BigFix

Profile Management ユーザーズ・ガイド

Special notice

Before using this information and the product it supports, read the information in Notices.

Edition notice

This edition applies to BigFix version 10 and to all subsequent releases and modifications until otherwise indicated in new editions.

目次

第 1 章. Profile Management の概要

BigFix Profile Management は、BigFix Lifecycle の WebUI ベースの機能です。

Profile Management は、デバイス上の個人別設定を管理するプロセスと見なされます。通常、管理対象で最も機密性の高い設定は、セキュリティーの領域にあります。例えば、パスワードまたはパスコードの長さや複雑性、ネットワーク・アクセス、ストレージ管理の制限、組み込みアプリケーションや外部アプリケーションを実行する権限などに対するポリシーを管理者が定義することが考えられます。また、特定のユーザー・アクティビティー、レジストリー・キーの内容、その他のプロパティーに対して制限を施行できます。

通常、組織がデバイスを導入するときには、検討する複数のシナリオがあります。多くの組織では、独自持ち込み (BYO) 個人デバイスと独自選択 (CYO) 会社所有デバイスの両方が導入されます。いずれの場合にも、組織全体のセキュリティー要件に準拠する必須設定を構成できるシステムにデバイスを登録する必要があります。また、デバイスは、従業員と部門の特定の役割ベースの要件にも準拠する必要があります。

BigFix Profile Management は、組織の特定のビジネス・ニーズとセキュリティー要件に基づいてデバイス構成プロファイルを適用できます。プロファイルは、組織の構造と特定の従業員役割に応じて、組織のセキュリティー要件に対応し、すべてのデバイスを継続的に準拠状態になるようにします。Profile Management では、高度な制御が確保され、デバイスのタイプとユーザーに応じた異なるポリシーを柔軟に確立できます。セキュリティー管理者は、BigFix server に登録された任意の企業デバイスに対してポリシー設定を定義および実装できます。

この機能は、Windows 10 デバイスおよび Mac OS デバイス用の、セキュリティー管理者のプロファイル管理機能を提供します。

プロファイル管理の用語

以下の用語が、機能の中核を表現します。

プロファイル

プロファイルは、デバイスに対して施行するセキュリティー設定のセットを表します。設定は、ユーザーに対する便宜上、4 つのカテゴリーにグループ化されます。各カテゴリーは、WeBUI のプロファイル・ページ内のタブに対応しています。施行できるカテゴリーは次のとおりです。

パスワード/パスコード

パスワードまたはパスコードの要件が含まれます。

装置

ハードウェア・デバイスの使用法を制限する設定が含まれます。

アプリケーション

アプリケーション機能を制限する設定が含まれます。

制約事項

特定のアプリケーションやデバイス機能の使用を無効にする設定が含まれます。

プロファイルの保存

Bigfix データベースにプロファイルを格納し、プロファイルで設定されている値について、このプロファイルがまだ施行されていないデバイスが関連するかどうかを検査する Fixlet を生成するアクション。

プロファイルのデプロイ

プロファイルに関連付けられている Fixlet を適用し、構成設定を継続的に施行できるようにするアクションを作成します。

サポートされるクライアント・オペレーティング・システム

Profile Management は、BigFix Lifecycle 9.5 で使用でき、BigFix プラットフォームのバージョン 9.5.3 で入手できる Windows 10 と MAC OS X 10.12 Sierra をサポートしています。サポートされる Windows 10 各エディションのリストについては、「詳細なシステム要件」を参照してください。

オペレーターの権限および関連プロファイル・アクション

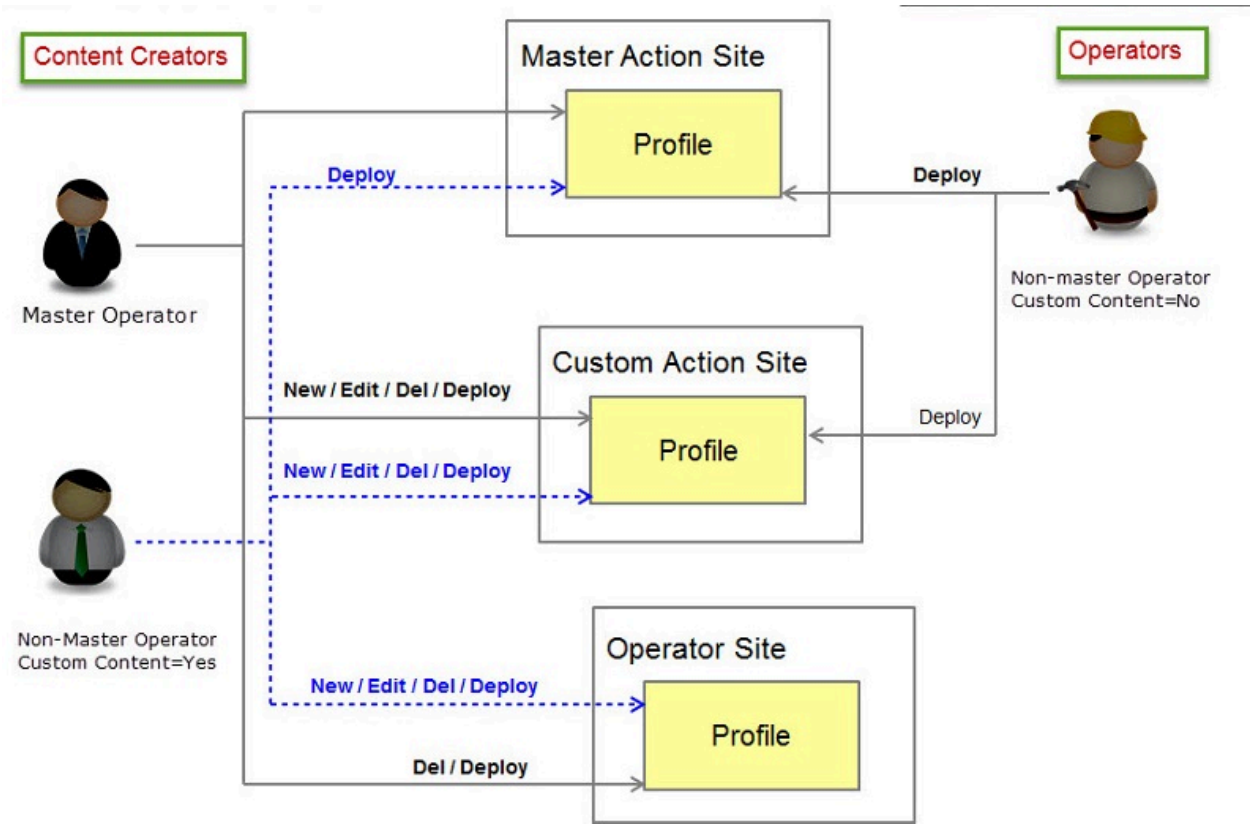
オペレーターが実行できるプロファイル・アクションは、オペレーターの役割および許可によって異なります。

Profile Management は、標準的な BigFix プラットフォーム許可モデルを実装します。このモデルは、以下の項目に基づいてオペレーターが実行を許可される操作を定義するルールを規定します。

- オペレーター役割: マスター・オペレーター (MO) またはマスター以外のオペレーター (NMO)
- サイトでのオペレーターの権限
- 特定のオペレーターの権限:
  - カスタム・コンテンツの作成
  - アクションの作成

重要: オペレーターが Profile Management で作業するには、オペレーターの WebUI インターフェース・ログイン特権を「yes」に設定しておく必要があります。オペレーター、役割、および権限について詳しくは、このリンクにある「*BigFix* コンソール・オペレーター・ガイド」を参照してください。ローカル・オペレーターの追加。

以下の図に、オペレーターの役割と許可および対応するプロファイル・アクションをまとめています。



プロファイル・リスト・ビュー

プロファイル・リスト・ビューには、現在ログインしているオペレーターがアクセスを許可されているプロファイルが表示されます。フィルタリングされたリストには、オペレーターがアクセスできるサイトで作成されたプロファイルが含まれています (それらのプロファイルが異なるオペレーターによって作成されたものであってもかまいません)。

プロファイル・アクションの追加 (作成)、編集、コピー、および削除

新規プロファイルを作成するには、Custom Contentアクセス許可がYesに設定されていなければなりません。プロファイルの作成時に、プロファイルが作成されるサイトを指定する必要があります。サイトを選択できるサイト・リストには、自分がアクセスできるサイトが含まれています。マスター以外のオペレーターは、自分が作成したプロファイルを編集および削除でき、自分が作成者権限を持つサイトで作成されたプロファイルも編集できます。

マスター・オペレーターは、常にプロファイルの編集または削除を許可されていますが、現在ログインしているオペレーターが所有していないオペレーター・サイトで作成されたプロファイルは除きます。

プロファイルのデプロイ

プロファイルをデプロイするには、Can Create Actions アクセス許可がYesに設定されていなければなりません。デプロイ・アクションは常に、現在ログインしているオペレーターが、プロファイル・リストに表示されているプロファイルに対して実行できます。オペレーターは、自分が権限を持つサイトにサブスクライブしているターゲットに、プロファイルをデプロイすることを許可されています。ただし、それ以上の制限が適用される場合を除きます。

プロファイルのデプロイメントの停止

マスター・オペレーターは、特定のオペレーター・サイトで作成されたものを除き、すべての適用を停止できます。
マスター以外のオペレーターは、自分が実行依頼した適用を停止できます。

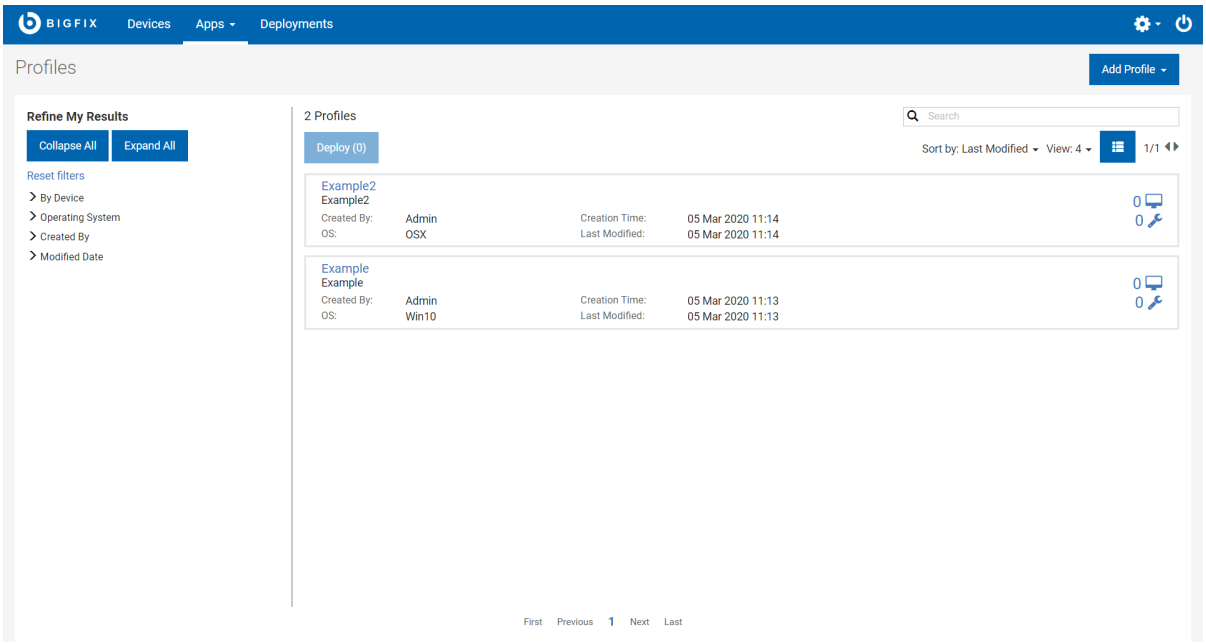
第 2 章. Profile Management タスク

プロファイルを作成およびデプロイすることによって、デバイスのコンプライアンスを適用することができます。

オペレーターは、コンテンツ・リストから**「プロファイル」**を選択することによって、Windows 10 プロファイルまたは MAC OS プロファイルを処理できます。

プロファイル・リスト・ビュー

このリストには、ログインしているオペレーターが管理を許可されているプロファイルが表示されます。特定のユーザー役割およびアクセス許可に応じて、一部のプロファイル・オプションを使用できない可能性があります。詳しくは、『オペレーターの権限および関連プロファイル・アクション』を参照してください。



プロファイル・リストでは、プロファイルが作成時刻順に表示されます。プロファイルを名前または最終更新日時によってソートすることもできます。左では、さらにフィルターを設定して、該当するデバイスがあるプロファイルのみを表示する選択、Windows 10 または MAC OS のデバイス用に作成されたプロファイルのみの表示、自分または別のオペレーターが所有するプロファイルのフィルター処理、指定した時間間隔内に変更されたプロファイルの表示などを実行できます。

プロファイルごとに、そのプロファイルに関連する (現在不適合である) デバイスの数を確認できます。そのすぐ下に、プロファイルの進行中のデプロイメントの数を確認できます。プロファイルの適用と、その機能については、プロファイル・コンプライアンスの動作を参照してください。

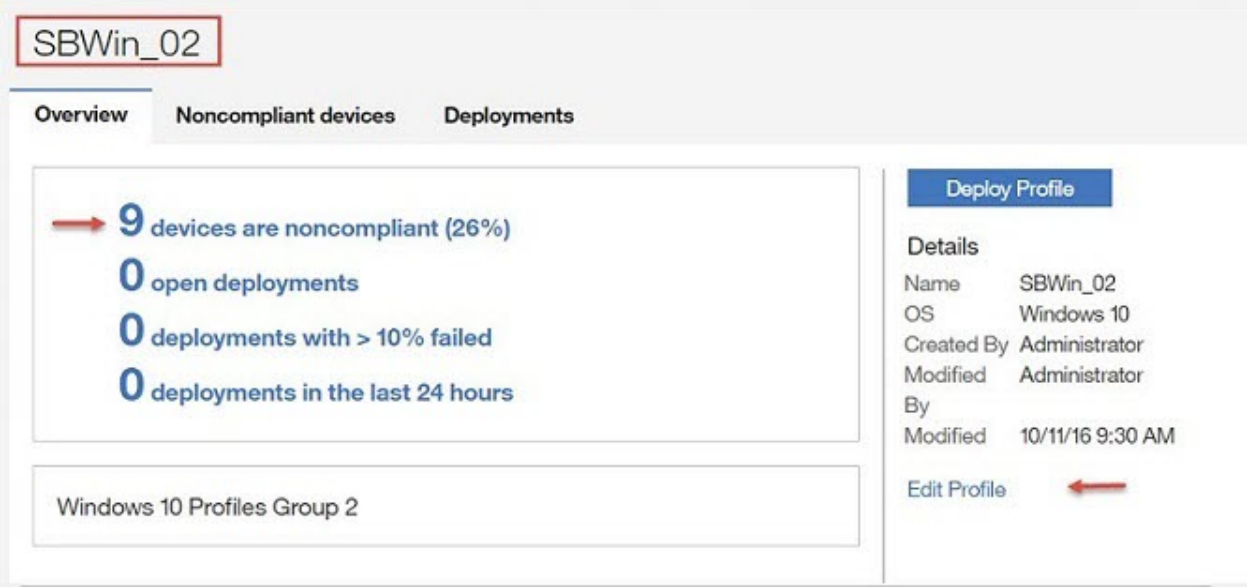
プロファイルの作成

新しいプロファイルを作成するには、プロファイル・リスト・ビューで**「プロファイルの追加」**をクリックし、オペレーティング・システムを選択します。「プロファイル名」、「説明」を指定し、プロファイルを作成する「サイト」を選択する必要があります。プロファイル・プロパティーについて詳しくは、Windows 10 デバイス用のプロ

ファイル属性および MAC OS X デバイスのプロファイル・プロパティーを参照してください。プロファイルを保存すると、Fixlet が作成されます。プロファイルを適用すると、指定したサイトをサブスクライブしているコンピューター上でその Fixlet が実行されます。Fixlet は、プロファイルに指定されているセキュリティー設定をデバイス上の現在の設定が満たしているかどうかを検査します。デバイス上の設定の方が制限が少ない場合、そのプロファイルに関連するとしてマークが付けられ、非準拠とみなされます。

プロファイルの表示または編集

プロファイル・プロパティーを表示または編集するには、プロファイル名をクリックします。プロファイルの「概説」ページが表示されます。



「概要」ページでは、要約のリンクを使用することで、ドリルダウンして詳細情報ページを表示できます。非準拠のデバイス、進行中の適用または失敗した適用のリスト、および過去 24 時間に発生した適用に関する詳細を表示できます。非準拠のデバイスのパーセンテージは、プロファイルが格納されているサイトにサブスクライブしているコンピューターの総数から計算されます。

右では、プロファイルを作成したオペレーターのログイン名、プロファイルを最後に変更したオペレーター、および最終変更の日時を表示できます。このページで、プロファイルを適用することもできます。

プロファイルを編集できるかどうかを判別するために、いくつかのチェックが実行されます。ロック・アイコンは、プロファイルについて進行中の適用があるか、現在ログインしているオペレーターにカスタム・コンテンツを作成 (編集) する権限がないために、プロファイルが編集できないことを示します。ロック記号の後に、リンク・テキスト「プロファイルの表示」が表示されます。警告メッセージに理由が示されます。プロファイルを開くと、**「保存」**オプションが無効になっています。プロファイルが編集可能な場合、リンクをクリックすると、プロファイルのページが編集モードで開かれます。必要な変更を行い、**「保存」**をクリックします。

進行中のデプロイメントおよびプロファイル更新

プロファイルの進行中のデプロイメントがある場合、そのプロファイルはロックされ、編集できません。プロファイル内のポリシーを変更する場合、編集して必要な変更を加えるには、先にそのプロファイルの進行中のデプロイメントをすべて停止する必要があります。新規プロファイル属性が保存されたら、プロファイルを再デプロイして、適用をアクティブにする必要があります。

プロファイルのコピー

選択したプロファイルの新しいコピーを作成できます。プロファイル・リスト・ビューで、コピーするプロファイルをクリックします。「概要」ページで、プロファイルが編集できるかどうかに応じて**「プロファイルの表示」**または**「プロファイルの編集」**をクリックします。プロファイル・プロパティーのページで、**「コピー」**をクリックします。ソース・プロファイルの設定の新しいプロファイル・ページが表示されます。新しいプロファイル名は、ソース・プロファイル名の後に `- Copy` が付きます。例えば、`Winprf1` という名前のプロファイルをコピーすると、新しいプロファイル名は `Winprf1 - Copy` になります。必要に応じて、名前、サイト、説明、その他のカテゴリーの設定を変更できます。**「保存」**をクリックして、プロファイルを作成します。

プロファイルの削除

プロファイルに対して進行中の適用が存在しない場合にのみ、「プロファイルの編集」ページでプロファイルを削除できます。対応するアクションを選択し、選択内容を確認します。

プロファイルのデプロイ

1. プロファイル・リスト・ビューでプロファイルを選択し、**「デプロイ」**をクリックします。別の方法として、プロファイル名をクリックし、プロファイルの「概説」ページからプロファイルを適用することもできます。
2. プロファイルが関連するデバイスのリストが表示されます。1 つ以上のデバイスまたはデバイス・グループを選択し、**「次へ」**をクリックします。フィルターを使用して、オペレーティング・システムや IP アドレスなどの特定の条件を満たすデバイスを選択できます。
3. 「構成」セクションで、デフォルトでは適用は無期限です。このオプションをクリアすると、終了時刻を指定できます。「**次へ**」をクリックします。オプションを確認し、**「デプロイ」**をクリックするか、または**「キャンセル」**をクリックしてプロファイル・リストに戻ります。

プロファイルをデプロイすると、**「デプロイメント」**ビューで、プロファイルの状態は**「進行中」**になっています。これは、継続的なコンプライアンス検査と自動施行がアクティブであることを示します。デフォルトでは、デバイスが非準拠、つまり選択したプロファイルに対してデバイスが再度関連状態になると、そのプロファイルによって施行される構成よりもターゲット上の現在の構成の方が制限が厳しくない限り、そのプロファイルが自動的に再施行されます。

重要:

- プロファイルは、再度関連状態になると、無期限に自動的に再施行されます。この動作は、適用を停止するか、無期限の適用オプションをクリアしない限り、常に有効です。オプションをクリアした場合、プロファイルが再施行されるのは、指定した終了時刻までになります。
- 適用が何らかの理由で失敗すると、関連付けられているタスクの状況は、WeBUI で「待機中」のままになります。この動作は、失敗時に再試行しますで説明されている「失敗時の再試行回数」メカニズムによって実装されます。

適用のトラブルシューティングについては、プロファイルの適用のトラブルシューティングを参照してください。

失敗時に再試行します

BigFix Profile Management は、「失敗時の再試行回数」メカニズムを実装しています。適用が失敗すると、対応するタスクが WebUI で「待機中」状態のままになり、15 分ごとに、この機能がプロファイルを 999 回再施行しようとします。適用の状態は、プロファイルが正常に再施行されるか、再試行間隔カウンターが満了すると変わります。前者の場合、適用の状況は**「修正済み」**に変わり、後者の場合、適用の状況は**「失敗しました」**に変わります。

適用の状況がまだ「待機中」のときに何が起きているかを確認するために、BigFix コンソールにログインできます。適用に関連する失敗したアクションに対する終了コードがあります。Mac OS X プロファイルの適用に関連する終了コードについては、プロファイルの適用のトラブルシューティングを参照してください。

デプロイメントの停止

デプロイメント・ビューで、停止する進行中の適用を選択し、対応するアクションをクリックします。デプロイメント・リストに、失敗率、発行者、デプロイメント・タイプなどの 1 つ以上のフィルターを適用することができます。停止要求を確認するように求められます。

プロファイル・コンプライアンスの動作

組織でのデバイスのセキュリティー方針は、プロファイルの適用により施行されます。

組織内には、全体的なセキュリティー要件に応じて、さまざまなレベルでセキュリティーを実装できます。組織の構造と単一のデバイスの重要度に応じて、マスター・アクション・サイト・レベルでは、共通レベルのセキュリティー・ポリシーを組織内のすべてのデバイスに施行するが、部門レベルでは、制限が厳しいポリシーを必要とすることがあります。組織で目標とするセキュリティー方針に基づいて、セキュリティー管理者は、すべてのデバイスに共通である必要がある必須セキュリティー・ポリシーの最小セットを施行する「企業」プロファイルを作成します。部門レベルでは、必要なセキュリティー・レベルとデバイスの重要度に応じて、オペレーターが、デバイスの特定のセットに対して制限が厳しいポリシーを施行する特定の「部門」プロファイルを作成できます。最終的な結果として、デバイス上には、適用されているプロファイルの最も制限が厳しいパラメーターを結合したものが存在します。

運用上は、プロファイル管理は、2 つのステップがあるプロセスとして実装されます。最初のステップでは、セキュリティー管理者は、デバイスに対して施行する必要のあるポリシーを特定することによって、組織のセキュリティー方針を定義します。これらのポリシーは、1 つ以上のプロファイルを作成することで定義されます。オペレーターが、指定のサイトでプロファイルを作成および保存すると、そのサイトをサブスクライブしているすべてのコンピューターが、プロファイルに設定されているポリシーとの関連度を検査されます。デバイスがそのプロファイルに

関連するようになった場合、それは、そのデバイスが不適合であることを意味します。デバイスが、プロファイルと照合して検査されたときに、さらに制限の厳しい設定が見つかった場合、そのデバイスは関連しないと判断されます。

2 つめのステップでは、ポリシーに準拠する必要があるターゲットにプロファイルが適用されると、プロファイルで定義された構成は、ターゲットとなるすべてのデバイスに施行されます。このステップは、選択されたターゲットで必要なプロファイル構成を設定する Fixlet によって実行されます。ターゲット上でローカルで構成パラメーターが変更された場合、構成は自動的に再施行されます。ただし、ターゲットでローカルに設定されているパラメーターの方が適用されているプロファイルに対して現在施行されているパラメーターよりも制限が厳しい場合を除きます。プロファイルが正常に適用されると、そのプロファイルに対するデバイス上の状況は**「修正済み」**になります。

ターゲット上の複数のプロファイルの管理 - プロファイルの階層化

プロファイルはカテゴリーに分割されます。ターゲットに施行する必要がある 1 つ以上の設定が含まれるカテゴリーを個別に有効にできます。Windows 10 のターゲットでは、プロファイル内で有効にしたカテゴリーの各パラメーターが、WMI インフラストラクチャーに従って特定のデバイスにマップされます。Mac OS X のターゲットでは、有効にしたカテゴリーごとに新しい OS X プロファイルが作成されます。1 台の Mac デバイス上で、施行したカテゴリーごとに 1 つずつ最大 4 つの OS X プロファイルが BigFix プロファイル内に作成されます。デバイスのシステム環境設定から使用できる「プロファイル」グラフィカル・ユーザー・インターフェースで、OS X プロファイルを表示できます。

オペレーターは、1 つ以上のカテゴリーの設定を適用する複数のプロファイルを定義できます。プロファイルがターゲットに適用されると、施行されたすべてのプロファイル・カテゴリーの各設定が、ターゲット上の対応する設定と照合して評価されます。プロファイルの少なくとも 1 つの設定がターゲット上の対応する設定より制限が厳しい場合、ターゲットは関連する (非準拠) とみなされ、プロファイルが施行されます。ターゲットには複数のプロファイルを適用できます。評価は、常に個々の設定を比較することで、完了します。ターゲットの最終的なセキュリティー構成 (セキュリティー方針) は、最も制限が厳しい値が施行されるさらに多くのプロファイルの集合で構成されます。

ポリシーが中央またはローカルで変更された場合、管理者は現在施行されているプロファイルの適用を停止し、組織内または特定の部門内のすべてのデバイスのプロファイル構成をリセットできます。次に、新しいプロファイルをターゲットに適用できます。詳しくは、『Profile Management の構成のリセット』を参照してください。

注:

Mac OS X デバイスでは、BigFix Profile Management に適用されていないプロファイルが 1 つ以上存在する場合、既存のプロファイルと同じカテゴリーに属するパラメーターを設定する BigFix プロファイルを適用するときに、「失敗時の再試行回数」カウンターの満了後、適用が失敗します。この問題を解決するには、まずデバイスから既存のプロファイルを削除し、次に BigFix プロファイルを再適用します。特定のエラー・コードについて詳しくは、Mac OS X プロファイルの適用エラーを参照してください。

Windows 10 デバイスでは、プロファイル内の 1 つ以上のパラメーターに、現在デバイス上にあるより制限が厳しい設定がある場合、そのプロファイルは既に施行されています。

ユース・ケース例 - Windows 10 デバイスがある組織

この例では、ある企業が、複数の地理的位置に分散した 30 の部門と数千台の Windows 10 デバイスを持っています。セキュリティー担当者は、特定の部門メンバーシップに関係なくすべてのデバイスが準拠する必要がある共通ポリシーのセットから成る、企業全体のセキュリティー方針を確立します。各部門の管理者は、デバイスとユーザーの役割に基づいて、特定の部門のみに有効な特定のセキュリティー設定を定義し、ローカルに適用できます。

この例では、Windows 10 デバイス *Win10_DeptB_SWAdm* は、地理的にはロンドンにある組織内の部門 B に属しています。デバイスは、部門内のデバイスへの必須ソフトウェアのインストールを担当するソフトウェア管理者によって使用されます。階層化の動作を説明すると、企業プロファイル、部門プロファイル、組織内のソフトウェア管理者に固有のプロファイルの 3 つのプロファイルが作成され、デバイスに適用されます。プロファイルの階層化では、カテゴリーごとに各設定が検査され、最も制限が厳しい設定が施行されるようにします。

企業レベルのセキュリティー方針では、組織内のすべてのパスワードの長さが 8 文字以上であり、20 日後に期限が切れることを確立します。さらに、Cortana の使用は許可されません。

この方針を施行するために、セキュリティー管理者は、次の設定の企業プロファイルを作成します。

表 1. ProfileCorp_Win10 - 会社内のすべての Windows 10 デバイスのプロファイル

プロファイル・カテゴリー	設定
パスワード設定	パスワードは **20** 日後に期限が切れます
	最短パスワード長は **8** 文字です
制約事項	Cortana は**無効**になっています

プロファイルが適用され、*Win10_DeptB_SWAdm* を含め、組織内のすべてのデバイスに対して施行されます。プロファイルがデバイスに正常に適用されると、デバイスは準拠状態になります。

セキュリティー管理者は、*Win10_DeptB_SWAdm* を含め、組織全体にまたがってソフトウェア管理者が使用するすべてのデバイスに適用する必要があるプロファイルを定義します。このプロファイルにより、次の設定が施行されます。

表 2. Profile_Corp_SWAdmins - 企業内のソフトウェア管理者が使用するすべてのデバイスのプロファイル

プロファイル・カテゴリー	設定
パスワード設定	パスワードの最小長は **15** 文字です
	3 回、正しくないパスワードを施行すると、デバイスは BitLocker 回復モードになります
	パスワードは **10** 日後に期限が切れます
制約事項	テレメトリー・レベルは**「セキュリティー」**に設定されます

ロンドンにいるローカルのセキュリティー管理者は、その地域の部門 A、B、および C に対して部門をまたがるプロファイルを定義します。このプロファイルの設定は次のとおりです。

表 3. Profile_London_DeptABC - ロンドンのすべての Windows 10 デバイスのプロファイル

プロファイル・カテゴリー	設定
パスワード設定	パスワードの最小長は **12** 文字です
アプリ・セキュリティー	「アプリ・ストアの自動更新を許可」は**無効**になっています
制約事項	Cortana は**有効**になっています (デフォルト)
	ロケーション・サービスは**「オフ」**に設定されます
	テレメトリー・レベルは**「基本」**に設定されます

このプロファイルは、*Win10_DeptB_SWAdm* を含め、ロンドンの部門 A、B、C に属するすべてのデバイスに適用されます。

結果として、デバイス *Win10_DeptB_SWAdm* のセキュリティー構成は、次の表に示すように、3 つすべてのプロファイルの最も制限が厳しい設定を結合したものになります。

表 4. ターゲット Win10_DeptB_SWAdm のセキュリティー構成

カテゴリー	設定
パスワード設定	パスワードの最小長は **15** 文字です (プロファイル *Profile_Corp_SWAdmins* より)
	パスワードは **10** 日後に期限が切れます (プロファイル *Profile_Corp_SWAdmins* より)
	3 回、正しくないパスワードを施行すると、デバイスは BitLocker 回復モードになります (プロファイル *Profile_Corp_SWAdmins* より)
アプリ・セキュリティー	「アプリ・ストアの自動更新を許可」は**無効**になっています (プロファイル *Profile_London_DeptABC* より)
制約事項	Cortana は**無効**になっています (プロファイル *ProfileCorp_Win10* より)
	ロケーション・サービスは**「オフ」**に設定されます (プロファイル *Profile_London_DeptABC* より)
	テレメトリー・レベルは**「セキュリティー」**に設定されます (プロファイル *Profile_Corp_SWAdmins* より)

Profile Management の構成のリセット

少なくとも 1 つのプロファイルが存在する各サイトで、デバイス上のプロファイル構成のリセットに対応するタスクが、Windows 10 デバイスと Mac OS X デバイスに対して使用できます。このタスクを Windows デバイスで実行

すると、Profile Management によって有効になったカテゴリーのパラメーターがすべて削除され、手動または他のアプリケーションによって設定されたパラメーターも削除されます。

MAC OS X デバイスでは、このタスクは Profile Management によって作成されたすべてのプロファイルが削除されます (施行されたカテゴリーごとに 1 つで、最大 4 つのプロファイルが削除されます)。このタスクを実行する状況は次のとおりです。

- 企業のセキュリティー・ポリシーが変更され、すべてのデバイスに対して新しいポリシーを施行するとき。
- ある部門から別の部門に数台のデバイスを移動しようとしていて、新しい部門には異なるセキュリティー要件があるとき。
- 一時的にまたは永続的に、より制限が少ないポリシーを 1 つ以上のデバイスに対して施行する必要があるとき。

「コンテンツ」 > 「カスタム」を選択し、検索フィールドに 「`Reset`」と入力します。Windows および MAC OS X 用の使用可能なリセット・タスクのリストが表示されます。フィルターを使用して、検索内容を特定のサイトやオペレーターに絞り込むこともできます。リセット・タスクの実行前に、プロファイル管理パラメーターをリセットするターゲットに対して現在施行されている、進行中のプロファイルのデプロイメントをすべて停止する必要があります。

オペレーターのログイン許可によっては、複数のリセット・タスクが表示される場合があります。リセット対象のデバイスがサブスクライブしているサイトに保管されているタスクを適用してください。

Windows 10 デバイス用のプロファイル属性

Windows 10 デバイスでセキュリティー・コンプライアンスを実施するには、必要な設定を含む 1 つ以上のプロファイルを作成します。このタスクを完了するには、正しい許可が必要です。『オペレーターの権限および関連プロファイル・アクション』を参照してください。

1. **「プロファイル名」**、**「説明」**を指定し、プロファイルが作成された**「サイト」**を選択します。使用可能なサイトは、自分がオペレーター・ログインを許可されているサイトです。これらのフィールドは必須です。左側のペインに表示されているカテゴリー用のセキュリティー・ポリシーを適用できます。カテゴリー内の属性を変更または指定するには、まず**「オン」**をクリックしてそれを有効にする必要があります。設定を変更せずにカテゴリーを有効にすると、グレーで表示されている値は、プロファイルを適用したときにデバイスに対して施行されません。プロファイルを保存するには、少なくとも 1 つのカテゴリーを有効にする必要があります。

   注: 「プロファイル名」フィールドと「説明」フィールドには、二重引用符 " を指定できません。

2. **「パスワード設定」**タブを選択して、Windows 10 デバイスの認証設定を変更します。以下のプロパティーを指定できます。

   `[0]` 日後にパスワードの有効期限が切れます

ユーザー・パスワードの変更が必要となるまでの期間を日数で指定します。許可される値は、0 から 730 までの範囲の値です。0 (ゼロ) は、パスワードが期限切れにならないことを意味します。最も制限が厳しい値は 1 です。

最後の [0] 個のパスワードのパスワード履歴の記録。

再利用できない直近のパスワードの数を指定します。許可される値は、0 から 24 までの範囲の値です。ここで、0 (ゼロ) は、この検査を有効にしないことを意味し、最も制限が厳しい値は 24 です。

パスワード制御のアクティブ化

このオプションを選択すると、パスワードに少なくとも 3 つの複合エレメント・タイプ (大文字と小文字、数字など) があることを要求する強力なパスワード・スキームが自動的に施行されます。オプションで、特殊文字も指定できます。PIN を使用する場合、同じ複雑性ルールが施行されます。これが、最も制限が厳しいポリシーです。また、以下の制御を設定したり変更したりすることができます。

[0] 回、正しくないパスワードを施行すると、デバイスは BitLocker 回復モードになります

許可される値は、4~16 までの範囲または 0 (ゼロ)で、 デフォルト値であるゼロは、ポリシーが施行されないことを意味します。デバイスで BitLocker が有効になっている場合、このポリシーで設定した値に達すると、デバイスは再起動されて BitLocker リカバリー・モードになり、ユーザーが BitLocker リカバリー・キーを指定する必要があります。BitLocker が有効になっていない場合、デバイスはリブートされるのみです。最も制限が厳しい値は 4 です。

無操作状態で [0] 分経過した後にデバイスがロックされる。

ユーザー入力がない状態で何分待機したらデバイスがロックされるかを指定します。指定された時間が経過すると、デバイスは PIN またはパスワードのロック状態になります。許可される値は、0 から 999 までの範囲の値です。0 の値は、タイムアウトはアクティブではなく、デバイスがロックされないことを示します。最も制限が厳しい値は 1 です。

パスワードの最小長は [4] 文字です

パスワードまたは PIN に必要な最短の長さを指定します。許可される値は、4 から 14 までの範囲の値で、デフォルト値は 4 です。ただし、ローカル・アカウントでは、常に最短パスワード長として 6 文字が強制されます。最も制限が厳しい値は 14 です。

単純なデバイス・パスワードの使用を許可 (Allow use of simple device passwords)

このオプションは、デバイスに対応する読み取り装置が装備されている場合、デバイス上のアカウントに対して、ピクチャー・パスワードまたは生体認証方式 (指紋認識、虹彩認識など) を使用したサインインを許可します。このオプションは、デフォルトで有効です。

3. **「デバイス・セキュリティー」**タブを選択して、次のプロパティーを変更します。

ストレージ・カードを許可

デバイス・ストレージとしてリムーバブル・ストレージ・カードの使用をユーザーに許可するかどうかを制御します。デフォルトでは許可します。リムーバブル SD カードの使用を防止し、デバイスの USB ドライブを無効にするには、この値の選択を解除してください。

デバイス検出を許可

このポリシーは、ロック画面が表示されたときに、デバイスが他のデバイスを検出できるかどうかを制御します。デフォルトでは許可します。これにより、別の画面に射影する `Win+P` や、無線モニターとオーディオ・デバイスを検索する `Win+K` などのショートカットを使用できるようになります。このオプションの選択を解除すると、これらのショートカット・キーの使用が無効になります。

デフォルトでは両方のオプションが選択されています。

4. **「アプリ・セキュリティー」**タブを選択して、Windows アプリケーションの次のセキュリティー オプションを指定します。

アプリ・ストアの自動更新を許可

この設定は、Windows ストアのアプリの自動更新を有効にします。

信頼済みアプリのインストール

このポリシー設定は、Windows ストア以外の、証明書によって信頼されたアプリケーションをデバイスにインストールできるようにします。使用可能な設定のいずれかを選択します。

構成されていません

これがデフォルト値で、ポリシーが使用されないことを意味します。

明示的に許可

デバイスに Windows 以外のストアの信頼されたアプリをインストールできます。

明示的に拒否

デバイスに Windows 以外のストアのアプリをインストールすることを許可しません。これは、最も制限が厳しいオプションです。

開発者モード

パッケージ化されていないアプリケーションの開発、適用、およびデバッグが許可されるかどうかを指定します。使用可能な設定のいずれかを選択します。

構成されていません

これがデフォルト値で、ポリシーが使用されないことを意味します。

明示的に許可

デバイスで、パッケージ化されていないアプリの開発および適用を有効にします。

明示的に拒否

このデバイスで、パッケージ化されていないアプリの開発およびデプロイメントは許可されません。これは、最も制限が厳しいオプションです。

注:「信頼済みアプリのインストール」ポリシー設定と**「開発者モード」**ポリシー設定に指定する値の組み合わせにより、デバイス上の「更新」と「セキュリティー」のページにある次の開発者機能の処理内容が影響を受けます。

- Windows ストア・アプリ
- サイドロード・アプリ
- 開発者モード

重要:「信頼済みアプリのインストール」に対して"「明示的に拒否」"を選択し、**「開発者モード」**に対して"「明示的に許可」"を選択した場合、後者のパラメーターが前者をオーバーライドするため、Windows ストア以外の信頼されるアプリケーションのインストールも許可されます。

「制限」タブを選択して、1 つ以上の特定のリソースへのアクセスを無効にします。制限できるリソースは、発話、タイプ入力、アカウント、電子メール、通知設定などの汎用的なリソースです。デフォルトでは、すべてのオプションが有効になっています。リスト内のすべてのリソースを無効にするには、**「すべて選択」**をクリックしてください。

カメラ

デバイス上でのカメラの使用を無効にします。

Microsoft アカウント接続

選択すると、Microsoft アカウントが電子メール以外に関連の接続認証とサービスを実行できないようにします。この制限は、ターゲットのデバイスにインストールされている Windows 10 ビルドによっては、Cortana の使用に影響する場合があります。

Microsoft 以外のアカウントの手動追加

選択すると、デバイス上のユーザーは Microsoft 以外の電子メール・アカウントを追加できなくなります。

設定の同期

デバイス上のすべての Windows 同期設定を無効にします。

Cortana

デバイス上のユーザーが Cortana にアクセスできるかどうかを指定します。

トースト

デバイスのロック画面上でのトースト通知を無効にします。

入力の個人情報設定

入力の個人情報設定の自動学習コンポーネント (Cortana が必要とする発話、手書き入力、タイプ入力、連絡先、およびカレンダーの情報を収集) を無効にします。選択すると、デバイス上で

自動学習が停止され、それまでに収集した学習情報がすべてクリアされます。Cortana と口述の無効化も行われます。

システム・テレメトリー・レベル (System Telemetry level)

デバイスが送信することを許可されるテレメトリー・イベントおよびデータ (診断、使用率、および信頼性などの情報) のレベルを定義します。4 つの異なるレベルを指定できます。レベルは累積的です。

セキュリティー

セキュリティー・データのみを送信します。セキュリティー更新に関連するデータのみが送信されます。これが、最も制限が厳しい値です。

基本

問題判別のためにシステム構成および正常性データのうちの限られた部分を送信します。このレベルには「セキュリティー」レベルのデータも含まれます。

拡張

アプリケーション使用率、パフォーマンス、デバイス固有のイベント、一部の診断に関するデータを送信します。このレベルには「基本」レベルおよび「セキュリティー」レベルのデータも含まれます。

全アクセス

問題を特定して解決するために必要なすべてのデータと、信頼性および使用率のデータを送信します。このレベルには「基本」、「拡張 (Enhanced)」、および「セキュリティー」の各レベルのデータも含まれます。

場所

ロケーション・サービスへのアクセスをアプリに許可するかどうかを指定します。

ロケーション・サービスを許可

ロケーション・サービスが有効になります。これはデフォルト値です。デバイス上のユーザーが、ロケーションのプライバシー設定 (オンまたはオフ) を制御および変更できます。

ロケーションを強制的にオフ

すべてのロケーションのプライバシー設定がグレーで表示されます。デバイスのユーザーは設定を変更できず、アプリは Cortana などのロケーション・サービスにアクセスできません。

ロケーションを強制的にオン

ロケーション・サービスが許可され、ロケーションのプライバシー設定がグレーで表示されます。デバイス上のユーザーは、ロケーション設定を変更できません。

MAC OS X デバイスのプロファイル・プロパティー

MAC OS X デバイスでセキュリティー・コンプライアンスを実施するには、必要な設定を含む 1 つ以上のプロファイルを作成します。このタスクを完了するには、正しい許可が必要です。『オペレーターの権限および関連プロファイル・アクション』を参照してください。

1. **「プロファイル名」**、**「説明」**を指定し、プロファイルが作成された**「サイト」**を選択します。使用可能なサイトは、自分がオペレーター・ログインを許可されているサイトです。これらのフィールドは必須です。左側のペインに表示されているカテゴリー用のセキュリティー・ポリシーを適用できます。カテゴリー内の属性を変更または指定するには、まず**「オン」**をクリックしてそれを有効にする必要があります。設定を変更せずにカテゴリーを有効にすると、グレーで表示されている値は、プロファイルを適用したときにデバイスに対して施行されません。プロファイルを保存するには、少なくとも 1 つのカテゴリーを有効にする必要があります。

   注: 「プロファイル名」フィールドと「説明」フィールドには、二重引用符 " を指定できません。

2. **「パスコード設定」**タブを選択して、次のプロパティーを設定または変更します。

   単純な値を許可

   パスコード内で、`AAAA` または `1234` などのように、連続する文字を使用することも、同じ文字を繰り返すこともできます。このオプションは、デフォルトで選択されています。

   パスコードの最小長は `[0]` 文字です

   パスコードの最短の長さを指定します。許可される値は、`0-50` までの範囲の値です。デフォルト値の `0` は、パスコードの長さが検査されないことを示します。最も制限が厳しい値は 50 です。

   パスワードには少なくとも `[0]` 個の複合文字が必要です

   パスコードに含まれている必要のある非英数字 ($ および ! など) の数を指定します。許可される値は、`0-50` までの範囲の値です。ここで、50 が最も制限が厳しい値です。

   `[0]` 日後にパスコードの有効期限が切れます

   許可される値は、`0-730` までの範囲の値です。ここで `0` は、パスコードが無期限に有効であることを意味します。デフォルトは `730` です。最も制限が厳しい値は `1` です。

   最後の `[0]` 個のパスワードのパスコード履歴を適用

   再利用できない直近のパスワードの数を指定します。許可される値は、`0-50` までの範囲の値です。ここで値 `0` は、この検査を有効にしないことを示します。新規パスコードを入力すると、指定された数の直近のパスコードと比較されます。一致するものが見つかった場合、そのパスコードは拒否されます。最も制限が厳しい値は `50` です。

   無操作状態で `[0]` 分経過した後に画面をロックする。

   許可される値は、`0-5` までの範囲の値です。デフォルト値の 0 は、画面がロックされないことを意味します。最も制限が厳しい値は `1` です。

   `[10]` 回ログイン試行に失敗するとデバイスをロックする。

指定された回数だけログイン試行が失敗すると、デバイスがロックされます。許可される値は、`0-11` までの範囲の値です。デフォルト値 `0` は、デバイスがロックされないことを示します。最も制限が厳しい値は 1 です。

ログイン・ウィンドウが再表示されるまでの `[0]` 分の「遅延の設定」

ログイン試行の失敗が定義された回数に達したためにデバイスがロックされると、デバイスは指定された分数だけ待機してから、ログイン・ウィンドウを再表示します。デフォルト値の 0 は、遅延がないことを意味します。「デバイスのロック」パラメーターで指定した値が 0 または 1 の場合、このオプションはグレーで表示され、変更できません。

デバイスがロックされたときにパスコードが必要になるまでの `[730]` 分の「猶予期間の設定」

有効な値は、`0-730` までの範囲の値です。ここで 0 は、猶予期間がなく、パスコードを直ちに入力する必要があることを意味します。これは、最も制限が厳しい値です。

3. **「デバイス・セキュリティー」**タブを選択して、次の設定を変更します。

外部ディスクの使用を許可

デバイス上で外部ディスク (USB キーなど) を使用できます。このオプションは、デフォルトで有効です。このオプションを無効にすることを選択する場合に、ターゲット・システムに外部ディスクが既にマウントされている場合、この制限を有効にするにはプロファイルのデプロイ後にシステムをリブートする必要があります。

リムーバブル・メディアの使用を許可

デバイス上で任意のタイプのリムーバブル・メディア (CD や DVD など) を使用できます。このオプションは、デフォルトで有効です。このオプションを無効にすることを選択する場合に、ターゲット・システムに CD/DVD が既にマウントされている場合、この制限を有効にするにはプロファイルのデプロイ後にシステムをリブートする必要があります。

ログアウト時にメディアを排出

ユーザーがログアウトしたときにすべてのリムーバブル・メディアを取り出すには、このオプションを選択します。デフォルトでは、このオプションは選択されていません。

AirDrop を有効化

デバイス上で AirDrop を使用して項目を共有することができます。このオプションは、デフォルトで有効です。

4. **「アプリ・セキュリティー」**タブを選択して、次の設定を変更します。

Game Center を有効化

デバイス上でゲーム・センターを使用できるかどうかを指定します。この設定は、デフォルトで有効に設定されています。以下のゲーム・センター・オプションの 1 つ以上を無効にすることができます。

マルチプレイヤー・ゲームを許可

複数のプレイヤーを許可します。

フレンドの追加を許可

プレイヤー・リストにフレンドを追加できます。

アカウント資格情報の変更を許可

ゲーム・センターにアクセスするためのユーザー ID およびパスコードを変更できます。

App Store によるプリインストール済みアプリの導入を制限

このオプションを選択すると、デバイス上にインストールされているオペレーティング・システムに含まれる無料のアプリケーションは、アプリ・ストアを通じて更新できなくなります。

App Store の使用を制限

MDM および Apple ソフトウェアによってインストールされたアプリケーションを更新するためにのみアプリ・ストアを使用する場合は、このオプションを選択します。

アプリの管理に管理者パスワードが必要

このオプションを有効にした場合、デバイス上でアプリケーションをインストールまたは更新するたびに、常に管理者パスワードを指定する必要があります。

Gatekeeper を有効化

Gatekeeper は、アプリがインストールされる前にマルウェアがあるかどうかをチェックして、デバイスを保護します。

Apple への診断データの送信を許可

Apple に診断データおよび使用状況データを送信します。このオプションは、デフォルトで有効です。

5. **「制限」**タブを選択して、デバイス上の「システム環境設定」で特定のリソースに対するユーザー・アクセスを無効にします。すべての環境設定が、デフォルトで有効になっています。無効にするリソースを 1 つ以上選択するか、**「すべて選択」**ボタンをクリックして、すべてのリソースを無効にします。選択するオプションのペインが、デバイス上でグレーで表示されるようになります。リソースは、次の 2 つのカテゴリーに分割されます。

    - システム環境設定:

      App Store

      Bluetooth

      CD および DVD (CDs and DVDs)

      デスクトップおよびスクリーン・セーバー (Desktop and Screen Saver)

      拡張

      iCloud

インターネット・アカウント

ネットワーク

プリンターおよびスキャナー (Printers and Scanners)

プロフィール

セキュリティー & プライバシー

共有

サウンド

Spotlight

起動ディスク

Time Machine

ユーザーおよびグループ

◦ その他

カメラ

組み込みカメラ、接続されているモニターの組み込みカメラ、または USB カメラの使用を無効にします。

iCloud ドキュメント & データ

iCloud ドライブ用にセットアップされているデバイス上に、プレゼンテーション、イメージ、その他の文書を格納する可能性を無効にします。

iCloud キーチェーン

iCloud キーチェーンが Safari Web サイトのユーザー名とパスワード、およびクレジット・カード情報を格納するのと、Wi-Fi ネットワークを最新に維持するのを防止します。この設定は、**「Safari」 > 「環境設定」 > 「パスワード」**にあります。

ローカル・アカウント用の iCloud パスワード

iCloud の ID とパスワードを使用して MAC OS X デバイスのロックを解除するのを防止します。この設定は、OS X の「システム環境設定」の下の「ユーザーとグループ」にあります。

Spotlight のインターネット候補 (Spotlight internet suggestions)

アプリ、文書、イメージ、その他のファイルの検索に対する Spotlight の使用を無効にします。

第 3 章. プロファイルの適用のトラブルシューティング

適用に失敗したときに、使用できるログとエラー・コード情報を表示して、エラーの原因を判別できます。

Profile Management は、エラーの原因を把握するのに役立つように、BigFix server、WebUI サーバー、デバイス上の適用アクションに関する情報を格納します。

MCM 削除ポリシーを使用して制限付きのプロファイルを削除できません。

WebUI からプロファイル管理アプリケーション (非推奨) を使用して制限プロファイルを作成してデプロイした場合、プロファイルはエンドポイントにローカルにインストールされます。この場合**「WebUI」 > 「アプリケーション」 > 「MDM」 > 「ポリシーの削除」**アクションを使用して制限を削除しようとすると、機能しません。ただし、コマンド・ラインで次のローカル・コマンドを使用して、エンドポイントからこのようなポリシーを削除できます。

1. プロファイル識別子を一覧表示するには

   ```
   sudo profiles -P
   ```

2. 指定された $profile_identifier を持つプロファイルを削除するには

   ```
   sudo profiles -R -p $profile_identifier
   ```

WebUI サーバーのログ・ファイル

WebUI サーバーでは、プロファイルが保存されるときに発生するエラーに関する情報を表示でき、対応する Fixlet が作成され、BigFix サーバーに送信されます。ログ・ファイルは、次の場所に格納されます。

- Windows: `\\Program Files (x86)\BigFix Enterprise|BES Server\WebUI\Logs\`
- Linux: `//var/opt/BESServer/WebUI/Logs`

Profile Manager に対する特定のログ・ファイルは次です。 `prfmgr.log`

Profile Management の WebUI サーバー・サイトのログ・レベルの設定方法

WebUI のロギング・レベルを変更するには、「サーバー設定の定義」の説明に従って、**_WebUI_Logging_Filter** クライアント設定を追加する必要があります。Profile Management のロギング・レベルを設定するには、特定のトークンを追加する必要があります。指定する値によって、`prfmgr.log` に書き込まれる内容が決まります。ロギング・レベル詳細 (debug、verbose、または error) も指定できます。使用可能なトークンは以下のとおりです。

```
bf:bfdata-prfmgr
bf:bfdata-prfmgr:all-creators
bf:bfdata-prfmgr:all
bf:bfdata-prfmgr:get-applicable-count
bf:bfdata-prfmgr:get-deployment-count
bf:bfdata-prfmgr:profile


bf:prfmgr
```

```
bf:prfmgr:deployments
bf:prfmgr:devices
bf:prfmgr:profile_action_handler
bf:prfmgr:profile_fixlet_creator
bf:prfmgr:initialize
bf:prfmgr:tasks
bf:prfmgr:profiles
```

例えば、すべての Profile Management トレースをログに記録するには、**_WebUI_Logging_Filter** クライアント設定に次の値を書き込みます。`bf:prfmgr:*`.

すべてのクエリーも表示する場合は、次を指定して、データベースによりログに記録されるメッセージを追加する必要があります。 `bf:prfmgr:*,bf:database:*`

ターゲットのログ・ファイル

プロファイルがターゲット・デバイスに適用されると、適用されるプロファイルごとに作成されるログ・ファイルで、役立つ情報を見つけることができます。

Windows 10

パス `\\Program Files (x86)\BigFix Enterprise|BES Client\_BESdata\_Global\PrfmgrLog` 内で、デプロイされたプロファイルごとにファイルが作成されます。ログ・ファイルの名前は、プロファイル名の後に拡張子 `.log` を付けて構成されます。プロファイルのログ・ファイルに含まれる情報は、次のとおりです。

- そのプロファイルで施行されるセキュリティー設定。
- ターゲット・デバイス上の現在の設定。
- デバイスの最終的な状態。エラーの場合は、失敗メッセージまたは WMI 終了コード。

Mac OS X

ターゲットの `/var/tmp/BES` ディレクトリーに次のログ・ファイルが格納されます。

- `PRF_Profile_WebUI_*`: このファイルには、指定したカテゴリーについて最後にインポートされたプロファイルが含まれます。
- `com.bigfix.profile.*`: エラー情報がある作業ファイルが含まれます。
- `profileLoad.output`: このファイルには、プロファイルの操作ログが含まれます。

Mac OS X プロファイルの適用エラー

BigFix Profile Management によって作成されたのではないプロファイルで、適用するのと同じカテゴリーのプロファイルを施行するプロファイルが存在する Mac OS X デバイスにプロファイルを適用すると、「デバイス結果」ページに、メッセージ `This action failed because another non-BigFix profile already enforces the category on this target` が、エラーの原因になったカテゴリーに対応する終了コード (詳細は下記リスト) とともに表示されます。

- 91 - パスコード
- 92 - デバイス・セキュリティー
- 93 - アプリ・セキュリティー
- 94 - 制限

重要:

これらの結果が WebUI に表示されるのは、「失敗時の再試行回数」カウンターの満了後のみです。カウンターがまだアクティブなとき、適用は「待機中」状態のままです。この時間フレーム中に、BigFix コンソールにログインして、終了コードを確認し、関連アクションら調べることができます。

Notices

This information was developed for products and services offered in the US.

HCL may not offer the products, services, or features discussed in this document in other countries. Consult your local HCL representative for information on the products and services currently available in your area. Any reference to an HCL product, program, or service is not intended to state or imply that only that HCL product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any HCL intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-HCL product, program, or service.

HCL may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

HCL
330 Potrero Ave.
Sunnyvale, CA 94085
USA
Attention: Office of the General Counsel

For license inquiries regarding double-byte character set (DBCS) information, contact the HCL Intellectual Property Department in your country or send inquiries, in writing, to:

HCL
330 Potrero Ave.
Sunnyvale, CA 94085
USA
Attention: Office of the General Counsel

HCL TECHNOLOGIES LTD. PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. HCL may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-HCL websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this HCL product and use of those websites is at your own risk.

HCL may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

HCL
330 Potrero Ave.
Sunnyvale, CA 94085
USA
Attention: Office of the General Counsel

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by HCL under terms of the HCL Customer Agreement, HCL International Program License Agreement or any equivalent agreement between us.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary.

Information concerning non-HCL products was obtained from the suppliers of those products, their published announcements or other publicly available sources. HCL has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-HCL products. Questions on the capabilities of non-HCL products should be addressed to the suppliers of those products.

Statements regarding HCL's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to HCL, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. HCL, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS," without warranty of any kind. HCL shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work must include a copyright notice as follows:
© (your company name) (year).
Portions of this code are derived from HCL Ltd. Sample Programs.

Trademarks

HCL Technologies Ltd. and HCL Technologies Ltd. logo, and hcl.com are trademarks or registered trademarks of HCL Technologies Ltd., registered in many jurisdictions worldwide.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other product and service names might be trademarks of HCL or other companies.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the HCL website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of HCL.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of HCL.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

HCL reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by HCL, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

HCL MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.