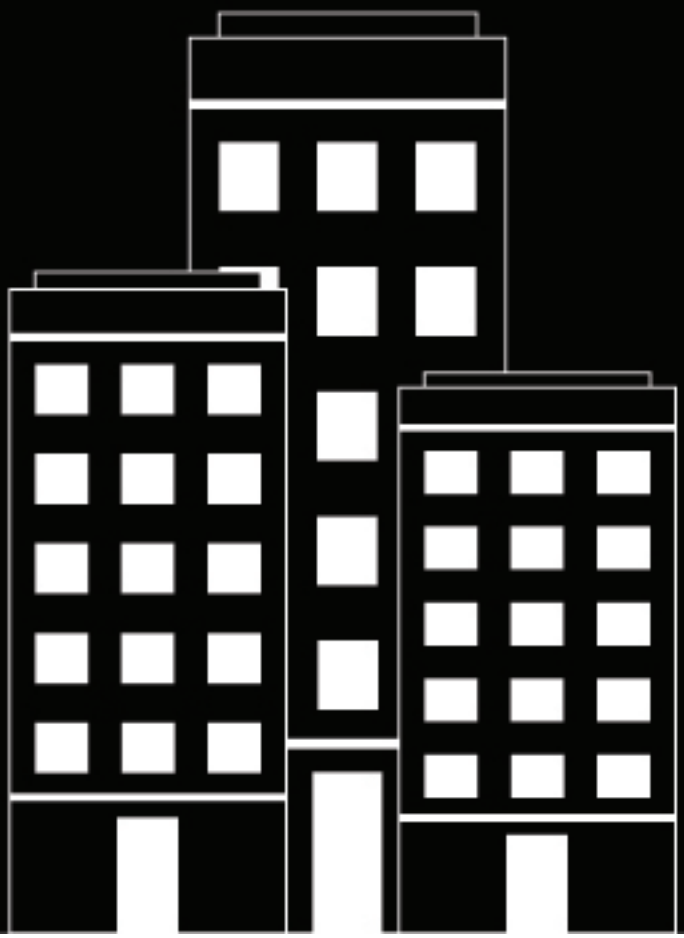

BlackBerry UEM

デバイス構成の管理

12.20

目次

デバイス設定の管理

このガイドでは、BlackBerry UEM プロファイル、IT ポリシー、その他の主な機能を使用して、組織のニーズとセキュリティ要件を満たすように仕事用デバイスを設定する手順について説明します。

タスク	説明
プロファイルを使用してデバイス機能を管理します。	UEM プロファイルを設定してユーザーおよびグループに割り当て、すべてのデバイスタイプのさまざまなデバイス機能を管理します。
プロファイル、メール、通知で変数を使用します。	プロファイル、コンプライアンス通知、アクティベーションメール、およびイベント通知で変数を使用して、個々のユーザーの設定とメッセージをカスタマイズします。
ユーザーにメッセージを送信するためにメールテンプレートを使用します。	メールテンプレートを使用して、UEM デバイスの有効化の手順の提供、コンプライアンスの問題に関するユーザーへの通知、BlackBerry Dynamics アプリのアクセスキーの提供など、さまざまな理由でユーザーに送信するメールメッセージをカスタマイズおよびパーソナライズします。
IT ポリシーによりデバイスを管理します。	IT ポリシーを使用して、デバイスの機能を制御します。たとえば、IT ポリシールールを使用して、パスワード要件の適用、特定のデバイス機能（カメラなど）の使用禁止、特定のアプリの可用性の制御を行うことができます。
Android デバイス上で無効化された機能のデバイスサポートメッセージの作成。	IT ポリシーによって機能が無効になっている場合、Android デバイスにサポートメッセージを表示します。
デバイスのコンプライアンスルールを強制します。	コンプライアンスプロファイルを使用して、ユーザーが組織のデバイス標準に従うように促します。コンプライアンスプロファイルは、組織内で受け入れられないデバイス条件を定義し、ユーザーがコンプライアンスの問題を修正しない場合に UEM が実行するための強制アクションを指定します。
ユーザーおよびデバイスにコマンドを送信します。	さまざまなコマンドを送信して、ユーザーアカウントとデバイスを管理できます。たとえば、デバイスをロックしたり、デバイスからすべての仕事用データを削除したりするコマンドを送信できます。
デバイスでインストールされるソフトウェア更新を制御します。	デバイス SR 要件プロファイルを使用して、デバイスにデバイスソフトウェア更新をインストールする方法を制御します。
アプリと設定の更新のためにデバイスが UEM に接続する方法を設定します。	Enterprise Management Agent プロファイルを使用して、デバイスがアプリまたは設定の更新のためにどのように UEM に接続するかを設定します。
デバイスで組織情報を表示します。	組織通知とデバイスプロファイルを使用して、デバイスで組織情報を表示します。

タスク	説明
デバイスで位置情報サービスを使用します。	位置情報サービスプロファイルを使用して、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します。
iOS デバイスのアクティベーションロックの有効化。	iOS デバイスのアクティベーションロック機能を使用して、ユーザーは、デバイスの紛失や盗難の場合に、デバイスを保護することができます。この機能が有効になっている場合、ユーザーは、［マイ iPhone を検索］を無効にするか、デバイスを消去するか、デバイスを再アクティブ化して使用するときに、Apple ID とパスワードを確認する必要があります。
カスタムペイロードプロファイルにより iOS 機能を管理します。	カスタムペイロードプロファイルを使用して、既存の UEM ポリシーまたはプロファイルで制御されていない iOS デバイスの機能を制御します。
Android デバイスの工場出荷時のリセット保護を管理します。	工場出荷時にリセットされた保護プロファイルを使用して、組織の Android Enterprise および Android Management デバイスの工場出荷時のリセット保護機能を制御します。
デバイスの認証を設定します。	チャレンジを送信して、Samsung Knox、Android、iOS および Windows 10 デバイスの完全性と整合性をテストします。
Windows 10 デバイス向けの Windows Information Protection の設定。	Windows 情報保護プロファイルを使用して、Windows 10 デバイス上の仕事用データを保護および管理します。
iOS または macOS デバイスの強化されたチャネルへの移行。	iOS または macOS デバイスをアクティブ化すると、デフォルトでデバイスは強化されたデータチャネルに割り当てられます。現在強化されたデータチャネルを使用していない iOS または macOS デバイスがある場合は、これらのデバイスのリストをエクスポートし、デバイスを強化されたチャネルに移動するためのアクションを実行できます。

デバイス機能を管理するためのプロファイルの使用

BlackBerry UEM は、iOS、macOS、Android、および Windows デバイスのさまざまなデバイス機能を管理するために、さまざまなタイプのプロファイルを使用します。組織のニーズに合わせてプロファイルを設定し、ユーザーアカウント、ユーザーグループ、およびデバイスグループに割り当てて、その設定をデバイスに適用します。

利用可能なプロファイルの完全なリストについては、「BlackBerry UEM プロファイル」を参照してください。

プロファイルはランク付けまたはランク付け解除できます。ランク付けされたプロファイルの場合、UEM はそのタイプのプロファイルを 1 つのデバイス（たとえば、1 つのコンプライアンスプロファイル）に割り当てます。ランク付けされたプロファイルがユーザーに直接割り当てられている場合は、そのユーザーが属するユーザーグループに割り当てられているそのタイプのどのプロファイルよりも優先されます。ユーザーが、そのタイプの異なるプロファイルが割り当てられている複数のユーザーグループに属している場合、どのプロファイルを割り当てるかを決定するためにランク付けが使用されます。ユーザーのデバイスがデバイスグループに属している場合、そのデバイスグループに割り当てられたプロファイルは、そのユーザーに直接割り当てられている同じタイプのプロファイルより優先されます。デバイスが、そのタイプの異なるプロファイルを持つ複数のデバイスグループに属している場合は、どのプロファイルを割り当てるかを決定するためにランク付けが使用されます。

ランク付けされていないプロファイルの場合、そのタイプの複数のプロファイルを、ユーザーアカウントへの直接割り当てから、またはグループ割り当てを介してデバイスに割り当てることができます（たとえば、デバイスに複数の Wi-Fi プロファイルを割り当てることができます）。

特定のプロファイルタイプでは、プロファイルをデバイスに割り当てる必要があります。プロファイルがユーザーに直接割り当てられていない場合、またはグループメンバーシップを介して 割り当てられていない場合、UEM は事前設定されたデフォルトプロファイルを割り当てます。UEM には、デフォルトのアクティベーションプロファイル、デフォルトのコンプライアンスプロファイル、デフォルトのエンタープライズ接続プロファイル、デフォルトの Enterprise Management Agent プロファイルが含まれています。

BlackBerry UEM プロファイル

プロファイル名	説明	サポートされるデバイスタイプ	ランク付け済みまたは未ランク付け	詳細について
ポリシー				
Knox Service Plugin	Knox Service Plugin をセットアップおよび設定します。	Android	ランク付け済み	OEM アプリの設定での Android デバイスの管理

プロファイル名	説明	サポートされるデバイスタイプ	ランク付け済みまたは未ランク付け	詳細について
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を設定します。	すべてのデバイス	ランク付け済み	アクティベーションプロファイルの作成
BlackBerry Dynamics	ユーザーに対して BlackBerry Dynamics を有効にし、アプリアクセス、データ保護、およびロギングの標準を設定します。	すべてのデバイス	ランク付け済み	デバイスでの BlackBerry Dynamics の制御
アプリロックモード	指定したアプリのみを実行するようにデバイスを設定します。	監視対象の iOS デバイス MDM でアクティブ化された Samsung Knox デバイス Windows 10 Education および Windows 10 Enterprise デバイス	ランク付け済み	デバイスで実行できるアプリの制限
エンタープライズ管理エージェント	アプリまたは設定の更新のためにデバイスが UEM に接続する方法を設定します。	iOS Android Windows	ランク付け済み	アプリと設定の更新のためにデバイスが BlackBerry UEM に接続する方法の設定
共有 iPad	複数のユーザーが共有できるように iPad デバイスを設定します。	iOS	ランク付け済み	共有 iPad グループの作成と管理
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。	すべてのデバイス	ランク付け済み	デバイスのコンプライアンスルールの強制

プロファイル名	説明	サポートされるデバイスタイプ	ランク付け済みまたは未ランク付け	詳細について
コンプライアンス（BlackBerry Dynamics）	これは、Good Control からオンプレミス UEM 環境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。	すべてのデバイス	該当なし	該当なし
デバイス SR 要件	デバイスにインストールする必要があるソフトウェアリリースバージョンを設定します。	Android	ランク付け済み	デバイスでインストールされるソフトウェア更新の制御
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、メールやカレンダーエントリ、オーガナイザデータを同期する方法を設定します。	すべてのデバイス	ランク付け済み	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設定します。	すべてのデバイス	未ランク付け	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。	すべてのデバイス	ランク付け済み	ゲートキーピングプロファイルの作成
CalDAV	デバイスがカレンダ情報の同期に使用するサーバー設定を指定します。	iOS macOS	未ランク付け	CardDAV および CalDAV プロファイルの設定
CardDAV	デバイスが連絡先情報の同期に使用するサーバー設定を指定します。	iOS macOS	未ランク付け	CardDAV および CalDAV プロファイルの設定
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接続方法を設定します。	すべてのデバイス	未ランク付け	デバイスの仕事用 Wi-Fi ネットワークの設定
VPN	仕事用 VPN へのデバイスの接続方法を設定します。	すべてのデバイス	未ランク付け	デバイスの仕事用 VPN の設定

プロファイル名	説明	サポートされるデバイスタイプ	ランク付け済みまたは未ランク付け	詳細について
DNS	デバイスが特定のドメインへのアクセスに使用する DNS サーバーを指定します。	iOS macOS	ランク付け済み	iOS および macOS デバイス用の DNS サーバーの指定
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設定します。	iOS macOS Android	ランク付け済み	デバイスのプロキシプロファイルのセットアップ
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を組織のリソースに接続する方法と、デバイスが BlackBerry Secure Connect Plus を使用できるかどうかを設定します。	iOS Android	ランク付け済み	仕事用リソースへの接続のための BlackBerry Secure Connect Plus の使用
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設定します。	すべてのデバイス	ランク付け済み	BlackBerry Dynamics アプリのネットワーク接続の設定
BlackBerry 2FA	ユーザーのツーファクタ認証を有効にし、事前認証および自己回復機能を設定します。	iOS Android	ランク付け済み	BlackBerry 2FA プロファイルの作成
ネットワーク使用	iOS デバイスの仕事用アプリで、モバイルネットワークやデータローミングを使用できるかどうかを設定します。	iOS	ランク付け済み	iOS デバイスでのアプリのネットワーク使用の制御
Web コンテンツフィルター	ユーザーが監視対象の iOS デバイスで表示できる Web サイトを制限します。	監視対象の iOS デバイス	未ランク付け	iOS デバイスでの Web コンテンツフィルタープロファイルの作成
シングルサインオン拡張	iOS デバイスを有効にして、組織のネットワーク内のドメインおよび Web サービスで自動的に認証します。	iOS	未ランク付け	iOS デバイスの自動認証の有効化

プロファイル名	説明	サポートされるデバイスタイプ	ランク付け済みまたは未ランク付け	詳細について
管理対象ドメイン	信頼済みドメイン外でのメール送信についてユーザーに通知し、内部ドメインからダウンロードしたドキュメントを開けるアプリを制限するように iOS デバイスを設定します。	iOS	未ランク付け	iOS デバイスのメールドメインと Web ドメインの指定
AirPrint	ユーザーの AirPrint プリンタリストにプリンタを追加します。	iOS	未ランク付け	iOS デバイス対応の AirPrint プロファイルの作成
AirPlay	デバイスをユーザーの AirPlay デバイスリストに追加します。	iOS	未ランク付け	iOS デバイス対応の AirPlay プロファイルの作成
アクセスポイント名	通信事業者への接続に使用するデバイスの APN を指定します。	Android	未ランク付け	Android デバイス用のアクセスポイント名プロファイルの作成
保護				
Windows Information Protection	Windows 10 で Windows Information Protection 設定を構成します。	Windows 10	ランク付け済み	Windows 10 デバイスの Windows 情報保護のセットアップ
Microsoft Intune アプリの保護	Office 365 アプリ内のデータを保護する方法を設定します。	iOS Android	未ランク付け	Microsoft Intune で保護されているアプリの管理
位置情報サービス	デバイスの位置を要求し、地図上でのデバイスのおおよその位置を表示します。	iOS Android Windows	ランク付け済み	デバイスで位置情報サービスを使用する
サイレント	オフの期間中は BlackBerry Work 通知をブロックします。	iOS Android	ランク付け済み	BlackBerry Work からの就業時間外の通知のオフ
工場出荷時のリセット保護	Android デバイスの工場出荷時のリセット保護機能を制御します。	Android	ランク付け済み	Android Enterprise および Android Management デバイスの工場出荷時リセット保護の管理

プロファイル名	説明	サポートされるデバイスタイプ	ランク付け済みまたは未ランク付け	詳細について
CylancePROTECT	CylancePROTECT Mobile for BlackBerry UEM のセキュリティ機能を設定します。	iOS Android	ランク付け済み	BlackBerry UEM 用 CylancePROTECT Mobile
カスタム				
デバイス	デバイスで表示する情報をを指定します。	iOS Android Windows	ランク付け済み	デバイスでの組織情報の表示
ホーム画面のレイアウト	iOS デバイスでのアプリのレイアウトを設定します。	iOS	ランク付け済み	iOS デバイスでのアプリのレイアウトの設定
カスタムペイロード	ペイロードコードを使用してカスタムデバイス設定情報を指定します。	iOS	未ランク付け	カスタムペイロードプロファイルによる iOS 機能の管理
アプリごとの通知	システムアプリと UEM により管理するアプリの通知を設定します。	監視対象の iOS デバイス	ランク付け済み	監視対象の iOS デバイスでのアプリ通知の管理
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。	すべてのデバイス	未ランク付け	デバイスおよびアプリへの CA 証明書の送信
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。	iOS macOS Android	未ランク付け	複数のデバイスへの同じクライアント証明書の送信
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。	iOS macOS Android	未ランク付け	ユーザー資格情報プロファイルを使用したデバイスおよびアプリへのクライアント証明書の送信

プロファイル名	説明	サポートされるデバイスタイプ	ランク付け済みまたは未ランク付け	詳細について
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。	すべてのデバイス	未ランク付け	SCEP を使用したデバイスおよびアプリへのクライアント証明書の送信
OCSP	デバイスで S/MIME 証明書のステータスをチェックできるようにします。	iOS Android	ランク付け済み	デバイスでの S/MIME 証明書のステータスの判別
CRL	S/MIME 証明書のステータスを検索するように UEM を設定します。	iOS Android	ランク付け済み	デバイスでの S/MIME 証明書のステータスの判別
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。	Android	ランク付け済み	証明書マッピングプロファイルの使用によるアプリが使用する証明書の指定

プロファイルの管理

1. 管理コンソールのメニューバーで、［ポリシーとプロファイル］をクリックします。
2. 適切なプロファイルの種類をクリックします。
3. 次の操作のいずれかを実行します。

タスク	手順
プロファイルをコピーします。	a. コピーするプロファイルの名前をクリックします。 b. をクリックします。 c. プロファイルの名前と説明を入力します。 d. プロファイルに適切な値を設定します。各タイプのプロファイルの詳細については、「BlackBerry UEM プロファイル」を参照してください。 e. ［保存］をクリックします。 f. プロファイルをユーザーおよびグループに割り当てます。
プロファイルを変更します。	a. 変更するプロファイルの名前をクリックします。 b. をクリックします。 c. プロファイルに変更を加えます。 d. ［保存］をクリックします。

タスク	手順
プロファイルをランク付けします。	**a.** をクリックします。 **b.** 矢印を使用して、ランキングでプロファイルを上下に移動します。 **c.** ［保存］をクリックします。
ユーザーアカウントからプロファイルを削除します。	**a.** 削除するプロファイルの名前をクリックします。 **b.** ［**x** ユーザーに割り当て済み］タブで、プロファイルを削除するユーザーアカウントを検索して選択します。 **c.** をクリックします。
グループからプロファイルを削除します。	**a.** 削除するプロファイルの名前をクリックします。 **b.** ［**x** グループに割り当て済み］タブで、プロファイルを削除するグループを検索して選択します。 **c.** をクリックします。
プロファイルを削除します。	デフォルトプロファイルは削除できません。カスタムプロファイルを削除すると、UEM により、それが割り当てられているユーザーとデバイスからプロファイルが削除されます。 **a.** 削除するプロファイルを選択します。 **b.** をクリックします。 **c.** ［削除］をクリックします。

プロファイル、メール、通知での変数の使用

BlackBerry UEM は、プロファイル、コンプライアンス通知、アクティベーションメール、およびイベント通知で使用できるデフォルト変数とカスタム変数をサポートしており、個々のユーザーの設定とメッセージをカスタマイズできます。デフォルト変数は、標準アカウント属性（たとえば、ユーザー名、メール）とその他の事前定義された属性（たとえば、デバイスのアクティベーションに使用されるサーバーアドレス）を表します。カスタム変数を使用して、追加の属性を定義できます。

変数は、［名前］および［説明］フィールドを除くプロファイルの任意のテキストフィールドで使用できます。たとえば、メールプロファイルの［メールアドレス］フィールドに「%UserName%@example.com」を指定できます。

管理コンソールで使用できるデフォルト変数のリストは、［設定］>［一般設定］>［デフォルト変数］で表示できます。

IT ポリシーと BlackBerry Dynamics アプリ設定では、変数の使用はサポートされていないことに注意してください。

カスタム変数の定義

パスワードなどの機密情報を表すために、最大 5 つのカスタムテキスト変数と最大 5 つのマスクされたテキスト変数を定義できます。カスタム変数を定義する場合は、変数のラベル（VPN パスワードなど）を指定します。ユーザーアカウントを作成または更新する場合に、ラベルは［カスタム変数］セクションのフィールド名として使用され、そのユーザーに適切な値を指定できます。管理者アカウントを含め、すべてのユーザーアカウントがカスタム変数をサポートしています。カスタム変数をデフォルト変数と同様に使用できます。

1. 管理コンソールのメニューバーで、［設定］>［一般設定］>［カスタム変数］をクリックします。
2. ［ユーザーを追加または編集するときにカスタム変数を表示する］チェックボックスをオンにします。
3. 使用する各カスタム変数のラベルを指定します。
4. ［保存］をクリックします。

ユーザーにメッセージを送信するためのメールテンプレートの使用

メールテンプレートを使用して、BlackBerry UEM デバイスの有効化の手順の提供、コンプライアンスの問題に関するユーザーへの通知、BlackBerry Dynamics アプリのアクセスキーの提供など、さまざまな理由でユーザーに送信するメールメッセージをカスタマイズおよびパーソナライズできます。

ユーザー名、メールアドレス、アクティベーションパスワードなどの項目に変数を使用してメールメッセージをパーソナライズしたり、さまざまなフォント、色、画像を使用してメッセージの外観をカスタマイズしたりできます。さまざまなデバイスタイプまたはアクティベーションタイプに対して、複数のテンプレートを作成して利用できます。デフォルトのメールテンプレートを編集するか、新しいテンプレートを作成することができます。

管理コンソールでさまざまなタスク（ユーザーの追加、コンプライアンスプロファイルの作成など）を実行する場合は、デバイスユーザーにメッセージを送信するために UEM が使用するメールテンプレートを選択できます。

使用可能なデフォルトテンプレートは、管理コンソールの［設定］>［一般設定］>［テンプレート］で表示できます。

メールテンプレートの編集

デフォルトのメールテンプレートを変更する場合は、後で元のテンプレートテキストを復元する場合に備えて、元のテンプレートテキストのバックアップを保存することをお勧めします。

1. 管理コンソールのメニューバーで、［設定］**>**［一般設定］**>**［テンプレート］をクリックします。
2. 編集するテンプレートをクリックします。
3. 必要に応じて、［名前］、［件名］、または［メッセージ］フィールドを編集します。
4. ［保存］をクリックします。

アクティベーションメールテンプレートを作成

1. 管理コンソールのメニューバーで、［設定］**>**［一般設定］**>**［テンプレート］をクリックします。
2. ＋>［デバイスのアクティベーション］を選択します。
3. ［名前］フィールドに、テンプレートの名前を入力します。
4. ［件名］フィールドに、アクティベーションメールの件名行を入力します。
5. ［メッセージ］フィールドに、アクティベーションメールの本文を入力します。

   書式設定のカスタマイズ、画像（企業ロゴなど）の挿入などに、HTML エディターを使用します。メールの一部をパーソナライズするための変数を挿入できます。『プロファイル、メール、通知での変数の使用』を参照してください。
6. アクティベーションパスワードではなく、ユーザーが QR Code を使用してデバイスをアクティブにする場合は、［**iOS** および **Android** デバイスのアクティブ化の場合 **QR** コードをメールメッセージに追加する］チェックボックスをオンにします。
7. アクティベーションパスワードまたは QR Code をアクティベーション手順とは別に送信するには、［**2** つのアクティベーションメールを別々に送信 **- 1** 番目は詳細な手順、**2** 番目はパスワード］を選択し、2 番目のア

クティベーションメールのコンテンツとオプションを指定します。アクティベーションメールを 1 通のみ送信する場合は、アクティベーションパスワード、アクティベーションパスワード変数、または QR Code が最初のメールに含まれていることを確認してください。

8. ［保存］をクリックします。

デバイスのアクティベーションの詳細は、「デバイスのアクティベーション」を参照してください。

コンプライアンス通知用のテンプレートの作成

ユーザーのデバイスが、割り当てられたコンプライアンスプロファイルで設定した要件に準拠していない場合、BlackBerry UEM は指定したテンプレートに基づいてユーザーにカスタマイズされたメールメッセージを送信できます。UEM には、編集可能で削除ができないデフォルトのコンプライアンス違反メールテンプレートが含まれています。ユーザーアカウントに別のテンプレートを割り当てない場合、UEM はデフォルトのテンプレートを使用します。

1. 管理コンソールのメニューバーで、［設定］ > ［一般設定］ > ［テンプレート］をクリックします。
2. ＋ > ［コンプライアンス違反］をクリックします。
3. ［名前］フィールドに、テンプレートの名前を入力します。
4. ［件名］フィールドに、メッセージの件名を入力します。
5. ［メッセージ］フィールドに、コンプライアンスメールの本文を入力します。

   書式設定のカスタマイズ、画像（企業ロゴなど）の挿入などに、HTML エディターを使用します。メールの一部をパーソナライズするための変数を挿入できます。『プロファイル、メール、通知での変数の使用』を参照してください。
6. ［保存］をクリックします。

デバイスコンプライアンスの詳細については、「デバイスのコンプライアンスルールの強制」を参照してください。

イベント通知メールテンプレートの作成

組織の UEM 環境で特定のイベントが発生したときに、BlackBerry UEM を使用して管理者にカスタムメッセージを送信できるイベント通知メールテンプレートを作成できます。

1. 管理コンソールのメニューバーで、［設定］ > ［一般設定］ > ［テンプレート］をクリックします。
2. ＋ > ［イベント通知］をクリックします。
3. ［名前］フィールドに、テンプレートの名前を入力します。
4. ［件名］フィールドに、メッセージの件名を入力します。イベントタイプを件名に追加する場合は、［メールの件名にイベントタイプを追加する］チェックボックスをオンにします。
5. ［メッセージ］フィールドに、イベント通知メールの本文を入力します。

   書式設定のカスタマイズ、画像（企業ロゴなど）の挿入などに、HTML エディターを使用します。メールの一部をパーソナライズするための変数を挿入できます。『プロファイル、メール、通知での変数の使用』を参照してください。
6. ［保存］をクリックします。

イベント通知の詳細については、「イベント通知の作成」を参照してください。

提案されるテンプレートテキスト

以下で提案されるテキストは、デフォルトのメールテンプレートで使用します。デフォルトのメールテンプレートを編集して後からデフォルトのテキストを使用する場合は、ここからコピーして貼り付けることができます。

名前	提案されるテキスト
Android 仕事用プロファイルのアクティベーションコード	件名：**Android** 仕事用プロファイルのアクティベーションコードが作成されました %UserDisplayName% 様 仕事用プロファイルのみを含む Android デバイスをアクティブ化するために、管理者が Android 仕事用プロファイルのアクティベーションコードを作成しました。BlackBerry UEM アクティベーションパスワードは、別のメールメッセージで受信します。 Android 仕事用プロファイルのアクティベーションコード：%GoogleActivationCode% Android 仕事用プロファイルのアクティベーションコードは、%ActivationPasswordExpiry% に期限切れになります。 不明な点がある場合は、管理者に問い合わせてください。
デフォルトの管理対象 Google アカウント認証情報	件名：**Google** アカウントが作成されました %UserDisplayName% 様 デバイス上で仕事用プロファイルを有効にするために、管理者が Google アカウントを作成しました。仕事用プロファイルをアクティブ化するときには、Google アカウントのパスワードが必要です。ここで表示された Google アカウントのパスワードは、BlackBerry UEM でデバイスをアクティベートするときに使用するパスワードではありません。BlackBerry UEM アクティベーションパスワードは、別のメールメッセージで受信することも、BlackBerry UEM Self-Service で BlackBerry UEM 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。 仕事用プロファイルをアクティブ化するときに、次の情報が必要になります。 • 仕事用メールアドレス：%UserEmailAddress% • Google アカウントパスワード：%Password% Google アカウントは、https://myaccount.google.com で管理できます。Google アカウントのパスワードを変更した場合は、このメールに含まれているパスワードは適用されなくなり、代わりに新しいパスワードを使用する必要があります。 この情報は大切に保管してください。 不明な点がある場合は、管理者に問い合わせてください。

名前	提案されるテキスト
Apple DEP デバイスアクティベーションメール 最初のメール	件名：**BlackBerry UEM** でのデバイスのアクティブ化 %UserDisplayName% 様 管理者は、お使いの iOS デバイスを BlackBerry UEM 用に有効化しました。デバイスをアクティブ化するには、次の情報が必要です。 • 仕事用メールアドレス：%UserEmailAddress% • デバイスアクティベーションパスワード：アクティベーションパスワード は、別のメールで通知されます。 自身のデバイスは、%UserSelfServicePortalURL% にある BlackBerry UEM Self-Service で管理できます。ログインの際に、次のユーザー名を使用します。 BlackBerry UEM Self-Service ユーザー名：%UserName% BlackBerry UEM Self-Service パスワードは、別のメールで通知された可能性があります。 受信していない場合は、管理者に問い合わせてください この情報は大切に保管してください。 不明な点がある場合は、管理者に問い合わせてください。
Apple DEP デバイスアクティベーションメール 2 番目のメール	件名：**BlackBerry UEM** でデバイスをアクティブ化するパスワード %UserDisplayName% 様 管理者は、お使いのデバイスを BlackBerry UEM 用に有効化しました。デバイスをアクティブ化するには、次の情報が必要です。 デバイスのアクティベーションパスワード：%ActivationPassword% パスワードの有効期限は %ActivationPasswordExpiry% です。 BlackBerry UEM でお使いの iOS デバイスをアクティブ化するには、「BlackBerry UEM でのデバイスのアクティブ化」のメールに記された手順に従ってください。 不明な点がある場合は、管理者に問い合わせてください。 BlackBerry UEM へようこそ！

名前	提案されるテキスト
BlackBerry Dynamics アクセスキーのメール	件名：**BlackBerry Dynamics** アプリのアクセスキーが作成されました %UserDisplayName% 様 管理者は BlackBerry Dynamics アプリのアクセスキーを作成しました。このメールには、アクセスキーと、アプリを設定する手順が記載されています。 複数のアプリを使用する権限が与えられている場合は、複数のメールを受信します。メールには、アプリの設定に使用できるアクセスキーが記されています。アプリの設定にはお使いのどのアクセスキーでも使用できますが、各アクセスキーは一度しか使用できません。 開始する前に、モバイルデータまたは Wi-Fi 通信可能範囲を保有していることを確認してください。 1. BlackBerry Dynamics アプリを開きます。 2. プロンプトが表示されたら、次の情報を入力します。 • メールアドレス：%UserEmailAddress% • アクセスキー：%AccessKeys% アクセスキーは、%AccessKeyExpiry% に期限切れになります。 3. パスワードの作成を求めるプロンプトが表示されることがあります。アプリを開くときに、このパスワードを入力する必要があります。 不明な点がある場合は、管理者に問い合わせてください。

名前	提案されるテキスト
デフォルトのアクティベーションメール 最初のメール	件名：**BlackBerry UEM** でのデバイスのアクティブ化 %UserDisplayName% 様 管理者は、お使いのデバイスを BlackBerry UEM 用に有効化しました。以下の情報の一部またはすべてを必要とするデバイスをアクティブ化するには： • 仕事用メールアドレス：%UserEmailAddress% • サーバー名：%ActivationURL% • アクティベーションユーザー名：%ActivationUserName% • デバイスアクティベーションパスワード：アクティベーションパスワード は、別のメールで通知されます。 Android デバイス： Android デバイスを使用している場合、BlackBerry UEM Client は Google Play からインストールする必要があります。 iOS デバイス： iOS デバイスを使用している場合、BlackBerry UEM Client は App Store からインストールする必要があります。 iOS デバイスでは、Safari を開いて workspace://apps に移動し、管理者から割り当てられたアプリをインストールします。利用可能な場合は、デバイスで Work Apps をタップすることもできます。 macOS デバイス： macOS デバイスを使用している場合、BlackBerry UEM Self-Service を使用してデバイスをアクティブ化する必要があります。 Windows 10 以降を実行しているデバイスの場合： デバイスをアクティブ化するには、次の情報が必要です。 • サーバー名：%ClientlessActivationURL% • 証明書サーバー URL：%RsaRootCaCertUrl% • RSA 証明書をインストールする必要があります。デバイスのブラウザーのアドレスバーに証明書サーバー URL を入力します。指示に従って、［信頼済みルート証明書機関］フォルダーに証明書をインストールします。 • デバイスで、［設定］>［アカウント］>［仕事または学校にアクセス］に移動し、［デバイス管理のみに登録］をタップします。 デバイスを管理するには、次の手順を実行します。 自身のデバイスは、%UserSelfServicePortalURL% にある BlackBerry UEM Self-Service で管理できます。ログインの際に、次のユーザー名を使用します。 BlackBerry UEM Self-Service ユーザー名：%UserName% BlackBerry UEM Self-Service パスワードは、別のメールで通知された可能性があります。 BlackBerry UEM へようこそ！

名前	提案されるテキスト
デフォルトのアクティベーションメール 2 番目のメール	件名：**BlackBerry UEM** でデバイスをアクティブ化するパスワード %UserDisplayName% 様 管理者は、お使いのデバイスを BlackBerry UEM 用に有効化しました。デバイスをアクティブ化するには、次の情報が必要です。 • デバイスのアクティベーションパスワード：%ActivationPassword% • パスワードの有効期限は %ActivationPasswordExpiry% です。 BlackBerry UEM でお使いの iOS、Android、または Windows デバイスをアクティブ化するには、「BlackBerry UEM でのデバイスのアクティブ化」のメールに記された手順に従ってください。 不明な点がある場合は、管理者に問い合わせてください。 BlackBerry UEM へようこそ！
デフォルトの Android Management アクティベーションメール	件名：**BlackBerry UEM** でのデバイスのアクティブ化 %UserDisplayName% 様 管理者がデバイスで Android Management を有効にしたため、仕事用プロファイルを作成できます。仕事用プロファイルを作成するには、デバイスから %ActivationAndroidManagementURL% のリンクをクリックします。 デバイスで QR コードをスキャンすることもできます。［設定］>［Google サービス］>［設定と復元］>［仕事用プロファイルを設定］の順に進み、次の QR コードをスキャンします。 アクティベーションリンクと QR コードは、%ActivationPasswordExpiry% に期限切れになります %ActivationAndroidManagementQRCode% この情報は大切に保管してください。 不明な点がある場合は、管理者に問い合わせてください。
デフォルトのコンプライアンスメール	件名：非準拠デバイスの通知 デバイスは組織のポリシーに準拠していません。この状態が続く場合は、管理者がデバイスから組織のデータへのアクセスを制限したり、デバイス上の組織のデータを削除したり、デバイスからすべてのコンテンツと設定を削除したりしている可能性があります。

名前	提案されるテキスト
デフォルトの仕事用領域専用（Android Enterprise）アクティベーションメール 最初のメール	件名：**BlackBerry UEM** でのデバイスのアクティブ化 %UserDisplayName% 様 管理者は、BlackBerry UEM に対してお使いの Android デバイス（9.0 以降）を有効にしました。デバイスをアクティベーションするには、次の情報が必要です。 • アクティベーションユーザー名：%ActivationUserName% • デバイスアクティベーションパスワード：アクティベーションパスワード は、別のメールで通知されます。 デバイスをアクティブ化するには、次の操作を実行します。 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. デバイスの設定中、［アカウントを追加］画面で Google アカウント認証情報を入力します。デバイスが一部の重要なシステムアプリを更新して UEM Client をダウンロードするまで待機します。 3. BlackBerry UEM Client で、画面の指示に従ってデバイスをアクティブ化します。 自身のデバイスは、%UserSelfServicePortalURL% にある BlackBerry UEM Self-Service で管理できます。ログインの際に、次のユーザー名を使用します。 BlackBerry UEM Self-Service ユーザー名：%UserName% BlackBerry UEM Self-Service パスワードは、別のメールで通知された可能性があります。 受信していない場合は、管理者に問い合わせてください この情報は大切に保管してください。 不明な点がある場合は、管理者に問い合わせてください。 BlackBerry UEM へようこそ！
デフォルトの仕事用領域専用（Android 仕事用プロファイル）アクティベーションメール 2 番目のメール	件名：**BlackBerry UEM** でデバイスをアクティブ化するパスワード %UserDisplayName% 様 管理者は、お使いの Android デバイスを BlackBerry UEM 用に有効化しました。デバイスをアクティブ化するには、次の情報が必要です。 • デバイスのアクティベーションパスワード：%ActivationPassword% • パスワードの有効期限は %ActivationPasswordExpiry% です。 BlackBerry UEM でお使いのデバイスをアクティブ化するには、「BlackBerry UEM でのデバイスのアクティブ化」のメールに記された手順に従ってください。 不明な点がある場合は、管理者に問い合わせてください。 BlackBerry UEM へようこそ！

名前	提案されるテキスト
BlackBerry UEM イベント通知メール	件名：**BlackBerry UEM** イベント通知 次のイベントが発生しました。 %AllEventVariables%
デバイスアクティブ化通知	件名：**BlackBerry UEM** でアクティブ化されたデバイス %UserDisplayName% 様 デバイスが BlackBerry UEM でアクティブ化されています。 デバイス情報 モデル：%DeviceModel% シリアル番号：%SerialNumber% IMEI：%DeviceIMEI% このデバイスをアクティブ化しなかった場合は、管理者に連絡してください。 件名：**BlackBerry UEM** でアクティブ化された **BlackBerry Dynamics** デバイス %UserDisplayName% 様 BlackBerry Dynamics デバイスが BlackBerry UEM でアクティブ化されています。 このデバイスをアクティブ化しなかった場合は、管理者に連絡してください。
セルフサービスログイン通知	件名：セルフサービスログイン通知 %UserDisplayName% 様 BlackBerry UEM Self-Service にログインしています。 IP アドレス：%IPAddress% 時間：%Timestamp% ログインしなかった場合は、管理者に連絡してください。

IT ポリシーによるデバイスの管理

IT ポリシーを使用して、組織の BlackBerry UEM 環境でデバイスのセキュリティと動作を管理できます。IT ポリシーは、デバイスの機能を制御するために使用できる一連のルールです。たとえば、IT ポリシールールを使用して、パスワード要件の適用、特定のデバイス機能（カメラなど）の使用禁止、特定のアプリの可用性の制御を行うことができます。

同一の IT ポリシーで、すべてのデバイスタイプのルールを設定できます。デバイス OS は、IT ポリシールールを使用して制御できる機能を決定します。デバイスアクティベーションタイプは、特定のデバイスに適用されるルールと、ルールを使用してデバイス全体または仕事用領域のみを制御できるかどうかを決定します。デバイスは、適用できない IT ポリシールールを無視します。

IT ポリシールールスプレッドシートをダウンロードして、UEM がサポートする各デバイスタイプで使用可能なすべての IT ポリシールールを包括的に参照できます。

UEM には、デフォルトの IT ポリシーと、デバイスタイプごとの事前設定済みのルールが含まれます。組織のニーズに合わせて、デフォルトの IT ポリシーを変更できます。IT ポリシーがユーザーアカウント、ユーザーが属するユーザーグループ、またはユーザーのデバイスが属するデバイスグループに割り当てられていない場合、UEM はデフォルトの IT ポリシーをユーザーのデバイスに送信します。ユーザーがデバイスをアクティブ化した場合、ユーザーが割り当てられた IT ポリシーを更新した場合、または異なる IT ポリシーがユーザーアカウントかデバイスに割り当てられた場合に、UEM は IT ポリシーをデバイスに送信します。

UEM は、デバイスに1つの IT ポリシーのみを割り当て、事前定義されたルールを使用して、割り当てる IT ポリシーを決定します。ユーザーに直接割り当てられた IT ポリシーは、ユーザーグループメンバーシップを介して割り当てられた IT ポリシーより優先されます。ユーザーが、IT ポリシーが異なる複数のユーザーグループのメンバである場合、どの IT ポリシーを割り当てるかを決定するために、ランク付けが使用されます。ユーザーのデバイスがデバイスグループに属している場合、デバイスグループに割り当てられている IT ポリシーは、ユーザーに直接割り当てられている IT ポリシーよりも優先されます。デバイスが、IT ポリシーが異なる複数のデバイスグループに属している場合は、どの IT ポリシーを割り当てるかを決定するためにランク付けが使用されます。

IT ポリシーの管理

デフォルトの IT ポリシーを変更したり、カスタム IT ポリシーを作成して割り当てたりすることができます。

1. 管理コンソールのメニューバーで、［ポリシーとプロファイル］ > ［ポリシー］ > ［**IT** ポリシー］をクリックします。
2. 次の操作のいずれかを実行します。

タスク	手順
IT ポリシーを作成します。	**a.** ＋をクリックします。 **b.** IT ポリシーの名前と説明を入力します。 **c.** 各デバイスタイプのタブをクリックして、IT ポリシールールの適切な値を設定します。IT ポリシールールの詳細については、「IT ポリシールールのスプレッドシート」を参照してください。 **d.** ［保存］をクリックします。 **e.** IT ポリシーをユーザーおよびグループに割り当てます。

タスク	手順
IT ポリシーをコピーします。	**a.** コピーする IT ポリシーの名前をクリックします。 **b.** をクリックします。 **c.** IT ポリシーの名前と説明を入力します。 **d.** 各デバイスタイプのタブをクリックして、IT ポリシールールの適切な値を設定します。IT ポリシールールの詳細については、「IT ポリシールールのスプレッドシート」を参照してください。 **e.** ［保存］をクリックします。 **f.** IT ポリシーをユーザーおよびグループに割り当てます。
IT ポリシーを変更します。	**a.** 変更する IT ポリシーの名前をクリックします。 **b.** をクリックします。 **c.** 各デバイスタイプの適切なタブで変更を加えます。 **d.** ［保存］をクリックします。
IT ポリシーをランク付けします。	**a.** をクリックします。 **b.** 矢印を使用して、IT ポリシーを上下に移動してランク付けします。 **c.** ［保存］をクリックします。
ユーザーアカウントから IT ポリシーを削除します。	**a.** 削除する IT ポリシーの名前をクリックします。 **b.** ［**x** ユーザーに割り当て済み］タブで、IT ポリシーを削除するユーザーアカウントを検索して選択します。 **c.** をクリックします。
グループから IT ポリシーを削除します。	**a.** 削除する IT ポリシーの名前をクリックします。 **b.** ［**x** グループに割り当て済み］タブで、IT ポリシーを削除するグループを検索して選択します。 **c.** をクリックします。
IT ポリシーを削除します。	デフォルトの IT ポリシーは削除できません。カスタム IT ポリシーを削除すると、UEM は、割り当てられていたユーザーとデバイスからその IT ポリシーを削除します。 **a.** 削除する IT ポリシーを選択します。 **b.** をクリックします。 **c.** ［削除］をクリックします。
IT ポリシーを .xml ファイルにエクスポートします。	**a.** エクスポートする IT ポリシーを選択します。 **b.** をクリックします。

IT ポリシーとデバイスメタデータの更新の手動インポート

BlackBerry は、IT ポリシーとデバイスメタデータの更新を BlackBerry UEM に定期的に送信します。たとえば、ベンダが新しいデバイスモデルをリリースした場合、BlackBerry は更新されたデバイスメタデータを UEM に送信して、アクティブ化プロファイルとコンプライアンスプロファイルに新しいデバイスモデルを含めることができます。ベンダが OS 更新をリリースすると、新しい IT ポリシーパックが UEM に送信され、新しい OS 機能を管理できるようになります。

デフォルトでは、UEM はこれらの更新を自動的に受信してインストールします。組織のセキュリティポリシーで自動更新が許可されていない場合に、オンプレミス UEM 環境がある場合、自動更新をオフにして、更新を手動でインポートできます。更新ファイルは累積されます。更新を行わなかった場合、次回の更新で、以前に更新されたすべての IT ポリシールールまたはデバイスメタデータがインストールされます。また、IT ポリシーとデバイスメタデータの更新がインストールされたときに管理者に通知するように、イベント通知を設定することもできます。

作業を始める前に： BlackBerry からの更新通知メールの指示に従って、メタデータまたは IT ポリシーパックをダウンロードします。

1. 管理コンソールのメニューバーで、［設定］ > ［インフラストラクチャ］ > ［設定データのインポート］をクリックします。
2. 次の操作のいずれかを実行します。
   - IT ポリシーパックの自動更新をオフにするには、［**IT** ポリシーパックデータを自動更新する］チェックボックスをオフにします。
   - デバイスメタデータの自動更新をオフにするには、［デバイスメタデータを自動更新する］チェックボックスをオフにします。
3. 適切な［参照］ボタンをクリックして、インポートするデータファイルに移動して選択します。［開く］をクリックします。

Android デバイス上で無効化された機能のデバイスサポートメッセージの作成

Android デバイスでは、機能が IT ポリシーによって無効になっているときにデバイスに表示されるサポートメッセージを作成できます。無効になっている機能の設定画面にメッセージが表示されます。サポートメッセージが作成されない場合、デバイスには OS のデフォルトのメッセージが表示されます。

1. 管理コンソールのメニューバーで、［設定］ > ［一般設定］ > ［カスタムデバイスサポートメッセージ］をクリックします。
2. ［デバイス言語］ドロップダウンリストで、通知を表示する言語を選択します。
3. ［無効機能通知］フィールドに、機能が無効になっているときにデバイスに表示するテキストを入力します。
4. 必要に応じて ［管理者サポートメッセージ］フィールドに、［デバイス管理者設定］画面に表示する通知を入力します。
5. 複数の言語でメッセージを作成する場合は、［追加の言語を追加］をクリックし、前の手順を繰り返します。
6. 複数の言語でメッセージを追加した場合は、指定した言語のいずれかを使用しないデバイスで使用する言語の［デフォルトの言語］ラジオボタンを選択します。
7. ［保存］をクリックします。

デバイスのコンプライアンスルールの強制

コンプライアンスプロファイルを使用して、デバイスの使用に関する組織の標準に準拠するようにユーザーに促すことができます。コンプライアンスプロファイルは、組織で許容できないデバイスの条件を定義します。たとえば、脱獄やルート化が行われたデバイス、またはオペレーティングシステムへの未許可アクセスに起因する整合性に関する通知が発行されたデバイスを許可しないように選択できます。

コンプライアンスプロファイルは、デバイスを非コンプライアンス状態にする条件、デバイスが非コンプライアンス状態であるときにユーザーが受け取る通知、およびコンプライアンスの問題が解決されない場合に BlackBerry UEM が実行するアクション（たとえば、組織のリソースへのユーザーのアクセスを制限する、デバイスから仕事用データを削除する、デバイスからすべてのデータを削除する）を指定します。

UEM には、デフォルトのコンプライアンスプロファイルが含まれます。デフォルトのコンプライアンスプロファイルは、コンプライアンス条件を強制しません。コンプライアンスルールを強制するために、デフォルトのコンプライアンスプロファイルの設定を変更するか、またはカスタムコンプライアンスプロファイルを作成して割り当てることができます。カスタムコンプライアンスプロファイルに割り当てられていないユーザーアカウントには、デフォルトのコンプライアンスプロファイルが割り当てられます。

Samsung Knox デバイスの場合、制限されたアプリのリストをコンプライアンスプロファイルに追加できますが、UEM はコンプライアンスルールを強制しません。その代わりに、制限付きアプリのリストがデバイスに送信され、これらのデバイスがコンプライアンスを強制します。制限付きアプリはインストールできず、またインストール済みの場合は無効になります。制限付きリストからアプリを削除すると、インストール済みアプリは再び有効になります。

BlackBerry Dynamics のコンプライアンスプロファイルは、Good Control と UEM を同期するときに Good Control からインポートされます。BlackBerry Dynamics コンプライアンスプロファイルは編集できませんが、UEM で新しいコンプライアンスプロファイルを作成するときに参照資料として利用できます。Good Control でコンプライアンスプロファイルに割り当てられたユーザーは、UEM と同期された後、同じプロファイルに割り当てられた状態に保たれます。ユーザーが BlackBerry Dynamics コンプライアンスプロファイルに割り当てられている場合、BlackBerry Dynamics のコンプライアンスプロファイルは、ユーザーに割り当てられる可能性がある UEM コンプライアンスプロファイルの BlackBerry Dynamics ルールよりも優先されます。

コンプライアンスプロファイルの作成

作業を始める前に：

- 特定のアプリを制限または許可するルールを定義する場合、これらのアプリを制限されたアプリリストに追加します。詳細については、「制限されたアプリリストへのアプリの追加」を参照してください。これは、監視対象の iOS デバイスの組み込みアプリには適用されません。組み込みアプリを制限するには、コンプライアンスプロファイルを作成し、プロファイル内の制限されたアプリリストにアプリを追加する必要があります。詳細については、「iOS および iPadOS：コンプライアンスプロファイル設定」を参照してください。
- デバイスが準拠していない場合にメール通知をユーザーに送信する場合は、デフォルトのコンプライアンスメールを編集するか、新しいコンプライアンスメールテンプレートを作成します。

メモ：脱獄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のルールを定義した場合、ユーザーは設定した強制アクションに関係なく、準拠していないデバイスの新しいアクティベーションを完了できなくなります。

1. 管理コンソールのメニューバーで、［ポリシーとプロファイル］ > ［コンプライアンス］ > ［コンプライアンス］をクリックします。

2. ＋をクリックします。
3. プロファイルの名前と説明を入力します。
4. ［違反が検出されたときに送信されるメール］ドロップダウンリストで、メールテンプレートを選択します。

   これは、コンプライアンス違反が検出されたときに、UEM がユーザーに送信するデフォルトのコンプライアンスメールです。手順 7 でコンプライアンスルールを有効にすると、該当する場合は、コンプライアンスルールごとに異なるメールテンプレートを選択することができます。
5. ［施行間隔］ドロップダウンリストで、BlackBerry Dynamics アプリのコンプライアンスチェックの頻度を選択します。BlackBerry Dynamics 以外のコンプライアンスチェックの施行間隔は一定のため、設定できません。
6. ［違反が検出されたときに送信されるデバイス通知］を展開し、必要に応じてメッセージを編集します。メッセージ内の変数を使用して、特定のユーザー、デバイス、およびコンプライアンス情報を追加できます。『プロファイル、メール、通知での変数の使用』を参照してください。
7. 組織内の各デバイスタイプのタブをクリックして、各プロファイル設定に適切な値を設定します。各プロファイル設定の詳細については、次を参照してください。
   - 共通：コンプライアンスプロファイル設定
   - iOS および iPadOS：コンプライアンスプロファイル設定
   - macOS ：コンプライアンスプロファイル設定
   - Android ：コンプライアンスプロファイル設定
   - Windows ：コンプライアンスプロファイル設定
8. ［保存］をクリックします。

終了したら：

- プロファイルをユーザーおよびグループに割り当てます。
- 必要に応じて、プロファイルをランク付けします。
- UEM で検出されたコンプライアンスイベントを監視するには、コンプライアンスイベントの監視 を参照してください。

共通：コンプライアンスプロファイル設定

デバイスタブで選択するコンプライアンスルールごとに、ユーザーのデバイスが非準拠の場合に BlackBerry UEM で実行するアクションを選択します。

コンプライアンスプロファイル設定	説明
プロンプトの動作	この設定では、UEM がユーザーにコンプライアンスの問題を修正するように求めるかどうかを指定して、ユーザーにアクションを実行する前に問題を解決する時間を与えるか、UEM による即時アクションを実行するかどうかを指定します。

コンプライアンスプロファイル設定	説明
プロンプトの方法	この設定では、UEM がデバイス通知またはメールメッセージとデバイス通知を送信してコンプライアンスの問題を解決するようにユーザーに求めるかどうかを指定します。 BlackBerry Dynamics アプリはこの設定に関係なく、デバイス通知のみを送信します。デバイス通知は Windows 10 デバイスではサポートされません。 この設定は、［強制アクション］が［コンプライアンス用のプロンプト］に設定されている場合にのみ有効です。
コンプライアンス違反が検出されたときに使用されるメールテンプレート	この設定では、ユーザーのデバイスが選択したコンプライアンスルールに準拠していない場合に、ユーザーに送信するメールテンプレートを指定します。［プロファイルのデフォルトを使用］を選択した場合、UEM はプロファイルに設定したデフォルトのメールテンプレートを送信します（違反が検出されたときに送信されるメール）。 この設定は、［プロンプトの方法］が［メールとデバイスの通知］に設定されている場合にのみ有効です。
プロンプトの回数	この設定は、ユーザーにコンプライアンスの問題を修正するように求める回数を指定します。 この設定は、［強制アクション］が［コンプライアンス用のプロンプト］に設定されている場合にのみ有効です。
プロンプトの間隔	この設定は、プロンプトの時間（分、時間、または日数）を指定します。 この設定は、［強制アクション］が［コンプライアンス用のプロンプト］に設定されている場合にのみ有効です。

コンプライアンスプロファイル設定	説明
デバイスの強制アクション	この設定は、準拠していないデバイスで UEM が実行するアクションを指定します。使用可能なオプションは、OS とコンプライアンスルールのタイプによって異なる場合があります。 • 監視とログ：UEM はコンプライアンス違反を特定しますが、デバイスには強制アクションを実行しません。 • 信頼しない：ユーザーがデバイスで仕事用リソースとアプリにアクセスできません。データとアプリは削除されません。iOS デバイスおよび iPadOS デバイスでは、仕事用メールアカウントが、ネイティブのメールアプリから削除されます。ユーザーは、デバイスがコンプライアンスの状態に戻ってから、メールアカウント設定をアプリに復元する必要があります。 • 仕事用データのみを削除 • すべてのデータを削除する • サーバーから削除 この設定は、ユーザーのプライバシー でアクティブ化されたデバイスには適用されません。 「仕事用と個人用 - ユーザーのプライバシー 」でアクティブ化されたデバイスでは、ユーザーのデバイス上のデータをすべて削除することはできません。［すべてのデータを削除］を選択した場合、UEM は［仕事用データのみを削除］と同じ操作を実行します。 監視対象の iOS デバイスおよび iPadOS デバイスでは、「制限付きアプリがインストールされています」ルールの強制操作は適用されません。ユーザーは、制限付きアプリのインストールが自動的にできなくなります。
BlackBerry Dynamics アプリの強制アクション	この設定は、デバイスが準拠していない場合、BlackBerry Dynamics アプリで行われるアクションを定義します。 • BlackBerry Dynamics アプリの実行を許可しない • BlackBerry Dynamics のアプリデータの削除 • 監視とログ：UEM はコンプライアンス違反を特定しますが、強制アクションは実行しません。

iOS および iPadOS：コンプライアンスプロファイル設定

デバイスがコンプライアンスルールに違反した場合に BlackBerry UEM が実行できる強制アクションの説明については、「共通：コンプライアンスプロファイル設定」を参照してください。

コンプライアンスプロファイル設定	説明
脱獄された OS	この設定では、デバイスが脱獄されていないことを確認するために、コンプライアンスルールを作成します。ユーザーまたは攻撃者がデバイスのさまざまな制限をバイパスして OS を改変すると、デバイスは脱獄された状態になります。 この設定を選択すると、設定した強制アクションに関係なく、ユーザーは脱獄された状態のデバイスの新しいアクティベーションを完了できません。
管理対象デバイス認証の失敗	この設定では、デバイスが管理対象デバイス認証に失敗した場合に発生するアクションを指定するコンプライアンスルールを作成します。
割り当てのないアプリがインストールされている	この設定では、ユーザーに割り当てられなかったアプリがデバイスにインストールされていないことを確認するコンプライアンスルールが作成されます。 この設定は、ユーザーのプライバシー アクティベーションタイプのデバイスには適用されません。
必須アプリがインストールされていません	この設定では、必須アプリがデバイスにインストールされていることを確認するコンプライアンスルールが作成されます。
制限された OS バージョンがインストールされています	この設定では、制限された OS バージョンがデバイスにインストールされていないことを確認するコンプライアンスルールが作成されます。制限された OS バージョンを選択できます。 この設定を選択すると、ユーザーは、設定した強制アクションに関係なく、準拠していないデバイスの新しいアクティベーションを完了できなくなります。
制限されたデバイスモデルが検出されました	この設定では、デバイスモデルを制限するコンプライアンスルールが作成されます。許可または制限されているデバイスモデルを選択できます。 この設定を選択すると、ユーザーは、設定した強制アクションに関係なく、準拠していないデバイスの新しいアクティベーションを完了できなくなります。
OS 更新が適用されていません	この設定では、指定した期間内にユーザーが保留中の OS 更新を適用しない場合に、コンプライアンスアクションを実行するコンプライアンスルールを作成します。
デバイスの応答がありません	この設定では、指定された時間を超えてデバイスが UEM と無応答になっていないことを確認するコンプライアンスルールが作成されます。コンプライアンス違反とみなされる前に、デバイスが UEM と無応答の状態を続けられる日数を指定します。
BlackBerry Dynamics ライブラリのバージョンの確認	この設定では、アクティブ化できない BlackBerry Dynamics ライブラリバージョンを選択できるようにするコンプライアンスルールが作成されます。ブロックされているライブラリバージョンを選択できます。

コンプライアンスプロファイル設定	説明
BlackBerry Dynamics 接続の確認	この設定では、指定された時間を超えて BlackBerry Dynamics アプリが UEM と無応答になっているかどうかを監視するコンプライアンスルールが作成されます。強制アクションは BlackBerry Dynamics アプリに適用されます。 ［認証委任アプリでのベース接続間隔］設定では、接続の検証が、認証委任アプリが UEM に接続するタイミングに基づいて行われることを指定します。この設定は、認証委任が BlackBerry Dynamics プロファイルで指定されている場合にのみ適用されます。 ［最終接続時刻］設定では、デバイスがコンプライアンス違反とみなされる前に、デバイスが UEM と無応答の状態を続けられる日数を指定します。 BlackBerry Dynamics アプリは、このルールに対するコンプライアンスをユーザーに確認しません。［プロンプトの動作］設定を［コンプライアンス用のプロンプト］に設定した場合、ユーザーにはプロンプトは表示されません。デバイスが UEM に接続できる場合、ユーザーが BlackBerry Dynamics アプリを開くと、デバイスはコンプライアンスの状態に戻ります。
iOS デバイスでの BlackBerry Dynamics 画面キャプチャ検出	メモ：このコンプライアンスルールは、BlackBerry Dynamics プロファイルの［iOS デバイスではスクリーンショットを許可しない］オプションに置き換えられました。BlackBerry では、プロファイル設定を使用し、このコンプライアンスルールを無効にすることをお勧めします。このコンプライアンスルールは、将来の UEM リリースで廃止されます。 この設定は、デバイス上の BlackBerry Dynamics アプリの画面キャプチャに対応するコンプライアンスルールを作成します。 ［期間内の画面キャプチャの最大数］設定では、指定した時間内に許可される画面キャプチャ数を指定します。 ［BlackBerry Dynamics アプリの強制アクション］設定では、ユーザーが許可されている画面キャプチャ数を超えた場合に発生するアクションを指定します。
制限付きアプリがインストールされています	この設定では、マーケットプレイスアプリを含め、制限されたアプリを定期的にチェックするための UEM のコンプライアンスルールを作成します。UEM の制限されたアプリリストからアプリを選択するか、組み込みアプリ（監視対象デバイスのみ）を選択して、プロファイルの制限アプリリストにアプリを追加します。 この設定を選択している場合、制限されたアプリがデバイスにインストールされると、警告メッセージとリンクが［管理対象デバイス］タブに表示されます。リンクをクリックすると、デバイスのコンプライアンス違反の原因になっているアプリがリストに表示されます。制限されたアプリのリストは、コンプライアンス通知でユーザーにも送信されます。 監視対象のデバイスには、このルールの強制アクションは適用されません。ユーザーは、制限付きアプリのインストールが自動的にできなくなります。制限されたアプリ（組み込みアプリまたはユーザーがインストールされたアプリ）が既にインストールされている場合、それらのアプリはデバイスから自動的に削除されます。

コンプライアンスプロファイル設定	説明
デバイスで許可されているアプリのみを表示する	この設定では、マーケットプレイスアプリを含め、デバイスにインストールできるアプリのリストを指定するコンプライアンスルールを作成します。他のすべてのアプリは許可されません。UEM アプリリストからアプリを選択するか、組み込みアプリを選択して、プロファイルの許可アプリリストにアプリを追加します。一部のアプリは、デフォルトで許可リストに含まれています。 この設定は監視対象デバイスに対してのみ有効です。

macOS：コンプライアンスプロファイル設定

デバイスがコンプライアンスルールに違反した場合に BlackBerry UEM が実行できる強制アクションの説明については、「共通：コンプライアンスプロファイル設定」を参照してください。

コンプライアンスプロファイル設定	説明
制限された OS バージョンがインストールされています	この設定では、制限された OS バージョンがデバイスにインストールされていないことを確認するコンプライアンスルールが作成されます。制限された OS バージョンを選択できます。 この設定を選択すると、ユーザーは、設定した強制アクションに関係なく、準拠していないデバイスの新しいアクティベーションを完了できなくなります。
制限されたデバイスモデルが検出されました	この設定では、デバイスモデルを制限するコンプライアンスルールが作成されます。許可または制限されているデバイスモデルを選択できます。 この設定を選択すると、ユーザーは、設定した強制アクションに関係なく、準拠していないデバイスの新しいアクティベーションを完了できなくなります。
BlackBerry Dynamics ライブラリのバージョンの確認	この設定では、アクティブ化できない BlackBerry Dynamics ライブラリバージョンを選択できるようにするコンプライアンスルールが作成されます。ブロックされているライブラリバージョンを選択できます。
BlackBerry Dynamics 接続の確認	この設定では、指定された時間を超えて BlackBerry Dynamics アプリが UEM と無応答になっているかどうかを監視するコンプライアンスルールが作成されます。強制アクションは BlackBerry Dynamics アプリに適用されます。 ［認証委任アプリでのベース接続間隔］設定では、接続の検証が、認証委任アプリが UEM に接続するタイミングに基づいて行われることを指定します。この設定は、認証委任が BlackBerry Dynamics プロファイルで指定されている場合にのみ適用されます。 ［最終接続時刻］設定では、デバイスがコンプライアンス違反とみなされる前に、デバイスが UEM と無応答の状態を続けられる日数を指定します。

Android ：コンプライアンスプロファイル設定

デバイスがコンプライアンスルールに違反した場合に BlackBerry UEM が実行できる強制アクションの説明については、「共通：コンプライアンスプロファイル設定」を参照してください。

コンプライアンスプロファイル設定	説明
ルート化された OS または失敗した Knox の認証	この設定では、ユーザーや攻撃者が Android デバイスのルートレベルにアクセスした場合に発生するアクションを指定するコンプライアンスルールが作成されます。 この設定を選択すると、ユーザーは、設定した強制アクションに関係なく、ルート化されたデバイスの新しいアクティベーションを完了することができなくなります。 ［BlackBerry Dynamics アプリ実行時にデバッガとエミュレータの検出を有効にする］を選択すると、BlackBerry Dynamics ランタイムはアクティブなデバッグツールまたはエミュレーションツールが検出された場合に、BlackBerry Dynamics アプリが停止されます。 ［BlackBerry Dynamics アプリのロック解除または未確認のブートデバイスの検出を有効にする］を選択すると、UEM がデバイスのブート状態を確認できるようになります。
SafetyNet または Play Integrity 認証失敗	この設定では、デバイスが SafetyNet または Play Integrity 認証に失敗した場合に発生するアクションを指定するコンプライアンスルールが作成されます。SafetyNet または Play Integrity 認証を使用する場合、UEM は、組織の環境内の Android デバイスとアプリの完全性と整合性をテストするためのチャレンジを送信します。『Android デバイスおよび BlackBerry Dynamics アプリの認証の設定』を参照してください。
割り当てのないアプリがインストールされている	この設定では、ユーザーに割り当てられなかったアプリがデバイスにインストールされていないことを確認するコンプライアンスルールが作成されます。 この設定を選択している場合、割り当てられていないアプリが Android デバイスにインストールされると、警告メッセージとリンクがコンソールの［管理されているデバイス］画面に表示されます。リンクをクリックすると、割り当てられていないアプリのリストが表示されます。 Android Enterprise、Android Management、および Samsung Knox デバイスの場合、ユーザーは割り当てのないアプリを仕事用領域にインストールできません。強制アクションは適用されません。 この設定は、ユーザーのプライバシー でアクティブ化されたデバイスには有効ではありません。

コンプライアンスプロファイル設定	説明
必須アプリがインストールされていません	この設定では、必須アプリがデバイスにインストールされていることを確認するコンプライアンスルールが作成されます。 この設定を選択している場合、必須アプリが Android デバイスにインストールされていないと、警告メッセージとリンクがコンソールの［管理されているデバイス］画面に表示されます。 Android Enterprise および Android Management デバイスには強制アクションは適用されません。Samsung Knox デバイスの場合、必須の内部アプリは自動的にインストールされます。強制アクションは、必須の一般のアプリにのみ適用されます。
制限された OS バージョンがインストールされています	この設定では、制限された OS バージョンがデバイスにインストールされていないことを確認するコンプライアンスルールが作成されます。制限された OS バージョンを選択できます。 この設定を選択すると、ユーザーは、設定した強制アクションに関係なく、準拠していないデバイスの新しいアクティベーションを完了できなくなります。
制限されたデバイスモデルが検出されました	この設定では、デバイスモデルを制限するコンプライアンスルールが作成されます。許可または制限されているデバイスモデルを指定できます。 この設定を選択すると、ユーザーは、設定した強制アクションに関係なく、準拠していないデバイスの新しいアクティベーションを完了できなくなります。
OS 更新が適用されていません	この設定では、指定した期間内にユーザーが保留中の OS 更新を適用しない場合に、コンプライアンスアクションを実行するコンプライアンスルールを作成します。
デバイスの応答がありません	この設定では、指定された時間を超えてデバイスが UEM と無応答であるかどうかを監視するコンプライアンスルールが作成されます。［最終接続時刻］設定では、デバイスがコンプライアンス違反となる前に、デバイスが UEM と無応答の状態を続けられる日数を指定します。
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ない	この設定では、必要なセキュリティパッチがデバイスにインストールされていることを確認するコンプライアンスルールが作成されます。セキュリティパッチをインストールする必要があるデバイスモデルとセキュリティパッチの日付を指定できます。指定されたセキュリティパッチの日付以降のセキュリティパッチを実行しているデバイスは、準拠していると見なされます。 ［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ない］設定が有効になっているコンプライアンスプロファイルを以前に作成している場合は、アップグレード後に、強制アクションは［監視とログ］に設定されます。
BlackBerry Dynamics ライブラリのバージョンの確認	この設定では、アクティブ化できない BlackBerry Dynamics ライブラリバージョンを選択できるようにするコンプライアンスルールが作成されます。ブロックされているライブラリバージョンを選択できます。

コンプライアンスプロファイル設定	説明
BlackBerry Dynamics 接続の確認	この設定では、指定された時間を超えて BlackBerry Dynamics アプリが UEM と無応答になっているかどうかを監視するコンプライアンスルールが作成されます。強制アクションは BlackBerry Dynamics アプリに適用されます。 ［認証委任アプリでのベース接続間隔］設定では、接続の検証が、認証委任アプリが UEM に接続するタイミングに基づいて行われることを指定します。この設定は、認証委任が BlackBerry Dynamics プロファイルで指定されている場合にのみ適用されます。 ［最終接続時刻］設定では、コンプライアンス違反とみなされる前に、デバイスが UEM と無応答の状態を続けられる日数を指定します。
制限付きアプリがインストールされています	この設定では、制限されたアプリがデバイスにインストールされていないことを確認するコンプライアンスルールが作成されます。アプリを制限する方法については、「制限されたアプリリストへのアプリの追加」を参照してください。 Android Enterprise および Android Management デバイスの場合、ユーザーは制限されたアプリを仕事用領域にインストールできません。強制アクションは適用されません。 Samsung Knox デバイスでは、仕事用領域の制限されたアプリは自動的に無効になります。強制アクションは適用されません。 仕事用と個人用 - フルコントロール （Samsung Knox）アクティベーションタイプのデバイスの場合、［個人用領域でコンプライアンスアクションを適用する］を選択して、仕事用プロファイルと個人用プロファイルの両方のアプリにルールを適用します。 この設定は、ユーザーのプライバシー でアクティブ化されたデバイスには有効ではありません。 この設定を選択している場合、制限されたアプリが Android デバイスにインストールされていないと、警告メッセージとリンクがコンソールの［管理されているデバイス］画面に表示されます。リンクをクリックすると、制限されたアプリのリストが表示されます。
パスワードが複雑さの要件を満たしていません。	この設定では、割り当てられた IT ポリシーで定義された複雑さの要件を満たす、デバイスまたは仕事用領域のパスワードをユーザーが設定していることを確認するコンプライアンスルールが作成されます。

Windows ：コンプライアンスプロファイル設定

デバイスがコンプライアンスルールに違反した場合に BlackBerry UEM が実行できる強制アクションの説明については、「共通：コンプライアンスプロファイル設定」を参照してください。

コンプライアンスプロファイル設定	説明
必須アプリがインストールされていません	この設定では、必須アプリがデバイスにインストールされていることを確認するコンプライアンスルールが作成されます。内部アプリの種別は監視できません。
制限された OS バージョンがインストールされています	この設定では、制限された OS バージョンがデバイスにインストールされていないことを確認するコンプライアンスルールが作成されます。制限された OS バージョンを選択できます。
制限されたデバイスモデルが検出されました	この設定では、デバイスモデルを制限するコンプライアンスルールが作成されます。許可または制限されているデバイスモデルを選択できます。
デバイスの応答がありません	この設定では、指定された時間を超えてデバイスが UEM と無応答になっていないことを確認するコンプライアンスルールが作成されます。
BlackBerry Dynamics ライブラリのバージョンの確認	この設定では、アクティブ化できない BlackBerry Dynamics ライブラリバージョンを選択できるようにするコンプライアンスルールが作成されます。ブロックされているライブラリバージョンを選択できます。
BlackBerry Dynamics 接続の確認	この設定では、指定された時間を超えて BlackBerry Dynamics アプリが UEM と無応答になっていないことを確認するコンプライアンスルールが作成されます。強制アクションは BlackBerry Dynamics アプリに適用されます。
ウイルス対策署名	この設定では、ウイルス対策署名がデバイスで有効になっていることを確認するコンプライアンスルールが作成されます。
ウイルス対策ステータス	この設定では、ウイルス対策ソフトウェアがデバイスで有効になっていることを確認するコンプライアンスルールが作成されます。許可されているベンダーを選択できます。
ファイアウォールステータス	この設定では、ファイアウォールがデバイスで有効になっていることを確認するコンプライアンスルールが作成されます。
暗号化ステータス	この設定では、デバイスで暗号化が必要になっていることを確認するコンプライアンスルールが作成されます。
Windows 更新ステータス	この設定では、デバイスが UEM に Windows OS 更新のインストールを許可しているか、必要な更新についてユーザーに通知しているかを確認するコンプライアンスルールが作成されます。
制限付きアプリがインストールされています	この設定では、制限されたアプリがデバイスにインストールされていないことを確認するコンプライアンスルールが作成されます。アプリを制限する方法については、「制限されたアプリリストへのアプリの追加」を参照してください。
Windows デバイスの正常性認証	
猶予期間が終了している	この設定では、立証猶予期間が終了している場合に行われるアクションを指定するコンプライアンスルールが作成されます。

コンプライアンスプロファイル設定	説明
立証 ID キーが存在していない	この設定では、AIK がデバイスに存在していない場合に行われるアクションを指定するコンプライアンスルールが作成されます。
データ実行防止ポリシーが無効	この設定では、DEP ポリシーがデバイスで無効になっている場合に行われるアクションを指定するコンプライアンスルールが作成されます。
BitLocker が無効	この設定では、BitLocker がデバイスで無効になっている場合に行われるアクションを指定するコンプライアンスルールが作成されます。
セキュリティで保護されたブートが無効	この設定では、セキュリティで保護されたブートがデバイスで無効になっている場合に行われるアクションを指定するコンプライアンスルールが作成されます。
コード整合性が無効	この設定では、コード整合性機能がデバイスで無効になっている場合に行われるアクションを指定するコンプライアンスルールが作成されます。
デバイスがセーフモード	この設定では、デバイスがセーフモードの場合に行われるアクションを指定するコンプライアンスルールが作成されます。
デバイスが Windows プレインストール環境にある	この設定では、デバイスが Windows プレインストール環境に置かれている場合に行われるアクションを指定するコンプライアンスルールが作成されます。
早期起動マルウェア対策ドライバーがロードされていない	この設定では、早期起動マルウェア対策ドライバーがロードされていない場合に行われるアクションを指定するコンプライアンスルールが作成されます。
仮想セキュアモードが無効	この設定では、仮想セキュアモードが無効になっている場合に行われるアクションを指定するコンプライアンスルールが作成されます。
ブートデバッグが有効	この設定では、ブートデバッグが有効になっている場合に行われるアクションを指定するコンプライアンスルールが作成されます。
OS カーネルデバッグが有効	この設定では、OS カーネルデバッグが有効になっている場合に行われるアクションを指定するコンプライアンスルールが作成されます。
テスト署名が有効	この設定では、テスト署名が有効になっている場合に行われるアクションを指定するコンプライアンスルールが作成されます。
ブートマネージャーリビジョンリストが想定のバージョンではない	この設定では、ブートマネージャーリビジョンリストが想定のバージョンではない場合に行われるアクションを指定するコンプライアンスルールが作成されます。予想されるバージョンを指定します。
コード整合性リビジョンリストが想定のバージョンではない	この設定では、コード整合性リビジョンリストが想定のバージョンではない場合に行われるアクションを指定するコンプライアンスルールが作成されます。予想されるバージョンを指定します。

コンプライアンスプロファイル設定	説明
コード整合性ポリシーのハッシュが存在し、許容値ではない	この設定では、コード整合性ポリシーのハッシュが存在し、許容値ではない場合に行われるアクションを指定するコンプライアンスルールが作成されます。許容値を指定します。
カスタムセキュアブート設定ポリシーのハッシュが存在し、許容値ではない	この設定では、カスタムセキュアブート設定ポリシーのハッシュが存在し、許容値ではない場合に行われるアクションを指定するコンプライアンスルールが作成されます。許容値を指定します。
PCR 値が許容値ではない	この設定では、PCR 値が許容値でない場合に行われるアクションを指定するコンプライアンスルールが作成されます。許容値を指定します。

コンプライアンスイベントの監視

コンプライアンスプロファイルを設定してユーザーに割り当てたら、コンプライアンスイベント画面を使用して、ユーザーの iOS、Android、macOS、Windows デバイスのコンプライアンス違反を監視および追跡できます。この画面には、UEM 用 CylancePROTECT Mobile 機能に関連するコンプライアンスイベントも表示されます。

作業を始める前に： コンプライアンスプロファイルを作成および編集します。

1. 管理コンソールのメニューバーで、［ユーザー］ > ［コンプライアンス違反］をクリックします。
2. 次の操作のいずれかを実行します。
   - デフォルトでは、この画面には、指定した日付範囲の新しいコンプライアンスイベントが表示されます。解決済みのアラート、無視されたアラート、すべてのアラートの表示、または日付範囲の変更を行うには［編集］をクリックします。ステータスと日付範囲を設定し、［送信］をクリックします。
   - ［フィルタ］セクションで、表示するコンプライアンスイベントに適切なフィルタを設定し、［送信］をクリックします。
   - をクリックして、表示する列を設定します。
   - 列をクリックして、その条件でイベントを並べ替えます。
   - 特定のコンプライアンスイベントを検索するには、検索フィールドを使用します。
3. このビューからイベントを削除する場合は、イベントを選択して をクリックします。イベントを無視するとこのビューから削除されますが、関連付けられているデバイスのコンプライアンスステータスには影響しません。
4. 選択したイベントを .csv ファイルにエクスポートするには、イベントを選択して をクリックします。

いずれかのステータスを持つコンプライアンスイベントは、120 日後にこのビューから自動的に削除されることに注意してください。ステータスが無視または解決済みのイベントは、7 日後に自動的に削除されます。

ユーザーおよびデバイスへのコマンドの送信

さまざまなコマンドを送信して、ユーザーアカウントとデバイスを管理できます。使用可能なコマンドのリストは、デバイスタイプとアクティベーションタイプによって異なります。特定のユーザーまたはデバイスにコマンドを送信することも、一括コマンドを使用して複数のユーザーおよびデバイスにコマンドを送信することもできます。

たとえば、次の環境でコマンドを使用できます。

- デバイスが一時的に置き忘れられた場合は、コマンドを送信して、デバイスをロックするか、デバイスから仕事用データを削除できます。
- デバイスを別のユーザーに再配布する場合、コマンドを送信してデバイスからすべてのデータを削除できます。
- 従業員が退職する場合は、ユーザーの個人用デバイスにコマンドを送信して、仕事用データのみを削除できます。
- ユーザーが仕事用領域のパスワードを忘れた場合は、コマンドを送信して仕事用領域のパスワードをリセットできます。
- 監視対象の DEP デバイスを所有しているユーザーには、OS のアップグレードをトリガーするコマンドを送信できます。

ユーザーおよびデバイスへのコマンドの送信

1. 管理コンソールのメニューバーで、［ユーザー］ > ［管理対象デバイス］をクリックします。
2. 次の操作のいずれかを実行します。

タスク	手順
特定のユーザーまたはデバイスにコマンドを送信します。	a. ユーザーを検索してクリックします。 b. ［デバイス］タブの［デバイスを管理］セクションで、適切なコマンドをクリックします。
複数のユーザーまたはデバイスに一括コマンドを送信します。	a. 複数のユーザーを検索して選択します。 b. ユーザーリストの上にあるコマンドメニューから、適切なコマンドをクリックします。

利用可能なコマンドの詳細については、以下を参照してください。

- iOS および iPadOS デバイスのコマンド。
- macOS デバイスのコマンド。
- Android デバイスのコマンド。
- Windows デバイスのコマンド。

終了したら：［すべてのデバイスデータを削除］および［仕事用データのみ削除］コマンドの有効期限を設定する場合は、「コマンドの有効期限の設定」を参照してください。

コマンドの有効期限の設定

デバイスに［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］コマンドを送信した場合、デバイスはコマンドを完了するために BlackBerry UEM に接続する必要があります。デバイスが UEM に接続できない場合、コマンドは保留状態のままとなり、手動で削除しない限りデバイスは UEM から削除されません。別の方法として、指定した時間でコマンドが完了しない場合にデバイスを自動的に削除するために、UEM を設定することができます。

1. 管理コンソールのメニューバーで、［設定］ > ［一般設定］ > ［コマンドの有効期限の削除］をクリックします。
2. 一方または両方のコマンドで、［コマンドの期限が切れた場合、デバイスを自動的に削除］を選択します。
3. ［コマンドの有効期限］フィールドで、コマンドの期限が切れてデバイスが UEM から自動的に削除されるまでの日数を入力します。
4. ［保存］をクリックします。

iOS および iPadOS 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保存したりできます。	MDM 制御 ユーザーのプライバシー
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。	MDM 制御 ユーザーのプライバシー
すべてのデバイスデータを削除	このコマンドは、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て、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 UEM に接続する場合、仕事用データのみがデバイスから削除されます。 iOS 17以降のデバイスにコマンドを送信する場合は、［サービス再開を有効にする］オプションを選択し、デバイスに割り当てる Wi-Fi プロファイルを選択することで、ユーザーがデータの削除後にデバイスを再設定できるようになります。 選択した 1 つまたは複数のデバイスで eSIM 情報が検出された場合は、データプラン情報を保存する必要があるかどうかを指定するように求められます。	MDM 制御

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、プロファイル、アプリ、証明書を含む仕事用データを削除します。 このコマンドを送信するときにデバイスが 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 UEM に接続する場合、仕事用データがデバイスから削除されます。	MDM 制御 ユーザーのプライバシー
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。Apple は、指定したメッセージのタイトルに「紛失した iPhone」または「紛失した iPad」と追加します。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。 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。 Apple TV デバイスでは、このコマンドはサポートされていません。	MDM 制御
ロック解除してパスワードをクリア	このコマンドは、デバイスのロックを解除して、既存のパスワードを削除します。ユーザーは、デバイスパスワードを作成するように要求されます。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。 Apple TV デバイスでは、このコマンドはサポートされていません。	MDM 制御
紛失モードをオンにする	このコマンドは、デバイスをロックし、またデバイスに電話番号とメッセージを表示できます。このコマンドの送信後に、管理コンソールにデバイスの場所を表示できます。 このコマンドは、監視対象デバイスでのみサポートされます。Apple TV デバイスでは、このコマンドはサポートされていません。	MDM 制御
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 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。 Apple TV デバイスでは、このコマンドはサポートされていません。	MDM 制御

コマンド	説明	アクティベーションタイプ
OS の更新	このコマンドは、利用可能な OS の更新をインストールするようにデバイスに強制します。 このコマンドは、監視対象デバイスでのみサポートされます。Apple TV デバイスでは、このコマンドはサポートされていません。	MDM 制御
デバイスを再起動する	このコマンドは、デバイスを強制的に再起動します。 このコマンドは、監視対象デバイスでのみサポートされます。Apple TV デバイスでは、このコマンドはサポートされていません。	MDM 制御
デバイスをオフにする	このコマンドは、デバイスを強制的にオフにします。 このコマンドは、監視対象デバイスでのみサポートされます。Apple TV デバイスでは、このコマンドはサポートされていません。	MDM 制御
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。	MDM 制御
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。	MDM 制御 ユーザーのプライバシー
Update time zone	このコマンドは、選択した地域に応じてデバイスの時刻を設定します。	MDM 制御
デバイスを削除	このコマンドは、デバイスを 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 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 UEM と通信できなくなります。	MDM 制御 ユーザーのプライバシー
eSIM を更新	eSIM ベースの携帯電話データアプリを持つデバイスの場合、このコマンドは、通信事業者の URL からそのデバイス向けの更新された携帯電話データアプリ詳細を照会します。	MDM 制御

macOS デバイスのコマンド

コマンド	説明
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保存したりできます。
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。
デスクトップをロック	このコマンドでは、PIN の設定とデバイスのロックを実行できます。
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、プロファイル、アプリ、証明書などの仕事用データを削除し、オプションで、デバイスを BlackBerry UEM から削除します。
すべてのデバイスデータを削除	このコマンドは、デバイスからすべてのユーザー情報とアプリデータを削除します。これは、デバイスを工場出荷の状態に戻し、セットした PIN でデバイスをロックし、必要に応じて UEM からデバイスを削除します。
デスクトップデータを更新	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。
デバイスを削除	このコマンドは、UEM からデバイスを削除します。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。

Android デバイスのコマンド

Android Management アクティベーションタイプについては、「Android Management のアクティベーションタイプに関する考慮事項」を参照してください。

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保存したりできます。	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。	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
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。 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。	仕事用と個人用 - フルコントロール（Android Management） 仕事用と個人用 - ユーザーのプライバシー（Android Management） 仕事用領域のみ （Android Management） 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） MDM 制御
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 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 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。	仕事用と個人用 - フルコントロール（Android Management） 仕事用領域のみ （Android Management） 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） MDM 制御

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残ります。 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。 このコマンドを送信するときにデバイスが 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 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。	仕事用と個人用 - フルコントロール（Android Management） 仕事用と個人用 - ユーザーのプライバシー（Android Management） 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） MDM 制御
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。 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。	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） MDM 制御 （Samsung デバイスのみ）
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。	仕事用と個人用 - ユーザーのプライバシー（Android Management） 仕事用領域のみ （Android Management） 仕事用領域のみ （Android Enterprise） 仕事用と個人用 - フルコントロール（Samsung Knox）

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）
仕事用領域パスワードの指定とロック	このコマンドでは、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 - 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（Android Management） 仕事用と個人用 - ユーザーのプライバシー（Android Management） 仕事用領域のみ（Android Management） 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）
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 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。	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。	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 Management） 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 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 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 UEM と通信できなくなります。	すべて（BlackBerry 2FA を除く）

Windows デバイスのコマンド

コマンド	説明
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保存したりできます。
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。
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。 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。 このコマンドは、Windows 10 Mobile を実行しているデバイスでのみサポートされています。

コマンド	説明
デバイスパスワードを生成してロック	このコマンドでデバイスパスワードが生成され、デバイスがロックされます。生成されたパスワードは、メールでユーザーに送信されます。選択済みのメールアドレスを使用することも、メールアドレスを指定することもできます。生成されるパスワードは、既存のパスワードルールに準拠しています。 このコマンドは、Windows 10 Mobile を実行しているデバイスでのみサポートされています。
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、プロファイル、アプリ、証明書などの仕事用データを削除し、オプションで、デバイスを BlackBerry UEM から削除します。 このコマンドを送信する場合、ユーザーアカウントは削除されません。 このコマンドの送信後、UEM からデバイスを削除するためのオプションが表示されます。デバイスが UEM に接続できない場合、UEM から削除できます。削除後にデバイスが 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。
すべてのデバイスデータを削除	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ます。デバイスを工場出荷時のデフォルト設定に戻し、オプションで UEM からデバイスを削除します。 このコマンドの送信後、UEM からデバイスを削除するためのオプションが表示されます。デバイスが UEM に接続できない場合、UEM から削除できます。削除後にデバイスが 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。
デスクトップ/デバイスを再起動	このコマンドは、デバイスを強制的に再起動します。
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。 また、コマンドはデバイスに要求を送信して、ヘルス証明書の検証要求を作成します。コンプライアンスの確認のために、デバイスは Microsoft Health Attestation Service に要求を送信します。この機能はオンプレミス環境でのみサポートされています。
デバイスを削除	このコマンドは、UEM からデバイスを削除します。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。

デバイスでインストールされるソフトウェア更新の制御

デバイス SR 要件プロファイルを使用して、Android Enterprise、Android Management、および Samsung Knox デバイスにデバイスソフトウェア更新をインストールする方法、およびフォアグラウンドで実行されているアプリのアプリ更新を管理する方法を制御できます。

IT ポリシールールを使用して、iOS デバイスでソフトウェア更新を制御できます。詳細については、『IT ポリシーリファレンススプレッドシート』を参照してください。管理コンソールを使用して、監視対象の iOS デバイスで OS を更新することもできます。

Android Enterprise および Android Management デバイスのデバイス SR 要件プロファイルの作成

OS 更新のルールは、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 および Android Management デバイスのみに適用されます。アプリ更新のルールはすべての Android Enterprise デバイスに適用されます。現在、Android Management デバイスでは OS の更新と自動アプリ更新の一時停止はサポートされていません。「Android Management のアクティベーションタイプに関する考慮事項」を参照してください。

1. 管理コンソールのメニューバーで、［ポリシーとプロファイル］ > ［コンプライアンス］ > ［デバイス **SR** 要件］をクリックします。
2. ＋ をクリックします。
3. プロファイルの名前と説明を入力します。
4. 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 デバイスの OS 更新ルールを設定するには、［**OS** 更新ルール］セクションで ＋ をクリックし、次の手順を実行します。
   a) ［機種］ドロップダウンリストで機種を選択します。
   b) ［**OS** バージョン］ドロップダウンリストで、インストールされている OS バージョンを選択します。
   c) ［更新ルール］ドロップダウンリストで、次のいずれかを選択します。
      - ［デフォルト］：ユーザーは更新をインストールするタイミングを選択できます。仕事用領域のみ（完全に管理されているデバイス）アクティベーションタイプを持つユーザーは、更新をインストールするタイミングを選択できません。
      - ［自動更新］：ユーザーにプロンプトを表示せずに更新がインストールされます。
      - ［時刻間で自動的に更新］：ユーザーにプロンプトを表示せずに指定した時間枠内に更新がインストールされます。ユーザーは、この時間枠外で更新をインストールすることもできます。
      - ［**30** 日まで延期］：更新のインストールを 30 日間ブロックします。30 日後、ユーザーは更新をインストールするタイミングを選択できます。デバイスの製造元と通信事業者によっては、セキュリティ更新を延期できない場合があります。
   d) ［追加］をクリックします。
5. 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 OS 更新を実行しない期間を指定するには、［**OS** 更新の一時停止］セクションで ＋ をクリックします。一時停止期間が開始する月と日、および一時停止期間を選択します。

   2 つ以上の停止期間を指定する場合、各期間の間には少なくとも 60 日が必要です。

6. 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するには、［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有効にする］を選択します。開始時刻と期間を選択します。
7. Google Play がフォアグラウンドで実行されているアプリ（Google Play のアプリの自動更新設定）に変更を適用する方法を指定するには、［アプリ自動更新ポリシー］ドロップダウンリストで、次のいずれかを選択します。
   - ［常に］：アプリは常に更新されます。常時実行されているアプリ（たとえば、BlackBerry UEM Client、BlackBerry Work、BlackBerry Connectivity）の場合、［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有効にする］オプションを選択していないと、ユーザーが手動で更新するまでアプリは更新されません。
   - ［**Wi-Fi** のみ］：アプリは、デバイスが Wi-Fi ネットワークに接続されている場合にのみ更新されます。常時実行されているアプリ（たとえば、UEM Client、BlackBerry Work、BlackBerry Connectivity）の場合、［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有効にする］オプションを選択していないと、ユーザーが手動で更新するまでアプリは更新されません。
   - ［ユーザーが承認できる］：デバイス上でアプリの更新を許可するよう求めるプロンプトがユーザーに表示されます。
   - ［無効］：アプリは更新されません。

   ［常時］、［**Wi-Fi** のみ］、［無効］のいずれかを選択した場合、ユーザーはそのデバイスで異なるオプションを選択できません。ユーザーは Google Play でアプリを手動で更新することはできます。
8. ［追加］をクリックします。

終了したら：

- プロファイルをユーザーおよびグループに割り当てます。
- 必要に応じて、プロファイルをランク付けします。
- 失効したソフトウェアリリース（通信事業者がサポートしなくなったソフトウェアリリース）を実行しているユーザーのリストを表示するには、［ポリシーとプロファイル］**>**［コンプライアンス］**>**［デバイス **SR** 要件］でプロファイルをクリックしてから、［**x** ユーザーが失効した **SR** を実行中］タブをクリックします。

Samsung Knox デバイスのデバイス SR 要件プロファイルの作成

Samsung Knox デバイスでは、Knox E-FOTA One（Enterprise Firmware Over the Air）を使用して、Samsung のファームウェア更新をインストールするタイミングを制御できます。組織で Samsung E-FOTA（2022 年 7 月 31 日サービス終了）を使用しており、E-FOTA ONE に移行する必要がある場合は、KB 69901 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）、仕事用領域のみ （Android Enterprise 完全管理のデバイス）、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）としてアクティベーションされた Samsung Knox デバイスは、E-FOTA One を使用したソフトウェア制限をサポートしています。

E-FOTA One は、仕事用と個人用 - ユーザーのプライバシー （Samsung Knox）または 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）のアクティベーションタイプではサポートされていません。

作業を始める前に：

- 管理コンソールのメニューバーで、 ［設定］**>**［ライセンスの概要］に移動して、E-FOTA ライセンスを BlackBerry UEM に追加します。
- E-FOTA を使用するには、デバイスに割り当てる IT ポリシーで Android の［OTA 更新を許可する］グローバルルールを有効にする必要があります。

1. 管理コンソールのメニューバーで、［ポリシーとプロファイル］ > ［コンプライアンス］ > ［デバイス **SR** 要件］をクリックします。
2. ＋をクリックします。
3. プロファイルの名前と説明を入力します。
4. Android OS の更新ルールを Samsung デバイスに適用できるようにするには、［すべての **Android** デバイスに制限を適用する］チェックボックスをオンにします。

   次の手順で設定するファームウェアルールは、これらのルールよりも優先されます。［OS 更新の一時停止］設定は、E-FOTA を使用する Samsung Knox デバイスには適用されません。
5. ［**Samsung** デバイスファームウェアルール］セクションで、＋をクリックします。
6. ［デバイスモデル］ドロップダウンリストにデバイスモデルを入力するか、リストからモデルを選択します。
7. ［言語］ドロップダウンリストで、言語を選択します。
8. ［通信事業者コード］フィールドに、通信事業者の CSC コードを入力します。
9. ［ファームウェアバージョンを取得］をクリックします。
10. 追加するファームウェアルールごとに前の手順を繰り返します。
11. 完了したら、［追加］をクリックします。
12. 強制更新をスケジュールする場合は、追加したファームウェアバージョンの横にある［スケジュール］をクリックします。［強制更新をスケジュール］ダイアログボックスで、次の操作を実行します。
    a) ［次の期間で強制更新をスケジュール］フィールドで、更新をインストールする必要がある日付範囲を選択します。
    b) ［次の時間帯で強制更新をスケジュール］ドロップダウンリストで、強制更新をインストールする必要がある時間を指定します。

    強制更新をスケジュールする場合、Knox デバイスはファームウェアバージョンに制限されなくなり、新しいバージョンが利用可能な場合は手動で更新できます。
13. ［保存］をクリックします。

終了したら：

- プロファイルをユーザーおよびグループに割り当てます。
- 必要に応じて、プロファイルをランク付けします。
- 失効したソフトウェアリリース（通信事業者がサポートしなくなったソフトウェアリリース）を実行しているユーザーのリストを表示するには、［ポリシーとプロファイル］ > ［コンプライアンス］ > ［デバイス **SR** 要件］でプロファイルをクリックしてから、［**x** ユーザーが失効した **SR** を実行中］タブをクリックします。

管理下の iOS デバイスでの OS の更新

管理コンソールを使用して、監視対象の iOS デバイスに利用可能な OS の更新を強制的にインストールできます。

1. 管理コンソールのメニューバーで、［ユーザー］ > ［管理対象デバイス］をクリックします。
2. 次の操作のいずれかを実行します。

タスク	手順
特定の監視対象 iOS デバイスでの OS 更新	**a.** ユーザーアカウントの名前を検索してクリックします。 **b.** 適切な［デバイス］タブで、ソフトウェア更新が利用可能な場合は、［今すぐ更新］をクリックします。 **c.** 適切な OS 更新設定を構成します。 **d.** ［更新］をクリックします。
複数の監視対象 iOS デバイスでの OS 更新	**a.** ユーザーアカウントを選択します。 **b.** をクリックします。 **c.** 適切な OS 更新設定を構成します。 **d.** ［更新］をクリックします。

アプリと設定の更新のためにデバイスが BlackBerry UEM に接続する方法の設定

アプリまたは設定の更新を確認するために、デバイスは定期的に BlackBerry UEM にアクセスするように、Enterprise Management Agent プロファイルに強制されています。デバイスの更新がある場合は、UEM にアクセスして更新を受信するように、UEM によりデバイスにプロンプトが表示されます。何らかの理由でデバイスにプロンプトが表示されない場合でも、指定した間隔でデバイスが UEM にアクセスするように Enterprise Management Agent プロファイルに強制されます。

オンプレミス環境では、Enterprise Management Agent プロファイルを使用しても、ユーザーデバイスに搭載された個人用アプリのリストを収集することを UEM に許可できます。

Enterprise Management Agent プロファイルの作成

1. 管理コンソールのメニューバーで、［ポリシーとプロファイル］ > ［ポリシー］ > ［エンタープライズ管理エージェント］をクリックします。
2. ＋をクリックします。
3. プロファイルの名前と説明を入力します。
4. デバイスタイプごとに設定します。設定の詳細については、以下を参照してください。
   - iOS ：Enterprise Management Agent プロファイル設定
   - Android ：Enterprise Management Agent プロファイル設定
   - Windows ：Enterprise Management Agent プロファイル設定
5. ［追加］をクリックします。

終了したら：

- プロファイルをユーザーおよびグループに割り当てます。
- 必要に応じて、プロファイルをランク付けします。

iOS ：Enterprise Management Agent プロファイル設定

設定	説明
Enterprise Management Agent のポーリングレート	Enterprise Management Agent サーバーコマンドに関するデバイスのポーリング間隔を秒単位で指定します。デバイスは、UEM Client が開かれている場合にのみポーリングします。
個人用アプリのコレクションを許可する	ユーザーの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 BlackBerry UEM で受信するかどうかを指定します。ユーザープライバシーでアクティベーションを行ったデバイスでは、この設定はサポートされていません。

Android ：Enterprise Management Agent プロファイル設定

設定	説明
アプリの変更	デバイスが、インストールされているアプリに変更がないかどうか確認する間隔を秒単位で指定します。
バッテリー残量のしきい値	デバイスが情報を BlackBerry UEM に送信するのに必要なバッテリ残量の変更をパーセントで指定します。
RAM の空き容量のしきい値	デバイスが情報を UEM に送信するために必要な空きメモリの量の変更をメガバイト単位で指定します。
内部ストレージのしきい値	デバイスが情報を UEM に送信するのに必要な内部空きストレージ領域量の変更をメガバイト単位で指定します。
メモリカードのしきい値	デバイスが情報を UEM に送信するのに必要な外部空き容量の変更をメガバイト単位で指定します。
Enterprise Management Agent のポーリングレート	Enterprise Management Agent サーバーコマンドに関するデバイスのポーリング間隔を秒単位で指定します。
個人用アプリのコレクションを許可する	ユーザーの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 UEM で受信するかどうかを指定します。ユーザープライバシーでアクティベーションを行ったデバイスでは、この設定はサポートされていません。

Windows ：Enterprise Management Agent プロファイル設定

設定	説明
デバイス設定更新のためのポーリング間隔	プッシュ通知が使用できない場合に設定更新のためにデバイスがポーリングを行う間隔を分で指定します。
最初の再試行セットでのポーリング間隔	デバイスの設定更新のポーリングが失敗した場合のために、最初の再試行セットで、各試行を実行する間隔を分単位で指定します。
最初の再試行回数	最初の再試行セットで実行する試行回数を指定します。
2 回目の再試行セットでのポーリング間隔	デバイスの設定更新のポーリングが失敗した場合のために、2 回目の再試行セットで、各試行を実行する間隔を分単位で指定します。
2 回目の再試行回数	2 回目の再試行セットで実行する試行回数を指定します。

設定	説明
スケジュールされた残りの再試行でのポーリング間隔	デバイスの設定更新のポーリングが失敗し、さらに 2 回目の再試行セットが失敗した場合に、それ以降の各試行を実行する間隔を分単位で指定します。
スケジュールされた残りの再試行回数	デバイスの設定更新のポーリングが失敗し、さらに 2 回目の再試行セットが失敗した場合に、それ以降の再試行回数を指定します。［0］に設定すると、接続が成功するか、またはデバイスが無効になるまで、デバイスはポーリングを続けます。
ユーザーログインでのポーリング	デバイスがユーザーのログインに基づいて管理セッションを開始するかどうかを指定します。
すべてのユーザーのポーリングを最初のログインで実行する	すべてのユーザーを対象として、デバイスが最初のユーザーログインに基づいて管理セッションを開始するかどうかを指定します。
個人用アプリのコレクションを許可する	ユーザーの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 BlackBerry UEM で受信するかどうかを指定します。

デバイスでの組織情報の表示

BlackBerry UEM は、デバイスで組織情報と組織のカスタム通知を表示するように設定できます。

iOS、macOS、Android、および Windows 10 デバイスでは、アクティベーションプロセス中に表示するカスタム組織通知を作成できます（たとえば、組織のセキュリティ要件に準拠するためにユーザーが順守する必要がある条件に関する通知を表示できます）。ユーザーがアクティベーションプロセスを続行するには、通知を受け入れる必要があります。複数の通知を作成することもできれば、異なる言語をサポートするために各通知の個別のバージョンを作成することもできます。

デバイスプロファイルを作成して、組織に関する情報をデバイスに表示することができます。iOS および Android デバイスの場合、組織情報は BlackBerry UEM Client に表示されます。Windows 10 の場合、電話番号とメールアドレスはデバイスのサポート情報に表示されます。Samsung Knox デバイスでは、デバイスプロファイルを使用して、ユーザーがデバイスを再起動したときに組織のカスタム通知を表示できます。

Samsung Knox および監視対象の iOS デバイスでは、デバイスプロファイルを使用して、ユーザーの情報を表示するカスタム壁紙画像を追加することもできます。たとえば、サポート連絡先情報、内部 Web サイト情報、または組織のロゴを含む画像を作成できます。Samsung Knox デバイスでは、壁紙は仕事用領域に表示されます。

デバイスプロファイルは、ユーザー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た iOS デバイスではサポートされません。

組織の通知の作成

1. 管理コンソールのメニューバーで、［設定］ > ［一般設定］ > ［組織の通知］の順にクリックします。
2. ＋ をクリックします。
3. 組織の通知 の名前を入力します。
4. オプションで、［組織の通知からコピーされたテキスト］ドロップダウンリストで既存の組織の通知を選択して、そのテキストを再利用できます。
5. ［デバイスの言語］ドロップダウンリストで、通知のデフォルト言語を選択します。
6. ［組織の通知］フィールドに、通知の内容を入力します。
7. オプションで、［追加の言語を追加］を必要に応じてクリックして、組織の通知をより多くの言語で投稿できます。
8. 組織通知を複数の言語で投稿する場合は、いずれかのメッセージの下にある［デフォルトの言語］オプションを選択して、デフォルトの言語を設定します。
9. ［保存］をクリックします。

終了したら：

- アクティベーション時に組織の通知を表示するには、組織の通知をアクティベーションプロファイルに割り当てます。
- Samsung Knox デバイスの再起動時に組織の通知を表示するには、組織の通知をデバイスプロファイルに割り当てます。

デバイスプロファイルの作成

作業を始める前に： Samsung Knox デバイスの場合、組織の通知の作成。

1. 管理コンソールのメニューバーで、［ポリシーとプロファイル］ > ［カスタム］ > ［デバイス］をクリックします。
2. ＋をクリックします。
3. プロファイルの名前と説明を入力します。
4. 次のタスクのいずれかを実行します。

タスク	手順
ユーザーがデバイスを再起動したときに、Samsung Knox デバイスに表示する組織の通知を割り当てます。	［**Android**］タブの［組織の通知を割り当てる］ドロップダウンリストで、適切な組織通知を選択します。
iOS および Android デバイスの場合、BlackBerry UEM Client に表示する組織情報を定義します。 Windows 10 の場合、デバイスのサポート情報に表示する電話番号とメールアドレスを定義します。	適切な［OS］タブで、名前、住所、電話番号、およびメールアドレスを指定します。

5. 必要に応じて、次のいずれかを実行します。

タスク	手順
Samsung Knox デバイスの仕事用領域で壁紙の画像を追加します。	**a.** ［**Android**］タブの ［仕事用領域の壁紙］セクションで、［参照］をクリックします。 **b.** 画像に移動して選択します。
監視対象の iOS デバイスに壁紙の画像を追加します。	［**iOS**］タブの［デバイスの壁紙］セクションで、次の操作のいずれかを実行します。 • ロック画面の壁紙を設定するには、［ロック画面の画像］の横にある［参照］をクリックします。画像に移動して選択します。 • ホーム画面の壁紙を設定するには、［ホーム画面の画像］の横にある［参照］をクリックします。画像に移動して選択します。

6. ［追加］をクリックします。

終了したら：

- プロファイルをユーザーおよびグループに割り当てます。
- 必要に応じて、プロファイルをランク付けします。

デバイスで位置情報サービスを使用する

位置情報サービスプロファイルを使用すると、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。また、BlackBerry UEM Self-Service を使用してデバイスを検索することもできます。iOS および Android デバイスで位置情報履歴を有効にした場合、デバイスは必須で定期的に位置情報を報告し、位置情報履歴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は、iOS、Android、および Windows 10 Mobile デバイス上で位置情報サービスを使用します。デバイスおよび利用可能なサービスに基づき、位置情報サービスは、デバイスの位置を決定するために GPS、携帯電話、および Wi-Fi ネットワークからの情報を使用することがあります。

位置情報サービスを有効にして使用するには、次の手順を実行します。

手順	アクション
1	位置情報サービスの設定。
2	位置情報サービスプロファイルの作成。
3	デバイスを検索する。
4	オプションで、監視対象の iOS デバイスの紛失モードの有効化。

位置情報サービスの設定

1. 管理コンソールのメニューバーで、［設定］ > ［一般設定］ > ［位置情報サービス］をクリックします。
2. オンプレミス環境がある場合は、［位置情報履歴の保存期間］フィールドで BlackBerry UEM でデバイスの位置情報履歴を保存する期間を指定します。デフォルトでは、UEM は 1 か月の履歴を保存します。
3. ［表示される速度単位］ドロップダウンリストで、［**km/h**］または［**mph**］をクリックします。
4. ［保存］をクリックします。

終了したら： 位置情報サービスプロファイルの作成。

位置情報サービスプロファイルの作成

作業を始める前に： 位置情報サービスの設定。

1. 管理コンソールのメニューバーで、［ポリシーとプロファイル］ > ［保護］ > ［位置情報サービス］をクリックします。
2. ＋をクリックします。
3. プロファイルの名前と説明を入力します。
4. オプションで、プロファイルを設定しないデバイスタイプのチェックボックスをオフにします。

5. 次のタスクを実行します。

タスク	手順
iOS デバイスで位置情報履歴を有効にする	［**iOS**］タブで、［デバイスの位置情報履歴を記録する］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。 BlackBerry UEM は、デバイスの位置情報に大きな変化（500 メートル以上など）があった場合、可能であれば、時間単位でデバイスの位置情報を収集します。
Android デバイスで位置情報履歴を有効にする	a. ［**Android**］タブで、［デバイスの位置情報を記録する］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。 b. ［デバイスの位置のチェック距離］フィールドで、デバイスの位置情報が更新されるまでの、デバイスの移動距離の最小間隔を指定します。 c. ［位置情報の更新頻度］フィールドで、デバイスの位置情報が更新される頻度を指定します。 デバイスの位置情報が更新される前に、距離および頻度の両条件が満たされる必要があります。

6. ［追加］をクリックします。

終了したら：

- プロファイルをユーザーおよびグループに割り当てます。管理コンソールまたは BlackBerry UEM Self-Service が地図上で iOS および Android デバイスの位置情報を表示できるようにする前に、ユーザーはプロファイルを承諾する必要があります。Windows 10 Mobile デバイスは、プロファイルを自動的に承諾します。
- 必要に応じて、プロファイルをランク付けします。
- デバイスを検索する。

デバイスを検索する

作業を始める前に： 位置情報サービスプロファイルの作成。

1. 管理コンソールのメニューバーで、［ユーザー］ > ［管理対象デバイス］をクリックします。
2. 検索するそれぞれのデバイス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. 現在の位置アイコン（）と最後の位置アイコン（）を使用して、地図上のデバイスを検索します。iOS または Android デバイスが最新の位置情報の問い合わせに応答しない場合、プロファイルで位置情報履歴が有効になっていると、地図は直近で取得した位置情報を表示します。
5. アイコンをクリックするか、アイコンの上にカーソルを置くと、緯度と経度、および場所が報告された時期などの位置情報が表示されます。
6. iOS または Android デバイスの位置情報履歴を表示するには、［位置情報履歴を表示］をクリックし、日付と時刻の範囲を選択して［送信］をクリックします。

監視対象の iOS デバイスの紛失モードの有効化

監視対象の iOS デバイスで紛失モードを有効にし、管理することができます。デバイスを紛失した場合は、紛失モードをオンにしてデバイスをロックし、表示するメッセージを設定できます。また、位置情報サービスプロファイルを使用せずにデバイスの現在位置を表示できます。

1. 管理コンソールのメニューバーで、［ユーザー］ > ［管理対象デバイス］をクリックします。
2. デバイスをクリックします。
3. ［デバイス］タブで［紛失モードをオンにする］をクリックします。
4. ［連絡先の電話番号］と［メッセージ］フィールドに、適切な情報を入力します。
5. オプションで［スライドを置換してテキストをロック解除］を選択し、表示するテキストを入力します。
6. ［有効］をクリックします。

終了したら：

- 紛失モードのデバイスを見つけるには、［デバイス］タブで［デバイスの場所を取得］をクリックします。
- 紛失モードをオフにするには、［デバイス］タブで［紛失モードをオフにする］をクリックします。

iOS デバイスのアクティベーションロックの有効化

iOS デバイスのアクティベーションロック機能を使用すると、ユーザーは、デバイスの紛失や盗難の場合に、デバイスを保護することができます。この機能が有効になっている場合、ユーザーは、［マイ iPhone を検索］を無効にするか、デバイスを消去するか、デバイスを再アクティブ化して使用するときに、Apple ID とパスワードを確認する必要があります。

デバイスが BlackBerry UEM でアクティブ化されていると、アクティベーションロックはデフォルトで無効になっています。これはデバイスごとに個々に有効にすることも、関連付けられている IT ポリシールールを使用して複数のデバイスに有効にすることもできます。アクティベーションロックを有効にすると、UEM は、ユーザーの Apple ID とパスワードがなくてもデバイスを消去して再アクティブ化できるように、ロックの解除に使用できるバイパスコードを格納します。

次の手順を実行して、各デバイスのアクティベーションロックを個別に有効にします。

作業を始める前に：

- デバイスは監視対象として設定されている必要があります。
- デバイスが iCloud アカウントに関連付けられている必要があります。
- デバイスでは［マイ iPhone を検索］または［マイ iPad を検索］が有効になっている必要があります。

1. 管理コンソールのメニューバーで、［ユーザー］をクリックします。
2. ユーザーアカウントを検索してクリックします。
3. ［デバイス］タブの［デバイスを管理］セクションで、［アクティベーションロックを有効にする］をクリックします。

終了したら：

- デバイスのアクティベーションロックを無効にするには、［アクティベーションロックを無効にする］をクリックします。IT ポリシールールを使用してアクティベーションロックを有効にした場合、このオプションを使用してロックを無効にすることはできません。
- デバイスのバイパスコードを表示するには、［ユーザー］ **>** ［**Apple** アクティベーションロック］に移動して、デバイスを検索してクリックします。

カスタムペイロードプロファイルによる iOS 機能の管理

カスタムペイロードプロファイルを使用して、既存の BlackBerry UEM ポリシーまたはプロファイルで制御されない iOS デバイスで機能を制御できます。既存の UEM ポリシーまたはプロファイルで機能を制御している場合、カスタムペイロードプロファイルが想定通りに機能しないことがあります。可能な場合は、常に既存のポリシーまたはプロファイルを使用する必要があります。

Apple Configurator を使用して Apple 設定プロファイルを作成して、UEM カスタムペイロードプロファイルに追加できます。カスタムペイロードプロファイルはユーザー、ユーザーグループ、およびデバイスグループに割り当てることができます。

たとえば、新しい iOS 更新にアップグレードするとデバイスで利用可能になる新しい機能を管理する必要があっても、UEM には、今後の UEM ソフトウェアリリースまで新しい機能の IT ポリシールールがありません。この問題を解決するため、UEM により公式にサポートされるまで、この機能を制御するカスタムペイロードプロファイルを作成できます。

カスタムペイロードプロファイルの作成

作業を始める前に： 最新バージョンの Apple Configurator をダウンロードしてインストールします。

1. Apple Configurator で Apple 設定プロファイルを作成します。
2. Apple 設定プロファイルの XML コードをコピーします。テキストをコピーするとき、次のコードサンプルで太字で示されている要素のみをコピーしてください。

```
<?xml version="1.0" encoding="UTF-8"?>
    <!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
    "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
    <plist version="1.0">
    <dict>
         <key>PayloadContent</key>
         <array>
               <dict>
                    <key>CalDAVAccountDescription</key>
                    <string>CalDAV Account Description</string>
                    <key>CalDAVHostName</key>
                    <string>caldav.server.example</string>
                    <key>CalDAVPort</key>
                    <integer>8443</integer>
                    <key>CalDAVPrincipalURL</key>
                    <string>Principal URL for the CalDAV account</string>
                    <key>CalDAVUseSSL</key>
                    </true>
                    <key>CalDAVUsername</key>
                    <string>Username</string>
                    <key>PayloadDescription</key>
                    <string>Configures CalDAV account.</string>
                    <key>PayloadDisplayName</key>
                    <string>CalDAV (CalDAV Account Description)</string>
                    <key>PayloadIdentifier</key>
                    <string>.caldav1</string>
                    <key>PayloadOrganization</key>
                    <string></string>
```

```
                    <key>PayloadType</key>
                    <string>com.apple.caldav.account</string>
                    <key>PayloadUUID</key>
                    <string>9ADCF5D6-397C-4E14-848D-FA04643610A3</string>
                    <key>PayloadVersion</key>
                    <integer>1</integer>
                </dict>
        </array>
        <key>PayloadDescription</key>
        <string>Profile description.</string>
        <key>PayloadDisplayName</key>
        <string>Profile Name</string>
        <key>PayloadOrganization</key>
        <string></string>
        <key>PayloadRemovalDisallowed</key>
        <false/>
        <key>PayloadType</key>
        <string>Configuration</string>
        <key>PayloadUUID</key>
        <string>7A5F8391-5A98-46EA-A3CF-C0D6EDC74632</string>
        <key>PayloadVersion</key>
        <integer>1</integer>
    </dict>
    </plist>
```

3. UEM 管理コンソールのメニューバーで、［ポリシーとプロファイル］ > ［カスタム］ > ［カスタムペイロード］をクリックします。
4. ＋をクリックします。
5. プロファイルの名前と説明を入力します。
6. 手順 2 でコピーした XML コードを［カスタムペイロード］フィールドに貼り付けます。
7. ［追加］をクリックします。

終了したら： プロファイルをユーザーおよびグループに割り当てます。

Android Enterprise および Android Management デバイスの工場出荷時リセット保護の管理

工場出荷時リセット保護プロファイルを使用すると、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 のアクティベーションタイプを使用してアクティベートされた組織の Android Enterprise および Android Management デバイスの工場出荷時リセット保護機能を制御できます。

工場出荷時リセット保護機能を使用する場合、工場出荷時設定にリセットされたデバイスをロック解除するには、Android デバイスのユーザーは Google アカウントの認証情報を入力する必要があります。ユーザーが Google アカウントをデバイスに追加すると、デフォルトで有効になります。このプロファイルを使用すると、デバイスを工場出荷時設定にリセットした後で、工場出荷時リセット保護を無効にしたりデバイスのロック解除に使用できるユーザーアカウントを指定したりできます。

工場出荷時のリセット保護プロファイルには、次のオプションがあります。

オプション	説明	サポートされているアクティベーションタイプ
工場出荷時のリセット保護を無効にする	誰でも紛失や盗難にあったデバイスを工場出荷時の設定にリセットして、デバイスを使用できるようになります。このオプションは、既知のユーザーが Google アカウント認証情報を忘れた場合や戻されている組織所有のデバイスをリセットする必要がある場合に便利です。	Android Enterprise
デバイスが工場出荷時設定にリセットされたときに、以前の Google アカウント認証情報を有効にして使用する	ユーザーは、工場出荷時リセット後にデバイスにすでに関連付けられている Google アカウント認証情報を使用できます。これがデフォルトの動作です。デバイスが工場出荷時設定にリセットされた場合、ユーザーはデバイスにすでに存在する Google アカウント認証情報を使用してデバイスにログインする必要があります。これにより、紛失や盗難にあったデバイスを誰かがリセットして使用することを防止できます。	Android Enterprise
デバイスを工場出荷時設定にリセットする際に Google アカウントの資格情報を有効にして指定する	工場出荷時の設定にリセットした後、ユーザーがデバイスにログインするために使用できる Google アカウント認証情報を指定できます。このオプションを使用すると、工場出荷時の設定にリセットした後、デバイスにログインできるユーザーを制御できます。BlackBerry では、デバイスのユーザーエクスペリエンスを完全に理解している場合にのみ、このオプションを使用することをお勧めします。 組織で管理対象 Google Play アカウントを使用している場合は、Google アカウントが組織のデバイスに存在せず、デバイスでは工場出荷時のリセット保護が利用できないため、このオプションを使用することをお勧めします。	Android Enterprise Android Management

デバイスを工場出荷時の初期設定にリセットするには、複数の方法があります。工場出荷時のリセット保護機能は、使用する方法に応じて反応が異なります。信頼できるリセットと信頼できないリセットの 詳細については、KB 56972 を参照してください。

工場出荷時のリセット保護プロファイルの作成

1. 管理コンソールのメニューバーで、［ポリシーとプロファイル］>［管理されているデバイス］>［保護］>［ファクトリーリセット保護］をクリックします。
2. ＋をクリックします。
3. プロファイルの名前と説明を入力します。
4. ［工場出荷時のリセット保護設定］ドロップダウンリストで、次のいずれかをクリックします。
   - 工場出荷時のリセット保護を無効にする：工場出荷時のリセット保護を無効にすると、デバイスを工場出荷時設定にリセットした後に、Google ユーザー ID の入力を求めるプロンプトが表示されません。このオプションは、Android Enterprise デバイス（仕事用と個人用 - フルコントロール および 仕事用領域のみ）でサポートされています。
   - デバイスが工場出荷時設定にリセットされたときに、以前の **Google** アカウント認証情報を有効にして使用する：これはデフォルトオプションです。信頼できない方法でユーザーがデバイスを工場出荷時設定にリセットし、かつリセットする前に Google アカウントが存在していた場合は、デバイスが工場出荷時設定にリセットされた後で、アカウントを検証する必要があります。組織で監視対象の Google アカウント構造を使用している場合、Google アカウントはデバイスに存在せず、工場出荷時のリセット保護はデバイスで使用できなくなります。このオプションは、Android Enterprise デバイス（仕事用と個人用 - フルコントロール および 仕事用領域のみ）でサポートされています。
   - デバイスを工場出荷時設定にリセットする際に **Google** アカウントの資格情報を有効にして指定する：このオプションを選択すると、信頼されない工場出荷時設定へのリセット後にデバイスにログインする際に使用する必要のある Google アカウントを指定できます。このオプションを選択した場合、ユーザーの個人用 Google アカウント資格情報は、工場出荷時設定にリセットした後は使用できません。このオプションは、Android Enterprise および Android Management デバイス（仕事用と個人用 - フルコントロール および 仕事用領域のみ）でサポートされています。

     管理対象 Google Play アカウントを使用する場合は、ユーザーに割り当てられた IT ポリシーで、［工場出荷時リセットを許可する］オプションをオフにします。これにより、デバイス設定の出荷時リセットオプションが無効になり、UEM Client の無効ボタンが無効になります。これにより、ユーザーは、UEM Client で信頼できない非アクティブ化オプションを使用して、デバイスの工場出荷時リセット保護をトリガーすることがなくなります。
5. ［デバイスを工場出荷時設定にリセットする際に **Google** アカウントの資格情報を有効にして指定する］を選択した場合は、＋をクリックし、次のいずれかの操作を行って Google アカウントを追加します（最大 20 個追加できます）。
   - Google 認証を使用するには、［**Google** 認証を使用して追加する］をクリックし、リセットされたデバイスへのログインに使用する Google アカウントにサインインします。
   - アカウントを手動で指定するには、［手動］をクリックします。メールアドレスと Google ID を指定します。Google ID を取得するには、Google 開発者の People API サイトで次の操作を行います。
     a. ［**resourceName**］に、「people/me」と入力します。
     b. ［**personalFields**］に「metadata」と入力します。
     c. ［**EXECUTE**］をクリックします。

d. ［アカウントの選択］画面で、工場出荷時のリセット保護プロファイルの設定に使用するアカウントを選択します。
e. ［**Google API Explorer** が **Google** アカウントへのアクセスをリクエストしています］画面で、［許可］をクリックします。
f. ［**People ID**］ ページで、21 桁のユーザー ID をメモします。

6. ［デバイスを工場出荷時設定にリセットする際に **Google** アカウントの資格情報を有効にして指定する］を選択し、組織に Google Workspace または Google Cloud ドメインがある場合に、工場出荷時設定へのリセット後にデバイスをロック解除できるアカウントのリストにユーザーの仕事用 Google アカウントを含める場合は、［**BlackBerry UEM** によって作成された **Google** アカウントを追加する］を選択します。
7. ［保存］をクリックします。

終了したら：

- プロファイルをユーザーおよびグループに割り当てます。
- 必要に応じて、プロファイルをランク付けします。
- デバイスで工場出荷時のリセット保護が起動すると、BlackBerry UEM でのエンタープライズアクティベーションは機能しなくなります。Android の初期設定を使用して、最初に工場出荷時のリセット保護をクリアする必要があります。『デバイスの工場出荷時リセット保護の解除』を参照してください。

デバイスの工場出荷時リセット保護の解除

デバイスで工場出荷時のリセット保護が起動すると、BlackBerry UEM でのエンタープライズアクティベーションは機能しなくなります。Android の初期設定を使用して、最初に工場出荷時のリセット保護をクリアする必要があります。

1. 任意の形式の自動アクティベーションシステム（ゼロタッチ登録や Samsung Knox Mobile Enrollment など）を使用している場合は、デバイスの初期設定を完了できるように、それらのシステムを無効にする必要があります。
2. デバイスを接続するとき、最初の Android アカウント画面で、デバイスに関連付けられている Google アカウント認証情報を入力するよう求められます。工場出荷時のリセット保護プロファイルで、特定の Google アカウントを設定した場合、ユーザーはそのアカウントに関連付けられているメールアドレスとパスワードを入力する必要があります。
3. ユーザーが Google アカウントのメールアドレスとパスワードを入力した後、このユーザーをデバイスに追加するかどうか尋ねられます。ユーザーは、デバイスで新しいユーザーを使用するオプションを選択する必要があります。
   - ゼロタッチ登録を使用していない Samsung 以外のデバイス：ユーザーはエンタープライズ Google アカウントの詳細を入力して BlackBerry UEM Client をインストールし、UEM でデバイスを再アクティブ化できます。
   - ゼロタッチ登録も Samsung Knox Mobile Enrollment も使用していない Samsung デバイス：初期設定を完了し、デバイス設定を使用してデバイスをリセットします。デバイスが再起動すると、再アクティブ化が可能になります。
   - ゼロタッチ登録または Samsung Knox Mobile Enrollment を使用しているデバイス：任意の形式の自動アクティベーションシステム（ゼロタッチ登録や Samsung Knox Mobile Enrollment など）を使用している場合は、初期設定を完了し、デバイス設定を使用してデバイスをリセットします。これでデバイスが再起動し、設定した自動アクティベーションシステムを使用できるようになります。

デバイスの認証の設定

認証をオンにすると、BlackBerry UEM は、デバイスの完全性と整合性をテストするためのチャレンジを送信します。Samsung Knox、Android、iOS、および Windows 10 デバイスで、認証をオンにすることができます。

Android デバイスおよび BlackBerry Dynamics アプリの認証設定

Android デバイスや BlackBerry Dynamics アプリの信頼性と整合性をテストするために、SafetyNet または Google Play Integrity 認証を使用して、BlackBerry UEM にチャレンジを送信させることができます。SafetyNet および Play Integrity は、組織のアプリを実行する環境のセキュリティと互換性を評価するのに役立ちます。BlackBerry の既存のルートおよび悪用検出に加えて、SafetyNet または Play Integrity 認証を使用できます。UEM コンプライアンスプロファイルを設定して割り当てて、デバイスまたはアプリが認証に失敗した場合に適切なコンプライアンスアクションを実行できます。

UEM は Play Integrity API を、それをサポートする UEM Client バージョンで使用して、アプリケーションの改ざんからの保護を強化します。Play Integrity は、Google によって決定された移行スケジュールに基づいて SafetyNet を置き換えます。SafetyNet は、UEM Client の古いバージョンで引き続きサポートされます。SafetyNet からの移行の詳細については、「Google Play：SafetyNET Attestation API からの移行」を参照してください。

次の場合に UEM は SafetyNet または Play Integrity 認証を実行します。

- BlackBerry UEM Client がインストールされている場合はデバイスのアクティベーション後。
- BlackBerry Dynamics アプリのアクティベーション中およびアクティベーション後。UEM は、古いバージョンのアプリを信頼しないことに注意してください。認証のチャレンジに合格するには、デバイスに利用可能な最新バージョンの BlackBerry Dynamics アプリが必要です。
- REST API を使用するオンデマンド。
- UEM Client がアクティブになっている場合は、デバイスが再起動されたとき。
- 指定したチャレンジ頻度を使用する定期的な認証チャレンジ。

UEM Client は、SafetyNet または Play Integrity 認証を有効にする際に必須ではありません。UEM Client は、SafetyNet または Play Integrity 認証に設定できる BlackBerry Dynamics アプリのリストに表示されませんが、UEM から認証チャレンジを受信して応答します。

ユーザーのデバイスが受信範囲外にあるか、電源がオフになっているか、バッテリーが切れている場合は、認証チャレンジに応答できません。このような状況では、UEM はデバイスのコンプライアンス状態を考慮し、割り当てられたコンプライアンスプロファイルで設定したアクションを実行します。

Android デバイスおよび BlackBerry Dynamics アプリの認証の設定

作業を始める前に： 最新バージョンの Google Play サービスがデバイスにインストールされている必要があります。

1. 管理コンソールのメニューバーで、［設定］ > ［一般設定］ > ［認証］をクリックします。
2. ［**SafetyNET** または **Play Integrity** を使用を使用する認証チャレンジを有効にする］チェックボックスをオンにします。
3. Google Compatibility Test Suite を有効にする場合は、［**CTS** プロファイルの一致を有効にする］チェックボックスをオンにします。

4. ［チャレンジの頻度］セクションで、デバイスが認証応答を BlackBerry UEM に返す必要がある頻度を指定します。デフォルトの最小値は 24 時間です。
5. ［猶予期間］セクションで、デバイスの猶予期間を指定します。認証に成功したという応答がない状態で猶予期間が終了すると、デバイスは非準拠であるとみなされ、割り当てられているコンプライアンスプロファイルで指定する操作の対象となります。
6. ［アプリの猶予期間］セクションで、BlackBerry Dynamics アプリの猶予期間を指定します。認証に成功したという応答がない状態で猶予期間が終了すると、BlackBerry Dynamics アプリは、割り当てられているコンプライアンスプロファイルで指定する操作の対象となります。猶予期間はアプリごとに適用されます。
7. 認証チャレンジの対象となる BlackBerry Dynamics アプリを指定するには、＋をクリックします。
8. アプリを選択し、［選択］をクリックします。
9. ［保存］をクリックします。

終了したら：

- デバイスに割り当てられたコンプライアンスプロファイルで、「SafetyNet または Play Integrity 認証の失敗」ルールを有効にし、デバイスまたは BlackBerry Dynamics アプリが認証に失敗したときに UEM で実行するアクションを設定します。
- 管理コンソールでは、デバイスの詳細でデバイスの認証ステータスを表示できます。

iOS デバイスの認証の設定

iOS デバイスの認証を有効にすると、許可された堅牢なデバイスのみが組織内で使用されるようになります。認証中には、デバイスのプロパティ（シリアル番号など）や識別子がスプーフィングされていないことが検証されます。この機能を使用するには監視対象外のデバイスが iOS 16 または iPadOS 16.1 以降を実行している必要があります。監視対象デバイスの場合は、iOS 17、または iPadOS 17 以降が必要です。

1. 管理コンソールのメニューバーで、［設定］ > ［一般設定］ > ［認証］をクリックします。
2. ［**iOS 16** 以降を実行している **Apple** デバイスの定期的な認証チャレンジを有効にする］チェックボックスをオンにします。
3. ［チャレンジの頻度］セクションで、デバイスが認証応答を UEM に返す必要がある頻度を指定します。最小のチャレンジ頻度は 9 日間です。
4. ［猶予期間］セクションで、デバイスの猶予期間を指定します。認証に成功したという応答がない状態で猶予期間が終了すると、デバイスは非準拠であるとみなされ、割り当てられているコンプライアンスプロファイルで指定する操作の対象となります。
5. ［保存］をクリックします。

終了したら：

- アクティベーションプロファイルで、認証をデバイスのアクティベーション中および/または定期的に実行するかどうかを指定します。管理対象デバイス認証は、MDM 制御 および ユーザーのプライバシー のアクティベーションタイプに適用されますが、ユーザーのプライバシー - ユーザー登録 アクティベーションタイプには適用されません。アクティベーションプロファイルで ユーザーのプライバシー アクティベーションタイプを選択する場合は、少なくとも 1 つの管理オプション（［VPN 管理を許可する］など）を選択する必要があります。
- コンプライアンスプロファイルで、［管理対象デバイス認証の失敗］ルールを選択し、認証に失敗したデバイスに対して実行するコンプライアンスアクションを指定します。
- 管理コンソールでは、デバイスの詳細でデバイスの認証ステータスを表示できます。

Samsung Knox デバイスの認証の設定

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

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

1. 管理コンソールのメニューバーで、［設定］ > ［一般設定］ > ［認証］をクリックします。
2. ［**KNOX Workspace** デバイスの定期的な認証チャレンジを有効にする］チェックボックスをオンにします。
3. ［チャレンジの頻度］セクションで、デバイスが認証応答を UEM に返す必要がある頻度を指定します。
4. ［猶予期間］セクションで、デバイスの猶予期間を指定します。認証に成功したという応答がない状態で猶予期間が終了すると、デバイスは非準拠であるとみなされ、割り当てられているコンプライアンスプロファイルで指定する操作の対象となります。
5. ［保存］をクリックします。

終了したら： デバイスに割り当てられたコンプライアンスプロファイルで、「ルート化された OS または失敗した Knox 認証」ルールを有効にし、デバイスが認証に失敗したときに UEM が実行するアクションを設定します。

Windows 10 デバイスの認証の設定

認証を有効にすると、BlackBerry UEM は、Windows 10 デバイスの完全性と整合性をテストするためのチャレンジを送信します。Windows 10 認証設定は、BlackBerry Desktop（BlackBerry Access + BlackBerry Work）には適用されないことに注意してください。

1. 管理コンソールのメニューバーで、［設定］ > ［一般設定］ > ［認証］をクリックします。
2. ［**Windows 10**デバイスの定期的な認証のチャレンジを有効にする］チェックボックスをオンにします。
3. ［チャレンジの頻度］セクションで、デバイスが認証応答を UEM に返す必要がある頻度を指定します。
4. ［猶予期間］セクションで、デバイスの猶予期間を指定します。認証に成功したという応答がない状態で猶予期間が終了すると、デバイスは非準拠であるとみなされ、割り当てられているコンプライアンスプロファイルで指定する操作の対象となります。
5. ［保存］をクリックします。

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

終了したら：

- デバイスに割り当てられたコンプライアンスプロファイルで、Windows デバイスの正常性認証ルールを設定し、デバイスが証明書に失敗したときに UEM が実行するアクションを設定します。
- 管理コンソールでは、デバイスの詳細でデバイスの認証ステータスを表示できます。

Windows 10 デバイス向けの Windows Information Protection の設定

次の操作を行うときに、Windows 10 デバイス向けに Windows Information Protection（WIP）を設定できます。

- デバイスで個人用データと仕事用データを分離する
- デバイス上の仕事用データのみを消去する
- ユーザーが、保護された仕事用アプリ外部で仕事用データを共有、または組織外部の人と共有できないようにする
- 他のデバイス（USB キーなど）に移動したり、共有したりする場合でも、データを保護する
- ユーザーの動作を監査し、データの漏えいを防ぐための適切なアクションを実行する

デバイスの WIP を設定するときに、WIP で保護するアプリを指定します。保護されたアプリは、仕事用ファイルの作成やアクセスで信頼されていますが、保護されていないアプリは仕事用ファイルへのアクセスがブロックされることがあります。仕事用データを共有するときにユーザーに求める動作に基づいて、保護対象アプリの保護レベルを選択できます。WIP が有効になっている場合、データ共有方法はすべて監査されます。指定したアプリは、エンタープライズ対応の場合も、非対応の場合もあります。対応アプリは仕事用データと個人用データを作成およびアクセスできます。非対応アプリは、仕事用データの作成およびアクセスだけが可能です。

1. 管理コンソールのメニューバーで、［ポリシーとプロファイル］ > ［保護］ > ［**Windows** 情報保護］をクリックします。
2. ＋をクリックします。
3. プロファイルの名前と説明を入力します。
4. プロファイル設定ごとに適切な値を設定します。『Windows 情報保護プロファイル設定』を参照してください。
5. ［追加］をクリックします。

終了したら：

- プロファイルをユーザーおよびグループに割り当てます。
- 必要に応じて、プロファイルをランク付けします。

Windows 情報保護プロファイル設定

プロファイル設定	説明
Windows 情報保護の設定	この設定では、Windows 情報保護を有効にするかどうか、および強制のレベルを指定します。 • ［オフ］：データは暗号化されず、監査ログはオフになります。 • ［サイレント］：データは暗号化され、保護データを共有しようとする操作はすべてログに記録されます。 • ［上書き］：データは暗号化され、保護データを共有しようとすると、ユーザーにプロンプトが表示されます。また、保護データを共有しようとする操作はすべてログに記録されます。 • ［ブロック］：データは暗号化され、ユーザは保護データを共有できません。また、保護データを共有しようとする操作はすべてログに記録されます。
エンタープライズ保護ドメイン名	この設定では、ユーザー ID のために組織で使用する仕事用ネットワークドメイン名を指定します。複数のドメインは、パイプ（|）で区切ります。最初のドメインは、WIP を使用するアプリによって保護するファイルにタグ付けするために、文字列として使用されます（例：example.com|example.net）。
データ復旧証明書ファイル（.der、.cer）	この設定は、デバイスでローカルに保護されていたファイルを復旧するために使用する、データ復旧証明書ファイルを指定します。ファイルは、.der または .cer ファイル拡張子が付いた PEM エンコード証明書または DER エンコード証明書にする必要があります。
BlackBerry UEM からデバイスを削除するときに Windows 情報保護設定を削除する	この設定では、デバイスが無効化されたときに WIP 設定を取り消すかどうかを指定します。WIP 設定が取り消されると、ユーザーは保護ファイルにアクセスできなくなります。
保護ファイル、およびエンタープライズコンテンツを作成できるアプリに Windows 情報保護オーバーレイを表示する	この設定では、ファイルでオーバーレイアイコンを表示するかどうかを指定します。さらにファイルまたはアプリが WIP によって保護されているかどうかを示すアプリアイコンを指定します。
仕事用ネットワークの IP 範囲	この設定では、WIP で保護されているアプリがデータを共有できる仕事用 IP アドレス範囲を指定します。ダッシュを使用して、アドレスの範囲を指定します。カンマを使用してアドレスを区切ります。
仕事用ネットワーク IP 範囲に限定する	この設定では、仕事用ネットワークの IP 範囲のみを、仕事用ネットワークの一部として受け入れるかどうかを指定します。この設定が有効になっている場合、他の仕事用ネットワークを検出しようとする操作は実行されません。

プロファイル設定	説明
エンタープライズ内部プロキシサーバー	この設定では、仕事用ネットワークの場所に接続するときに使用する内部プロキシサーバーを指定します。これらのプロキシサーバーは、エンタープライズクラウドリソース設定にリストされているドメインに接続する場合にのみ使用されます。
エンタープライズクラウドリソース	この設定では、クラウドでホストされており、保護する必要があるエンタープライズリソースドメインをリスト形式で指定します。これらのリソースから取得されるデータは、エンタープライズデータと見なされ、保護されます。
クラウドリソースドメイン	この設定では、ドメイン名を指定します。
ペアのプロキシ	この設定では、クラウドリソースとペアリングされるプロキシを指定します。クラウドリソースへのトラフィックは、指定されたプロキシサーバーを介して、エンタープライズネットワーク経由でルーティングされます（ポート 80 で）。この目的に使用するプロキシサーバーは、［エンタープライズ内部プロキシサーバー］フィールドにも設定する必要があります。
エンタープライズプロキシサーバー	この設定では、インターネットプロキシサーバーのリストを指定します。
エンタープライズプロキシサーバーに限定する	この設定では、クライアントがプロキシの設定リストを受け入れて、他のエンタープライズプロキシを検出しないようにするかどうかを指定します。
ニュートラルリソース	この設定では、仕事用または個人用リソースに使用できるドメインを指定します。
エンタープライズネットワークドメイン名	この設定では、企業の境界を構成するドメインをカンマ区切りリストで指定します。これらのドメインの 1 つからデバイスに送信されるデータは、エンタープライズデータと見なされ、保護されます。これらの場所は、エンタープライズデータを共有できる安全な送信先と見なされます。

プロファイル設定	説明

デスクトップアプリのペイロードコード	Windows 10 デバイスでアプリの起動制限を設定するために、デスクトップアプリのキーと値を指定します。設定するペイロードの種類に対して、Microsoft で定義されたキーを使用する必要があります。
	
	アプリを指定するには、AppLocker policy.xml ファイルから XML コードをコピーして、このフィールドに貼り付けます。テキストをコピーするとき、次のコードサンプルで示されている要素のみをコピーしてください。
	
	`<RuleCollection Type="Appx" EnforcementMode="Enabled">`
	`  <FilePublisherRule Id="0c9781aa-bf9f-4352-`
	`b4ba-64c25f36f558"`
	`  Name="WordMobile" Description="`
	` UserOrGroupSid="S-1-1-0" Action="Allow">`
	`  <Conditions>`
	`  <FilePublisherCondition`
	`  PublisherName="CN=Microsoft Corporation, O=Microsoft`
	` Corporation, L=Redmond, S=Washington, C=US"`
	`  ProductName="Microsoft.Office.Word" BinaryName="*">`
	`  <BinaryVersionRange LowSection="*"`
	` HighSection="*" />`
	`  </FilePublisherCondition>`
	`  </Conditions>`
	`  </FilePublisherRule>`
	`</RuleCollection>`

プロファイル設定	説明

ユニバーサル Windows プラットフォームアプリのペイロードコード	Windows 10 デバイスで WIP を設定するために、ユニバーサル Windows プラットフォームアプリのキーと値を指定します。設定するペイロードの種類に対して、Microsoft で定義されたキーを使用する必要があります。
	
	アプリを指定するには、AppLocker policy.xml ファイルから XML コードをコピーして、このフィールドに貼り付けます。テキストをコピーするとき、次のコードサンプルで示されている要素のみをコピーしてください。
	
	`<RuleCollection Type="Exe" EnforcementMode="Enabled">`
	`  <FilePathRule Id="921cc481-6e17-4653-8f75-050b80acca20"`
	`  Name="(Default Rule)`
	`  All files" Description="" UserOrGroupSid="S-1-1-0"`
	`  Action="Allow">`
	`  <Conditions>`
	`  <FilePathCondition Path="*" />`
	`  </Conditions>`
	`  </FilePathRule>`
	`  <FilePublisherRule Id="ddd0bc90-`
	`dada-4002-9e2f-0fc68e1f6af0" Name="WORDPAD.EXE,`
	`  from O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON,`
	`  C=US" Description=""`
	`  UserOrGroupSid="S-1-1-0" Action="Deny">`
	`  <Conditions>`
	`  <FilePublisherCondition PublisherName="O=MICROSOFT`
	`  CORPORATION`
	`  L=REDMOND, S=WASHINGTON, C=US" ProductName="*"`
	`  BinaryName="WORDPAD.EXE">`
	`  <BinaryVersionRange LowSection="*"`
	`  HighSection="*" />`
	`  </FilePublisherCondition>`
	`  </Conditions>`
	`  </FilePublisherRule>`
	`  <FilePublisherRule Id="c8360d06-f651-4883-`
	`abdd-9c3a95a415ff" Name="NOTEPAD.EXE,`
	`  from O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON,`
	`  C=US" Description=""`
	`  UserOrGroupSid="S-1-1-0" Action="Allow">`
	`  <Conditions>`
	`  <FilePublisherCondition PublisherName="O=MICROSOFT`
	`  CORPORATION,`
	`  L=REDMOND, S=WASHINGTON, C=US" ProductName="*"`
	`  BinaryName="NOTEPAD.EXE">`
	`  <BinaryVersionRange LowSection="*"`
	`  HighSection="*" />`
	`  </FilePublisherCondition>`
	`  </Conditions>`
	`  </FilePublisherRule>`
	`</RuleCollection>`

関連付けられている VPN プロファイル	この設定では、WIP 保護アプリの使用時に、VPN に接続するためにデバイスで使用される VPN プロファイルを指定します。この設定は、［WIP で使用されるセキュリティ保護された接続］で［VPN プロファイルの使用］を選択した場合にのみ有効です。

プロファイル設定	説明
デバイス監査ログの収集	この設定では、デバイス監査ログを収集するかどうかを指定します。

iOS または macOS デバイスの強化されたチャネルへの移行

iOS または macOS デバイスをアクティブ化すると、デフォルトでデバイスは強化されたデータチャネルに割り当てられます。現在強化されたチャネルを使用していない iOS または macOS デバイスがある場合は、これらのデバイスのリストをエクスポートし、デバイスを強化されたチャネルに移動するためのアクションを実行できます。デバイスを強化されたチャネルに移動する場合は、デバイスを再度アクティブ化する必要があります。

Apple DEP に登録されているデバイスを移動すると、デバイスは DEP 登録設定を失います。デバイスユーザーは、デバイスを工場出荷時の状態にリセットして、再度 BlackBerry UEM をアクティブにする必要があります。

作業を始める前に： すべての該当するアプリのアプリ設定で、［**BlackBerry UEM** からデバイスが削除されたらアプリをデバイスから削除する］オプションをオフにします。このオプションをクリアにせずにデバイスを強化されたチャネルへ移行しようとすると、アプリが削除され、デバイスが UEM から登録解除される場合があります。このチェックボックスをオフにしても、設定がデバイスに配信されていない場合は、アプリが削除される場合があることに注意してください。デバイスに配信されるトラッキングコマンドの 詳細については、KB 102688 を参照してください。

1. 管理コンソールのメニューバーで、［設定］ > ［移行］ > ［**iOS** の強化されたチャネル］または［設定］ > ［移行］ > ［**macOS** の強化されたチャネル］をクリックします。

   これらのメニューオプションのいずれかが表示されない場合は、 強化されたチャネルに移動する必要のある iOS または macOS デバイスが UEM 環境に存在しません。
2. 現在、強化されたチャネルを使用していないデバイスのリストをダウンロードするには、［エクスポート］をクリックします。
3. 次の操作のいずれかを実行します。

タスク	手順
複数の iOS デバイスを強化されたチャネルに移動します。	［参照］をクリックし、手順 2 でダウンロードしたファイルに移動して選択します。 共有デバイスグループに属するデバイスは、情報提供の目的でのみファイルに含まれ、この方法では強化されたチャネルには移動されません。共有デバイスグループに属するすべてのデバイスについて、ユーザーはデバイスを工場出荷時の状態にリセットしてから、再度 UEM をアクティブにする必要があります。 この方法では、一度に最大 1,000 エントリを処理できます。ダウンロードしたファイルに 1,000 を超えるエントリが含まれている場合は、それぞれ最大 1,000 エントリを含む個別のファイルに分割します。
特定の iOS デバイスを強化されたチャネルに移動します。	**a.** 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。 **b.** iOS デバイスを検索してクリックします。 **c.** ［デバイス］タブで、［**iOS** の強化されたチャネルに移行］をクリックします。 **d.** ［送信］をクリックします。

タスク	手順
macOS デバイスを強化されたチャネルに移行します。	デバイスユーザーに連絡し、UEM Self-Service を使用してデバイスを再アクティブ化するよう指示します。

商標などに関する情報

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Published in Canada