトをブラウザーに保存します。
8. 言語を選択します。［次へ］をクリックします。
9. BlackBerry Connectivity Node をアクティブ化すると、ポート 443（HTTPS）を介してデータが BlackBerry Infrastructure に送信されます（na.bbsecure.com または eu.bbsecure.com など）。BlackBerry Connectivity Node はアクティブ化されると、BlackBerry Infrastructure を経由する他のすべてのアウトバウンド接続にポート 3101（TCP）を使用します。組織のファイアウォールの内側にある既存のプロキシサーバー経由で BlackBerry Connectivity Node からデータを送信する場合は、［ここをクリックして組織の環境にプロキシを設定］をクリックして［プロキシサーバー］オプションを選択し、次のいずれかを実行します。
   - アクティベーションデータをプロキシサーバー経由で送信するには、［プロキシの登録］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。プロキシサーバーは、ポート 443 を介して、データを bbsecure.com に送信できる必要があります。［保存］をクリックします。
   - BlackBerry Connectivity Node のコンポーネントから他のアウトバウンド接続をプロキシサーバー経由で送信するには、該当するフィールドに、プロキシサーバーの FQDN または IP アドレスとポート番号を入力します。プロキシサーバーは、ポート 3101 を介してデータを bbsecure.com に送信できる必要があります。［保存］をクリックします。
10. ［登録名］フィールドに、BlackBerry Connectivity Node の名前を入力します。［次へ］をクリックします。
11. ［参照］をクリックします。アクティベーションプロファイルを選択します。
12. ［アクティブにする］をクリックします。

    BlackBerry Connectivity Node インスタンスをアクティブにするときに既存のサーバーグループに追加するには、組織のファイアウォールが、BlackBerry Connectivity Node をアクティブ化するために、BlackBerry Infrastructure を介してポート 443 経由で、またメイン BlackBerry Connectivity Node インスタンスとして同じ bbsecure.com 領域へ、そのサーバーからの接続を許可する必要があります。
13. ＋ をクリックして、設定する会社のディレクトリのタイプを選択します。
14. 組織のディレクトリタイプについては、次の手順に従います。

ディレクトリのタイプ	手順
Microsoft Active Directory	**a.** ［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。Microsoft Entra ID ディレクトリが設定されている場合、この接続名は Entra ディレクトリ接続の名前と異なる必要があります。 **b.** ［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。 **c.** ［ドメイン］フィールドに、Microsoft Active Directory をホストするドメインの FQDN を入力します。たとえば、domain.example.com などです。 **d.** ［パスワード］フィールドに、Microsoft Active Directory アカウントのパスワードを入力します。 **e.** ［ドメインコントローラー検出］ドロップダウンリストで、次のいずれかをクリックします。 • 自動検出を使用する場合は、［自動］をクリックします。 • ドメインコントローラーコンピューターを指定する場合は、［以下のリストから選択］をクリックします。＋をクリックして、コンピューターの FQDN を入力します。さらにコンピューターを追加するには、この手順を繰り返します。 **f.** ［グローバルカタログ検索ベース］フィールドに、アクセスする検索ベースを入力します（たとえば、OU=Users,DC=example,DC=com）。グローバルカタログ全体を検索するには、フィールドを空白にしておきます。 **g.** ［グローバルカタログ検出］ドロップダウンリストで、次のいずれかをクリックします。 • 自動カタログ検出を使用する場合は、［自動］をクリックします。 • カタログコンピューターを指定する場合は、［以下のリストから選択］をクリックします。＋をクリックして、コンピューターの FQDN を入力します。必要に応じてこの手順を繰り返して、さらにコンピューターを指定します。 **h.** 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。 Microsoft Active Directory でアクセスするフォレストごとに UEM Cloud 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。フォレスト名、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どのドメインにも属することができます）、ユーザー名、およびパスワードを指定します。 **i.** 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。 **j.** ［保存］をクリックします。

ディレクトリのタイプ	手順
LDAP ディレクトリ	**a.** ［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。Microsoft Entra ID ディレクトリが設定されている場合、この接続名は Entra ディレクトリ接続の名前と異なる必要があります。 **b.** ［**LDAP** サーバー検出］ドロップダウンリストで、次のいずれかをクリックします。 • 自動検出を使用する場合は、［自動］をクリックします。［**DNS** ドメイン名］フィールドに、DNS ドメイン名を入力します。 • LDAP コンピューターを指定する場合は、［以下のリストからサーバーを選択］をクリックします。＋をクリックして、コンピューターの FQDN を入力します。さらにコンピューターを追加するには、この手順を繰り返します。 **c.** ［**SSL** を有効にする］ドロップダウンリストで、LDAP トラフィックに対して SSL 認証を有効にするかどうかを選択します。［はい］をクリックした場合は、［参照］をクリックして LDAP コンピューターの SSL 証明書を選択します。 **d.** ［**LDAP** ポート］フィールドに、LDAP コンピューターのポート番号を入力します。 **e.** ［認証が必須］ドロップダウンリストで、UEM Cloud が LDAP コンピューターで認証する必要があるかどうかを選択します。［はい］をクリックする場合は、LDAP アカウントのユーザー名とパスワードを入力します。ユーザー名は DN 形式（たとえば、CN=Megan Ball,OU=Sales,DC=example,DC=com）にする必要があります。 **f.** ［検索ベース］フィールドに、アクセスする検索ベースを入力します（たとえば、OU=Users,DC=example,DC=com）。 **g.** ［**LDAP** ユーザー検索フィルター］フィールドに、LDAP ユーザーに対して使用するフィルターを入力します。たとえば、(&(objectCategory=person)(objectclass=user)(memberOf=CN=Local,OU=Users,DC=example,DC=com))。 **h.** ［**LDAP** ユーザー検索範囲］ドロップダウンリストで、次のいずれかをクリックします。 • ベース DN の下にあるすべてのレベルにユーザー検索を適用する場合は、［すべてのレベル］をクリックします。 • ベース DN の 1 レベル下にユーザー検索を制限する場合は、［**1** レベル］をクリックします。 **i.** ［固有 **ID**］フィールドに、各ユーザーの固有 ID の属性を入力します（たとえば、uid）。この属性は、全ユーザーに対して、不変でグローバルに固有であることが必要です。 **j.** ［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）。 **k.** ［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）。 **l.** ［ログイン属性］フィールドに、各ユーザーのログイン属性を入力します（たとえば、cn）。この属性は、ディレクトリ資格情報で BlackBerry UEM Self-Service にログインするために、ユーザーが入力する値として使用されます。 **m.** ［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（mail など）。 **n.** ［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）。 **o.** 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、名とオフィスの電話番号が含まれます。

15. 管理コンソールで、［設定］ > ［外部統合］ > ［**BlackBerry Connectivity Node** のセットアップ］をクリックします。
16. 手順 4：［テスト接続］セクションで［次へ］をクリックします。

BlackBerry Connectivity Node インスタンスのステータスを表示するには、管理コンソールのメニューバーで、［設定］ > ［外部統合］ > ［**BlackBerry Connectivity Node** のステータス］をクリックします。

終了したら：

- 追加の BlackBerry Connectivity Node インスタンスをインストールするには、インストールファイルおよびアクティベーションファイルを再度ダウンロードし、別のコンピューターでこのタスクを繰り返します。この操作は、1 つ目のインスタンスのアクティベーションが完了した後に行う必要があります。
- 複数の BlackBerry Connectivity Node をインストールする場合は、各インスタンスに同じディレクトリ接続を設定する必要があります。BlackBerry Connectivity Node コンソールを使用して、インスタンス（.txt ファイル）のディレクトリ接続をエクスポートし、そのインスタンスのコンソールを使用してそれらの接続を別の BlackBerry Connectivity Node に転送してインポートできます。ディレクトリ設定をインポートする前に、インスタンスから既存のディレクトリ接続をすべて削除します。
- オプションで、地域接続を管理するサーバーグループの作成。
- BlackBerry Dynamics NOC に到達する前に HTTP プロキシ経由でデータを送信する場合は、BlackBerry Connectivity Node コンソールで［一般設定］ > ［**BlackBerry Router** とプロキシ］をクリックします。［**HTTP** プロキシを有効にする］チェックボックスをオンにして、プロキシを設定します。
- BlackBerry Connectivity Node インスタンスのデフォルト設定を変更する場合は、管理コンソールのメニューバーで、［設定］ > ［外部統合］ > ［**BlackBerry Connectivity Node** のセットアップ］をクリックし、 をクリックします。ロギング設定の変更、BlackBerry Gatekeeping Service のインスタンスの無効化、および BlackBerry Secure Gateway 設定を行うことができます。
- BlackBerry Connectivity Node への更新が通知されたら、このタスクを繰り返して各インスタンスをアップグレードします。BlackBerry Connectivity Node コンソールを使用して、ディレクトリ設定を記録またはエクスポートします。BlackBerry Connectivity Node のインスタンスはすべて同じバージョンへアップグレードする必要があります。最初のインスタンスをアップグレードすると、すべてのノードが同じバージョンにアップグレードされるまで、ディレクトリサービスは無効になります。
- BlackBerry Secure Connect Plus の有効化手順の詳細については、管理関連の資料の「仕事用リソースへの接続のための BlackBerry Secure Connect Plus の使用」を参照してください。
- BlackBerry Secure Gateway の有効化手順 については、管理関連の資料の「BlackBerry Secure Gateway を使用して iOS デバイスに送信されたメールデータを保護する」を参照してください。
- BlackBerry Gatekeeping Service の設定手順については、管理関連の資料の「Exchange ActiveSync にアクセス可能なデバイスの制御」を参照してください。

地域接続を管理するサーバーグループの作成

BlackBerry Connectivity Node で利用できるエンタープライズ接続機能の地域接続を管理する場合は、専用地域にある BlackBerry Connectivity Node の複数のインスタンスを 1 つのサーバーグループとして展開できます。サーバーグループを作成するときに、コンポーネントを BlackBerry Infrastructure に接続するのに使用する地域データパスを指定します。サーバーグループは、BlackBerry Connectivity Node インスタンスの冗長性、高可用性、およびロードバランシングもサポートします。

作業を始める前に： BlackBerry Connectivity Node の複数のインスタンスをインストールして設定します。

1. 管理コンソールのメニューバーで、［設定］ > ［外部統合］ > ［**BlackBerry Connectivity Node** のセットアップ］をクリックします。

2. をクリックします。
3. サーバーグループの名前と説明を入力します。
4. ［国］ドロップダウンリストで、該当する国を選択します。
5. サーバーグループでインスタンスの会社のディレクト接続を無効にするには、［ディレクトリサービス設定を上書きする］チェックボックスをオンにします。
6. デフォルトでは、各 BlackBerry Gatekeeping Service インスタンスの BlackBerry Connectivity Node はアクティブです。ゲートキーピングデータをメイン BlackBerry Connectivity Node インスタンスのみで管理する場合は、［**BlackBerry Gatekeeping Service** 設定を上書きする］チェックボックスをオンにして、サーバーグループ内の各 BlackBerry Gatekeeping Service を無効にします。
7. デフォルト設定（［設定］ > ［インフラストラクチャ］ > ［BlackBerry Secure Connect Plus］）と異なる BlackBerry Secure Connect Plus の DNS 設定を使用する場合は、［**DNS** 設定を上書きする］チェックボックスをオンにします。次の手順に従います。
   a) ［**DNS** サーバー］セクションで ＋ をクリックします。ドット付き 10 進法（例：192.0.2.0）で DNS サーバーアドレスを指定します。［追加］をクリックします。必要に応じて繰り返します。
   b) ［**DNS** 検索サフィックス］セクションで ＋ をクリックします。DNS 検索サフィックス（例：domain.com）を入力します。［追加］をクリックします。必要に応じて繰り返します。
8. サーバーグループの BlackBerry Connectivity Node インスタンスのログ設定を実行する場合は、［ロギング設定を上書きする］チェックボックスをオンにします。次の操作のいずれかを実行します。
   - ［サーバーログのデバッグレベル］ドロップダウンリストで、適切なログレベルを選択します。
   - ログイベントを syslog サーバーにルーティングする場合は、［**Syslog**］チェックボックスを選択し、syslog サーバーのホスト名とポートを指定します。
   - ローカルログ設定を変更する場合は、［ローカルのファイル保存先を有効にする］チェックボックスをオンにします。サイズ制限（MB 単位）、経過時間制限（日数単位）を指定し、ログフォルダーを圧縮するかどうかを選択します。
   - BlackBerry Connectivity Node コンポーネントに異なるログレベルを設定する場合は、［サービスログの上書き］セクションで ＋ をクリックして、適切なコンポーネントとログレベルを選択します。必要に応じて繰り返します。
9. 1 つの接続タイプのみにサーバーグループのインスタンスを使用する場合は、［シングルサービスパフォーマンスモードを有効にする］チェックボックスをオンにします。［接続タイプ］ドロップダウンメニューで、接続タイプ（BlackBerry Secure Connect Plus のみ、BlackBerry Secure Gateway のみ、または BlackBerry Proxy のみ）を選択します。
10. サーバーグループのインスタンスの BlackBerry Secure Gateway 設定を指定する場合は、［**BlackBerry Secure Gateway** 設定を上書きする］チェックボックスをオンにします。モダン認証を使用して Microsoft Exchange Online に接続する iOS デバイスの場合、検出エンドポイントとメールサーバーリソースを指定します。
    a) ［メールサーバー認証の **OAuth** を有効にする］ チェックボックスをオンにします。
    b) ［検出エンドポイント］フィールドで、検出要求に使用する URL を指定します。検出エンドポイントを、https://<*identity provider*>/.well-known/openid-configuration の形式（たとえば、`https://login.microsoftonline.com/common/.well-known/openid-configuration` や `https://login.windows.net/common/.well-known/openid-configuration`）で入力します。
    c) ［メールサーバーリソース］フィールドで、OAuth を使用した認可およびトークン要求に使用するメールサーバーリソースの URL を指定しますたとえば、`https://outlook.office365.com` などです。
11. ［保存］をクリックします。

終了したら： サーバーグループを選択し、 をクリックして BlackBerry Connectivity Node インスタンスを追加します。サーバーグループのインスタンスはいつでも追加したり削除したりできます。

トラブルシューティング：BlackBerry Connectivity Node

問題	解決策
BlackBerry Connectivity Node が UEM Cloud でアクティブ化されない	• 管理コンソールで生成した最新のアクティベーションファイルをアップロードしたことを確認してください。最新のアクティベーションファイルのみが有効です。 • アクティベーションファイルの有効期限は 60 分です。新しいアクティベーションファイルを生成してアップロードし、もう一度アクティベーションを実行します。 • 「KB 38964」を参照してください。

BlackBerry Connectivity Node を UEM Cloud に接続できない	• BlackBerry Connectivity Node コンポーネント（および関連するプロキシサーバー）が BlackBerry Infrastructure （*region*.bbsecure.com）と通信できるように、次のアウトバウンドポートが組織のファイアウォールで開いていることを確認します。
	  • BlackBerry Connectivity Node をアクティブ化する場合は 443（HTTPS）
	  • その他のすべてのアウトバウンド接続の場合は 3101（TCP）
	• BlackBerry Connectivity Node が UEM Cloud と接続できない理由の詳細については、最新のログファイルを参照してください。ログファイルは、デフォルトでは *<drive:>*:\Program Files\BlackBerry Cloud Connector\logs にあります。

BlackBerry Connectivity Node を会社のディレクトリに接続できない	• BlackBerry Connectivity Node のインスタンスが複数ある場合は、すべて同じバージョンであることを確認します。 • 会社のディレクトリに対して正しい設定を指定したことを確認してください。 • すべてのインスタンスにディレクトリ接続があり、それらがすべてのインスタンスで同じように設定されていることを確認します。 • ディレクトリアカウントに対して正しいログイン情報を指定したこと、および会社のディレクトリにアクセスできる十分な権限がアカウントにあることを確認してください。 • 組織のファイアウォールで正しいポートが開いていることを確認します。 • 2 つの異なるインストールに同じアクティベーションファイルを使用していなかったことを確認します。 • 最新のアクティベーションファイルを使用していることを確認します。 • BlackBerry Connectivity Node が会社のディレクトリにアクセスできない理由の詳細については、最新のログファイルを参照してください。ログファイルは、デフォルトでは *<drive:>*:\Program Files\BlackBerry Cloud Connector\logs にあります。 • Microsoft Active Directory を使用している場合は、「KB 36955」を参照してください。

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

BlackBerry UEM 環境では、次のプロキシ設定を使用できます。

環境	プロキシオプション
オンプレミスの UEM	UEM に到達する前に、TCP プロキシサーバーを介してデータを送信するように BlackBerry Infrastructure を設定できます。 デフォルトでは、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、TCP プロキシサーバーをインストールできます。TCP プロキシサーバーは、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プロキシサーバーをインストールできます。DMZ に TCP プロキシサーバーをインストールすると、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。プロキシサーバーのみがファイアウォールの外側から UEM に接続します。UEM とデバイスの間の BlackBerry Infrastructure へのすべての接続は、プロキシサーバーを通過します。
UEM Cloud	BlackBerry Connectivity Node でプロキシサーバーを使用するには、BlackBerry Router をインストールしてプロキシサーバーとして機能させることができます。または、組織の環境内にインストール済みの TCP プロキシサーバーを使用することもできます。 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、セキュリティレベルを一段引き上げることができます。ファイアウォールの外側から BlackBerry Connectivity Node に接続するのは BlackBerry Router またはプロキシサーバーのみです。BlackBerry Connectivity Node とデバイスの間の BlackBerry Infrastructure へのすべての接続は、プロキシサーバーを通過します。 デフォルトでは、BlackBerry Connectivity Node 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 Connectivity Node と BlackBerry Infrastructure の間の仲介として動作します。

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

オンプレミスの UEM 環境では、BlackBerry UEM Core サービスの透過型 TCP プロキシサーバーを設定できます。こ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。

UEM Cloud 環境では、BlackBerry Connectivity Node はポート 443（HTTPS）経由でアクティベーションデータを送信します。アクティベーション後、BlackBerry Connectivity Node はデータをポート 3101（TCP）で送受信します。BlackBerry Connectivity Node を設定して、組織のファイアウォール内のプロキシサーバーを介して、HTTPS または TCP データをルーティングできます。BlackBerry Connectivity Node はプロキシサーバーでの認証をサポートしません。

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、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。

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 UEM ドメインにインストールします。

1. 使用環境に応じた手順に従ってください。

環境	手順
オンプレミスの UEM	a. 管理コンソールのメニューバーで、［設定］ > ［インフラストラクチャ］ > ［**BlackBerry Router** とプロキシ］をクリックします。 b. ［グローバル設定］で、［プロキシサーバー］を選択します。 c. プロキシサーバーを使用する各サービスについて、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指定します。各フィールドには 1 つの値が必要です。
UEM Cloud	a. BlackBerry Connectivity Node コンソール（http:/localhost:8088）で、［一般設定］ > ［プロキシ］をクリックします。 b. ［プロキシサーバー］を選択します。 c. BlackBerry Connectivity Node への HTTPS のアクティベーションデータをプロキシサーバー経由でルーティングする場合は、［プロキシの登録］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。プロキシサーバーは、ポート 443 を介してデータを *<region>*.bbsecure.com に送信できる必要があります。 d. BlackBerry Connectivity Node のコンポーネントからのアウトバウンド接続をプロキシサーバー経由でルーティングする場合は、該当するフィールドに、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。プロキシサーバーは、ポート 3101 を介してデータを *<region>*.bbsecure.com に送信できる必要があります。

2. ［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 UEM ドメインにインストールします。

1. 次の操作のいずれかを実行します。
   - オンプレミスの UEM 環境では、管理コンソールのメニューバーで、［設定］ > ［インフラストラクチャ］ > ［**BlackBerry Router** とプロキシ］をクリックします。
   - UEM Cloud 環境では、BlackBerry Connectivity Node コンソール（http:/localhost:8088）で、［一般設定］ > ［プロキシ］をクリックします。
2. ［プロキシサーバー］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 2〜6 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。

スタンドアロンの BlackBerry Router の UEM Cloud 環境へのインストール

BlackBerry Router はオプションのコンポーネントで、組織のファイアウォール外の DMZ にインストールできます。BlackBerry Router はインターネットに接続し、BlackBerry Connectivity Node と BlackBerry Infrastructure を使用するデバイスとの間でデータを送信します。BlackBerry Router はプロキシサーバーとして機能し、SOCKS v5（認証なし）をサポートできます。

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。デフォルトでは、BlackBerry Connectivity Node はポート 3102 を使用して BlackBerry Router に接続します。BlackBerry Router は、BlackBerry Connectivity Node コンポーネント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。

作業を始める前に：

- スタンドアロンの BlackBerry Router を BlackBerry Connectivity Node のインスタンスをホストしないコンピューターにインストールする必要があります。
- SRP ホスト名を確認します。通常、SRP ホスト名は *<country code>*.srp.blackberry.com です（*us*.srp.blackberry.com など）。

1. UEM 管理コンソールのメニューバーで、［設定］ > ［外部統合］ > ［**BlackBerry Connectivity Node** のセットアップ］をクリックします。
2. をクリックします。
3. ［ダウンロード］をクリックします。

4. ソフトウェアダウンロードのページで、必要な質問に回答して［ダウンロード］をクリックします。インストールパッケージを保存して展開します。
5. ［ルーター］フォルダーで **setupinstaller.zip** ファイルを解凍します。この .zip ファイル内の **Installer** フォルダーには、BlackBerry Router をインストールするために使用する **Setup.exe** ファイルが格納されています。
6. **Setup.exe** ファイルを、BlackBerry Router をインストールするコンピューターに転送し、ダブルクリックしてセットアップアプリケーションを実行します。

   インストールはバックグラウンドで実行され、ダイアログボックスが表示されません。インストールが完了すると、BlackBerry Router サービスがサービスウィンドウに表示されます。
7. BlackBerry Connectivity Node コンソール（http:/localhost:8088）で、［一般設定］ **>** ［プロキシ］をクリックします。
8. ［**BlackBerry Router**］を選択します。
9. ＋をクリックします。
10. 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。
11. ［追加］をクリックします。
12. ［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。
13. ［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

組織が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している場合は、次のようにオンプレミスの BlackBerry UEM 環境を設定する必要があります。

- UEM Core が別のコンピューターにインストールされている場合は、管理コンソールと通信できるようにします。
- 認証機関や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、UEM が他の内部サービスと通信できるようにします。

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。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、「プロキシサーバーを介してデータを送信する BlackBerry UEM の設定」を参照してください。

1. 管理コンソールのメニューバーで、［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. 次の操作のいずれかを実行します。

タスク	手順
UEM ドメインのほとんどまたはすべてのサーバーのグローバルプロキシを設定する	**a.** ［グローバルサーバー側のプロキシ設定］を展開します。 **b.** ［種類］ドロップダウンリストで、［**PAC** 設定］または［手動設定］をクリックします。 **c.** 必須フィールドに入力します。 **d.** ［保存］をクリックします。
グローバルプロキシ設定とは異なる 1 つまたは複数のサーバーのプロキシを設定する	**a.** サーバー名を展開します。 **b.** ［種類］ドロップダウンリストで、［なし］、［**PAC** 設定］、または［手動設定］をクリックします。 **c.** 必須フィールドに入力します。 **d.** ［保存］をクリックします。

メール通知を送信するための SMTP サーバーへの接続

オンプレミスの BlackBerry UEM を SMTP サーバーに接続して、アクティベーション手順、デバイスコンプライアンスの警告、UEM Self-Service のパスワード、およびメール通知をデバイスユーザーに送信できるように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］ > ［外部統合］ > ［**SMTP** サーバー］の順にクリックします。
2. をクリックします。
3. ［送信者の表示名］フィールドに、UEM からのメール通知に使用する名前を入力します（`donotreply` や `UEM Admin` など）。
4. ［送信者アドレス］フィールドに、メール通知の送信に UEM で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
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］ドロップダウンリストで、適切な暗号化の種類を選択します。
8. SMTP サーバーが認証を必要とする場合は、ユーザー名とパスワードを指定します。
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 証明書ファイルに移動して選択し、［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。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。

会社のディレクトリに接続する

BlackBerry UEM を組織の会社のディレクトリに接続して、次の機能を活用できます。

- ディレクトリからユーザーデータを使用して UEM にユーザーアカウントを作成でき、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 UEM グループにリンクして、会社のディレクトリと同じ方法でユーザーを整理し、ユーザーの IT ポリシー、プロファイル、アプリの割り当てと管理を簡素化できます。これらはディレクトリにリンクされているグループと呼ばれます。
- 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、UEM ユーザーを自動的に作成することができます。これらはオンボーディングディレクトリグループと呼ばれます。これらのディレクトリグループに新しいユーザーを追加すると、UEM でこれらのユーザーの新しいユーザーアカウントが作成されます。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で無効化または削除されたときに、デバイスデータおよび UEM 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。

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。

手順	アクション
1	オンプレミスの UEM 環境で、「Microsoft Active Directory インスタンスに接続する」または「LDAP ディレクトリに接続する」を行います。 UEM Cloud 環境で、BlackBerry Connectivity Node をインストールして設定し、会社のディレクトリに接続します。 オンプレミスの UEM または UEM Cloud を Entra ID に接続する手順については、「BlackBerry UEM の Microsoft Entra ID への接続」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する。
3	オプションで、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。
4	必要に応じて、ディレクトリ同期を設定します。

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

以下のタスクがオンプレミスの UEM 環境に適用されます。UEM Cloud 環境で、BlackBerry Connectivity Node をインストールして設定し、会社のディレクトリに接続します。

作業を始める前に：

- UEM が使用できる Microsoft Active Directory アカウントを作成します。アカウントは、以下の要件を満たす必要があります。
  - Microsoft Exchange フォレストの一部である Windows ドメインに配置されていることが必要です。

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

- 組織で Microsoft Exchange リソースフォレストを使用している場合は、各ユーザーアカウントのリソースフォレストにメールボックスを作成し、アカウントフォレスト内のユーザーアカウントに関連付ける必要があります。UEM は、メールボックスを使用して、個々のドメインのユーザーアカウントを検索します。UEM にログインするユーザーを認証するには、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 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 資格情報、そして必要に応じて 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。

1. UEM 管理コンソールのメニューバーで、［設定］ > ［外部統合］ > ［会社のディレクトリ］の順にクリックします。
2. ＋ > ［**Microsoft Active Director** 接続］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（example.com など）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、次のいずれかを実行します。
   - 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。
   - 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、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、次のいずれかを実行します。
   - 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。
   - 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、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。
    - 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。
    - UEM が認証することのできるユーザーアカウントを制御するには、ユーザーコンテナ（例：OU=sales,DC=example,DC=com）の識別名を入力します。
11. グローバルグループのサポートを有効にする場合は、［グローバルグループのサポート］ドロップダウンリストで［はい］をクリックします。

オンボーディングにグローバルグループを使用する場合は、［はい］を選択する必要があります。グローバルグループドメインを設定するには、［グローバルグループドメインのリスト］セクションで、＋をクリックします。［ドメイン］フィールドで、追加するドメインをクリックします。［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 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、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、UEM で認証に使用する KDC のリストを指定することができます［追加］をクリックします。

12. 環境に Microsoft Exchange リソースフォレストが含まれている場合、リンクされている Microsoft Exchange メールボックスのサポートを有効にするには、［リンクされた **Microsoft Exchange** メールボックスのサポート］ドロップダウンリストで［はい］をクリックします。

    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、UEM で検索する KDC を指定します。必要に応じて、UEM でアクセスするグローバルカタログサーバーを指定します。［追加］をクリックします。

13. シングルサインオンを有効にするには、［**Windows** シングルサインオンを有効にする］チェックボックスをオンにします。シングルサインオンの詳細については、管理関連の資料の「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：

- 次のオプションタスクのいずれかを実行します。
  - ディレクトリにリンクされたグループを有効にする。
  - 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。
  - ディレクトリ同期を設定する。
- ディレクトリ接続を削除すると、そのディレクトリから UEM に追加されていたすべてのユーザーがローカルユーザーに変換されます。ユーザーがローカルユーザーに変換されると、後で会社のディレクトリへの接続を再び追加しても、ディレクトリにリンクされたユーザーには変換できません。ユーザーは引き続きローカルユーザーとして機能しますが、UEM は会社のディレクトリからの更新を同期することはできません。

LDAP ディレクトリに接続する

以下のタスクがオンプレミスの UEM 環境に適用されます。UEM Cloud 環境で、BlackBerry Connectivity Node をインストールして設定し、会社のディレクトリに接続します。

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 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。

- LDAP 接続が SSL 暗号化されている場合は、LDAP 接続のサーバー証明書があること、および LDAP サーバーが TLS 1.2 をサポートしていることを確認します。SSL が有効な場合、UEM への LDAP 接続は TLS 1.2 を使用する必要があります。
- 組織で使用する LDAP 属性値を確認します（以下の手順では、一般的な属性値の例を示します）。以下の手順でその属性値を使用します。

1. UEM 管理コンソールのメニューバーで、［設定］ > ［外部統合］ > ［会社のディレクトリ］の順にクリックします。
2. ＋ > ［**LDAP** 接続］ 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 サーバーをさらに追加するには、＋ 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)`」と入力します。
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、`dominoUNID` などです。
12. ［名］フィールドに、各ユーザーの名の属性を入力します（`givenName` など）。
13. ［姓］フィールドに、各ユーザーの姓の属性を入力します（`sn` など）。
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（`uid` など）。
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（`mail` など）。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（`displayName` など）。値を設定しない場合、デフォルト値が使用されます。

17. ［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（mail など）。
18. ［部門］フィールドに、各ユーザーの部門の属性を入力します。
19. ［職名］フィールドに、各ユーザーの職名の属性を入力します。
20. LDAP ディレクトリから追加のフィールドを同期する場合は、［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。必要に応じて、追加フィールドの属性を入力します。
21. 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。
    a) ［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。
    b) ［**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)」と入力します。
    c) ［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必要があります（たとえば、「cn」と入力）。
    d) ［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」と入力）。
    e) ［グループメンバーシップの属性］フィールドに、グループメンバーシップの属性の名前を入力します。属性値は DN 形式である必要があります（「CN=jsmith,CN=Users,DC=example,DC=com」など）。
    f) ［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既存のグループ名を入力します。
    g) グループメンバーのページ検索を有効にするには、［ページグループ検索を有効にする］チェックボックスをオンにします。
22. ［保存］をクリックします。
23. ［閉じる］をクリックします。

終了したら：

- 次のオプションタスクのいずれかを実行します。
  - ディレクトリにリンクされたグループを有効にする。
  - 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。
  - ディレクトリ同期を設定する。
- ディレクトリ接続を削除すると、そのディレクトリから UEM に追加されていたすべてのユーザーがローカルユーザーに変換されます。ユーザーがローカルユーザーに変換されると、後で会社のディレクトリへの接続を再び追加しても、ディレクトリにリンクされたユーザーには変換できません。ユーザーは引き続きローカルユーザーとして機能しますが、UEM は会社のディレクトリからの更新を同期することはできません。

ディレクトリにリンクされたグループを有効にする

会社のディレクトリのグループに BlackBerry UEM のグループをリンクして、ディレクトリと同じ方法で UEM のユーザーを整理し、ユーザーの IT ポリシー、プロファイル、アプリの割り当てと管理を簡素化できます。詳細については、管理関連の資料の「ユーザーグループの作成と管理」を参照してください。

作業を始める前に：

- 組織のディレクトリに接続します。
  - オンプレミスの UEM：「Microsoft Active Directory インスタンスに接続する」または「LDAP ディレクトリに接続する」

  - UEM Cloud：「BlackBerry Connectivity Node をインストールして設定し、Microsoft AD または LDAP に接続」
  - オンプレミスまたはクラウド：「UEM を Microsoft Entra ID に接続」
- 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. 管理コンソールのメニューバーで、［設定］ > ［外部統合］ > ［会社のディレクトリ］の順にクリックします。
2. ［会社のディレクトリ接続］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場合は、［同期を強制する］チェックボックスをオンにします。

   有効にした場合、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。
5. ［同期制限］フィールドで、各同期プロセスが完了できる変更の最大数を入力します。

   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。UEM では、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に対する変更の総数を定めています。
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：

- オプションで、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。
- 必要に応じて、ディレクトリ同期を設定します。
- 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「ユーザーグループの作成と管理」を参照してください。

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

オンボーディングを有効にすると、ユニバーサルまたはグローバルディレクトリグループをオンボーディングディレクトリグループとして UEM に追加します（オンボーディングはドメインローカルグループではサポートされません）。同期プロセス中に、UEM が、オンボーディングディレクトリグループに対応する UEM ユーザーアカウントのないディレクトリユーザーを検出した場合、そのユーザーアカウントを UEM に作成します。オンボーディングを有効にすると、オフボーディングも設定できます。オンボーディングディレクトリグループのユーザーを無効または削除すると、UEM はデバイスデータを削除し、UEM からユーザーを削除できます。

メモ：オフボーディングが有効になっている場合、オンボーディングディレクトリグループのメンバーでない UEM ユーザーアカウントは、どのように UEM に追加されたかに関係なく、次の同期プロセス中にオフボーディングされます。

作業を始める前に：

- 組織のディレクトリに接続します。

- オンプレミスの UEM：「Microsoft Active Directory インスタンスに接続する」または「LDAP ディレクトリに接続する」
- UEM Cloud：「BlackBerry Connectivity Node をインストールして設定し、Microsoft AD または LDAP に接続」
- オンプレミスまたはクラウド：「UEM を Microsoft Entra ID に接続」

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

1. 管理コンソールのメニューバーで、［設定］ > ［外部統合］ > ［会社のディレクトリ］の順にクリックします。
2. ［会社のディレクトリ接続］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. 次の操作のいずれかを実行します。

タスク	手順
オンボーディングディレクトリグループを追加し、デバイスのアクティベーションオプションを設定します。	**a.** ＋をクリックします。 **b.** ユニバーサルまたはグローバルディレクトリグループを検索して追加します。 **c.** 各ディレクトリグループについて、ネストされたグループをリンクするかどうかを選択します。 **d.** ［デバイスのアクティベーション］セクションで、オンボーディングされたユーザーに自動生成されたアクティベーションパスワードが記載されたメールを送信するか、またはアクティベーションパスワードを送信し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。
BlackBerry Dynamics アプリのみを使用するユーザーをオンボードします。	BlackBerry Dynamics アプリのみを使用するユーザーをオンボードする場合は、次の手順に従います。これらのユーザーは UEM で UEM Client を使用してもデバイスをアクティブ化できず、それらのデバイスは UEM によって管理されません。 **a.** ［**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。 **b.** ＋をクリックします。 **c.** ユニバーサルまたはグローバルディレクトリグループを検索して追加します。 **d.** 各ディレクトリグループについて、ネストされたグループをリンクするかどうかを選択します。 **e.** 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指定します。

タスク	手順
オフボーディングを設定します。	ユーザーが UEM からオフボーディングされたときにデバイスデータを削除する場合は、［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。次の手順に従います。 • デバイスから削除するデータに適したオプションを選択します。 • 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ときに UEM からユーザーを削除する場合は、［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］チェックボックスをオンにします。 • 同期サイクル後ユーザーとデバイスデータを削除するまで 2 時間待機する場合は、［オフボーディング保護］チェックボックスをオンにします。このオプションを使用すると、ディレクトリレプリケーションの遅延によって予期せず削除されないようにすることができます。

6. 会社のディレクトリグループの同期を強制する場合は、［同期を強制する］チェックボックスをオンにします。

   有効にした場合、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。
7. ［同期制限］フィールドで、各同期プロセスが完了できる変更の最大数を入力します。

   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。UEM では、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に対する変更の総数を定めています。
8. ［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。
9. ［保存］をクリックします。

終了したら： 必要に応じて、ディレクトリ同期を設定します。

ディレクトリ接続の同期

UEM を組織の会社のディレクトリに接続した後は、いつでも手動で同期プロセスを開始することも、定期的な同期をスケジュールすることもできます。次の同期が発生する前に同期レポートをプレビューしたり、同期プロセスが完了した後にレポートを表示したりできます。

作業を始める前に：

- 組織のディレクトリに接続します。
  - オンプレミスの UEM：「Microsoft Active Directory インスタンスに接続する」または「LDAP ディレクトリに接続する」
  - UEM Cloud：「BlackBerry Connectivity Node をインストールして設定し、Microsoft AD または LDAP に接続」
  - オンプレミスまたはクラウド：「UEM を Microsoft Entra ID に接続」

- 必要に応じて、「ディレクトリにリンクされたグループを有効にする」および「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」を行います。

1. 管理コンソールのメニューバーで、［設定］ > ［外部統合］ > ［会社のディレクトリ］の順にクリックします。
2. 次の操作のいずれかを実行します。

タスク	手順
同期のプレビュー	a. 同期をプレビューするディレクトリ接続の をクリックします。 b. ［今すぐプレビュー］をクリックします。 c. 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。
ディレクトリ同期を手動で開始	a. 同期するディレクトリ接続の をクリックします。 b. 同期が完了したら、［最終レポート］列の日付をクリックします。 c. レポートの .csv ファイルをエクスポートするには、 をクリックします。
同期スケジュールを追加	a. 同期をスケジュールするディレクトリ接続をクリックします。 b. ［同期スケジュール］タブで ＋ をクリックします。 c. ［同期タイプ］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。 • すべてのグループとユーザー：ユーザーは必要に応じてオンボーディングおよびオフボーディングされ、グループメンバーシップの変更が同期され、ユーザー属性への変更が同期されます。 • オンボーディンググループ：ユーザーは必要に応じてオンボーディングおよびオフボーディングされ、ユーザー属性の変更が同期されます。 • ディレクトリにリンクされたグループ：グループメンバーシップの変更が同期され、ユーザー属性への変更が同期されます。 • ユーザー属性：ユーザー属性に対する変更のみが同期されます。 d. ［繰り返し］ドロップダウンリストで、適切なオプションを選択し、必要に応じて繰り返しの設定を行います。 e. ［追加］をクリックします。 f. ［保存］をクリックします。

BlackBerry UEM の Microsoft Entra ID への接続

Microsoft Entra ID 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。UEM を Entra に接続すると、次の機能が利用できます。

- UEM を Entra ID に接続して UEM でディレクトリユーザーアカウントを作成できます。『BlackBerry UEM を Entra ID に接続する』を参照してください。
- UEM を使用して Microsoft Intune アプリ保護プロファイルの作成、管理、割り当てを行い、Office 365 アプリ内のデータを保護できます。『Microsoft Intune アプリ保護プロファイルを管理するための BlackBerry UEM の設定』を参照してください。
- 組織で Entra ID 条件付きアクセスを使用している場合は、UEM をコンプライアンスパートナーとして設定できます。これにより、UEM で管理されるデバイスが Office 365 などのクラウドベースのアプリにアクセスしようとしたときに、Intune に準拠していると認識されます。『BlackBerry UEM を Intune のコンプライアンスパートナーとして Entra に設定』を参照してください。

BlackBerry UEM を Entra ID に接続する

BlackBerry UEM を Microsoft Entra ID に接続して、UEM でディレクトリユーザーアカウントを作成できます。接続を設定すると、ディレクトリからユーザーデータを検索してインポートし、UEM ユーザーを作成できるようになります。ディレクトリユーザーは、ディレクトリの資格情報を使用して BlackBerry UEM Self-Service にアクセスできます。ディレクトリユーザーに管理ロールを割り当てると、ユーザーがディレクトリの資格情報を使用して管理コンソールにログインすることができるようになります。

組織でオンプレミスの Active Directory を使用しており、アカウントが Entra ID と同期されている場合、代わりにオンプレミスの Active Directory へのディレクトリ接続を作成する必要があります（Microsoft Active Directory インスタンスに接続する を参照）。UEM を Entra ID に接続するのは、Entra ID がプライマリディレクトリサービスで、オンプレミスの Active Directory がない場合に適しています。

作業を始める前に： Microsoft Entra ID アカウントが必要です。アカウントをお持ちでない場合は、「https://azure.microsoft.com」にアクセスしてアカウントを作成してください。このアカウントを使用して、Entra ポータルにログインします。

1. Entra ポータルにログインします。
2. Entra ID アプリ登録のセクションで、新しい登録を追加します。
3. 次の項目を指定して、登録を完了します。
   a) 登録するアプリの名前を入力します。
   b) アプリケーションを使用するか、API にアクセスできるアカウントタイプを選択します。
   c) リダイレクト URI の場合は、［**Web**］をクリックし、「`http://localhost`」と入力します。
4. アプリケーション ID をコピーします。
   これは UEM で登録するクライアント ID です。
5. API 権限の管理（［登録］ボタン）のセクションで権限を追加して、次のいずれかを選択します。
   - **Microsoft Graph**
   - アプリケーション権限
   - 次の権限を設定：**Group.Read.All**（アプリケーション）、**User.Read**（委任）、**User.Read.All**（アプリケーション）
6. 現在のディレクトリにあるすべてのアカウントに管理者の同意を付与します。

7. 証明書とシークレットを管理するセクションで、新しいクライアントシークレットを追加し、説明と期間を指定します。
8. シークレット ID ではなく、新しいクライアントシークレットの［値］フィールドをコピーします。
   これは UEM で登録するクライアントキーです。
9. UEM の管理コンソールのメニューバーで、［設定］ > ［外部統合］ > ［会社のディレクトリ］の順にクリックします。
10. ＋ > ［**Microsoft Azure Active Directory** 接続］をクリックします。
11. ［ディレクトリ接続名］フィールドに、接続先の名前を入力します。
12. ［ドメイン］フィールドに Entra ID ドメインを入力します。
13. ［クライアント **ID**］フィールドに、手順 4 で記録した ID を入力します。
14. ［クライアントキー］フィールドに、手順 8 で記録した値を入力します。
15. ［続行］をクリックします。
16. ［保存］をクリックします。

終了したら： 次のオプションタスクのいずれかを完了できます。

- ディレクトリにリンクされたグループを有効にする
- 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
- ディレクトリ接続の同期

Microsoft Intune アプリ保護プロファイルを管理するための BlackBerry UEM の設定

BlackBerry UEM を使用して Microsoft Intune アプリ保護プロファイルの作成、管理、割り当てを行い、Office 365 アプリ内のデータを保護するには、次の手順を実行する必要があります。

手順	アクション
1	Intune アプリ保護をサポートするための前提条件 を確認します。
2	Entra でのアプリ登録の作成。
3	BlackBerry UEM を設定して Microsoft Intune と同期する。

Intune アプリ保護をサポートするための前提条件

- BlackBerry UEM を Intune と同期するには、Intune ライセンスを持ち、かつ Entra ポータルで、グローバル管理者、Intune Service 管理者ロールを持つ制限付き管理者、または「KB 50341」に記載されている権限を持つカスタムロールのいずれかの権限を持つ Microsoft 管理者アカウントを使用する必要があります。
- Intune アプリ保護プロファイルを割り当てるユーザーアカウントは、Entra ID に存在する必要があります。
- ユーザーは UEM にディレクトリユーザーとして追加する必要があります。

- オンプレミスの Microsoft Active Directory を統合した場合は、ユーザーを Entra ID に同期する必要があります。詳細については、Microsoft 用の Entra ID Connect のドキュメントを参照してください。

Entra でのアプリ登録の作成

UEM が Entra での認証に使用できるアプリ登録を Entra で作成する必要があり ます。

作業を始める前に：

- Intune アプリ保護をサポートするための前提条件 を確認します。
- UEM 管理コンソールのメニューバーで、［設定］ > ［外部統合］ > ［**Microsoft Intune**］の順にクリックします。［返信 **URL**］の値を記録します。この URL は手順 3 で使用します。

1. Entra ポータルにログインします。
2. アプリ登録のセクションで、新しい登録を追加します。
3. 次の項目を指定して、登録を完了します。
   a) 登録するアプリの名前を入力します。
   b) アプリケーションを使用するか、API にアクセスできるアカウントタイプを選択します。
   c) リダイレクト URI の場合は、［モバイルクライアント/デスクトップ］をクリックし、管理コンソールから返信 URL を入力します。
4. アプリケーション ID をコピーします。
   これは UEM で登録するクライアント ID です。
5. API 権限を管理するセクションで、権限を追加し、次の項目を選択します。
   - **Microsoft Graph**
   - 委任されたアクセス許可
   - 次の委任されたアクセス許可を設定します。
     - **Microsoft Intune** アプリの読み取りと書き込み（［**DeviceManagementApps**］ > ［**DeviceManagementApps.ReadWrite.All**］）
     - すべてのグループの読み取り（［グループ］ > ［**Group.Read.All**］）
     - すべてのユーザーの基本プロファイルの読み取り（［ユーザー］ > ［**User.ReadBasic.All**］）
6. 現在のディレクトリにあるすべてのアカウントに管理者の同意を付与します。
7. 証明書とシークレットを管理するセクションで、新しいクライアントシークレットを追加し、説明と期間を指定します。
8. シークレット ID ではなく、新しいクライアントシークレットの［値］フィールドをコピーします。
   これは UEM で登録するクライアントキーです。

終了したら： BlackBerry UEM を設定して Microsoft Intune と同期する。

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

作業を始める前に： Entra でのアプリ登録の作成。

1. 管理コンソールのメニューバーで、［設定］ > ［外部統合］ > ［**Microsoft Intune**］の順にクリックします。
2. ［**Azure** テナント **ID**］フィールドに、組織の Entra ID テナントの ID を入力します。
3. ［クライアント **ID**］フィールドに、Entra でのアプリ登録の作成 で記録した ID を入力します。
4. ［クライアントキー］フィールドに、Entra でのアプリ登録の作成 で記録した値を入力します。
5. ［次へ］をクリックします。

6. 同期プロセスに使用する Intune 管理者アカウントの資格情報を指定します。

終了したら：

- 管理関連の資料の「Microsoft Intune で保護されているアプリの管理」を参照してください。
- Intune 管理者アカウントの資格情報を再入力する必要がある場合（アカウントのパスワードを変更する場合など）は、［設定］ > ［外部統合］ > ［**Microsoft Intune**］で、［資格情報を更新］をクリックします。

BlackBerry UEM を Intune のコンプライアンスパートナーとして Entra に設定

組織で Entra ID 条件付きアクセスを設定すると、BlackBerry UEM をコンプライアンスパートナーとして設定できます。これにより、UEM によって管理されている iOS デバイスおよび Android デバイスが Office 365 などのクラウドベースのアプリにアクセスするときに、Intune に準拠していると認識されます。Entra テナントごとに複数の UEM テナントを設定できますが、すべての UEM テナントが同じパートナーコンプライアンス管理エントリを共有します。Entra は、コンプライアンスステータスの更新の元となる UEM テナントを識別できません。

Entra ID 条件付きアクセスで UEM を設定すると、デバイスがコンプライアンス違反になった場合、UEM が Entra ID に通知します。

UEM のコンプライアンス強制アクション	動作
強制アクション：監視とログ	Intune には何も報告されません。
強制アクション： • 信頼しない • 仕事用データのみを削除 • すべてのデータを削除する	すべてのユーザープロンプトが期限切れになると、UEM は Entra ID に通知します。
BlackBerry Dynamics アプリへの強制アクション：監視とログ	Intune には何も報告されません。
BlackBerry Dynamics への強制アクション： • BlackBerry Dynamics アプリの実行を許可しない • BlackBerry Dynamics のアプリデータの削除	UEM は Entra ID にコンプライアンス違反が検出されるとすぐに通知します。

Entra ID 条件付きアクセスの設定

作業を始める前に：

- Intune ライセンスを持ち、かつ Entra ポータルで、グローバル管理者、Intune Service 管理者ロールを持つ制限付き管理者、または「KB 50341」に記載されている権限を持つカスタムロールのいずれかの権限を持つ Microsoft アカウントがあることを確認します。
- Microsoft Endpoint Manager 管理センターの［パートナーコンプライアンス管理］セクションで、iOS デバイスおよび Android デバイスの両方で［**BlackBerry UEM Azure** 条件付きアクセス］をコンプライアンスパートナーとして追加して、ユーザーおよびグループに割り当てます。
- この機能を使用するには、デバイスユーザーが次の要件を満たす必要があります。

- ユーザーが Entra ID に存在し、有効な Intune ライセンスを持っている必要があります。詳細については、「Microsoft Intune ライセンス」を参照してください。
- オンプレミス Active Directory を Entra ID と同期する場合、ユーザーのオンプレミス Active Directory UPN は Entra ID UPN と一致している必要があります。
- ユーザーは UEM にディレクトリユーザーとして追加する必要があります。
- ユーザーが、Microsoft Authenticator アプリと UEM Client の両方をデバイスにインストールしている必要があります。

1. UEM 管理コンソールのメニューバーで、［設定］ > ［外部統合］ > ［**Azure Active Directory** 条件付きアクセス］をクリックします。
2. ＋ をクリックします。
3. 設定の名前を入力します。
4. ［**Azure cloud**］ドロップダウンリストで［グローバル］をクリックします。
5. ［**Azure** テナント **ID**］フィールドに、組織のテナント名を FQDN 形式で入力するか、GUID 形式で一意のテナント ID を入力します。
6. ［デバイスマッピングの上書き］で、［**UPN**］または［メール］を選択します。

   UPN を選択した場合は、接続を保存する前に、Entra ID テナントとマッピングされたすべてのディレクトリが同じ UPN 値をユーザーと共有していることを確認してください。接続を保存すると、デバイスマッピングの上書きを変更することができなくなります。
7. ［使用可能な会社のディレクトリ］リストで、適切な会社のディレクトリを選択して追加します。
8. ［保存］をクリックします。
9. 組織の Entra テナントへのログインに使用する管理者アカウントを選択します。
10. Microsoft 権限要求を受け入れます。
11. メニューバーで、［ポリシーとプロファイル］ > ［ポリシー］ > ［**BlackBerry Dynamics**］をクリックします。デバイスユーザーに割り当てる BlackBerry Dynamics プロファイル（デフォルトプロファイルやカスタムプロファイルなど）では、次の手順を実行します。
    a) プロファイルを開いて編集します。
    b) ［**BlackBerry Dynamics** に登録する **UEM Client** を有効にする］を選択します。
    c) ［保存］をクリックします。
    d) 必要に応じ、プロファイルをユーザーおよびグループに割り当てます。
12. メニューバーで、［ポリシーとプロファイル］ > ［ネットワークと接続］ > ［**BlackBerry Dynamics** 接続］の順にクリックします。デバイスユーザーに割り当てる BlackBerry Dynamics 接続プロファイル（デフォルトプロファイルやカスタムプロファイルなど）では、次の手順を実行します。
    a) プロファイルを開いて編集します。
    b) ［アプリサーバー］セクションで、［追加］をクリックします。
    c) ［機能 - **Azure** 条件付きアクセス］を検索してクリックします。
    d) ［保存］をクリックします。
    e) ［**Azure** 条件付きアクセス］テーブルで ＋ をクリックします。
    f) ［サーバー］フィールドに、「`gdas-<UEM_SRP_ID>.<region_code>.bbsecure.com`」と入力します。
    g) ［ポート］フィールドに「443」と入力します。
    h) ［ルートタイプ］で、［直接］をクリックします。
    i) ［保存］をクリックします。

j) 必要に応じ、プロファイルをユーザーおよびグループに割り当てます。

13. ［機能 - **Azure** 条件付きアクセス］アプリをユーザーまたはグループに割り当てます。詳細については、「ユーザーアカウントの管理」および「ユーザーグループの管理」を参照してください。

終了したら：

- ユーザーがデバイスをアクティブ化すると、Active Directory 条件付きアクセスで登録するように求められます。アクティブ化されたデバイスのユーザーは、次回 UEM Client を開いたときに Active Directory 条件付きアクセスで登録するように求められます。
- UEM からデバイスを削除しても、デバイスは Entra ID 条件付きアクセス用に登録されたままになります。ユーザーが Microsoft Authenticator アプリのアカウント設定から Entra ID アカウントを削除できます。または、Entra ポータルからそのデバイスを削除することもできます。

APNs 証明書を取得して iOS および macOS デバイスを管理する

APNs は、Apple プッシュ通知サービスです。BlackBerry UEM を使用して iOS または macOS デバイスを管理するには、APNs 証明書を取得して登録する必要があります。複数の 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。

APN 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。

各 APNs 証明書は 1 年間有効です。管理コンソールは、有効期限を表示します。期限が切れる前に、証明書の取得時に使用したものと同じ Apple ID を使用して、APNs 証明書を更新する必要があります。管理コンソールで Apple ID を確認できます。期限切れの 30 日前に証明書の更新を通知するように、メールイベント通知を作成することもできます。証明書の期限が切れると、デバイスは 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。

Google Chrome または Safari を使用して、管理コンソールおよび 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は、APN 証明書の要求と登録を最適にサポートしています。

APN 証明書の要求および登録

1. 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。
2. ［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。
3. コンピューターに署名付き CSR ファイルを保存します。
4. ［手順 **2/3 - Apple** 発行の **APN** 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。
5. 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。
6. 指示に従って署名付き CSR をアップロードします。

   無効なファイルタイプエラーが表示された場合は、ファイルの名前を .txt ファイルに変更し、再度アップロードできます。
7. APN 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。
8. 管理コンソールの［手順 **3/3 - APN** 証明書を登録］セクションで、［参照］をクリックします。
9. APN 証明書に移動して選択します。
10. ［送信］をクリックします。

終了したら：

- 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 証明書は 1 年間有効です。毎年期限が切れる前に、元の APN 証明書の取得時に使用したものと同じ Apple ID を使用して、APN 証明書を更新する必要があります。証明書を更新するには、上記の手順を繰り返しますが、手順 2 では［証明書を更新］をクリックします。

トラブルシューティング：APN

問題	解決策
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」	「KB 37266」を参照してください。
APN 証明書を登録しようとすると、「APN 証明書が CSR と一致しません」というエラーが表示されます。	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。
iOS デバイスまたは macOS デバイスをアクティブ化できません。	APN 証明書が正しく登録されていない可能性があります。以下を確認します。 • 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。 • ［**APN** 証明書をテスト］をクリックし、BlackBerry UEM と APN サーバーの間の接続をテストします。 • 必要に応じて、BlackBerry 発行の新しい署名付き CSR と新しい APNs 証明書を取得します。

DEP 用の BlackBerry UEM の設定

Device Enrollment Program（DEP）用に組織が購入した iOS デバイスのアクティベーションを管理するために UEM 管理コンソールを使用すると、Apple の DEP と同期するように BlackBerry UEM を設定できます。

1. 管理コンソールのメニューバーで、［設定］ > ［外部統合］ > ［**Apple Device Enrollment Program**］に移動します。
   オンプレミスの UEM を使用している場合は、＋をクリックし、アカウントの名前を入力します。
2. ［**1/4**：**Apple DEP** アカウントを作成］セクションで、［**Apple DEP** アカウントを追加］をクリックします。
3. 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。
4. ［**2/4**：パブリックキーをダウンロード］セクションで、［パブリックキーをダウンロード］をクリックします。
5. ローカルマシンにパブリックキーを保存します。
6. ［**3/4**：**Apple DEP** アカウントからサーバートークンを生成］セクションで、［**Apple DEP** ポータルを開く］をクリックします。
7. DEP アカウントにサインインし、プロンプトに従ってサーバートークンを生成します。
8. ［**4/4**：サーバートークンを **BlackBerry UEM** に登録］セクションで、［参照］をクリックします。
9. .p7m サーバートークンファイルに移動して選択します。［開く］をクリックし、［次へ］をクリックします。
10. 登録設定ウィンドウに、設定の名前を入力します。
11. 登録設定を Apple の DEP で登録するときに、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。UEM 管理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、このオプションを選択しないでください。
12. 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。
13. ［デバイス設定］セクションで、次のオプションのいずれかを選択します。
    - ペアリングを許可する：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。
    - 必須：ユーザーが、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化できるようにします。
    - **MDM** プロファイルの削除を許可：ユーザーがデバイスを無効にできるようにします。
    - デバイスが設定されるまで待機する：UEM でのアクティベーションが完了するまで、ユーザーがデバイスのセットアップをキャンセルできないようにします。
14. ［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。

オプション	選択された場合の影響
パスコード	デバイスのパスコード作成を求めるプロンプトが表示されなくなります。
位置情報サービス	デバイスで位置情報サービスが無効になります。
復元	ユーザーがバックアップファイルからデータを復元できなくなります。

オプション	選択された場合の影響
Android から移行	Android デバイスからデータを復元できなくなります。
Apple ID	ユーザーが Apple ID と iCloud にサインインできなくなります。
使用条件	ユーザーには iOS の使用条件が表示されなくなります。
Siri	Siri がデバイスで無効になります。
診断	セットアップ時に診断情報がデバイスから自動的に送信されなくなります。
バイオメトリック	ユーザーが Touch ID を設定できなくなります。
支払い	ユーザーが Apple Pay を設定できなくなります。
ズーム	ユーザーが Zoom を設定できなくなります。
ホームボタンの設定	ユーザーがホームボタンのクリックを調整できなくなります。
画面時間	DEP の登録時に画面時間をセットアップするオプションがスキップされます。
ソフトウェア更新	必須のソフトウェア更新画面がデバイスに表示されなくなります。
iMessage および FaceTime	iMessage および FaceTime の画面がデバイスに表示されなくなります。
ディスプレイトーン	ディスプレイトーン画面がデバイスに表示されなくなります。
プライバシー	プライバシー画面がデバイスに表示されなくなります。
オンボーディング	オンボーディング情報画面がデバイスに表示されなくなります。
移行の監視	移行の監視画面がデバイスに表示されなくなります。
SIM のセットアップ	通信プランをセットアップする画面がデバイスに表示されなくなります。
デバイスからデバイスへの移行	デバイスからデバイスへの移行画面がデバイスに表示されなくなります。

15. ［保存］をクリックします。［新しいデバイスをこの設定に自動的に割り当てる］を選択した場合は、［はい］をクリックします。

終了したら：

- iOS デバイスをアクティベーションします。DEP に登録されているデバイスのアクティベーションの詳細については、「DEP に登録されている iOS デバイスのアクティベーション」を参照してください。

- 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。トークンを更新するには、［設定］ **>** ［外部統合］ **>** ［**Apple Device Enrollment Program**］で、DEP アカウントをクリックし、［サーバートークンを更新］をクリックします。両方の手順を完了して、新しいサーバートークンを生成し、それを UEM に登録します。
- 作成した DEP 接続はいずれも削除できます。すべての DEP 接続を削除すると、DEP で新しい Apple デバイスをアクティベーションできなくなります。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、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、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。

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

Android Enterprise デバイスは、Android デバイスを管理することを望む組織に、強化されたセキュリティを提供します。次の表に、Android Enterprise デバイスをサポートするための BlackBerry UEM の設定に関するさまざまなオプションをまとめています。

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
1 つの UEM ドメインを Google Workspace ドメインに接続する	組織が Google Workspace ドメインを使用する場合	Google Workspace アカウント（組織用）	• Gmail、Google Calendar、Drive などのすべての Google Workspace サービス • Google Play を通じたアプリ管理
1 つの UEM ドメインを Google Cloud ドメインに接続する	組織が Google Cloud ドメインを使用する場合	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）	• Google Workspace と同様ですが、Gmail、Google Calendar、Drive などの有料製品にはアクセスできません。 • Google Play を通じたアプリ管理
UEM が管理対象の Google Play アカウントとして Android Enterprise デバイスを管理することを許可する	組織が Google ドメインを使用しないか、すでに UEM ドメインの 1 つに接続されている Google ドメインを使用しており、Android Enterprise デバイスを 2 つ目の UEM ドメインで使用したい場合	管理 Google Play アカウントを持つ Android Enterprise デバイス	• Google Play を通じたアプリ管理 • Google サービスはサポートされていません。

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

作業を始める前に： 以前に UEM ドメインを Google ドメインに接続していて、新しい UEM ドメインを接続する場合は、既存の接続を削除する必要があります。管理コンソールのメニューバーで、［設定］ > ［外部統合］ > ［**Google** ドメイン接続］の順にクリックし、接続を削除します。接続の作成に使用したのと同じ Google アカウントを使用して、Google Play（「https://play.google.com/work」）の管理設定から接続を削除することもできます。接続を削除した場合、Android Enterprise アクティベーションタイプでアクティブ化されたすべてのデバイスが非アクティブ化されます。

1. 管理コンソールのメニューバーで、［設定］ > ［外部統合］ > ［**Android** および **Chrome** 管理］の順にクリックします。
2. 次の操作のいずれかを実行します。

タスク	手順
Google Play アカウントで管理された Android Enterprise デバイスを使用する	a. ［**BlackBerry UEM** での **Google Play** アカウントの管理を許可する］を選択します。 b. ［次へ］をクリックします。 c. ［**Android** で作業する］ウィンドウで、Google アカウント（Google または Gmail アカウント）を使用してサインインします。使用するアカウントは［Android で作業する］サービスの管理者アカウントになります。 d. ［開始］をクリックします。 e. 組織の名前を入力します。［確認］をクリックします。 f. ［登録を完了］をクリックします。
Google ドメインを使用する	a. ［**BlackBerry UEM** を既存の **Google** ドメインに接続する］を選択します。 複数の UEM ドメイン間で Google ドメインを共有することはできません。このオプションは、Android Enterprise および Chrome OS Enterprise をサポートします。 b. ［次へ］をクリックします。 c. サービスアカウントを作成するためのフィールドに入力し、［次へ］をクリックします。

3. 次の操作のいずれかを実行します。
   - BlackBerry Infrastructure を使用してアプリ設定の詳細を送信するには、［**UEM Client** を使用してアプリ設定を送信する］を選択します。
   - Google インフラストラクチャを使用してアプリ設定の詳細を送信するには、［**Google Play** を使用してアプリ設定を送信する］を選択します。
4. メッセージが表示されたら、［承諾］をクリックして、表示された Google および BlackBerry 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。
5. ［完了］をクリックします。

終了したら：

- Android Enterprise デバイスをアクティブ化する手順を完了します。デバイスのアクティベーションの詳細については、管理関連の資料の「Android デバイスのアクティベーション」を参照してください。
- ［設定］ > ［外部統合］から Google ドメイン接続を編集し、使用する Google ドメインのタイプを変更したり、ドメイン接続をテストしたりすることができます。
- Google に接続されている UEM ドメインを廃棄する予定がある場合は、ドメインを廃棄する前に接続を削除してください（［設定］ > ［外部統合］ > ［Google ドメイン接続］）。接続の作成に使用したのと同じ Google Play アカウントを使用して、Google（「https://play.google.com/work」）の管理設定から接続を削除することもできます。接続を削除した場合、Android Enterprise アクティベーションタイプでアクティブ化されたすべてのデバイスが非アクティブ化されます。

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

組織で Android Management API を使用してデバイスを管理する場合は、Android Management デバイスによりセキュリティを強化できます。

Android Management アクティベーションタイプのデバイスをアクティブ化する前に、「Android Management のアクティベーションタイプに関する考慮事項」を確認してください。

Google Cloud コンソールでの Android Management の設定

Android Management を設定するオプションにアクセスする前に、管理対象の Google Play アカウントを使用して Android Enterprise を設定する必要があります。

Android Management を設定するときは、専用のメールアドレスを使用する必要があります。Android Enterprise の設定に使用されたメールアドレスは使用できません。

作業を始める前に： Android Enterprise が UEM ですでに設定されていることを確認します。『Android Enterprise デバイスをサポートするための BlackBerry UEM の設定』を参照してください。

1. 「https://console.developers.google.com」にアクセスし、Android Management で使用するメールアドレスを使用してサインインします。
2. Cloud コンソールで、［新しいプロジェクト］をクリックします。
3. ［**API** とサービス］ > ［ライブラリを選択］をクリックします。
4. 検索バーで、Android Management API を検索します。
5. 検索結果のリストで、［**Android Management API**］および［**Cloud Pub/Sub API**］を有効にします。
6. Cloud コンソールのメニューバーで、［**IAM** と管理］ > ［サービスアカウント］ > ［選択］ > ［サービスアカウントを作成］をクリックします。
7. ［このサービスアカウントにプロジェクトへのアクセスを許可する］セクションの［ロール］ドロップダウンリストで、［**Android Management** のユーザー］を選択します。
8. 2 番目の［ロール］ドロップダウンリストで、［**Pub/Sub** 管理］を選択します。
9. ［ユーザーにサービスアカウントへのアクセスを許可する］セクションで、手順 1 で使用したメールアドレスを入力します。
10. ［完了］をクリックします。
11. メニューバーで［サービスアカウント］をクリックし、作成したアカウントを選択します。
12. ［キー］ > ［鍵を追加］をクリックします。
13. ［<*service_account_name*>のプライベートキーを作成する］ダイアログボックスで、［**JSON**］を選択します。［作成］をクリックします。
14. サービスアカウント名、サービスアカウント管理者のメールアドレス、および JSON のプライベートキーを記録します。

終了したら： BlackBerry UEM での Android Management の設定。

BlackBerry UEM での Android Management の設定

作業を始める前に：

- Google Cloud コンソールでの Android Management の設定。
- Android Management サービスのアカウント名、サービスアカウント管理者のメールアドレス、および JSON のプライベートキーがあることを確認します。

1. UEM の管理コンソールのメニューバーで、［設定］ > ［外部統合］ > ［**Android** および **Chrome** 管理］の順にクリックします。
2. ［**Android Management** への接続を追加］をクリックします。
3. ［**Enterprise** 表示名］フィールドに、サービスアカウント名を入力します。
4. ［管理者のメールアドレス］フィールドに、サービスアカウントのメールアドレスを入力します。
5. ［サービスアカウント情報（**JSON** 形式）］フィールドに、JSON のプライベートキーを入力します。
6. ［保存］をクリックします。
7. ［ドメイン名またはビジネス名］ダイアログボックスの［回答］フィールドに、Android Management サービスのアカウント名を入力します。［次へ］をクリックします。

Chrome OS デバイスの管理を BlackBerry UEM に拡張

BlackBerry UEM を Google 管理対象ドメインと統合して Chrome OS の管理機能の一部を UEM に拡張できます。Google ドメインに Chrome Enterprise Upgrade が含まれている必要があります。Chrome OS デバイスの登録と一部の管理は、引き続き Google 管理対象ドメインコンソールを介して行うことに注意してください。

UEM は、Google 管理コンソールの組織単位を UEM の組織単位グループに同期します。初期同期後、UEM は Google ドメインに登録して、組織単位、ユーザー、またはデバイスの変更がすべて通知されるようにします。UEM が変更を通知されると、それに応じてデータベースが同期され、更新されます。

手順	アクション
1	Google ドメインで認証するためのサービスアカウントの作成。
2	UEM による Chrome OS データの同期の有効化。
3	UEM の Google ドメインとの統合。

Android Enterprise デバイスをサポートするように UEM を設定済みの場合は、次の手順に従って UEM で Chrome OS デバイスを管理できます。

手順	アクション
1	組織の Google で、Chrome OS エンタープライズが有効になっていることを確認します。
2	Chrome Policy API で、組織の Google ドメインが有効になっていることを確認します。詳細については、「Google ドメインで認証するためのサービスアカウントの作成」を参照してください。
3	すべての範囲が追加されていることを確認します。詳細については、「UEM による Chrome OS データの同期の有効化」を参照してください。
4	UEM コンソールで、Chrome OS の管理を有効にします。詳細については、「UEM の Google ドメインとの統合」を参照してください。

Google ドメインで認証するためのサービスアカウントの作成

BlackBerry UEM が既存の Google 管理対象ドメインにまだ接続されていない場合にのみ、これらの手順を実行します。

1. プロジェクトの管理に使用する Google アカウントで、Google デベロッパーコンソールにログインします。
2. プロジェクトを作成します。

3. プロジェクトを選択し、そのプロジェクトのサービスアカウントを作成します。
4. サービスアカウントに［基本］ > ［編集者］ロールを付与します。
5. サービスアカウントを選択し、新しい P12 キーを追加します。
6. プライベートキーのパスワードをコピーし、ローカルマシンに証明書を保存します。
7. サービスアカウントの一意のクライアント ID とメールアドレスを検索してコピーします。
8. ［有効な API とサービス］セクションで、次の API を検索して有効にします。
   - **Admin SDK API**
   - **Google Play EMM API**
   - **Chrome** ポリシー **API**

終了したら： UEM による Chrome OS データの同期の有効化。

UEM による Chrome OS データの同期の有効化

組織の Google 管理コンソールを使用して、UEM で Chrome OS データの同期を可能にする追加の API を有効にする必要があります。

作業を始める前に： Google ドメインで認証するためのサービスアカウントの作成。

1. Google ドメインの管理者アカウントを使用して、Google 管理コンソールにログインします。
2. モバイルデバイスの［サードパーティとの連携］セクションに移動します。
3. サードパーティの Android モバイル管理が有効になっていることを確認します。
4. EMM プロバイダーを追加するセクションで、トークンを生成します。
5. トークンをコピーします。
6. セキュリティの API を管理するセクションで、ドメイン全体の委任を管理するオプションをクリックします。
7. 新しい設定を追加します。
8. クライアント ID には、Google サービスアカウントの一意のクライアント ID を貼り付けます。
9. OAuth スコープには、以下をカンマ区切りリストで入力するか貼り付けます。
   - https://www.googleapis.com/auth/admin.directory.user
   - https://www.googleapis.com/auth/admin.directory.customer
   - https://www.googleapis.com/auth/admin.directory.device.chromeos
   - https://www.googleapis.com/auth/admin.directory.device.mobile
   - https://www.googleapis.com/auth/admin.directory.orgunit
   - https://www.googleapis.com/auth/admin.directory.user
   - https://www.googleapis.com/auth/chrome.management.policy
   - https://www.googleapis.com/auth/admin.reports.audit.readonly
10. 接続を承認します。

終了したら： UEM の Google ドメインとの統合。

UEM の Google ドメインとの統合

作業を始める前に： UEM による Chrome OS データの同期の有効化。

1. セキュリティ管理者アカウントを使用して、UEM 管理コンソールにログインします。
2. メニューバーで、［設定］**>**［外部統合］**>**［**Android** および **Chrome** 管理］をクリックします。
3. ［**BlackBerry UEM** を既存の **Google** ドメインに接続する］を選択します。
4. ［アプリ設定の送信方法］で、［**Google Play** を使用してアプリ設定を送信する］を選択します。
5. ［次へ］をクリックします。
6. ［プライベートキーパスワード］フィールドに、Google デベロッパーコンソールからプライベートキーパスワードを貼り付けます。
7. ［参照］をクリックします。
8. Google デベロッパーコンソールから証明書ファイルに移動し、その証明書を選択します。
9. ［サービスアカウントのメールアドレス］フィールドに、Google デベロッパーコンソールから Google サービスアカウントのメールアドレスを貼り付けます。
10. ［**Google** ドメイン管理者のメールアドレス］フィールドに、Google ドメインで Google Cloud または Google Workspace を管理するために使用する管理者アカウントのメールアドレスを入力します。
11. ［トークン］フィールドに、生成したトークンを貼り付けます。
12. ［仕事用プロファイルで **Android** デバイスを管理するドメインのタイプを選択］セクションで、対応する Google ドメインのタイプを選択します。
13. ［**Google Cloud** ドメイン］を選択した場合は、次のオプションのいずれかを選択します。
    - **BlackBerry UEM** によるドメイン内のユーザー作成を許可しない：このオプションを選択した場合は、Google Cloud ドメインでユーザーを作成し、UEM で同じメールアドレスを持つローカルユーザーを作成する必要があります。
    - **BlackBerry UEM** によるドメイン内のユーザー作成を許可する：このオプションを選択した場合は、次のいずれかを選択します。
      - **BlackBerry UEM** による **Google** ドメイン内のユーザー削除を許可しない
      - **BlackBerry UEM** による **Google** ドメイン内のユーザー削除を許可する
14. ［次へ］をクリックして、UEM に追加するアプリケーションを選択します。
15. ［次へ］をクリックします。
16. もう一度［次へ］をクリックします。

終了したら：UEM を Google 管理コンソールと同期させるには、メニューバーで［設定］**>**［外部統合］**>**［**Android** および **Chrome** 管理］をクリックします。［**Chrome OS** の管理］セクションで、［有効にする］をクリックします。UEM では 10 分以内にデータの初期同期が行われ、定期的な同期のスケジュールも設定されます。同期が完了したら、この画面のオプションを使用して、組織単位、ユーザー、およびデバイスの予定されていない同期を開始できます。

Windows 10 アクティベーションの簡易化

ユーザーが BlackBerry UEM で Windows 10 デバイスをアクティブ化する場合、ユーザーは UEM サーバーのアドレスを指定する必要があります。次の方法を使用して、ユーザーのアクティベーションプロセスを簡易化できます。

方法	説明
UEM と Entra ID 参加を統合する	Entra ID 参加が設定されている場合、ユーザーは Entra ID のユーザー名とパスワードのみでデバイスをアクティブ化することができます。ただし、Entra ID プレミアムライセンスが必要です。 『UEM と Entra ID 参加の統合』を参照してください。
Windows Autopilot を設定します。	Windows Autopilot を設定すると、登録が初期設定の一環となり、ユーザーが Entra ID のユーザー名とパスワードのみを使用して設定を完了したときに、デバイスが自動的にアクティブ化されます。これには、Entra ID 参加の統合と Entra ID プレミアムライセンスが必要です。 『デバイスのアクティベーションのための Windows Autopilot の設定』を参照してください。
検出サービスを導入する	JavaWeb アプリケーションを BlackBerry から検出サービスとして使用できます。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。 『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』を参照してください。

UEM と Entra ID 参加の統合

Windows 10 デバイスの登録プロセスを簡素化するために、BlackBerry UEM と Entra ID 参加を統合できます。これが設定されている場合、ユーザーは、Entra ID のユーザー名とパスワードを使用して、デバイスを UEM に登録することができます。Entra ID 参加は、Windows 10 の初期設定中に Windows 10 デバイスを UEM で自動的にアクティブ化できるようにする Windows Autopilot をサポートするためにも必要です。UEM 証明書は、デバイスに手動でインストールすることも、管理者が SCCM を使用して証明書を展開することもできます。

作業を始める前に： 以下の手順を実行するには、MDM 使用条件 URL、MDM 探索 URL、およびアプリ ID URI が必要です。これらの URL を決定するには、UEM 管理コンソールでテストユーザーアカウントを作成し、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してユーザーにアクティベーションメールを送信します。デフォルトのテンプレートには、受信したメールで適切な値に変換される %ClientlessActivationURL% 変数が含まれています。以下の手順で、次の URL にその値を使用します。

- MDM 使用条件 URL：*%ClientlessActivationURL%*/azure/termsofuse
- MDM 探索 URL：*%ClientlessActivationURL%*/azure/discovery
- アプリ ID URI： *%ClientlessActivationURL%*

1. Microsoft Entra ID 管理コポータルにログインします。

2. MDM および MAM を管理するセクションで、オンプレミス MDM アプリケーションを追加し、分かりやすい名前（たとえば `BlackBerry UEM`）を付けます。
3. 追加したアプリケーションをクリックして設定します。
4. ユーザースコープを指定します。該当する場合は、グループを選択します。
5. MDM 使用条件 URL および MDM 探索 URL を指定します。
6. 変更を保存します。
7. オンプレミス MDM アプリケーション設定のプロパティで、アプリ ID URI を指定します。
8. 保存します。

終了したら： オプションで、デバイスのアクティベーションのための Windows Autopilot の設定。

デバイスのアクティベーションのための **Windows Autopilot** の設定

Windows Autopilot を設定する場合は、ユーザーが Entra ID ユーザー名とパスワードのみを使用して初期設定を完了すると、デバイスが自動的にアクティブ化されます。

作業を始める前に： UEM と Entra ID 参加の統合。

1. Microsoft Entra ID 管理コポータルにログインします。
2. Windows デバイス登録のセクションで、Windows Autopilot 導入プロファイルを作成します。
3. プロファイルの名前と説明を入力します。
4. Out-of-Box Experience 設定を構成します。
5. プロファイルを適切なユーザーグループに割り当てます。
6. プロファイルを保存します。
7. Windows Autopilot でアクティブ化する各 Windows 10 デバイスで、次の手順を完了します。
   a) デバイスをオンにし、初期設定をロードして Wi-Fi ネットワークに接続します。
   b) CTRL+SHIFT+F3 を押して再起動し、監査モードに入ります。
   c) 管理者として Windows PowerShell を実行し、次のコマンドを実行します。

```
Save-Script -Name Get-WindowsAutoPilotInfo -Path C:\Windows\Temp
```

```
Install-Script -Name Get-WindowsAutoPilotInfo
```

```
Get-WindowsAutoPilotInfo.ps1 -OutputFile C:\Windows\Temp\MyComputer.csv
```

   d) 結果として生じた .csv ファイルを各デバイスから収集します。
8. Microsoft Entra ID 管理ポータルの Windows デバイス登録および Windows Autopilot デバイスのセクションで、各デバイスから .csv ファイルをインポートします。
9. ［システム準備ツール］ダイアログで、次の操作を実行します。
   a) ［システムクリーンアップアクション］で、［システムの OOBE（Out-of-Box Experience）に入る］オプションを選択し、［一般化する］を選択解除します。
   b) ［シャットダウンオプション］で、［再起動］オプションを選択します。

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

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。

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。以下の手順ではタスクの概要を述べています。具体的なアクションは、組織の環境によって異なります。

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。
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ブ化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. 設定した静的 IP アドレスを指し示す、**enterpriseenrollment** という<*email_domain*> 名前の DNS Host A レコードを作成します。
4. 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。
5. myAccount にログインして、自動検出プロキシツールをダウンロードします。.exe ファイルを実行して、.war ファイルを抽出します。
   .exe ファイルはファイル `W10AutoDiscovery-<version>.war` を `C:\BlackBerry` に抽出します。
6. `W10AutoDiscovery-<version>.war` の名前を `ROOT.war` に変更します。このファイルを Java アプリケーションサーバーのルートフォルダーに移動します。
7. ディスカバリサービス Web アプリケーションの wdp.properties ファイルを更新して、UEM インスタンスの SRP ID（UEM オンプレミス）またはテナント ID（UEM Cloud）のリストを含めます。これらの ID は myAccount で確認できます。

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

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オンプレミスのソース UEM サーバーから移行できます。オンプレミスの UEM 環境では、スタンドアロンの Good Control サーバーから移行することもできます。

手順	アクション
1	「移行の前提条件」および「ベストプラクティスと考慮事項」を確認します。
2	ソースサーバーへの接続。
3	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。
4	ソースサーバーからのユーザーの移行。
5	ソースサーバーからのデバイスの移行。

前提条件：ソースの BlackBerry 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

項目	前提条件
セキュリティ管理者の権限	セキュリティ管理者として、このセクションの手順を完了します。
サポートされているソースサーバーのバージョン	オンプレミスの UEM の場合は、次のソースサーバーから移行できます。 • オンプレミスの UEM 12.15 以降 • Good Control（スタンドアロン）5.0 以降 UEM Cloud の場合は、オンプレミスの UEM からのみデータを移行できます。ソースのオンプレミスの UEM インスタンスは、最近リリースされた主要な 3 つのバージョンのいずれかである必要があります。それ以前のバージョンでは、移行はサポートされていません。

項目	前提条件
BlackBerry Connectivity Node（UEM Cloud のみ）	すべての移行機能をサポートするには、BlackBerry Connectivity Node バージョン 2.13 以降の少なくとも 1 つをアクティブ化する必要があります。
UEM の会社のディレクトリ接続	移行先である UEM の会社のディレクトリ接続を、ソースサーバーでの設定と同じ方法で設定します。会社のディレクトリ接続が一致しない場合、移行は機能しません。
データベースのデフラグ（オンプレミスの UEM のみ）	移行を開始する前に、移行元および移行先の UEM データベースをデフラグします。多数のユーザーまたはデバイスを移行する場合は、ユーザーまたはデバイスの各セットを移行した後に移行先の UEM データベースをデフラグする必要があります。
BlackBerry UEM Client	• オンプレミスの UEM：BlackBerry Dynamics に登録済みの UEM Client アプリおよび BlackBerry Dynamics アプリを移行する場合は、最新の UEM Client をデバイスにインストールする必要があります。 • UEM Cloud：UEM Client はバージョン 12.x 以降である必要があります。
BlackBerry Dynamics アプリ	• オンプレミスの UEM：移行する BlackBerry Dynamics アプリは、すべて BlackBerry Dynamics SDK バージョン 7.1 以降を使用している必要があります。Good Control からの移行では、アプリは SDK バージョン 4.0.0 以降を使用している必要があります。 • UEM Cloud：移行する BlackBerry Dynamics アプリは、すべて BlackBerry Dynamics SDK バージョン 8.0 以降を使用している必要があります。 • 移行がサポートされていない BlackBerry Dynamics アプリは、移行プロセス中にデバイスから削除されます。

項目	前提条件
BlackBerry Dynamics アプリの権利	• 移行先の UEM サーバーには、ソースサーバーと同じ BlackBerry Dynamics アプリの権利のリストがある必要があります。 • 移行されたユーザーアカウントには、移行先の UEM 上で、ソースサーバー上と同じ BlackBerry Dynamics アプリの権利のリストが割り当てられている必要があります。 • 認証委任は、ソースサーバーと移行先サーバー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。 • ソースサーバー上の BlackBerry Dynamics プロファイルで UEM Client が BlackBerry Dynamics によってアクティブ化できる場合は、移行先サーバー上でも同じように設定します。 • 認証委任は、ソースサーバーと移行先の UEM サーバー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。 • Good Control インスタンスからの移行では、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。 ソースサーバーと移行先サーバーの間で権利が一致しない場合、移行後に BlackBerry Dynamics アプリが無効になります。
カスタム BlackBerry Dynamics アプリ	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組織 ID の場合にのみ移行します。組織の結合の詳細については、「KB 47626」を参照してください。
ポート	• オンプレミスの UEM：Microsoft SQL Server でポート 1433（TCP）およびポート 1434（UDP）がブロック解除されていることを確認します。 • UEM Cloud：ポート 8887（TCP）が、オンプレミス UEM サーバーと BlackBerry Connectivity Node 間で開いている必要があります。オンプレミス UEM データベースをホストする Microsoft SQL Server によって使用されているポートが開いており、BlackBerry Connectivity Node からアクセスできることを確認します（ポート 1433 など）。

UEM の移行のベストプラクティスと考慮事項

ITポリシー、プロファイル、およびグループの移行

項目	考慮事項とベストプラクティス
ソースの UEM サーバーからコピーされる項目	• 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 接続プロファイル • BlackBerry Dynamics プロファイル • アプリの設定 • CA 証明書プロファイル • 共有証明書プロファイル • 証明書の取得 • ユーザー資格情報プロファイル • SCEP プロファイル • CRL プロファイル • OSCP プロファイル • 認証局設定（Entrust および PKI コネクターのみ） • クライアント証明書（アプリの使用状況） • 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
ソースの Good Control サーバーからオンプレミスの UEM のみにコピーされる項目	• 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
グループの移行	ユーザー、ロール、およびソフトウェア設定の割り当ては移行されません。これらの割り当ては、移行先の UEM サーバー上で、手動で再作成する必要があります。
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、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 ポリシーは適宜変更してください。
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。

項目	考慮事項とベストプラクティス
BlackBerry Dynamics 接続プロファイル	［アプリサーバー］タブの値は移行されません。値は、移行先の UEM サーバーのデフォルト値を使用して設定されます。［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。
アプリグループ（Good Control からオンプレミスの UEM のみ）	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、移行先の UEM サーバーの［すべてのユーザー］グループに関連付けられていません。
証明書の使用状況（UEM）	証明書の使用状況は、以下を除き、移行されます。 • 移行先サーバーにすでに存在する証明書の使用状況 • BlackBerry Dynamics 以外のアプリ • 他の Good Control 組織からのカスタムアプリ
BlackBerry Dynamics ユーザーの移行後のタスク	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 からオンプレミスの UEM、またはソースのオンプレミスの UEM サーバーから UEM Cloud に移行した後、次のタスクを完了します。 • 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 Good Control 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 UEM に移動します。 • 移行された接続プロファイルで、アプリサーバーと BlackBerry Proxy クラスターの情報を指定します。

ユーザーの移行

項目	
ユーザーの最大数	ソースサーバーから一度に移行できるユーザー数は、最大 1,000 人です。最大数を超えるユーザーを選択した場合、最大数までは移行されますが、残りはスキップされます。必要に応じて移行プロセスを繰り返すことで、すべてのユーザーをソースサーバーから移行できます。

項目	
メールアドレス	• 関連付けられているメールアドレスのユーザーのみを移行できます。 • すでに移行先の UEM サーバー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。 • ソースデータベースの 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 人だけが表示されます。
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。 • 共有デバイスグループの所有者であるユーザーは移行できません。このユーザーは、移行するユーザーのリストには表示されません。
BlackBerry UEM Self-Service	• 移行後、ユーザーは移行前に使用したのと同じ BlackBerry UEM Self-Service のログイン情報を使用する必要があります。 • 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 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、移行後に自動で権限を付与されません。

ソースサーバーからのデバイスの移行

項目	考慮事項とベストプラクティス
設定の確認	固有の設定ごとに（異なるグループ、ポリシー、アプリの設定など）デバイスを 1 台移行し、移行先サーバーが正しく設定されていることを確認してから残りのデバイスを移行することをお勧めします。
デバイスの最大数	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。
ユーザー	• デバイスのユーザーが移行先の UEM ドメインに存在している必要があります。 • ユーザーのデバイスをすべて同時に移行する必要があります。

項目	考慮事項とベストプラクティス
ソースの UEM 上の管理対象の iOS デバイス	• デバイスの UEM Client は最新のバージョンである必要があります。 • アプリロックプロファイルを割り当てられているデバイスは、移行の際に UEM Client を開くことができないため移行できません。 • UEM Client を持たない Apple DEP デバイスは、移行がサポートされていないデバイスのリストに表示されますが、別の方法でも移行できます。DEP デバイスを移行するには、UEM Client を持っているか否かにかかわらず、追加の手順を実行する必要があります。『ソースサーバーからの DEP デバイスの移行』を参照してください。 • ユーザー登録デバイスは移行できません。 • すべての適用可能なアプリのアプリ設定で、［**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。この手順を実行せずに移行しようとすると、アプリが削除されてデバイスが UEM の登録を解除されます。
ソースの Android 上の管理対象の UEM デバイス	• Android Enterprise デバイスに最新バージョンの UEM Client がインストールされている必要があります。 • Google アカウントまたは Google ドメインを使用する仕事用プロファイルを含む Android デバイスは移行できません。
Chrome OS デバイス	Chrome OS デバイスは UEM のソースサーバーから移行できます。
移行がサポートされていないデバイス	• Windows • macOS
共有デバイスグループ	共有デバイスグループに属するデバイスは移行できません。これらのデバイスは移行リストに表示されません。

項目	考慮事項とベストプラクティス
BlackBerry Dynamics 対応デバイス	• ［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。 • BlackBerry Access for Windows、BlackBerry Access for macOS、BlackBerry Bridge では、移行はサポートされていません。移行が完了した後、ユーザーはこれらのアプリを再登録する必要があります。 • 移行プロセスでは、デバイスのデータがキャッシュされた後にデバイス上でアクティベートされた UEM Client およびアプリの移行を追跡および保証しません。それぞれの移行の前にユーザーキャッシュを更新することをお勧めします。 • BlackBerry Dynamics 対応デバイスは、必ず移行先サーバーで BlackBerry Dynamics に登録されます。 • Good Control （スタンドアロン）インスタンスからの移行の場合、Good Dynamics MDM の登録は移行されません。 • 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。 • 移行が開始された後にユーザーが BlackBerry Dynamics アプリのパスワードを忘れた場合でも、コンテナが移行を完了する前であれば、ロック解除アクセスキーを UEM のソースサーバーから取得する必要があります。移行が完了したら、キーを移行先の UEM サーバーから取得する必要があります。 • 移行をデバイス上で開始するには、最初にデバイス上で認証委任として設定されているアプリを開くことをお勧めします。

ソースサーバーへの接続

データを移行するには、BlackBerry UEM をソースサーバーに接続する必要があります。アクティブなソースサーバーは一度に 1 つしか保有できません。

作業を始める前に：

- 「移行の前提条件」および「ベストプラクティスと考慮事項」を確認します。
- オンプレミスの UEM 環境で、ログイン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ます。
- UEM Cloud 環境で、複数の BlackBerry Connectivity Node がアクティブ化されている場合は、BlackBerry Connectivity Node のすべてのインスタンスを同じソースデータベースに接続するように設定します。

UEM 環境の種類に応じて、次の手順に従います。

環境	手順
オンプレミスの UEM	**a.** 管理コンソールのメニューバーで、［設定］ > ［移行］ > ［設定］をクリックします。 **b.** ＋をクリックします。 **c.** ［ソースの種類］ドロップダウンリストで、該当するソースサーバーの種類をクリックします。 **d.** ソースサーバーの情報を指定します。 ソースの Good Control サーバーからデータを移行する場合は、サードパーティの証明書に置き換えられていない証明書をエクスポートしてアップロードするだけで済みます。UEM はサードパーティプロバイダーからの証明書を基本的に信頼します。 **e.** ［テスト接続］をクリックします。 **f.** ［保存］をクリックします。
UEM Cloud	**a.** BlackBerry Connectivity Node 管理コンソールのメニューバーで、［一般設定］ > ［移行］をクリックします。 **b.** ＋をクリックします。 **c.** ソースサーバーの情報を指定します。 • ［データベースサーバー］フィールドで、動的ポートは *<host>\<instance>* の形式、静的ポートは *<host>:<port>* の形式を使用します。 • Windows NT 認証を選択した場合、BlackBerry UEM - BlackBerry Cloud Connector サービスのログオンプロパティを、ソースサーバーをインストールしたアカウントと同じアカウントに変更します。移行が完了したら、ローカルシステムアカウントを使用して、ログオンプロパティを元に戻します。 **d.** ［保存］をクリックします。 **e.** UEM 管理コンソールで、［設定］ > ［移行］ > ［設定］をクリックします。 **f.** ＋をクリックします。 **g.** ソースデータベースの名前を入力します。 **h.** ［テスト接続］をクリックします。 **i.** ［保存］をクリックします。

終了したら： 次の操作のいずれかを実行します。

- 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。
- 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のデバイスの移行。

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

作業を始める前に： ソースサーバーへの接続。

1. 管理コンソールのメニューバーで、［設定］ > ［移行］をクリックします。

UEM オンプレミス環境で複数のソースサーバーを構成した場合は、データを移行するソースサーバーを選択します。

2. ［**IT** ポリシー、プロファイル、グループ］をクリックします。
3. ［次へ］をクリックします。
4. 移行する項目を選択します。

   移行先サーバーへの移行時に、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。
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。

終了したら：

- 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。
- 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。
- 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のユーザーの移行

作業を始める前に：

- ソースサーバーへの接続。
- 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。

1. 管理コンソールのメニューバーで、［設定］ > ［移行］ > ［ユーザー］をクリックします。
2. ［キャッシュを更新］をクリックします。

   更新には、ユーザー 1,000 人ごとに約 10 分かかります。キャッシュの更新は、最初のユーザーのセットを移行する場合のみ必須です。移行中にソースサーバーに変更を加えた場合は、キャッシュを再度更新することをお勧めします。
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。

   デフォルトでは、最初の 20,000 人のユーザーのみが表示されます。必要に応じて特定のユーザーを検索することもできます。［すべてのユーザー］を選択しても、最初のページに表示されているユーザーしか選択されませんのでご注意ください。
5. ［次へ］をクリックします。
6. 選択したユーザーに IT ポリシー、グループ、およびプロファイルを割り当てます。
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。

移行されたユーザーアカウントは、ソースサーバーから削除されないことに注意してください。

終了したら： 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：

- ソースサーバーへの接続。
- 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。
- ソースサーバーからのユーザーの移行。
- DEP デバイスを移行するには、「ソースサーバーからの DEP デバイスの移行」を参照してください。その他のデバイスについては、以下の手順で行ってください。
- iOS デバイスのユーザーに、BlackBerry UEM Client を開いて移行が完了するまで開いたままにしておく必要があることを通知します。

1. 管理コンソールのメニューバーで、［設定］ > ［移行］ > ［デバイス］をクリックします。
2. ［キャッシュを更新］をクリックします。

   更新には、デバイス 1,000 台ごとに約 10 分かかります。キャッシュの更新は、最初のデバイスのセットを移行する場合のみ必須であり、その後はオプションです。移行中にソースサーバーに変更を加えた場合は、キャッシュを再度更新することをお勧めします。
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。

   デフォルトでは、最初の 20,000 台のデバイスのみが表示されます。必要に応じて特定のデバイスを検索することもできます。［すべてのデバイス］を選択しても、最初のページに表示されているデバイスしか選択されませんのでご注意ください。
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］ > ［ステータス］をクリックします。

終了したら： 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］の順にクリックします。

ソースサーバーからの 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、ソースの UEM サーバーから移行先の UEM サーバーに移行できます。DEP デバイスの移行をサポートするには、以下に示す追加タスクを実行します。以下の手順を完了すると、UEM 管理コンソールを使用して、BlackBerry UEM Client および MDM 制御 のアクティベーションタイプを持つ DEP デバイスを移行できます。UEM Client を持たないか、他のアクティベーションタイプを持つ DEP デバイスでは、代わりに、移行先サーバーで工場出荷時の設定にリセットし、再アクティベーションする必要があります。

DEP 登録設定は移行されず、デバイスは移行先環境では登録設定を失うことに注意してください。

作業を始める前に： 管理コンソールのメニューバーで、［アプリ］をクリックします。UEM Client を検索してクリックします。［**iOS**］タブで、［**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。このオプションをオフにせずにデバイスを移行しようとすると、UEM Client が削除されてデバイスが UEM から登録解除される場合があります。

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 UEM インスタンスを新しい仮想 MDM サーバーに接続します。手順については、「DEP 用の BlackBerry UEM の設定」を参照してください。

   移行先の UEM サーバーの DEP プロファイルが、ソースサーバーの 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. 次の操作のいずれかを実行します。

   - UEM Client および MDM 制御 のアクティベーションタイプを持つ DEP デバイスの場合、UEM 管理コンソールを使用してデバイスを移行先サーバーに移行します。
   - UEM Client を持たないか、他のアクティベーションタイプを持つ DEP デバイスの場合は、各デバイスを工場出荷時の設定にリセットし、移行先サーバーでデバイスを再アクティブ化します。

終了したら： UEM Client および MDM 制御 のアクティベーションタイプを持つ DEP デバイスの場合、認証委任として設定されているアプリを開くようにユーザーに指示します。これにより、デバイスでの移行が開始されます。

BlackBerry Dynamics アプリのネットワーク通信とプロパティの設定

このセクションの手順に従って、BlackBerry Dynamics アプリのネットワーク通信およびその他のプロパティを設定します。

タスク	説明
BlackBerry Proxy クラスターの管理。	BlackBerry Dynamics アプリのデータをルーティングする BlackBerry Proxy クラスターを作成および管理します。
ポート転送を使用した Direct Connect の設定。	BlackBerry Proxy インスタンスの Direct Connect を設定します。
BlackBerry Dynamics プロパティの設定（オンプレミスのみ）	組織の環境への展開を予定している BlackBerry Dynamics アプリのプロパティを設定します。
BlackBerry Dynamics アプリの通信設定（オンプレミスのみ）	組織の環境への展開を予定している BlackBerry Dynamics アプリの通信設定を、このアプリで使用される通信プロトコルを含めて設定します。
HTTP プロキシを介した BlackBerry Dynamics アプリデータの送信。	BlackBerry Proxy とアプリケーションサーバーとの間で HTTP プロキシを介して BlackBerry Dynamics アプリデータを送信するように UEM を設定します。
BlackBerry Dynamics アプリのトラフィックをルーティングする方法。	BlackBerry Dynamics アプリのトラフィックをルーティングするのに使用できるさまざまな方法の詳細です。
BlackBerry Dynamics アプリ用の Kerberos 認証の設定（オンプレミスのみ）	Kerberos の制限付き委任または Kerberos PKINIT を設定して、ユーザーの認証を簡素化します。

BlackBerry Dynamics アプリの展開と管理の詳細については、管理関連の資料の「BlackBerry Dynamics アプリの管理」を参照してください。

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はクラスターに追加されずに、割り当てられていないと見なされるため、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**］ > ［クラスター］をクリックします。
2. 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。 **b.** クラスターの名前を入力します。 **c.** ［保存］をクリックします。
BlackBerry Proxy クラスターの名前を変更します。	**a.** クラスター名をクリックします。 **b.** クラスター名を変更します。クラスターごとに固有の名前が必要です。 **c.** ［**OK**］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。 **b.** ［**BlackBerry Proxy** クラスター］ドロップダウンリストで、インスタンスを追加するクラスターを選択します。 **c.** ［保存］をクリックします。
空の BlackBerry Proxy クラスターを削除します。	**a.** そのクラスターの ✕ をクリックします。 **b.** ［削除］をクリックします。
クラスターのアプリプロキシを設定します。	**a.** クラスター名をクリックします。 **b.** ［グローバル設定を上書き］をクリックします。 **c.** 『BlackBerry Dynamics アプリプロキシの設定』を参照してください。
すべてのクラスターの PAC ファイルの更新をダウンロードします。	［**PAC** キャッシュを更新］をクリックします。
信頼されたルート証明書を指定して、サーバーから PAC ファイルをダウンロードします。	**a.** 管理コンソールからアクセスできるネットワークの場所に X.509 形式（*.cer、*.der）で証明書が保存されていることを確認してください。 **b.** メニューバーで、［設定］ **>** ［外部統合］ **>** ［信頼済み証明書］をクリックします。 **c.** ［**PAC** サーバー信頼］の横にある ＋ をクリックします。 **d.** ［参照］をクリックします。 **e.** 使用する証明書ファイルに移動して選択します。 **f.** ［開く］をクリックします。 **g.** 証明書の説明を入力します。 **h.** ［追加］をクリックします。
アクティベーションに使用できるように BlackBerry Proxy を有効にします（オンプレミスの UEM のみ）。	アクティベーションのために使用する BlackBerry Proxy インスタンスの［アクティベーションのための有効化］オプションを選択します。少なくとも 1 つのインスタンスを選択する必要があります。

ポート転送を使用した Direct Connect の設定

作業を始める前に：

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

1. 管理コンソールのメニューバーで、［設定］ > ［**BlackBerry Dynamics**］ > ［**Direct Connect**］をクリックします。
2. BlackBerry Proxy インスタンスをクリックします。
3. Direct Connect をオンにするには、［**Direct Connect** をオンにする］チェックボックスをオンにします。［**BlackBerry Proxy** ホスト名］フィールドで、ホスト名が正しいことを確認します。作成したパブリック DNS エントリがサーバーの FQDN と異なる場合は、代わりに外部 FQDN を指定します。
4. クラスター内のすべての BlackBerry Proxy インスタンスについて繰り返します。

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

BlackBerry Dynamics プロパティの設定

オンプレミスの UEM 環境では、BlackBerry Dynamics アプリのセキュリティ、動作、通信に関連するさまざまなプロパティを設定できます。

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. 次の操作のいずれかを実行します。

タスク	手順
BlackBerry Dynamics アプリのグローバルプロパティを変更する	• ［グローバルプロパティ］をクリックします。 • 必要に応じてプロパティを設定します。『BlackBerry Dynamics グローバルプロパティ』を参照してください。 • ［保存］をクリックします。

タスク	手順
特定の UEM サーバーの BlackBerry Dynamics プロパティを変更する	• ［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 UEM サーバーを選択します。 • 必要に応じてプロパティを設定します。『BlackBerry Dynamics プロパティ』を参照してください。 • ［保存］をクリックします。
BlackBerry Proxy インスタンスのプロパティを変更する	• ［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。 • 必要に応じてプロパティを設定します。『BlackBerry Proxy プロパティ』を参照してください。 • ［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。

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したりクライアント認証を行ったりするのにアップロードできる PKCS12 証明書のキーストアの使用期間（秒）。 このプロパティは読み取り専用で、変更できません。	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。	17317	はい

プロパティ	説明	デフォルト	再起動
cntmgmt.max.conns.above.limit	cntmgmt.max.conns.persec プロパティで設定されている制限を超過して許可される接続の最大数。 メモ： BlackBerry テクニカルサポートに相談せずにこの設定を変更しないでください。	3	はい
cntmgmt.max.conns.persec	コンテナ管理のための 1 秒あたりの最大接続数。 メモ： BlackBerry テクニカルサポートに相談せずにこの設定を変更しないでください。	30	はい
cntmgmt.max.active.sessions	コンテナ管理のアクティブなセッションの最大数。	10000	はい
cntmgmt.max.idle.count	コンテナ管理に許可されているアイドル接続の最大数。 メモ： BlackBerry テクニカルサポートに相談せずにこの設定を変更しないでください。	0	はい
cntmgmt.max.read.throughput	コンテナ管理の同時読み取り操作の最大数。 メモ： BlackBerry テクニカルサポートに相談せずにこの設定を変更しないでください。	500	はい
cntmgmt.max.write.throughput	コンテナ管理の同時書き込み操作の最大数。 メモ： BlackBerry テクニカルサポートに相談せずにこの設定を変更しないでください。	500	はい
cntmgmt.ssl.external.enable	外部コンテナ管理で SSL を有効にするかどうかを制御します。 このプロパティは読み取り専用で、変更できません。	オン	—
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。 このプロパティは読み取り専用で、変更できません。	オン	—

コンテナの複製

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、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、UEM で重複するコンテナを自動的に削除するかどうかを指定します。この設定を選択している場合は、他の重複するコンテナのプロパティよりも優先されます。	オン	いいえ
重複するコンテナを自動的に削除するジョブを有効にする（オン/オフ）	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）	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）	UEM で重複するコンテナを識別して削除するジョブを実行する間隔（秒）。	86400	いいえ
1 つのジョブで削除するコンテナの最大数	1 つのジョブでデバイスから削除できる非アクティブなコンテナの最大数。	100	いいえ

Kerberos 制約付き委任

プロパティ	説明	デフォルト	再起動
明示的な UPN を使用	Microsoft Active Directory または Office 365 の Exchange ActiveSync と統合されたサービスへの認証時に BlackBerry Dynamics アプリが明示的な UPN または暗黙的な UPN を使用するかどうかを指定します。組織の Active Directory は、環境に応じて、両方のオプションをサポートするか、いずれか 1 つのオプションのみをサポートする場合があります。	オフ	いいえ
KCD を有効にする（gc.krb5.enabled）	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、UEM が待機する時間（秒）。	60	はい
config.command.retry	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、UEM はタスクを実行しません。	900	はい
gc.entgw.report.userinfo	ユーザーの表示名が BlackBerry Dynamics NOC に報告されるかどうかを指定します。	オフ	いいえ
policy.compliance.interval	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取得する頻度（分）。	1440	はい

非アクティブなコンテナの消去

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。UEM は、コンテナがデフォルトの 90 日間 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、UEM ログファイルに記録されます。

認証委任が設定されているコンテナは、このプロセスによって消去されません。

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）	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）	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）	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
gc.purge.dbJobs サーバージョブの消去	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
gc.purge.dbJobs.interval サーバージョブの消去間隔	［サーバージョブの消去］がオンになっている場合に、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

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）	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

プロパティ	説明	デフォルト	再起動
領域 - Active Directory（gc.krb5.realm）	Kerberos アカウントの領域。	設定なし	はい

BlackBerry Proxy プロパティ

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

プロパティ	説明	デフォルト	再起動
gp.gps.max.sessions	アクティブなセッションの最大数	15000	—
gp.gps.dns.server.ttl.ms	DNS サーバーの応答を待機する時間（ミリ秒）。	1800000	—
gp.gps.server.flowcontrol	サーバーでフロー制御が有効になっているかどうかを指定します。	オフ	—
gp.gps.tcp.keepalive	サーバーで TCP キープアライブが有効になっているかどうかを指定します。	オフ	—
gp.gps.unalias.hostname	このオプションを選択した場合、BlackBerry Proxy は、アプリサーバーの IP アドレスを使用したリバース DNS 参照を使用します。 このオプションを選択しない場合、BlackBerry Proxy は、DNS 参照にアプリサーバーのホスト名を使用します。	オフ	はい
gps.directconnect.supported.ciphers	BlackBerry Direct Connect を介して行われたブリッジングと通信を暗号化する暗号スイートを追加または変更します。 独自のプロキシサーバーを Direct Connect 用に設定し、クライアントデバイスと BlackBerry Proxy サーバーとの間に配置することもできます。独自のプロキシサーバーを追加した場合は、BlackBerry Proxy サーバーの暗号が独自のプロキシサーバーで必要な暗号と対応していることを確認してください。 すべての暗号は、Java でサポートされている必要があります。	UI に表示	はい
gp.directconnect.supported.protocols	システムの直接接続ブリッジでサポートする暗号化プロトコルを追加または変更します。	TLSv1、TLSv1.1、TLSv1.2	はい

プロパティ	説明	デフォルト	再起動
gp.eacp.command.service.nslookup.srv.ldap	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 プロトコルを介して LDAP サービスを提供します。クライアントは、DNS に _ldap._tcp.DnsDomainName 形式のレコードを照会することによって、LDAP サーバーを検索します。 このオプションを選択した場合、BlackBerry Proxy は、指定されたサービスホスト名の nslookup に LDAP を使用します。 このオプションを選択しない場合、BlackBerry Proxy は、指定したサービスホスト名を使用して、リバース DNS 参照を直接使用します。	オフ	はい
gc.mdc.hb.timeout	ハートビートタイムアウトを指定します。	0	—
gp.server.secure.ciphers	BlackBerry Proxy サーバーを介して行われた通信を暗号化する暗号スイートを追加または変更します。 すべての暗号は、Java でサポートされている必要があります。	UI に表示	—
gp.server.secure.protocols	BlackBerry Proxy サーバーでサポートする暗号化プロトコルを追加または変更します。	TLSv1.2	—

BlackBerry Dynamics アプリの通信設定

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

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

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

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

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

BlackBerry Proxy で PAC ファイルを使用する場合の考慮事項

考慮事項	詳細
サポートされている PAC ファイルディレクティブ	• DIRECT • PROXY（HTTPS プロキシとして処理。つまり HTTP CONNECT を使用して確立された接続） • HTTPS（HTTP CONNECT を使用して確立された接続）
サポートされていない PAC ファイルディレクティブ	次の場合、接続エラーが発生します。 • SOCKS • SOCKS4 • SOCKS5 • HTTP • BlackBerry Access によって定義されたカスタム「NATIVE」ディレクティブ BLOCK ファイルディレクティブは DIRECT として扱われます。
制限事項	• dnsDomainIs 関数には、「_」および「*」の文字を含めることはできません。 • shExpMatch 関数には、「[0-9]」、「?」、「/^d」、または「d+」の表現を含めることはできません。 • URI からパスとクエリーを削除するオプションはサポートされていません。
PAC キャッシュ	BlackBerry Proxy は、パフォーマンスを向上させるために PAC ファイルをダウンロードしてキャッシュします。PAC キャッシュは 24 時間ごとに更新されます。 キャッシュを手動で更新する場合は、管理コンソールで［設定］>［インフラストラクチャ］>［BlackBerry Router とプロキシ］>［グローバル設定］の順に移動し、［PAC キャッシュを更新］をクリックします。

BlackBerry Dynamics アプリプロキシの設定

1. UEM の使用環境に応じた手順に従います。

環境	タスク
オンプレミスの UEM	UEM 管理コンソールで、次のいずれかを実行します。 • グローバルアプリプロキシを設定する場合は、［設定］ > ［インフラストラクチャ］ > ［**BlackBerry Router** とプロキシ］の順にクリックし、［グローバル設定］を展開します。 • クラスターのアプリプロキシを設定する場合は、［設定］ > ［**BlackBerry Dynamics**］ > ［クラスター］の順にクリックします。クラスターの名前をクリックし、［グローバル設定を上書き］チェックボックスをオンにします。 • サーバーの手動アプリプロキシを設定する場合は、［設定］ > ［インフラストラクチャ］ > ［**BlackBerry Router** とプロキシ］の順にクリックします。サーバーを開き、［グローバル設定を上書き］チェックボックスをオンにします。サーバーのグローバルプロキシ設定を上書きする場合、PAC ファイルはサポートされないことに注意してください。
UEM Cloud	BlackBerry Connectivity Node 管理コンソールで、［設定］ > ［**BlackBerry Router** とプロキシ］ > ［グローバル設定］をクリックします。

2. 適切なオプションを選択し、必要な手順を完了します。

オプション	手順
手動 HTTP プロキシを有効にする	**a.** 適切なプロキシ設定を選択します。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、＋をクリックしてサーバーを追加します。 **b.** プロキシサーバーのアドレスおよびそのサーバーが待機するポート番号を指定します。 **c.** プロキシサーバーが認証を必要とする場合は、［認証を使用］チェックボックスをオンにして認証資格情報を指定します。
PAC を有効にする	［**PAC URL**］フィールドに、PAC ファイルの URL を入力します。 PAC ファイルで指定されたプロキシに認証が必要な場合は、［プロキシ認証をサポート］チェックボックスをオンにして、認証資格情報を指定します。プロキシ認証では、エンドユーザー認証資格情報はサポートされていません。

3. ［保存］をクリックします。

BlackBerry Dynamics アプリのトラフィックをルーティングする方法

BlackBerry UEM には、BlackBerry Dynamics トラフィックのルーティング方法を制御できるオプションがいくつかあります。デフォルトでは、すべての BlackBerry Dynamics アプリのトラフィックがインターネットに直接

ルーティングされ、Web プロキシサーバーは設定されません。本セクションでは、ルーティング全体に影響する設定のみについて説明します。

BlackBerry Dynamics アプリのルーティングは、次の設定で変更できます。

設定	詳細
割り当てられる BlackBerry Dynamics 接続プロファイル	• デフォルトの BlackBerry Dynamics 接続プロファイルで設定されている唯一の項目は、［デフォルトの許可されたドメインルートタイプ］であり、［直接］に設定されています。 • デフォルトの BlackBerry Dynamics 接続プロファイルを使用している場合、BlackBerry Dynamics アプリから内部サーバーまたはドメインにアクセスすることはできません。デフォルトの接続プロファイルを変更するか、新しい接続プロファイルを作成すると、内部サーバーへの接続を許可できます。 • 詳細については、管理関連の資料の「BlackBerry Dynamics 接続プロファイルの作成」を参照してください。

BlackBerry Proxy Web プロキシサーバーの設定	• デフォルトでは、BlackBerry Proxy は Web プロキシサーバーを使用しないように設定されています。各 BlackBerry Proxy サーバーはインターネットに直接接続して接続を確立しようとします。これは、アプリケーションサーバーのトラフィックと BlackBerry Dynamics NOC 接続の両方に適用されます。
	• BlackBerry Proxy の設定の詳細については、「HTTP プロキシを介した BlackBerry Dynamics アプリデータの送信」を参照してください。
	• BlackBerry Dynamics 接続プロファイルでは、BlackBerry Dynamics アプリが BlackBerry Proxy を使用してファイアウォールからアクセスできるサーバーを指定できます。詳細については、管理関連の資料の「BlackBerry Dynamics 接続プロファイルの作成」を参照してください。
	• BlackBerry Proxy を介したトラフィックのルーティングによって、デバイス上の Web ブラウザーおよび BlackBerry Dynamics アプリが、BlackBerry Proxy が到達可能なファイアウォールの内側にある任意のサーバーに接続できます。また、BlackBerry Dynamics アプリと組織のリソース間のデータトラフィックを簡単に監視できます。
	• BlackBerry Proxy サーバー経由でデータをルーティングする場合は、次の点を考慮してください。
	  • インターネット上のサーバーへの接続の確立には時間がかかる場合があります。
	  • Web プロキシを使用して外部サイトへのアクセスを許可し、特定のサイトを制限するようにプロキシで設定されている設定を使用する場合、［すべてのトラフィックをルーティング］オプションを選択するときに、BlackBerry Proxy でプロキシのプロパティを設定する必要もあります。そうしないと、アプリは外部サイトにアクセスできません。
	  • BlackBerry Access は、許可サイトを決定する PAC ファイルで設定できます。この場合、PAC ファイルによってプロキシ設定が決定されます。詳細については、『BlackBerry Access 管理ガイド』を参照してください。

設定	詳細
アプリ固有の設定	• アプリを特定のサーバーに接続するには、アプリ固有の設定が必要な場合があります（Microsoft Exchange Server の URL を使用して設定された BlackBerry Work など）。BlackBerry Dynamics アプリのドキュメントを確認して、どのアプリ設定を適用するかを把握してください。 • BlackBerry Access および一部のサードパーティアプリケーションでは、アプリレベルの Web プロキシサーバー設定が可能です。BlackBerry Access のデフォルト設定には、適用される Web プロキシサーバー設定はありません。 • アプリサーバーとは、Microsoft Exchange Server の URL、BEMS の URL、Skype for Business の URL、BlackBerry Access が参照するすべての URL など、BlackBerry Dynamics アプリが接続するサーバーです。BlackBerry Dynamics NOC と BlackBerry UEM Core サーバーはアプリサーバーではありません。

BlackBerry Proxy サーバーに BlackBerry Dynamics 接続プロファイルおよび Web プロキシ設定を行って割り当てると、BlackBerry Dynamics 接続プロファイルが常に最初にチェックされます。トラフィックが BlackBerry Proxy サーバーに到達すると、BlackBerry Proxy サーバーに設定されている PAC または Web プロキシサーバーの設定が接続について評価されます。BlackBerry Proxy サーバーで Web プロキシを設定すると、BlackBerry Proxy でインターネットに送信するトラフィックをどのように処理するかを制御できますが、デバイス上の BlackBerry Dynamics アプリによる接続の評価には影響しません。

BlackBerry Dynamics トラフィックのルーティングシナリオの例

次のシナリオは、一般的な設定の例です。

シナリオ	**BlackBerry Dynamics** 接続プロファイル	**BlackBerry Proxy** 用の **Web** プロキシの設定	アプリ固有の設定
BlackBerry Proxy を介してトラフィックを特定のサーバーまたはドメインにルーティングする 一部の内部アプリサーバーは BlackBerry Dynamics アプリにアクセスできる必要があるものの、一般的なパブリックサーバーへのトラフィックは直接アクセスのままでよいシナリオに適しています。	• デフォルトの許可されたドメインルートタイプ：直接 • 許可されたドメイン：BlackBerry Proxy を介してルーティングする内部ドメインを追加し、クラスターを選択 • サーバーの追加：必要に応じて特定のサーバー名を追加し、クラスターを選択	設定は不要です。	設定は不要です。

シナリオ	**BlackBerry Dynamics** 接続プロファイル	**BlackBerry Proxy** 用の **Web** プロキシの設定	アプリ固有の設定
すべてのトラフィックを BlackBerry Proxy 経由でルーティングしてから、Web プロキシサーバー経由でルーティングする 仕事用アプリからのすべてのトラフィックを内部でルーティングする必要がある組織に適しています。	デフォルトで許可されるドメインルートタイプ：BlackBerry Proxy クラスター	手動の Web プロキシサーバー設定または PAC ファイルを使用します。	設定は不要です。
ほとんどのアプリのトラフィックを内部的にルーティングするが、BlackBerry Access を使用した Web ブラウジング専用のプロキシサーバーを設定する アプリケーションのトラフィックを内部でルーティングする必要がある一方で、ブラウザーのトラフィックは Web プロキシサーバー経由でルーティングする必要がある組織に適しています。	• デフォルトの許可されたドメインルートタイプ：直接 • 許可されたドメイン：BlackBerry Proxy を介してルーティングする内部ドメインを追加し、クラスターを選択 • サーバーの追加：必要に応じて特定のサーバー名を追加し、クラスターを選択	BlackBerry Proxy サーバーがインターネットに直接アクセスできない場合、または BlackBerry Dynamics NOC 接続にプロキシが必要な場合は、必要に応じて Web プロキシサーバーを設定します。	BlackBerry Access のアプリ設定で、［Web プロキシを有効にする］および［プロキシ自動設定を使用］を選択します。

BlackBerry Dynamics アプリ用の Kerberos 認証の設定

BlackBerry Dynamics アプリは、オンプレミスの BlackBerry UEM 環境で Kerberos 制約付き委任（KCD）および Kerberos PKINIT をサポートします。BlackBerry Dynamics アプリでは、KCD または Kerberos PKINIT のどちらか一方をサポートできますが、両方はサポートできません。

Kerberos 認証	説明
KCD	KCD を使用すると、ユーザーはネットワーク資格情報を入力しなくても、企業リソースにアクセスできます。KCD では、ユーザーの資格情報を含まないキーで暗号化および復号化されるサービスチケットを使用します。 KCD が設定されている場合、BlackBerry Dynamics アプリは UEM に認証を委任し、その代理として仕事用リソースへのアクセスを要求してもらいます。UEM が使用するアカウントが特定のサービスに対してのみ信頼されるように設定することにより、ユーザーがアクセスできるネットワークリソースを制限できます。 たとえば、KCD が設定されておらず、アプリが mypage.mydomain.com などのリソースを要求した場合、アプリはユーザーに資格情報の入力を求めます。KCD を設定すると、BlackBerry Dynamics インフラストラクチャが認証を処理するため、ユーザーは資格情報の入力を求められません。 「BlackBerry Dynamics アプリの KCD を設定するための前提条件」および「BlackBerry Dynamics アプリ用 KCD の設定」を参照してください。
Kerberos PKINIT	Kerberos PKINIT 認証は、BlackBerry Dynamics アプリと Windows KDC の間で信頼を直接確立します。ユーザー認証は、Microsoft Active Directory 証明書サービスによって発行された証明書に基づきます。 『BlackBerry Dynamics アプリでの Kerberos PKINIT のサポート要件』を参照してください。

BlackBerry Dynamics アプリの KCD を設定するための前提条件

項目	説明
Active Directory ポート	Active Directory サービスのポート 88 は、すべての UEM サーバーからアクセスできる必要があります。
Kerberos 環境	Kerberos 環境には、次のコンポーネントが含まれている必要があります。 • Microsoft Active Directory サーバー：Windows ネットワークに関連付けられているすべてのユーザーとコンピューターを認証および承認するディレクトリサービス • Kerberos キー配布センター（KDC）：Active Directory ドメイン内のユーザーとコンピューターにセッションチケットとキーを提供する Active Directory サーバー上の認証サービス
サービスプリンシパル名（SPN）	BlackBerry Enterprise Mobility Server を含むすべての HTTP サービスの SPN を作成します。デバイスがアクセスできるようにするターゲットリソースごとに SPN を設定する必要があります。 SPN の作成および変更方法の詳細については、「Kerberos 接続のサービスプリンシパル名の登録」を参照してください。

項目	説明
複数レルム Kerberos 環境	• 各 Kerberos レルムには少なくとも 1 つの UEM Core をインストールする必要があります。レルム間のリソース委任はサポートされていないため、UEM はリソースと同じ Kerberos レルム内に存在する必要があります。 • 複数レルム KCD を設定する前に、単一レルム KCD が動作していることを確認します。 • すべての信頼は、双方向で推移的なフォレストの信頼である必要があります。 • UEM Core インスタンスと Microsoft SQL Server データベースの間には、最大 5 ミリ秒の遅延時間を確保してください。

BlackBerry Dynamics アプリ用 KCD の設定

作業を始める前に：

- BlackBerry Dynamics アプリの KCD を設定するための前提条件 を確認します。
- BlackBerry Docs 用に KCD を設定する場合は、BlackBerry Enterprise Mobility Server 関連の資料の「Docs サービスの Kerberos 制約付き委任の設定」を参照してください。

1. Kerberos サービスアカウントを SPN にマッピングするには、Active Directory サーバーで管理者としてコマンドプロンプトを開き、ホストサーバー名、ドメイン、および Kerberos サービスアカウントを指定して以下のように入力します。Kerberos サービスアカウントは、UEM で KCD サービスを設定するサービスアカウント名（gc.krb5.principal.name）です。このアカウントは、UEM サービスアカウントと同じである必要はありませんが、同じでもかまいません。

   ```
   setspn –s GCSvc/<UEM_Core_host_machine> <domain>\<Kerberos_service_account>
   ```

   例：

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

2. 新しい Kerberos keytab ファイルを生成して Kerberos アカウントパスワードを設定するには、次の手順に従います。
   a) KDC サーバーで、コマンドプロンプトを開きます。
   b) 次のコマンドを実行し、適切な値を指定します。

      ```
      ktpass -out <output_filename>.keytab -mapuser
       <Kerberos_account>@<KERBEROS_REALM_IN_ALL_CAPS> -princ
       <Kerberos_account>@<KERBEROS_REALM_IN_UPPERCASE> /ptype KRB5_NT_PRINCIPAL -
      pass <Kerberos_account_password>
      ```

   c) 新しい keytab ファイルを、同じ KCD 管理者アカウントを使用するすべての UEM サーバーにコピーします。
3. Active Directory ユーザーオブジェクトグループメンバーシップの列挙を有効にします。詳細については、「補足説明 B：Active Directory の特権アカウントとグループ」を参照してください。
4. 各 UEM サーバーで、次の手順に従って UEM サービスアカウントの権限を設定し、Kerberos システムにユーザー資格情報を送信できるようにします（これは、SPN が関連付けられているのと同じアカウントです）。

a) Microsoft 管理コンソールで、［ローカルセキュリティポリシー］ > ［ローカルポリシー］ > ［ユーザー権限の割り当て］の順に移動します。
b) ［オペレーティングシステムの一部として機能］のプロパティを開き、［ユーザーまたはグループの追加］をクリックします。
c) サービスアカウントの名前を入力し、［**OK**］をクリックします。

5. UEM 管理コンソールのメニューバーで、［設定］ > ［**BlackBerry Dynamics**］ > ［グローバルプロパティ］をクリックします。
6. ［明示的な **UPN** を使用］チェックボックスをオンにします。
7. ［**KCD** を有効にする］チェックボックスをオンにします。
8. ［保存］をクリックします。
9. メニューバーで、［設定］ > ［**BlackBerry Dynamics**］ > ［プロパティ］の順にクリックし、サーバー名をクリックします。
10. ［**KDC** の完全修飾名（**gc.krb5.kdc**）］フィールドに、KDC の完全修飾名を入力します。通常、Active Directory ドメインコントローラーの FQDN に対応します。
11. ［**keytab** ファイルの場所（**gc.krb5.keytab.file**）］フィールドに、keytab ファイルの場所を入力します。パス名にはスラッシュを使用します。
12. ［**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**）］フィールドに、KCD サービスが使用するサービスアカウントの名前を入力します。
13. ［領域 **- Active Directory**（**gc.krb5.realm**）］フィールドに、Active Directory 領域の名前をすべて大文字で入力します。
14. 環境で複数の Kerberos ドメインとの CAPATH 信頼関係が必要な場合は krb5.conf ファイルを作成します。［**GC** サーバー上の **krb5.config** ファイル（**gc.krb5.config.file**）の場所］フィールドに、ファイルの場所を入力します。
15. ［保存］をクリックします。

BlackBerry Dynamics アプリでの Kerberos PKINIT のサポート要件

BlackBerry UEM は、PKI 証明書を使用した BlackBerry Dynamics ユーザー認証に Kerberos PKINIT をサポートしています。BlackBerry Dynamics アプリで Kerberos PKINIT を使用する場合、組織で次の要件を満たす必要があります。

項目	要件
KDC	• KDC ホストを、割り当てられた BlackBerry Dynamics 接続プロファイルの許可されたドメインのリストに追加する必要があります。詳細については、管理関連の資料の「BlackBerry Dynamics 接続プロファイルの作成」を参照してください。 • KDC ホストは、TCP ポート 88（Kerberos デフォルトポート）で待機する必要があります。 • KDC は、DNS に A レコード（IPv4）または AAAA レコード（IPv6）を必要とします。 • BlackBerry Dynamics は、UDP を介した KDC をサポートしていません。 • BlackBerry Dynamics は、正しい KDC の検索に、Kerberos 設定ファイル（krb5.conf など）を使用しません。 • KDC は、クライアントに別の KDC ホストを参照させることができます。BlackBerry Dynamics は、参照される KDC ホストが BlackBerry Dynamics 接続プロファイルの許可されたドメインのリストに追加されている限り、照会に従います。 • KDC は、別の KDC ホストから BlackBerry Dynamics へ TGT を透過的に取得できます。 • Kerberos 制約付き委任を無効にする必要があります。

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

クライアント証明書	• 証明書の最小キー長は 2,048 バイトにする必要があります。 • 証明書の拡張キー使用法プロパティは Microsoft スマートカードログオン（1.3.6.1.4.1.311.20.2.2）である必要があります。 • クライアント証明書には、オブジェクト ID szOID_NT_PRINCIPAL_NAME 1.3.6.1.4.1.311.20.2.3 のサブジェクト別名にユーザープリンシパル名（user@domain.com など）が含まれている必要があります。 • ユーザーが複数のクライアント証明書を発行された場合、正しい証明書が使用されるように、ユーザープリンシパル名のドメインは、アクセスされているリソースのドメインと一致する必要があります。 • 証明書が有効である必要があります。上記のサーバーに照らして確認してください。

BlackBerry UEM と Cisco ISE を統合

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

Cisco ISE とオンプレミスの BlackBerry UEM 間の接続を作成できるため、Cisco ISE は UEM 上でアクティブ化されたデバイスに関するデータを取得できるようになります。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 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 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。また、管理者はデバイスのロック、デバイスからの仕事用データの削除、デバイスからのすべてのデータの削除なども実行できます。ネットワークアクセスおよびデバイス制御の詳細については、「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」を参照してください。

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 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	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。

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。

アクション	説明
デバイスデータを表示する	BlackBerry UEM に関連付けられたデバイスに関する情報を表示できます。次の情報が表示されます。 • MAC アドレス • デバイスが UEM に準拠しているかどうか • デバイスデータが暗号化されているかどうか • デバイスが UEM でアクティブ化（登録）されているかどうか • デバイスがルート化または脱獄されているかどうか • デバイスがパスワードを使用しているかどうか • 製造元 • 機種 • シリアル番号 • OS バージョン
NAC ポリシーを設定する	デバイスが仕事用 Wi-Fi または VPN アクセスポイントに接続できるかどうかを制御する、アクセスポリシーを設定します。たとえば、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	ユーザーのデバイスをロックします。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。UEM は、IT 管理コマンドを使用してデバイスをロックします。ユーザーは、ロックを解除するために、デバイスパスワードを入力する必要があります。 デバイスユーザーが My Device portal を使用してこの操作を実行することもできます。
仕事用データを削除する	デバイスから、ユーザーの個人用データやアプリをそのまま残して、仕事用データのみと仕事用アプリを削除します。この機能は、ユーザーのデバイスが紛失したり、ユーザーの退職があったりした場合に役立ちます。UEM は、IT 管理コマンドを使用して仕事用データを削除します。 デバイスユーザーが My Device portal を使用してこの操作を実行することもできます。
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にあったり、デバイスが別のユーザーに渡されたりした場合に役立ちます。UEM は、IT 管理コマンドを使用してすべてのデバイスデータを削除します。 デバイスユーザーが My Device portal を使用してこの操作を実行することもできます。

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。
サポートされる OS	UEM がサポートする、デスクトップ向け Windows 10 を除くすべてのオペレーティングシステム。
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 UEM 待機ポート 18084 を使用します。 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 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。
管理者アカウント	Cisco 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 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ロールとエンタープライズ管理者ロールには、これらの権限があります。また、これらの権限を持つカスタムロールを作成することもできます。詳細については、管理関連の資料の「管理者の作成」を参照してください。

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、UEM および 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。最新の Cisco ISE ドキュメントについては、Cisco ISE の設定ガイドを参照してください。

作業を始める前に： ブラウザーで **https://<*server_name*>:<*BlackBerry_Web_Services_port*>/enterprise/admin/util/ws?wsdl** に移動します。この *<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。ブラウザーを使用して 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。

1. Cisco ISE 管理コンソールにログインします。
2. BlackBerry Web Services 証明書を Cisco ISE の信頼済み証明書ストアにインポートします。クライアント認証と syslog を信頼するオプションと、Cisco サービスの認証を信頼するオプションを選択します。
3. 外部 MDM サービスを追加し、UEM ドメインの FQDN または IP アドレス、ポート（デフォルトは 18084）、UEM 管理者アカウントの資格情報など、UEM インスタンスの詳細を指定します。
4. ポーリング間隔では、デバイスデータについて Cisco ISE が UEM をポーリングする間隔を分単位で指定します。デフォルト値を使用することをお勧めします。

   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 UEM をポーリングしません。
5. UEM への接続を有効にしてテストします。

接続が確立されると、UEM のディクショナリ属性を Cisco ISE 管理コンソールで確認できます。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。

- ワイヤレス LAN コントローラーで ACL を設定します。
- UEM でアクティブ化されていないデバイスが仕事用ネットワークにアクセスしようとした場合に、そのデバイスを BlackBerry UEM Self-Service コンソールにリダイレクトする認証プロファイルを設定します。ユーザーが 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。Cisco ISE により登録ページへリダイレクトされた場合は、UEM 管理者に問い合わせるようユーザーに指示してください。
- UEM でアクティブ化されていないデバイスまたは UEM に準拠していないデバイスを、Cisco ISE がどのように処理するかを決定する認証ポリシールールを設定します。

ダークサイト環境の UEM に対する Knox StrongSwan を使用した VPN の設定

ダークサイト環境の UEM で、Samsung Knox デバイスが社内のサーバーおよびリソースにアクセスできるように、組織の環境への VPN アクセスを設定する必要があります。ダークサイト環境での UEM の詳細については、インストール関連の資料の「ダークサイト環境での BlackBerry UEM のインストールまたはアップグレード」を参照してください。

作業を始める前に： Knox Service Plugin および Android VPN Management for Knox StrongSwan アプリをダウンロードし、.apk ファイルを内部アプリの共有ネットワークの場所に追加します。

1. Knox Service Plugin および Android VPN Management for Knox StrongSwan アプリをアプリリストに追加します。
2. Knox Service Plugin アプリを選択し、＋をクリックしてアプリの設定オプションを設定します。
   a) ［**VPN** プロファイル］で、［**Knox** に組み込まれた **VPN**］を選択します。
   b) ［**StrongSwan** の **Knox** に組み込まれた **VPN** のパラメーター］で、次のオプションを設定します。
      - ［認証の種類］を「ipsec_ike2_rsa」に設定します。
      - ［ユーザー証明書のエイリアス］を、ユーザー名の後ろに「_1 [Knox]」を追加して設定します。ユーザー名には変数を使用できます（`%UserFirstName% %UserLastName% _1 [Knox]` など）。
      - ［**CA** 証明書のエイリアス］を、ユーザー名の後ろに「[Knox]」を追加して設定します。ユーザー名には変数を使用できます（`%UserFirstName% %UserLastName% [Knox]` など）。
3. アプリをユーザーに割り当てます。
4. CA 証明書のプロファイルを作成して VPN サーバーの証明書をデバイスに送信し、ユーザーに割り当てます。
5. 各ユーザーに VPN クライアントの証明書を追加します。

商標などに関する情報

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Published in Canada