BlackBerry UEM

デバイス機能を管理する

管理

12.17

目次

デバイスの機能と動作の管理

デバイスの動作を制御するためのオプションがいくつかあります。プロファイルと IT ポリシーを使用すると、多数の機能を有効にしたり使用を制限したりすることができます。デバイスにコマンドを送信して、さまざまなアクションを開始することもできます。

同一の IT ポリシーまたはプロファイルで、さまざまなデバイスタイプに対して設定を指定してから、その IT ポリシーまたはプロファイルをユーザーアカウント、ユーザーグループ、またはデバイスグループに割り当てることができます。

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、組織内の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、デバイス上の機能を制御するルールのセットです。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。デバイスの OS によって、IT ポリシーを使用して制御できる機能のリストが決まり、デバイスのアクティベーションタイプによって IT ポリシー内のどのルールがデバイスに適用されるかが決まります。デバイスは、適用されない IT ポリシー内のルールを無視します。

BlackBerry 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。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、BlackBerry 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、BlackBerry UEM は IT ポリシーをデバイスに送信します。

BlackBerry UEM オンプレミスは毎日、ポート 3101 経由で BlackBerry Infrastructure との同期を行い、IT ポリシー情報が更新されていないかどうかを判断します。更新済みの IT ポリシー情報が使用可能な場合では、BlackBerry UEM はこの情報を取得し、デフォルトで更新を BlackBerry UEM データベースに保存します。［IT ポリシーを表示する］および［IT ポリシーを作成および編集する］権限を持っている管理者がログインすると、更新に関する通知が表示されます。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は、自動更新をオフにして、重要な更新を BlackBerry UEM に手動でインポートできます。詳細については、「IT ポリシーとデバイスメタデータの更新のインポート」を参照してください。

更新された IT ポリシー情報は、UEM Cloud インスタンス内で自動的に適用されます。

各デバイスタイプの IT ポリシールールの詳細については、『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。

デバイス機能の制限または許可

IT ポリシールールを設定すると、デバイス機能を制限または許可することができます。各デバイスタイプで利用可能な IT ポリシールールは、デバイスの OS とバージョン、およびデバイスのアクティベーションタイプによって決定されます。例えば、デバイスとアクティベーションタイプに応じて、IT ポリシールールを使用して次のことを実行できます。

- デバイスのパスワード要件またはデバイスの仕事用領域を強制する
- カメラなどのデバイス機能の使用を防止する
- Bluetooth ワイヤレステクノロジを使用する接続を制御する
- 特定のアプリの可用性を制御する
- 暗号化およびその他のセキュリティ機能を要求する

デバイスのアクティベーションタイプによって異なりますが、IT ポリシールールを使用すると、デバイス全体の制御、デバイスの仕事用領域のみの制御、または、これらの両方の制御を行うことができます。

Android 8.0 以降のデバイスでは、IT ポリシールールによって一部の機能が無効にされたときに表示される、デバイスサポートメッセージを作成できます。

各デバイスタイプの IT ポリシールールの詳細については、『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。

デバイスのパスワード要件の設定

IT ポリシールールを使用して、デバイスにパスワードの要件を設定します。パスワードの文字数と複雑さ、パスワードの有効期限、正しくないパスワードの入力試行の結果に対して、要件を設定することができます。このトピックでは、さまざまなデバイスおよびアクティベーションタイプに適用されるパスワードのルールについて説明します。

IT ポリシールールの詳細については、『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。

iOS のパスワード要件の設定

iOS および iPadOS デバイスでパスワードを必須とするかどうかを選択できます。パスワードを必須にする場合、パスワードの要件を設定できます。

メモ：iOS および iPadOS デバイスおよび一部のデバイスのパスワードルールでは、「パスコード」という用語を使用します。「パスワード」と「パスコード」は両方とも同じ意味です。

ルール	説明
デバイスのパスワードを必須にする	デバイスパスワードを設定する必要があるようにするかどうかを指定します。
単純な値を許可する	パスワードに、DEFG や 3333 などの反復または連続する文字を含めることができるようにするかどうかを指定します。
英数字値を要求する	パスワードに文字と数字の両方を含める必要があるかどうかを指定します。
パスコードの最小文字数	パスワードの最小文字数を指定します。デバイスで要求される最小値より小さい値を入力すると、デバイスの最小値が使用されます。
複雑な文字の最小文字数	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。
パスコードの最大期限	パスワードを使用できる最大日数を指定します。
最大自動ロック時間	自動ロック時間に設定できる最大値を指定します。つまり、ユーザーアクティビティのない状態で、ここに指定された分数が経過した後に、デバイスがロックされます。［なし］に設定すると、デバイスでサポートされるすべての値を使用できます。選択値がデバイスのサポート範囲に含まれていない場合、デバイスでサポートされる最も近い値が使用されます。
パスコードの履歴	最近の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数を指定します。
デバイスロックの最大猶予期間	デバイスロックの猶予期間に設定できる最大値を指定します。デバイスのロック後この時間が経過すると、ロック解除のためのパスワードが要求されます。［なし］に設定すると、デバイスですべての値を使用できます。［即座］に設定すると、デバイスのロック後、即座にパスワードが要求されます。

ルール	説明
パスワードの最大失敗試行回数	デバイスが消去される前に、間違ったパスワードを入力できる回数を指定します。
パスワードの変更を許可する（監視下のみ）	ユーザーがパスワードを追加、変更、または削除できるかどうかを指定します。

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。

macOS のパスワード要件の設定

macOS デバイスのパスワードルールをデバイスに適用するか、ユーザーに適用するか、およびパスワードを必須にするかどうかを選択できます。パスワードを必須にする場合、パスワードの要件を設定できます。

ルール	説明
IT ポリシールールの対象	このルールは、パスワードの IT ポリシールールが、割り当てられたユーザーのアカウントにのみ適用されるか、デバイス全体に適用されるかを指定します。
デバイスのパスワードを必須にする	デバイスパスワードを設定する必要があるようにするかどうかを指定します。
単純なパスワードを許可する	パスワードに、DEFG や 3333 などの反復または連続する文字を含めることができるようにするかどうかを指定します。
英数字値を要求する	パスワードに文字と数字の両方を含める必要があるかどうかを指定します。
パスワードの最小文字数	パスワードの最小文字数を指定します。
複雑な文字の最小文字数	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。
パスワードの最大期限	パスワードが期限切れになり、ユーザーが新しいパスワードを設定する必要が生じるまでパスワードを使用できる最大日数を指定します。
最大自動ロック時間	ユーザーアクティビティのない時間が最大何分経過したらデバイスをロックするかを指定します。［なし］に設定すると、ユーザーは任意の値を選択できます。
パスワードの履歴	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。
デバイスロックの最大猶予期間	デバイスロックの猶予期間に設定できる最大値を指定します。デバイスのロック後この時間が経過すると、ロック解除のためのパスワードが要求されます。
パスワードの最大失敗試行回数	デバイスがワイプされる前に、間違ったパスワードを入力できる回数を指定します。

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 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。
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。

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 - 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
パスワードの複雑さ（グローバル（すべての Android デバイス））	デバイスパスワードの最低限の複雑さのレベルを指定します。次のいずれかのオプションを選択できます。 • ［低］：パターンと、繰り返しや連続した値のある PIN を許可します。 • ［中］：繰り返しや連続した値がなく、長さが 4 文字以上ある PIN、または長さが 4 文字以上あるパスワードを必要とします。 • ［高］：繰り返しや連続した値がなく、長さが 8 文字以上ある PIN、または長さが 6 文字以上あるパスワードを必要とします。 メモ： パスワードの複雑さを［高］に設定し、IT ポリシーの［仕事用プロファイル（すべての Android デバイス）］セクションでパスワードの複雑さを［中］に設定すると、グローバル設定が仕事用プロファイル設定よりも優先され、ユーザーは複雑さの高いパスワードを設定する必要があります。

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。
パスワードの複雑さ（仕事用プロファイル（すべての Android デバイス））	デバイスパスワードの最低限の複雑さのレベルを指定します。次のいずれかのオプションを選択できます。 • ［低］：パターンと、繰り返しや連続した値のある PIN を許可します。 • ［中］：繰り返しや連続した値がなく、長さが 4 文字以上ある PIN、または長さが 4 文字以上あるパスワードを必要とします。 • ［高］：繰り返し値または連続値がなく、長さが 8 以上の PIN、または長さが 6 以上のパスワードが必要です。 メモ：パスワードの複雑さを［中］または［低］に設定し、IT ポリシーの［グローバル（すべての Android デバイス）］セクションでパスワードの複雑さを［高］に設定すると、グローバル設定が仕事用プロファイル設定よりも優先され、ユーザーは複雑さの高いパスワードを設定する必要があります。
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。

ルール	説明
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。
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。
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。

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。

Android ：**Knox MDM** のパスワードルール

Knox MDM 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、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 - フルコントロール （Samsung Knox）
- MDM 制御 （Knox MDM）

これらのアクティベーションタイプのデバイスでは、デバイスのパスワードが必須になります。

Android Enterprise のアクティベーションタイプで、デバイスをアクティベーションして Knox Platform for Enterprise を使用する場合は、Android グローバルパスワードルールを使用してください。Samsung Knox アクティベーションタイプと Knox MDM IT ポリシールールは、将来のリリースで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：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。 • 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。
パスワードの最小文字数	パスワードの最小文字数を指定します。パスワードは 4 文字以上にする必要があります。
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。

ルール	説明
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複雑な文字種の最小数	複雑なパスワードに含める必要のある複雑な文字（数字や記号など）の最小数を指定します。この値を 1 に設定すると、数字が 1 文字以上必要になります。2 以上の値を設定すると、数字と記号がそれぞれ 1 文字以上必要になります。
文字列の最大長さ	英字、英数字、または複雑なパスワードで許可するアルファベット順の英字の最大長さを指定します。たとえば、この長さを 5 に設定すると、連続する英字「abcde」は許可されますが、「abcdef」は許可されません。0 に設定すると、アルファベット順に制限は適用されません。
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期間が最大でどのぐらい経過したらデバイスをロック（キーガードロック）するかを指定します。複数の EMM ソリューションで管理されているデバイスでは、アクティビティのない期間として最低値が使用されます。パスワードを使用しているデバイスでは、パスワードでデバイスをロック解除する必要があります。0 に設定すると、アクティビティがない場合のタイムアウトがデバイスに適用されません。
パスワードの最大失敗試行回数	デバイスがワイプされる前に、間違ったパスワードを入力できる回数を指定します。
パスワード履歴の制限	最近の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。
パスワード有効期限のタイムアウト	デバイス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、パスワードは期限切れになり、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。
パスワードの表示を許可する	ユーザーがデバイスパスワードを入力するときに、パスワードを表示できるかどうかを指定します。このルールが選択されていない場合、ユーザーとサードパーティアプリは表示設定を変更できません。
指紋認証を許可する	デバイスの指紋認証をユーザーが使用できるかどうかを指定します。

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 ： **Knox Premium - Workspace** パスワードルール

Knox Premium - Workspace 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 （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）

これらのアクティベーションタイプのデバイスでは、仕事用領域のパスワードが必須になります。

アクティベーションタイプが Android Enterprise のデバイスをアクティベーションして Knox Platform for Enterprise を使用する場合は、Android 仕事用のパスワードルールを使用してください。Samsung Knox アクティベーションタイプと Knox Premium IT ポリシールールは、今後のリリースで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。

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。 • 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。 • 複雑な数字：パスワードには、反復（例：4444）や連続（例：1234、4321、2468）がない状態で、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複雑な文字種の最小数	複雑なパスワードに含める必要のある複雑な文字（数字や記号など）の最小数を指定します。数字と記号を各 1 文字以上含めて、3 文字以上の複雑な文字が必要です。
文字列の最大長さ	英字、英数字、または複雑なパスワードで許可するアルファベット順の英字の最大長さを指定します。たとえば、この長さを 5 に設定すると、連続する英字「abcde」は許可されますが、「abcdef」は許可されません。0 に設定すると、アルファベット順に制限は適用されません。
パスワードの最小文字数	パスワードの最小文字数を指定します。Knox Workspace で要求される最小値より小さい値を入力すると、Knox Workspace の最小値が使用されます。
ロックまでの最大アクティビティなし時間	仕事用領域でユーザーアクティビティのない期間が最大どのぐらい経過したら仕事用領域をロックするかを指定します。0 に設定すると、アクティビティがない場合のタイムアウトが仕事用領域に適用されません。
パスワードの最大失敗試行回数	仕事用領域が消去される前に、間違ったパスワードを入力できる回数を指定します。0 に設定すると、ユーザーが間違ったパスワードを入力できる回数が無制限になります。
パスワード履歴の制限	最近の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。

ルール	説明
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日数を指定します。指定された日数が経過すると、パスワードは期限切れとなるため、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。
新しいパスワードで変更される文字の最小数	以前のパスワードと比較して新しいパスワードで変更されている必要がある文字の最小数を指定します。0に設定すると、制限は適用されません。
キーガードのカスタマイズを許可する	デバイスが、信頼エージェントなどのキーガードのカスタマイズを使用できるようにするかどうかを指定します。このルールが選択されていない場合、キーガードのカスタマイズはオフになります。
キーガードの信頼エージェントを許可する	ユーザーが、アクティビティなしタイムアウトの最大時間が経過した後に、仕事用領域がロック解除された状態を 2 時間維持できるようにするかどうかを指定します。アクティビティなしタイムアウトの時間を設定していない場合は、ユーザーはデフォルトでこの操作を実行できます。
パスワードの表示を許可する	ユーザーがデバイスパスワードを入力するときに、パスワードを表示できるかどうかを指定します。このルールが選択されていない場合、ユーザーとサードパーティアプリは表示設定を変更できません。
ツーファクター認証を強制する	ユーザーが仕事用領域にアクセスするときにツーファクター認証を要求するかどうかを指定します。たとえば、このルールを使用して、ユーザーに指紋とパスワードを使用する認証を要求できます。
指紋認証を許可する	ユーザーが仕事用領域にアクセスするときに指紋認証を使用できるかどうかを指定します。

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。

Windows 10 のパスワード要件の設定

Windows 10 デバイスでパスワードを必須とするかどうかを選択できます。パスワードを必須にする場合、パスワードの要件を設定できます。

ルール	説明
デバイスのパスワードを必須にする	デバイスパスワードを設定する必要があるようにするかどうかを指定します。
単純なパスワードを許可する	パスワードに、DEFG や 3333 などの反復または連続する文字を含めることができるようにするかどうかを指定します。
パスワードの最小文字数	パスワードの最小文字数を指定します。パスワードは 4 文字以上にする必要があります。

ルール	説明
パスワードの複雑さ	パスワードの複雑さを指定します。次のオプションを選択できます。 • 英数字：パスワードに文字と数字を含める必要があります。 • 数字：パスワードには数字のみを含める必要があります。
文字タイプの最大数	英数字パスワードに含める必要のある文字タイプの最小数を指定します。次のオプションから選択します。 1. 数字を必須とする 2. 数字と小文字のアルファベットを必須とする 3. 数字、小文字のアルファベット、大文字を必須とする 4. 数字、小文字のアルファベット、大文字のアルファベット、特殊文字を必須とする Windows 10 コンピューターとタブレットでは、パスワード文字の要件は、この設定ではなく、ユーザーアカウントの種類によって決定されます。
パスワードの有効期限	パスワードを使用できる最大日数を指定します。0 に設定すると、パスワードは期限切れになりません。
パスワードの履歴	最近の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。
パスワードの最大失敗試行回数	デバイスが消去される前に、間違ったパスワードを入力できる回数を指定します。0 に設定すると、ユーザーが間違ったパスワードを入力した回数にかかわらず、デバイスは消去されません。 このルールは、Windows 10 コンピューターやタブレットなど、複数のユーザーアカウントを使用できるデバイスには適用されません。
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期間がどのぐらい経過したらデバイスをロックするかを指定します。0 に設定すると、デバイスは自動ではロックされません。
パスワードなしでのアイドルからの復帰を許可する	アイドル猶予期間の終了時にパスワードの入力を要求するかどうかを指定します。このルールを選択すると、ユーザーはデバイスでパスワードの猶予期間タイマーを設定できます。このルールは、Windows 10 コンピューターおよびタブレットには適用されません。

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。

IT ポリシーの作成と管理

デフォルトの IT ポリシーを使用するか、カスタム IT ポリシー（たとえば、組織内の異なるユーザーグループまたはデバイスグループに IT ポリシールールを指定するため）を作成することができます。デフォルトの IT ポリシーを使用予定の場合は、それらを見直して、必要に応じて、ルールが組織のセキュリティ標準を確実に満たすように更新する必要があります。

IT ポリシーの作成

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］ > ［IT ポリシー］をクリックします。
3. ＋をクリックします。
4. IT ポリシーの名前と説明を入力します。
5. 組織内の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。
   ルールの名前の上にマウスを置くと、ヘルプヒントが表示されます。
6. ［追加］をクリックします。

終了したら： IT ポリシーのランク付け

IT ポリシーをコピー

既存の IT ポリシーをコピーして、組織内のさまざまなグループ用にカスタム IT ポリシーをすばやく作成することができます。

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］ > ［IT ポリシー］をクリックします。
3. コピーする IT ポリシーの名前をクリックします。
4.  をクリックします。
5. 新しい IT ポリシーの名前と説明を入力します。
6. 各デバイスタイプの適切なタブで変更を加えます。
7. ［追加］をクリックします。

終了したら： IT ポリシーのランク付け

IT ポリシーのランク付け

ランキングは、次のシナリオで、BlackBerry UEM がデバイスに送信する IT ポリシーを決定するために使用されます。

- ユーザーが、異なる IT ポリシーを持つ複数のユーザーグループのメンバーである。
- デバイスが、異なる IT ポリシーを持つ複数のデバイスグループのメンバーである。

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］ > ［IT ポリシー］をクリックします。
3. ↓↑をクリックします。
4. 矢印を使用して、IT ポリシーを上下に移動してランキングします。
5. ［保存］をクリックします。

IT ポリシーの表示

IT ポリシーに関する次の情報を表示できます。

- 各デバイスタイプに固有の IT ポリシールール
- IT ポリシーが割り当てられている（直接および間接）ユーザーアカウントのリストと数
- IT ポリシーが割り当てられている（直接）ユーザーグループのリストと数

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］ > ［**IT** ポリシー］をクリックします。
3. 表示する IT ポリシーの名前をクリックします。

IT ポリシーの変更

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］ > ［**IT** ポリシー］をクリックします。
3. 変更する IT ポリシーの名前をクリックします。
4.  をクリックします。
5. 各デバイスタイプの適切なタブで変更を加えます。
6. ［保存］をクリックします。

終了したら： 必要に応じて、IT ポリシーのランキングを変更します。

ユーザーアカウントまたはユーザーグループからの IT ポリシーの削除

IT ポリシーがユーザーアカウントまたはユーザーグループに直接割り当てられている場合は、ユーザーまたはグループから IT ポリシーを削除できます。IT ポリシーがユーザーグループによって間接的に割り当てられている場合は、グループから IT ポリシーを削除するか、またはグループからユーザーアカウントを削除することができます。ユーザーグループから IT ポリシーを削除すると、IT ポリシーは選択したグループに属する各ユーザーから削除されます。

メモ： デフォルトの IT ポリシーは、ユーザーに直接割り当てられている場合にのみ、ユーザーアカウントから削除できます。

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］ > ［**IT** ポリシー］をクリックします。
3. ユーザーアカウントまたはユーザーグループから削除する IT ポリシーの名前をクリックします。
4. 次のタスクのいずれかを実行します。

タスク	手順
ユーザーアカウントから IT ポリシーを削除する	**a.** ［ユーザーに割り当て済み］タブをクリックします。 **b.** 必要に応じて、ユーザーアカウントを検索します。 **c.** IT ポリシーを削除するユーザーアカウントを選択します。 **d.** をクリックします。
ユーザーグループから IT ポリシーを削除する	**a.** ［グループに割り当て済み］タブをクリックします。 **b.** 必要に応じて、ユーザーグループを検索します。 **c.** IT ポリシーを削除するユーザーグループを選択します。 **d.**  をクリックします。

IT ポリシーを削除する

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、BlackBerry 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。

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］ > ［**IT** ポリシー］をクリックします。
3. 削除する IT ポリシーのチェックボックスをオンにします。
4. をクリックします。
5. ［削除］をクリックします。

IT ポリシーのエクスポート

IT ポリシーを監査目的で .xml ファイルにエクスポートすることができます。

メモ：

IT ポリシーに関連付けられているプロファイルはエクスポートされません。

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］ > ［**IT** ポリシー］をクリックします。
3. エクスポートする IT ポリシーのチェックボックスをオンにします。
4. をクリックします。
5. ［次へ］をクリックします。
6. ［エクスポート］をクリックします。

BlackBerry UEM が割り当てる IT ポリシーを選択する方法

BlackBerry UEM は、1 つの IT プロファイルのみをデバイスに送信し、事前定義されたルールを使用して、ユーザーとユーザーがアクティブ化するデバイスにどの IT プロファイルを割り当てるかを決定します。

割り当て先	ルール
ユーザーアカウント （［概要］タブの表示）	1. ユーザーアカウントに直接割り当てられた IT ポリシーは、ユーザーグループによって間接的に割り当てられた IT ポリシーより優先されます。 2. ユーザーが、異なる IT ポリシーを持つ複数のユーザーグループのメンバーである場合、BlackBerry UEM はランキングが最高の IT ポリシーを割り当てます。 3. IT ポリシーが直接、またはユーザーグループメンバーシップを通じてユーザーアカウントに割り当てられていない場合は、デフォルトの IT ポリシーが割り当てられます。
デバイス （デバイスタブの表示）	デフォルトでは、デバイスは BlackBerry UEM がデバイスをアクティブ化したユーザーに割り当てた IT ポリシーを継承します。デバイスがデバイスグループに属する場合は、次のルールが適用されます。 1. デバイスグループに割り当てられた IT ポリシーは、BlackBerry UEM がユーザーアカウントに割り当てた IT ポリシーより優先されます。 2. デバイスが、異なる IT ポリシーを持つ複数のデバイスグループのメンバーである場合、BlackBerry UEM はランキングが最高の IT ポリシーを割り当てます。

次のいずれかの操作を実行した場合、BlackBerry UEM で IT ポリシーの競合を解決する必要が生じる場合があります。

- IT ポリシーをユーザーアカウント、ユーザーグループ、またはデバイスグループに割り当てる
- IT ポリシーをユーザーアカウント、ユーザーグループ、またはデバイスグループから削除する
- IT ポリシーのランキングを変更する
- IT ポリシーを削除する
- ユーザーグループメンバーシップを変更する（ユーザーアカウントとネストされたグループ）
- デバイス属性を変更する
- デバイスグループメンバーシップを変更する
- ユーザーグループまたはデバイスグループを削除する

IT ポリシーとデバイスメタデータの更新のインポート

BlackBerry は、IT ポリシーとデバイスメタデータの更新を BlackBerry UEM のインストール環境に定期的に送信し、デバイスおよび OS ベンダーからの更新に関する情報を提供します。

たとえば、デバイスベンダーが新しいデバイスモデルをリリースすると、BlackBerry は更新されたデバイスメタデータを BlackBerry UEM のインストール環境に送信します。これにより、アクティベーション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が含めて、プロファイルによる許可や制限ができるようにします。Apple、Google、または Microsoft が OS の更新をリリースすると、新しい IT ポリシーパックが BlackBerry UEM UEM のインストール環境に送信され、OS 更新の新機能を制御できるようになることがあります。

デフォルトでは、BlackBerry UEM はこれらの更新を自動的に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は、自動更新をオフにして、重要な更新を BlackBerry UEM に手動でインポートできます。

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。

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、新しい更新が利用可能になったときに通知を送信します。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。

作業を始める前に： 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. メニューバーで［設定］をクリックします。
2. ［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。
3. 次の操作のいずれか、または両方を実行します。
   - 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。
4. 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を探し、ファイルを見つけたら［開く］をクリックします。

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。

［デバイス管理者設定］画面に表示される管理者サポートメッセージを指定することもできます。たとえば、組織が仕事用プロファイル内のアプリとデータを監視および管理できるという免責事項を表示できます。

複数の言語で作業するユーザーが組織にいる場合は、別の言語でサポートメッセージを追加し、使用可能な言語のいずれかを使用しないデバイスで表示するデフォルト言語を指定できます。

デバイスサポートメッセージの作成

デバイスサポートメッセージは Android 8.0 以降のデバイスでサポートされています。

1. メニューバーで［設定］**>**［一般設定］をクリックします。
2. ［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。
3. ［カスタムデバイスサポートメッセージ］タブで［追加］をクリックします。
4. 通知を表示する言語を選択します。
5. ［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通知を入力します。このメッセージには、最大 200 文字まで使用できます。
6. 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。
7. 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、言語ごとに手順 4〜6 を繰り返します。
8. 複数の言語でメッセージを追加した場合は、デバイスに表示する言語の横にある［デフォルトの言語］を選択します。たとえば、英語とフランス語が使用可能な言語で、英語がデフォルトの言語である場合は、英語のメッセージがドイツ語を使用するデバイスに表示されます。
9. ［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次の情報を指定します。

- デバイスを非準拠と見なす条件
- コンプライアンス条件に違反した場合にユーザーが受信するメールメッセージおよびデバイス通知
- ユーザーが問題を修正しない場合に実行される操作。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などが含まれます。

Samsung Knox デバイスの場合、制限付き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。ただし、BlackBerry 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 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。

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 ：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、新しいメールテンプレートを作成します。詳細については、「コンプライアンス用メール通知のテンプレートの作成」を参照してください。

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. 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. ［コンプライアンス］ > ［コンプライアンス］をクリックします。
3. ＋をクリックします。
4. コンプライアンスプロファイルの名前と説明を入力します。
5. デバイスが非準拠の場合にユーザーへ通知メッセージを送信する場合は、次のいずれかの操作を実行します。

- ［違反が検出されたときに送信されるメール］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。デフォルトのコンプライアンスメールを表示するには、［設定］ > ［一般設定］ > ［メールテンプレート］をクリックします。
- ［施行間隔］ドロップダウンリストで、コンプライアンスチェックの頻度を選択します。この設定は BlackBerry Dynamics のコンプライアンスチェックにのみ適用されます。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。
- ［違反が検出されたときに送信されるデバイス通知］を展開します。必要に応じてメッセージを編集します。

変数を使用して、通知にユーザー、デバイス、、およびコンプライアンス情報を入力できます。詳細については、「変数」を参照してください。

6. 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、「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。
7. ［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。

コンプライアンスプロファイル設定

コンプライアンスプロファイルは、以下のデバイスタイプでサポートされています。

- iOS
- macOS
- Android
- Windows

共通：コンプライアンスプロファイル設定

iOS、iPadOS、および **Android** デバイス

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。

共通：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、BlackBerry 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、BlackBerry 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。 使用できる値： • コンプライアンス用のプロンプト • 即時強制アクション

共通：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、BlackBerry 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方法を指定します。 使用できる値 • デバイス通知 • メールとデバイスの通知 BlackBerry Dynamics アプリはユーザーにメール通知を送信しません。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。 デバイスに適用されるコンプライアンスルールの場合、デフォルト値は「メールとデバイスの通知」、BlackBerry Dynamics アプリにのみ適用されるコンプライアンスルールの場合、デフォルト値は「デバイス通知」です。 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。 デフォルト値は［3］です。 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。 デフォルト値は［4 時間］です。 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。

共通：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 BlackBerry UEM が実行するアクションを指定します。 使用できる値： • 監視とログ：BlackBerry 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：iOS、iPadOS、macOS、Android、および Windows デバイスで、このオプションは、ユーザーがデバイスから仕事用リソースとアプリケーションにアクセスできないようにします。データとアプリは、デバイスから削除されません。 メモ：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：iOS、iPadOS、Android、および Windows デバイスで、「応答不能」ルールに違反している場合、デバイスを BlackBerry UEM から無効化できます。 デフォルト値は「監視とログ」です。 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。 「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、BlackBerry UEM は［仕事用データのみを削除］と同じ操作を実行します。 仕事用領域だけを含む Samsung Knox Workspace デバイスの場合、［仕事用データのみを削除］、［すべてのデータを削除］、または［サーバーから削除］を選択すると、すべてのデータがデバイスから削除されます。 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。

共通：コンプライアンスプロファイル設定	説明
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。 使用できる値： • 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：BlackBerry 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。 デフォルト値は「監視とログ」です。

Windows 10 デバイスおよび **macOS** デバイス

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。

共通：コンプライアンスプロファイル設定	説明
強制アクション	この設定は、準拠していないデバイスで BlackBerry UEM が実行するアクションを指定します。 使用できる値： • コンプライアンス用のプロンプト • 信頼しない：Windows デバイスで、このオプションは、ユーザーがデバイスから仕事用リソースとアプリケーションにアクセスできないようにします。データとアプリは、デバイスから削除されません。 メモ：信頼しないは、BlackBerry Dynamics アプリでサポートされていません。 • 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：Windows デバイスで、「応答不能」ルールに違反している場合、デバイスを BlackBerry UEM から無効化できます。 • なし：コンプライアンス違反を識別しますが、アクションは実行しません。 デフォルト値は「コンプライアンス用のプロンプト」です。

共通：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	指定できる値は次のとおりです。 • メール通知 • デバイス通知 • 両方 デフォルト値は［両方］です。 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。 デバイス通知は Windows 10 デバイスではサポートされません。
プロンプトの回数	この設定は、ユーザーに違反を修正するように求める回数を指定します。 デフォルト値は［3］です。 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。 デフォルト値は［4 時間］です。 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。
プロンプトの間隔の満了時のアクション	この設定は、［プロンプトの回数］で定義されたプロンプトの合計回数をユーザーが受信し、違反を修正しないときに行われるアクションを定義します。 使用できる値： • None • 信頼しない：Windows デバイスで、このオプションは、ユーザーがデバイスから仕事用リソースとアプリケーションにアクセスできないようにします。データとアプリケーションは、デバイスから削除されません。 メモ：信頼しないは、BlackBerry Dynamics アプリでサポートされていません。別の強制アクションを使用します。 • 仕事用データのみを削除 • すべてのデータを削除する デフォルト値は［信頼しない］です。 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。

共通：コンプライアンスプロファイル設定	説明
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。 使用できる値： • BlackBerry Dynamics のアプリデータの削除 • BlackBerry Dynamics アプリの実行を許可しない デフォルト値は［BlackBerry Dynamics アプリデータを削除する］です。

iOS ：コンプライアンスプロファイル設定

コンプライアンスルールを選択する場合、利用可能な操作の説明については「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。

これらの設定は iPadOS デバイスにも適用されます。

iOS ：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、ユーザーは、設定した強制アクションに関係なく、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することもできなくなります。
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。 この設定を選択している場合、割り当てられていない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。 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を行ったデバイスでは、この設定は有効ではありません。
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。 この設定を選択している場合、必須アプリが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［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ケーションがリストに表示されます。

iOS ：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。 次のいずれかのオプションを選択できます。 • 選択されたデバイスモデルを許可する • 選択されたデバイスモデルを許可しない 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。
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 BlackBerry 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。
最終接続時刻	この設定では、デバイスが BlackBerry UEM と無応答の状態を続けられる日数を指定します。 この設定は、［デバイスの応答がありません］設定が選択されている場合にのみ有効です。
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。

iOS ：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 BlackBerry 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 BlackBerry 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なる前に、デバイスが BlackBerry 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。
検出された BlackBerry Dynamics アプリの画面キャプチャ	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、［期間の長さ］フィールドで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。

iOS ：コンプライアンスプロファイル設定	説明
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、制限されたアプリを定期的にチェックするための BlackBerry UEM のコンプライアンスルールが作成されます。 アプリを制限するには、次のタスクのいずれかを完了します。 • 制限付きアプリのリストからアプリを選択します。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。 次の操作のいずれかを実行します。 • アプリ名を使用してアプリを選択するには、アプリリストオプションから［アプリを選択］をクリックします。 • アプリパッケージ ID を使用してアプリを選択するには、［アプリパッケージ ID を指定］オプションをクリックします。一般のアプリを追加する場合は、パッケージ ID を使用しないでください。代替の方法としては、制限付きアプリのリストに一般のアプリを追加して、次に［使用可能なアプリのリストから選択］オプションを使用してアプリを選択します。 • 組み込みアプリを選択します（監視対象デバイスのみ）。 リストからアプリを削除するには、✕をクリックします。 この設定を選択している場合、制限付き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ケーションがリストに表示されます。 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。
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、コンプライアンスルールを作成して、ユーザーデバイスへのインストールを許可するアプリのリストを指定します。他のすべてのアプリは許可されません。 特定のアプリを許可するには、次のいずれかのタスクを完了します。 • 制限付きアプリのリストからアプリを選択します。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。 • 組み込みアプリを選択します。 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。リストからアプリを削除するには、✕をクリックします。 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

コンプライアンスルールを選択する場合、利用可能な操作の説明については「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。

macOS ：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。 次のいずれかのオプションを選択できます。 • 選択されたデバイスモデルを許可する • 選択されたデバイスモデルを許可しない 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 BlackBerry 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 BlackBerry 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なる前に、デバイスが BlackBerry 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

コンプライアンスルールを選択する場合、利用可能な操作の説明については「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。

Android ：コンプライアンス設定	説明
ルート化された OS または失敗した Knox の認証	この設定により、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。ユーザーまたは攻撃者が Android OS のルートレベルへのアクセス権を得たときに、デバイスはルート化されます。このルールは、デバイスのルート化された状態に適用されます。UEM Client、BlackBerry Dynamics SDK、または Knox 認証が検出します。 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。 ［ルート化された OS または失敗した Knox の認証］に対するコンプライアンスルールを設定した場合、［BlackBerry Dynamics アプリのアンチデバッグを有効にする］を選択すると、BlackBerry Dynamics ランタイムがアクティブなデバッグツールを検出すると、BlackBerry Dynamics アプリを停止します。
SafetyNet 認証の失敗	この設定では、デバイスが SafetyNet 認証されなかっ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 認証を使用する場合、BlackBerry UEM は、組織環境内の Android デバイスとアプリの完全性と整合性をテストするチャレンジを送信します。 これらの設定を有効にするには、管理コンソール（［設定］ > ［認証］ > ［SafetyNet 認証の頻度］）で SafetyNet 認証機能を有効にする必要があります。 SafetyNet 認証の設定の詳細については、「SafetyNet を使用した Android デバイスおよび BlackBerry Dynamics アプリの認証設定」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［管理されているデバイス］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ケーションがリストに表示されます。 Android Enterprise デバイスと 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。

Android ：コンプライアンス設定	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［管理されているデバイス］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ケーションがリストに表示されます。 Android Enterprise 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。 次のいずれかのオプションを選択できます。 • 選択されたデバイスモデルを許可する • 選択されたデバイスモデルを許可しない 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。
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 BlackBerry 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 BlackBerry UEM と無応答の状態を続けられる日数を指定します。

Android ：コンプライアンス設定	説明
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。 この設定は、デバイスおよび BlackBerry Dynamics SDK 6.0 以降で開発された BlackBerry Dynamics アプリに対して有効です。
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 BlackBerry 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 BlackBerry 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なる前に、デバイスが BlackBerry 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。

Android ：コンプライアンス設定	説明
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 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。 Android Enterprise 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を使用する Samsung Knox 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。このオプションは、Android 10 以前のデバイスでのみサポートされています。 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、制限付きアプリが 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［管理されているデバイス］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ケーションがリストに表示されます。 メモ： Android Enterprise - 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デバイスをアクティベーションし、このオプションを使用してデバイスの個人側のアプリを無効にした場合、デバイスを Android 10 から Android 11 にアップグレードすると、デバイスを再度アクティベーションしない限り、これらのアプリは永続的に無効になります。詳細については、support.blackberry.com/community にアクセスし、記事 76852 を参照してください。
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

コンプライアンスルールを選択する場合、利用可能な操作の説明については「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。

Windows ：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。

Windows ：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、この設定で指定されている制限された 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、この設定で指定されている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。 使用できる値： • 選択されたデバイスモデルを許可する • 選択されたデバイスモデルを許可しない 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 BlackBerry 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 BlackBerry 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 BlackBerry 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。

Windows ：コンプライアンスプロファイル設定	説明
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。
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。
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。

Windows ：コンプライアンスプロファイル設定	説明
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。
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。
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。
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。
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。

BlackBerry Dynamics のコンプライアンスプロファイルの管理

BlackBerry Dynamics のコンプライアンスプロファイルは、Good Control と BlackBerry 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、BlackBerry 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、BlackBerry 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、ユーザーが割り当てられる可能性がある BlackBerry 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。

設定	説明
脱獄された OS	この設定では、OS の改変、承認されていないアプリのインストール、昇格した権限の取得などを目的として、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た場合に備えて、対応アクションを指定します。また、脱獄された OS が使用される場合に備えて、BlackBerry Dynamics アプリに対するアクションを指定します。
OS バージョンの確認	この設定では、許可する、および制限する OS のバージョンを指定します。また、制限付き OS がデバイスにインストールされた場合に備えて、BlackBerry Dynamics アプリに対するアクションを指定します。

設定	説明
ハードウェアモデルの確認	この設定では、許可する、および制限するハードウェアモデルを指定します。また、制限付きのハードウェアモデルが使用された場合に備えて、BlackBerry Dynamics アプリに対するアクションを指定します。
BlackBerry Dynamics ライブラリのバージョンの確認	この設定では、使用できる BlackBerry Dynamics ライブラリを指定します。また、デバイスで許されていないライブラリバージョンが使用された場合に備えて、BlackBerry Dynamics アプリに対するアクションを指定します。
接続の確認	この設定では、デバイスが所定の日数の間 BlackBerry UEM に接続する必要があるかどうかを指定します。また、デバイスが BlackBerry UEM に接続しなかった場合に備えて、BlackBerry Dynamics アプリに対するアクションを指定します。 ［認証委任アプリの基本接続間隔］サブ設定では、認証委任アプリとして設定されたアプリで接続間隔を管理するかどうかを指定します。認証委任を使用して接続間隔を管理している場合、使用頻度の低いアプリが BlackBerry UEM に接続していない場合でも、これらのアプリがブロックまたは消去されることはありません。

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。
- デバイスを組織内の別のユーザーに再配布する場合や、デバイスが紛失または盗難された場合に、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。

デバイスへのコマンド送信

作業を始める前に：

デバイスからデータを削除するコマンドに対して、BlackBerry UEM で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。

1. メニューバーで、［ユーザー］ > ［管理対象デバイス］をクリックします。
2. ユーザーアカウントを検索します。
3. 検索結果で、ユーザーアカウントの名前をクリックします。
4. デバイスのタブをクリックします。
5. ［デバイスを管理］ウィンドウで、デバイスに送信するコマンドを選択します。

一括コマンドの送信

ユーザーリストからユーザーまたはデバイスを選択して、一括コマンドを送信することで、複数のユーザーアカウントまたはデバイスにコマンドを同時に送信することができます。

作業を始める前に： デバイスからデータを削除するコマンドに対して有効期限を設定する場合、「コマンドの有効期限の設定」を参照してください。

1. メニューバーで、［ユーザー］ > ［管理対象デバイス］をクリックします。
2. 必要に応じて、ユーザーリストをフィルターします。
3. 次の操作のいずれかを実行します。
   - ユーザーリストの一番上にあるチェックボックスをオンにして、リストですべてのユーザーおよびデバイスを選択します。

- 含めるそれぞれのユーザーおよびデバイスのチェックボックスをオンにします。複数のユーザーを選択するには、Shift キーを押しながらクリックします。

4. メニューから、次のアイコンのいずれかをクリックします。

アイコン	説明
	デバイスを見つける 一度に選択できるデバイスは最大 100 台です。 詳細については、「デバイスを検索する」を参照してください。
	メールを送信 詳細については、「ユーザーへのメールの送信」を参照してください。
	アクティベーションメールを送信 詳細については、「アクティベーションメールを複数のユーザーに送信」を参照してください。
	ユーザーグループに追加 一度に選択できるデバイスは最大 200 台です。 詳細については、「ユーザーグループへのユーザーの追加」を参照してください。
	エクスポート 詳細については、「ユーザーリストの .csv ファイルへのエクスポート」を参照してください。
	デバイスを削除 この一括コマンドを使用するには、セキュリティ管理者である必要があります。一度に選択できるデバイスは最大 200 台です。 詳細については、「コマンドリファレンス」を参照してください。
	デバイス情報を更新します。 詳細については、「コマンドリファレンス」を参照してください。
	すべてのデバイスデータを削除 このコマンドを使用するには、セキュリティ管理者である必要があります。一度に選択できるデバイスは最大 200 台です。この一括コマンドは、macOS デバイスではサポートされていません。 詳細については、「コマンドリファレンス」を参照してください。
	仕事用データのみを削除 このコマンドを使用するには、セキュリティ管理者である必要があります。一度に選択できるデバイスは最大 200 台です。 詳細については、「コマンドリファレンス」を参照してください。

アイコン	説明
	デバイスの所有権を編集 一度に選択できるデバイスは最大 100 台です。 詳細については、「デバイスの所有権ラベルの変更」を参照してください。
	OS の更新 OS の利用可能な更新をインストールするように、監視対象の iOS デバイスに強制することができます。このコマンドを使用するには、セキュリティ管理者である必要があります。一度に選択できるデバイスは最大 200 台です。 詳細については、「監視対象の iOS デバイスでの OS の更新」を参照してください。
	コンソールパスワードを変更 BlackBerry UEM Self-Service パスワードを一度に複数のユーザーに送信できます。 詳細については、「複数のユーザーへの BlackBerry UEM Self-Service パスワードの送信」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 BlackBerry 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 BlackBerry 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、BlackBerry UEM を設定することができます。

1. メニューバーで、［設定］ > ［一般設定］ > ［コマンドの有効期限を削除］をクリックします。
2. ［すべてのデバイスデータを削除］と［仕事用データのみを削除］の一方または両方に対し、［コマンドが完了しない場合、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 BlackBerry 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。

コマンドリファレンス

デバイスに送信できるコマンドは、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。コマンドの中には、複数のデバイスに同時に送信できるものがあります。

iOS デバイスのコマンド

これらのコマンドは iPadOS デバイスにも適用されます。

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。	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。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。	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 BlackBerry 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。 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 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、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 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。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。 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
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す。またこのコマンドでは、デバイスに表示する電話番号とメッセージを設定できます。例えば、デバイスが拾われたときに、連絡先情報を表示させることができます。 このコマンドの送信後、BlackBerry UEM から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 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。 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
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。 詳細については、「監視対象の iOS デバイスでの OS の更新」を参照してください。 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。 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

コマンド	説明	アクティベーションタイプ
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。 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。	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。	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 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。	MDM 制御 ユーザーのプライバシー
eSIM の携帯電話データアプリを更新	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。
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。
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。 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 BlackBerry 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。
デバイスを削除	このコマンドは、BlackBerry 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。 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。

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）

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。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）
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）

コマンド	説明	アクティベーションタイプ
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）
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）

コマンド	説明	アクティベーションタイプ
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）
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）

コマンド	説明	アクティベーションタイプ
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）

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。
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。
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。 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。
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。

コマンド	説明
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、BlackBerry 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 BlackBerry UEM に接続できない場合、BlackBerry UEM からデバイスを削除できます。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。
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 BlackBerry UEM からデバイスを削除します。 このコマンドの送信後、BlackBerry 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 BlackBerry UEM に接続できない場合、BlackBerry UEM からデバイスを削除できます。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。
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。 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。
デバイスを削除	このコマンドは、BlackBerry 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。 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。

デバイスの無効化

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は削除されます。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、［仕事用データのみを削除］または［すべてのデバイスデータを削除］コマンドを使用してデバイスを無効化できます。デバイスがコンプライアンスプロファイルに違反し、指定された強制アクションがデバイスを無効化する場合、BlackBerry UEM も、そのデバイスを無効化できます。ユーザーは、次の方法でデバイスを無効化することができます。

- iOS および Android デバイスの場合、ユーザーは BlackBerry UEM Client アプリの［バージョン情報］画面で［デバイスを無効にする］を選択できます。
- Windows 10 デバイスの場合、［設定］>［アカウント］>［仕事用アクセス］>［削除］を選択します。

Knox MDM を使用するデバイスの場合、デバイスを無効化すると、内部アプリはアンインストールされます。また、必要に応じてアプリリストからインストールされた一般のアプリで、アンインストールオプションが使用できるようになります。

仕事用プロファイルだけを含む Android Enterprise デバイスでは、デバイスを無効化する場合、SD カードからすべてのデータを削除し、工場出荷時のリセット保護を解除するオプションがあります。

仕事用と個人用 - ユーザーのプライバシー 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が行われた Android Enterprise デバイスでは、［仕事用データのみを削除］コマンドを使用すると、ユーザーのデバイスの通知に表示される理由を入力して、作業プロファイルが削除された理由を説明できます。コンプライアンスルールに違反してデバイスが非アクティブ化された場合、通知にはデバイスがコンプライアンスに違反した理由が示されます。

仕事用と個人用 - フルコントロール アクティベーションが行われた Android Enterprise デバイスの場合、Android 10 以前を実行しているデバイスでは、［すべてのデバイスデータを削除］コマンドのみがサポートされます。［仕事用データのみを削除］コマンドは、Android 11 以降を実行しているデバイスでサポートされています。［仕事用データのみを削除］コマンドを使用すると、すべての仕事用データとアプリが削除されますが、ユーザーは個人データとアプリを保持して、管理されていないデバイスを引き続き使用できます。

仕事用と個人用 - フルコントロール または 仕事用領域のみ のアクティベーションタイプを使用してアクティブ化された Samsung Knox Workspace デバイスの場合、デバイスを無効化すると、デバイスまたは仕事用領域のみからすべてのデータが削除されます。［無効化でのデータ消去］IT ポリシールールを使用して、消去するデータを指定できます。

デバイスにインストールされているソフトウェアの更新の制御

Android Enterprise および Samsung Knox デバイスにインストールされたデバイスソフトウェアリリースを制御できます。Android Enterprise デバイスの場合、フォアグラウンドで実行されているアプリの更新期間も設定できます。

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 でアクティベーションされた Android Enterprise デバイスでは、使用可能なソフトウェア更新をインストールするタイミングをユーザーが選択するか、ソフトウェア更新を自動的にインストールするかを選択できます。デバイスモデルと現在インストールされている OS のバージョンに応じて、異なるルールを指定できます。すべての Android Enterprise デバイスでは、フォアグラウンドで実行されているアプリの更新期間も設定できます。これは、アプリがフォアグラウンドで実行されている場合、デフォルトでは、Google Play がアプリを更新できないためです。また、Google Play がデバイスに変更を適用する方法も制御できます。たとえば、変更をユーザーが許可できるかどうか、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変更を行うかどうかを指定できます。

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を使用する Android Enterprise デバイスの場合、デフォルトルール以外の OS アップデートルールを指定したデバイスでは、アップデートが禁止されている期間にアップデートを一時停止することもできます。たとえば、休日期間中にアップデートを一時停止することができます。すべてのデバイスのアップデートを一時停止する場合は、まずすべてのデバイスに対して OS アップデートルールを作成する必要があります。たとえば、Android 7.0 以降を実行しているすべてのデバイスに OS アップデートルールを作成して、後で特定の時間に自動的にアップデートを適用することができます。

Samsung Knox デバイスでは、Enterprise Firmware Over the Air（E-FOTA）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。

メモ：Samsung E-FOTA のサービス終了日は、2022 年 7 月 31 日です。詳細については、Samsung の情報を参照してください。Samsung E-FOTA One への移行については、support.blackberry.com にアクセスし、記事 69901 を参照してください。

仕事用領域のみ （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（Android Enterprise 完全管理のデバイス）、および 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 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 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。

ファームウェアバージョンを制御することにより、ユーザーのデバイスで使用されるファームウェアバージョンが、アプリでサポートされ、組織のポリシーを準拠しているものになります。デバイス SR 要件プロファイルを使用して、UEM でアクティブ化されている Samsung Knox デバイスのファームウェアルールを作成できます。ファームウェア更新がインストールされるタイミングをスケジュールし、強制更新をインストールする必要のあるときを指定できます。E-FOTA の詳細については、「https://seap.samsung.com/sdk/enterprise-fota」を参照してください。

メモ：デバイスが使用する通信事業者によっては、E-FOTA 更新を利用できない場合があります。一部の通信事業者（AT&T および Verizon など）は、独自のシステムを使用してワイヤレス更新を管理しています。

MDM 制御 アクティベーションを使用したデバイスでは、ユーザーがデバイス OS を更新するタイミングと方法を制御できませんが、コンプライアンスプロファイルを使用してデバイス OS バージョンを制限することはでき

ます。すべてのデバイスでは、制限されたソフトウェアリリースバージョンがデバイスにインストールされている場合に、特定の操作を強制実行するには、コンプライアンスプロファイルを作成して、そのコンプライアンスプロファイルをユーザー、ユーザーグループ、またはデバイスグループに割り当てる必要があります。コンプライアンスプロファイルは、ユーザーが制限されたソフトウェアリリースをデバイスから削除しない場合に実行される操作を指定します。

iOS デバイスにインストールされているソフトウェアリリースは制御できませんが、監視対象の iOS デバイスに対し、利用可能な更新を強制的にインストールすることができます。詳細については、「監視対象の iOS デバイスでの OS の更新」を参照してください。

Android Enterprise 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 デバイスにのみ適用されます。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。E-FOTA を使用する Samsung Knox デバイスのルールの設定詳細については、「Samsung Knox デバイスのデバイス SR 要件プロファイルの作成」を参照してください。

メモ：Samsung E-FOTA のサービス終了日は、2022 年 7 月 31 日です。詳細については、Samsung の情報を参照してください。Samsung E-FOTA One への移行については、support.blackberry.com にアクセスし、記事 69901 を参照してください。

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. ［コンプライアンス］ > ［デバイス **SR** 要件］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. ［**Android**］タブをクリックします。
6. 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 デバイスの場合、次の手順を実行して OS 更新のルールを設定します。
   a) ［**OS** 更新ルール］テーブルで ＋ をクリックします。
   b) ［機種］ドロップダウンリストで機種を選択します。
   c) ［**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。
   d) ［更新ルール］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。
      - 更新をインストールするタイミングの選択をユーザーに許可するには、［デフォルト］を選択します。
      - ユーザーにプロンプトを表示せずに更新をインストールするには、［自動的に更新］を選択します。
      - ユーザーにプロンプトを表示せずに、指定した時刻の間に更新をインストールするには、［時刻間で自動的に更新］を選択します。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 日間、更新のインストールをブロックするには、［**30** 日まで延期］を選択します。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。
   e) 完了したら、［追加］をクリックします。
   f) 追加するルールごとに手順 6 を繰り返します。

   E-FOTA を使用する Samsung Knox デバイスに設定されたルールは、これらのルールよりも優先されます。
7. 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 デバイスの場合、OS の更新を行わない期間を指定するには、次の手順を実行します。

a) ［**OS** 更新の一時停止］テーブルで ＋ をクリックします。
b) ［開始月］ドロップダウンリストで、一時停止期間を開始する月を選択します。
c) ［開始日］ドロップダウンリストで、一時停止期間を開始する日を選択します。
d) ［期間］ドロップダウンリストで、一時停止の期間を選択します。

停止は 90 日を超えることはできません。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。

これらの設定は、E-FOTA を使用する Samsung Knox デバイスには適用されません。

8. 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、次のオプションを設定します。
   - 開始時刻（ローカルデバイス時間）：アプリの更新を開始する時刻を指定します。
   - 期間：アプリの更新を許可する時間数を指定します。
9. フォアグラウンドで実行されているアプリに対して Google Play が変更を適用する方法を指定するには、アプリの自動更新ポリシーを選択します。次のオプションのいずれかを選択します。
   - 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。［アプリ自動更新ポリシー］オプションを選択していない場合は、これがデフォルト設定になる点に注意してください。
   - 常に：アプリは常に更新されます。BlackBerry UEM Client、BlackBerry Work、BlackBerry Connectivity のように常時実行されているアプリの場合、［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、ユーザーがデバイス上のアプリを手動で更新するまでアプリが更新されない点に注意してください。
   - **Wi-Fi** のみ：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アプリが更新されます。BlackBerry UEM Client、BlackBerry Work、BlackBerry Connectivity のように常時実行されているアプリの場合、［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、ユーザーがデバイス上のアプリを手動で更新するまでアプリが更新されない点に注意してください。
   - 無効：アプリは更新されません。

     メモ：

     このプロファイルは、Google Play のアプリの自動更新設定に影響します。［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。たとえば、プロファイルで［無効］を選択した場合、ユーザーはデバイスでアプリの更新を有効にすることはできません。ただし、ユーザーは Google Play でアプリを手動で更新できます。
10. ［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。

Samsung Knox デバイスのデバイス SR 要件プロファイルの作成

メモ：デバイスが使用する通信事業者によっては、E-FOTA 更新を利用できない場合があります。一部の通信事業者（T&T および Verizon など）は、独自のシステムを使用してワイヤレス更新を管理しています。

作業を始める前に： E-FOTA ライセンスが BlackBerry UEM に追加されていることを確認します。E-FOTA を使用するには、BlackBerry UEM 管理コンソールの関連 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選択する必要があります。

メモ：Samsung E-FOTA のサービス終了日は、2022 年 7 月 31 日です。詳細については、Samsung の情報を参照してください。Samsung E-FOTA One への移行については、support.blackberry.com にアクセスし、記事 69901 を参照してください。

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. ［コンプライアンス］ > ［デバイス **SR** 要件］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. ［**Samsung** デバイスファームウェアルール］テーブルで＋をクリックします。
6. ［すべての **Android** デバイスに制限を適用する］を選択して、Android OS の更新が Samsung デバイスに適用されるようにします。
7. ［デバイスモデル］フィールドにデバイスモデルを入力するか、ドロップダウンリストから選択します。
8. ［言語］ドロップダウンリストで、言語を選択します。
9. ［通信事業者コード］フィールドに、デバイスの通信事業者の CSC コードを入力します。
10. ［ファームウェアバージョンを取得］をクリックします。
11. 追加するファームウェアルールごとに、手順 5〜8 を繰り返します。
12. 完了したら、［追加］をクリックします。
13. ［**Samsung** デバイスファームウェアルール］テーブルで、追加したファームウェアバージョンの横の［スケジュール］をクリックします。
14. ［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（注：強制更新のスケジュールオプションを選択した場合、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）。
    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。日付の範囲は 3〜7 日にする必要があります。デフォルト値は 7 日です。
    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、およびユーザーのタイムゾーンを指定します。時間の範囲は 1〜12 時間にする必要があります。
15. ［保存］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。

E-FOTA ライセンスの追加

Enterprise Firmware Over The Air（E-FOTA）を使用し、Samsung からのファームウェアの更新を Samsung Knox デバイスにインストールするタイミングを制御することができます。ファームウェアバージョンを制御することにより、ユーザーのデバイスで使用されるファームウェアバージョンが、アプリでサポートされ、組織のポリシーを準拠しているものになります。

ファームウェアのバージョンを制御するためのデバイス SR 要件プロファイルを作成する前に、UEM で E-FOTA ライセンスを追加する必要があります。

メモ：Samsung E-FOTA のサービス終了日は、2022 年 7 月 31 日です。詳細については、Samsung の情報を参照してください。Samsung E-FOTA One への移行については、support.blackberry.com にアクセスし、記事 69901 を参照してください。

1. メニューバーで［ライセンス］ > ［ライセンスの概要］をクリックします。
2. ［**E-FOTA**］セクションで［ライセンスを追加］をクリックします。

3. ［**E-FOTA** ライセンスの追加］ダイアログボックスで、名前、クライアント ID、クライアントシークレット、顧客 ID、およびライセンスキーを入力します。
4. ［保存］をクリックします。

失効したソフトウェアリリースを実行しているユーザーの表示

失効したソフトウェアリリースを実行しているユーザーを一覧表示することができます。失効したソフトウェアリリースとは、通信事業者がサポートしなくなったが、ユーザーのデバイスにまだインストールされている可能性があるソフトウェアリリースのことです。

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. ［コンプライアンス］ > ［デバイス **SR** 要件］をクリックします。
3. 表示するプロファイルの名前をクリックします。
4. ［**x** ユーザーが失効した **SR** を実行中］タブをクリックして、失効したソフトウェアリリースを実行しているユーザーを一覧表示します。

MDM 制御 アクティベーションが行われたデバイスでの OS アップグレードの管理

MDM 制御 アクティベーションが行われたデバイスにソフトウェアリリースをインストールするタイミングを制御することはできません。ただし、コンプライアンスプロファイルを使用して、ユーザーは組織で許可されていない OS バージョンに更新したデバイスを管理することができます。たとえば、Android 10 以降のデバイスは MDM 制御 アクティベーションをサポートしていません。Android 9.x デバイスを使用しているユーザーが Android 10 にアップグレードする場合、一部のデバイス管理機能が動作しなくなり、デバイスは侵害状態になります。デバイスグループとコンプライアンスプロファイルを使用して、MDM 制御 アクティベーションタイプの Android デバイスを検出し、コンプライアンスルールを設定して、ユーザーへの通知、デバイスの信頼解除、デバイスの管理解除などの適切なアクションを実行できます。

以下の手順に従って、MDM 制御 アクティベーションが行われたデバイスでの OS アップグレードを管理します。

手順	アクション
1	次のパラメータに適合するデバイスを含むデバイスグループを作成します。 • MDM 制御 アクティベーションの種類 • 制限するデバイスの OS バージョン ユーザーがデバイスを指定された OS にアップグレードした場合、そのデバイスは自動的にデバイスグループの一部になります。
2	コンプライアンスプロファイルを作成し、デバイスの OS バージョンを制限された OS バージョンとして指定します。

手順	アクション
3	コンプライアンスプロファイルで、組織に適した強制アクションを指定します。たとえば、デバイス OS ではアクティベーションタイプがサポートされていないことをユーザーに通知し、別のアクティベーションタイプでデバイスを再アクティベーションすることを推奨したり、デバイスを非アクティブにしたりできます。
4	コンプライアンスプロファイルをデバイスグループに割り当てます。
5	必要に応じて、デバイスがコンプライアンスプロファイルに違反したときに、管理者に通知するイベント通知を作成します。

iOS デバイスの利用可能な更新の表示

ユーザーの iOS デバイスで、ソフトウェアを最新バージョンにアップグレードできるように、そのデバイスでソフトウェア更新が使用できるかどうかを確認できます。

1. メニューバーで、［ユーザー］ > ［管理されているデバイス］をクリックします。
2. ユーザーアカウントを検索します。
3. 検索結果で、ユーザーアカウントの名前をクリックします。
4. デバイスのタブを選択します。
5. ［アクティブ化されたデバイス］セクションで、更新が利用可能かどうかを確認します。

監視対象の iOS デバイスでの OS の更新

OS の利用可能な更新をインストールするように、iOS デバイスに強制することができます。複数のデバイス上で OS を更新する場合は、「一括コマンドの送信」を参照してください。

また、IT ポリシールール「ソフトウェア更新の遅延」および「ソフトウェア更新の遅延期間」を使用して、iOS ソフトウェア更新のタイミングを制御することもできます。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。

1. メニューバーで、［ユーザー］ > ［管理されているデバイス］をクリックします。
2. ユーザーアカウントを検索します。
3. 検索結果で、ユーザーアカウントの名前をクリックします。
4. デバイスのタブをクリックします。
5. 左側ペインで、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。
6. ドロップダウンリストで、次のオプションのいずれかを選択します。
   - ダウンロードとインストール：更新は自動的にデバイスにダウンロードされインストールされます。
   - ダウンロードのみ：更新が自動的にデバイスにダウンロードされ、ユーザーにはこの更新をインストールするように求めるプロンプトが表示されます。
   - ダウンロードしたアップデートのインストール：更新が既にデバイスにダウンロードされている場合は、自動的にインストールされます。

7. ［**OS** バージョン］リストで、デバイスを更新する OS バージョンを選択します。
8. ［更新］をクリックします。

デバイスと BlackBerry UEM の通信の設定

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、BlackBerry UEM にアクセスして更新を受信するように、BlackBerry 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 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 BlackBerry UEM に許可できます。個人用アプリのコレクションをオフにするには、［個人用アプリのコレクションを許可する］設定をオフにする必要があります。詳細については、「個人アプリコレクションのオフ」を参照してください。

Enterprise Management Agent 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。

Enterprise Management Agent 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］ > ［エンタープライズ管理エージェント］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. 組織の要求に応じて、各デバイスタイプの値を設定します。
6. ［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。

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 がデバイスで開かれている場合にのみポーリングします。 使用できる値： • 900～86400 デフォルト値は、［3600］です。
個人用アプリのコレクションを許可する	この設定では、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。 使用できる値： • 3600～86400 秒 デフォルト値は、［3600］です。
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ー残量の変更をパーセント（5～100%）で指定します。 使用できる値： • 5～100% デフォルト値は、［20］です。
RAM の空き容量のしきい値	デバイスが情報を BlackBerry 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。 デフォルトでは、デバイスはこの情報を BlackBerry UEM に送信しません。
内部ストレージのしきい値	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。 デフォルト値は、［250］です。
メモリカードのしきい値	デバイスが情報を BlackBerry UEM に送信するのに必要な外部空き容量の変更をメガバイト単位で指定します。 デフォルト値は、［500］です。
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。 使用できる値： • 最小値：900 デフォルト値は、［900］です。
個人用アプリのコレクションを許可する	この設定では、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。

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。
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	この設定では、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 デバイスの場合、組織のカスタム通知を作成し、アクティベーション中に表示させることができます。たとえば、ユーザーが組織のセキュリティ要件に準拠するために従う必要のある条件を、通知に含められます。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。異なる要件をカバーした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、組織情報はデバイスの 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。

メモ：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。

組織情報が表示される場合	組織情報の設定方法
iOS、macOS、Android、および Windows 10 デバイスのアクティベーション時に組織通知を表示する	組織の通知を作成し、それ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通知を表示する	組織通知を作成し、それをデバイスプロファイルの［Android］タブに割り当てます。デバイスの再起動時に表示する通知を変更するには、デバイスプロファイルを更新する必要があります。
iOS および Android デバイスの BlackBerry UEM Client、または Windows 10 デバイス上のサポート情報に組織情報を表示する	デバイスプロファイルの適切なタブに表示する情報を入力します。
Samsung Knox または監視対象の iOS デバイスの壁紙の画像	デバイスプロファイルの適切なタブで、画像ファイルを選択します。

組織の通知の作成

組織のカスタム通知を作成して、iOS、macOS、Android、および Windows 10 デバイスのアクティベーション中に表示できます。

Samsung Knox デバイスでは、ユーザーがデバイスを再起動しているときに、組織の通知を表示させることもできます。

1. メニューバーで［設定］をクリックします。
2. 左ペインで、［全般設定］を開きます。

3. ［組織の通知］をクリックします。
4. 画面の右側にある＋をクリックします。
5. ［名前］フィールドに、組織の通知の名前を入力します。
6. 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。
7. ［デバイスの言語］ドロップダウンリストで、組織の通知のデフォルトの言語として使用する言語を選択します。
8. ［組織の通知］フィールドに組織の通知のテキストを入力します。
9. オプションで、［追加の言語を追加］を複数回クリックして、組織の通知をより多くの言語で投稿できます。
10. 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。
11. ［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 デバイスに、組織通知を作成します。

メモ：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。

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. ［カスタム］ > ［デバイス］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。デバイスプロファイルごとに固有の名前が必要です。
5. 次のタスクのいずれかを実行します。

タスク	手順
デバイスの再起動時に、Samsung Knox デバイス上に表示する組織の通知を割り当てる	a. ［**BlackBerry**］または［**Android**］をクリックします。 b. ［組織の通知を割り当てる］ドロップダウンリストで、デバイス上に表示する組織の通知を選択します。

タスク	手順
iOS および Android デバイスの場合、BlackBerry UEM Client アプリ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。	**a.** ［**iOS**］、［**Android**］、または［**Windows**］をクリックします。 **b.** 組織の名称、住所、電話番号、メールアドレスを入力します。

6. 必要に応じて、次のタスクを実行します。

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する	**a.** ［**BlackBerry**］または［**Android**］をクリックします。 **b.** ［仕事用領域の壁紙］セクションで、［参照］をクリックします。 **c.** 壁紙に使用する画像を選択します。 **d.** ［開く］をクリックします。
監視対象の iOS デバイスに壁紙の画像を追加する	**a.** ［**iOS**］をクリックします。 **b.** ［デバイスの壁紙］セクションで、壁紙を［ホームスクリーン］、［ロック画面］、またはその［両方］に表示するかを選択します。 **c.** ［参照］をクリックして、壁紙に使用する画像を選択します。 **d.** ［開く］をクリックします。 **e.** ［以下の項目に壁紙を設定する］フィールドで、壁紙を表示する場所を選択します。

7. ［追加］をクリックします。

終了したら：

- 必要に応じて、プロファイルをランク付けします。

デバイス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、管理者は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。

位置情報サービスの設定

地図上で位置情報を参照するときにデバイスに表示する速度単位などの設定を、位置情報サービスプロファイルで設定できます。iOS および Android デバイスで位置情報履歴を有効にすると、BlackBerry UEM はデフォルトで 1 ヶ月の位置情報履歴を記録します。

1. 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. オンプレミス環境の場合は、［位置情報履歴の保存期間］フィールドに、BlackBerry UEM でデバイスの位置情報履歴を保存する期間を日、週、または月単位で指定します。
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。

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は、ユーザー、ユーザーグループ、またはデバイスグループに割り当てることができます。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。

作業を始める前に： 位置情報サービスの設定

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. ［保護］ > ［位置情報サービス］をクリックします。
3. ＋ をクリックします。
4. 位置情報サービスプロファイルの名前と説明を入力します。
5. 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。
6. 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	**a.** ［**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。 メモ：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。 メモ：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。

7. ［追加］をクリックします。

終了したら： 必要に応じて、プロファイルをランク付けします。

デバイスを検索する

iOS、Android、および Windows 10 Mobile デバイスを検索できます（デバイスの紛失時や盗難時など）。管理コンソールが地図上で 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、ユーザーは位置情報サービス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。位置情報履歴は、プロファイルで有効にした場合に iOS および Android デバイスで利用可能です。

作業を始める前に： 位置情報サービスプロファイルを作成または割り当てます。

1. メニューバーで、［ユーザー］ > ［管理されているデバイス］をクリックします。
2. 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. 地図上でデバイスを検索するには、次のアイコンを使用します。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。
   - 現在位置：
   - 直近で取得した位置情報：

   アイコンをクリックするかアイコンの上にカーソルを合わせると、緯度または経度のような位置情報や、位置情報がいつ取得されたのか（たとえば、1 分前または 2 分前など）を表示することができます。
5. iOS または Android デバイスで位置情報履歴を表示するには、次の操作を実行します。
   a) ［位置情報履歴を表示］をクリックします。
   b) 日付および時刻の範囲を選択します。

c) ［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使用

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ときに、紛失モードを有効にすると次の処理を行えます。

- デバイスをロックし、表示するメッセージを設定する（たとえば、デバイスが見つかったときに連絡先情報を表示できる）。
- ロケーションサービスプロファイルを使用せずに、デバイスの現在の場所を表示する。
- 管理コンソールから、紛失モードのすべてのデバイスを追跡する。

紛失モードをオンにする

紛失モードは監視対象 iOS デバイスでサポートされます。

1. メニューバーで、［ユーザー］ > ［管理されているデバイス］をクリックします。
2. 紛失モードをオンにする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［「スライドでロック解除」テキストを置換］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。

紛失モードでのデバイスの検索

作業を始める前に： 紛失モードをオンにする

1. メニューバーで、［ユーザー］ > ［管理対象デバイス］をクリックします。
2. 紛失モードがオンになっているデバイスをクリックします。
3. ［デバイス］タブで［デバイスの位置の取得］をクリックします。

紛失モードをオフにする

作業を始める前に： 紛失モードをオンにする

1. メニューバーで、［ユーザー］ > ［管理対象デバイス］をクリックします。
2. 紛失モードがオンになっているデバイスをクリックします。
3. ［デバイス］タブで ［紛失モードをオフにする］をクリックします。

iOS デバイスでのアクティベーションロックの使用

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際に、デバイスを保護できます。この機能が有効になっていると、ユーザーは、［マイ iPhone を検索］の無効化やデバイスの消去の際、またはデバイスを再アクティブ化して使用する際に、Apple ID とパスワードを確認する必要があります。

BlackBerry UEM でアクティベーションロック機能を管理するには、次の手順を実行します。

- 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。
- デバイスに iCloud アカウントが設定されている必要があります。
- デバイスで［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。

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、IT ポリシーを使用して強制的に適用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、BlackBerry UEM はロックを解除できるバイパスコードを格納するので、ユーザーの Apple ID とパスワードなしでデバイスの消去と再アクティブ化が可能になります。

アクティベーションロックを有効にする

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。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適用した場合、既に有効になっています。

メモ：アクティベーションロック機能を有効にすると、BlackBerry UEM と Apple の間に短い遅延が発生する可能性があります。

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。
- デバイスに iCloud アカウントが設定されている必要があります。
- デバイスで［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. 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ます。
3. 検索結果で、ユーザーアカウントの名前をクリックします。
4. デバイスのタブをクリックします。
5. ［デバイスを管理］ウィンドウで、［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：デバイスのバイパスコードのリストを表示するには、「」を参照してください。 アクティベーションロックバイパスコードの表示

アクティベーションロックを無効にする

次の手順を完了して、各デバイスのアクティベーションロックを個別に無効にします。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強制した場合、ロックは無効にできません。

メモ：アクティベーションロック機能を有効にすると、BlackBerry UEM と Apple の間に短い遅延が発生する可能性があります。

1. 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ます。
3. 検索結果で、ユーザーアカウントの名前をクリックします。
4. デバイスのタブをクリックします。
5. ［デバイスを管理］ウィンドウで［アクティベーションロックを無効にする］を選択します。

アクティベーションロックバイパスコードの表示

アクティベーションロックバイパスコードとバイパスコードが生成された日付を表示できます。

1. メニューバーで、［ユーザー］ **>** ［**Apple** アクティベーションロック］をクリックします。
2. デバイスを検索します。
3. 検索結果で該当するデバイスをクリックします。
4. 必要に応じて、メイン画面の右側にスクロールしてバイパスコードを表示します。

カスタムペイロードプロファイルを使用した iOS の機能の管理

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ていない iOS デバイスの機能を制御できます。

メモ：既存の BlackBerry UEM ポリシーまたはプロファイルで機能が制御されていると、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、BlackBerry 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。

- BlackBerry UEM ポリシーおよびプロファイルに含まれていない既存の iOS 機能を管理します。たとえば、BES10 の場合、組織の最高経営責任者（CEO）のアシスタントは、iPhone で自分自身のメールアカウントと CEO のアカウントの両方にアクセスできました。BlackBerry UEM では、1 台のデバイスに 1 つのメールプロファイルのみを割り当てることができます。そのため、アシスタントは自分自身のメールアカウントにしかアクセスできません。この問題を解決するため、アシスタントの iPhone がアシスタントのメールアカウントにアクセスできるようにするメールプロファイルに加えて、アシスタントの iPhone が CEO のメールアカウントにアクセスできるようにするカスタムペイロードプロファイルも割り当てられるようになっています。
- 最新の BlackBerry UEM ソフトウェアのリリース後にリリースされた新しい iOS 機能を管理します。たとえば、最新の iOS 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、BlackBerry UEM では、次回の BlackBerry UEM ソフトウェアのリリースまで新しい機能の IT ポリシーを利用できません。この問題を解決するため、次の BlackBerry UEM ソフトウェアのリリース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： 最新のバージョンの Apple Configurator を Apple から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. BlackBerry UEM 管理コンソールで［ポリシーとプロファイル］をクリックします。
3. ［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. Apple Configurator で 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>
```

7. Apple Configurator からコピーした 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。
8. ［追加］をクリックします。

Android Enterprise 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 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。

このプロファイルには 3 つのオプションがあります。

- 管理者が工場出荷時リセット保護を無効する。工場出荷時リセット保護を無効にすると、紛失や盗難にあったデバイスを誰でも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。
- 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ユーザーに使用させる。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。
- デバイスが工場出荷時設定にリセットされた後、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管理者が指定する。このオプションを使用すると、組織はデバイスが工場出荷時設定にリセットされた後にデバイスにログイン可能な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。

工場出荷時のリセット保護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］**>**［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プロファイル］をクリックします。
2. プロファイルの名前と説明を入力します。
3. ［工場出荷時のリセット保護設定］を選択します。次のオプションのいずれかを選択します。
   - 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。
   - 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。
   - ［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。

4. ［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、［**+**］ > ［**Google** 認証を使用して追加する］をクリックしてから、リセットされたデバイスにログインするために使用する Google アカウントにサインインします。

   最大 20 アカウントを追加できます。アカウントは手動で指定することもできます。詳細については、「Google アカウントのユーザー ID の手動取得」を参照してください。
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、組織に G Suite 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。
6. ［保存］をクリックします。

Google アカウントのユーザー ID の手動取得

既存の Google アカウントを使用することも、工場出荷時のリセット保護機能専用のアカウントを作成することもできます。アカウントを Google 認証を使用せずに手動で追加する場合は、そのアカウントのユーザー ID を取得する必要があります。

1. Google Developers の People API サイト（https://developers.google.com/people/api/rest/v1/people/get）にアクセスします。
2. ［**resourceName**］フィールドに「people/me」と入力します。
3. ［**personalFields**］フィールドに、「metadata」と入力します。
4. ［**EXECUTE**］をクリックします。
5. ［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。
6. ［**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。
7. ［People ID］ページの右側にある［ID］フィールドに、21 桁のユーザー ID が表示されます。ID は、番号「200」が表示されている緑色のヘッダーの下に表示されます。

デバイスリセットに対する工場出荷時リセット保護の反応

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。デバイスのリセット方法に応じて、工場出荷時リセット保護の反応が異なります。信頼されるリセットと信頼されないリセットの詳細については、support.blackberry.com/community にアクセスして、KB56972 を参照してください。

- BlackBerry UEM Client デバイスの無効化は、信頼されるリセットとはみなされません。これは無効化の前にデバイスユーザーが検証されないためです。そのため、デバイスがリセットされて無効化が完了すると、工場出荷時リセット保護がトリガーされます。
- 管理コンソールから「すべてのデバイスデータを削除」コマンドを送信すると、信頼されるリセットになる場合も、信頼されないリセットになる場合もあります。コマンドの送信時に［工場出荷時リセット保護を解除］オプションを選択すると、デバイスのリセットしたときに、工場出荷時リセット保護がトリガーされません。

- デバイス設定からデバイスをリセットする場合は、リセット前にユーザーが自分自身を認証する必要があります。これは信頼されるリセットと見なされ、工場出荷時リセット保護はトリガーされません。
- デバイスのブートローダー/リカバリーまたはデバッグツール（ADB）を使用して、デバイスを工場出荷時の設定にリセットできます。工場出荷時の状態にリセットされる前にユーザー ID が検証されないので、信頼されないリセットとみなされます。そのため、デバイスがリセットされると、工場出荷時リセット保護がトリガーされます。

工場出荷時のリセット保護プロファイルを設定する際に、特定の監視対象 Google Play アカウントを使用する場合の考慮事項

組織内で監視対象の Google Play アカウントを使用している場合は、工場出荷時リセット保護プロファイルで［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］オプションの使用を検討してください。これは、デバイスのリセットに使用する組織のデバイスに Google アカウントが存在しないので、工場出荷時リセット保護を使用できないことが理由です。

［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］オプションを使用する場合は、考慮すべき点がいくつかあります。

- プロファイルに入力する 21 桁のユーザー ID が正しいことを確認してください。この番号が組織で使用する Google アカウントと一致していない場合は、デバイス上で工場出荷時リセット保護がトリガーされると、それを解除できません。詳細については、「Google アカウントのユーザー ID の手動取得」を参照してください。
- BlackBerry は、工場出荷時リセット保護プロファイルを割り当てる組織ユーザーの 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することをお勧めします。このオプションをオフにすると、デバイス設定の工場出荷時リセットオプションが無効になり、BlackBerry UEM Client の無効化ボタンが使用できなくなります。これにより、ユーザーは UEM Client で信頼されない無効化オプションを使う（常にデバイスの工場出荷時リセット保護をトリガーする操作）ことができなくなります。このオプションが有効にされている場合、ユーザーがデバイスをリセットするには、組織の BlackBerry UEM 管理者に連絡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使用に関する情報と、工場出荷時リセット保護がデバイス上でトリガーされた場合に解除する手順を、組織のユーザーに伝えてください。詳細については、「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。BlackBerry UEM 管理者は、工場出荷時リセット保護を解除できるようにユーザーにアカウントの詳細を提供するのか、それともユーザーがローカルのサポート担当者にデバイスのロック解除を依頼する方式にするのかを選択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

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。初期設定済みの Android 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、最初の Android アカウント画面で、デバイスに関連付ける 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すると、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「afw#blackberry」また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、BlackBerry UEM に対してデバイスを再度アクティベートできます。
   - 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。デバイスの再起動後に、エンタープライズで再度アクティベートできます。
   - 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、事前設定を完了し、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。

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。

- デバイス上の個人用データと仕事用データを分離し、仕事用データだけを消去する
- 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したり、組織外部の人と共有したりできないようにする
- USB キーなどの他のデバイスに移動したり、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。WIP の詳細については、「https://technet.microsoft.com/itpro/windows/keep-secure/protect-enterprise-data-using-wip」を参照してください。

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。対応アプリと非対応アプリの詳細については、「https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/enlightened-microsoft-apps-and-wip」を参照してください。

Windows 情報保護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. ［保護］ > ［**Windows** 情報保護］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. プロファイル設定ごと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、「Windows 10 : Windows 情報保護プロファイルの設定」を参照してください。
6. ［追加］をクリックします。

Windows 10 ：Windows 情報保護プロファイルの設定

Windows 10 ：Windows 情報保護プロファイルの設定	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。この設定が［オフ］に設定されている場合、データは暗号化されず、監査ログがオフになります。この設定が［サイレント］に設定されている場合、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。この設定が［上書き］に設定されている場合、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。この設定が［ブロック］に設定されている場合、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。 使用できる値： • オフ • サイレント • 上書き • ブロック デフォルト値は［オフ］です。
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（|）で区切ることができます。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。 例えば、`example.com|example.net` のような形式になります。
データ復旧証明書ファイル（.der、.cer）	この設定では、データ復旧証明書ファイルを指定します。指定するファイルは、.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。 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には、データ復旧証明書ファイルを使用します。例えば、組織が WIP によって保護されているデータをデバイスから復旧する場合です。 データ復旧証明書の作成については、『Microsoft Windows 情報保護のドキュメント』を参照してください。
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。

Windows 10 ：**Windows** 情報保護プロファイルの設定	説明
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。 デフォルトでは、このオプションはオフです。
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。

Windows 10 ：Windows 情報保護プロファイルの設定	説明
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。 例えば、`example.com,example.net` のようなリストです。

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>`
	
	AppLocker の使い方の詳細については、Microsoft AppLocker の文書を参照してください。

Windows 10 ：Windows 情報保護プロファイルの設定	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>`
	
	AppLocker の使い方の詳細については、Microsoft AppLocker の文書を参照してください。

Windows 10 ：**Windows** 情報保護プロファイルの設定	説明
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。
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。

Windows 10 デバイスでの BitLocker 暗号化の許可

BitLocker ドライブ暗号化は、オペレーティングシステムのデータ保護機能で、デバイスの紛失や盗難時に不正なデータアクセスの軽減に役立ちます。起動時に追加の認証を要求するオプション（起動キー、PIN、リムーバブル USB ドライブなど）を提供するトラステッドプラットフォームモジュール（TPM）がデバイスに搭載されている場合は、Windows 10 デバイスで BitLocker 暗号化を許可でき、保護を強化できます。BlackBerry UEM では、コンプライアンスプロファイルを作成して、ユーザーが BitLocker を無効にして、暗号化が必要なデバイスで BitLocker の使用を強制されないようにすることも防止できます。

回復オプションを設定して、BitLocker で保護されたオペレーティングシステムまたはデータドライブにアクセスできます。ユーザーは Active Directory コンソールから回復キーにアクセスできます。有効になっている場合は、管理者が BitLocker 回復パスワードビューアツールを使用して回復できるように、回復パスワードを Active Directory ドメインサービスにバックアップできます。

Windows 10 デバイスで BitLocker 暗号化をサポートするために、次の UEM IT ポリシールールを設定します。

- デスクトップの BitLocker 暗号化方式
- デバイスでのストレージカードの暗号化プロンプトを許可する
- BitLocker デバイス暗号化にデバイスで暗号化を有効にするのを許可する
- 各ドライブタイプにデフォルトの暗号化方式を設定する
- 起動時に追加の認証を要求する
- 起動時に最小 PIN 長を要求する
- 起動前の復旧メッセージと URL
- BitLocker OS ドライブ回復オプション
- BitLocker 固定ドライブ回復オプション
- 固定データドライブの BitLocker 保護を要求する
- リムーバブルデータドライブの BitLocker 保護を要求する
- 回復キーの場所のプロンプトを許可する
- 標準ユーザーの暗号化を有効化する

BitLocker IT ポリシールールの詳細については、『ポリシーリファレンススプレッドシート』を参照してください。

デバイスの認証の管理

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。次のデバイスで、認証をオンにすることができます。

- Samsung Knox デバイス
- Android デバイス
- Windows 10 デバイス

Samsung Knox デバイスの認証の管理

認証をオンにすると、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）
- 仕事用領域のみ （Samsung Knox）
- 仕事用と個人用 - ユーザーのプライバシー （Samsung Knox）

1. メニューバーで［設定］ > ［一般設定］ > ［認証］をクリックします。
2. Samsung Knox デバイスの認証をオンにするには、［**KNOX Workspace** デバイスの定期的な認証チャレンジを有効にする］を選択します。
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 BlackBerry UEM に返す必要がある頻度を日数または時間数で指定します。
4. ［猶予期間］セクションで、猶予期間を指定します。認証応答が得られずに猶予期間が終了すると、デバイスが準拠していないと見なされ、そのデバイスは、ユーザーに割り当てられているコンプライアンスプロファイルに指定された条件を適用されます。注：ユーザーのデバイスは、通信可能範囲にないか、電源オフにされているか、バッテリー切れである場合、BlackBerry UEM から送信された認証チャレンジに応答できないため、BlackBerry UEM はそのデバイスを非準拠であると見なします。コンプライアンス違反時にデバイスを削除するように組織のコンプライアンスポリシーが設定されている場合、猶予期間が満了する前にデバイスが応答しないと、デバイス上のデータは削除されます。
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

SafetyNet を使用した Android デバイスおよび BlackBerry Dynamics アプリの認証の管理

Android SafetyNet 認証を使用する場合、BlackBerry UEM は、組織の環境内の Android デバイスと BlackBerry Dynamics 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。SafetyNet 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 認証を使用できます。SafetyNet の詳細については、Google の情報を参照してください。

次の場合に BlackBerry UEM は SafetyNet 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 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中
- BlackBerry Dynamics アプリのアクティベーション中
- BlackBerry Dynamics アプリのアプリアクティベーション後
- REST API を使用してオンデマンドで
- BlackBerry UEM Client がアクティブ化されている場合はデバイスの再起動時

SafetyNet 認証の設定に関する考慮事項

- Google SafetyNet 認証失敗オプションは、Android デバイスおよび BlackBerry Dynamics アプリ用のコンプライアンスプロファイル設定であり、デバイスまたはアプリが SafetyNet 認証に不合格になった場合に発生するアクションを指定できます。このオプションを設定するには、［ポリシーとプロファイル］**>**［コンプライアンス］**>**［**Android**］タブに移動します。
- ［Google SafetyNet 認証失敗］コンプライアンスルールを有効にしていない場合、既にアクティブ化されているアプリにはコンプライアンスアクションが強制されません。
- SafetyNet を有効にすると、アクティベーション中の認証が実行されます。ポリシーを使用してアクティベーション中の認証を強制することはできません。
- BlackBerry UEM Client は、SafetyNet 認証を有効にするのに必須ではありません。
- BlackBerry UEM Client は、SafetyNet 認証用に設定できる BlackBerry Dynamics アプリのリストには表示されません。BlackBerry UEM は、認証チャレンジを BlackBerry UEM Client に送信し、そこから応答を受信します。
- BlackBerry UEM は、認証チャレンジを、設定者が設定したそれぞれの BlackBerry Dynamics アプリに送信します。
- BlackBerry UEM は、古いバージョンのアプリを信頼しません。たとえば、BlackBerry Work に対して認証チャレンジを有効にする場合は、組織のデバイス上の BlackBerry Work のバージョンが最新バージョンであることを確認する必要があります。最新バージョンでない場合、新しいアクティベーションは失敗します。既存のアクティブ化されたユーザーが古いバージョンのアプリを使用していても、組織のコンプライアンスプロファイルで［Google SafetyNet 認証失敗］オプションを有効にするまで、アプリまたはデバイスに対して障害となるアクションは実行されません。
- BlackBerry UEM では、アクティベーション認証および定期的な認証に加えて、新しい REST API を使用しており、これによって設定者はカスタムサーバーワークフローを作成できます。たとえば、アプリが特定のセキュリティ保護されたリモートアイテムにアクセスする必要がある場合、アクセスを許可する前に、アプリサーバーが BlackBerry UEM と通信してアプリまたはデバイス上で SafetyNet 認証を強制します。
- ユーザーのデバイスは、通信可能範囲にないか、電源オフにされているか、バッテリー切れである場合、BlackBerry UEM から送信された認証チャレンジに応答できないため、BlackBerry UEM は、そのデバイスを非準拠であると見なします。準拠から外れているデバイスを消去するように組織のコンプライアンスポリシーが設定されている場合、猶予期間が終了する前にそのデバイスが応答しなければ、そのデバイスがワイヤレスネットワークに接続したときにそのデバイス上のデータが削除されます。
- ［アプリの猶予期間］フィールドに時間を設定した場合、設定したその時間枠内に応答しないアプリに対してのみアクションが実行されます。たとえば、［アプリの猶予期間］の値を 7 日間に設定し、ユーザーが BlackBerry Work を毎日使用しているが、BlackBerry Tasks を 7 日以内に使用しなかった場合、BlackBerry Tasks に対してのみアクションが実行されます。
- 新しいアプリを BlackBerry UEM に追加し、そのアプリがアクティベーション中の認証に失敗した場合、組織のコンプライアンスプロファイルの［Google SafetyNet 認証失敗］セクションでどのオプションを設定しているかに関係なく、そのアプリはアクティブ化されません。アプリは、既にアクティブ化されている場合、コンプライアンスプロファイルで指定したルールの対象となります。
- 組織のユーザーは、最新バージョンの Google Play サービスをインストールしている必要があります。
- デバイスが認証に失敗しても、［管理対象デバイス］ページの［OS 侵害］列には失敗の表示はありません。

- Android デバイス用の BlackBerry Dynamics アプリの開発については、開発者関連の資料を参照してください。

SafetyNet を使用した Android デバイスおよび BlackBerry Dynamics アプリの認証設定

1. メニューバーで［設定］ > ［一般設定］ > ［認証］をクリックします。
2. Android デバイスの認証をオンにするには、［**SafetyNet** を使用した定期的な認証チャレンジを有効にする］を選択します。
3. Google の Compatibility Test Suite をオンにする場合は、［**CTS** プロファイルの一致を有効にする］を選択します。CTS の詳細については、Google の情報を参照してください。
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日数または時間数で指定します。チャレンジ頻度を設定する際の考慮事項：
   - BlackBerry UEM がデバイスの信頼性と完全性をテストする頻度は設定できますが、アプリのアクティベーション中には認証が必須になります。
   - BlackBerry UEM Client を導入している場合、BlackBerry UEM が SafetyNet 認証を自動的にテストするアプリの 1 つとして追加されます。
   - BlackBerry UEM Client は、BlackBerry UEM に対して、他の BlackBerry Dynamics アプリとは異なる通信チャネルを使用します。ポリシーの更新を受信するためには、このチャネルを実行し、また BlackBerry UEM への接続を承認されている必要があります。BlackBerry UEM は、BlackBerry UEM Client とプロアクティブに通信し、アプリが実行されていない場合は起動することができます。チャレンジ頻度を 3 時間に設定すると、BlackBerry UEM は BlackBerry UEM Client と 3 時間ごとに通信して検証チェックを実行します。ただし、BlackBerry Dynamics アプリコマンドは、アプリが BlackBerry UEM に接続するまで保存され、最新の認証コマンドのみが保存されます。そのため、アプリが 24 時間使用されていない場合は、ユーザーが起動すると認証チャレンジが 1 回だけ実行されます。
5. ［猶予期間］セクションで、猶予期間を指定します。認証応答が得られずに猶予期間が終了すると、デバイスが準拠していないと見なされ、そのデバイスは、ユーザーに割り当てられているコンプライアンスプロファイルに指定された条件を適用されます。また、ユーザーのデバイスは、通信可能範囲にないか、電源オフにされているか、バッテリー切れである場合、BlackBerry UEM から送信された認証チャレンジに応答できないため、BlackBerry UEM がそのデバイスを非準拠であると見なします。準拠から外れているデバイスを消去するように組織のコンプライアンスポリシーが設定されている場合、猶予期間が終了する前にそのデバイスが応答しなければ、そのデバイスがワイヤレスネットワークに接続したときにそのデバイス上のデータが削除されます。
6. ［アプリの猶予期間］セクションで、猶予期間を指定します。猶予期間が終了すると、BlackBerry Dynamics アプリは、ユーザーに割り当てられているコンプライアンスプロファイルに指定された条件を適用されます。猶予期間はアプリごとに適用されます。BlackBerry UEM Client のみをデバイスに導入した場合、猶予期間は無視されます。また、BlackBerry UEM Client は BlackBerry Dynamics アプリのリストに表示されません。認証チャレンジの対象となるアプリのリストに BlackBerry Dynamics アプリを追加する場合、次のルールが適用されます。
   - このリストのアプリのみに認証チャレンジを送信
   - このリストのアプリのみ、アプリの猶予期間チェックの評価を受ける
   - このリストのアプリのみが、アプリのアクティベーション中に認証の対象となる

     メモ：SafetyNet 専用に開発された BlackBerry Dynamics アプリのみがリストに表示されます。詳細については、開発者関連の資料を参照してください。
7. 認証チャレンジの対象となるアプリを追加するには、［+］をクリックします。
8. 次の操作のいずれかを実行します。
   - 既にリストに載っているアプリ名をクリックします。

- アプリ名を検索してクリックします。

9. ［選択］をクリックします。
10. ［保存］をクリックします。

Windows 10 デバイスの認証の管理

認証をオンにすると、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。デバイスは Microsoft Health Attestation Service と通信し、組織のコンプライアンスプロファイルで設定した設定に基づいてコンプライアンスを確認します。

メモ： Windows 10 認証設定は、BlackBerry Desktop（BlackBerry Access + BlackBerry Work）には適用されません。

1. 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 デバイスの認証をオンにするには、［**Windows 10** デバイスの定期的な認証チャレンジを有効にする］を選択します。
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 BlackBerry UEM に返す必要がある頻度を日数または時間数で指定します。
4. ［猶予期間］セクションで、猶予期間を指定します。認証応答が得られずに猶予期間が終了すると、デバイスが準拠していないと見なされ、そのデバイスは、ユーザーに割り当てられているコンプライアンスプロファイルに指定された条件を適用されます。また、ユーザーのデバイスが通信範囲外にある場合、電源がオフになっている場合、またはバッテリーが切れている場合、BlackBerry UEM が送信する認証チャレンジに応答できず、BlackBerry UEM が非準拠であると判断されることも考慮してください。コンプライアンス違反時にデバイスを削除するように組織のコンプライアンスポリシーが設定されている場合、猶予期間が満了する前にデバイスが応答しないと、デバイス上のデータは削除されます。
5. ［保存］をクリックします。

デバイスの詳細ページには、コンプライアンス違反を表示することができます。

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

iOS デバイスを移行して強化されたチャネルを使用する

強化されたチャネルをまだ使用していないデバイスのリストをエクスポートするには、次の手順を実行します。移行中にデバイスが再アクティブ化され、ユーザーが仕事用アプリやプロファイルの再インストールなどの影響を受ける可能性があります。詳細については、support.blackberry.com にアクセスし、KB99869 を参照してください。

メモ：DEP に登録されているデバイスの場合、DEP 登録設定は移行されず、デバイスは移行先環境の登録設定を失います。ユーザーは、移行後にデバイスを工場出荷時の状態にリセットしてから、BlackBerry UEM Client を再アクティブ化する必要があります。詳細については、support.blackberry.com にアクセスし、KB100525 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］をクリックします。
2. ［エクスポート］をクリックします。強化されたチャネルをまだ使用していないデバイスのリストがダウンロードされます。共有デバイスグループ内のデバイスは、情報提供のみを目的としてエクスポートに含まれることに注意してください。これらのデバイスはインポート時にスキップされるため、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、BlackBerry UEM Client を再アクティブ化する必要があります。
3. ［参照］をクリックし、移行するデバイスが含まれているファイルへ移動します。手順 2 でダウンロードしたリストに 1,000 件を超えるエントリが含まれている場合は、アップロードするファイルに最大で 1,000 件となるようにエントリを分割して、複数のファイルをアップロードする必要があります。

単一の iOS デバイスを移行して強化されたチャネルを使用する

個々のデバイスを移行して、強化されたチャネルを使用できます。

1. 移行するデバイスを移動します。
2. ［デバイスの管理］セクションで、［**iOS** の強化されたチャネルに移行］をクリックします。
3. ［送信］をクリックします。

強化されたチャネルを使用するために再アクティブ化する必要がある macOS デバイスのリストをエクスポートする

KB99869 で通知されたセキュリティ問題の影響を受けるデバイスのリストをエクスポートするには、次の手順を実行します。エクスポートするファイルにリストされているデバイスを所有する各ユーザーは、セルフサービスポータルでデバイスを再アクティブ化する必要があります。

1. ［設定］ > ［移行］ > ［**macOS** の強化されたチャネル］に移動します。
2. ［エクスポート］をクリックします。再アクティブ化が必要なデバイスのリストがダウンロードされます。
3. リストにデバイスを登録しているユーザーに連絡し、セルフサービスポータルでデバイスを再アクティブ化してもらいます。セルフサービスポータルでの再アクティブ化については、『ユーザーガイド』を参照してください。

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