BlackBerry UEM

Android デバイスの管理

管理

12.16

Contents

Android デバイスの管理

BlackBerry UEM では、Android デバイスがネットワークに接続する方法、有効にするデバイス機能、利用可能にするアプリを詳細に管理できます。デバイスの所有者が組織かユーザーかにかかわらず、組織の情報にモバイルアクセスを提供しながら、アクセス権を持たないユーザーから保護することができます。

このガイドでは、Android デバイスの管理オプションについて説明しています。また、利用可能なすべての機能を活用するために必要な詳細情報を確認できます。

ウェアラブルデバイスの管理

BlackBerry UEM では、Android ベースの特定のウェアラブルデバイスをアクティブにして管理できます。スマートグラスなどのウェアラブルデバイスでは、通知、ステップバイステップの手順説明、画像、ビデオなど、視覚的な情報にハンズフリーでアクセスできます。また、音声コマンドの発行、バーコードのスキャン、GPS ナビゲーションの利用も可能にします。

BlackBerry UEM では、次のウェアラブルデバイスがサポートされています。

- Vuzix M300 Smart Glasses

ウェアラブルデバイスを管理するには、Android デバイス向けの手順に従います。ウェアラブルデバイスでは、次の BlackBerry UEM 機能がサポートされています。

- QR Code を使用したデバイスのアクティベーション
- IT ポリシー
- Wi-Fi、VPN、エンタープライズ接続、コンプライアンス、および証明書プロファイル
- BlackBerry Secure Connect Service
- デバイスのコマンド
- アプリ管理
- デバイスグループ
- 位置情報サービス

ウェアラブルデバイスは、BlackBerry UEM Client を使用してアクティベーションを行います。アクティベーションパスワードではなく QR コードを使用して、ウェアラブルデバイスをアクティブにできます。

Android デバイスで制御できるもの

BlackBerry UEM は、Android デバイスで管理できる機能の制御に必要なツールをすべて備えています。また、デバイスを完全に管理しなくても、デバイスユーザーに作業リソースへの安全なアクセスを提供できる機能も含まれています。

制御レベル	説明
管理対象外のデバイス ユーザーのプライバシー アクティベーション	BlackBerry UEM のデバイスを、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すると、デバイスを完全に管理することなく、作業リソースへの安全なアクセスを提供できます。このオプションは、BYOD デバイスによく使用されます。 これらのアクティベーションにより、ユーザーは BlackBerry 2FA を使用して VPN 経由でネットワークにアクセスし、BlackBerry Workspaces を使用してファイルを安全に共有し、BlackBerry Work や BlackBerry Access などの BlackBerry Dynamics アプリをインストールして、仕事用のメールや職場のイントラネットにアクセスできます。
仕事用プロファイルがある管理対象デバイス 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	Android Enterprise デバイスは管理できますが、デバイス上に仕事用データと個人データを分ける仕事用プロファイルを作成すれば、個人使用が可能になります。このオプションでは、ユーザーの個人用データのプライバシーを保護しながら、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。BlackBerry Dynamics アプリなどの仕事用アプリをデバイス上で管理できます。 デバイスから仕事用データは消去できますが、個人用データは消去できません。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。このオプションは、企業所有の個人使用可能な（COPE：Corporate-Owned, Personally Enabled）デバイス、および BYOD デバイスによく使用されます。
仕事用プロファイルがある完全管理のデバイス 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	Android Enterprise デバイスは完全に管理できますが、デバイス上に仕事用と個人用のデータを分離する仕事用プロファイルを作成すれば、個人使用も一部可能です。ただし、組織はデバイスを完全に管理して、デバイスからすべてのデータを削除できます。IT ポリシールールには、仕事用プロファイルと個人用プロファイルに個別に適用できるものがあります。BlackBerry Dynamics アプリなどの仕事用アプリをデバイス上で管理できます。 デバイスで送受信された SMS、MMS、および通話をログに記録できます。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。このオプションは、COPE デバイスによく使用されます。

制御レベル	説明
完全管理のデバイス 仕事用領域のみ（Android Enterprise）アクティベーション	Android Enterprise デバイスは完全管理が可能で、仕事用プロファイルはありますが、個人用プロファイルはありません。このオプションでは、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。BlackBerry Dynamics アプリなどの仕事用アプリをデバイス上で管理できます。 デバイスで送受信された SMS、MMS、および通話をログに記録できます。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。このオプションは、企業所有の業務専用（COBO：Corporate-Owned Business Only）デバイスによく使用されます。
デバイス管理 MDM 制御 アクティベーション	Android 9.x 以前のデバイスは、コマンドと IT ポリシールールを使用して管理できます。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。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。 このアクティベーションタイプは Android 10 デバイスでは推奨されません。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。 デバイスグループおよびコンプライアンスプロファイルを使用して、Android 10 に更新される「MDM 制御 」アクティベーションでアクティブ化されたデバイスの動作を管理できます。詳細については、管理関連の資料を参照してください。

Android Enterprise は、次の機能を含む Android デバイス管理を完全にサポートします。

- パスワード要件を強制する
- IT ポリシーを使用してデバイスの機能を制御する（カメラや Bluetooth を無効にするなど）
- コンプライアンスルールを強制する
- Wi-Fi および VPN 接続プロファイル（プロキシを使用）を作成する
- メール、連絡先、カレンダーをデバイスと同期する
- 認証と S/MIME のために CA およびクライアント証明書をデバイスに送信する
- 必須アプリと許可された一般アプリおよび内部アプリを管理する
- 紛失または盗難にあったデバイスの捜索

BlackBerry UEM でアクティブ化された Android Enterprise デバイスは、エンタープライズデバイスおよび Android. を搭載した BlackBerry デバイスの Samsung Knox プラットフォームでのみ利用できるその他の制御もサポートします。

また、BlackBerry UEM は、企業向けのサポート Samsung Knox プラットフォームに加え、Samsung Knox Workspace アクティベーションのデバイスもサポートしていますが、今後のリリースでは Samsung Knox アクティベーションタイプは廃止される予定です。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。

メモ：一部の機能と BlackBerry Dynamics アプリは、ライセンスレベルによってはご利用いただけません。利用可能なライセンスの詳細については、ライセンス関連の資料を参照してください。

Android デバイスを管理する手順

手順	アクション
1	インストール手順に従って、BlackBerry UEM をインストールして設定します。
2	組織で Android Enterprise デバイスを管理する場合は、管理対象 Google Play アカウントか、Google Cloud または G Suite ドメインへの接続を設定します。
3	デバイスの IT ポリシーを設定します。IT ポリシーをユーザーグループまたは個々のユーザーに割り当てます。
4	デバイス用プロファイルを設定します。プロファイルをユーザーグループまたは個々のユーザーに割り当てます。
5	デバイスがインストールできる、またはインストールする必要があるアプリを指定します。
6	デバイスをアクティベーションします。
7	デバイスを管理および監視します。

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。

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。
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。

設定	説明
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。
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。

IT ポリシーによる Android デバイスの制御

BlackBerry UEM は IT ポリシーを各デバイスに送信します。デフォルトの IT ポリシーを使用することも、独自の IT ポリシーを作成することもできます。さまざまな状況やユーザーに応じて必要な数だけ IT ポリシーを作成できますが、デバイス上でアクティブになる IT ポリシーは 1 つだけです。

Android の IT ポリシールールは、デバイスの機能と、Google で提供されるデバイス設定オプションに基づいています。Google が新しい機能や設定オプションを備えた OS 更新を新規にリリースすると、次の機会に新しい IT ポリシールールが UEM に追加されます。

検索およびソート可能な IT ポリシールールのスプレッドシートをダウンロードできます。このスプレッドシートには、ルールをサポートする最小限のデバイス OS など、UEM で利用可能なルールがすべて記載されています。

IT ポリシーで制御するデバイスの動作には、次のようなオプションがあります。

- デバイスのパスワード要件
- カメラや Bluetooth などのデバイス機能を許可する
- あるプロファイル内のアプリが別のプロファイル内のデータにアクセスできるようにする
- 仕事用プロファイル内のアプリとデータに対してのみ機能を制限する

IT ポリシーのデバイスへの送信の詳細については、管理関連の資料を参照してください。

Android のパスワード要件の設定

Android のパスワードには、4 つのグループの IT ポリシールールがあります。使用するルールのグループは、デバイスのアクティベーションタイプや、デバイスのパスワードまたは仕事用領域のパスワードに要件を設定するかどうかで異なります。

IT ポリシーでパスワードルールを設定したら、コンプライアンスプロファイルを使用してパスワードの要件を強制します。

アクティベーションタイプ	サポートされるパスワードのルール
仕事用と個人用 - ユーザーのプライバシー （Android Enterprise）および 仕事用と個人用 - フルコントロール （Android Enterprise）	グローバルパスワードルールを使用して、デバイスパスワードの要件を設定します。 仕事用プロファイルのパスワードルールを使用して、仕事用プロファイルのパスワード要件を設定します。 Knox のパスワードルールはデバイスで無視されます。
仕事用領域のみ （Android Enterprise）	グローバルパスワードルールを使用して、デバイスのパスワード要件を設定します。デバイスには仕事用領域のみがあるため、このパスワードは仕事用領域のパスワードも兼ねています。 その他のすべてのパスワードルールはデバイスで無視されます。

アクティベーションタイプ	サポートされるパスワードのルール
MDM 制御	グローバルパスワードルールを使用して、デバイスパスワードの要件を設定します。 その他のすべてのパスワードルールはデバイスで無視されます。 メモ：MDM 制御 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。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。
MDM 制御 （Samsung Knox）	Knox MDM のパスワードルールを使用して、デバイスパスワードの要件を設定します。 その他のすべてのパスワードルールはデバイスで無視されます。
仕事用と個人用 - ユーザーのプライバシー （Samsung Knox）	管理者には、デバイスのパスワードの管理権限はありません。 Knox Premium - Workspace のパスワードルールを使用して、仕事用領域のパスワード要件を設定します。 その他のすべてのパスワードルールはデバイスで無視されます。 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。
仕事用と個人用 - フルコントロール （Samsung Knox）	Knox MDM のパスワードルールを使用して、デバイスパスワードの要件を設定します。 Knox Premium - Workspace のパスワードルールを使用して、仕事用領域のパスワード要件を設定します。 その他のすべてのパスワードルールはデバイスで無視されます。
仕事用領域のみ （Samsung Knox）	Knox Premium - Workspace のパスワードルールを使用して、仕事用領域のパスワード要件を設定します。 その他のすべてのパスワードルールはデバイスで無視されます。

Android ：グローバルパスワードルール

グローバルパスワードルールは、次のアクティベーションタイプのデバイスに対して、デバイスのパスワード要件を設定します。

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

メモ：MDM 制御 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。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。

ルール	説明
パスワードの要件	パスワードの最小要件を指定します。次のいずれかのオプションを選択できます。 • 指定しない：パスワードは必須ではありません。 • 任意：パスワードを設定する必要がありますが、長さや質に関する要件はありません。 • 数字：パスワードには 1 文字以上の数字を含める必要があります。 • 英字：パスワードには 1 文字以上の英字を含める必要があります。 • 英数字：パスワードには、英字と数字を各 1 文字以上含める必要があります。 • 複雑：異なる文字タイプで特定の要件を設定できます。
パスワードの最大失敗試行回数	デバイスがワイプまたは無効にされる前に、間違ったパスワードを入力できる回数を指定します。 アクティベーションタイプが［MDM 制御］であるデバイスは消去されます。 アクティベーションタイプが「仕事用および個人用 - ユーザープライバシー」および「仕事用および個人用 - ユーザープライバシー（Premium）」であるデバイスは無効になり、仕事用プロファイルが削除されます。
ロックまでの最大アクティビティなし時間	ユーザーアクティビティのない時間が最大で何分経過したらデバイスまたは仕事用領域をロックするかを指定します。仕事用プロファイルがある Android デバイスでは、仕事用領域もロックされます。ユーザーは、より短い時間をデバイスに設定できます。パスワードが必須ではない場合、このルールは無視されます。
パスワード有効期限のタイムアウト	パスワードを使用できる最大時間を指定します。指定された時間が経過すると、新しいパスワードを設定する必要があります。0 に設定すると、パスワードは期限切れになりません。
パスワード履歴の制限	最近の数字、英字、英数字、複雑なパスワードの再利用を防ぐため、デバイスがチェックする以前のパスワードの最大数を指定します。0 に設定すると、以前のパスワードはチェックされません。
パスワードの最小文字数	数字、英字、英数字、または複雑なパスワードの最小文字数を指定します。
パスワードに必要な大文字の数	複雑なパスワードに含める必要がある大文字の最小数を指定します。
パスワードに必要な小文字の数	複雑なパスワードに含める必要がある小文字の最小数を指定します。
パスワードに必須の最小文字数	複雑なパスワードに含める必要がある英字の最小数を指定します。

ルール	説明
パスワードの英数字以外の文字の最小数	複雑なパスワードに含める必要がある英字以外の文字（数字や記号など）の最小数を指定します。
パスワードに必要な数字の最小数	複雑なパスワードに含める必要がある数字の最小数を指定します。
パスワードに必要な記号の数	複雑なパスワードに含める必要がある英数字以外の文字の最小数を指定します。

IT ポリシーのパスワードの詳細については、『ポリシーリファレンススプレッドシート』をダウンロードしてください。

Android ：仕事用プロファイルのパスワードルール

仕事用プロファイルのパスワードルールは、次のアクティベーションタイプのデバイスに対して、仕事用領域のパスワード要件を設定します。

- 仕事用と個人用 - ユーザーのプライバシー （Android Enterprise）
- 仕事用と個人用 - フルコントロール （Android Enterprise）

ルール	説明
パスワードの要件	仕事用領域のパスワードの最小要件を指定します。次のいずれかのオプションを選択できます。 • 任意：パスワードを設定する必要がありますが、長さや質に関する要件はありません。 • 数字：パスワードには 1 文字以上の数字を含める必要があります。 • 英字：パスワードには 1 文字以上の英字を含める必要があります。 • 英数字：パスワードには、英字と数字を各 1 文字以上含める必要があります。 • 複雑：異なる文字タイプで特定の要件を設定できます。 • 複雑な数字 - パスワードには数字を含める必要がありますが、反復列（4444）や連続列（1234、4321、2468）は使用できません。 • 弱いバイオメトリック - パスワードではセキュリティの低いバイオメトリック識別テクノロジが許容されます。 Android を搭載した BlackBerry デバイスの場合、BlackBerry デバイスの「デバイスと仕事用領域のパスワードを異なるものに強制」ルールを使用して、仕事用領域のパスワードとデバイスパスワードを別々にするように強制できます。
パスワードの最大失敗試行回数	デバイスが無効化され、仕事用領域プロファイルが削除されるまでに、ユーザーが間違った仕事用領域パスワードを入力できる回数を指定します。

ルール	説明
ロックまでの最大アクティビティなし時間	ユーザーアクティビティのない時間が最大で何分経過したらデバイスおよび仕事用領域をロックするかを指定します。このルールと Android グローバルの「ロックまでの最大アクティビティなし時間」ルールの両方を設定した場合、デバイスと仕事用領域はどちらかのタイマーが切れるとロックされます。ユーザーは、より短い時間をデバイスに設定できます。
パスワード有効期限のタイムアウト	仕事用領域パスワードを使用できる最大時間を指定します。指定された時間が経過すると、新しい仕事用領域パスワードを設定する必要があります。0 に設定すると、パスワードは期限切れになりません。
パスワード履歴の制限	最近の数字、英字、英数字、複雑なパスワードの再利用を防ぐため、デバイスがチェックする以前の仕事用領域パスワードの最大数を指定します。0 に設定すると、以前のパスワードはチェックされません。
パスワードの最小文字数	数字、英字、英数字、または複雑な仕事用領域パスワードの最小文字数を指定します。
パスワードに必要な大文字の数	複雑な仕事用領域パスワードに含める必要がある大文字の最小数を指定します。
パスワードに必要な小文字の数	複雑な仕事用領域パスワードに含める必要がある小文字の最小数を指定します。
パスワードに必須の最小文字数	複雑な仕事用領域パスワードに含める必要がある英字の最小数を指定します。
パスワードの英数字以外の文字の最小数	複雑な仕事用領域パスワードに含める必要がある英字以外の文字（数字や記号など）の最小数を指定します。
パスワードに必要な数字の最小数	複雑な仕事用領域パスワードに含める必要がある数字の最小数を指定します。
パスワードに必要な記号の数	複雑な仕事用領域パスワードに含める必要がある英数字以外の文字の最小数を指定します。
デバイスと仕事用プロファイルのパスワードが異なるように強制する	ユーザーがデバイスと仕事用プロファイルに異なるパスワードを設定する必要があるかどうかを指定します。パスワードが同じ場合、デバイスのロックを解除すると、仕事用プロファイルがロック解除されます。

IT ポリシーのパスワードの詳細については、『ポリシーリファレンススプレッドシート』をダウンロードしてください。

プロファイルによる Android デバイスの制御

BlackBerry UEM には、デバイス機能のさまざまな側面の制御に使用できるプロファイルがいくつか含まれています。最も一般的に使用されるプロファイルは次のとおりです。

プロファイル名	説明	設定
アクティベーション	アクティベーションタイプ、方法、およびユーザーがアクティブ化できるデバイスの数や種類など、ユーザーのデバイスアクティベーション設定を指定します。	アクティベーションプロファイルの作成
Wi-Fi	仕事用 Wi-Fi ネットワークに接続するデバイスの設定を指定します。	Wi-Fi プロファイルの作成
VPN	仕事用 VPN に接続するデバイスの設定を指定します。	VPN プロファイルの作成
プロキシ	デバイスがインターネットまたは仕事用ネットワークで Web サービスにアクセスする際のプロキシサーバーの使用方法を指定します。	プロキシプロファイルの作成
メール	デバイスを仕事用メールサーバーに接続し、メールやカレンダーエントリ、オーガナイザーデータを同期する方法を指定します。BlackBerry Work をデバイスにインストールして構成する場合は、メールプロファイルをセットアップする必要はありません。	メールプロファイルの作成
BlackBerry Dynamics	デバイスが BlackBerry Work、BlackBerry Access、BlackBerry Connect などの BlackBerry Dynamics アプリにアクセスできるようにします。	BlackBerry Dynamics プロファイルの作成
BlackBerry Dynamics 接続	BlackBerry Dynamics アプリを使用するときにデバイスが接続できるネットワーク接続方法、インターネットドメイン、IP アドレス範囲、およびアプリサーバーを定義します。	BlackBerry Dynamics 接続プロファイルの作成
コンプライアンス	組織で許容できないデバイスの条件を定義し、強制する操作を設定します。	コンプライアンスプロファイルの作成
エンタープライズ接続	デバイスが BlackBerry Secure Connect Plus を使用できるかどうかを指定します。	BlackBerry Secure Connect Plus を有効化する
CA 証明書	仕事用ネットワークまたはサーバーとの信頼性を確立するためにデバイスが使用できる CA 証明書を指定します。	CA 証明書プロファイルの作成

プロファイル名	説明	設定
ユーザー資格情報	仕事用ネットワークまたはサーバーで認証を実行するためにデバイスがクライアント証明書を取得する方法を指定します。	ユーザー資格情報プロファイルを作成
SCEP	仕事用ネットワークまたはサーバーとの認証に使用されるクライアント証明書を取得するために使用する SCEP サーバーを指定します。	SCEP プロファイルの作成

デバイスへの情報送信の詳細については、管理関連の資料を参照してください。

プロファイルリファレンス - Android デバイス

次の表に、BlackBerry UEM デバイスでサポートされる Android のすべてのプロファイルを示します。

プロファイル名	説明	設定
ポリシー		
アクティベーション	アクティベーションタイプやデバイスの数および種類など、ユーザーのデバイスアクティベーション設定を指定します。	アクティベーションプロファイルの作成
BlackBerry Dynamics	デバイスが BlackBerry Work、BlackBerry Access、BlackBerry Connect などの BlackBerry Dynamics アプリにアクセスできるようにします。	BlackBerry Dynamics プロファイルの作成
アプリロックモード	デバイスで実行する単一のアプリを指定します。 MDM のみでアクティブ化された Samsung Knox デバイス	アプリロックモードプロファイルを作成
エンタープライズ管理エージェント	プッシュ通知を使用できない場合に、デバイスが BlackBerry UEM に接続してアプリと設定の更新の有無を確認するタイミングを指定します。	エンタープライズ管理エージェントプロファイルの作成
コンプライアンス		
コンプライアンス	組織で許容できないデバイスの条件を定義し、強制する操作を設定します。	コンプライアンスプロファイルの作成

プロファイル名	説明	設定
コンプライアンス（BlackBerry Dynamics）	これは、Good Control からオンプレミス BlackBerry UEM にインポートされたコンプライアンス設定を表示する読み取り専用のプロファイルです。	BlackBerry Dynamics コンプライアンスプロファイルの管理
デバイス SR 要件	デバイスにインストールされている必要があるソフトウェアリリースバージョンを定義し、フォアグラウンドで実行されているアプリの更新期間を指定します。	デバイス SR 要件プロファイルの作成
メール、カレンダー、および連絡先		
メール	デバイスを仕事用メールサーバーに接続し、Exchange ActiveSync や IBM Notes Traveler を使ってメールやカレンダーエントリ、オーガナイザーデータを同期する方法を指定します。	メールプロファイルの作成
IMAP/POP3 メール	デバイスの IMAP や POP3 メールサーバーへの接続方法とメールメッセージの同期方法を指定します。	IMAP/POP3 メールプロファイルを作成
ゲートキーピング	自動ゲートキーピングに使用する Microsoft Exchange サーバーを指定します。	ゲートキーピングプロファイルの作成
ネットワークと接続		
Wi-Fi	仕事用 Wi-Fi ネットワークへのデバイスの接続方法を指定します。	Wi-Fi プロファイルの作成
VPN	仕事用 VPN へのデバイスの接続方法を指定します。	VPN プロファイルの作成
プロキシ	デバイスがインターネットまたは仕事用ネットワークで Web サービスにアクセスする際のプロキシサーバーの使用方法を指定します。	プロキシプロファイルの作成
エンタープライズ接続	エンタープライズ接続を使用して、デバイスが組織のリソースに接続する方法を指定します。Android Enterprise および Samsung Knox Workspace デバイスの場合、エンタープライズ接続プロファイルは、デバイスが BlackBerry Secure Connect Plus を使用できるかどうかを指定します。	BlackBerry Secure Connect Plus を有効化する

プロファイル名	説明	設定
BlackBerry Dynamics 接続	BlackBerry Dynamics アプリを使用するときにデバイスが接続できるネットワーク接続、インターネットドメイン、IP アドレス範囲、およびアプリサーバーを定義します。	BlackBerry Dynamics 接続プロファイルの作成
BlackBerry 2FA	ユーザーのツーファクター認証を有効にし、事前認証および自己回復機能の設定を指定します。	BlackBerry 2FA プロファイルの作成
アクセスポイント名プロファイル	通信事業者への接続に使用するデバイスの APN を指定できます。	アクセスポイント名プロファイルの作成
保護		
Microsoft Intune アプリの保護	Microsoft Intune で保護されているアプリを管理できます。	Microsoft Intune アプリ保護プロファイルの作成
位置情報サービス	デバイスの位置を要求し、地図上のおおよその位置を表示することができます。	位置情報サービスプロファイルの作成
サイレント	定義した日数および時間数の間、BlackBerry Work for Android の通知をブロックできます。	サイレントプロファイルの作成
カスタム		
デバイス	デバイスに表示する情報を設定できます。	デバイスプロファイルの作成
証明書		
CA 証明書	仕事用ネットワークまたはサーバーとの信頼性を確立するためにデバイスが使用できる CA 証明書を指定します。	CA 証明書プロファイルの作成
共有証明書	仕事用ネットワークまたはサーバーでユーザーを認証するためにデバイスが使用できるクライアント証明書を指定します。	共有の証明書プロファイルの作成
ユーザー資格情報	仕事用ネットワークまたはサーバーとの認証に使用されるクライアント証明書を取得するために使用する CA 接続を指定します。	ユーザー資格情報プロファイルを作成
SCEP	仕事用ネットワークまたはサーバーとの認証に使用されるクライアント証明書を取得するために使用する SCEP サーバーを指定します。	SCEP プロファイルの作成

プロファイル名	説明	設定
CRL	証明書のステータスを確認するために BlackBerry UEM が使用できる CRL 設定を指定します。 Android を搭載した BlackBerry デバイスのみ	CRL プロファイルの作成
証明書マッピングプロファイル	アプリが使用する必要があるクライアント証明書を指定します。	証明書マッピングプロファイルの作成

Android デバイスでのアプリの管理

デバイスで管理および監視するアプリのライブラリを作成できます。Android Enterprise デバイスの場合、許可したアプリのみを仕事用プロファイルにインストールできます。BlackBerry UEM は、Android デバイス上のアプリを管理するために、次のオプションを提供します。

- Google Play から、オプションアプリまたは必須アプリとして、デバイスに一般のアプリを割り当てます。
- UEM にカスタムアプリをアップロードし、オプションまたは必須のアプリとして展開します。
- アプリで許可されている場合、接続設定などのアプリ設定を事前設定します。
- ユーザーによるアプリへのアクセスをブロックします。
- 一般、ISV、およびカスタムの BlackBerry Dynamics アプリを設定して、ユーザーが仕事用リソースにアクセスできるようにします。
- UEM を Microsoft Intune に接続して、Intune アプリ保護ポリシーを UEM 管理コンソール内から設定し、Office 365 アプリを導入および管理します。
- デバイスにインストールされている個人用アプリのリストを表示します。
- 環境内の他のユーザーのために、各ユーザーがアプリを評価およびレビューできるようにします。

Android Enterprise デバイスでのアプリの動作

BlackBerry Dynamics が有効になっているデバイスの場合、「機能 - BlackBerry App Store」資格をユーザーに割り当てている場合は、仕事用アプリのカタログが BlackBerry Dynamics Launcher に表示されます。詳細については、「BlackBerry Dynamics Launcher への仕事用アプリカタログの追加」を参照してください。

Android Enterprise デバイスの場合、次の動作が行われます。

アプリタイプ	アプリがユーザーに割り当てられるとき	アプリが更新されるとき	アプリがユーザーから割り当て解除されるとき	デバイスが **BlackBerry UEM** から削除されるとき
種別が必須になっている一般のアプリ	アプリは自動的にインストールされます。	アプリは自動的に更新されます。	アプリは自動的にデバイスから削除されます。	仕事用プロファイルと割り当てられた仕事用アプリケーションはデバイスから削除されます。
種別がオプションになっている一般のアプリ	ユーザーはアプリをインストールするかどうかを選択できます。 アプリは仕事用 Google Play に表示されます。	Google Play for Work は、ユーザーに更新を通知します。	アプリは自動的にデバイスから削除されます。	仕事用プロファイルと割り当てられた仕事用アプリケーションはデバイスから削除されます。

アプリタイプ	アプリがユーザーに割り当てられるとき	アプリが更新されるとき	アプリがユーザーから割り当て解除されるとき	デバイスが **BlackBerry UEM** から削除されるとき
BlackBerry UEM でホストされている必須の種別になっている内部アプリ	仕事用領域のみ デバイスでのみサポートされます。 アプリは自動的にインストールされます。	仕事用領域のみ デバイスでのみサポートされます。 アプリは自動的にインストールされます。	アプリは自動的にデバイスから削除されます。	アプリは自動的にデバイスから削除されます。
BlackBerry UEM でホストされているオプションの種別になっている内部アプリ	ユーザーはアプリをインストールするかどうかを選択できます。 アプリは仕事用 Google Play に表示されます。	Google Play for Work は、ユーザーに更新を通知します。	アプリは自動的にデバイスから削除されます。	仕事用プロファイルと割り当てられた仕事用アプリケーションはデバイスから削除されます。
Google Play でホストされている必須の種別になっている内部アプリ	アプリは自動的にデバイスにインストールされます。	Google Play for Work は、ユーザーに更新を通知します。	アプリは自動的にデバイスから削除されます。	仕事用プロファイルと割り当てられた仕事用アプリケーションはデバイスから削除されます。
Google Play でホストされているオプションの種別になっている内部アプリ	ユーザーはアプリをインストールするかどうかを選択できます。 アプリは仕事用 Google Play に表示されます。	Google Play for Work は、ユーザーに更新を通知します。	アプリは自動的にデバイスから削除されます。	仕事用プロファイルと割り当てられた仕事用アプリケーションはデバイスから削除されます。

デバイス SR 要件プロファイルでフォアグラウンドで実行されているアプリケーションの更新動作を指定できます。

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

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。 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 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。 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。 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。 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、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。 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。 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. 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。

11. ［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。

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。
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。

タスク	手順
	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。

アクティブ化された Android デバイスの管理と監視

デバイスがアクティブ化され、IT ポリシーとプロファイルによって管理されると、ユーザーのデバイスを制御するいくつかの機能を使用できるようになります。

次のオプションがあります。

オプション	説明
デバイスにインストールするソフトウェア更新と、更新のタイミングを制御します。	デバイス SR 要件プロファイルを使用して、次に示すデバイスに OS 更新をインストールするかどうか、また更新をいつ行うかを指定できます。 • 仕事用領域のみ がアクティブ化されている Android Enterprise デバイス • Samsung Knox デバイス 詳細については、管理関連の資料を参照してください。 コンプライアンスプロファイルを使用して、指定対象の OS バージョンを制限できます。詳細については、管理関連の資料を参照してください。
位置情報の設定をオンにしてデバイスを探す	位置情報設定をオンにして、Android デバイスの位置を追跡できます。 詳細については、管理関連の資料を参照してください。
デバイスログの取得	デバイスからログを取得して、監視やトラブルシューティングを行うことができます。 詳細については、管理関連の資料を参照してください。
デバイスを無効にする	管理者またはユーザーがデバイスを無効化すると、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。 管理者は、［すべてのデバイスデータを削除］または［仕事用データのみを削除］コマンドを使用してデバイスを無効化できます。 ユーザーは、Android アプリの［バージョン情報］画面で［デバイスを無効にする］を選択することで、BlackBerry UEM Client デバイスを無効化できます。

Android デバイスのコマンド

コマンド	説明	アクティベーションタイプ
デバイスレポートを表示	このコマンドを実行すると、デバイスに関する詳細情報が表示されます。デバイスレポートをエクスポートしたりコンピューターに保存したりできます。詳細については、「デバイスレポートの表示と保存」を参照してください。	すべて（BlackBerry 2FA を除く）
デバイスでの操作を表示	このコマンドを実行すると、デバイスで実行中のアクションが表示されます。詳細については、「デバイスアクションの表示」を参照してください。	すべて（BlackBerry 2FA を除く）
デバイスのロック	このコマンドは、デバイスをロックします。ユーザーは、デバイスのロックを解除するために、既存のデバイスパスワードを入力する必要があります。一時的にデバイスが見つからない場合、このコマンドを使用することができます。 このコマンドを送信すると、既存のデバイスパスワードが存在する場合に限ってデバイスがロックされます。それ以外の場合、デバイスでは何の操作も実行されません。	MDM 制御 仕事用と個人用 - フルコントロール（Android Enterprise） 仕事用と個人用 - ユーザーのプライバシー（Android Enterprise） 仕事用領域のみ（Android Enterprise）
すべてのデバイスデータを削除	このコマンドは、仕事用領域内の情報を含め、デバイスに保存されているユーザー情報とアプリデータをすべて削除し、デバイスを工場出荷時のデフォルト設定に戻します。 このコマンドを送信するときにデバイスが BlackBerry UEM に接続できない場合、このコマンドをキャンセルするか、コンソールからデバイスを削除することができます。削除後にデバイスが BlackBerry UEM に接続する場合で、状況が該当する場合は、仕事用領域を含めて、仕事用データのみがデバイスから削除されます。 このコマンドを複数のデバイスに送信するには、「一括コマンドの送信」を参照してください。	MDM 制御 仕事用と個人用 - フルコントロール（Android Enterprise） 仕事用と個人用 - フルコントロール（Samsung Knox） 仕事用領域のみ -（Samsung Knox）

コマンド	説明	アクティベーションタイプ
仕事用データのみを削除	このコマンドは、デバイス上の IT ポリシー、アプリ、証明書を含む仕事用データを削除し、デバイスを無効化します。デバイスに仕事用領域がある場合は、仕事用領域の情報と領域自体がデバイスから削除されますが、すべての個人アプリとデータはデバイスに残ります。詳細については、「デバイスの無効化」を参照してください。 Android Enterprise デバイスでこのコマンドを使用すると、作業プロファイルが削除された理由としてユーザーのデバイスの通知に表示される説明文を入力できます。 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の場合、このコマンドは Android 11 以降を実行しているデバイスでのみサポートされます。 このコマンドを送信するときにデバイスが BlackBerry UEM に接続できない場合、このコマンドをキャンセルするか、コンソールからデバイスを削除することができます。削除後にデバイスが BlackBerry UEM に接続する場合で、状況が該当する場合は、仕事用領域を含め、仕事用データがデバイスから削除されます。 このコマンドを複数のデバイスに送信するには、「一括コマンドの送信」を参照してください。	MDM 制御 仕事用と個人用 - ユーザーのプライバシー（Android Enterprise） 仕事用と個人用 - フルコントロール（Android Enterprise） 仕事用と個人用 - ユーザーのプライバシー（Samsung Knox） 仕事用と個人用 - フルコントロール（Samsung Knox） 仕事用領域のみ -（Samsung Knox）
デバイスをロック解除してパスワードをクリア	このコマンドは、デバイスをロック解除し、ユーザーに新しいデバイスパスワードを作成するように求めるプロンプトを表示します。ユーザーが［デバイスパスワードを作成］画面をスキップした場合、以前のパスワードが保持されます。このコマンドは、ユーザーがデバイスパスワードを忘れた場合に使用できます。 メモ：このコマンドは、Samsung Knox SDK 3.2.1 以降を実行しているデバイスではサポートされていません。	MDM 制御（Samsung デバイスのみ） 仕事用と個人用 - フルコントロール（Samsung Knox） 仕事用と個人用 - ユーザーのプライバシー（Samsung Knox）
デバイスパスワードの指定とロック	このコマンドを使用して、デバイスパスワードを作成し、デバイスをロックできます。既存のパスワードルールに準拠したパスワードを作成する必要があります。デバイスのロックを解除するには、新しいパスワードを入力する必要があります。 メモ：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場合、Android 8.x 以降を搭載した BlackBerry デバイスだけがこのコマンドをサポートしています。 メモ：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の場合、Android 11 より前のバージョンの Android OS を使用しているデバイスだけがこのコマンドをサポートしています。	仕事用と個人用 - フルコントロール（Samsung Knox） 仕事用領域のみ（Android Enterprise） 仕事用と個人用 - フルコントロール（Android Enterprise） 仕事用と個人用 - ユーザーのプライバシー（Android Enterprise）

コマンド	説明	アクティベーションタイプ
仕事用領域パスワードをリセット	このコマンドは、現在の仕事用領域パスワードをデバイスから削除します。ユーザーが仕事用領域を開くと、新しい仕事用領域パスワードを設定するように要求されます。	仕事用と個人用 - フルコントロール（Samsung Knox） 仕事用と個人用 - ユーザーのプライバシー -（Samsung Knox） 仕事用領域のみ -（Samsung Knox）
仕事用領域パスワードの指定とロック	仕事用プロファイルのパスワードを指定して、デバイスをロックできます。ユーザーは、仕事用アプリを開くときに、指定されたパスワードを入力する必要があります。	仕事用と個人用 - ユーザーのプライバシー（Android Enterprise） 仕事用と個人用 - フルコントロール（Android Enterprise）
仕事用領域を無効化/有効化	このコマンドは、デバイス上の仕事用領域アプリへのアクセスを無効または有効にします。	仕事用と個人用 - フルコントロール（Samsung Knox） 仕事用と個人用 - ユーザーのプライバシー -（Samsung Knox） 仕事用領域のみ -（Samsung Knox）
BlackBerry 2FA を無効化	このコマンドは、BlackBerry 2FA アクティベーションタイプでアクティベーションされているデバイスを無効にします。デバイスは BlackBerry UEM から削除され、ユーザーは BlackBerry 2FA 機能を使用することができません。	BlackBerry 2FA
アプリを消去	このコマンドは、Microsoft Intune で管理している全アプリのデータをデバイスから消去します。アプリはデバイスから削除されません。 詳細については、「Microsoft Intune で管理されているアプリの消去」を参照してください。	すべて（BlackBerry 2FA を除く）
デバイス情報を更新	このコマンドは更新されたデバイス情報を送受信します。たとえば、新たに更新された IT ポリシールールやプロファイルをデバイスに送信したり、OS バージョンやバッテリー残量などのデバイスに関する最新情報を受信したりすることができます。 このコマンドを複数のデバイスに送信するには、「一括コマンドの送信」を参照してください。	すべて（BlackBerry 2FA を除く）

コマンド	説明	アクティベーションタイプ
バグレポートを要求	このコマンドは、デバイスにクライアントログの要求を送信します。デバイスユーザーは、要求を承認または拒否する必要があります。	仕事用領域のみ（Android Enterprise） 仕事用と個人用 - フルコントロール（Android Enterprise）
デバイスを再起動する	このコマンドは、デバイスに再起動の要求を送信します。デバイスが 1 分後に再起動するというメッセージがユーザーに表示されます。デバイスユーザーには、再起動を 10 分間スヌーズするオプションがあります。	仕事用領域のみ（Android Enterprise）
デバイスを削除	このコマンドは、デバイスを BlackBerry UEM から削除しますが、デバイスからデータを削除しません。デバイスはメールなどの仕事用データをひき続き受信する場合があります。 このコマンドは、回復不能なほど失われたまたは損傷したデバイスを対象としており、サーバーに再度接続することは想定されていません。削除されたデバイスが BlackBerry UEM に接続しようとすると、ユーザーは通知を受信し、再アクティブ化しない限り、デバイスは BlackBerry UEM と通信できなくなります。 このコマンドを複数のデバイスに送信するには、「一括コマンドの送信」を参照してください。	すべて（BlackBerry 2FA を除く）

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