BlackBerry UEM

デバイスのアクティブ化

12.20

Contents

BlackBerry UEM によるデバイスのアクティベーション

管理者またはユーザーがデバイスをアクティブ化すると、デバイスは BlackBerry UEM と関連付けられます。これにより、デバイスの設定を管理および割り当て、デバイス上の仕事用データにユーザーがアクセスできるようになります。

デバイスがアクティブ化されたら、IT ポリシーとプロファイルを送信して、機能を制御および設定し、仕事用データのセキュリティを管理できます。ユーザーがインストールするアプリを割り当てることもできます。選択したアクティベーションタイプがどの程度の制御を許可するかに応じて、アクセスの特定データへの制限、リモートでのパスワードの設定、デバイスのロック、またはデータの削除を実行して、デバイスを保護することもできます。

組織が所有するデバイスおよびユーザーが所有するデバイスのそれぞれの要件に適合するようにアクティベーションタイプを割り当てることができます。アクティベーションタイプによって、すべてのデータに対するフルコントロール権限から仕事用データのみの特定の制御権限まで、デバイス上の仕事用データと個人用データを制御できる度合いは異なります。

ユーザーがデバイスをアクティブ化できるように UEM を設定するには、次の操作を実行します。

手順	アクション
1	アクティブ化するデバイスごとに、UEM ライセンスが使用可能であることを確認します。iOS、iPadOS、および Android デバイスの場合は、最新バージョンの BlackBerry UEM Client が適切なアプリストアからデバイスにインストールされていることを確認します。
2	デフォルトのアクティベーションの設定。
3	UEM 環境およびデバイスユーザーに関連する情報を確認します。 • Android Enterprise および Android Management アクティベーションのサポート • Windows 10 アクティベーションのサポート • iOS および iPadOS デバイスでの Apple ユーザー登録のサポート • Samsung Knox DualDAR のサポート • Android ゼロタッチ登録のサポートの構成 • Knox Mobile Enrollment を使用した複数のデバイスのアクティブ化 • DEP に登録されている iOS デバイスのアクティベーション • Apple Configurator 2 を使用した iOS デバイスのアクティブ化
4	アクティベーションメールのテンプレートを更新します。
5	アクティベーションプロファイルを作成し、それをユーザーアカウントまたはユーザーグループに割り当てます。

手順	アクション
6	アクティベーションメールを複数のユーザーに送信、アクティベーションメールを特定のユーザーに送信するか、UEM Self-Service でのユーザーによるアクティベーションパスワードの設定を許可します。
7	ユーザーにアクティベーション手順を送信します。 • Android デバイスのアクティベーション • iOS デバイスのアクティベーション • BlackBerry UEM Self-Service による macOS または Apple TV デバイスのアクティブ化 • Windows 10 タブレットまたはコンピューターのアクティベーション

アクティベーションタイプ：iOS デバイス

アクティベーションタイプ	説明
MDM 制御	このアクティベーションタイプは、iOS および iPadOS によって利用可能なデバイス制御権限を使用して基本的なデバイス管理を提供します。個別の仕事用領域はデバイスにインストールされず、仕事用データのセキュリティも追加されません。 コマンドと IT ポリシーを使用してデバイスを制御できます。アクティベーションの実行時に、ユーザーはデバイスにモバイルデバイス管理プロファイルをインストールする必要があります。 BlackBerry UEM がデバイス ID によるアクティベーションを制限できるかどうかを指定するには、［承認されたデバイス ID のみを許可する］を選択します。

アクティベーションタイプ	説明
ユーザーのプライバシー	このアクティベーションタイプでは、ユーザーの個人データがプライベートの状態であることを確認しながら、デバイスの基本的な制御を提供します。別個のコンテナはデバイスにインストールされず、仕事用データのセキュリティも追加されません。デバイスは、［電話を探す］や［ルートの検出］などのサービスを利用することができますが、管理者はデバイスポリシーを制御できません。 メモ：SIM ベースのライセンスの場合は、アクティベーションプロファイルで［SIM ベースのライセンスを有効にするには、SIM カードとデバイスのハードウェア情報へのアクセスを許可します］を選択する必要があります。ユーザーは、SIM カードとデバイスハードウェアの情報のみにアクセスできる MDM プロファイルをインストールする必要があります。これらの情報は、適切な SIM ライセンス（ICCID、IMEI など）が利用可能であるかどうかを確認するために必要です。 このアクティベーションタイプは Apple TV デバイスではサポートされません。 ユーザーのプライバシー アクティベーションを許可する場合は、組織のニーズに基づいて、デバイスで管理するプロファイルを選択します。次のいずれかを選択できます。 • SIM ベースのライセンスを有効にするには、SIM カードとデバイスのハードウェア情報へのアクセスを許可します：このオプションは、UEM が SIM カードと ICCID や IMEI などのデバイスハードウェア情報にアクセスして、適切な SIM ライセンスが使用可能なことを確認できるかどうかを指定します。 • アプリの管理を許可する：このオプションでは、デバイスの仕事用アプリをインストールするか削除するかを指定します。ユーザーの詳細画面には、インストール済みの仕事用アプリが一覧で表示されます。アプリのショートカットを許可するかどうかを指定することもできます。 • IT ポリシーの管理を許可する：このオプションでは、IT ポリシールールの限定されたセットをデバイスに適用するかどうかを指定します（パスワードポリシー、スクリーンショットの許可、管理されている送信元から管理されていない送信先にドキュメントを送信する許可、管理されていない送信元から管理されている送信先にドキュメントを送信する許可）。 • メールプロファイル管理を許可する：このオプションでは、ユーザーに割り当てられているメールプロファイル設定をデバイスに適用するかどうかを指定します。 • Wi-Fi プロファイル管理を許可する：このオプションでは、ユーザーに割り当てられている Wi-Fi プロファイル設定をデバイスに適用するかどうかを指定します。 • VPN プロファイル管理を許可する：このオプションでは、ユーザーに割り当てられている VPN プロファイル設定をデバイスに適用するかどうかを指定します。

アクティベーションタイプ	説明
ユーザーのプライバシー - ユーザー登録	このアクティベーションタイプは、iOS および iPadOS デバイスに使用して、ユーザーデータがプライベートに保持され、仕事用データから分離されていることを確認できます。仕事用アプリとネイティブ Notes、iCloud ドライブ、メール（添付ファイルとメール本文全体）、カレンダ（添付ファイル）、および iCloud Keychain アプリ用の個別の仕事用領域がデバイスにインストールされます。 このアクティベーションタイプにより、アプリ管理、IT ポリシー管理、メールプロファイル、Wi-Fi プロファイル、per-app VPN が有効になります。管理者は、個人データに影響を与えることなく、仕事用データを管理（たとえば、仕事用データの削除）ができます。 このアクティベーションタイプは、非監視対象の iPhone および iPad デバイスでサポートされます。
BlackBerry 2FA 専用のデバイス登録	このアクティベーションタイプは、UEM によって管理されないデバイス向けの BlackBerry 2FA ソリューションをサポートします。このアクティベーションタイプではデバイス管理や制御は提供されませんが、デバイスは BlackBerry 2FA 機能を使用できます。このアクティベーションタイプを使用するには、BlackBerry 2FA プロファイルをユーザーにも割り当てる必要があります。 デバイスがアクティベーションされた場合、管理コンソールで限定されたデバイスの情報を表示したり、コマンドを使用してデバイスを無効にしたりできます。 このアクティベーションタイプは Microsoft Active Directory ユーザーのみサポートします。Apple TV デバイスではサポートされていません。 詳細については、BlackBerry 2FA 関連の資料を参照してください。

アクティベーションタイプ：Android デバイス

Android デバイスの場合、複数のアクティベーションタイプの選択とランク付けを行って、BlackBerry UEM が目的のデバイスに最適なアクティベーションタイプを確実に割り当てるように設定できます。たとえば、［仕事用と個人用 - ユーザーのプライバシー （Samsung Knox）］を第 1 位、［仕事用と個人用 - ユーザーのプライバシー （Android Enterprise）］を第 2 位とランク付けした場合、Samsung Knox Workspace をサポートするデバイスは、第 1 位のアクティベーションタイプを受け取り、Samsung Knox Workspace をサポートしないデバイスは第 2 位を受け取ります。

Android Management デバイス

Android Management アクティベーションタイプのある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。

アクティベーションタイプ	説明
仕事用と個人用 - ユーザーのプライバシー（仕事用プロファイルがある Android Management）	このアクティベーションタイプでは、個人用データのプライバシーが保護されますが、コマンドと IT ポリシールールを使用して仕事用データを管理できます。仕事用データと個人用データを分離する仕事用プロファイルがデバイスで作成されます。仕事用データと個人用データは両方とも、暗号化とパスワード認証によって保護されます。
仕事用と個人用 - フルコントロール（仕事用プロファイルがある Android Management 完全管理のデバイス）	このアクティベーションタイプでは、コマンドと IT ポリシールールを使用してデバイス全体を管理できます。仕事用データと個人用データを分離する仕事用プロファイルがデバイスで作成されます。仕事用領域のデータはすべて暗号化と何らかの認証方式を使用して保護されます。認証方式には、パスワード、PIN、パターン、指紋などがあります。このアクティベーションタイプでは、UEM ログファイルで、デバイスアクティビティ（SMS、MMS、および電話通話）のログがサポートされます。 アクティベーション後、仕事用と個人用 - フルコントロール デバイスには、個人用領域内のカメラ、電話、および設定などの標準のプリインストールアプリの限定されたセットのみがあります。保持されているプリインストールアプリのリストは、デバイスベンダーと OS バージョンによって異なります。 このアクティベーションタイプを使用するには、アクティベーション前にデバイスを工場出荷時のデフォルト設定にリセットする必要があります。BlackBerry UEM Client が削除された場合、または仕事用プロファイルがデバイスから削除された場合、自動的に工場出荷時のデフォルト設定にリセットされます。
仕事用領域のみ（Android Management 完全管理のデバイス）	このアクティベーションタイプでは、コマンドと IT ポリシールールを使用してデバイス全体を管理できます。このアクティベーションタイプを使用する場合、ユーザーはアクティベーションの前にデバイスを工場出荷時の設定にリセットする必要があります。このアクティベーションプロセスでは、仕事用プロファイルのみインストールされ、個人用プロファイルはインストールされません。ユーザーは、デバイスにアクセスするためにパスワードを作成する必要があります。デバイス上のデータはすべて暗号化とパスワードなどの認証方式を使用して保護されます。 アクティベーションの実行時に、デバイスによって UEM Client が自動的にインストールされ、管理者権限が付与されます。ユーザーは、管理者権限を取り消したり、アプリをアンインストールしたりすることはできません。 アクティベーション後、仕事用領域のみ デバイスには、カメラ、電話、設定などの標準のプリインストールアプリの限定されたセットと、必須の種別に割り当てられたアプリのみがあります。保持されているプリインストールアプリのリストは、デバイスベンダーと OS バージョンによって異なります。 このアクティベーションタイプを使用するには、アクティベーション前にデバイスを工場出荷時のデフォルト設定にリセットする必要があります。UEM Client が削除された場合、または仕事用プロファイルがデバイスから削除された場合、自動的に工場出荷時のデフォルト設定にリセットされます。

Android Enterprise デバイス

アクティベーションタイプ	説明
仕事用と個人用 - ユーザーのプライバシー（仕事用プロファイルがある Android Enterprise）	このアクティベーションタイプでは、個人用データのプライバシーが保護されますが、コマンドと IT ポリシールールを使用して仕事用データを管理できます。仕事用データと個人用データを分離する仕事用プロファイルがデバイスで作成されます。仕事用データと個人用データは両方とも、暗号化とパスワード認証によって保護されます。 Android Enterprise デバイスの Google Play アプリ管理を許可するには、アクティベーションプロファイルで［Google Play を仕事用領域に追加］を選択します（デフォルトで有効）。デバイスが Google Play にアクセスできない場合、ユーザーは別のソースから最新の UEM Client をダウンロードする必要があります。最新の UEM Client の .apk ファイルをダウンロードするには、KB 42607 を参照してください。 BlackBerry Secure Connect Plus および Knox Platform for Enterprise サポートを有効にするには、アクティベーションプロファイルで［Android Enterprise デバイスをアクティブ化する場合、BlackBerry Secure Connect Plus などのプレミアム UEM の機能を有効にする］オプションを選択する必要があります。 ユーザーは管理者の権限を UEM Client に与える必要はありません。

アクティベーションタイプ	説明
仕事用と個人用 - フルコントロール（仕事用プロファイルがある Android Enterprise 完全管理のデバイス）	このアクティベーションタイプでは、コマンドと IT ポリシールールを使用してデバイス全体を管理できます。仕事用データと個人用データを分離する仕事用プロファイルがデバイスで作成されます。仕事用領域のデータはすべて暗号化と何らかの認証方式を使用して保護されます。認証方式には、パスワード、PIN、パターン、指紋などがあります。このアクティベーションタイプでは、UEM ログファイルで、デバイスアクティビティ（SMS、MMS、および電話通話）のログがサポートされます。 Android Enterprise デバイスの Google Play アプリ管理を許可するには、アクティベーションプロファイルで［Google Play アカウントを仕事用領域に追加］を選択します（デフォルトで有効）。 アクティベーション後、仕事用と個人用 - フルコントロール デバイスには、個人用領域内のカメラ、電話、および設定などの標準のプリインストールアプリの限定されたセットのみがあります。保持されているプリインストールアプリのリストは、デバイスベンダーと OS バージョンによって異なります。 BlackBerry Secure Connect Plus および Knox Platform for Enterprise サポートを有効にするには、アクティベーションプロファイルで［Android Enterprise デバイスをアクティブ化する場合、BlackBerry Secure Connect Plus などのプレミアム UEM の機能を有効にする］オプションを選択する必要があります。 UEM がデバイス ID によるアクティベーションを制限できるかどうかを指定するには、アクティベーションプロファイルで［承認されたデバイス ID のみを許可する］を選択します。 このアクティベーションタイプを使用するには、アクティベーション前にデバイスを工場出荷時のデフォルト設定にリセットする必要があります。UEM Client が削除された場合、または仕事用プロファイルがデバイスから削除された場合、自動的に工場出荷時のデフォルト設定にリセットされます。 アクティベーションの実行時に、ユーザーは管理者の権限を UEM Client に与える必要があります。

アクティベーションタイプ	説明
仕事用領域のみ（Android Enterprise 完全管理のデバイス）	このアクティベーションタイプでは、コマンドと IT ポリシールールを使用してデバイス全体を管理できます。ユーザーはアクティベーションの前にデバイスを工場出荷時の設定にリセットする必要があります。このアクティベーションプロセスでは、仕事用プロファイルのみインストールされ、個人用プロファイルはインストールされません。ユーザーは、デバイスにアクセスするためにパスワードを作成する必要があります。デバイス上のデータはすべて暗号化とパスワードなどの認証方式を使用して保護されます。 Android Enterprise デバイスの Google Play アプリ管理を許可するには、アクティベーションプロファイルで［Google Play を仕事用領域に追加］を選択します（デフォルトで有効）。デバイスが Google Play にアクセスできない場合、ユーザーはアプリの .apk ファイルを使用して UEM Client をダウンロードできます。ユーザーに送信するアクティベーションメールメッセージに、UEM Client ソースファイルの場所を含む QR Code を設定して含めることができます。ユーザーが QR Code コードをスキャンすると、UEM Client が自動的にダウンロードされます。 QR Code アクティベーションメールメッセージにを設定して含めるには、アクティベーションのデフォルトページ（［設定］ > ［一般設定］ > ［アクティベーションのデフォルト］）の［デバイスアクティベーションに QR コードを許可する］チェックボックスをオンにする必要があります。また、［QR コードに UEM Client アプリソースファイルの場所を含む］チェックボックスをオンにして、UEM Client アプリソースファイルの場所を指定する必要があります。UEM Client の最新バージョンの .apk ファイルを取得するには、KB 42607 を参照してください。 アクティベーションの実行時に、デバイスによって UEM Client が自動的にインストールされ、管理者権限が付与されます。ユーザーは、管理者権限を取り消したり、アプリをアンインストールしたりすることはできません。 アクティベーション後、仕事用領域のみ デバイスには、カメラ、電話、設定などの標準のプリインストールアプリの限定されたセットと、必須の種別に割り当てられたアプリのみがあります。保持されているプリインストールアプリのリストは、デバイスベンダーと OS バージョンによって異なります。 BlackBerry Secure Connect Plus および Knox Platform for Enterprise サポートを有効にするには、アクティベーションプロファイルで［Android Enterprise デバイスをアクティブ化する場合、BlackBerry Secure Connect Plus などのプレミアム UEM の機能を有効にする］オプションを選択する必要があります。 UEM がデバイス ID によるアクティベーションを制限できるかどうかを指定するには、アクティベーションプロファイルで［承認されたデバイス ID のみを許可する］を選択します。 このアクティベーションタイプを使用するには、アクティベーション前にデバイスを工場出荷時のデフォルト設定にリセットする必要があります。UEM Client が削除された場合、または仕事用プロファイルがデバイスから削除された場合、自動的に工場出荷時のデフォルト設定にリセットされます。

仕事用プロファイルがない **Android** デバイス

次のアクティベーションタイプはすべての Android デバイスに適用されます。

アクティベーションタイプ	説明
ユーザーのプライバシー	ユーザーのプライバシー アクティベーションタイプを使用して、ユーザーの個人データがプライベートの状態であることを確認しながら、デバイスの基本的な制御（仕事用アプリの管理など）を提供できます。個別のコンテナはデバイスに作成されません。仕事用データのセキュリティを確保するために、BlackBerry Dynamics アプリをインストールできます。ユーザーのプライバシー でアクティベーションされたデバイスは、［電話を探す］や［ルートの検出］などのサービスを利用することができますが、管理者はデバイスポリシーを制御できません。 ユーザーのプライバシー アクティベーションタイプを使用して Chrome OS デバイスをアクティベーションし、AndroidBlackBerry Dynamics アプリをインストールして管理できるようにします。
BlackBerry 2FA 専用のデバイス登録	このアクティベーションタイプは、UEM によって管理されないデバイス向けの BlackBerry 2FA ソリューションをサポートします。このアクティベーションタイプではデバイス管理や制御は提供されませんが、デバイスは BlackBerry 2FA 機能を使用できます。このアクティベーションタイプを使用するには、BlackBerry 2FA プロファイルをユーザーにも割り当てる必要があります。 デバイスがアクティベーションされた場合、管理コンソールで限定されたデバイスの情報を表示したり、コマンドを使用してデバイスを無効にしたりできます。 このアクティベーションタイプは Microsoft Active Directory ユーザーのみサポートします。 詳細については、BlackBerry 2FA 関連の資料を参照してください。

Samsung Knox Workspace デバイス

メモ： Samsung Knox アクティベーションタイプは、将来のリリースで廃止されます。Knox Platform for Enterprise をサポートするデバイスは、Android Enterprise アクティベーションタイプを使用してアクティブ化できます。詳細については、KB 54614 を参照してください。

アクティベーションタイプ	説明
仕事用と個人用 - ユーザーのプライバシー -（Samsung Knox）	このアクティベーションタイプでは、個人用データのプライバシーが保護されますが、コマンドと IT ポリシールールを使用して仕事用データを管理できます。このアクティベーションタイプでは、Knox MDM IT ポリシールールはサポートされていません。デバイス上に個別の仕事用領域が作成されます。ユーザーは仕事用領域にアクセスするためのパスワードを作成する必要があります。仕事用領域のデータはすべて暗号化と何らかの認証方式を使用して保護されます。認証方式には、パスワード、PIN、パターン、指紋などがあります。また、ユーザーは、画面ロックパスワードを作成して、デバイス全体を保護する必要があります。ユーザーは、USB デバッグモードを使用できません。 アクティベーションの実行時に、ユーザーは管理者の権限を UEM Client に与える必要があります。
仕事用と個人用 - フルコントロール （Samsung Knox）	このアクティベーションタイプでは、コマンド、Knox MDM、および Knox Workspace IT ポリシールールを使用してデバイス全体を管理できます。デバイス上に個別の仕事用領域が作成されます。ユーザーは仕事用領域にアクセスするためのパスワードを作成する必要があります。仕事用領域のデータはすべて暗号化と何らかの認証方式を使用して保護されます。認証方式には、パスワード、PIN、パターン、指紋などがあります。 アクティベーションの実行時に、ユーザーは管理者の権限を UEM Client に与える必要があります。

アクティベーションタイプ：**macOS** デバイス

アクティベーションタイプ	説明
MDM 制御	このアクティベーションタイプは、macOS によって利用できるデバイス制御権限を使用して、基本的なデバイス管理を提供します。 ユーザーが macOS デバイスをアクティベーションすると、デバイスとユーザーが BlackBerry UEM で別々の存在として設定されます。独立した通信チャネルは、UEM、デバイス、UEM、およびユーザーアカウントの間で確立され、デバイスとユーザーの個別の管理を可能にします。一部のプロファイルは、ユーザーのみに割り当てられています（メールプロファイルなど）。一部のプロファイルは、デバイスのみに割り当てられています（プロキシプロファイルなど）。一部のプロファイルは、デバイスまたはユーザーにプロファイルを適用するかどうかの選択を可能にします（Wi-Fi プロファイルなど）。 コマンドと IT ポリシーを使用してデバイスを制御できます。ユーザーは、BlackBerry UEM Self-Service を使用して macOS デバイスをアクティベーションします。

アクティベーションタイプ：Windows 10 デバイス

メモ：Windows 10 Mobile デバイスは Microsoft でサポートされなくなり、UEM でのサポートが制限されます。

アクティベーションタイプ	説明
MDM 制御	このアクティベーションタイプは、Windows 10 デバイスによって利用可能なデバイス制御権限を使用して基本的なデバイス管理を提供します。個別の仕事用領域はデバイスにインストールされず、仕事用データのセキュリティも追加されません。 コマンドと IT ポリシーを使用してデバイスを制御できます。Windows 10 ユーザーは、Windows 10 の仕事用アクセスアプリを介してデバイスをアクティベーションします。

アクティベーション設定の管理

ユーザーがアクティベーションパスワードを入力する必要があるかどうか、または QR Code をスキャンできるかどうか、アクティベーションパスワード または QR Code の有効期間の長さ、およびユーザーが同じパスワード または QR Code を使用して複数のデバイスをアクティベーションできるかどうかなど、ユーザーによるデバイスのアクティベーション方法を管理できます。

デフォルトのアクティベーションの設定

1. 管理コンソールのメニューバーで、［設定］ > ［一般設定］ > ［アクティベーションのデフォルト］をクリックします。
2. ［デバイスアクティベーションデフォルト］セクションで、アクティベーションパスワードと QR Code オプションを指定します。
3. デバイスがアカウントでアクティブ化されるたびに BlackBerry UEM からメールメッセージでユーザーに通知する場合は、［デバイスアクティブ化通知を送信する］チェックボックスをオンにします。
4. ユーザーが QR Code で BlackBerry Dynamics アプリをアクティブ化できるようにするには、［デフォルトの **BlackBerry Dynamics** アプリ制御］セクションで、［**QR** コードを使用して **BlackBerry Dynamics** アプリのロックを解除する］チェックボックスをオンにします。詳細については、「BlackBerry Dynamics アプリのアクセスキー、アクティベーションパスワード、または QR コードの生成」を参照してください。
5. ユーザーがモバイルデバイスをアクティブにする方法を簡素化するには、［**BlackBerry Infrastructure**］セクションで［**BlackBerry Infrastructure** への登録をオンにする］チェックボックスをオンにします。このオプションをクリアした場合、デバイスをアクティブ化しようとすると、UEM のサーバーアドレスの入力を求められます。
6. 承認済みデバイス ID のリストをインポートまたはエクスポートするには、［デバイス **ID** をインポートまたはエクスポート］セクションで［参照］をクリックします。承認済みデバイス ID のリストを含む .csv ファイルに移動して選択します。詳細については、「承認されたデバイス ID のリストのインポートまたはエクスポート」を参照してください。
7. ［保存］をクリックします。

アクティベーションパスワードの設定とアクティベーションメールの送信

アクティベーションパスワードを設定し、1 台以上のデバイスのアクティベーションするための手順を含むアクティベーションメールをユーザーに送信できます。オンプレミス環境では、メールメッセージは、SMTP サーバー設定で設定したメールアドレスから送信されます。

作業を始める前に： アクティベーションメールテンプレートを作成します。

1. 管理コンソールのメニューバーで、［ユーザー］ > ［管理対象デバイス］をクリックします。
2. ユーザーアカウントの名前を検索してクリックします。
3. ［アクティベーションの詳細］ペインで、［アクティベーションパスワードを設定］をクリックします。
4. ［アクティベーションオプション］ドロップダウンリストで、次のタスクのいずれかを実行します。

- 現在割り当てられているアクティベーションプロファイルでデバイスをアクティブにする場合は、［デフォルトのデバイスアクティベーション］を選択します。
- アクティベーションパスワードと特定のアクティベーションプロファイルをペアリングするには、［指定されたアクティベーションプロファイルでデバイスアクティベーション］を選択します。詳細については、「ユーザーによる、アクティベーションタイプが異なる複数のデバイスのアクティブ化の許可」を参照してください。

5. ［アクティベーションパスワード］ドロップダウンリストで、次のいずれかを実行します。
   - パスワードを自動的に生成する場合は、［デバイスアクティベーションパスワードを自動生成し、アクティベーションの手順を記載したメールを送信する］を選択します。このオプションを選択した場合は、ユーザーに情報を送信するためにメールテンプレートを選択する必要があります。
   - ユーザーのアクティベーションパスワードを設定し、オプションでアクティベーションメールを送信する場合、［デバイスアクティベーションパスワードを設定する］を選択し、パスワードを入力します。
6. 必要に応じて、アクティベーションパスワードの有効期間を指定するには、アクティベーション期間の有効期限を変更します。
7. 1 回のデバイスアクティベーションに対してのみアクティベーションパスワードを有効にする場合は、［最初のデバイスがアクティブになったら、アクティベーションの有効期限が切れる］を選択します。
8. ［アクティベーションメールテンプレート］ドロップダウンリストで、使用するメールテンプレートを選択します。
9. ［送信］をクリックします。

アクティベーションメールを複数のユーザーに送信

アクティベーションメールを一度に複数のユーザーに送信できます。複数のユーザーにアクティベーションメールを送信する場合、アクティベーションパスワードは自動生成されます。メールは、SMTP サーバー設定で設定したメールアドレスから送信されます。

作業を始める前に： アクティベーションメールテンプレートを作成します。

1. 管理コンソールのメニューバーで、［ユーザー］ > ［管理対象デバイス］をクリックします。
2. アクティベーションメールを送信する各ユーザーの横にあるチェックボックスをオンにします。
3. をクリックします。
4. ［アクティベーションオプション］ドロップダウンリストで、次のいずれかを実行します。
   - 現在割り当てられているアクティベーションプロファイルでデバイスをアクティベーションする場合は、［デフォルトのデバイスアクティベーション］を選択します。
   - アクティベーションパスワードと特定のアクティベーションプロファイルをペアリングするには、［指定されたアクティベーションプロファイルでデバイスアクティベーション］を選択します。アクティベーションパスワードとアクティベーションプロファイルのペアリングの詳細については、「ユーザーによる、アクティベーションタイプが異なる複数のデバイスのアクティブ化の許可」を参照してください。
5. ［アクティベーションパスワード］ドロップダウンリストで、［デバイスアクティベーションパスワードを自動生成し、アクティベーションの手順を記載したメールを送信する］を選択します。
6. アクティベーションパスワードの有効期間を指定するには、アクティベーション期間の有効期限を変更します。
7. 1 回のデバイスアクティベーションに対してのみアクティベーションパスワードを有効にする場合は、［最初のデバイスがアクティブになったら、アクティベーションの有効期限が切れる］を選択します。

8. ［アクティベーションメールテンプレート］ドロップダウンリストで、使用するメールテンプレートを選択します。
9. ［送信］をクリックします。

ユーザーによるアクティベーションパスワードの設定の許可（BlackBerry UEM Self-Service）

iOS、Android、および Windows デバイスのユーザーには、BlackBerry UEM Self-Service を使用して独自のアクティベーションパスワードを作成することを許可できます。

1. メニューバーで［設定］>［セルフサービス］>［セルフサービス設定］をクリックします。
2. ［セルフサービスコンソールでのデバイスのアクティブ化をユーザーに許可する］チェックボックスをオンにして、次の手順を実行します。
3. アクティベーションパスワードが期限切れになるまでに、ユーザーがデバイスをアクティブ化する必要がある時間を指定します。
4. アクティベーションパスワードに必要な最小文字数を指定します。
5. ［最低限のパスワードの複雑さ］ドロップダウンリストで、必要な複雑さのレベルを選択します。
6. アクティベーションパスワードを作成したときにアクティベーションメールをユーザーに自動的に送信するには、［アクティベーションメールを送信］チェックボックスをオンにします。［アクティベーションメールテンプレート］ドロップダウンリストで、メールテンプレートを選択します。
7. カスタムアクティベーションメッセージをユーザーに送信するには、［カスタムアクティベーションメッセージを送信］チェックボックスをオンにします。適切なドロップダウンリストから、各デバイスタイプのメッセージテンプレートを選択します。
8. UEM Self-Service にログインするたびにユーザーにログイン通知メールを送信するには、［セルフサービスログイン通知を送信］チェックボックスをオンにします。
9. ［保存］をクリックします。

ユーザーによる、アクティベーションタイプが異なる複数のデバイスのアクティブ化の許可

ユーザーがアクティベーションタイプの異なるデバイスをアクティブ化できるように、ユーザーのアクティベーションパスワードを複数作成して、アクティベーションパスワードを特定のアクティベーションプロファイルと組み合わせることができます。

たとえば、ユーザーに、デバイスのフルコントロールを認めるアクティベーションタイプで仕事用デバイスをアクティブ化させる一方で、ユーザーのプライバシーを許可するアクティベーションタイプで個人用デバイスをアクティブ化させることができます。1 つのアクティベーションパスワードを、フルデバイスコントロールを許可するアクティベーションプロファイルと組み合わせ、2 番目のアクティベーションパスワードを、ユーザープライバシーアクティベーションプロファイルと組み合わせることにより、ユーザーは各デバイスをアクティブ化して異なる結果を得ることができます。各パスワードの目的の用途を説明するメールテンプレートを作成できます。

アクティベーションパスワードを特定のアクティベーションプロファイルと組み合わせるには、ユーザーアカウントを作成するか、アクティベーションメールを送信するときに、［指定されたアクティベーションプロファイルでデバイスアクティベーション］オプションを選択します。

特定のアクティベーションプロファイルと組み合わされたアクティベーションパスワードを最大 2 つ所有できます。それぞれのパスワードは、複数のデバイスをアクティブにするために使用できます。アクティベーションプロファイルと組み合わされたアクティベーションパスワードの場合、アクティベーションプロファイルの［ユーザーがアクティブ化できるデバイス数］オプションは適用されないことに注意してください。

アクティベーションパスワードと組み合わされているアクティベーションプロファイルを削除すると、そのアクティベーションパスワードは自動的に期限切れになります。必要に応じて、いつでもユーザーのアクティベーションパスワードを期限切れにすることができます。

ユーザーは BlackBerry UEM Self-Service で特定のアクティベーションプロファイルと組み合わされたアクティベーションパスワードを作成することはできません。

このオプションは、DEP に登録された iOS デバイスではサポートされていません。

アクティベーションパスワードの有効期限の強制

ユーザー用に生成されたアクティベーションパスワードを手動で期限切れにすることができます。

1. 管理コンソールのメニューバーで、［ユーザー］ > ［管理対象デバイス］をクリックします。
2. ユーザーアカウントの名前を検索してクリックします。
3. ［アクティベーションの詳細］セクションで、期限切れにするアクティベーションパスワードの下にある［期限切れ］をクリックします。

アクティベーションパスワードは即座に期限切れになります。通常のアクティベーションパスワードを強制的に期限切れにすると、パスワードが期限切れになった日時が表示されます。特定のアクティベーションプロファイルと組み合わされていたアクティベーションパスワードを期限切れにする場合、デバイスアクティベーションパスワードの詳細は表示されなくなります。

Android Enterprise および Android Management アクティベーションのサポート

ユーザーの Android Enterprise および Android Management デバイスをアクティブ化する方法は、デバイスの Android OS バージョンやユーザーのデバイスに対する組織の制御の量など、いくつかの要因によって異なります。また、管理対象 Google Play アカウント、Google Workspace ドメインまたは Google Cloud ドメインを使用して組織が Google サービスとやり取りするかどうか、または Google サービスを使用しないかどうかによっても異なります。

監視対象 Google Play アカウントを使用した Android Enterprise および Android Management アクティベーションのサポート

組織に Google ドメインがない場合、または BlackBerry UEM を Google ドメインに接続したくない場合は、管理対象 Google Play アカウントを使用して Android Enterprise および Android Management デバイスをアクティブ化できます。管理対象 Google Play アカウントを使用すると、Android Enterprise デバイスユーザーがダウンロードできる内部アプリを Google Play に追加できます。

UEM で管理対象 Google Play アカウントを使用するには、任意の Google または Gmail アカウントを使用して UEM を Google に接続します。ユーザーに関して個人を特定できる情報が Google に送信されることはありません。UEM を Google に接続した後、ユーザーが Android Enterprise および Android Management デバイスをアクティベーションし、Google Play を使用して仕事用アプリをダウンロードできるようにします。Android Enterprise および Android Management デバイスをサポートするように UEM を設定する方法については、「Android Enterprise デバイスサポートに必要な BlackBerry UEM の設定」および「Android Management 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。

Android Enterprise ドメインによる Google Workspace アクティベーションのサポート

BlackBerry UEM を組織の Google Workspace ドメインに接続する設定にした場合に、ユーザーが Android Enterprise デバイスをアクティベーションする前に、次のタスクを実行します。

作業を始める前に： Android Enterprise デバイスをサポートするように BlackBerry UEM を設定します。

1. Google Workspace ドメインで、Android ユーザー用にユーザーアカウントを作成します。
2. ［**EMM** ポリシーの強制］設定を選択します。

   この設定は、仕事用領域のみ および 仕事用と個人用 - フルコントロール アクティベーションタイプが割り当てられるデバイスでは必須で、他のアクティベーションタイプのデバイスでも強く推奨されています。この設定が選択されていない場合、ユーザーは、管理されている Google アカウントを、仕事用プロファイルに含まれていない仕事用アプリにアクセスできるデバイスに追加できます。
3. UEM で、Android ユーザー用にローカルユーザーアカウントを作成します。各アカウントのメールアドレスは、対応する Google Workspace アカウントのメールアドレスと一致しなければなりません。
4. UEM で、ユーザー、ユーザーグループ、またはデバイスグループに、メールプロファイルと生産性向上アプリを割り当てます。

Android Enterprise ドメインによる Google Cloud アクティベーションのサポート

BlackBerry UEM を Google Cloud ドメインに接続する設定にしている場合、ユーザーが Android Enterprise でデバイスをアクティベーションできるようにするには、次のタスクを実行する必要があります。

作業を始める前に： Android Enterprise デバイスをサポートするように BlackBerry UEM を設定します。Google Cloud ドメインに接続するように UEM を設定する場合、ドメインでのユーザーアカウント作成を UEM に許可するかどうかを選択する必要があります。この選択は、ユーザーが Android Enterprise デバイスをアクティブ化する前に、管理者が実行する必要のあるタスクに影響します。

1. UEM で、Android Enterprise ユーザー用にディレクトリユーザーアカウントを追加します。
2. UEM に Google Cloud ドメインへのユーザーアカウントの作成を許可しない場合は、自分の Google Cloud ドメインと UEM にユーザーアカウントを作成する必要があります。次の操作のいずれかを実行します。
   - Google Cloud ドメインで、Android Enterprise ユーザー用にユーザーアカウントを作成します。各メールアドレスは、対応する UEM ユーザーアカウントのメールアドレスと一致しなければなりません。Android Enterprise ユーザーが自身の Google Cloud アカウントのパスワードを知っていることを確認してください。
   - Google Apps Directory Sync ツールを使用し、自分の Google Cloud ドメインを会社のディレクトリと同期します。これを行った場合、Google Cloud ドメインにユーザーアカウントを手動で作成する必要はありません。
3. 仕事用領域のみ または 仕事用と個人用 - フルコントロール アクティベーションタイプを割り当てる場合、Google Cloud ドメインで ［**EMM** ポリシーの強制］設定を選択します。

   この設定は、仕事用領域のみ および 仕事用と個人用 - フルコントロール アクティベーションタイプのデバイスでは必須で、他のアクティベーションタイプのデバイスでも強く推奨されています。この設定が選択されていない場合、ユーザーは、管理されている Google アカウントを、仕事用プロファイルに含まれていない仕事用アプリにアクセスできるデバイスに追加できます。
4. UEM で、ユーザー、ユーザーグループ、またはデバイスグループに、メールプロファイルと生産性向上アプリを割り当てます。

Google Play にアクセスできない Android Enterprise デバイスのサポート

Google Play にアクセスできないデバイスをアクティブ化するには、ユーザーは別のソースから最新の BlackBerry UEM Client デバイスをダウンロードする必要があります。UEM Client をダウンロードする方法は、OS のバージョンとアクティベーションタイプによって異なります。

- 仕事用領域のみ または 仕事用と個人用 - フルコントロール のアクティベーションタイプでアクティブ化されたデバイスの場合、UEM Client をインストールする前に、デバイスを工場出荷時のデフォルト設定に戻す必要があります。QR Code に指定されたダウンロード場所を含めることができます。
- 仕事用と個人用 - ユーザーのプライバシー アクティベーションタイプでアクティブ化されるデバイスを工場出荷時のデフォルト設定にリセットする必要はありません。これらのデバイスでは、事前定義済みのセットアップが完了したら、UEM Client をインストールできます。

最新の UEM Client の .apk ファイルをダウンロードするには、KB 42607 を参照してください。

Google Play にアクセスできないデバイスをアクティブ化する場合は、次のことを確認します。

要件	説明
BlackBerry UEM 環境	Google Play にアクセスできないデバイスのみをサポートする場合は、UEM 環境を Android Enterprise に統合する必要はありません。Google Play にアクセスできるデバイスとアクセスできないデバイスを混在させてサポートする場合は、環境を Android Enterprise に統合する必要があります。
デフォルトのアクティベーション設定	QR コードに UEM Client の場所を含める場合は、デフォルトのアクティベーション設定で、［QR コードに UEM クライアントアプリソースファイルの場所を含む］および［デフォルトの場所を使用する］を選択します。 これらのオプションを使用すると、ユーザーはアクティベーションメールの QR コードをスキャンして、UEM Client を BlackBerry ダウンロードサイトからダウンロードできます。このオプションは、UEM 環境が Android Enterprise と統合されている場合にのみ使用できます。
アクティベーションプロファイル設定	アクティベーションプロファイルの次の設定を確認します。 • ［Google Play アカウントを仕事用領域に追加する］オプションをクリアします。 • BlackBerry Secure Connect Plus を有効にするには、［Android Enterprise デバイスをアクティブ化する場合、BlackBerry Secure Connect Plus などのプレミアム UEM の機能を有効にする］オプションを選択します。BlackBerry Connectivity アプリを内部アプリとしてアップロードし、ユーザーに割り当てる必要があります。
IT ポリシールール	仕事用と個人用 - ユーザーのプライバシー（Android Enterprise）アクティベーションタイプが割り当てられているユーザーに対して、Google Play の外部でのアプリのインストールを許可するには、［Google Play 以外のアプリのインストールを許可する］IT ポリシールールを有効にします。
BlackBerry Dynamics 以外のアプリ	BlackBerry Dynamics 以外のアプリの場合は、アプリを内部アプリとして UEM に追加し、ユーザーに割り当てます。 1. 割り当てるアプリの .apk ファイルを取得します。 2. 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。 3. > ［内部アプリ］をクリックします。 4. ［参照］をクリックして、.apk ファイルを選択します。 5. ［送信先］フィールドで、［すべての **Android** デバイス］を選択します。 6. ［**Google** ドメインでアプリを公開］の選択を解除します。 7. ［追加］をクリックします。 8. 追加するアプリごとに前の手順を繰り返します。 9. ユーザーにアプリを割り当てます。アプリケーション種別は［必須］に設定する必要があります。

要件	説明
BlackBerry Dynamics アプリ	BlackBerry Dynamics アプリの場合、内部アプリのソースファイルをアップロードし、アプリをユーザーに割り当てます。 Google Play にアクセスできないデバイスで内部アプリをインストールまたは更新するには、次の手順を実行します。 1. 割り当てる BlackBerry Dynamics アプリの .apk ファイルを取得します。 2. 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。 3. BlackBerry Dynamics アプリをクリックします。 4. ［**Android**］タブをクリックします。 5. ［内部アプリのソースファイルを追加する］をクリックします。 6. ［参照］をクリックして、.apk ファイルを選択します。 7. ［追加］をクリックします。 8. ［保存］をクリックします。 9. 追加するアプリごとに前の手順を繰り返します。 10. ユーザーにアプリを割り当てます。アプリケーション種別は［必須］に設定する必要があります。
BlackBerry UEM Client アプリを更新する	デバイスで UEM Client アプリを更新するには、ユーザーは手動で最新バージョンの .apk ファイルをダウンロードしてインストールする必要があります。

Windows 10 アクティベーションのサポート

次の方法で、ユーザーによる Windows 10 デバイスのアクティベーションを支援することができます。

- Windows 10 アクティベーション情報を提供するアクティベーションメールテンプレートを作成または編集します。詳細については、「アクティベーションメールテンプレートの作成」を参照してください。
- UEM と Entra ID 参加の統合：Entra ID の参加が設定されている場合、ユーザーは、Entra ID ユーザー名とパスワードのみを使用してデバイスをアクティブ化することができます。
- Windows Autopilot の設定：Windows Autopilot を設定すると、登録が初期設定の一部になり、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。
- 検出サービスの導入：BlackBerry から検出サービスとして Java Web アプリケーションを使用して、Windows 10 デバイスのユーザー向けの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。

iOS および iPadOS デバイスでの Apple ユーザー登録のサポート

iOS および iPadOS デバイスに ユーザーのプライバシー - ユーザー登録 アクティベーションタイプを使用して、ユーザーデータがプライベートに保持され、仕事用データから分離されていることを確認できます。このアクティベーションタイプでは、デバイスに、仕事用アプリとネイティブ Notes、iCloud ドライブ、メール（添付ファイルとメール本文全体）、カレンダー（添付ファイル）、および iCloud Keychain アプリ用の個別の仕事用領域がインストールされます。このアクティベーションタイプにより、アプリ管理、IT ポリシー管理、メールプロファイル、Wi-Fi プロファイル、per-app VPN が有効になります。管理者は、個人データに影響を与えることなく、作業データを管理（たとえば、作業データの消去）ができます。このアクティベーションタイプは、サポートされるバージョンの iOS または iPadOS を実行する非監視対象の iPhone および iPad デバイスでサポートされています。

Apple ユーザー登録をサポートする場合は、次の手順を実行します。

- このアクティベーションタイプを使用してアクティブ化するデバイスが監視対象でないことを確認します。
- 各ユーザーの管理対象 Apple ID アカウントを作成します。管理対象 Apple ID のメールアドレスは、BlackBerry UEM のユーザーのメールアドレスと一致している必要があります。
- ユーザーのデバイスアクティベーションパスワードを設定するときは、Apple ユーザー登録アクティベーションメールテンプレートを選択します。
- ユーザーが他の BlackBerry Dynamics アプリのアクティベーション、証明書のインポート、BlackBerry 2FA 機能の使用、CylancePROTECT の使用、およびコンプライアンスステータスの確認を簡単に行えるようにする場合は、VPP ライセンスを使用して BlackBerry UEM Client を割り当てます。種別を必須に設定すると、ユーザーはアプリをインストールするように求められます。種別をオプションに設定した場合、ユーザーは仕事用アプリからアプリを手動でダウンロードする必要があります。

Samsung Knox DualDAR のサポート

Samsung Knox DualDAR 暗号化をサポートするデバイスでは、2 層の暗号化を使用して仕事用データを保護できます。Knox DualDAR の外部層は、Android ファイルベースの暗号化に基づいて構築され、MDFPP 要件を満たすために Samsung によって強化されています。アクティベーションプロファイルでは、デフォルトの組み込み暗号化アプリを使用するか、仕事用プロファイルの暗号化の内部層に使用する内部暗号化アプリを使用するかを指定できます。

デフォルトのアプリの使用を選択した場合、仕事用プロファイルは、Samsung Knox フレームワークに含まれている FIPS 140-2 認定の暗号化モジュールを使用して保護されます。内部暗号化アプリは、組織またはサードパーティによって開発された専用の暗号化モジュールであり、FIPS 140-2 認定されている必要があります。ユーザーがデバイスを使用していない場合、仕事用プロファイルのすべてのデータはロックされ、バックグラウンドで実行されているアプリからはアクセスできません。

要件	説明
サポートされるデバイス	Samsung のフラグシップモデルがサポートされています。
暗号化アプリ	Knox DualDAR 暗号化に使用する暗号化アプリがある場合、 管理コンソールで内部アプリとして追加する必要があります。Knox DualDAR をサポートするデバイスのアクティベーションプロファイルを作成するときに、この暗号化アプリを選択します。代わりにデフォルトの暗号化アプリを使用することもできます。
アクティベーションプロファイル	アクティベーションプロファイルで Knox DualDAR 暗号化を有効にする場合は、プロファイルのみをサポートするデバイスにプロファイルを割り当てる必要があります。組織で Knox DualDAR をサポートしているデバイスとサポートしていないデバイスが混在している場合は、アクティベーションプロファイルをデバイスグループに割り当てる必要があります。サポートされていないデバイスに対して Knox DualDAR アクティベーションを有効にすると、アクティベーションは正常に完了しません。 Knox DualDAR 暗号化をサポートするには、Android デバイス用に次の設定でアクティベーションプロファイルを作成します。 • 仕事用と個人用 - フルコントロール（仕事用プロファイルがある Android Enterprise 完全管理のデバイス）のアクティベーションタイプを選択します。 • ［Android Enterprise デバイスをアクティブ化する場合、BlackBerry Secure Connect Plus などのプレミアム UEM の機能を有効にする］オプションを選択します。 • ［Samsung KNOX DualDAR Workspace を有効にする］オプションを選択します。 • デフォルトの暗号化アプリを使用するには、［デフォルトの組み込み暗号化アプリ］オプションを選択します。別の暗号化アプリを使用するには、［暗号化用の内部アプリを選択する］オプションを選択し、アプリリストから希望する暗号化アプリを選択します。
BlackBerry UEM Client	Android 用 BlackBerry UEM Client の最新バージョンをお勧めします。

アクティベーションプロファイルの作成

アクティベーションプロファイルを使用して、デバイスをアクティブ化し管理する方法を制御できます。アクティベーションプロファイルは、ユーザーがアクティブ化できるデバイスの数と種類、および各デバイスタイプで使用するアクティベーションタイプを指定します。アクティベーションタイプを使用することにより、アクティブ化されたデバイスをどの程度制御できるかを決定できます。

割り当てられたアクティベーションプロファイルは、管理者がプロファイルを割り当てた後に、ユーザーがアクティブ化したデバイスのみに適用されます。既にアクティブ化されているデバイスは、新しいまたは更新されたアクティベーションプロファイルに適合するように自動的には更新されません。

ユーザーを BlackBerry UEM に追加すると、デフォルトのアクティベーションプロファイルがユーザーアカウントに割り当てられます。要件に応じてデフォルトのアクティベーションプロファイルを変更することもできれば、カスタムアクティベーションプロファイルを作成して、ユーザーまたはグループに割り当てることもできます。

アクティベーションプロファイルの作成

1. 管理コンソールのメニューバーで、［ポリシーとプロファイル］ > ［ポリシー］ > ［アクティベーション］をクリックします。
2. ＋をクリックします。
3. プロファイルの名前と説明を入力します。
4. ［ユーザーがアクティブ化できるデバイス数］フィールドで、ユーザーがアクティブ化できるデバイスの最大数を指定します。
5. ［デバイスの所有］ドロップダウンリストで、次のいずれかを選択します。
   - 一部のユーザーが個人用のデバイスをアクティブ化し、別のユーザーが仕事用デバイスをアクティブ化する場合は、［指定なし］を選択します。
   - ほとんどのユーザーが、仕事用デバイスをアクティベーションする場合は、［仕事用］を選択します。
   - ほとんどのユーザーが、個人用デバイスをアクティベーションする場合は、［個人用］を選択します。
6. 必要に応じて、［組織の通知を割り当てる］ドロップダウンリストで組織の通知を選択します。組織の通知を割り当てている場合、iOS、iPadOS、macOS、または Windows 10 デバイスをアクティベーションするユーザーは、そのプロセスを完了するために通知に承諾する必要があります。
7. ［ユーザーがアクティブ化できるデバイスの種類］セクションで、アクティブ化したいデバイスの OS の種類を選択します。
8. アクティベーションプロファイルに含めるデバイスタイプごとに、次のアクションを実行します。
   a) デバイスタイプのタブをクリックします。
   b) ［デバイスモデルの制限］ドロップダウンリストで、次のいずれかのオプションを選択します。
      - 制限なし：ユーザーは、任意のデバイスモデルをアクティブ化できます。
      - 選択されたデバイスモデルを許可する：ユーザーは、指定したデバイスモデルのみをアクティブ化できます。
      - 選択されたデバイスモデルを許可しない：ユーザーは、指定したデバイスモデルをアクティブ化できません。

   ユーザーがアクティブ化できるデバイスモデルを制限する場合は、［編集］をクリックして許可または制限するデバイスを選択し、［保存］をクリックします。

c) ［許可される最低限のバージョン］ドロップダウンリストで、許可される最低限の OS バージョンを選択します。
d) サポートされているアクティベーションタイプを選択します。

Android デバイスでは、複数のアクティベーションタイプを選択し、ランク付けすることができます。他のすべてのデバイスタイプでは、1 つのアクティベーションタイプのみを選択できます。

メモ：Android Enterprise と Android Management に対して個別のアクティベーションプロファイルを作成する必要があります。Android Enterprise と Android Management のアクティベーションタイプが同じプロファイルで指定されている場合、Android Management タイプが Android Enterprise より低いランクになっていても、タイプが優先されます。Android Management アクティベーションタイプのパスワードとアクティベーション情報のみが QR コードに埋め込まれます。

9. iOS および iPadOS デバイスの場合は、次のアクションを実行します。
a) ユーザーのプライバシー アクティベーションタイプを選択して SIM ベースのライセンスを有効にする場合、［**SIM** ベースのライセンスを有効にするには、**SIM** カードとデバイスのハードウェア情報へのアクセスを許可します］を選択する必要があります。
b) ユーザーのプライバシー アクティベーションタイプを選択して特定の機能を管理する場合は、該当するチェックボックスを選択します。
c) ［MDM コントロール］または「ユーザーのプライバシー」アクティベーションタイプを選択（SIM ベースのライセンスを使用）し、監視対象デバイスのみをアクティブにする場合は、［非監視対象デバイスのアクティブ化を許可しない］を選択します。
d) 必要に応じて、［**iOS** アプリの整合性チェック］セクションで、次の証明方法のいずれかを選択します。

- **BlackBerry Dynamics** アプリのアクティベーションでアプリの整合性チェックを実行する：この方法は、デバイスがアクティブ化されたときに、デバイスにチャレンジを送信して iOS 仕事用アプリの整合性をチェックするために使用します。
- 定期的なアプリの整合性チェックを実行する：この方法は、デバイスにチャレンジを送信して iOS 仕事用アプリの整合性をチェックするために使用します。

iOS アプリの整合性チェックを実行するには、UEM ドメインで CylancePROTECT を有効にする必要があります。詳細については、「UEM ドメインでの CylancePROTECT モバイルの有効化」を参照してください。
e) 必要に応じて、［管理対象デバイス認証］セクションで、次の証明方法のいずれかを選択します。

- ［デバイスアクティベーション時に管理対象デバイス認証を実行する］：この方法を使用して、デバイスがアクティブ化されたときにデバイスにチャレンジを送信して、デバイスプロパティの整合性をチェックします。
- ［定期的な管理対象デバイス認証を実行する］： この方法を使用して、定期的にチャレンジを送信し、デバイスプロパティの整合性をチェックします。

iOS デバイスで管理対象デバイスの認証を実行するには、この機能を有効にする必要があります。詳細については、管理関連の資料で「iOS デバイスの認証の設定」を参照してください。

管理対象デバイス認証は、MDM 制御 および ユーザーのプライバシー のアクティベーションタイプに適用されますが、ユーザーのプライバシー - ユーザー登録 アクティベーションタイプには適用されません。ユーザーのプライバシー アクティベーションタイプを選択する場合は、少なくとも 1 つの管理オプション（［VPN 管理を許可する］など）を選択する必要があります。

10. Android デバイスの場合は、次の処理を実行します。
a) 複数のアクティベーションタイプを選択した場合は、上下の矢印をクリックしてランク付けします。デバイスは、サポートする最もランクの高いプロファイルを受信します。

b) Samsung Knox アクティベーションタイプを選択し、仕事用アプリの管理に Google Play を使用する場合は、［**Samsung Knox Workspace** デバイス用の **Google Play** アプリ管理］を選択します。このオプションは、ドメインへの接続を設定している場合にのみ使用できます。

   Samsung Knox アクティベーションタイプは、将来のリリースで廃止されます。Knox Platform for Enterprise をサポートするデバイスは、Android Enterprise アクティベーションタイプを使用してアクティブ化できます。

c) Android Enterprise アクティベーションタイプを選択した場合は、適切な Android Enterprise オプションを選択します。

   - 適切なライセンスを持つデバイスで企業向け BlackBerry Secure Connect Plus および Knox プラットフォーム機能（Samsung Knox をサポートするデバイス用）を有効にするには、［**Android Enterprise** デバイスをアクティブ化する場合、**BlackBerry Secure Connect Plus** などのプレミアム **UEM** の機能を有効にする］を選択します。
   - サポートするデバイスに対して Samsung Knox DualDAR 暗号化を有効にするには、［**Samsung KNOX DualDAR Workspace** を有効にする］を選択します。
   - 仕事用領域で Google Play アプリ管理を許可するには、［**Google Play** アカウントを仕事用領域に追加］を選択します。
   - UEM が、デバイス ID によるアクティベーションを制限できるようにするには、［承認されたデバイス **ID** のみを許可する］を選択します。このオプションは 仕事用領域のみ および 仕事用と個人用 - フルコントロール デバイスでのみサポートされます。
   - ユーザーがデバイスをアクティブ化できるネットワークタイプを指定するには、［**QR** コード登録］ドロップダウンリストでネットワークを選択します。このオプションは 仕事用領域のみ および 仕事用と個人用 - フルコントロール デバイスでのみサポートされます。

d) 必要に応じて、［**SafetyNet** または **Play Integrity** 認証オプション］セクションで、オプションで次のいずれかの認証方法を選択します。

   - ［デバイスの **SafetyNet** または **Play Integrity** 認証を実行する］：この方法は、デバイスの完全性と整合性をテストするチャレンジを送信するために使用します。
   - ［デバイスアクティベーション時に **SafetyNet** アテステーションを実行する］（**Play Integrity** をサポートしない **UEM Client** バージョンにのみ適用されます）：この方法は、デバイスがアクティブ化されたときにデバイスの完全性と整合性をテストするチャレンジを送信するために使用します。
   - ［**BlackBerry Dynamics** アプリのアクティベーション時に **SafetyNet** または **Play Integrity** 認証を実行する］：この方法は、BlackBerry Dynamics アプリがアクティブ化されたときに BlackBerry Dynamics アプリの完全性と整合性をテストするチャレンジを送信するために使用します。

e) ［ハードウェアアテステーションオプション］セクションで、必要なセキュリティパッチレベルがインストールされていることを確認するために、デバイスがアクティブ化されたときに UEM からチャレンジを送信するには、［アクティベーション中にアテステーションコンプライアンスルールを適用する］を選択します。

11. Windows 10 デバイスの場合は、1 つまたは両方のフォームファクターオプションを選択します。

12.［追加］をクリックします。

終了したら：

- 必要に応じて、アクティベーションプロファイルをランク付けします。
- プロファイルをユーザーアカウントおよびグループに割り当てます。

Android デバイスのアクティベーション

ユーザーが BlackBerry UEM Client をインストールして Android デバイスをアクティベーションするために従う手順は、Android OS のバージョン、デバイスの製造元、組織の Google サービスの使用方法、デバイスアクティベーションプロファイルで指定されているアクティベーションタイプ、組織の環境設定など、いくつかの要因によって異なります。ユーザーに送信するアクティベーションメールでユーザーにデバイスのアクティベーション手順を伝えることができます。アクティベーションメールテンプレートの作成についての詳細は、「アクティベーションメールテンプレートを作成」を参照してください。

Android Management デバイスは、次のアクティベーション方法をサポートしています。

アクティベーション方法	説明
Android Management ユーザープライバシのアクティベーション	仕事用と個人用 - ユーザーのプライバシー アクティベーションタイプでアクティブ化されるデバイスの場合、ユーザーは仕事用プロファイルを設定し、提供された QR コードを使用して Google Play から UEM Client をダウンロードし、UEM でデバイスをアクティブ化できます。 詳細については、「仕事用と個人用 - ユーザーのプライバシー アクティベーションタイプの Android Management デバイスのアクティベーション」を参照してください。
Android Management フルコントロールと仕事用領域のみのアクティベーション	仕事用と個人用 - フルコントロール および 仕事用領域のみ アクティベーションタイプでアクティブ化されるデバイスの場合、ユーザーは、デバイスを工場出荷時のデフォルト設定にリセットし、提供された QR コードを使用して Google Play から UEM Client をダウンロードし、UEM でデバイスを有効にする必要があります。 詳細については、「管理対象 Google Play アカウントを使用した Android Management デバイスのアクティベーション」を参照してください。

Android Enterprise デバイスは、次のアクティベーション方法をサポートしています。

アクティベーション方法	説明
UEM Client を Google Play からインストールします。	仕事用と個人用 - ユーザーのプライバシー アクティベーションタイプでアクティブ化されるデバイスは、アクティベーションの前に工場出荷時のデフォルト設定にリセットする必要はありません。これらのデバイスをアクティブにするために、ユーザーは UEM Client を Google Play からダウンロードできます。 詳細については、「仕事用と個人用 - ユーザーのプライバシー アクティベーションタイプの Android Enterprise デバイスのアクティベーション」を参照してください。

アクティベーション方法	説明
BlackBerry ダウンロードサイトから UEM Client .apk ファイルをダウンロードします。	Android ユーザーが Google Play にアクセスできない場合、仕事用と個人用 - ユーザーのプライバシー アクティベーションタイプでアクティブ化されるデバイスについて、ユーザーは BlackBerry ダウンロードサイトから UEM Client .apk ファイルをダウンロードできます。また、BlackBerry からファイルをダウンロードし、ユーザーがアクセスできる場所にファイルを配置することもできます。 UEM Client の最新バージョンの .apk ファイルを取得するには、KB 42607 を参照してください。
デバイスのセットアップ中に Google ドメイン資格情報を使用します。	BlackBerry UEM が組織の Google Workspace または Google Cloud ドメインに接続されている場合、仕事用領域のみ または 仕事用と個人用 - フルコントロール アクティベーションタイプが割り当てられているデバイスをアクティベーションするために、ユーザーがデバイスのセットアップ中に仕事用 Google 資格情報を入力するときに、デバイスが UEM Client をダウンロードし、アクティベーションプロセスが開始されます。 詳細については、「BlackBerry UEM が Google ドメインに接続されている場合の Android Enterpriseデバイスのアクティベーション」を参照してください。
UEM Client のダウンロード先が含まれている QR コードをスキャンします。	BlackBerry UEM では、ユーザーに送信するアクティベーションメールに含めることができる QR コードに、UEM Client のダウンロード場所を含めることができます。仕事用領域のみ または 仕事用と個人用 - フルコントロール が割り当てられているユーザーは、QR コードをスキャンして UEM Client をダウンロードできます。 詳細については、「管理対象 Google Play アカウントを使用した Android Enterprise デバイスのアクティベーション」を参照してください。
Android ゼロタッチ登録または Samsung Knox Mobile Enrollment。	Android ゼロタッチ登録では、多数の Android Enterprise デバイスを同時に導入できます。Knox Mobile Enrollment では、Android Enterprise のアクティベーションを使用して多数の Samsung Knox デバイスを導入できます。このオプションを使用するには、デバイスを認定販売代理店から購入するときにデバイスをゼロタッチ登録または Knox Mobile Enrollment 用にプロビジョニングする必要があります。 詳細については、「Android ゼロタッチ登録のサポートの構成」または「Knox Mobile Enrollment を使用した複数のデバイスのアクティブ化」を参照してください。

Android Enterprise デバイスの場合、各アクティベーションオプションは特定のアクティベーションタイプでのみサポートされます。仕事用領域のみ および 仕事用と個人用 - フルコントロール アクティベーションタイプの場合、サポートされるオプションは、組織での Google サービスの使用方法にも依存します。

アクティベーションタイプ	AE ユーザープライバシー	AE フルコントロール			AE 仕事用領域のみ		
方法		Google ドメイン	管理対象の Google Play	Google アクセスなし	Google ドメイン	管理対象の Google Play	Google アクセスなし
Google Play から UEM Client をインストールするかユーザーがダウンロードする	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
Google ドメイン資格情報	はい	はい	いいえ	いいえ	はい	いいえ	いいえ
QR コードのスキャン	はい	はい	はい	はい	はい	はい	はい
Android ゼロタッチ登録/Samsung Knox Mobile Enrollment	いいえ	はい	はい	はい	はい	はい	はい

仕事用と個人用 - ユーザーのプライバシー アクティベーションタイプの Android Enterprise デバイスのアクティベーション

仕事用と個人用 - ユーザーのプライバシー（Android Enterprise）アクティベーションタイプを使用してデバイスをアクティブ化するには、次のアクティベーション手順をデバイスユーザーに送信します。このアクティベーションタイプのデバイスは、アクティベーション前にデバイスを工場出荷時のデフォルト設定にリセットする必要がありません。

作業を始める前に： デバイス管理者から、デバイスのアクティベーションに必要な情報を記載したメールが 1 つ以上送信されました。メールにアクティベーション QR コードが含まれている場合は、それを使用してデバイスをアクティベーションできます。QR Code を受け取っていない場合は、次の情報があることを確認してください。

- 仕事用メールアドレス
- UEM ユーザー名（通常は仕事用ユーザー名）
- UEM アクティベーションパスワード
- UEM サーバーアドレス（必要な場合）

1. BlackBerry UEM Client からデバイスに Google Play をインストールします。

デバイスが Google Play にアクセスできない場合は、.apk ファイルを使用して UEM Client を手動でダウンロードしてインストールできます。UEM Client の最新バージョンの .apk ファイルを取得するには、KB 42607 を参照してください。

2. UEM Client を開きます。
3. 使用許諾契約書を読み、［使用許諾契約に同意します］チェックボックスをタップします。
4. 次の操作のいずれかを実行します。

タスク	手順
QR コードをスキャンしてデバイスをアクティベーションします。	a. をタップします。 b. UEM Client に写真撮影とビデオ録画を許可するには、［許可］をタップします。 c. アクティベーションメールに管理者が入力した QR コードをスキャンします。
デバイスを手動でアクティベーションします。	a. 仕事用メールアドレスを入力して、［次へ］をタップします。 b. アクティベーションパスワードを入力し、［デバイスをアクティブ化］をタップします。 c. 必要に応じて、サーバーアドレスを入力し、［次へ］をタップします。 d. 必要な場合て、ユーザー名とアクティベーションパスワードを入力して、［次へ］をタップします。

5. UEM Client に通話の発信と管理を許可するには、［許可］をタップします。
6. ［プロファイルの設定］画面で、［設定］をタップします。仕事用プロファイルを設定するのに時間がかかる場合があります。
7. プロンプトが表示されたら、Google アカウントにログインして、Google メールアドレスとパスワードを入力します。
8. 画面のロック解除方法を選択します。
9. デバイスの起動時にパスワードが要求されるように、［安全な起動］画面でプロンプトが表示されたら、［はい］をタップします。
10. デバイスのパスワードを入力し、確認のためにもう一度入力します。［**OK**］をタップします。
11. 通知の表示方法を選択します。［完了］をタップします。
12. UEM Client パスワードを作成し、［**OK**］をタップします。BlackBerry Dynamics アプリを使用している場合、すべての BlackBerry Dynamics アプリにサインインする際にもこのパスワードを使用します。
13. ［登録］ をタップします。
14. UEM Client および BlackBerry Dynamics アプリの指紋認証を設定する場合は、画面の指示に従います。それ以外の場合は、［キャンセル］をタップします。
15. デバイスからサインアウトしている場合は、UEM のアクティベーションを完了するためにデバイスのロックを解除します。
16. BlackBerry Secure Connect Plus への接続の許可を求めるプロンプトが表示されたら、［**OK**］をタップして、接続が有効になるまで待ちます。
17. デバイスに仕事用アプリをインストールするように促すプロンプトが表示されたら、画面の手順に従います。

終了したら： アクティベーションプロセスの正常な完了を確認するには、次のいずれかを実行します。

- UEM Client で、⋮ > ［バージョン情報］をタップします。［アクティブ化されたデバイス］セクションで、デバイス情報とアクティベーションのタイムスタンプが存在していることを確認します。
- BlackBerry UEM Self-Service コンソールで、デバイスがアクティブ化されたデバイスとして一覧に表示されていることを確認します。ユーザーがデバイスをアクティブ化した後、ステータスの更新に最大で 2 分かかることがあります。

BlackBerry UEM が Google ドメインに接続されている場合の Android Enterpriseデバイスのアクティベーション

これらの手順は、BlackBerry UEM が Google Workspace または Google Cloud ドメインに接続しているときに、アクティベーションタイプ 仕事用領域のみ （Android Enterprise）または 仕事用と個人用 - フルコントロール（Android Enterprise）が割り当てられているデバイスに適用されます。仕事用と個人用 - ユーザーのプライバシー アクティベーションタイプの Google ドメインに接続されているデバイスをアクティベーションするには、「仕事用と個人用 - ユーザーのプライバシー アクティベーションタイプの Android Enterprise デバイスのアクティベーション」を参照してください。

次のアクティベーション手順をデバイスユーザーに送信します。

作業を始める前に： デバイス管理者から、デバイスのアクティベーションに必要な情報を記載したメールが 1 つ以上送信されました。メールメッセージにアクティベーション QR Code が含まれる場合は、それを使用してデバイスをアクティベーションできます。情報を入力する必要はありません。QR Code を受け取っていない場合は、次の情報を受け取っていることを確認してください。

- 仕事用メールアドレス
- UEM ユーザー名（通常は仕事用ユーザー名）
- UEM アクティベーションパスワード
- UEM サーバーアドレス（必要に応じて）

1. デバイス設定のウェルカム画面が表示されない場合は、デバイスを工場出荷時のデフォルト設定にリセットします。
2. デバイス設定時に、Google アカウントのログイン画面に仕事用の Google メールアドレスとパスワードを入力します。
3. デバイスで［インストール］をタップして BlackBerry UEM Client をインストールします。
4. 使用許諾契約書を読み、［使用許諾契約に同意します］チェックボックスをタップします。
5. 次の操作のいずれかを実行します。

タスク	手順
QR Code を使用して、デバイスをアクティベーションします。	**a.** をタップします。 **b.** UEM Client の写真撮影とビデオ録画を許可するには、［許可］をタップします。 **c.** 受信したアクティベーションメールの QR Code をスキャンします。

タスク	手順
デバイスを手動でアクティベーションします。	**a.** 仕事用メールアドレスを入力します。［次へ］をタップします。 **b.** アクティベーションパスワードを入力します。［デバイスをアクティブ化する］をタップします。 **c.** 必要に応じて、サーバーアドレスを入力します。サーバーアドレスは、受信したアクティベーションメールまたは BlackBerry UEM Self-Service で確認できます。［次へ］をタップします。 **d.** 必要に応じて、ユーザー名とアクティベーションパスワードを入力します。［次へ］をタップします。

6. プロファイルと設定がデバイスにプッシュされるまで待ちます。
7. ［プロファイルの設定］画面で、［設定］をタップします。仕事用プロファイルを設定するのに時間がかかる場合があります。
8. プロンプトが表示されたら、Google メールアドレスとパスワードを使用して Google アカウントにログインします。
9. ロック解除の選択画面で、画面のロック解除方法を選択します。
10. ［安全な起動］画面でプロンプトが表示されたら、［はい］をタップし、デバイスの起動時にパスワードが要求されるようにします。
11. デバイスのパスワードを入力し、確認のためにもう一度入力します。［**OK**］をタップします。
12. 通知の表示方法について、いずれかのオプションを選択します。［完了］をタップします。
13. UEM Client パスワードを作成し、［**OK**］をタップします。BlackBerry Dynamics アプリを使用している場合、すべての BlackBerry Dynamics アプリにサインインする際にもこのパスワードを使用します。
14. UEM Client および持っている任意の BlackBerry Dynamics アプリの指紋認証を設定する場合は、次の画面で［登録］をタップし、画面の指示に従います。それ以外の場合は、［キャンセル］をタップします。
15. デバイスからサインアウトしている場合は、UEM のアクティベーションを完了するためにデバイスのロックを解除します。
16. プロンプトが表示されたら、［**OK**］をタップして BlackBerry Secure Connect Plus への接続を許可し、接続が有効になるまで待ちます。
17. プロンプトが表示されたら、画面の手順に従ってデバイスに仕事用アプリをインストールします。

終了したら： アクティベーションプロセスの正常な完了を確認するには、次のいずれかを実行します。

- UEM Client で、⋮ > ［バージョン情報］をタップします。［アクティブ化されたデバイス］セクションで、デバイス情報とアクティベーションのタイムスタンプが存在していることを確認します。
- BlackBerry UEM Self-Service コンソールで、デバイスがアクティブ化されたデバイスとして一覧に表示されていることを確認します。ユーザーがデバイスをアクティブ化した後、ステータスの更新に最大で 2 分かかることがあります。

管理対象 **Google Play** アカウントを使用した **Android Enterprise** デバイスのアクティベーション

次のアクティベーション手順は、アクティベーションタイプ 仕事用領域のみ （Android Enterprise）または 仕事用と個人用 - フルコントロール （Android Enterprise）が割り当てられたサポートされる Android デバイスに適用されます。Android Enterprise 仕事用と個人用 - ユーザーのプライバシー アクティベーションタイプの管理対象

Google Play アカウントに接続されているデバイスをアクティベーションするには、「仕事用と個人用 - ユーザーのプライバシー アクティベーションタイプの Android Enterprise デバイスのアクティベーション」を参照してください。

ユーザーに送信するアクティベーションメールメッセージに、UEM Client アプリソースファイルの場所を含む QR Code を設定して含めることができます。ユーザーが QR Code コードをスキャンすると、UEM Client が自動的にダウンロードされます。アクティベーションメールメッセージに QR Code を設定して含めるには、アクティベーションのデフォルトページ（［設定］ > ［一般設定］ > ［アクティベーションのデフォルト］）の［デバイスアクティベーションに QR コードを許可する］チェックボックスをオンにする必要があります。また、［QR コードに UEM Client アプリソースファイルの場所を含む］チェックボックスをオンにして、 UEM Client アプリソースファイルの場所を指定する必要があります。UEM Client の最新バージョンの .apk ファイルを取得するには、KB 42607 を参照してください。

次のアクティベーション手順をデバイスユーザーに送信します。

作業を始める前に： デバイス管理者から、デバイスのアクティベーションに必要な情報を記載したメールが 1 つ以上送信されました。メールメッセージには、UEM Client をインストールしてデバイスをアクティベーションするために必要な QR Code が含まれています。

1. アクティベーションするデバイスで、デバイス設定画面が表示されない場合は、デバイスを工場出荷時のデフォルト設定にリセットします。
2. デバイスの QR Code リーダを開くには、デバイスの画面を 7 回タップします。
3. UEM Client をダウンロードするには、管理者がアクティベーションメールで指定した QR Code をスキャンします。
4. UEM Client を開きます。
5. 使用許諾契約書を読み、［使用許諾契約に同意します］チェックボックスをタップします。
6. ［プロファイルの設定］画面で、［設定］をタップします。仕事用プロファイルを設定するのに時間がかかる場合があります。
7. 画面のロック解除方法を選択します。
8. デバイスの起動時にパスワードが要求されるように、［安全な起動］画面でプロンプトが表示されたら、［はい］をタップします。
9. デバイスのパスワードを入力し、確認のためにもう一度入力して、［**OK**］をタップします。
10. 通知の表示方法を選択します。［完了］をタップします。
11. UEM Client パスワードを作成し、［**OK**］をタップします。BlackBerry Dynamics アプリを使用している場合、すべての BlackBerry Dynamics アプリにサインインする際にもこのパスワードを使用します。
12. ［登録］ をタップします。
13. UEM Client および BlackBerry Dynamics アプリの指紋認証を設定する場合は、画面の指示に従います。それ以外の場合は、［キャンセル］をタップします。
14. デバイスからサインアウトしている場合は、UEM のアクティベーションを完了するためにデバイスのロックを解除します。
15. BlackBerry Secure Connect Plus への接続の許可を求めるプロンプトが表示されたら、［**OK**］をタップして、接続が有効になるまで待ちます。
16. デバイスに仕事用アプリをインストールするように促すプロンプトが表示されたら、画面の手順に従います。

終了したら： アクティベーションプロセスの正常な完了を確認するには、次のいずれかを実行します。

- UEM Client で、⋮ > ［バージョン情報］をタップします。［アクティブ化されたデバイス］セクションで、デバイス情報とアクティベーションのタイムスタンプが存在していることを確認します。

- BlackBerry UEM Self-Service コンソールで、デバイスがアクティブ化されたデバイスとして一覧に表示されていることを確認します。ユーザーがデバイスをアクティブ化した後、ステータスの更新に最大で 2 分かかることがあります。

Google Play にアクセスできない Android Enterprise デバイスのアクティベーション

次のアクティベーション手順は、仕事用領域のみ（Android Enterprise）および 仕事用と個人用 - フルコントロール（Android Enterprise）アクティベーションタイプが割り当てられ、Google Play にアクセスできないデバイスに適用されます。ユーザーは、アプリの .apk ファイルを使用して BlackBerry UEM Client をダウンロードできます。ユーザーに送信するアクティベーションメールメッセージに、UEM Client ソースファイルの場所を含む QR Code を設定して含めることができます。ユーザーが QR Code コードをスキャンすると、UEM Client が自動的にダウンロードされます。

QR Code アクティベーションメールメッセージにを設定して含めるには、アクティベーションのデフォルトページ（［設定］ > ［一般設定］ > ［アクティベーションのデフォルト］）の［デバイスアクティベーションに QR コードを許可する］チェックボックスをオンにする必要があります。また、［QR コードに UEM Client アプリソースファイルの場所を含む］チェックボックスをオンにして、 UEM Client アプリソースファイルの場所を指定する必要があります。UEM Client の最新バージョンの .apk ファイルを取得するには、KB 42607 を参照してください。

次のアクティベーション手順をデバイスユーザーに送信します。

作業を始める前に： デバイス管理者から、デバイスのアクティベーションに必要な情報を記載したメールが 1 つ以上送信されました。管理者からアクティベーション QR Code を受信した場合は、デバイスのアクティベーションに使用できます。QR Code を受け取っていない場合は、次の情報があることを確認してください。

- 仕事用メールアドレス
- UEM ユーザー名（通常は仕事用ユーザー名）
- UEM アクティベーションパスワード
- UEM サーバーアドレス（必要に応じて）

1. アクティベーションするデバイスで、デバイス設定画面が表示されない場合は、デバイスを工場出荷時のデフォルト設定にリセットします。
2. デバイスの QR Code リーダを開くには、デバイスの画面を 7 回タップします。
3. UEM Client をダウンロードするには、管理者がアクティベーションメールメッセージで指定した QR Code をスキャンします。
   UEM Client は、自動的にデバイスにダウンロードされます。
4. UEM Client を開きます。
5. 使用許諾契約書を読み、［使用許諾契約に同意します］チェックボックスをタップします。
6. 次の操作のいずれかを実行します。

タスク	手順
QR Code を使用して、デバイスをアクティベーションします。	a. UEM Client で、 をタップします。 b. UEM Client の写真撮影とビデオ録画を許可するには、［許可］をタップします。

タスク	手順
デバイスを手動でアクティベーションします。	**a.** 仕事用メールアドレスを入力して、［次へ］をタップします。 **b.** アクティベーションパスワードを入力し、［デバイスをアクティブ化］をタップします。 **c.** 必要に応じて、サーバーアドレスを入力し、［次へ］をタップします。 **d.** 必要に応じてユーザー名とアクティベーションパスワードを入力し、［次へ］をタップします。

7. ［プロファイルの設定］画面で、［設定］をタップします。仕事用プロファイルを設定するのに時間がかかる場合があります。
8. 画面のロック解除方法を選択します。
9. デバイスの起動時にパスワードが要求されるように、［安全な起動］画面でプロンプトが表示されたら、［はい］をタップします。
10. デバイスのパスワードを入力し、確認のためにもう一度入力します。［**OK**］をタップします。
11. 通知の表示方法を選択します。［完了］をタップします。
12. UEM Client パスワードを作成し、［**OK**］をタップします。BlackBerry Dynamics アプリを使用している場合、すべての BlackBerry Dynamics アプリにサインインする際にもこのパスワードを使用します。
13. 次の画面で、［登録］をタップします。
14. UEM Client および BlackBerry Dynamics アプリの指紋認証を設定する場合は、画面の指示に従います。それ以外の場合は、［キャンセル］をタップします。
15. デバイスからサインアウトしている場合は、UEM のアクティベーションを完了するためにデバイスのロックを解除します。
16. BlackBerry Secure Connect Plus への接続の許可を求めるプロンプトが表示されたら、［**OK**］をタップして、接続が有効になるまで待ちます。
17. デバイスに仕事用アプリをインストールするように促すプロンプトが表示されたら、画面の手順に従います。
18. 必要に応じて、スマートフォンにメールを設定するには、組織で使用するメールアプリを開き、指示に従います。

仕事用と個人用 - ユーザーのプライバシー アクティベーションタイプの **Android Management** デバイスのアクティベーション

ユーザーに送信するアクティベーションメールに QR Code を含めることができます。ユーザーが QR Code コードをスキャンすると、UEM Client が自動的にダウンロードされます。アクティベーションメールメッセージに QR Code を設定して含めるには、アクティベーションのデフォルトページ（［設定］ > ［一般設定］ > ［アクティベーションのデフォルト］）の［デバイスアクティベーションに QR コードを許可する］チェックボックスをオンにする必要があります。デフォルトの Android Management アクティベーションメールテンプレート（または同等のカスタム）を使用します。

次のアクティベーション手順をデバイスユーザーに送信します。

作業を始める前に： デバイス管理者から、デバイスのアクティベーションに必要な情報を記載したメールが 1 つ以上送信されました。メールメッセージには、QR Code をインストールしてデバイスをアクティベーションするために必要な UEM Client が含まれています。

1. デバイスで、［設定］ > ［**Google** サービスと環境設定］の順に選択します。
2. ［設定と復元］をタップします。
3. ［仕事用プロファイルを設定］をタップします。
4. ［次へ］をタップします。
5. ［デバイスポリシーによる写真の撮影とビデオの録画を許可］ダイアログボックスで、［今回のみ］をタップします。
6. 管理者から受け取った QR コードをスキャンします。
7. ［同意する］をタップします。
8. ［次へ］をタップします。
9. 管理者がアクティベーションをどのように設定したかによって、デバイスまたは仕事用領域のロックを設定するように求められる場合があります。
10. ［仕事チェックリスト］画面の［仕事用アプリをインストール］の下で［インストール］をタップします。
11. UEM Client がインストールされたら、［完了］をタップします。
12. ［**BlackBerry UEM** をセットアップ］をタップします。
13. ライセンス使用許諾契約書を参照して、［同意する］をタップします。

デバイスが仕事用プロファイルの設定を終了します。

終了したら： デバイスを無効にして UEM から削除する場合は、UEM Client から削除できます。

管理対象 Google Play アカウントを使用した Android Management デバイスのアクティベーション

次のアクティベーション手順は、アクティベーションタイプ 仕事用と個人用 - フルコントロール （Android Management）または 仕事用領域のみ （Android Management）が割り当てられた Android デバイスに適用されます。Android Management 仕事用と個人用 - ユーザーのプライバシー アクティベーションタイプの管理対象 Google Play アカウントに接続されているデバイスをアクティベーションするには、「仕事用と個人用 - ユーザーのプライバシー アクティベーションタイプの Android Management デバイスのアクティベーション」を参照してください。

ユーザーに送信するアクティベーションメールに QR Code を含めることができます。ユーザーが QR Code コードをスキャンすると、UEM Client が自動的にダウンロードされます。アクティベーションメールメッセージに QR Code を設定して含めるには、アクティベーションのデフォルトページ（［設定］ > ［一般設定］ > ［アクティベーションのデフォルト］）の［デバイスアクティベーションに QR コードを許可する］チェックボックスをオンにする必要があります。デフォルトの Android Management アクティベーションメールテンプレート（または同等のカスタム）を使用します。

次のアクティベーション手順をデバイスユーザーに送信します。

作業を始める前に： デバイス管理者から、デバイスのアクティベーションに必要な情報を記載したメールが 1 つ以上送信されました。メールメッセージには、QR Code をインストールしてデバイスをアクティベーションするために必要な UEM Client が含まれています。

1. アクティベーションするデバイスで、デバイス設定画面が表示されない場合は、デバイスを工場出荷時のデフォルト設定にリセットします。
2. デバイスの QR Code リーダーを開くには、デバイスの画面を 7 回タップします。
3. UEM Client をダウンロードするには、管理者がアクティベーションメールメッセージで指定した QR Code をスキャンします。
   UEM Client が自動的にダウンロードされます。
4. UEM Client を開きます。
5. 使用許諾契約書を読み、［使用許諾契約に同意します］チェックボックスをタップします。
6. ［プロファイルの設定］画面で、［設定］をタップします。仕事用プロファイルを設定するのに時間がかかる場合があります。
7. 画面のロック解除方法を選択します。
8. デバイスの起動時にパスワードが要求されるように、［安全な起動］画面でプロンプトが表示されたら、［はい］をタップします。
9. デバイスのパスワードを入力し、確認のためにもう一度入力して、［**OK**］をタップします。
10. 通知の表示方法を選択し、［完了］をタップします。
11. UEM Client パスワードを作成し、［**OK**］をタップします。BlackBerry Dynamics アプリを使用している場合、すべての BlackBerry Dynamics アプリにサインインする際にもこのパスワードを使用します。
12. 次の画面で、［登録］をタップします。
13. UEM Client および BlackBerry Dynamics アプリの指紋認証を設定する場合は、画面の指示に従います。それ以外の場合は、［キャンセル］をタップします。
14. デバイスからサインアウトしている場合は、BlackBerry UEM のアクティベーションを完了するためにデバイスのロックを解除します。
15. BlackBerry Secure Connect Plus への接続の許可を求めるプロンプトが表示されたら、［**OK**］をタップして、接続が有効になるまで待ちます。
16. デバイスに仕事用アプリをインストールするように促すプロンプトが表示されたら、画面の手順に従います。

終了したら： アクティベーションプロセスの正常な完了を確認するには、次のいずれかを実行します。

- UEM Client で、⋮> ［バージョン情報］をタップします。［アクティブ化されたデバイス］セクションで、デバイス情報とアクティベーションのタイムスタンプが存在していることを確認します。
- BlackBerry UEM Self-Service コンソールで、デバイスがアクティブ化されたデバイスとして一覧に表示されていることを確認します。ユーザーがデバイスをアクティブ化した後、ステータスの更新に最大で 2 分かかることがあります。

iOS デバイスのアクティベーション

ユーザーが BlackBerry UEM Client をインストールして iOS と iPadOS デバイスをアクティブ化する手順は、デバイスの OS バージョン、およびアクティベーションタイプに MDM コントロールが含まれているかどうかによって異なります。ユーザーに送信するアクティベーションメールでユーザーにデバイスのアクティベーション手順を伝えることができます。アクティベーションメールテンプレートの作成についての詳細は、「アクティベーションメールテンプレートを作成」を参照してください。

MDM 制御 アクティベーションタイプで iOS または iPadOS デバイスをアクティブ化する

MDM 制御 アクティベーションタイプまたは MDM オプションを有効にした ユーザーのプライバシー アクティベーションタイプのデバイスをアクティブにするには、次のアクティベーション手順をデバイスユーザーに送信します。

アクティベーション中、ユーザーは BlackBerry UEM Client を終了して手動で MDM プロファイルをインストールする必要があります。

作業を始める前に： デバイスでロックダウンモードが有効になっている場合（iOS および iPadOS 16 以降）、デバイスをアクティベーションするにはロックダウンモードを無効にする必要があります。ロックダウンモードでは、アクティベーションに必要な設定プロファイルのインストールができません。必要に応じて、アクティベーション後にロックダウンモードを有効にすることができます。

1. デバイスで、UEM Client を App Store からインストールします。
2. UEM Client を開き、使用許諾契約書を承諾します。
3. 次の操作のいずれかを実行します。

タスク	手順
QR Code をスキャンして、デバイスをアクティベーションします。	a. をタップします。 b. UEM Client の写真撮影とビデオ録画を許可するには、［許可］をタップします。 c. 受信したアクティベーションメールの QR Code をスキャンします。
デバイスを手動でアクティベーションします。	a. 仕事用メールアドレスを入力して、アクティベーションパスワードを入力します。 b. 必要に応じて、サーバーアドレスを入力します。サーバーアドレスは、受信したアクティベーションメールまたは BlackBerry UEM Self-Service で確認できます。 c. ［次へ］をタップします。

4. UEM Client に通知の送信を許可するには、［許可］をタップします。［許可しない］を選択すると、デバイスがアクティブ化されなくなります。
5. 設定プロファイルのインストールを求めるプロンプトが表示されたら、［**OK**］をタップします。
6. 設定プロファイルのダウンロードを求めるプロンプトが表示されたら、［許可］をタップします。

7. ダウンロードが完了したら、［設定］を開きます。
8. ［全般］をタップして［**VPN** とデバイス管理］に移動します。
9. プロファイルをインストールするには、［**BlackBerry UEM** プロファイル］をタップし、画面の指示に従います。
10. インストールが完了したら、アクティベーションを完了するために、UEM Client に戻ります。
11. デバイスに仕事用アプリをインストールするように促すプロンプトが表示されたら、画面の手順に従います。

終了したら： アクティベーションプロセスの正常な完了を確認するには、次のいずれかの操作を実行します。

- デバイスで UEM Client を開いて、［バージョン情報］をタップします。［アクティブ化されたデバイス］および［コンプライアンスステータス］セクションで、デバイス情報とアクティベーションのタイムスタンプが存在することを確認します。
- BlackBerry UEM Self-Service で、デバイスがアクティブ化されたデバイスとして一覧に表示されていることを確認します。ユーザーがデバイスをアクティブ化した後、ステータスの更新に最大で 2 分かかることがあります。

Apple ユーザー登録を使用した iOS または iPadOS デバイスのアクティブ化

Apple ユーザー登録は、サポートされているバージョンの iOS および iPadOS を実行しているデバイスでサポートされています。Apple ユーザー登録を使用してデバイスをアクティベーションするには、次のアクティベーション手順をデバイスユーザーに送信します。

作業を始める前に：

- Apple ユーザー登録用の QR Code が記載されたアクティベーションメールを受信したことを確認します。メールを受信していない場合は、管理者に連絡してください。
- BlackBerry UEM でデバイスがすでにアクティブ化されている場合は、デバイスを無効にする必要があります。
- BlackBerry UEM Client をアンインストールします。
- 組織を通じて管理されている Apple ID アカウントが必要です。
- デバイスは監視対象のデバイスであってはなりません。デバイスが監視対象である場合、Apple ID の近くの設定アプリに表示されます。
- デバイス（iOS および iPadOS 16 以降）でロックダウンモードが有効になっている場合、デバイスをアクティブ化するには無効にする必要があります。ロックダウンモードでは、アクティベーションに必要な設定プロファイルのインストールができません。必要に応じて、アクティベーション後にロックダウンモードを有効にすることができます。

1. Apple ユーザー登録用の QR Code が含まれているアクティベーションメールを開きます。QR Code の有効期限が切れている場合は、BlackBerry UEM Self-Service に新しいアクティベーションコードを要求するか、管理者に連絡できます。
2. デバイスでカメラアプリを開き、アクティベーションメールの QR コードをスキャンします。プロンプトが表示されたら、通知をタップして Safari で URL を開きます。
3. UEM 設定プロファイルのダウンロードを求めるプロンプトが表示されたら、［許可］をタップします。
4. ダウンロードが完了したら、［閉じる］をタップします。
5. ［設定］ **>** ［一般］ **>** ［プロファイル］に移動します。

6. ［**UEM** プロファイル］をタップします。
7. ［ユーザー登録］画面で、［**iPhone** を登録］または［**iPad** を登録］をタップします。
8. パスコードを入力します。
9. 管理 Apple ID 資格情報を使用して Apple ID にログインします。
10. 管理者が UEM Client を割り当てた場合は、プロンプトが表示されたら［インストール］をタップするか、仕事用アプリを開きます。
11. UEM Client をセットアップするには、アプリを開き、使用許諾契約に同意します。画面に表示される手順に従って、アクティベーションプロセスを完了します。

終了したら： アクティベーションプロセスの正常な完了を確認するには、次のいずれかの操作を実行します。

- デバイスで UEM Client を開いて、［バージョン情報］をタップします。［アクティブ化されたデバイス］および［コンプライアンスステータス］セクションで、デバイス情報とアクティベーションのタイムスタンプが存在することを確認します。
- BlackBerry UEM Self-Service で、デバイスがアクティブ化されたデバイスとして一覧に表示されていることを確認します。ユーザーがデバイスをアクティブ化した後、ステータスの更新に最大で 2 分かかることがあります。

BlackBerry UEM Self-Service による macOS または Apple TV デバイスのアクティブ化

ユーザーは、BlackBerry UEM Self-Service を使用して macOS および Apple TV デバイスをアクティベーションします。詳細および手順については、『UEM Self-Service ユーザーガイド』を参照してください。

Windows 10 タブレットまたはコンピューターのアクティベーション

Windows 10 デバイスをアクティベーションするには、次のアクティベーション手順をデバイスユーザーに送信します。MDM 制御 アクティベーションタイプを使用して Windows 10 デバイスを管理する場合、デバイスは Microsoft System Center Configuration Manager で管理できないことに注意してください。

次のアクティベーション手順をデバイスユーザーに送信します。

作業を始める前に： 証明書サーバーアドレスが記載されたアクティベーションメールを受信したことを確認します。メールを受信していない場合は、管理者に連絡してください。

1. 証明書サーバーのアドレスをデバイスのブラウザーに入力するか貼り付けます。
2. ［保存］をクリックします。
3. 証明書ダウンロードの通知で、［開く］をクリックします。
4. ［開く］をクリックします。
5. ［証明書のインストール］をクリックします。
6. ［現在のユーザー］オプションを選択して、［次へ］をクリックします。
7. ［次の保存先にすべての証明書を保存する］オプションを選択し、［参照］をクリックします。
8. ［信頼済みルート証明機関］を選択し、［**OK**］をクリックします。
9. ［次へ］ **>** ［完了］ **>** ［**OK**］ **>** ［**OK**］をクリックします。
10. ［スタート］ボタンをクリックします。
11. 次の操作のいずれかを実行します。

デバイスの **OS** バージョン	手順
Windows 10 バージョン 1607 以降	**a.** ［設定］ **>** ［アカウント］ **>** ［仕事または学校のアクセス］をタップします。 **b.** ［デバイス管理のみに登録］をタップします。
バージョン 1607 より前の Windows 10	**a.** ［設定］ **>** ［アカウント］ **>** ［仕事用アクセス］をタップします。 **b.** ［接続］をタップします。

12. ［メールアドレス］フィールドにメールアドレスを入力して、［続行］をタップします。
13. プロンプトが表示されたら、［サーバー］フィールドにサーバー名を入力し、［続行］をタップします。サーバー名は、管理者から受信したアクティベーションメールに記載されているか、アクティベーションパスワードを設定するときに BlackBerry UEM Self-Service で見つけることができます。
14. ［アクティベーションパスワード］フィールドにアクティベーションパスワードを入力して［続行］をタップします。アクティベーションパスワードは、管理者から受信したアクティベーションメールに記載されています。または UEM Self-Service で、別のアクティベーションパスワードを設定することもできます。
15. ［完了］をタップします。

終了したら：

- アクティベーションプロセスの正常な完了を確認するには、次のいずれかの操作を実行します。

    - デバイスで［設定］>［アカウント］>［仕事または学校のアクセス］（または［仕事用アクセス］）をクリックし、デバイスが UEM に接続されることを確認します。
    - UEM Self-Service で、デバイスがアクティブ化されたデバイスとして一覧に表示されていることを確認します。ユーザーがデバイスをアクティブ化した後、ステータスの更新に最大で 2 分かかることがあります。
- 管理者から要求された場合は、他のアプリで使用されるアカウントに仕事用アカウントを追加して、必須オンラインアプリにアクセスできるようにします。
    - Windows 10 バージョン 1607 以降の場合、［設定］>［アカウント］>［仕事および学校のアクセス］>［接続］をクリックします。仕事用メールアドレスを入力して、パスワードを入力します。
    - 1607 よりも前のバージョンの Windows 10 の場合、［設定］>［アカウント］>［メールとアカウント］をクリックします。［他のアプリで使用されるアカウント］の下で、［仕事または学校のアカウントを追加］をクリックし、仕事用のメールアドレスとパスワードを入力します。

Android ゼロタッチ登録のサポートの構成

BlackBerry UEM で Android ゼロタッチ登録を使用して、多数の Android Enterprise デバイスを同時に導入できます。デバイスはゼロタッチ登録をサポートしている必要があります。

組織が、認定販売代理会社からサポートされているデバイスを購入すると、その販売代理会社がゼロタッチ登録アカウントを設定して、デバイスをアカウントに追加します。ユーザーがこれらのデバイスを初めて設定するときまたは工場出荷時の設定にデバイスをリセットするときに、デバイスは自動的に BlackBerry UEM Client をダウンロードし、UEM アクティベーションプロセスを開始します。

ユーザーがアクティベーションの完了前にデバイスを再起動した場合、アクティベーションをキャンセルした場合、またはアクティベーションの完了前にバッテリーがなくなった場合、デバイスは自動的に工場出荷時の設定にリセットされ、アクティベーションプロセスが再開されることに注意してください。

1. 管理コンソールのメニューバーで、［設定］ > ［外部統合］をクリックします。
2. ［**Android** エンタープライズ］をクリックします。
3. ［ゼロタッチコンソールを起動する］をクリックします。
4. UEM を使用して Android ゼロタッチに初めて接続する場合は、［次へ］をクリックして、組織のゼロタッチアカウントに関連付けられているアドレスを使用して Google にサインインします。
5. 登録設定を作成または管理し、デバイスに割り当てます。

   Android ゼロタッチポータルを使用して、登録設定を管理することもできます。

終了したら：

- UEM で、適切なプロファイルと IT ポリシーがユーザーに割り当てられていることを確認します。ゼロタッチ登録を使用するには、「仕事用および個人用 - フルコントロール（Android Enterprise 完全管理のデバイス）」または「仕事用領域のみ（Android Enterprise）」アクティベーションタイプを有効にして、アクティベーションプロファイルを割り当てる必要があります。
- ユーザーにデバイスを配布します。

Knox Mobile Enrollment を使用した複数のデバイスのアクティブ化

Samsung Knox Mobile Enrollment を使用して、同時に多数の Samsung Knox デバイスを導入できます。組織は、認定販売代理店または、デバイスが Knox Mobile Enrollment を使用できるように、Samsung とデバイス IMEI を進んで直接共有する販売代理店からデバイスを購入しします。ユーザーがこれらのデバイスを初めて設定するときまたは工場出荷時の設定にデバイスリセットするときに、デバイスは自動的に BlackBerry UEM Client をダウンロードし、BlackBerry UEM でアクティベーションプロセスを開始します。

ユーザーがアクティベーションの完了前にデバイスを再起動した場合やアクティベーションをキャンセルした場合、またはアクティベーションの完了前にバッテリーがなくなった場合、デバイスは自動的に工場出荷時の設定にリセットされ、アクティベーションプロセスが再開されます。

メモ：Android 11 以降を実行しているデバイスの場合、Knox Mobile Enrollment は、デバイス管理者ベースの登録をサポートしません。詳細については、「Knox Mobile Enrollment 1.36 リリースノート」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］ > ［外部統合］ > ［**KNOX Mobile Enrollment**］をクリックします。
2. UEM JSON ファイルをダウンロードします。
3. 画面に表示される手順を完了します。

終了したら： アクティベーションが完了したら、ダウンロードした JSON ファイルを使用して、CFPrint セクションのエントリを Knox Mobile Enrollment の設定時に追加したエントリと比較します。エントリが異なる場合は、Knox Mobile Enrollment ページの ［カスタム **JSON** データ］ フィールドで、.json ファイルからテキスト全体をコピーします。

DEP に登録されている iOS デバイスのアクティベーション

BlackBerry UEM 管理コンソールを使用して、Apple の Device Enrollment Program（DEP）に iOS および iPadOS デバイスを登録し、デバイスに登録設定を割り当てることができます。登録設定には、MDM 登録中にデバイスに割り当てられた追加のルールが含まれています。

UEM を DEP と同期するには、Apple Business Manager アカウントを使用できます。Apple Business Manager は、DEP 内の iOS デバイスの登録や管理、Apple VPP アカウントの管理を行える Web ベースのポータルです。組織で DEP または VPP を使用している場合は、Apple Business Manager にアップグレードできます。

DEP に登録されているデバイスをアクティベーションするには、次の操作を実行します。

手順	アクション
1	DEP での iOS デバイスの登録および BlackBerry UEM サーバーへの割り当て。
2	DEP 登録設定の追加。
3	オプションで、BlackBerry UEM Client をアプリリストに追加してユーザーアカウントまたはユーザーグループに割り当てるには、「アプリリストへの iOS アプリの追加」を参照してください。
4	デフォルトのアクティベーションプロファイルを使用しない場合は、アクティベーションプロファイルを作成し、それを DEP デバイスに割り当てます（［ユーザー］ > ［Apple DEP デバイス］）。
5	ユーザーがデバイスをアクティブ化する方法を選択します。 • アクティベーションメールを複数のユーザーに送信 または、Apple DEP メールテンプレートを使用して、アクティベーションメールを特定のユーザーに送信します。 • UEM を会社のディレクトリに接続している場合、ユーザーは会社のディレクトリのユーザー名とパスワードを使用できます。ユーザーは、domain\username の形式でユーザー名を入力する必要があります（資格情報は組織のドメインおよびユーザー名変数（「%UserDomain%/%UserName%」）に一致します）。 • ユーザーが iOS デバイスへのユーザーの割り当て できます。UEM でユーザーをデバイスに割り当てると、デバイスのアクティベーション中にユーザー名またはパスワードの入力を求められません。
6	デバイスをユーザーに配布し、アクティベーションを完了できるようにします。アクティベーションの完了後、ユーザーは UEM Client をインストールして起動する必要があります。

DEP での iOS デバイスの登録および BlackBerry UEM サーバーへの割り当て

iOS デバイスを Apple Device Enrollment Program（DEP）に登録するには、Apple Business Manager または DEP ポータルにデバイスのシリアル番号を入力し、デバイスを BlackBerry UEM サーバーに割り当てる必要があります。シリアル番号を入力するには、各番号を入力するか、購入時に Apple によりデバイスに割り当てられた注文番号を選択するか、シリアル番号を含む .csv ファイルをアップロードします。

作業を始める前に： DEP 用 BlackBerry UEM を設定します。

1. Apple Business Manager または DEP ポータルにログインします。
2. ［**Device Enrollment Program**］セクションで、［デバイスを管理］をクリックします。
3. デバイスのシリアル番号を入力するには、画面の手順に従います。
4. UEM サーバーにシリアル番号を割り当てます。

終了したら： DEP 登録設定の追加。

DEP 登録設定の追加

登録設定では、DEP に登録するデバイスを BlackBerry UEM でアクティブにするときの設定方法を定義できます。組織で必要な数の登録設定を作成できます。

作業を始める前に： DEP での iOS デバイスの登録および BlackBerry UEM サーバーへの割り当て。

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**］をクリックします。
2. DEP アカウントの名前をクリックします。
3. ［**DEP** 登録設定］セクションで、＋をクリックします。
4. 設定の名前を入力します。
5. DEP デバイスを UEM と同期するときに、UEM により登録設定を自動的に割り当てる場合、［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 は Apple DEP と毎日、および Apple DEP デバイスページが表示されるごとに同期されます。新しい DEP デバイスには登録設定を 1 つだけ自動的に割り当てることができます。この設定で登録設定を以前に作成していた場合、設定は前の登録設定から削除され、新しい登録設定に追加されます。以前作成した登録設定でこの設定が選択されていて、この登録設定がデバイスに適用されている場合、UEM が新しい登録設定を割り当てることはありません。
6. 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。
7. ［デバイス設定］リストで、次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］：登録設定を受け入れるように求めるプロンプトは表示されません。
   - ［**MDM** プロファイルの削除を許可］：ユーザーはデバイスを無効にできます。
   - ［デバイスが設定されるまで待機する］：アクティベーションプロセスが完了するまで、ユーザーはデバイス設定をキャンセルできません。
8. ［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は表示されません。
位置情報サービス	このデバイスでは位置情報サービスが無効にされています。
復元	ユーザーはバックアップファイルからデータを復元できません。
Android から移動	Android デバイスからデータを復元することはできません。
Apple ID	ユーザーは Apple ID と iCloud にサインインできません。
使用条件	ユーザーに iOS 使用条件が表示されません。
Siri	Siri は、デバイスで無効にされています。
診断	診断情報はセットアップ時にデバイスから自動的に送信されません。
バイオメトリック	ユーザーは Touch ID を設定できません。
支払い	ユーザーは Apple Pay を設定できません。
ズーム	ユーザーは Zoom を設定できません。
ホームボタンの設定	ユーザーはホームボタンのクリックを調整できません。
画面時間	DEP の登録時は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ません。
iMessage および FaceTime	iMessage および FaceTime 画面がデバイスに表示されません。
ディスプレイトーン	ディスプレイトーンがデバイスに表示されません。
プライバシー	プライバシー画面がデバイスに表示されません。
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ません。
監視の移行	監視の移行画面がデバイスに表示されません。
SIM 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ません。
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ません。

9. ［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］チェックボックスを選択した場合は、［はい］をクリックします。

終了したら：

- ［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選択しなかった場合は、適切な登録設定をデバイスに割り当てる必要があります。［ユーザー］ > ［**Apple DEP** デバイス］で、同じ DEP アカウントに登録されているデバイスを選択し、 をクリックします。登録設定を選択して割り当てます。
- デフォルトのアクティベーションプロファイルを使用しない場合は、アクティベーションプロファイルを作成し、Apple DEP に登録されているデバイスに割り当てます。［ユーザー］ > ［**Apple DEP** デバイス］で、同じ DEP アカウントに登録されているデバイスを選択し、 をクリックします。プロファイルを選択して割り当てます。
- デバイスのアクティベーション中に、ユーザーにユーザー名とパスワードの入力を求めるメッセージが表示される場合があります。ユーザーがデバイスをアクティブ化する方法を選択します。
  - アクティベーションメールを複数のユーザーに送信 または、Apple DEP メールテンプレートを使用して、アクティベーションメールを特定のユーザーに送信します。
  - UEM を会社のディレクトリに接続している場合、ユーザーは会社のディレクトリのユーザー名とパスワードを使用できます。ユーザーは、domain\username の形式でユーザー名を入力する必要があります（資格情報は組織のドメインおよびユーザー名変数（「%UserDomain%/%UserName%」）に一致します）。
  - ユーザーが iOS デバイスへのユーザーの割り当て できます。UEM でユーザーをデバイスに割り当てると、デバイスのアクティベーション中にユーザー名またはパスワードの入力を求められません。
- デバイスをユーザーに配布し、アクティベーションを完了できるようにします。アクティベーションの完了後、ユーザーは BlackBerry UEM Client をインストールして起動する必要があります。

iOS デバイスへのユーザーの割り当て

デバイスをアクティブにする前に、Apple DEP に登録されているデバイスにユーザーを直接割り当てられます。ユーザーをデバイスに直接割り当てると、デバイスのアクティベーション中にユーザー名またはパスワードの入力を求められません。

1. メニューバーで［ユーザー］ > ［**Apple DEP** デバイス］をクリックします。
2. 割り当てるデバイスの［ユーザーの関連付け］列で、［選択］をクリックします。
3. ［ユーザーの選択］検索ボックスで、デバイスに割り当てるユーザーを検索します。
4. 検索結果のリストで、ユーザーアカウントをクリックします。
5. ［保存］をクリックします。

終了したら：

- アクティブ化されたデバイスの所有者を表示するには、［ユーザーの関連付け］列で、［ユーザー名］リンクをクリックします。
- iOS デバイスからユーザーを削除するには、［ユーザーの関連付け］列で、ユーザーを削除するデバイスのユーザー名のリンクをクリックします。［割り当て解除］をクリックします。

Apple Configurator 2 を使用した iOS デバイスのアクティブ化

オンプレミスに BlackBerry UEM がある場合は、Apple Configurator 2 を使用してアクティベーションできるように iOS および iPadOS デバイスを準備できます。ユーザーは、BlackBerry UEM Client を使用せずに、準備のできたデバイスをアクティベーションできます。ユーザーには、ユーザー名とアクティベーションパスワードだけが必要です。

Apple Configurator は UEM Cloud でサポートされていません。

メモ： 一部の UEM 機能では、UEM Client をユーザーに割り当てる必要があります。ユーザーは、デバイスをアクティブにした後で UEM Client を起動する必要があります。詳細については、KB 39313 を参照してください。

Apple Configurator 2を使用して iOS デバイスをアクティブにするには、次の操作を実行します。

手順	アクション
1	オプションで、UEM Client をアプリリストに追加して、ユーザーアカウントまたはユーザーグループに割り当てます。「iOS アプリをアプリリストに追加」を参照してください。
2	BlackBerry UEM サーバー情報の Apple Configurator 2 への追加。
3	Apple Configurator 2 を使用した iOS デバイスの準備。
4	アクティベーションプロファイルを作成し、それをユーザーアカウントまたはグループに割り当てます。
5	アクティベーションメールを複数のユーザーに送信 またはアクティベーションメールを特定のユーザーに送信します。
6	デバイスをユーザーに配布し、アクティベーションを完了できるようにします。コンプライアンスプロファイルを強制するには、セットアップの完了後に、ユーザーが UEM Client アプリをインストールして起動する必要があります。

BlackBerry UEM サーバー情報の Apple Configurator 2 への追加

作業を始める前に： Apple から最新のバージョンの Apple Configurator 2 をダウンロードしインストールします。

1. Apple Configurator 2 メニューで［プレゼンス］ > ［サーバー］を選択します。
2. ＋ > ［次へ］をクリックします。
3. ［名前］フィールドに、サーバーの名前を入力します。
4. ［ホスト名または **URL**］フィールドに、*<http or https>://<servername>:<port>* の形式で、UEM サーバーの URL を入力します。ここで、デフォルトのポート番号は 8885 です。

5. ［次へ］をクリックします。
6. ［サーバー］ウィンドウを閉じます。

終了したら： Apple Configurator 2 を使用した iOS デバイスの準備。

Apple Configurator 2 を使用した iOS デバイスの準備

デバイスを準備するときに、Apple Configurator 2 は、デバイスを消去し、デバイス OS を最新バージョンにアップグレードします。

作業を始める前に： BlackBerry UEM サーバー情報の Apple Configurator 2 への追加。

1. Apple Configurator 2 を開きます。
2. 1 台以上の iOS デバイスをコンピューターに接続します。
3. ［準備］をクリックします。
4. ［設定］ドロップダウンリストで［手動］を選択します。［次へ］をクリックします。
5. ［サーバー］ドロップダウンリストで、BlackBerry UEM サーバーを選択します。［次へ］をクリックします。
6. 必要に応じて［デバイスを監視する］チェックボックスをオンにします。［次へ］をクリックします。
7. ［デバイスを監視する］をオンにした場合、組織の情報を入力します。
8. ［準備］をクリックして、デバイスが準備されるまで待機します。このプロセスには、最大 15 分かかります。

終了したら： アクティベーションのためにデバイスをユーザーに分散します。

承認されたデバイス ID のリストのインポートまたはエクスポート

固有のデバイス識別子のリストをインポートおよびエクスポートして、BlackBerry UEM に登録できるデバイスを制限できます。現在、UEM でサポートされている唯一の一意の識別子は、デバイスのシリアル番号です。

作業を始める前に： リストをインポートするには、固有のデバイス識別子のリストを含む .csv ファイルがあることを確認します。

1. 管理コンソールのメニューバーで、［設定］ > ［一般設定］ > ［アクティベーションのデフォルト］をクリックします。
2. ［承認されたデバイス **ID**（**.csv**）のアップロード］フィールドの横にある［デバイス **ID** をインポートまたはエクスポート］セクションで、［参照］をクリックします。
3. .csv ファイルに移動します。
4. ［開く］をクリックします。
5. ［保存］をクリックします。

終了したら： リストをエクスポートするには、［承認されたデバイス **ID**（**.csv**）のエクスポート］をクリックします。

デバイスの無効化

デバイスが無効化されると、BlackBerry UEM 内の、デバイスとユーザーアカウント間の接続が削除されます。デバイスは管理できなくなり、管理コンソールに表示されなくなります。ユーザーはデバイス上の仕事用データにアクセスできません。

デバイスは、次のいずれかの方法を使用して無効化できます。

- 管理者は、［仕事用データのみを削除］または［すべてのデバイスデータを削除］コマンドを使用して UEM 管理コンソールからデバイスを無効化できます。
- デバイスが割り当てられたコンプライアンスプロファイルのルールに違反し、指定された強制アクションがデバイスを無効化する場合も UEM はそのデバイスを無効化できます。
- ユーザーは、［仕事用データのみを削除］または［すべてのデバイスデータを削除］コマンドを使用して UEM Self-Service からデバイスを無効化できます。
- ユーザーは UEM Client を使用して iOS および Android デバイスを無効化できます。
- ユーザーは、［設定］>［アカウント］>［仕事用アクセス］>［削除］から Windows 10 デバイスを無効にできます。

指定されたアクティベーションタイプを持つデバイスを無効にする場合は、次の点に注意してください。

アクティベーションタイプ	考慮事項
仕事用プロファイルのみがある Android Enterprise デバイス	SD カードからすべてのデータを削除し、工場出荷時リセット保護を削除するオプションがあります。
仕事用と個人用 - フルコントロール アクティベーションを使用する Android Enterprise デバイス	• ［すべてのデバイスデータを削除］コマンドは、Android 10 でのみサポートされています。UEM は、2024 年 1 月時点で Android 10 をサポートしなくなります。 • ［仕事用データのみを削除］コマンドは、Android 11 以降でサポートされています。このコマンドを使用すると、すべての仕事用データとアプリが削除されますが、ユーザーは個人データとアプリを保持して、管理されていないデバイスを引き続き使用できます。
Android Enterprise および 仕事用と個人用 - ユーザーのプライバシー アクティベーションを備えた 仕事用と個人用 - フルコントロール デバイス	［仕事用データのみを削除］コマンドを使用する場合は、ユーザーのデバイスの通知に表示される理由を指定できます。コンプライアンスルールに違反してデバイスが非アクティブ化された場合、通知にはデバイスがコンプライアンスに違反した理由が示されます。
Knox MDM	• 内部アプリがアンインストールされます。 • 必要に応じて、アプリリストからインストールされた一般のアプリでアンインストールオプションが使用できるようになります。
仕事用と個人用 - フルコントロール を搭載した Samsung Knox Workspace デバイス	デバイスを無効にすると、デバイスからすべてのデータが削除されます。［無効化でのデータ消去］IT ポリシールールを使用して、消去するデータを指定できます。

デバイスアクティベーションのトラブルシューティング

デバイスのアクティベーションのトラブルシューティングを実行する場合は、必ず次の内容を確認してください。

- デバイスタイプとアクティベーションタイプのライセンスが使用可能であることを確認します。
- デバイスに割り当てられているアクティベーションプロファイルがデバイスタイプをサポートしていることを確認します。
- デバイスでネットワーク接続を確認します。
  - モバイルまたは Wi-Fi ネットワークがアクティブで、十分な通信可能範囲があることを確認してください。
  - 仕事用 Wi-Fi の場合は、デバイスのネットワークパスが利用可能であることを確認してください。
  - ユーザーが VPN または仕事用 Wi-Fi プロファイルを手動で設定して、組織のファイアウォール内のコンテンツにアクセスする必要がある場合は、デバイスでユーザーのプロファイルが正しく設定されていることを確認してください。
- 改造またはルート化された OS、制限された OS バージョン、または制限されたデバイスモデルを持つデバイスのコンプライアンスルールを設定している場合、デバイスが準拠していることを確認します。
- UEM がオンプレミス環境にインストールされ、デバイスが組織のファイアウォールを介して UEM または BlackBerry Infrastructure との接続を試みている場合は、適切なファイアウォールが開いていることを確認してください。
- デバイスログを取得します。デバイスログの取得の詳細については、iOS の場合は KB 36986 を、Android の場合は KB 32516 を参照してください。

Android Management デバイス

- Android Enterprise と Android Management に対して個別のアクティベーションプロファイルを作成する必要があります。Android Enterprise と Android Management のアクティベーションタイプが同じプロファイルで指定されている場合、Android Management タイプが Android Enterprise より低いランクになっていても、タイプが優先されます。Android Management アクティベーションタイプのパスワードとアクティベーション情報のみが QR コードに埋め込まれます。
- 一部のデバイスでは、デバイスが正常にアクティベーション処理を完了した後、不必要な［セットアップと復元］画面が表示されることがあります。

Knox Workspace デバイスおよび **Android Enterprise** デバイス

Samsung Knox Workspace を使用する Samsung デバイスのアクティベーションのトラブルシューティングを行う場合は、Knox コンテナのバージョンがサポートされていることを確認します。Knox Workspace には、Knox Container 2.0 以降が必要です。

Android Enterprise デバイスのアクティベーションのトラブルシューティングを行うときは、UEM ユーザーアカウントに Google ドメインと同じメールアドレスがあることを確認します。メールアドレスが一致しない場合は、デバイスに「デバイスをアクティブ化できません - サポートされていないアクティベーションタイプです」というエラーが表示されます。

トラブルシューティング：アクティベーションエラーと問題

アクティベーションエラー

エラー	解決策
サーバーのライセンスが使用できないためデバイスのアクティベーションを完了できません。管理者に問い合わせてください。	UEM 管理コンソールで、ライセンスが使用可能であることを確認します。必要に応じて、ライセンスをアクティブ化するか、追加のライセンスを購入します。
プロファイルのインストールに失敗しました。証明書「AutoMDMCert.pfx」をインポートできませんでした。	このエラーは、プロファイルが既に iOS デバイスに存在する場合に、デバイスに表示されます。 デバイスで［設定］>［全般］>［プロファイル］の順に選択し、プロファイルが既に存在していることを確認します。プロファイルを削除して、再度アクティブ化してみてください。問題が存続する場合は、データがキャッシュされている可能性があるため、デバイスをリセットする必要が生じることがあります。
プロファイルのインストールに失敗しました：新しい MDM ペイロードが古いペイロードと一致しません。	このエラーは、プロファイルが既に iOS デバイスに存在する場合に、デバイスに表示されます。 デバイスで［設定］>［全般］>［プロファイル］の順に選択し、プロファイルが既に存在していることを確認します。プロファイルを削除して、再度アクティブ化してみてください。問題が存続する場合は、データがキャッシュされている可能性があるため、デバイスをリセットする必要が生じることがあります。
エラー3007:サーバーを使用できません。	このエラーは、iOS デバイスに送信する MDM プロファイルに署名するために UEM が使用する証明書がデバイスから信頼されていない場合に発生することがあります（デバイスをアクティブ化すると、ユーザーはこの証明書を信頼するように求められます）。オンプレミス環境で、証明書を発行した CA のルート証明書をインストールします。設定関連の資料で「BlackBerry UEM が認証に使用する証明書の変更」を参照してください。 このエラーは、Blue Coat などの透過プロキシを設定して、標準外のトラフィックをポート 443 で監視する場合にも発生する可能性があり、UEM Client は必要な HTTP CONNECT コールおよび HTTP OPTIONS コールを UEM に対して作成できません。プロキシ設定によって UEM Client がこれらのコールをブロックしていないことを確認します。

エラー	解決策
サーバーに接続できません。接続またはサーバーアドレスを確認してください。	このエラーは、ユーザー名（または、BlackBerry Infrastructure への登録が無効になっている場合は顧客の住所）が正しく入力されていない場合、またはアクティベーションパスワードが設定されていない場合、または有効期限が切れている場合に発生することがあります。 ユーザー名、パスワード、およびお客様の住所（該当する場合）が正確であることを確認するか、UEM Self-Service を使用して新しいアクティベーションパスワードを設定してから、再試行してください。

アクティベーションの問題

問題	解決策
APN 証明書が無効なため、iOS または macOS デバイスをアクティベーションできません。	APN 証明書が正しく登録されていない可能性があります。 次の操作を 1 つ以上実行します。 • 管理コンソールのメニューバーで、［設定］ > ［外部統合］ > ［**Apple** プッシュ通知］をクリックします。APN 証明書のステータスが［インストール済み］であることを確認します。ステータスが正しくない場合は、APN 証明書の再登録を試みます。 • 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。 • 必要に応じて、新しい署名付きの CSR を BlackBerry から取得し、新しい APN 証明書を要求して登録します。詳細については、設定関連の資料で「APNs 証明書を取得して iOS および macOS デバイスを管理する」を参照してください。
ユーザーがアクティベーションメールを受信しません。	ユーザーがサードパーティのメールサーバーを使用している場合、UEM からのメールがスパムとしてマークされ、スパムメールフォルダーまたは迷惑メールフォルダーに入れられていることがあります。
Windows の［ユーザーの詳細］画面に、予測より多くのアクティベーションされた UEM デバイスが表示されています。	ユーザーがコンピューターに Windows 用の BlackBerry Access と BlackBerry Work をインストールすると、これらのアプリは Windows ユーザー詳細画面にデバイスとして表示されます。これは予期される動作です。

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