BlackBerry UEM

デバイスのアクティベーション

管理

12.17

目次

デバイスのアクティベーション..... 6
アクティベーションタイプ：iOS デバイス..... 6
アクティベーションタイプ：macOS デバイス..... 9
アクティベーションタイプ：Android デバイス..... 9
アクティベーションタイプ：Windows 10 デバイス..... 15

デバイスをアクティブ化する手順..... 16

要件：アクティベーション..... 17

BlackBerry Infrastructure でのユーザー登録の有効化..... 18

アクティベーション設定の管理..... 19
デフォルトのアクティベーション設定の指定..... 19
デフォルトのデバイスアクティベーションの設定..... 20
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..... 22
アクティベーションパスワードの有効期限の強制..... 23
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..... 23
アクティベーションメールを複数のユーザーに送信..... 24
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）..... 24

Android Enterprise アクティベーションのサポート..... 26
監視対象 Google Play アカウントを使用した Android Enterprise アクティベーションのサポート..... 26
G Suite ドメインを使用した Android Enterprise アクティベーションのサポート..... 27
Google Cloud ドメインを使用した Android Enterprise アクティベーションのサポート..... 27
Google Play にアクセスできない Android Enterprise デバイスのサポート..... 28
NFC ステッカーをプログラムしてデバイスをアクティブ化する..... 31

Windows 10 アクティベーションのサポート..... 32

iOS および **iPadOS** デバイスでの **Apple** ユーザー登録のサポート..... 33

Samsung Knox DualDAR のサポート..... 34

デバイスアクティベーション時のユーザー通知の有効化..... 35

アクティベーションプロファイルの作成.....36
アクティベーションプロファイルの作成.....36

デバイスのアクティベーション手順.....39
Android デバイスのアクティベーション.....39
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.....42
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.....43
監視対象の Google Play アカウントを使用して、仕事用領域のみ アクティベーションタイプで Android Enterprise デバイスをアクティベーションする.....45
監視対象の Google Play アカウントを使用して、仕事用と個人用 - フルコントロール アクティベーションタイプで Android Enterprise デバイスをアクティベーションする.....47
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.....48
MDM 制御 アクティベーションタイプの Android デバイスのアクティベーション.....50
iOS デバイスのアクティベーション.....51
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.....51
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.....52
macOS デバイスのアクティベーション.....53
Apple TV デバイスのアクティベーション.....54
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.....54

Android ゼロタッチ登録のサポートの構成.....56

Knox Mobile Enrollment を使用した複数のデバイスのアクティブ化..... 57

非監視対象 **iOS** デバイスの制限.....58

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..... 59

DEP に登録されている **iOS** デバイスのアクティベーション..... 60
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手順.....60
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.....61
iOS デバイスに登録設定を割り当てる.....62
登録設定の追加.....62
iOS デバイスに割り当てられた登録設定を削除.....64
登録設定の削除.....64
登録設定の設定を変更.....64
デバイスに割り当てられている登録設定の設定を表示.....64

iOS デバイスにアクティベーションプロファイルを割り当てる....65
iOS デバイスに割り当てられたアクティベーションプロファイルの削除....65
iOS デバイスへのユーザーの割り当て....65
iOS デバイスからのユーザー割り当ての解除....66
アクティブ化されたデバイスの所有者の表示....66

Apple Configurator 2 を使用した iOS デバイスのアクティブ化....67
Apple Configurator 2 を使用してデバイスをアクティブ化する手順....67
BlackBerry UEM サーバー情報の Apple Configurator 2 への追加....68
Apple Configurator 2 を使用した iOS デバイスの準備....68

デバイスのアクティベーションに関するトラブルシューティングのヒント....69
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。....70
ユーザー名とパスワードを確認して、再度実行してください。....70
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。....71
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。....71
エラー3007：サーバーが使用できません....71
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....72
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。....72
ユーザーがアクティベーションメールを受信していません....73
［ユーザーの詳細］画面に UEM でアクティベーションされている Windows デバイスとして表示されるデバイスが予測より多い....73

商標などに関する情報....74

デバイスのアクティベーション

ユーザーがデバイスをアクティブ化すると、デバイスが BlackBerry UEM に関連付けられます。これにより、管理者がデバイスを管理したり、ユーザーがデバイス上の仕事用データにアクセスしたり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、使用可能な機能を制御し、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。

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	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を提供できます。このアクティベーションタイプでは、別個のコンテナはデバイスにインストールされず、仕事用データの追加セキュリティも提供されません。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、BlackBerry UEM でアクティベーションされ、［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することはできません。 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、BlackBerry UEM が SIM カードおよび 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 ライセンスが利用可能かどうか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も指定できます。 • ［**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	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、iOS および iPadOS 13.1 以降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。
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、BlackBerry 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。 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。 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：**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 が提供す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。BlackBerry UEM とデバイスの間、および BlackBerry UEM とユーザーアカウントの間で独立した通信チャネルが確立されるため、デバイスとユーザーを個別に管理できます。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：**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、サポートしないデバイスは第 2 位を受け取ります。

Android のアクティベーションタイプを以下の表に示します。

- Android Enterprise デバイス
- 仕事用プロファイルがない Android デバイス
- Samsung Knox Workspace デバイス

Android Enterprise デバイス

次のアクティベーションタイプは Android Enterprise デバイスにのみ適用されます。

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。このアクティベーションタイプでは、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上に作成されます。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、［**Google Play** をワークスペースに追加］を選択します。この設定はデフォルトで有効になっています。デバイスが Google Play にアクセスできない場合は、この設定を選択解除し、アクティベーションプロセス中にセカンダリデバイスから BlackBerry UEM 登録アプリを使用する必要があります。 BlackBerry Secure Connect Plus および Knox Platform for Enterprise サポートを有効にするには、［**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 BlackBerry 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。このアクティベーションタイプでは、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上に作成されます。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は、BlackBerry 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）のログをサポートしています（Android 10 以前を実行している場合）。 Android Enterpriseデバイスの 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。この設定はデフォルトで有効になっています。デバイスが Google Play にアクセスできない場合は、この設定の選択を解除する必要があります。 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。 BlackBerry Secure Connect Plus および Knox Platform for Enterprise サポートを有効にするには、［**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。 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。 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 BlackBerry 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。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。 Android Enterpriseデバイスの Google Play アプリ管理を許可するには、［**Google Play** をワークスペースに追加］を選択します。この設定はデフォルトで有効になっています。デバイスが Google Play にアクセスできない場合は、この設定を選択解除し、アクティベーションプロセス中にセカンダリデバイスから BlackBerry UEM 登録アプリを使用する必要があります。 アクティベーションの実行時に、デバイスによって BlackBerry 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、［**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。 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。 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
MDM 制御	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を管理できます。個別の仕事用領域はデバイスに作成されず、仕事用データのセキュリティも追加されません。 メモ：このアクティベーションタイプは、Android 10 を使用するデバイスでは推奨されません。MDM 制御 アクティベーションタイプで Android 10 以降のデバイスをアクティベーションしようとすると失敗します。詳細については、https://support.blackberry.com/community にアクセスし、記事 48386 を参照してください。 デバイスが Knox MDM をサポートする場合、このアクティベーションタイプでは Knox MDM IT ポリシールールが適用されます。Knox MDM ポリシールールを適用しない場合は、［**MDM** 制御アクティベーションタイプが割り当てられた **Samsung** デバイスでは **Samsung KNOX** をアクティブ化する］チェックボックスをオフにします。 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 BlackBerry UEM Client に与える必要があります。
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。このアクティベーションタイプでは、個別のコンテナはデバイスにインストールされません。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、BlackBerry 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

次のアクティベーションタイプは、Knox Workspace をサポートする Samsung デバイスのみに適用されます。

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、https://support.blackberry.com/community にアクセスし、記事 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。このアクティベーションタイプでは、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 BlackBerry 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。このアクティベーションタイプでは、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。このアクティベーションタイプは、BlackBerry 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）のログをサポートしています（Android 11 以前を実行している場合）。 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 BlackBerry UEM Client に与える必要があります。
仕事用領域のみ -（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。このアクティベーションタイプでは、個人用領域が削除されて、仕事用領域がインストールされます。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は、BlackBerry 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）のログをサポートしています。 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 BlackBerry 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：Windows 10 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、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。 メモ：Windows 10 Mobile デバイスは、Microsoft でサポートされなくなりました。 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。

デバイスをアクティブ化する手順

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

手順	アクション
1	すべてのアクティベーション要件が満た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設定を構成します。
3	該当する場合は、次の情報を確認してください。 • Android Enterprise デバイスをサポートする予定がある場合は、「Android Enterprise アクティベーションのサポート」を参照してください。 • Windows 10 デバイスをサポートする予定がある場合は、「Windows 10 アクティベーションのサポート」を参照してください。 • Apple ユーザー登録デバイスをサポートする予定がある場合は、「iOS および iPadOS デバイスでの Apple ユーザー登録のサポート」を参照してください。 • Android Enterprise のゼロタッチ登録、Knox Mobile Enrollment、Apple DEP、または Apple Configurator 2 を使用して、デバイスをアクティベーションする予定の場合は、関連のドキュメントを参照してください。
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。
6	ユーザーのアクティベーションパスワードを設定します。

要件：アクティベーション

すべてのデバイス：

- アクティブ化するデバイス向けの BlackBerry UEM で利用可能なライセンス。
- 動作しているワイヤレス接続

iOS、iPadOS、および Android デバイス：

- 最新バージョンの BlackBerry UEM Client アプリがデバイスにインストールされていること

Windows 10 デバイス：

- BlackBerry Enterprise Server ルート RSA 証明書がデバイスにインストールされていること
- プロキシ設定を使用するデバイスの場合は、認証を必要としないプロキシを使用します。詳細については、次を参照してください。 https://docs.microsoft.com/ja-jp/windows/client-management/mdm/new-in-windows-mdm-enrollment-management
- Windows 10 Home のサポートは限られています。

メモ：ユーザーは、デバイスのアクティベーション方法について説明するビデオを視聴できます。

BlackBerry Infrastructure でのユーザー登録の有効化

BlackBerry Infrastructure に登録すると、ユーザーがモバイルデバイスをアクティブ化する方法が簡単になります。登録が有効な場合、ユーザーはデバイスをアクティブ化する際にサーバーアドレスを入力する必要がありません。登録はデフォルトで有効になっています。この設定を変更する場合は、ユーザーがデバイスをアクティブ化する際に実行する手順を記載したアクティベーションメールを更新する必要が生じることがあります。

Windows 10 を実行するデバイスは、同じ方法を使用して BlackBerry Infrastructure に接続しません。このため、ユーザー登録が有効か無効かに関係なく、これらのデバイスのアクティベーションプロセスは変わりません。Windows 10 のアクティベーションプロセスを簡素化する方法の詳細については、オンプレミスの設定関連の資料またはクラウドの設定関連の資料を参照してください。

1. メニューバーで［設定］をクリックします。
2. 左ペインで、［全般設定］を展開します。
3. ［アクティベーションのデフォルト］をクリックします。
4. ［**BlackBerry Infrastructure** への登録をオンにする］チェックボックスがオンになっていることを確認します。
5. ［保存］をクリックします。

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必要とするかどうか、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、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。

以下に、アクティベーション設定を管理する方法について例を示します。

- ユーザーのアクティベーションパスワードを設定する場合、次の操作を実行できます。
  - BlackBerry UEM にアクティベーションパスワードを自動生成させるか、またはアクティベーションパスワードを手動で指定できます。
  - アクティベーションパスワードの有効期間を指定します（分数または日数）。
  - ユーザーがデバイスをアクティブにするとすぐにアクティベーション期間が満了するように指定し、結果的に、ユーザーがそのパスワードでアクティブにできるデバイスの台数を 1 台に制限します。

  詳細については、「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」を参照してください。
- アクティベーションパスワードを QR Code に含めると、ユーザーはパスワードを入力するのではなく、アクティベーションメールの QR Code をスキャンするだけでアクティベーションできます。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 アクティベーションタイプを使用してユーザーがアクティブ化する Android Enterprise デバイスでは、BlackBerry UEM Client のダウンロード先の場所も QR Code に含めることができます。
- ユーザーのために複数のパスワードを作成し、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できます。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。
- BlackBerry UEM Self-Service でユーザーがアクティベーションパスワードを設定できるようにすると、ユーザーは必要に応じてアクティベーションパスワードを作成できますが、アクティブ化できるデバイス数は、アクティベーションプロファイルで指定されているデバイス数に限定されます。詳細については、「ユーザーによるアクティベーションパスワードの設定の許可（BlackBerry UEM Self-Service）」を参照してください。
- ユーザーのアクティベーションパスワードは、いつでも強制的に期限切れにできます。詳細については、「アクティベーションパスワードの有効期限の強制」を参照してください。
- Samsung Knox Mobile Enrollment を使用してデバイスを導入している場合、デバイスユーザーが自身の Microsoft Active Directory 資格情報を使用してデバイスをアクティブ化することを許可できます。各ユーザーのアクティベーションパスワードを管理する代わりに、ユーザーに Active Directory 資格情報を使用するように指示できます。このオプションは、オンプレミス環境と組織の Knox Mobile Enrollment アカウントに登録されているデバイスにのみ適用されます。詳細については、「デフォルトのアクティベーション設定の指定」を参照してください。

デフォルトのアクティベーション設定の指定

アクティベーションパスワードが期限切れになるまでのデフォルト時間、ユーザーに送信される自動生成パスワードの長さ、QR Code がアクティベーションに使用できるかどうか、およびその他のオプションを含む、デバイスアクティベーションのデフォルト設定を指定できます。

デバイスアクティベーションのデフォルト設定の詳細については、「デフォルトのデバイスアクティベーションの設定」を参照してください。

1. メニューバーで［設定］>［一般設定］をクリックします。
2. ［アクティベーションのデフォルト］をクリックします。
3. ［デバイスアクティベーションデフォルト］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。
4. Android 9.0 以前のデバイスを管理していて、MDM 制御 アクティベーションタイプを使用する場合は、［**Android** デバイスで **MDM** コントロールのアクティベーションタイプを有効にする］チェックボックスを選択して、MDM 制御 をアクティベーションプロファイルのアクティベーションタイプのリストに追加します。

   BlackBerry UEM が以前のバージョンからアップグレードされると、デフォルトでこのオプションが有効になります。有効になっているオプションを、無効にすることはできません。
5. ［**QR** コードを使用して **BlackBerry Dynamics** アプリのロックを解除する］を選択すると、ユーザーは BlackBerry Dynamics アプリを QR Code を使用してアクティベーションできます。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 Code の生成」を参照してください。
6. ［**BlackBerry Infrastructure** への登録をオンにする］チェックボックスをオンまたはオフにして、ユーザーがモバイルデバイスをアクティブ化する方法を変更します。このオプションをオフにした場合、ユーザーがデバイスをアクティブ化しようとすると、BlackBerry UEM のサーバーアドレスの入力を求められます。詳細については、「BlackBerry Infrastructure でのユーザー登録の有効化」を参照してください。
7. 承認されたデバイス ID のリストをインポートまたはエクスポートするには、承認されたデバイス ID のリストを含む組織の .csv ファイルを参照してください。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。
8. ［保存］をクリックします。

デフォルトのデバイスアクティベーションの設定

設定	説明
アクティベーションの有効期限	この設定では、アクティベーションパスワードまたは QR Code が期限切れになる前に有効のままにするデフォルトの時間を指定します。時間には、1 分〜30 日を指定できます。
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	この設定では、デバイスのアクティベーションに使用されたアクティベーションパスワードまたは QR Code をその後に期限切れにするかどうかを指定します。
デバイスアクティベーションに QR Code を許可する	この設定では、QR Code をアクティベーションメールメッセージに含めて、BlackBerry UEM Self-Service に表示することができるかどうかを指定します。ユーザーは、QR Code をスキャンしてデバイスのアクティベーションを開始できます。このオプションが選択されていない場合、アクティベーションメールテンプレートでは、QR Code を送信するオプションは使用できません。
QR Code にアクティベーションパスワードを含めることを許可する	この設定は、アクティベーションパスワードを QR Code に含めるかどうかを指定します。このオプションを選択した場合、ユーザーはデバイスをアクティベーションするために QR コードをスキャンした後でパスワードを別に入力する必要がありません。

設定	説明
QR Code に UEM Client アプリソースファイルの場所を含めることを許可する	この設定では、デバイスで UEM Client アプリソース（.apk）ファイルをダウンロードする場所を QR Code コードに含めるかどうかを指定します。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 Android Enterprise デバイスをアクティブ化する場合にのみ関係します。デバイスで QR Code をスキャンすると、BlackBerry UEM Client のダウンロードとインストールが開始されます。
デフォルトの場所を使用する	QR Code に UEM Client ソースファイルの場所を含めることを許可する場合は、このオプションを選択して、デバイスが BlackBerry ダウンロードサイトから .apk ファイルを取得するように指定します。
UEM Client アプリソースファイルの場所	QR Code に UEM Client ソースファイルの場所を含めることを許可する場合、この設定でデバイスがファイルをダウンロードする場所を指定します。工場出荷時のデフォルト設定で指定されている場所であれば、デバイスがアクセス可能な任意の場所を指定できます。
Microsoft Active Directory ユーザー名とパスワードの使用を許可する	Samsung Knox Mobile Enrollment を使用してアクティブ化されるデバイスの場合、この設定では、ユーザーが自身の Microsoft Active Directory 資格情報を使用してデバイスをアクティブ化できるようにするかどうかを指定します。
デバイスアクティベーション完了通知を送信する	この設定では、デバイスがアクティブ化されたときにユーザーがメールメッセージを受信するかどうかを指定します。
自動生成アクティベーションパスワードの長さ	この設定では、自動的に生成されるパスワードの文字数を指定します。使用できる値は、4〜16 です。
自動生成されるパスワードの複雑さ	この設定では、自動的に生成されるパスワードの種類を指定します。パスワードには、次の種類の文字を含めることができます。 • 小文字 • 大文字 • 数字 • 特殊文字または記号
Android デバイスで MDM コントロールのアクティベーションタイプを有効にする	この設定では、アクティベーションプロファイルの Android アクティベーションタイプのリストに MDM 制御 が含まれるかどうかを指定します。 Google は、Android 10 以降のデバイスで、このアクティベーションタイプを廃止しました。詳細については、https://support.blackberry.com/community にアクセスし、記事 48386 を参照してください。 BlackBerry UEM が以前のバージョンからアップグレードされると、デフォルトでこのオプションが有効になります。有効になっているオプションを、無効にすることはできません。

設定	説明
QR コードを使用して BlackBerry Dynamics アプリのロックを解除する	この設定は、ユーザーが QR Code を使用して BlackBerry Dynamics アプリをアクティベーションできるかどうかを指定します。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 Code の生成」を参照してください。
BlackBerry Infrastructure での登録の有効化	この設定では、［**BlackBerry Infrastructure** への登録をオンにする］チェックボックスをオンまたはオフにして、ユーザーが iOS、iPadOS、macOS、Android デバイスをアクティブ化する方法を変更します。このオプションをオフにした場合、ユーザーがデバイスをアクティブ化しようとすると、BlackBerry UEM のサーバーアドレスの入力を求められます。詳細については、「BlackBerry Infrastructure でのユーザー登録の有効化」を参照してください。

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。

ユーザーアカウントを作成する際、またはアクティベーションのメールメッセージを送信する際には、［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］オプションを選択します。

所定の時間に、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。

メモ：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］設定は適用されません。

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、特定のユーザーのアクティベーションパスワードをいつでも期限切れにすることができます。詳細については、「アクティベーションパスワードの有効期限の強制」を参照してください。

通常のアクティベーションパスワードとは異なり、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. メニューバーで、［ユーザー］ > ［管理されているデバイス］をクリックします。
2. ユーザーアカウントを検索します。
3. 検索結果で、ユーザーアカウントの名前をクリックします。
4. ［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を探します。［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の有効期限は即座に終了します。

   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。

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に必要な情報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. メニューバーで、［ユーザー］ > ［管理対象デバイス］をクリックします。
2. ユーザーアカウントを検索します。
3. 検索結果で、ユーザーアカウントの名前をクリックします。
4. ［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。
5. ［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。［概要］タブの［IT ポリシーおよびプロファイル］セクションでは、ユーザー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を確認できます。
   - 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。
6. ［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、以下のタスク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］を選択します。
7. オプションで、アクティベーション期間の有効期限を変更します。アクティベーションの有効期限は、アクティベーションパスワードを有効のままにする時間を指定しています。

8. 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。
9. ［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。
10. ［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。アクティベーションパスワードを設定する場合は、「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」を参照してください。

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. 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. オプションで、アクティベーション期間の有効期限を変更します。アクティベーションの有効期限は、アクティベーションパスワードを有効のままにする時間を指定しています。
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］を選択して、次のタスクを完了します。
   a) アクティベーションパスワードが期限切れになるまでに、デバイスをアクティブ化できる分数、時間数、日数を指定します。
   b) 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。
   c) ［最低限のパスワードの複雑さ］ドロップダウンリストで、アクティベーションパスワードに必要な複雑さのレベルを選択します。
   d) アクティベーションパスワードの作成時に、アクティベーションメールを自動的にユーザーに送信するには、［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、［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からメールテンプレートを選択します。
   e) 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。
   f) BlackBerry 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。
3. ［保存］をクリックします。

Android Enterprise アクティベーションのサポート

ユーザーが Android Enterprise デバイスをアクティブ化する方法は、Android の OS バージョン、組織がユーザーのデバイスをどの程度制御したいか、組織がどのように Google サービスを使用するかなど、いくつかの要因によって異なります。組織は、次の方法で Google サービスとやり取りすることができます。

Google サービス接続	説明
監視対象の Google Play アカウント	BlackBerry UEM は、Google ドメインに接続されていません。監視対象の Google Play アカウントを使用して、ユーザーが Google Play で仕事用アプリをダウンロードおよびインストールできるようにすることができます。 詳細については、次を参照してください。 監視対象 Google Play アカウントを使用した Android Enterprise アクティベーションのサポート
G Suite ドメイン	組織には G Suite ドメインがあり、これで Gmail、Google Calendar、Google ドライブなどのすべての G Suite サービスをサポートします。 詳細については、次を参照してください。 G Suite ドメインを使用した Android Enterprise アクティベーションのサポート
Google Cloud ドメイン	組織には、監視対象の Google アカウントをユーザーに提供する Google Cloud ドメインがあります。組織では、組織のメール、カレンダー、およびデータを管理するために、Gmail、Google Calendar、Google ドライブなどの G Suite サービスを使用しません。 詳細については、次を参照してください。 Google Cloud ドメインを使用した Android Enterprise アクティベーションのサポート
Google サービスなし	組織のセキュリティポリシーでは、Google サービスの使用は許可されていません。 詳細については、次を参照してください。 Google Play にアクセスできない Android Enterprise デバイスのサポート

Google ドメインに接続するため、または管理対象の Google Play アカウントを使用するために BlackBerry UEM を設定する方法の詳細については、オンプレミスの設定関連の資料またはクラウドの設定関連の資料を参照してください。

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

組織で Google ドメインを使用していない場合、または BlackBerry UEM を Google ドメインに接続したくない場合は、Android Enterprise デバイスをアクティブにして監視対象の Google Play アカウントを使用できます。監視対象 Google Play アカウントを使用すると、ユーザーがアクティブ化したデバイスのみ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。監視対象 Google Play アカウントの詳細については、https://support.google.com/googleplay/work/ を参照してください。

BlackBerry UEM で監視対象 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、BlackBerry UEM を Google に接続します。ユーザー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。BlackBerry UEM を Google に接続した後で、ユーザーが Android Enterprise 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なります。Android Enterprise デバイスをサポートするように BlackBerry UEM を設定する方法の詳細については、オンプレミスの設定関連の資料または UEM Cloud 設定関連の資料を参照してください。

G Suite ドメインを使用した Android Enterprise アクティベーションのサポート

BlackBerry UEM を G Suite 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。Android Enterprise デバイスをサポートするように BlackBerry UEM を設定する方法の詳細については、オンプレミスの設定関連の資料または UEM Cloud 設定関連の資料を参照してください。

1. G Suite ドメインで、Android ユーザーのユーザーアカウントを作成します。
2. G Suite ドメインで［**EMM** ポリシーの強制］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。この設定を選択していない場合、ユーザーは、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、監視対象 Google アカウントを追加できます。
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は、G Suite ドメインで［**EMM** ポリシーの強制］を選択します。
4. BlackBerry UEM で、Android ユーザーの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 G Suite アカウントのメールアドレスと一致する必要があります。
5. ユーザーが自身の G Suite 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。
6. BlackBerry 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 Cloud ドメインを使用した Android Enterprise 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 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 BlackBerry UEM を設定する場合は、ドメインでのユーザーアカウント作成を BlackBerry 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。Android Enterprise デバイスをサポートするように BlackBerry UEM を設定する方法の詳細については、オンプレミスの設定関連の資料または UEM Cloud 設定関連の資料を参照してください。

1. BlackBerry 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. Google Cloud ドメインでのユーザーアカウントの作成を BlackBerry UEM に許可しない場合は、Google Cloud ドメインと BlackBerry 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 ユーザーの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 BlackBerry UEM ユーザーアカウントのメールアドレスと一致する必要があります。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。この設定を選択していない場合、ユーザーは、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、監視対象 Google アカウントを追加できます。
4. BlackBerry 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。デバイスへのダウンロード場所を指定するには、ユーザーがスキャンしてアクティベーションを開始する QR Code の場所を含めるか、NFC を使用してデバイスがダウンロード情報を取得できるようにします（NFC ステッカーや別のデバイスをタップするなど）。
  - UEM Client の場所を QR Code に含める方法については、「デフォルトのデバイスアクティベーションの設定」を参照してください。
  - NFC ステッカーのプログラミングについては、「NFC ステッカーをプログラムしてデバイスをアクティブ化する」を参照してください。
  - NFC 経由で UEM Client のダウンロード手順を提供するために、BlackBerry UEM Enroll をセカンダリデバイスで使用する方法については、UEM Enroll のマニュアルを参照してください。この方法を使用するには、BlackBerry UEM Enroll アプリが Android 9 デバイスにインストールされていることと、アクティブ化するデバイスに Android 9 以前がインストールされていることが必要です。
- 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、最初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。これらのデバイスでは、ユーザーは、デバイスの初期設定が完了したら、BlackBerry ダウンロードサイトまたはその他の利用可能な場所から BlackBerry UEM Client をダウンロードできます。

最新の UEM Client または UEM Enroll アプリの .apk ファイルをダウンロードするには、support.blackberry.com/community にアクセスして記事 42607 を参照してください。

Android Enterprise デバイスをアクティブ化する手順については、次を参照してください。 Android デバイスのアクティベーション

要件

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	• **Android Enterprise** との統合：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 と Android Enterprise の統合は必要ありません。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、UEM 環境を Android Enterprise に統合する必要があります。
デバイスアクティベーションのデフォルト設定	QR コードに UEM Client の場所を含める場合は、以下のデバイスアクティベーションのデフォルト設定を確認します。 • ［**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めることを許可する］ および ［デフォルトの場所を使用する］オプションを選択します。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 をワークスペースに追加する］オプションの選択を解除します。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。 • 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の場合、IT ポリシーで次のことを確認します。 • ［**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て、Google Play 以外のアプリのインストールを許可します。

要件	説明
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。たとえば、BlackBerry Connectivity アプリの最新バージョンをダウンロードするには、BlackBerry myAccount ポータルにアクセスします。 2. BlackBerry UEM 管理コンソールのメニューバーで、［アプリ］をクリックします。 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。
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。たとえば、BlackBerry Work をダウンロードするには、support.blackberry.com/community にアクセスし、記事 42607 を参照してください。 2. BlackBerry UEM 管理コンソールのメニューバーで、［アプリ］をクリックします。 3. BlackBerry Dynamics アプリ（たとえば、BlackBerry Work）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。詳細については、support.blackberry.com/community にアクセスし、記事 42607 を参照してください。

Google Play にアクセスできない Android Enterprise デバイスをサポートする方法の詳細については、support.blackberry.com/community にアクセスして、記事 57492 を参照してください。

NFC ステッカーをプログラムしてデバイスをアクティブ化する

ユーザーは、BlackBerry UEM Client をダウンロードし、NFC タグまたはステッカーのデバイスをタップすることで、デバイスのアクティブ化を開始できます。この方法は、Google Play にアクセスできない 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）デバイスをアクティブ化するオプションの 1 つです。

この方法を使用して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、UEM Client をダウンロードしてアクティブ化を開始するようにデバイスに指示するために必要な値を使用して、サードパーティの NFC ステッカーをプログラムします。

作業を始める前に： 次の項目が必要です。

- NFC タグまたはステッカー
- NFC ステッカーの読み取りと NFC ステッカーへの書き込みが可能な Android アプリなどのステッカーをプログラムする方法。

1. 管理コンソールで、［設定］ **>** ［外部統合］ **>** ［**Android** エンタープライズ］をクリックします。
2. ［**NFC** 登録］で［詳細］をクリックします。
3. NFC ステッカーにデータを書き込むことができるアプリを搭載したデバイスで、アプリを開いて、プログラムするステッカーにアプリを接続し、次の設定を追加します。
   a) NFC データの種類を［カスタム］に設定します。
   b) コンテンツタイプを `application/com.android.managedprovisioning` に設定します。
   c) 管理コンソールのテキストボックスから、アプリの［設定］フィールドに詳細をコピーします。
4. ステッカーに設定を書き込みます。

プログラムがステッカーに書き込まれたら、ユーザーが新しいデバイスでステッカーをタップするか、デバイスを工場出荷時の設定にリセットして UEM Client をダウンロードし、アクティベーションを開始できます。

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。
- **BlackBerry UEM** と **Azure Active Directory** の参加の統合：Azure Active Directory の参加が設定されている場合、ユーザーは、Azure Active Directory 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。Azure Active Directory プレミアムライセンスが必要です。詳細については、オンプレミスの設定関連の資料またはクラウドの設定関連の資料を参照してください。
- **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 Azure Active Directory 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。AzureActive Directory の参加の統合と Azure Active Directory プレミアムライセンスが必要です。Windows Autopilot の詳細については、Microsoft の Web サイトにアクセスしてください。
- 検出サービスの導入：Java Web 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。詳細については、オンプレミスの設定関連の資料またはクラウドの設定関連の資料を参照してください。

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、iOS または iPad OS 13.1 以降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、次のことを確認します。

- 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、必ず 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てください。
- 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 をユーザーに割り当てます。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 Galaxy S 10、Samsung Galaxy Note 10、および将来の Samsung フラグシップモデル
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、BlackBerry UEM 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	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。 メモ：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。
BlackBerry UEM Client	バージョン 12.35.2.155980 以降の Android 用 BlackBerry UEM Client が必要です。

デバイスアクティベーション時のユーザー通知の有効化

アカウントでデバイスがアクティベーションされるたびに、ユーザーに通知するように、UEM を有効にできます。メール通知は、デバイスのアクティベーションに使用されたユーザーアカウントのメールアドレスに送信されます。デフォルトでは、メールにデバイスのモデル、シリアル番号、IMEI が含まれます。予期せず通知を受信した場合、ユーザーは管理者に連絡する必要があります。

1. メニューバーで［設定］>［一般設定］をクリックします。
2. ［アクティベーションのデフォルト］をクリックします。
3. ［デバイスアクティベーション完了通知を送信する］をオンにします。
4. ［保存］をクリックします。

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設定できます。ユーザーに支給するデバイスを完全に制御したほうがいい場合があります。また、ユーザーが所有し職場で使用しているデバイスの個人用データを一切制御できないようにしたほうがいい場合もあります。

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、ユーザーまたはユーザー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. メニューバーで［ポリシーとプロファイル］をクリックします。
2. ［ポリシー］ > ［アクティベーション］をクリックします。
3. ＋をクリックします。
4. プロファイルの名前と説明を入力します。
5. ［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。
6. ［デバイスの所有権］ドロップダウンリストで、デバイスの所有権のデフォルト設定を選択します。
   - 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ブにする場合は、［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ブにする場合は、［個人用］を選択します。
7. 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。
8. ［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。選択していないデバイスの種類はアクティベーションプロファイルに含まれず、ユーザーはこれらのデバイスをアクティベーションすることはできません。
9. アクティベーションプロファイルに含まれるデバイスの種類それぞれについて、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。このオプションを使用して、許可されるデバイスを一部のモデルのみに制限します。

- 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。特定のメーカーの一部のデバイスモデルまたはデバイスのアクティベーションをブロックするには、このオプションを使用します。

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。

古い OS バージョンの多くは、BlackBerry UEM ではサポートされていません。BlackBerry UEM で現在サポートされている古いバージョンをサポートしない場合は、最小バージョンを選択するだけです。サポートされるバージョンの詳細については、「互換性一覧表」を参照してください。

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。

「MDM 制御」アクティベーションタイプは、Android 10 以降を使用するデバイスでは推奨されません。これは、デフォルトのアクティベーション設定で、［**Android** デバイスで **MDM** コントロールのアクティベーションタイプを有効にする］設定が選択されている場合のみ、アクティベーションタイプのリストに含まれます。

10. 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。各オプションの詳細については、「アクティベーションタイプ：iOS デバイス」を参照してください。

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) ［**iOS** アプリの整合性チェック］セクションで、必要に応じて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、BlackBerry 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、CylancePROTECT Mobile 関連の資料を参照してください。

11. 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。たとえば、最初に「MDM コントロール」とランク付けした場合、「MDM コントロール」をサポートしていないデバイスは、次にランク付けされたアクティベーションタイプを受け取ります。

b) 「MDM 制御」アクティベーションタイプを選択し、Knox MDM ポリシールールをサポートするデバイスに適用しない場合は［**MDM** コントロールのアクティベーションで **Samsung KNOX API** をアクティブ化する］チェックボックスをオフにします。

c) 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。詳細については、https://support.blackberry.com/community にアクセスし、記事 54614 を参照してください。

d) 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 オプションを有効にします。

- ［**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］は、適切なライセンスを持つデバイスで BlackBerry Secure Connect Plus および Knox Platform for Enterprise 機能（Samsung Knox をサポートするデバイスの場合）を有効にします。
- ［**Samsung KNOX DualDAR Workspace** を有効にする］は、Samsung Knox DualDAR 暗号化をサポートするデバイスで有効にできます。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。
- ［**Google Play** アカウントを仕事用領域に追加する］を選択すると、仕事用領域での Google Play アプリの管理が可能になります。デバイスが Google Play にアクセスできない場合は、このオプションを選択解除する必要があります。
- ［承認されたデバイス **ID** のみを許可する］を選択すると、デバイス ID を指定した個々のデバイスにアクティベーションを制限できます。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。

e) ［**SafetyNet** アテステーションオプション］セクションで、オプションで次のいずれかのアテステーションメソッドを選択します。

- デバイスの **SafetyNet** アテステーションを実行する：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：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** アテステーションを実行する：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ます。

f) ［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、［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］を選択すると、BlackBerry UEM は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チャレンジを送信します。

12. 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。

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

13. ［追加］をクリックします。

終了したら： 必要に応じて、プロファイルをランク付けします。

デバイスのアクティベーション手順

必要に応じて、デバイスをアクティブ化するステップバイステップの手順をユーザーに提供できます。

個々のユーザーが行う手順は、ユーザーのデバイスモデルや OS のバージョンによって、ここに記載されている手順とは多少異なる場合があります。

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 デバイスのアクティベーションを開始する手順は、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。BlackBerry UEM が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指示を与えることができます。詳細については、「メールテンプレート」を参照してください。

Android Enterprise デバイスは、ユーザーがアクティベーションプロセスを開始するためのいくつかの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
Google Play から UEM Client をインストールする	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 Google Play から UEM Client をデバイスに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。
ユーザーが BlackBerry ダウンロードサイトから UEM Client をダウンロードする	Android ユーザーが、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ベーションされるデバイスのために Google Play にアクセスできない場合、ユーザーが UEM Client .apk ファイルを BlackBerry ダウンロードサイトからダウンロードするか、管理者が BlackBerry からファイルをダウンロードして、ユーザーがアクセスできる場所に置くことができます。 詳細については、support.blackberry.com/community にアクセスし、記事 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入力する	BlackBerry UEM が組織の G Suite 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。

アクティベーション方法	説明
UEM Client のダウンロード先が含まれている QR Code をスキャンする	BlackBerry UEM では、UEM Client のダウンロード場所を QR Code に含めて、ユーザーに送信されるアクティベーションメールに追加することができます。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 アクティベーションタイプが割り当てられたデバイスをアクティベーションするために、ユーザーは、デバイスのスタート画面を 7 回タップして、QR Code リーダーを開き、QR Code をスキャンすることができます。 一部のデバイスメーカーは、この機能をサポートしていない場合があります。 詳細については、「監視対象の Google Play アカウントを使用して、仕事用と個人用 - フルコントロール アクティベーションタイプで Android Enterprise デバイスをアクティベーションする」を参照してください。
デバイスのセットアップ中に afw#blackberry ハッシュタグを入力する	組織が管理対象の Google Play アカウントを使用して Google サービスに接続している場合、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を割り当てられたデバイスをアクティベーションするには、ユーザーがデバイスのセットアップ中に Google 資格情報を入力する画面で、代わりに `afw#blackberry` と入力して、UEM Client のダウンロードを開始し、アクティベーションプロセスを開始することができます。 Android 11 以降のデバイスの場合、`afw#blackberry` は 仕事用領域のみ アクティベーションタイプでのみサポートされます。 Android 8 および 9 デバイスでは、`afw#blackberry` はサポートされなくなりました。 詳細については、「監視対象の Google Play アカウントを使用して、仕事用領域のみ アクティベーションタイプで Android Enterprise デバイスをアクティベーションする」を参照してください。
UEM Client のダウンロード場所がプログラムされた BlackBerry UEM Enroll アプリで NFC ステッカーまたはセカンダリデバイスをタップする	NFC ステッカーをプログラムするか、UEM Enroll アプリがインストールされたセカンダリデバイスをセットアップすることができます。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 アクティベーションタイプが割り当てられたデバイスをアクティベーションするために、ユーザーが、NFC ステッカーまたはセカンダリデバイスをタップして UEM Client のダウンロードを開始することができます。 同じセカンダリデバイスまたは NFC ステッカーを使用して、複数のユーザーのデバイスをアクティベートできます。 詳細については、「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」を参照してください。

アクティベーション方法	説明
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。これら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。

UEM Client をダウンロードしてデバイスアクティベーションを開始する各オプションは、特定のアクティベーションタイプでのみサポートされています。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	仕事用と個人用 - ユーザーのプライバシー	仕事用と個人用 - フルコントロール			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 Code のスキャン	いいえ	はい	はい	はい	はい	はい	はい
afw#blackberry ハッシュタグ	いいえ	いいえ	Android 10	いいえ	いいえ	Android 10 以降	いいえ
NFC ステッカーまたはセカンダリデバイスをタップする	いいえ	はい	はい	はい	はい	はい	はい

アクティベーションタイプ	仕事用と個人用 - ユーザーのプライバシー	仕事用と個人用 - フルコントロール			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
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

これらの手順は、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たデバイスに適用されます。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。

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するか、次のワークフローへのリンクを送信します。Android デバイスのアクティベーション。

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

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、UEM Client を BlackBerry から手動でダウンロードしてインストールできます。最新の UEM Client .apk ファイルをダウンロードするには、support.blackberry.com/community にアクセスして記事 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 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する	**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。

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、デバイスに仕事用プロファイルが設定されるまで待ちます。
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 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、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。
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、次のいずれかの操作を実行します。

- 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 G Suite または Google Cloud ドメインに接続されているときに、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）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。

このトピックでは、Android Enterprise デバイスをアクティベーションする 1 つの方法について説明します。その他のオプションについては、「Android 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
- BlackBerry UEM アクティベーションユーザー名（通常は仕事用ユーザー名）
- BlackBerry UEM アクティベーションパスワード
- BlackBerry 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。
デバイスを手動でアクティベーションする	**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、デバイスに仕事用プロファイルが設定されるまで待ちます。
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 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、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。
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、次のいずれかの操作を実行します。

- 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。

監視対象の **Google Play** アカウントを使用して、仕事用領域のみ アクティベーションタイプで **Android Enterprise** デバイスをアクティベーションする

このトピックでは、Android Enterprise デバイスをアクティベーションする 1 つの方法について説明します。その他のオプションについては、「Android デバイスのアクティベーション」を参照してください。

これらの手順は、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使用した Android 10 デバイスにも適用できます。

Android 8 および 9 デバイスの場合は、代わりに「監視対象の Google Play アカウントを使用して、仕事用と個人用 - フルコントロール アクティベーションタイプで Android Enterprise デバイスをアクティベーションする」を参照してください。Android 8 および 9 デバイスは、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を開始するための afw#blackberry ハッシュタグをサポートしなくなりました。

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 を受け取った場合は、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
- BlackBerry UEM アクティベーションユーザー名（通常は仕事用ユーザー名）
- BlackBerry UEM アクティベーションパスワード
- BlackBerry 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. デバイスのセットアップ中に、Google アカウントのログイン画面に afw#blackberry と入力します。
3. ［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。
デバイスを手動でアクティベーションする	**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、デバイスに仕事用プロファイルが設定されるまで待ちます。
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 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、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。
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、次のいずれかの操作を実行します。

- 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。

監視対象の **Google Play** アカウントを使用して、仕事用と個人用 - フルコントロール アクティベーションタイプで **Android Enterprise** デバイスをアクティベーションする

このトピックでは、Android Enterprise デバイスをアクティベーションする 1 つの方法について説明します。その他のオプションについては、「Android デバイスのアクティベーション」を参照してください。

Android 10 デバイスの場合、監視対象の Google Play アカウントを使用して、仕事用領域のみ アクティベーションタイプで Android Enterprise デバイスをアクティベーションする手順は、仕事用と個人用 - フルコントロール アクティベーションタイプでも機能します。Android 11 では、afw#blackberry ハッシュタグを使用して 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開始することはサポートされなくなりました。

これらの手順では、QR Code を使用して、BlackBerry UEM Client をダウンロードしてインストールするようにデバイスに指示します。QR Code を使用してユーザーがダウンロードを開始できるようにするには、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］を選択する必要があります。詳細については、「デフォルトのアクティベーション設定の指定」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、QR Code と、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情報が含まれています。

1. アクティベーションするデバイスで、最初の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. デバイス画面を 7 回タップします。

   デバイスで QR Code リーダーが開きます。
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. 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。
5. ［プロファイルの設定］画面で［設定］をタップし、デバイスに仕事用プロファイルが設定されるまで待ちます。
6. 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。
7. 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。
8. ［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。
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ます。［**OK**］をタップします。
10. 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。
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. UEM Client および 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。
13. 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。
14. 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。
15. 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、次のいずれかの操作を実行します。

- 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

これらの手順は、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で、Google Play にアクセスできない Android デバイスをアクティベーションする場合に適用されます。仕事用と個人用 - ユーザーのプライバシー （Android Enterprise）アクティベーションタイプでデバイスをアクティブ化にするには、次を参照してください。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。

アクティベーションを開始するには、デバイスを工場出荷時のデフォルト設定に戻し、QR Code または NFC を使用して BlackBerry UEM Client をダウンロードする手順を受け取る必要があります。

- UEM Client のダウンロード先を、ユーザーがアクティベーションメールで受け取る QR コードに含めることができます。ユーザーは、QR Code をスキャンしてダウンロードを開始できます。詳細については、「デフォルトのデバイスアクティベーションの設定」を参照してください。
- ユーザーがタップしてデバイスのアクティベーションを開始できる NFC ステッカーを事前にプログラムできます。
- Android 9 以前のデバイスでは、ユーザーは NFC を使用して、BlackBerry UEM Enroll アプリがインストールされているセカンダリデバイスをタップできます。UEM Enroll アプリをセカンダリデバイスにダウンロードしてインストールするには、support.blackberry.com/community にアクセスし、記事 42607 を参照してください。

同じセカンダリデバイスまたは NFC ステッカーを使用して、複数のユーザーのデバイスをアクティベートできます。

QR Code を使用してユーザーがデバイスのアクティベーションを開始する場合は、監視対象の Google Play アカウントを使用して、仕事用と個人用 - フルコントロール アクティベーションタイプで Android Enterprise デバイスをアクティベーションする 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。

ユーザーが NFC を使用してデバイスのアクティベーションを開始する場合は、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：

- 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 を受け取った場合は、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
  - BlackBerry UEM アクティベーションユーザー名（通常は、仕事用ユーザー名）
  - BlackBerry UEM アクティベーションパスワード
  - BlackBerry UEM サーバーアドレス（必要に応じて）
- 管理者は、事前にプログラムされた NFC ステッカーまたは UEM Enroll アプリがインストールされているセカンダリデバイスを提供します。

1. アクティブ化するデバイスで、デバイス設定のようこそ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. 次の操作のいずれかを実行します。

タスク	手順
NFC ステッカーを使用してアクティベーションを開始します。	a. デバイスで管理者から提供された NFC ステッカーをタップします。デバイスが UEM Client をダウンロードしてインストールします。 b. デバイスがアクティベーションの準備をしている間、表示される手順に従います。
セカンダリデバイスでアクティベーションを開始します。	a. セカンダリデバイスで、UEM Enroll アプリを開きます。デバイスで NFC が有効になっていることを確認します。 b. ［デバイスをアクティブ化する］をタップします。 c. 両方のデバイスの背面を合わせます。プロンプトが表示されたら、セカンダリデバイスの画面上の任意の場所をタップします。 d. アクティブ化するデバイスで、画面の指示に従い、UEM Client をダウンロードしてインストールします。

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 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。
デバイスを手動でアクティベーションする	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。

5. 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。
6. ［プロファイルの設定］画面で［設定］をタップし、デバイスに仕事用プロファイルが設定されるまで待ちます。
7. 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。
8. ［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。
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ます。［**OK**］をタップします。
10. 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。
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. UEM Client および 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。

13. 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。
14. 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。
15. 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。
16. 必要に応じて、組織で使用するメールアプリを開き、指示に従ってスマートフォンにメールを設定します。

MDM 制御 アクティベーションタイプの Android デバイスのアクティベーション

メモ： これらの手順は、MDM 制御 アクティベーションタイプが割り当てられたデバイスにのみ適用されます。このアクティベーションタイプは Android 10 では推奨されません。MDM 制御 アクティベーションタイプで Android 10 以降のデバイスをアクティベーションしようとすると失敗します。詳細については、https://support.blackberry.com/community にアクセスし、記事 48386 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。

1. BlackBerry UEM Client からデバイスに Google Play をインストールします。
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 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。
デバイスを手動でアクティベーションする	**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。

5. ［次へ］をタップします。
6. デバイス管理者をアクティブ化するには、［アクティベーション］をタップします。デバイス上の仕事用データにアクセスするには、デバイス管理者をアクティブ化する必要があります。
7. 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。
8. 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、次のいずれかの操作を実行します。

- 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

ユーザーによる入力が必要な情報、および iOS と iPadOS デバイスをアクティブ化する手順は、iOS のバージョンや、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る場合があります。アクティベーションメールテンプレートには、ユーザーが必要とする情報が含まれています。必要に応じて、メールテンプレートのテキストを更新できます。詳細については、「メールテンプレート」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

これらの手順は、MDM オプションを有効にして MDM 制御 または ユーザーのプライバシー を使用してアクティブ化された iOS および iPadOS デバイスに適用されます。

アクティベーション中、ユーザーは BlackBerry UEM Client アプリを終了して手動で MDM プロファイルをインストールする必要があります。デバイスでロックダウンモードが無効になっている必要があります（iOS および iPadOS 16 以降）。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。

デバイスユーザーに次のアクティベーション手順を送信するか、次のワークフローへのリンクを送信します。iOS デバイスのアクティベーション

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. デバイスに BlackBerry UEM Client をインストールします。BlackBerry UEM Client は App Store からダウンロードできます。
2. デバイスで、［**UEM Client**］をタップし、使用許諾契約に同意します。
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.** BlackBerry 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する	**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. ［許可］をタップして、通知の送信を UEM Client に許可します。［許可しない］を選択すると、デバイスが完全に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［プロファイルとデバイス管理］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 BlackBerry UEM Client アプリに戻り、アクティベーションを完了します。
11. 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、次のいずれかの操作を実行します。

- デバイスで BlackBerry UEM Client アプリを開いて、［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、iPad および iPadOS 13.1 以降を実行しているデバイスでのみサポートされています。

登録を開始するには、ユーザーはデバイス上のカメラアプリを使用して、Apple ユーザー登録アクティベーションメールに記載されている QR Code をスキャンし、MDM プロファイルを手動でダウンロードしてデバイスにインストールします。デバイスをアクティブ化するには、ユーザーは、BlackBerry UEM ユーザーアカウントのメールアドレスと一致する管理 Apple ID アカウントにログインします。ユーザーが他の BlackBerry Dynamics アプリのアクティブ化、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 UEM Client をユーザーに割り当てる必要があります。ユーザーが使用許諾契約に同意すると、UEM Client のセットアップが開始されます。

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：

- 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管理対象 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 の有効期限がすでに切れている場合は、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、管理者に連絡してください。
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 BlackBerry UEM Client アプリ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. BlackBerry UEM Client アプリを設定するには、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 BlackBerry UEM Client アプリを開いて、［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。

macOS 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をデバイスユーザーに送信します。

作業を始める前に： 次の BlackBerry UEM Self-Service ログイン情報が必要です。

- BlackBerry UEM Self-Service の Web アドレス
- ユーザー名とパスワード
- ドメイン名

1. アクティブ化するデバイスで、管理者から受信したログイン情報を使用し、BlackBerry UEM Self-Service にログインします。
2. デバイスが既に表示されている場合は、［デバイスのアクティブ化］をクリックします。
3. ［デバイス］ドロップダウンメニューで、［**macOS**］をクリックします。
4. アクティベーションのチュートリアルを視聴します。
5. ［送信］をクリックします。
6. 指示に従って必須プロファイルをインストールし、デバイスのアクティベーションを完了します。アクティベーションが完了すると、デバイスが BlackBerry UEM Self-Service に表示されます。

Apple TV 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をデバイスユーザーに送信します。

作業を始める前に：

- BlackBerry UEM Self-Service の Web アドレスとログイン認証情報が必要です。
- Apple Configurator 2 がインストールされた macOS コンピューターが必要です。
- USB-C または Micro-USB ケーブル（Apple TV のバージョンにより異なります）が必要です。
- Apple TV デバイスが管理モードになっていることを確認します。
- HDMI ケーブルと電源コードを Apple TV デバイスから外します。

1. USB-C または Micro-USB ケーブルを使用して、Apple TV デバイスを macOS コンピューターに接続します。
2. Apple TV の第 3 世代および第 4 世代のバージョンでは、電源コードを接続します。
3. macOS コンピューターで BlackBerry UEM Self-Service にログインします。
4. デバイスを初めてアクティブ化しているか、アクティブ化されたデバイスが既にあるかに応じて、をクリックするか、> ［デバイスをアクティブ化］をクリックします。
5. ［デバイス］ドロップダウンメニューで、［**Apple TV**］をクリックします。
6. ［送信］をクリックします。
7. ［プロファイルをダウンロード］をクリックします。
8. ［閉じる］をクリックします。
9. Apple Configurator 2 を開きます。
10. Apple TV を選択し、［追加］ **>** ［プロファイル］をクリックします。
11. 手順 7 でダウンロードした設定ファイルを選択し、［追加］をクリックします。
12. アクティベーションが完了すると、デバイスが BlackBerry UEM Self-Service に表示されます。

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

メモ：MDM を使用して Windows 10 デバイスを管理する場合、Microsoft System Center Configuration Manager ではデバイスを管理できません。

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。

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。証明書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に示されています。証明書へのリンクを受信していない場合は、サポートのために管理者にお問い合わせください。
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］をタップします。
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ます。［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ます。［参照］をクリックします。
8. ［信頼済みルート証明書機関］を選択します。［**OK**］をクリックします。

9. ［次へ］をクリックします。
10. ［完了］をクリックします。
11. ［**OK**］をクリックします。
12. ［**OK**］をクリックします。
13. ［スタート］ボタンをクリックします。
14. 次のタスク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。
Windows 10 バージョン 1607 より前	**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。

15. ［メールアドレス］フィールドにメールアドレスを入力します。［続行］をタップします。
16. 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で確認できます。また、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 で確認することもできます。
17. ［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 BlackBerry 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。
18. ［完了］をタップします。
19. アクティベーションプロセスは完了です。

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、次の操作を実行できます。
  - 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 BlackBerry UEM に接続されることを確認します。ブリーフケースアイコン > ［情報］をクリックして、同期ステータス情報を確認します。
  - BlackBerry UEM Self-Service で、当該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。
  - Windows 10 バージョン 1607 よりも前の場合、［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

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。

組織は、認定販売代理会社からこれらのデバイスを購入し、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、デバイスをアカウントに追加してデバイス管理用にプロビジョニングします。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が完了する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が完了する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。アクティベーションが完了するまで、デバイスのホーム画面を表示してデバイス機能を使用することはできません。

BlackBerry UEM デバイスでゼロタッチ登録を使用するには、デバイスでゼロタッチ登録が有効になっている必要があります。ゼロタッチ登録の詳細と設定方法については、Android Enterprise ヘルプと https://support.google.com/work/android/answer/7514005 を参照してください。

1. 認定販売代理会社からサポート対象のデバイスを購入してください。販売代理会社が、組織のゼロタッチ登録アカウントを設定します。
2. ゼロタッチプラットフォームでは、購入したデバイスは販売代理会社によって追加されます。
3. 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。
4. ［**Android** エンタープライズ］をクリックします。
5. ［ゼロタッチコンソールを起動する］をクリックします。
6. 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。
   ゼロタッチ登録を管理するための Android 設定が UEM に表示されます。
7. 構成を作成または管理し、購入したデバイスに割り当てます。
   Android ゼロタッチポータルを開いて、そこから登録構成を管理することもできます。

終了したら：

- BlackBerry 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 では、同時に多数の Samsung Knox デバイスを導入できます。詳細については、Samsung の情報（https://www.samsungknox.com/ja/products/knox-mobile-enrollment）を参照してください。

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加入をサポートしません。詳細については、Samsung の情報（https://docs.samsungknox.com/admin/knox-mobile-enrollment/release-notes/November-4-2020.htm）を参照してください

組織は、認定販売代理店または直接 Samsung とデバイス IMEI を進んで共有する販売代理店からこれらのデバイスを購入し、デバイスが Knox Mobile Enrollment を使用できるようにします。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。アクティベーションが完了するまで、デバイスのホーム画面を表示してデバイス機能を使用することはできません。

1. メニューバーで、［設定］ > ［外部統合］をクリックします。
2. ［**KNOX Mobile Enrollment**］をクリックします。
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］をクリックして、configuration.json ファイルをダウンロードします。ファイルで、CFPrint セクションのエントリと、Knox Mobile Enrollment を設定したときに追加したエントリを比較します。エントリが異なる場合、.json ファイルのテキスト全体を Knox Mobile Enrollment ページの［カスタム JSON データ］フィールドにコピーします。

非監視対象 iOS デバイスの制限

BlackBerry UEM で非監視対象 iOS デバイスを制限する方法は 2 つあります。

- デフォルトで監視モードが有効になっている Apple DEP デバイスを使用します。Apple DEP デバイスでは監視モードを無効にできません。
- ［非監視対象デバイスのアクティブ化を許可しない］設定がユーザーアカウントに対して選択されているアクティベーションプロファイルを割り当てることができます。この設定は、「MDM コントロール」と「ユーザープライバシー」（SIM ベースのライセンスが有効）のアクティベーションタイプでサポートされています。BlackBerry UEM は、非監視対象デバイスがアクティブ化しないように防止し、デバイスが BlackBerry UEM Client でアクティブ化されたか、DEP を使用してアクティブ化されたかに関わらず非監視対象になると、自動的にデバイスを削除します。詳細については、「アクティベーションプロファイルの作成」を参照してください。

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、BlackBerry 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。

注意：LG デバイスはこの機能をサポートしていません。

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. ［設定］ > ［一般設定］ > ［アクティベーションのデフォルト］の順に選択します。
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. 組織の .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。
6. リストをインポートした後、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。

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 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。

BlackBerry 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。

デバイスがアクティベーションされると、BlackBerry UEM は割り当てられた IT ポリシーとプロファイルをユーザーに送信します。

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手順

Apple の Device Enrollment Program に登録された iOS 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	登録の設定を作成したときに、［新しいデバイスをこの設定に自動的に割り当てる］を選択しなかった場合、または別の設定を割り当てる場合は、登録設定を割り当てます。
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。
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、それをユーザーアカウントまたはユーザーが属するグループに割り当てる」を参照してください。 オプションで、iOS デバイスにアクティベーションプロファイルを割り当てる。

手順	アクション
5	ユーザーのアクティベーションパスワードを設定し、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ユーザーに送信します。 アクティベーションパスワードを設定する場合、［デフォルトのデバイスアクティベーション］オプションを選択する必要があります。 会社ディレクトリのユーザーは、会社ディレクトリのユーザー名とパスワードを利用できます。したがって、アクティベーションパスワードを作成する必要はありません。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）。変数の詳細については、「デフォルトの変数」を参照してください。 ユーザーは、自分のメールアドレスと Active Directory パスワードを使用して登録することもできます。 オプションで、iOS デバイスへのユーザーの割り当てできます。BlackBerry 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、ユーザーがセットアップを完了できるようにします。セットアップの完了後、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。

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

デバイスを登録するには、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、これらのデバイスを BlackBerry UEM サーバーに割り当てます。シリアル番号は次の方法で入力できます。

- 番号を個別に入力する
- 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
- シリアル番号が記録された .csv ファイルをアップロードする

作業を始める前に： DEP を使用するように BlackBerry UEM を設定します。詳細については、オンプレミスの設定関連の資料または UEM Cloud の設定関連の資料を参照してください。

1. ブラウザーで、**business.apple.com** または **deploy.apple.com** と入力します。
2. Apple Business Manager または DEP アカウントにサインインします。
3. ［**Device Enrollment Program**］セクションで、［デバイスを管理］をクリックします。
4. 手順に従って、デバイスのシリアル番号を入力します。
5. BlackBerry UEM サーバーにシリアル番号を割り当てます。

終了したら： iOS デバイスに登録設定を割り当てる。

iOS デバイスに登録設定を割り当てる

登録設定を作成し、［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］を選択した場合、DEP デバイスが UEM と同期する際に、BlackBerry UEM は自動的にこの設定を割り当てます。それ以外の場合は、登録の設定をデバイスに割り当てる必要があります。UEM が DEP と同期されるのは、日常的なスケジュールに従った場合、および Apple DEP デバイスページが表示された場合です。

デバイスのアクティベーションステータスがまだ保留中の場合は、既存の登録設定を削除して、新しい登録設定を割り当てることができます。

BlackBerry UEM 管理コンソールでは、次のアイコンが登録設定のステータスを示します。

ステータス	アイコン
✓	登録設定が割り当てられています。 デバイスがアクティブ化された後で Apple Device Enrollment Program 外部統合設定で、適用される DEP 登録設定が更新または再保存された場合、BlackBerry UEM は、アクティブ化されたデバイスのチェックマークも表示します。設定が更新された場合、UEM は、デバイスがアクティブ化されたときに使用された登録設定が、割り当てられた設定と一致していることを確認できません。
?	登録設定が割り当てられていません。
🕘	登録設定が適用されますが、アクティベーションが保留されています。
📱	アクティベーションに成功しました。

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. 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. 登録設定の割り当て先デバイスの横にあるチェックボックスをオンにします。同じ DEP アカウントに登録されているデバイスを選択する必要があります。
3. をクリックします。
4. ［登録設定］ドロップダウンリストで、割り当てる登録設定を選択します。
5. ［割り当て］をクリックします。

終了したら：

iOS デバイスをユーザーに配布します。デバイスセットアップの一環として、デバイスが UEM でアクティブにされます。ユーザー名とパスワードの入力を求めるプロンプトが表示されます。会社ディレクトリのユーザーは、会社ディレクトリのユーザー名（domain\username の指定形式）とパスワードを使用できます。ローカルユーザーは、アクティベーションパスワードを使用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の設定」を参照してください。

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。

1. メニューバーで［設定］をクリックします。
2. 左ペインで、［外部統合］ > ［**Apple Device Enrollment Program**］をクリックします。
3. DEP アカウントの名前をクリックします。
4. ［**DEP** 登録設定］セクションで、＋をクリックします。
5. 設定の名前を入力します。
6. 次のタスクのいずれかを実行します。
   - DEP デバイスと BlackBerry UEM を同期するときに、BlackBerry 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。BlackBerry UEM が Apple DEP と同期されるのは、日常的なスケジュールに従った場合、および Apple DEP デバイスページが表示された場合です。

     メモ：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、BlackBerry UEM が新しい登録設定を割り当てることはありません。

     メモ：新しい DEP デバイスに自動的に割り当てる登録設定は、1 つだけ選択できます。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。
   - 登録設定を特定のデバイスに手動で割り当てる場合は、［すべての新しいデバイスをこの設定に自動的に割り当てる］チェックボックスをオフにしておきます。
7. 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。
8. ［デバイス設定］セクションで、次のオプションから選択します。
   - ペアリングを許可する：オンの場合、ユーザーはデバイスとコンピューターをペアリングできます。
   - 必須：オンの場合、登録設定を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：オンの場合、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 - オンの場合、BlackBerry UEM でのアクティベーションが完了するまでデバイスのセットアップをキャンセルできません。
9. ［セットアップ時にスキップ］セクションでは、デバイスのセットアップに含めない項目を選択します。
   - パスコード - オンの場合、デバイスのパスコード作成を求めるプロンプトは表示されません。
   - 位置情報サービス - オンの場合、デバイスで位置情報サービスが無効になります。
   - 復元 - オンの場合、ユーザーはバックアップファイルからデータを復元できません。
   - Android から移動 - オンの場合、ユーザーは Android デバイスからデータを復元できません。
   - Apple ID - オンの場合、ユーザーは Apple ID と iCloud にサインインできません。
   - 使用条件 - オンの場合、ユーザーには iOS の使用条件が表示されません。
   - Siri - オンの場合、デバイスで Siri が無効になります。
   - 診断 - オンの場合、診断情報はセットアップ時にデバイスから自動的に送信されません。
   - バイオメトリック - オンの場合、ユーザーは Touch ID を設定できません。
   - 支払い - オンの場合、ユーザーは Apple Pay を設定できません。
   - Zoom - オンの場合、ユーザーは Zoom を設定できません。
   - ホームボタンのセットアップ - オンの場合、ユーザーはホームボタンのクリックを調整できません。
   - デバイスからデバイスへの移行 - オンの場合、ユーザーは以前のデバイスから新しいデバイスにデータを転送できません。
10. ［保存］をクリックします。
11. ［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：［新しいデバイスをこの設定に自動的に割り当てる］を選択しなかった場合は、「iOS デバイスに登録設定を割り当てる」を参照してください。

iOS デバイスに割り当てられた登録設定を削除

登録設定をデバイスに割り当てたが、適用はまだであるという場合は、デバイスから登録設定を削除できます。

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. 削除したい登録設定が割り当てられているデバイスの横にあるチェックボックスをオンにします。同じ DEP アカウントに登録されているデバイスを選択する必要があります。
3. をクリックします。
4. ［削除］をクリックします。

終了したら： iOS デバイスに登録設定を割り当てる.

登録設定の削除

デバイスに設定を適用するより先にこれらのデバイスに割り当てられていた登録設定を削除した場合、BlackBerry UEM はデバイスレコードに割り当てられた登録設定を削除します。

1. メニューバーで［設定］をクリックします。
2. 左ペインで、［外部統合］ > ［**Apple Device Enrollment Program**］をクリックします。
3. DEP アカウントの名前をクリックします。
4. ［**DEP** 登録設定］セクションで ✕ をクリックします。
5. ［削除］をクリックします。

終了したら： BlackBerry UEM がデバイスから登録設定を削除する場合はデバイスに登録設定を割り当てます。

登録設定の設定を変更

デバイスに登録設定を割り当てたが、この設定をデバイスに適用していない場合、変更内容を設定に保存すると、BlackBerry UEM はこのデバイスに適用された登録設定を更新します。

1. メニューバーで［設定］をクリックします。
2. 左ペインで、［外部統合］ > ［**Apple Device Enrollment Program**］をクリックします。
3. DEP アカウントの名前をクリックします。
4. ［**DEP** 登録設定］セクションで、変更する設定の名前をクリックします。
5. 設定を変更します。
6. ［保存］をクリックします。

デバイスに割り当てられている登録設定の設定を表示

登録設定は iOS デバイスに割り当てられているが、設定が保留されている場合は、登録設定の設定を表示できます。

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. ［登録設定］列で、登録設定の名前をクリックします。

iOS デバイスにアクティベーションプロファイルを割り当てる

Apple DEP に登録されている各デバイスに、特定のアクティベーションプロファイルを割り当てることができます。たとえば、ユーザーが異なるアクティベーションタイプを必要とする複数の iOS デバイスを所有している場合、各デバイスにアクティベーションプロファイルを指定できます。デバイスがアクティベーションされると、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、そのユーザーアカウント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よりも優先されます。

作業を始める前に： アクティベーションプロファイルの作成.

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. アクティベーションプロファイルを割り当てるデバイスの横にあるチェックボックスをオンにします。同じ DEP アカウントに登録されているデバイスを選択する必要があります。
3. をクリックします。
4. ［アクティベーションプロファイル］ドロップダウンリストで、アクティベーションプロファイルを選択します。
5. ［割り当て］をクリックします。

iOS デバイスに割り当てられたアクティベーションプロファイルの削除

Apple DEP 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を削除すると、ユーザーアカウント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有効になります。

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. アクティベーションプロファイルを削除するデバイスの横にあるチェックボックスをオンにします。同じ DEP アカウントに登録されているデバイスを選択する必要があります。
3. をクリックします。
4. ［削除］をクリックします。

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。

iOS デバイスからのユーザー割り当ての解除

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. ［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。
3. ［割り当て解除］をクリックします。

アクティブ化されたデバイスの所有者の表示

デバイスが正常にアクティブ化されると、デバイスの所有者を表示できます。

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. ［ユーザーの関連付け］列で、ユーザー名のリンクをクリックします。

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

オンプレミス環境に BlackBerry UEM がある場合は、Apple Configurator 2 を使用して BlackBerry UEM でアクティブ化できるように iOS および iPadOS デバイスを準備できます。ユーザーは、BlackBerry UEM Client アプリを使用せずに、準備のできたデバイスをアクティブ化できます。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になります。

デバイスがアクティブ化されると、BlackBerry UEM はユーザーに割り当てられた IT ポリシーとプロファイルをデバイスに送信します。

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

メモ：特定の機能を使用する場合、BlackBerry UEM Client アプリ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 BlackBerry UEM Client を起動する必要があります。どのような場合に BlackBerry UEM Client アプリをユーザーに割り当てる必要があるかについては、support.blackberry.com/community にアクセスし、記事 39313 を参照してください。

Apple Configurator 2 を使用してデバイスをアクティブ化する手順

手順	アクション
1	オプションで、BlackBerry UEM Client アプリ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パスワードの設定とアクティベーションメールの送信。
6	デバイスをユーザーに配布し、ユーザーがセットアップ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、ユーザーが BlackBerry UEM Client アプリをインストールし、セットアップの完了後にアプリを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 から最新バージョンの Apple Configurator 2 をダウンロードしてインストールします。

1. Apple Configurator 2 のメニューで［プリファレンス］ > ［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 または https>://<*サーバー名*>:<*ポート*>* の形式で、BlackBerry 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。ポート設定の詳細については、計画関連の資料にある「BlackBerry UEM 待機ポート」を参照してください。
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。

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］をオンにした場合は、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。

デバイスのアクティベーションに関するトラブルシューティングのヒント

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。

- 対象のデバイスタイプが BlackBerry UEM でサポートされていることを確認します。サポートされるデバイスタイプの詳細については、「互換性一覧表」を参照してください。
- ユーザーがアクティベーションするデバイスタイプに対して利用可能なライセンスと、ユーザーに割り当てられているアクティベーションタイプがあることを確認します。詳細については、ライセンス関連の資料を参照してください。
- 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。
  - 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。
  - 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。BlackBerry UEM と連携するようにネットワークのファイアウォールを設定する方法の詳細については、support.blackberry.com/community にアクセスし、記事 36470 を参照してください。
- 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、アクティベートされるデバイスタイプをサポートし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定義している場合、デバイスが準拠していることを確認します。
- BlackBerry 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 BlackBerry 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。必須ポートの詳細については、計画関連の資料を参照してください。
- デバイスログを取得します。
  - iOS デバイスログファイルを取得する方法の詳細については、support.blackberry.com/community にアクセスし、記事 36986 を参照してください。
  - Android デバイスログファイルを取得する方法の詳細については、support.blackberry.com/community にアクセスし、記事 32516 を参照してください。

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実行する場合は、次の内容を確認してください。

- デバイスが Knox Workspace をサポートしていることを確認してください。Samsung の情報を参照してください。
- 保証ビットがトリガーされていないことを確認してください。Samsung の情報を参照してください。
- Knox のコンテナバージョンがサポートされていることを確認してください。Knox Workspace には、Knox Container 2.0 以降が必要です。Samsung Knox のサポートされるバージョンの詳細については、Samsung の一覧表を参照してください。

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実行する場合は、次の内容を確認してください。

- デバイスが Android Enterprise をサポートしていることを確認してください。詳細については、https://support.google.com/work/android/answer/6174145 にアクセスし、記事 6174145 を参照してください。
- 利用可能なライセンスがあり、アクティベーションタイプが 仕事用と個人用 - ユーザーのプライバシー に設定されていることを確認してください。
- 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を使用するには、デバイスで Android OS バージョン 5.1 以降が実行されている必要があります。
- BlackBerry UEM のユーザーアカウントで、Google ドメインと同じメールアドレスが使用されていることを確認してください。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。コアログファイルで次の内容を探します。
  - ```
    ERROR AfW: Could not find user in Google domain.Aborting user creation and
     activation.
    ```
  - ```
    ERROR job marked for quarantine due to: Unable to activate device -
     Unsupported activation type
    ```

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。

説明

このエラーは、アクティベーション時に、ライセンスが使用できないか、ライセンスが期限切れの場合に、デバイスに表示されます。

解決策

BlackBerry UEM で、次の操作を実行します。

- アクティベーションをサポートするための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。

詳細については、「デバイスのライセンス管理」を参照してください。

ユーザー名とパスワードを確認して、再度実行してください。

説明

このエラーは、アクティベーション時に、ユーザーが間違ったユーザー名、パスワード、またはその両方を入力すると、デバイスに表示されます。

解決策

正しいユーザー名とパスワードを入力します。

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。

説明

このエラーは、アクティベーション時に、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。

解決策

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ます。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。

説明

このエラーは、アクティベーション時に、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。

解決策

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ます。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：サーバーが使用できません

説明

このエラーは、アクティベーション時に、次のことが原因でデバイスに表示されます。

- iOS デバイスに送信される MDM プロファイルに署名するために BlackBerry UEM が使用している証明書は、デバイスに信頼されていません。ユーザーは、デバイスのアクティベーション時にこの証明書を信頼するように求められます。

- 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、BlackBerry UEM Client は必要な HTTP CONNECT コールおよび HTTP OPTIONS コールを BlackBerry UEM に対して作成できません。

解決策

解決策は、次のとおりです。

- オンプレミス環境では、iOS デバイス用の MDM プロファイルに署名するために BlackBerry UEM が使用した証明書を発行した CA に対して、ルート証明書をインストールします。この証明書の詳細については、「オンプレミスの設定関連の資料」を参照してください。
- BlackBerry UEM Client が BlackBerry UEM に対して HTTP CONNECT コールおよび HTTP OPTIONS コールを作成する処理が、プロキシの設定でブロックされていないことを確認します。詳細については、support.blackberry.com/community にアクセスし、記事 38644 を参照してください。

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

説明

このエラーは、アクティベーション時に、次のことが原因でデバイスに表示されます。

- ユーザー名が間違ってデバイスに入力された。
- デバイスアクティベーション用のお客様のアドレスが、デバイスに正しく入力されなかった。

  メモ： これは、BlackBerry Infrastructure での登録が無効になっている場合にのみ必要です。
- アクティベーションパスワードが設定されていない、またはパスワードが期限切れである。

解決策

解決策は、次のとおりです。

- ユーザー名とパスワードを確認します。
- デバイスアクティベーションの顧客アドレスを確認します。
- BlackBerry 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ます。

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。

考えられる原因

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

解決策

次の操作を 1 つ以上実行します。

- 管理コンソールのメニューバーで、［設定］ > ［外部統合］ > ［**Apple** プッシュ通知］をクリックします。APN 証明書のステータスが［インストール済み］であることを確認します。ステータスが正しくない場合は、APN 証明書の再登録を試みます。
- BlackBerry UEM と APN サーバー間の接続をテストするには、［**APN** 証明書をテスト］をクリックします。
- 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。

ユーザーがアクティベーションメールを受信していません

説明

BlackBerry UEM 内の設定はすべて正しいが、ユーザーがアクティベーションメールを受信していません。

解決策

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、BlackBerry 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。

ユーザーがスパムメールフォルダーまたは迷惑メールフォルダーでアクティベーションメールがないかチェックしたことを確認します。

［ユーザーの詳細］画面に **UEM** でアクティベーションされている **Windows** デバイスとして表示されるデバイスが予測より多い

説明

ユーザーが BlackBerry Access と BlackBerry Work for Windows をコンピューターにインストールする際、BlackBerry Access と BlackBerry Work for Windows は、BlackBerry UEM 管理コンソールの［ユーザーの詳細］画面に「Windows 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

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