BigFix
WebUI ユーザーズ・ガイド

Special notice

Before using this information and the product it supports, read the information in Notices (on page 506).

本書に関する注意事項

本書は、BigFix 10 の MCM バージョン 1.1、および新しい版で明記されていない限り、以降のすべてのリリースおよびモディフィケーションに適用されます。

目次

第 1 章. ようこそ.....1

第 2 章. WebUI の概要.....2

概要ページ.....2

ナビゲーション・バー.....6

グリッド表示.....6

リスト・ビュー.....8

文書ビュー.....9

フィルターおよび検索ツール.....11

テキスト検索.....12

リスト・コントロール.....13

すべてを選択.....14

権限とその効力.....15

WebUI ワークフローおよびデプロイ・シーケンス.....15

レポート.....16

第 3 章. デバイス入門.....21

デバイス・リスト.....22

デバイス文書.....30

ファイルの送信.....38

デバイスへのメッセージの送信.....42

第 4 章. パッチ入門.....45

パッチ・リスト.....45

パッチ文書.....52

第 5 章. パッチ・ポリシー入門.....54

パッチ・ポリシーの概要....54
パッチ・ポリシー・リスト....68
パッチ・ポリシーの作成....70
パッチ・ポリシー文書....87
デプロイ済みポリシーのモニタリング....91
パッチ・ポリシー運用: タスクのリファレンス....92
第 6 章. IVR 入門....98
IVR リスト....98
IVR 文書....115
Rapid 7 のサポート....116
WebUI IVR 設定....119
IVR のトラブルシューティング....123
リリース・ノート....126
第 7 章. ソフトウェア入門....128
ソフトウェア・パッケージ・リスト....128
ソフトウェア文書....129
ソフトウェア・カタログの操作....131
ソフトウェア・パッケージの追加....131
ソフトウェア・パッケージの編集....138
ソフトウェア・パッケージの削除....139
第 8 章. カスタム・コンテンツ入門....140
カスタム・コンテンツ・リスト....140
カスタム・コンテンツ文書....140
カスタム・コンテンツの作成....141
カスタム・コンテンツの編集....145

第 9 章. BigFix Query 入門.....148
サンプル照会の実行.....156
照会の作成.....160
タイトルなしタブ.....163
関連度の作成.....165
関連度の検索.....179
照会のパラメーターの管理.....182
第 10 章. アクションの実行: デプロイ・シーケンス.....184
デプロイ・シーケンスの要約.....184
デプロイ手順.....186
ターゲットの選択.....191
構成オプション.....199
第 11 章. デプロイメント入門.....209
デプロイメント・リスト.....209
デプロイメント文書.....214
デプロイメントのモニタリング: 状態、状況、結果.....215
デバイス結果.....215
デプロイメント状況.....217
デプロイメント状態.....218
複数のアクションを持つデプロイメントの評価.....218
デプロイメントの停止.....219
第 12 章. コンテンツ・アプリケーション入門.....220
第 13 章. Extension Management アプリケーション入門.....234
サイトからの拡張機能のインストール.....236
ファイルからの拡張機能のインストール.....238

拡張に対する作業....239
拡張機能の更新....242
拡張機能のアンインストール....245
第 14 章. Modern Client Management と BigFix Mobile....247
Modern Client Management ダッシュボード....250
MCM の役割と権限....259
デバイスのインベントリー....261
正常性チェック....264
対象デバイスを選択します。....269
プライマリー・ユーザー・フィルターと登録タイプ・フィルターの追加....269
MCM および BigFix Mobile コンポーネントのインストールと管理 - オンプレミスのみ....273
Windows 用の BigFix MDM サービスのインストール....276
Apple 用の BigFix MDM サービスのインストール....279
Android 用 BigFix MDM サービスのインストール....283
MDM サーバー機能の管理....288
Windows 用の MDM プラグインのインストール....292
Apple 用の MDM プラグインのインストール....294
Android 用の MDM プラグインのインストール....296
MDM コンポーネントの更新....297
MDM コンポーネントのアンインストール....298
資格情報の追加....302
資格情報の更新....304
資格情報の削除....305
ODJ サービスのインストールと管理....306

インストール....306
アップグレード....308
ODJ サービスの構成の更新....309
アンインストール....310
MDM サーバーの構成....311
MDM サーバーの構成の更新....313
MDM サーバーの構成の削除....315
BigFix MCM および BigFix モバイルの構成....317
スマート・グループ....318
グループの定義....322
属性の定義....324
スマート・グループの管理....329
デバイスの登録....335
一括登録 - Windows....335
ユーザーによる登録 - Windows....346
Autopilot 登録....347
Apple 自動デバイス登録....351
アプリケーションの管理....354
macOS BigFix インストーラーの事前ステージ....355
Windows BigFix インストーラーの事前ステージ....357
Apple Volume Purchase Program の有効化....359
アプリ構成....360
よくある質問....367
デバイスの管理....368
フル・ディスク暗号化....368

MCM ポリシーのデプロイ ... 376
BigFix エージェントのデプロイ ... 379
ポリシーの管理 ... 382
ポリシー・グループ ... 386
アプリ・デプロイメント・ポリシー ... 396
証明書ポリシー ... 402
テンプレートからカスタム ... 403
ディスク暗号化ポリシー ... 431
フル・ディスク・アクセス ... 435
カーネル拡張ホワイトリスト ... 436
キオスク・ポリシー ... 439
OS の更新ポリシー ... 443
パスコード・ポリシー ... 446
制限ポリシー ... 451
システム拡張ホワイトリスト ... 454
カスタム・ポリシーのアップロード ... 458
MCM アクションのデプロイ ... 460
デバイスの登録解除 ... 475
第 15 章. BigFix 管理機能の拡張 ... 480
クラウド・プラグインの管理 ... 481
プラグイン・ポータルのインストール ... 481
クラウド・プラグインのインストール ... 482
クラウド・プラグインでの作業 ... 488
AWS リージョンの制限によるデバイス検出範囲の設定 ... 491
クラウドで検出されたデバイスへの BigFix エージェントのインストール ... 497

クラウド・ネイティブのデバイスへの BigFix エージェントのインストール.....501

付録 A. サポート.....505

Notices.....506

索引.....

第 1 章. ようこそ

BigFix WebUI へようこそ。WebUI は、BigFix オペレーターのために優れた機能を提供します。WebUI は、BigFix ワークフローを簡易化し、データへのアクセスを加速し、柔軟性、可視性、パフォーマンスを向上させます。

WebUI を学習、使用するにあたり、BigFix の使用経験はほとんど必要ありません。必要なものは、ブラウザー、WebUI URL、BigFix ユーザー名とパスワードのみです。サポート対象ブラウザーに含まれているのは、最新バージョンの Edge、Safari、Firefox、Chrome です。

BigFix console に詳しい管理者およびオペレーターにとって、このガイドは有用な WebUI の手引きとなります。WebUI のインストールと管理について詳しくは、「BigFix WebUI 管理ガイド」を参照してください。

WebUI を開くには、管理者から提供された URL を使用し、BigFix ユーザー名とパスワードを入力します。シングル・サインオン・ユーザーは、BigFix ログイン画面をバイパスして、サービス・プロバイダー経由で認証されます。ログインが成功すると、ユーザーに BigFix の「概要」ダッシュボードが表示されます。

注: BigFix インターフェースの外観は変更されています。新しい色とテーマを反映したものに、本書のグラフィックを更新中です。作業が完了するまでご不便をおかけいたします。

第 2 章. WebUI の概要

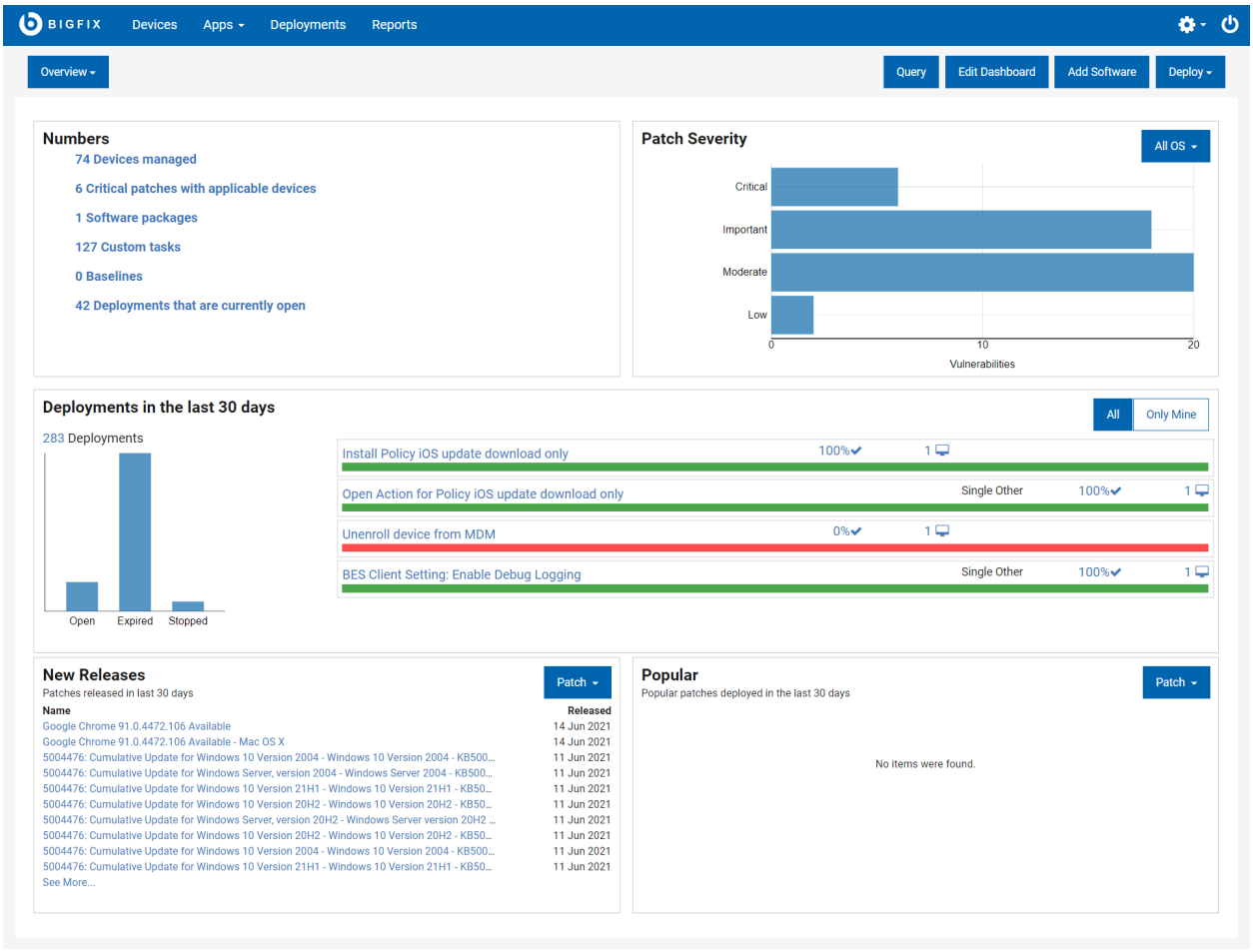
WebUI の画面、コントロール、およびワークフローについて簡単に説明します。

デプロイ・シーケンスとそのオプションなどの WebUI の各メイン画面の詳細説明については、デバイス入門 (（ページ） 21)を参照してください。BigFix の用語と概念の概要については、用語集 (（ページ）　　)を参照してください。

概要ページ

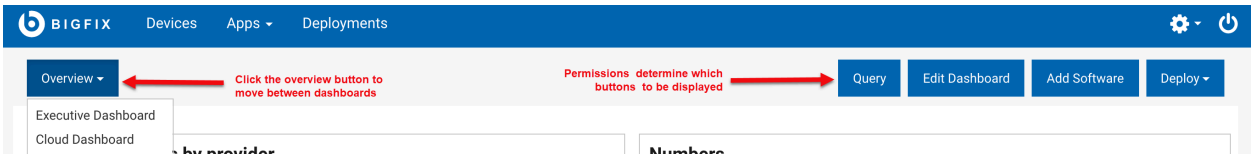
WebUI の「概要」には、ご使用の環境の要約が記載されます。インタラクティブ・グラフと豊富なリンクのセットによって、早急な対応を必要とする領域への迅速な移動が容易になります。

WebUI では、「概要」ページがデフォルトのランディング・ページです。「ナビゲーション・バー」（（ページ） 6)の BigFix ロゴをクリックすると、ユーザーは任意の WebUI 画面から概要ページに移動できます。ページ内のリンクは、各ビューへのショートカットとして使用できます。



- 最新データを表示するには、画面を更新します。
- 動的リンクをクリックすると、環境内の現在進行中の変更に対処できます。
- グラフや集計をクリックすると、詳細が表示されます。
- グラフィック要素にマウス・オーバーすると、基になる値が表示されます。
- 新規リリースと一般的なコンテンツをタイプ別にフィルターに掛けます。

オペレーターの権限、およびサイトと役割の割り当てによって、各 WebUI ページに表示されるページやデータ要素が制御されます。例えば、ソフトウェア配布コンポーネントへのアクセス権限のないオペレーターには、**「概要」**で**「ソフトウェアの追加」**ボタンが表示されません。



マスター・オペレーターのみが、アクティブなダッシュボードを編集してカスタマイズできます。詳しくは、「https://help.hcl-software.com/bigfix/10.0/platform/WebUI/Admin_Guide/c_permission_effects_in_the_webu.html」を参照してください。

- **概要**:「概要」のドロップダウン・リストでオプションを選択して、ダッシュボードを切り替えます。
  - 監視ダッシュボード「監視ダッシュボード」では、IT 担当者、セキュリティー担当者、アナリストに特に有益な情報が提供されます。監視ダッシュボードを表示するには、ナビゲーション・バーの下の**「概要」**ボタンをクリックし、**「監視ダッシュボード」**を選択します。ダッシュボード間を移動するには、**「概要」**ボタンを使用します。「監視ダッシュボード」およびそのタイルについて詳しくは、『WebUI 管理ガイド ((ページ)　　)』を参照してください。
  - クラウド・ダッシュボード:

    クラウド・プラグインをインストールしてクラウド・リソースを見つけたら、「クラウド・ダッシュボード」の「WebUI の概要」にクラウド・デバイスの要約が表示されます。クラウド・ダッシュボードを表示するには、ナビゲーション・バーの下の**「概要」**ボタンをクリックし、**「クラウド・ダッシュボード」**を選択します。ダッシュボードには、環境内のクラウド・リソース量を監視するタイルがあり、エージェントのインストールの有無にかかわらず、タイプと地域ごとの分布が表示されます。任意の棒グラフをクリックすると「デバイス」ページが開き、BigFix エージェント状況でフィルタリングされ、「管理対象」が事前選択されたリソースのリストが表示されます。
- **照会:** このボタンをクリックすると、照会エディターが開きます。
- **ダッシュボードの編集:** マスター・オペレーターのみが、アクティブなダッシュボードを編集してカスタマイズできます。詳しくは、「権限とその効力 ((ページ) *15)*」を参照してください。

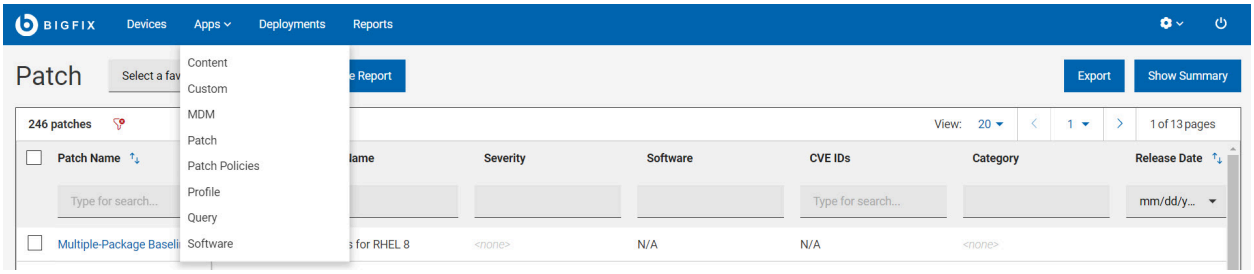
- **ソフトウェアの追加:** このボタンをクリックすると、ソフトウェア・パッケージをすばやくアップロードできます。
- **デプロイ**: このドロップダウンからオプションを選択して、カスタム・コンテンツ、パッチ、プロファイル、またはソフトウェアをデプロイします。
- **番号:** 環境に関する重要な統計を表示します。リンクをクリックすると、特定の項目のフィルターされたリストが表示されます。
- **パッチの重要度:** デフォルトでは、脆弱性に基づいて、すべてのオペレーティング・システムで使用可能なパッチの数が表示されます。特定のオペレーティング・システムのデータを表示するには、ドロップダウンからオプションを選択します。特定のタイプのパッチのフィルターされたリストを表示するには、それぞれの青色のバーをクリックします。
- **過去 30 日間のデプロイメント:** 環境内のすべてのデプロイメントの概要が表示されます。使用可能なリンクをクリックすると、その項目の詳細が表示されます。自分のデプロイメントの概要のみを表示するには、**「自分のもののみ」**をクリックします。
- **新しいリリース:** デフォルトでは、最新の 10 個の新しいパッチ・リリースが表示されます。ドロップダウンからオプションを選択して、環境に合わせて新しくリリースされたソフトウェアまたはカスタム・コンテンツを表示することもできます。**「詳細の表示...」**をクリックすると、項目の完全なリストが表示されます。
- **人気:** デフォルトでは、過去 30 日間にデプロイされた一般的なパッチが表示されます。ドロップダウンからオプションを選択して、過去 30 日間にデプロイされた一般的なソフトウェアやカスタム・コンテンツを表示することもできます。

WebUI セッションは、無操作状態の期間の後に自動的にクローズされます。セッションが期限切れになった場合、次回ログイン時は、最後に表示されていたページに戻ります。

注: ダッシュボード上のタイルを読み込むのに要する時間が 10 秒を超えると、読み込み時間の詳細がタイル上に表示されます。メッセージを消去するには、**「閉じる」**をクリックしてください。応答時間に影響を与える要因として、ハードウェアの変更、エンドポイント数の変更、アクセス可能なデータ量が挙げられます。

ナビゲーション・バー

ナビゲーション・バーを使用して、「概要」、「デバイス」、「デプロイメント」ページや、「アプリ」にあるさまざまなアプリケーションにアクセスできます。



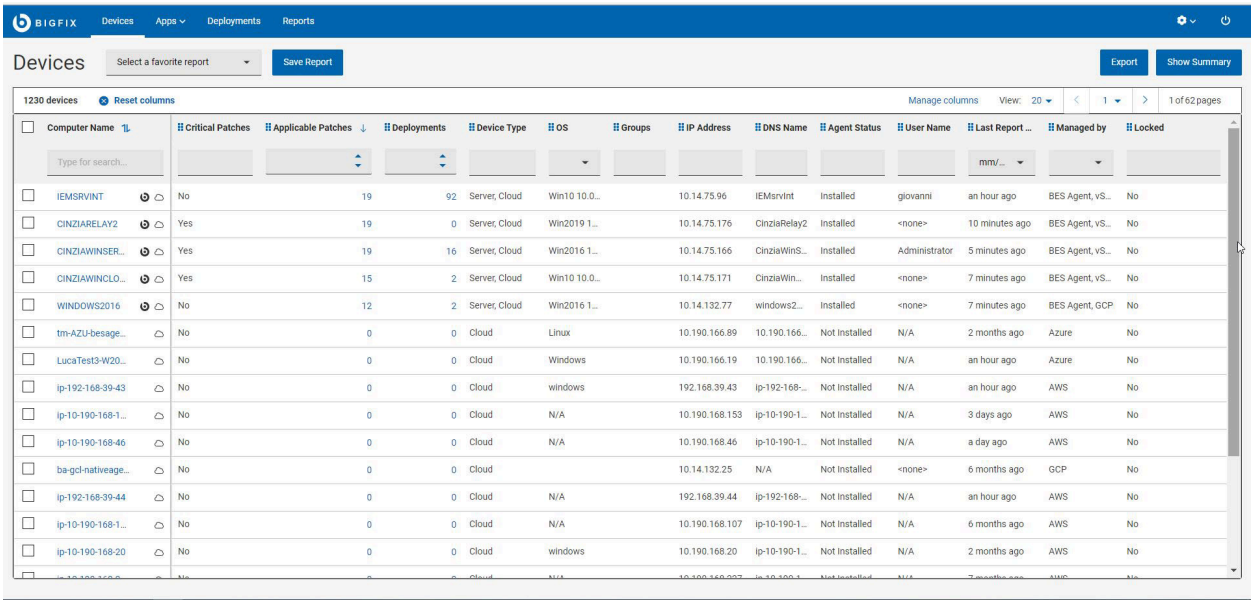
- BigFix ロゴおよび**「ホーム」**アイコンの両方から「概要」を開くことができます。
- メイン・メニューから**「デバイス」**をクリックして、レポートの BigFix デバイスのリストを表示し、それらのデバイスにアクションを適用します。
- メイン・メニューから**「デプロイメント」**をクリックして、BigFix アクションのリストの表示、詳細の検索、またはオープンなアクションの停止ができます。
- **「アプリ」**メニューから、コンテンツ、カスタム、MDM、パッチ、パッチ・ポリシー、プロファイル、照会、ソフトウェアなどの WebUI アプリケーションを起動します。
- **「レポート」**をクリックして、保存されたレポートを表示し、レポートを処理します。
- 歯車アイコンをクリックして、WebUI アプリケーションの設定を構成します。
- 「ログアウト」ボタンをクリックして、WebUI からログオフします。「ログアウト」ボタンの上にカーソルを移動すると、ログインしているユーザーの名前が表示されます。

グリッド表示

列をカスタマイズできる対話式テーブルの、すべてのプロパティーを表示します。

グリッド表示を使用すると、テーブルの項目をすばやく表示できます。項目のリンクをクリックすると、関連する資料のページが開きます。すべての列には、検索またはフィルターのオプションがあります。列の追加、削除、およびサイズ変更を行うことができま

す。現在のビューを「レポート」 (（ページ） 16)として保存することや、データのエクスポート、データの視覚化などができます。



注: オペレーター権限 (（ページ） 15)設定、接続済みデバイス、サイト割り当てによって、リストのコンテンツが左右されます。

デバイス・データ・グリッドのカスタマイズ

列の追加、削除、サイズ変更、または位置の変更によって、データ・グリッド・ビューをカスタマイズできます。「列のリセット」をクリックして、デフォルトのビューに戻ることもできます。

- **列幅のサイズを変更するには**
  1. 目的の列の境界線の近くにマウス・カーソルを移動します。
  2. マウスの左ボタンをクリックしたまま、右に境界線をドラッグして列を広げるか左にドラッグして列を狭くし、目的の幅に達したらマウス・ボタンを離します。
- **列の位置を変更するには**

1. 目的の列名にマウス・カーソルを移動します。
2. マウスの左ボタンをクリックしたまま、ドラッグしてデータ・グリッド内の任意の位置にドロップします。

結果の絞り込み

- データをフィルターするには、次の手順を実行します。
  - 目的の列で、リストからオプションを選択します。

    または
  - 目的の列のテキスト・フィールドをクリックし、検索文字列を入力します。

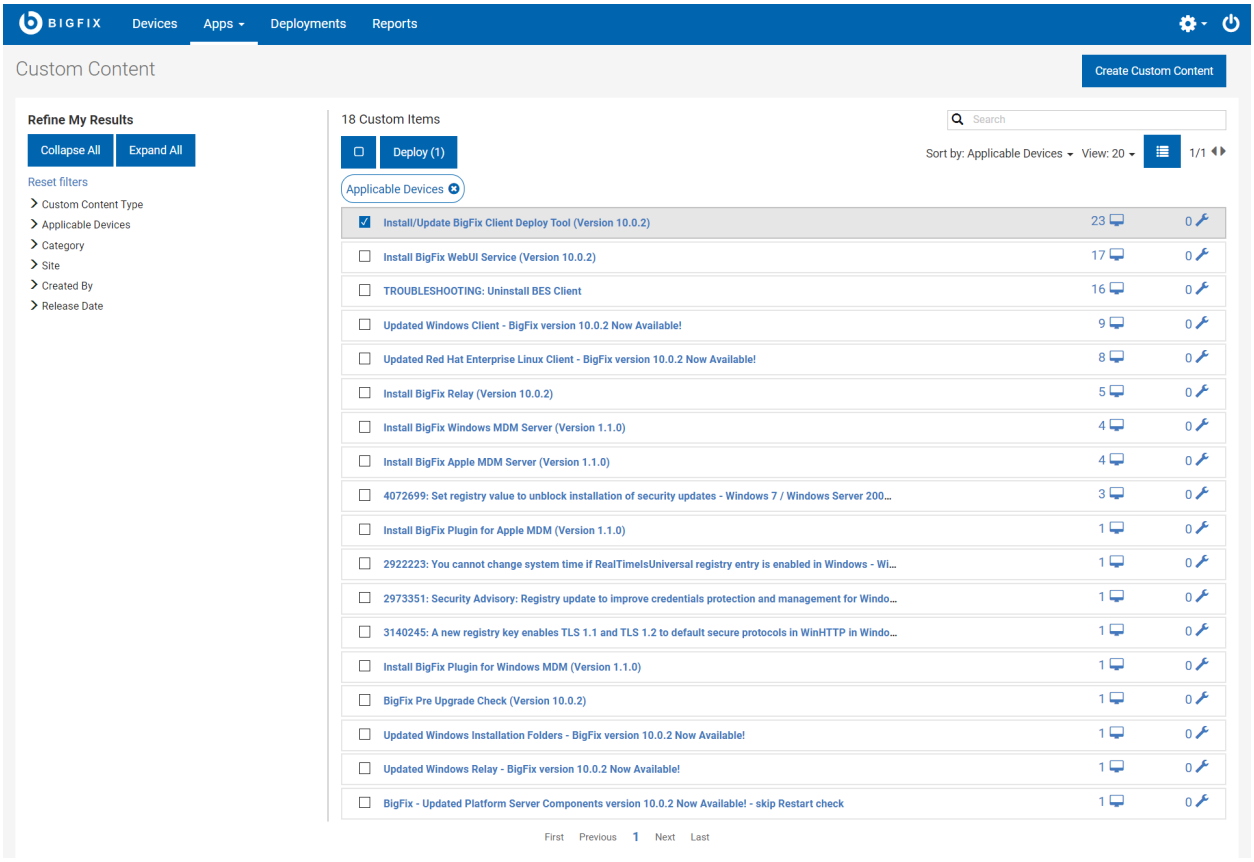
    注: 予約済みおよび集約コンピューター・プロパティーのサブセットに対してのみ、自動補完により、最初にいくつか入力した文字に基づいて、候補の単語のリストが表示されます。ユーザー定義のコンピューター・プロパティーを含むその他のプロパティーでは、自動補完は検索のパフォーマンスに影響するため機能しません。
- 検索を高速化するには、フィルターを組み合わせます。

  注: デフォルトでは、最大 5 つのフィルターを組み合わせて同時に処理できます。フィルターの最大数を超えると、パフォーマンスに影響します。デフォルト値は、`_WebUIAppEnv_MAX_FILTERS_NUMBER` (（ページ）　　) の設定を使用して構成できます。
- すべての選択済みフィルターをクリアするには、「すべてのフィルターのリセット」をクリックします。

リスト・ビュー

柔軟で、検索可能な索引であるリスト・ビューには、ご使用の BigFix 環境がディレクトリー形式で表示されます。

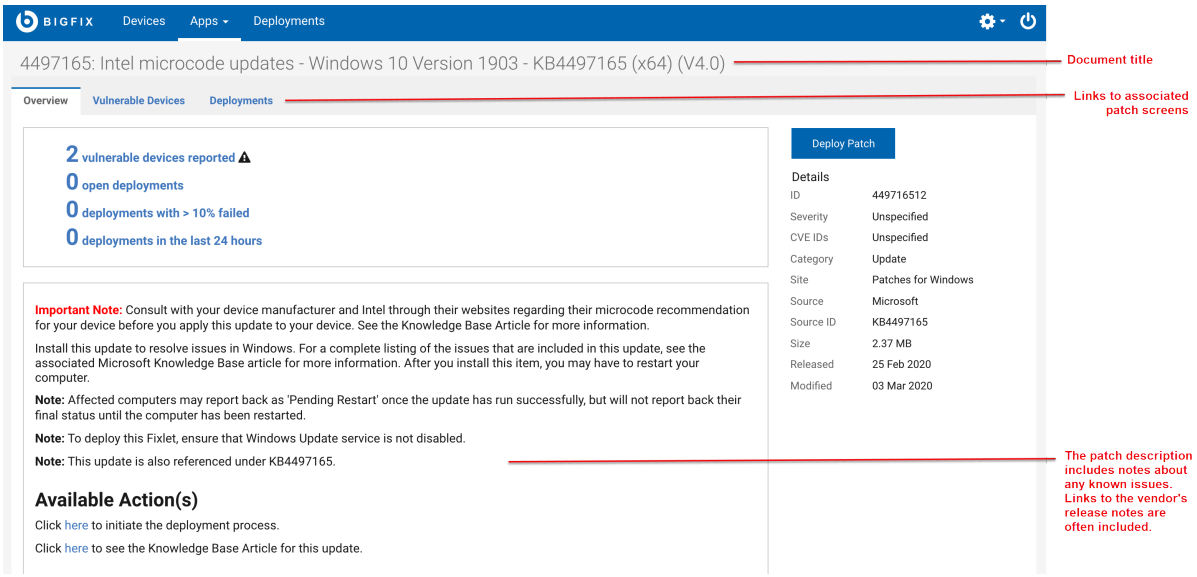
カード上のタイトルをクリックすることで、対応する文書を開きます。対象デバイスにカスタム コンテンツをデプロイするなどのアクションを実行するには、そのカードを強調表示して、**「デプロイ」**ボタンをクリックします。



- カードを選択するには、そのカードの任意の場所をクリックします。
- 選択済みのカードをクリアするには、そのカードをクリックします。
- カードの文書を表示するには、そのカードのタイトルをクリックします。
- カードに対して長すぎるタイトルをプレビューするには、カーソルをそのタイトルの上に移動します。

文書ビュー

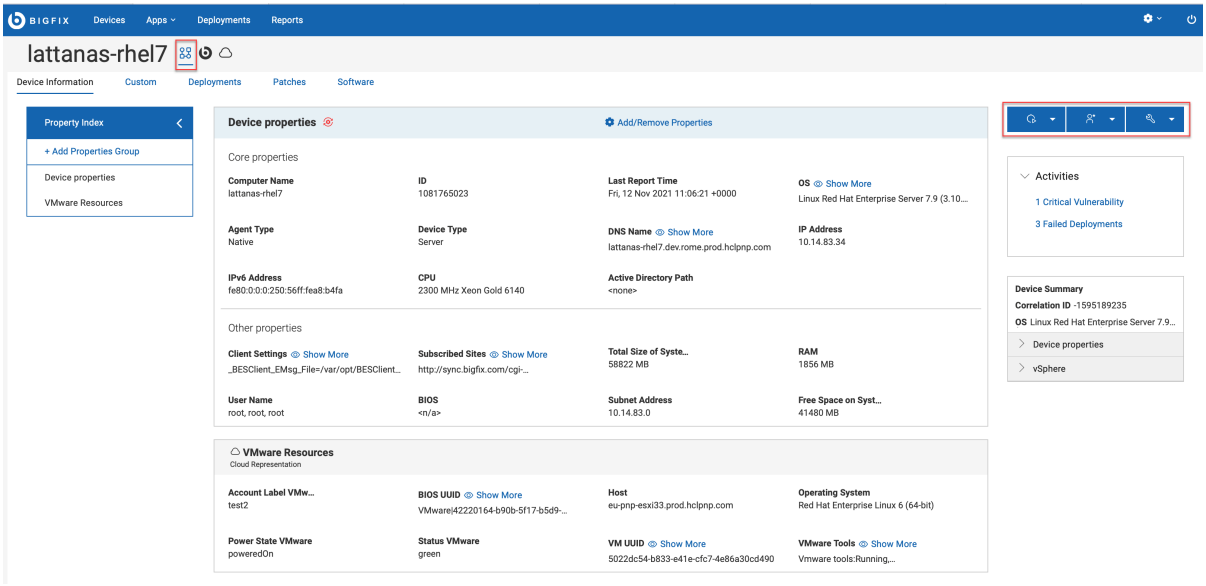
WebUI の文書ビューには、特定のデバイス、デプロイメント、またはコンテンツの一部に関する詳細情報が表示されます。文書のナビゲーション・リンクを使用して、関連付けられたビューでデータを掘り下げます。以下の図ではパッチ文書が表示されています。



右側のパネルには重要な詳細が要約され、すべてのデバイス文書とコンテンツ文書には**「デプロイ」**ボタンが表示されます。

以下はデバイス文書の「デバイス情報」ビューの画像です。タブを使って、追加のビューを表示します。

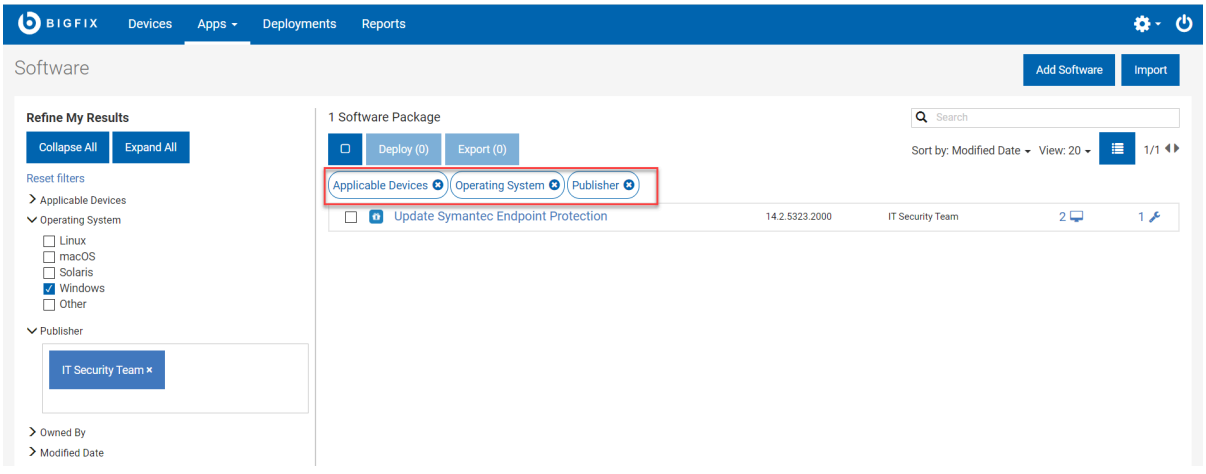
- **デプロイ**：  ボタンをクリックして、コンテンツをデバイスにデプロイします。
- **構成**：  ボタンをクリックして、照会の発行、ファイルの送信、このデバイスへのメッセージ送信を行います。



フィルターおよび検索ツール

WebUI のフィルターを使用し、長いリストを特定の項目の短いリストに縮小します。

例えば、ソフトウェア・リストをオペレーティング・システムでフィルターに掛け、OS X コンピューターのソフトウェアを表示します。フィルターを組み合わせることで、特定の発行元が発行したオペレーティング・システムごとのソフトウェア・リストなどを検索できます。

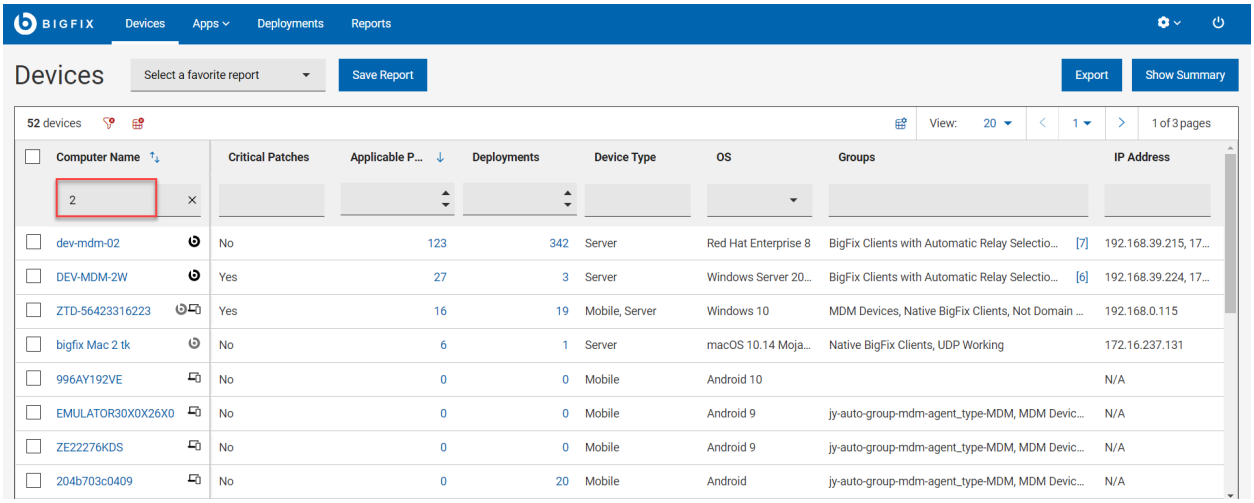


アクティブ・フィルター・グループのリストがリストの上部に表示されます。

- 「すべて縮小」をクリックしてフィルターを縮小表示
- 「すべて展開」をクリックしてフィルターを展開し、すべてのサブ・フィルターを表示
- 「フィルターのリセット」をクリックしてすべての選択済みフィルターをクリア
- 検索をスピードアップするには、フィルターを結合
- 「テキスト」フィールドをクリックし、オプションのリストから選択するか、検索ストリングの最初の数文字を入力

テキスト検索

テキストに含まれる単語や文字に基づいて項目を見つけるには、テキスト検索を使用します。例えば、名前に“「2」”という文字が含まれるデバイスをすべて見つけるには、デバイス・リストで“「2」”を検索します。

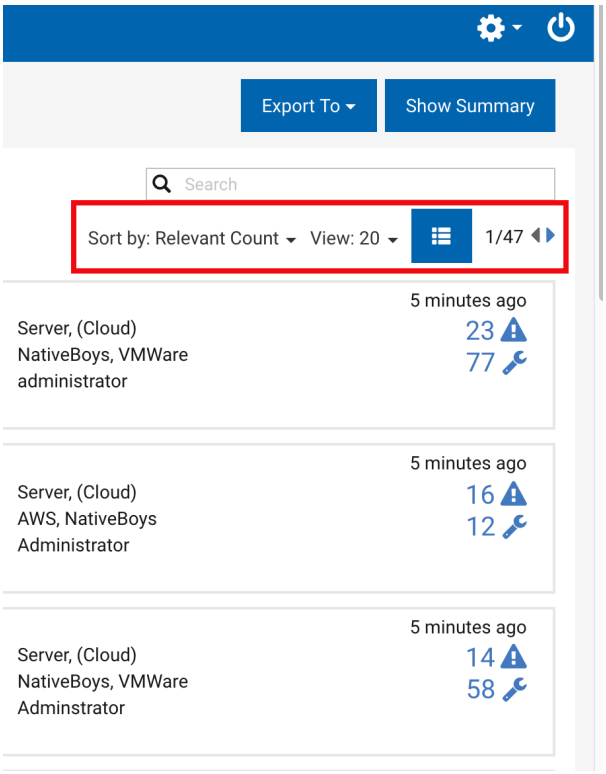


- 複数の用語が含まれる項目を見つけるには、複数語検索を使用します。例えば、“「MS13-035 Vista」”の検索結果には、パッチ“「MS13-035 *MSHTML Security Vulnerability* Vista」”が含まれます。
- 検索では大文字と小文字は区別されません。例えば、単語“「advisory」”でパッチ・リストを検索すると、名前に“「advisory」”または“「Advisory」”のいずれかが含まれるパッチが返されます。
- ワイルドカード検索、および文書の本文内のテキスト検索は現在サポートされていません。

リスト・コントロール

リスト・ビュー・コントロールを使用して、リストのソート、リスト項目の数と表示の調整、ページ間の移動を行います。

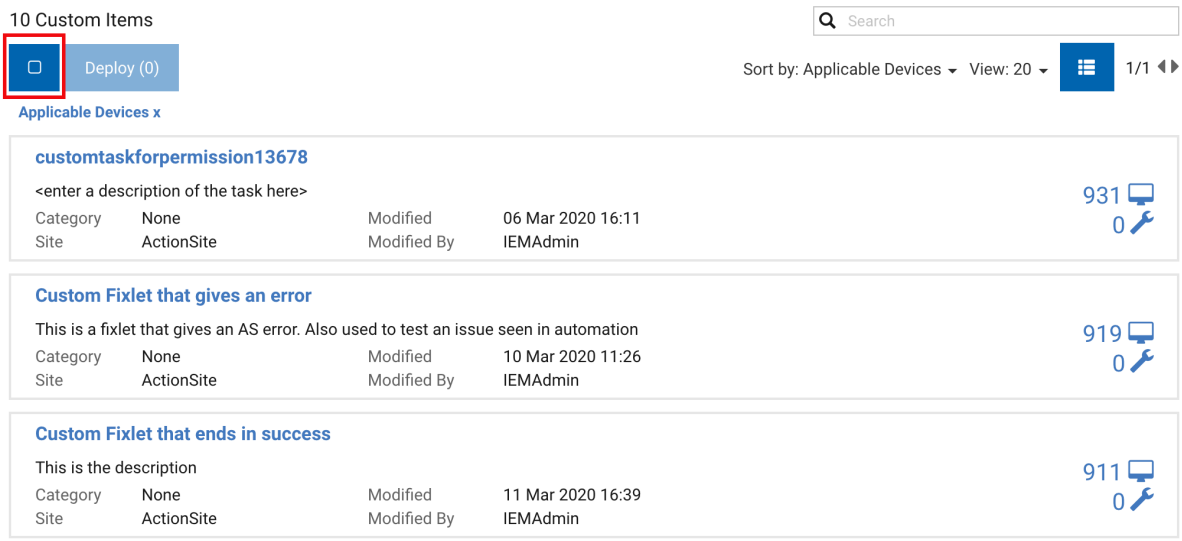
- ソート基準 - リストの上位に表示する項目を設定します
- 表示 - 表示されるレコード数を調整します
- 詳細の表示と非表示 - ページ上により多くの項目を表示します
- ページ・レイアウト・コントロール - 現在のページ番号、ページ数の表示、ページ間の移動



すべてを選択

「すべて選択」チェックボックスを使用して、ページ上のすべての項目を選択または選択解除します。

- 1 つのページ上のすべての項目を選択または選択解除します
- ページ上のすべての項目を選択または選択解除します
- 「デプロイ」ボタンにページを通しての合計が表示されます
- 選択内容はページを移動しても維持されます。



権限とその効力

WebUI 画面に表示される要素は、ユーザーの権限レベル、および BigFix 管理者によってそのユーザーに設定されたデバイス、サイト、グループの割り当てを反映します。

例えば、Windows マシンへのパッチ適用を担当するオペレーターには、パッチ・リストに Linux パッチが表示されることも、デバイス・リストに Linux マシンが表示されることもありません。ソフトウェアをデプロイするが、パッチ適用は行わないオペレーターには、コンテンツ・サブメニューにパッチ・コンテンツやカスタム・コンテンツのオプションが表示されません。権限と、WebUI 画面とデータ要素への権限の影響について詳しくは、「BigFix WebUI 管理者ガイド」を参照してください。

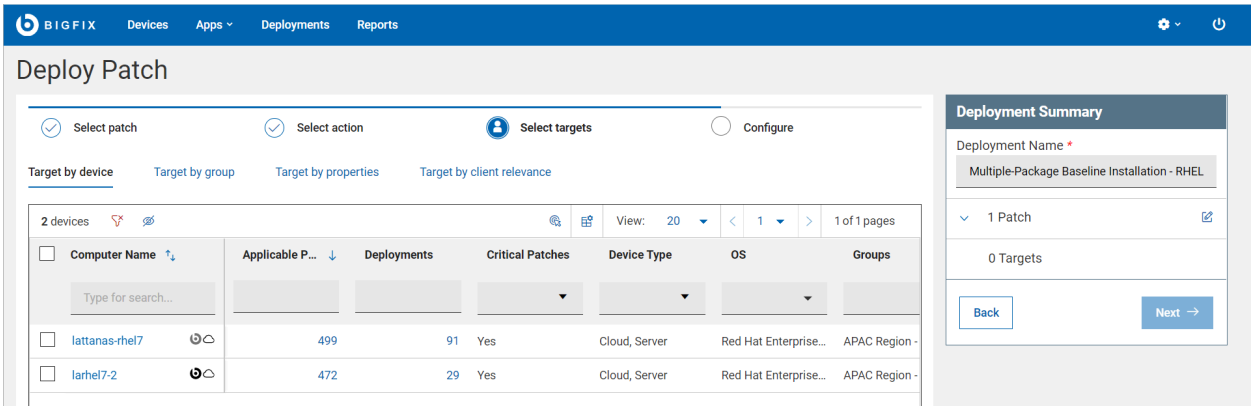
WebUI ワークフローおよびデプロイ・シーケンス

デプロイとは、アプリケーション、モジュール、更新、パッチなどのコンテンツを 1 つ以上のエンドポイントにディスパッチすることを意味します。例えば、ソフトウェア・パッケージをデプロイすることで、選択したソフトウェアをターゲット・エンドポイントにインストールします。BigFix WebUI を使用すると、コンテンツとターゲット・デバイスを構成してデプロイメントを作成し、デプロイメント構成を保存して必要に応じて再利用し、デプロイメント状況をモニターできます。デプロイメントの作成に必要なすべてのステッ

プ、プロセス、アクティビティーを含むワークフローは、まとめてデプロイ・シーケンスと呼ばれます。

デプロイメントは、デバイス・グリッドかコンテンツ画面、または「概要」ページから開始できます。エントリー・ポイントに従ってシーケンスの変更をデプロイします。

詳しくは、アクションの実行: デプロイ・シーケンス (（ページ） 184)を参照してください。



- 「デプロイ・シーケンス」のさまざまなタブを使用して進捗状況をトラッキングします
- デバイスやコンテンツを見つけるには、検索ツール、ソート・ツール、フィルタリング・ツールを使用します。
- 「デプロイメントの要約」セクションで、選択したコンテンツとデバイスを確認し、必要に応じて 「編集」ボタンをクリックして変更を加えます。

レポート

WebUI レポートを使用すると、エンドポイントのデバイス、パッチ、およびデプロイメントに関するより具体的な情報を取得するカスタム・レポートを作成できます。

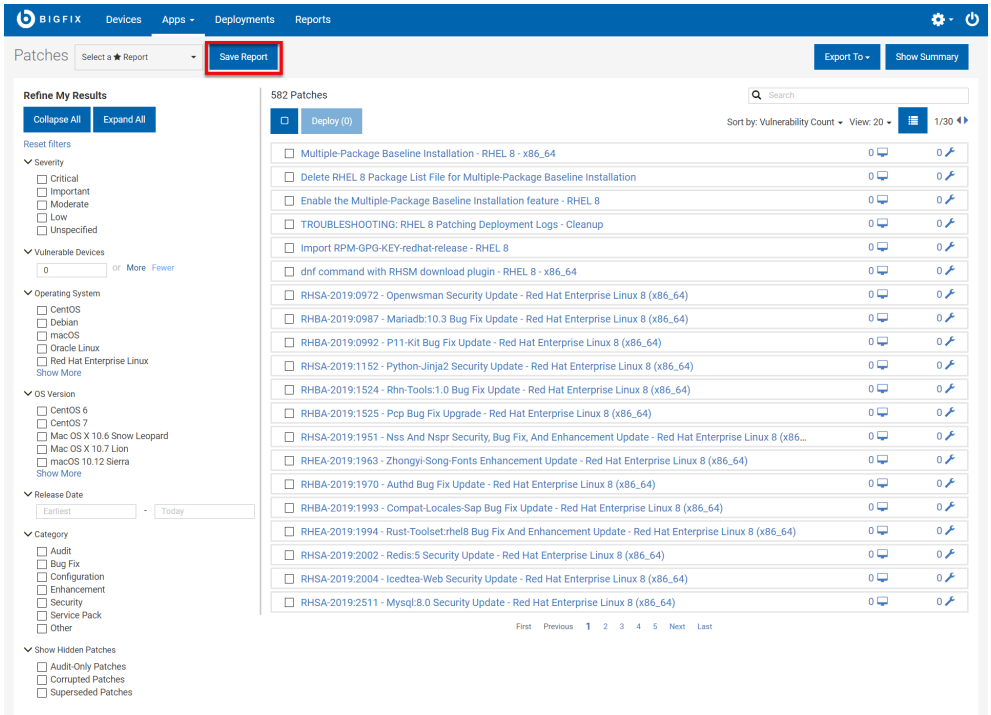
重要:

- マスター・オペレーターとマスター以外のオペレーターは、レポートを作成および保存できます。
- マスター・オペレーターは、他のユーザーが作成したプライベート・レポートを含むすべてのレポートを表示/編集/削除できます。
- マスター以外のオペレーターは次のことができます。
  - すべてのパブリック・レポートと自分のプライベート・レポートを表示する
  - 自分のレポートを編集/削除する

レポートの作成

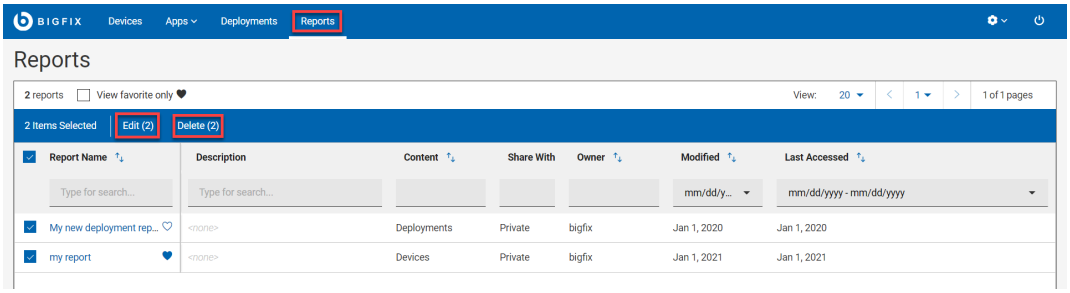
新しいレポートを作成するには

1. **「デバイス」**、**「デプロイメント」**、または**「パッチ」**ページを開きます。
2. 目的のフィルターを選択します。フィルター条件に一致する関連項目のリストが表示されます。



3. **「レポートの保存」**をクリックします。
4. 「レポートの保存」ウィンドウで、次の手順を実行します。
   a. **「レポート名」**を入力します。
   b. レポートの、**「レポートの説明」**を入力します (オプション)。
   c. レポートの表示設定を**「プライベート」**または**「すべてのユーザー」**に設定して、レポートを表示できるユーザーを制限します。
   d. レポートのリンクが自動生成されます。リンクをコピーし、ブラウザーから直接レポートにアクセスするには、**「リンクのコピー」**をクリックします。
5. **「保存」**をクリックします。

保存されたレポートの処理



- 表示: 保存されたパブリック・レポートとプライベート・レポートの一覧は、ユーザーの役割に応じて表示できます。表示するには、WebUI のメイン・ページから、**「レポート」**をクリックします。
- お気に入り: レポートをお気に入りのレポートとしてマークし、必要に応じて「デバイス」、「デプロイメント」、または「パッチ」ページからすばやくアクセスします。これを行うには、目的のレポートの横にある  をクリックします。
- お気に入りのみ表示: このチェックボックスを選択すると、お気に入りとしてマークされたレポートのみが表示されます。

- ソート: レポートは、「名前」、「コンテンツ」、「所有者」、「変更日時」、または「最終アクセス日時」で並べ替えることができます。
- フィルター: すべての列でレポートをフィルターできます。ストリングを入力するか、列からオプションを選択すると、それぞれのレポートがフィルターされて表示されます。
- 編集: レポート名、説明、可視性を編集できます。編集するには、目的のレポートを選択し、**「編集」** をクリックします。複数のレポートの表示を編集するには、目的のレポートを選択し、**「編集」**ボタンをクリックします。
- 削除: 1 つ以上のレポートを削除するには、削除するレポートを選択し、**「削除」**をクリックします。
- 削除の取り消し: 最後に削除したレポートを取得するには、レポートを削除した直後に表示される  をクリックします。

  注: このオプションは短時間だけ表示され、この時間にのみ取得できます。

- 更新:
  1. レポートをクリックして表示します。
  2. フィルター、並べ替えの基準を変更、またはプロパティーを表示します。「更新」ボタンが表示されます。
  3. **「更新」**をクリックします。レポートが更新され、保存されます。
- 新規保存:
  1. レポートをクリックして表示します。
  2. フィルター、ソート基準、またはビューのプロパティーを変更すると、「新規保存」ボタンが表示されます。
  3. **「新規保存」**をクリックします。「レポートの保存」ウィンドウが表示されます。

4. **「レポート名」**と**「レポートの説明」**を入力します。**「プライベート」**または**「すべてのユーザー」**として可視性を選択し、**「保存」**をクリックします。変更されたレポートは、新しいレポートとして保存されます。

第 3 章. デバイス入門

デバイス画面を使って、環境下にあるすべてのデバイスを権限レベルに応じて表示、管理します。特定のデバイスを探したり、デバイス文書にアクセスしたり、デプロイするデバイスを選択したり、デバイス・レポートを生成したりエクスポートしたり、他にもさまざまなことができます。

クラウド・デバイス

BigFix 11 によって、クラウド上 (パブリック、プライベート、ハイブリッド) の物理エンドポイントと仮想エンドポイントを、安全かつ費用対効果の高い方法で管理できるようになります。クラウド・プラグインを有効化している場合は、ネイティブの BigFix agent がインストールされているかに関係なく、クラウド・リソースを表示できます。

Modern Client Management (MCM) デバイス

BigFix では、使用環境下の最新のクライアントをより高いセキュリティーのもと、MCM ポリシーとアクションで制御できます。MCM プラグインを有効化している場合は、MCM のデバイスを登録し、BigFix WebUI から管理できます。詳細については、Modern Client Management と BigFix Mobile (（ページ） *247)*を参照してください。

デバイスの重複を避け、管理の効率化するため、BigFix はデバイスを検出すると、それが一意のものか判断し、デバイスのタイプ (ネイティブ、クラウド、MCM) を示すアイコンを追加します。デバイスに 2 つ以上の表記またはアイコンがある場合、そのデバイスは相関デバイスと呼ばれます。詳しくは、『相関デバイス (（ページ）　　) デバイス』を参照してください。

関連情報

デバイス・リスト (（ページ） *22)*

デバイス文書 (（ページ） *30)*

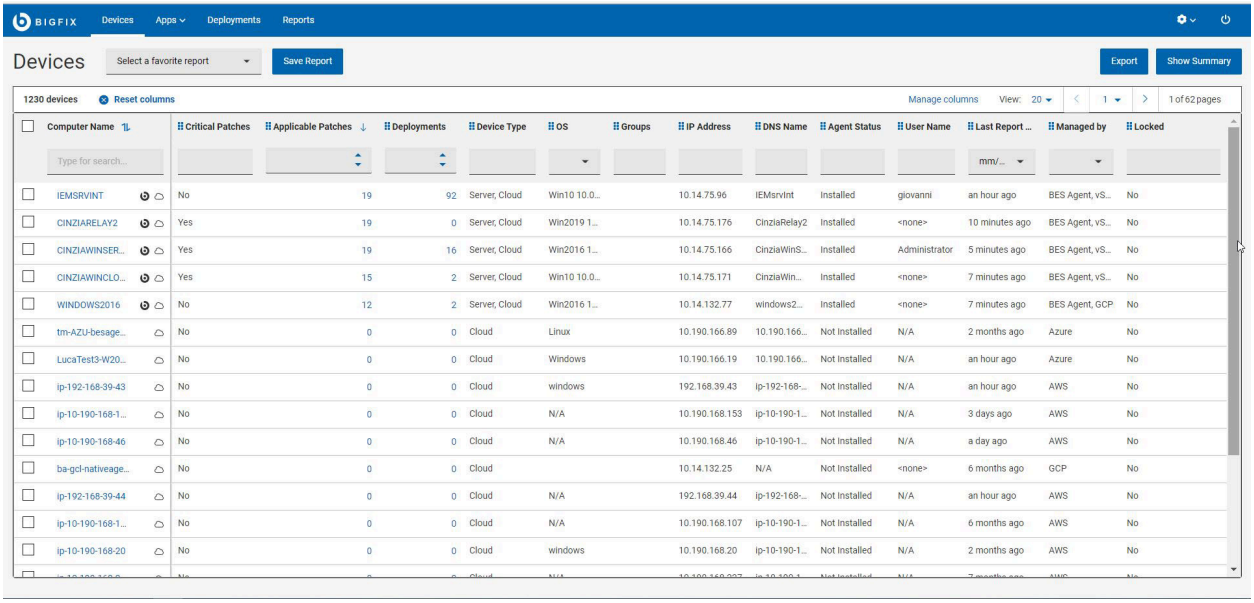
デバイス・リスト

BigFix マネージド・デバイスのリストを表示、カスタマイズされたデバイス・レポートを作成、各デバイスの詳細情報を確認してアクションを効率的に実行し、エンドポイントの正常性を積極的にモニターします。

「デバイス」ページにアクセスするには、WebUI メイン・ページで **「デバイス」**をクリックします。

重要: オペレーター権限設定、接続済みデバイス、サイト割り当てによって、リストのコンテンツが左右されます。

次の図は、デフォルトのプロパティー列とその位置 (コンピューター名、きわめて重要なパッチ、適用可能なパッチ、デプロイメント、デバイス・タイプ、OS、グループ、IP アドレス、DNS 名、エージェント・ステータス、ユーザー 名、前回のレポート時刻 、管理者、ロック状態) を持つデバイス・データ・グリッドを示しています。デフォルトでは、データはアプリケーション・パッチの数に基づいて降順にソートされます。



デバイスの管理

デバイスを管理するには、リストから 1 つ以上のデバイスを選択します。青いバーが表示され、使用可能なアクションがタイプ別に整理されています。アクションのリストは、システムにインストールされているコンポーネントによって異なる場合があります。例えば、MDM がインストールされていない場合、MDM に関連するアクションは「デプロイメント」ドロップダウンに表示されません。

- デプロイ (（ページ） *184)*: このメニューから、カスタム・コンテンツ、パッチ、ソフトウェア、MDM ポリシー、アクションなど、さまざまな種類のコンテンツをデプロイできます。

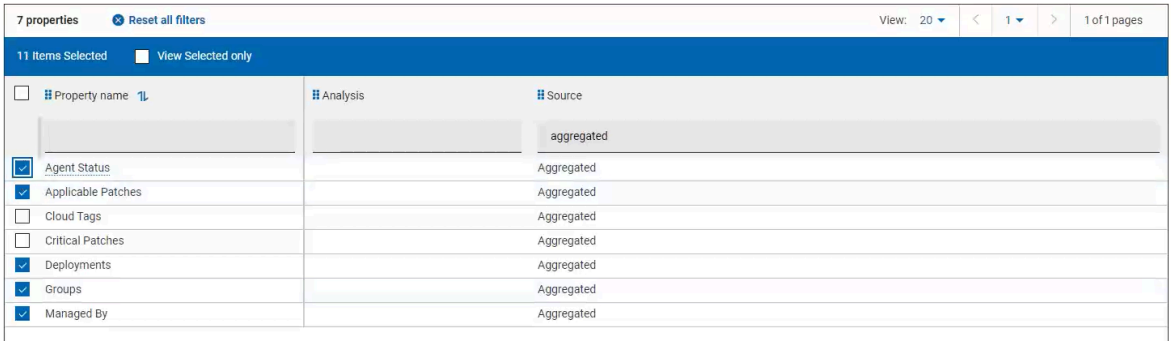
  注: プロファイルをデプロイするオプションは非推奨になります。

- 管理: このメニューから、MDM サーバーへの登録と MDM サーバーからの登録解除、BigFix agent のインストール、クライアント更新のアクションの送信など、デバイスに関連する一般的な管理タスクの中から選択できます。
- 構成: このメニューから、メッセージを送信したり (ターゲット・マシンに SSA がインストールされている場合)、ファイルを送信したり、照会アプリケーションにアクセスしたりできます。

コンピューターのプロパティー

これには、標準の BigFix クライアントの標準プロパティーと、BigFix コンソール・ユーザーが作成したプロパティーが含まれます。コンピューターのプロパティーは、次のように分類されます。

- 予約済み: BigFix プラットフォームで予約済みプロパティーと定義済みプロパティーとしてフラグが設定された一連のプロパティー。例えば、BIOS 日付、CPU タイプ、空きハード・ディスク・スペース、オペレーティング・システム、メモリー、ユーザー名など。
- 集約: WebUI が計算するプロパティーのセット。適用可能なパッチ、デプロイメント、きわめて重要なパッチ、グループ、エージェント・ステータス、クラウド・タグ、および管理者。



- BigFix agent によって取得された予約済みおよび集約プロパティー以外のすべてのコンピューターのプロパティー。

注: パフォーマンスを向上させるために、プロパティー値の最初の 5000 文字以降は切り捨てられます。

結果の絞り込み

- デバイス・データをフィルターするには:
  - 目的の列で、リストからオプションを選択します。

    または
  - 目的の列のテキスト・フィールドをクリックし、検索文字列を入力します。

    注: 予約済みおよび集約コンピューター・プロパティーのサブセットに対してのみ、自動補完により、最初にいくつか入力した文字に基づいて、候補の単語のリストが表示されます。ユーザー定義のコンピューター・プロパティーを含むその他のプロパティーでは、自動補完は検索のパフォーマンスに影響するため機能しません。
- 検索を高速化するには、フィルターを組み合わせます。

注: デフォルトでは、最大 5 つのフィルターを組み合わせて同時に処理できます。フィルターの最大数を超えると、パフォーマンスに影響します。デ

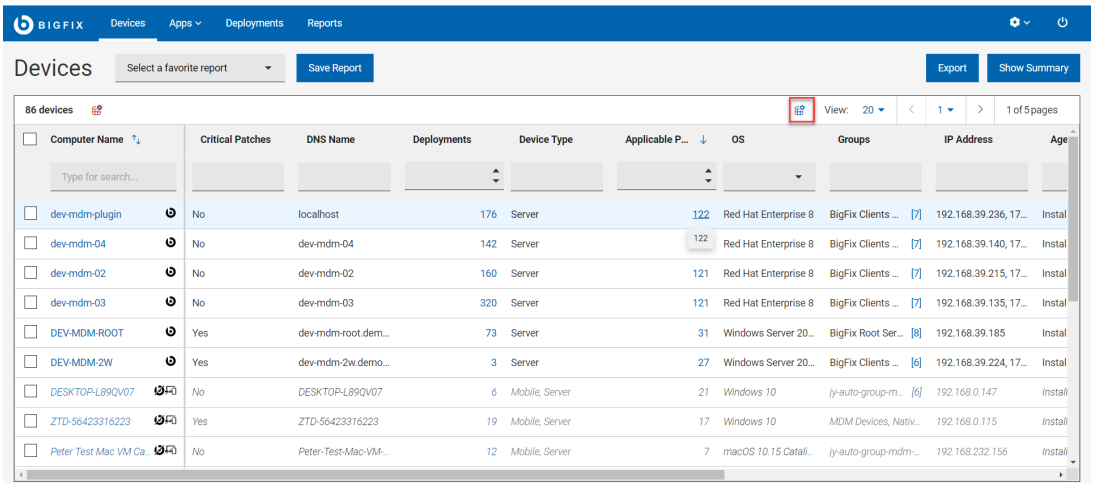
フォルト値は、`_WebUIAppEnv_MAX_FILTERS_NUMBER`（（ページ）　　）の設定を使用して構成できます。

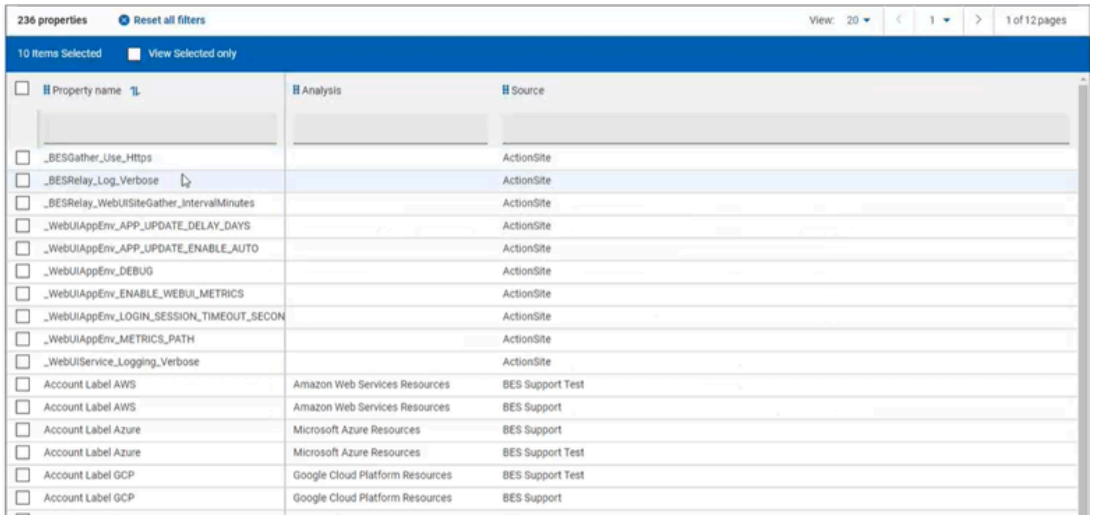
- すべての選択済みフィルターをクリアするには、「すべてのフィルターのリセット」をクリックします。

デバイス・データ・グリッドのカスタマイズ

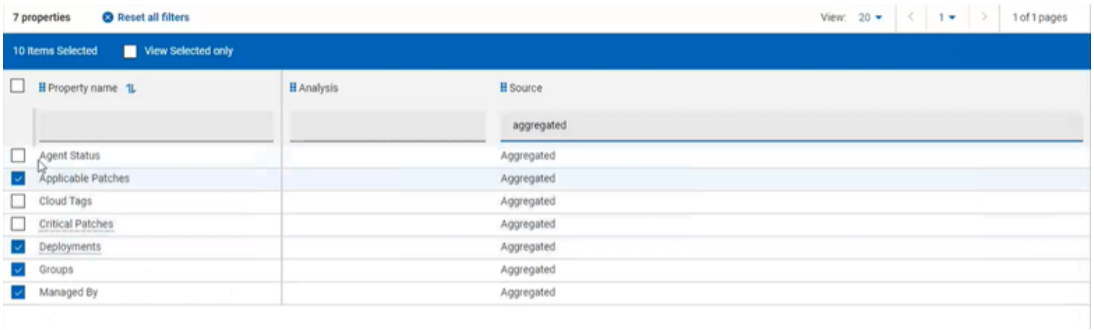
列の追加、削除、サイズ変更、または位置の変更によって、データ・グリッド・ビューをカスタマイズできます。「列のリセット」をクリックして、デフォルトのビューに戻ることもできます。

- **デバイス・データ・グリッドに追加のプロパティー列を含めるには**
  1. **「列の管理」**をクリックします。「その他のプロパティー」ページが表示されます。





2. 目的の列のテキスト・フィールドをクリックし、検索文字列を入力します。入力した文字列に基づいて検索結果が表示されます。例えば、「ソース」列で「集計」と入力すると、次の図のような結果が表示されます。



3. 目的の**「プロパティー名」**の横にあるチェック・ボックスをオンにし、**「保存」**をクリックします。「デバイス」ページには、選択したプロパティーが新しい列に表示されます。

• デバイス・データ・グリッドからプロパティー列を削除するには

1. **「列の管理」**をクリックします。
2. 「その他のプロパティー」ページで、**「選択済み項目のみを表示」**オプションを有効にします。結果には、データ・グリッド・ビューで選択されたプロパティーのみが表示されます。
3. データ・グリッドから削除する 1 つまたは複数のプロパティーの選択を解除し、**「保存」**をクリックします。「デバイス」ページに選択したプロパティーが表示されます。選択解除されたプロパティー列は消えます。

• 列幅のサイズを変更するには

1. 目的の列の境界線の近くにマウス・カーソルを移動します。
2. マウスの左ボタンをクリックしたまま、右に境界線をドラッグして列を広げるか左にドラッグして列を狭くし、目的の幅に達したらマウス・ボタンを離します。

• 列の位置を変更するには

1. 目的の列名にマウス・カーソルを移動します。
2. マウスの左ボタンをクリックしたまま、ドラッグしてデータ・グリッド内の任意の位置にドロップします。

レポートの処理

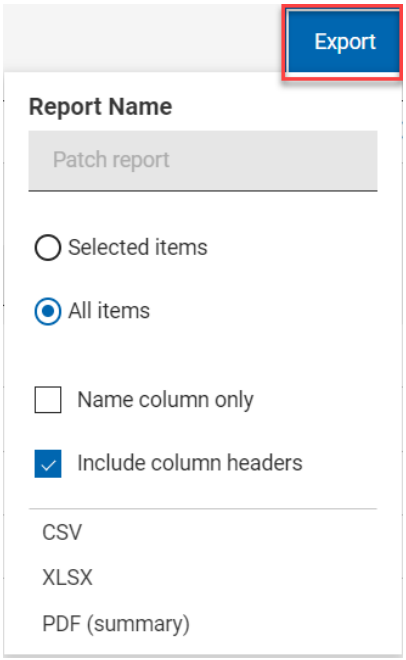
レポートの保存

後で参照できるように、フィルター処理およびカスタマイズされたデバイス・レポートを保存できます。必要に応じて、レポートを編集、更新、または削除することもできます。レポートにすばやくアクセスするには、お気に入りのレポートとしてマークします。レポートの操作の詳細については、「レポート (（ページ） 16)」を参照してください。

エクスポート

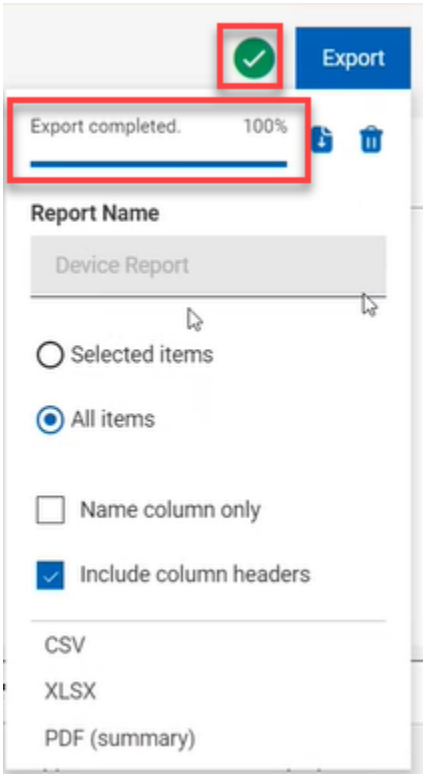
フィルターされたレポートは `.csv`、`.xlsx`、または `.pdf` の形式でエクスポートできます。

1. **「デバイス」**ページで、必要なフィルターを選択します。
2. **「エクスポート」**をクリックします。

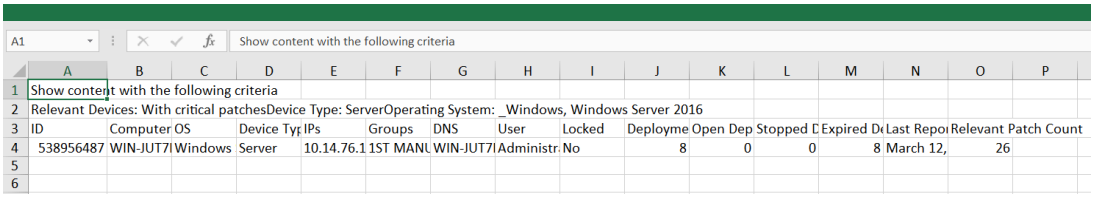


3. **「選択された項目」**オプションを使用すると、フィルターされた結果から項目を選択してエクスポートできます。**「すべての項目」**を使用すると、フィルター処理されたリストからすべての項目をエクスポートできます。最適なオプションを選択してください。

4. 名前列のみ: フィルターされた項目の名前のみをエクスポートする場合は、このオプションを選択します。
5. 列ヘッダーを含める: 項目のすべての列の詳細をエクスポートする場合は、このオプションを選択します。
6. エクスポート先のファイル形式 (CSV、XLSX、PDF) を選択します。
    - ファイルのエクスポートが開始し、状態が進行状況表示バーに表示されます。
    - エクスポートが完了すると、レポートがダウンロード可能であることを示す緑色のチェック・マークが表示されます。
    - エクスポートされたレポートは自動的にはダウンロードされません。ダウンロードするには、進行状況表示バーの横にある 「ダウンロード」ボタンをクリックする必要があります。
    - エクスポートしたレポートを削除する場合は、 「削除」ボタンをクリックします。
    - エクスポート中に、進行を中断することなく、他のページにナビゲートできます。



- ダウンロードすると、デフォルトでは、レポートは「ダウンロード」フォルダーにダウンロードされ、デフォルトのファイル名 (Device_Report_mm_dd_yyyy_username) が付けられます。ブラウザー内でダウンロード設定を変更すると、ファイル名やダウンロードの保存先を変更できます。レポートを保存して後で参照したり、利害関係者と共有したりできます。
- PDF 形式を選択した場合、数値データを含む `.csv` ファイルとデータの表示形式を含む `.pdf` ファイルを含む `.zip` ファイルがダウンロードされます。
- エクスポートされたデバイス・レポートには、フィルターや検索条件を介して選択した管理対象デバイスに関する主な情報が含まれます。これらの情報には、オペレーティング・システム、デバイス・タイプ、IP アドレス、さらにすべてのデバイスを展開したときに画面に表示される他のすべての詳細情報が含まれます。以下はサンプル・レポートです。



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1	Show content with the following criteria															
2	Relevant Devices: With critical patches	Device Type: Server	Operating System: _Windows, Windows Server 2016													
3	ID	Computer	OS	Device Ty	IPs	Groups	DNS	User	Locked	Deployme	Open Dep	Stopped D	Expired D	Last Repo	Relevant Patch Count	
4	538956487	WIN-JUT7I	Windows	Server	10.14.76.1	1ST MANU	WIN-JUT7I	Administr	No	8	0	0	8	March 12,	26	
5																
6																

要約の表示

1. **「デバイス」**ページで、必要なフィルターを選択します。
2. **「要約を表示」** をクリックします。フィルターされたすべてのデバイスの要約をグラフやテーブルとして表示できます。グラフ上の調べたいエリアにカーソルを合わせると、そのデータ・ポイントとパーセンテージ・データの詳細が表示されます。文字が切り詰められたラベルにカーソルを合わせると、ツール・ヒントにすべてのテキストが表示されます。クリック可能領域をクリックすると、関連するデータが動的にフィルタリングされ、デバイス・リストに表示され、クリックした項目の要約が表示されます。フィルターを変更するか、検索テキストを入力すると、該当する情報がレポートに動的に表示されます。

- **レポート時間ごとのデバイス・タイプ**: すべてのデバイス・タイプに対して一定期間にレポートされた固有デバイスの総数を表示します。
- **OS ファミリーごと**: 各オペレーティング・システムのデバイスの総数を表示します。テーブルは OS 名のアルファベット順にソートされています。
- **最大グループごと**: フィルターと検索条件に該当する最大 10 のコンピューター・グループをデバイス数とともに表示します。

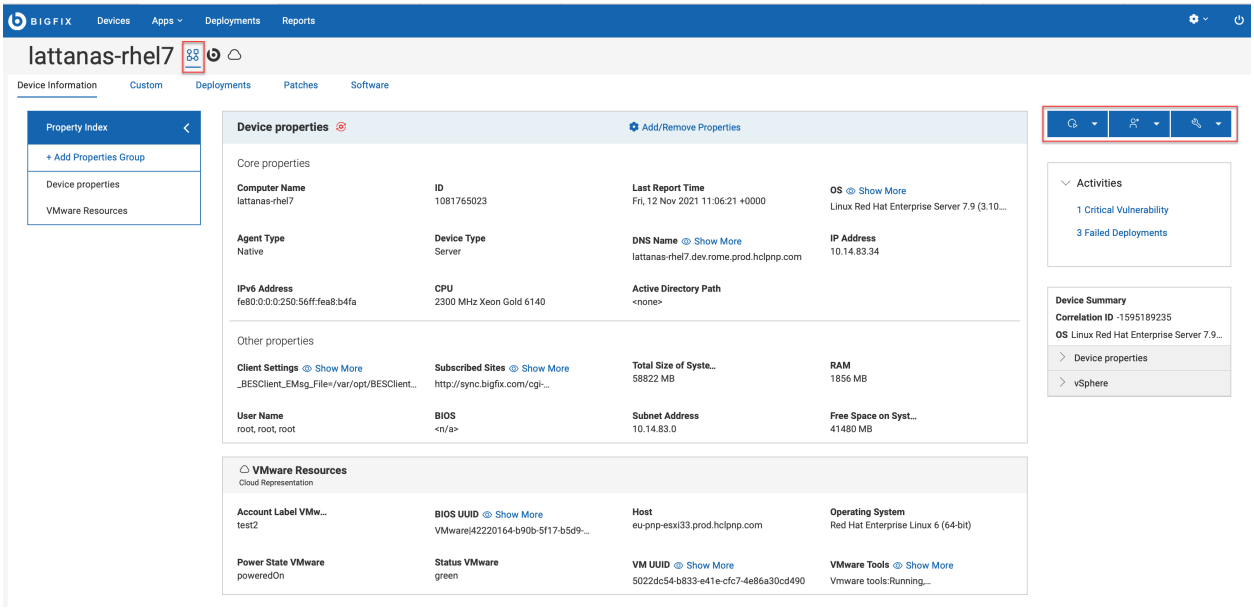
デバイス文書

デバイス名をクリックすると、デバイスのプロパティー、状況、関連コンテンツ、デプロイメント状況、履歴など、そのデバイスに関連する情報が表示されます。関連付けられたビューを使用することで、デバイスの詳細を掘り下げます。

BigFix オペレーターは、デバイス文書を表示できます。デバイス文書には、さまざまなソースから収集された情報が記載されています。

注: パフォーマンスを向上させるために、プロパティー値の最初の 5000 文字以降は切り捨てられます。

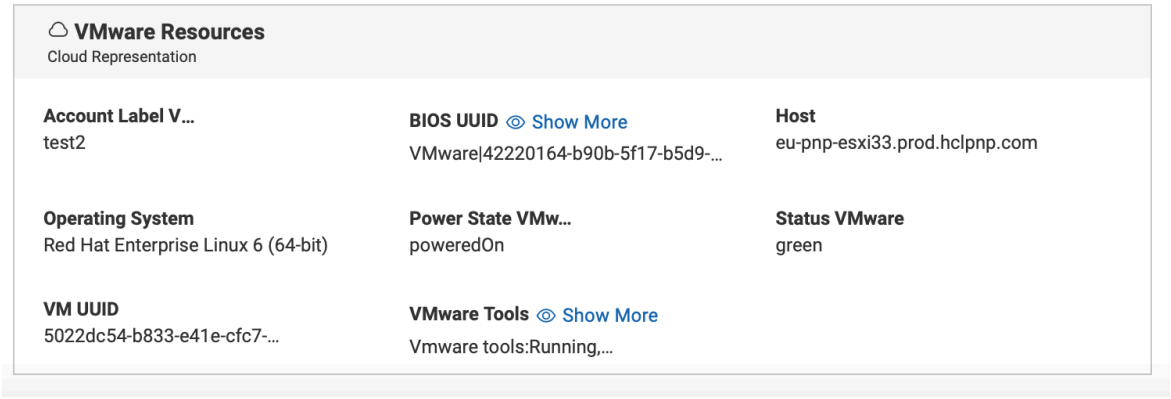
以下の画像は、 「相関」（（ページ） *21)*デバイスのデバイス文書ページを示しています。



アイコンと表現

デバイス名の横にあるアイコンは、デバイスに関連するさまざまな表現を示しています。特定の表現の特定のプロパティーを表示するには、デバイス名の横にあるアイコンをクリックします。

- 相関デバイス: のアイコンは、デバイスが相関していることを表しています。相関デバイスの場合、以下のことが可能です。
  - デバイスの一般的なプロパティを表示する。
  - BigFix、Cloud、MDMなど、さまざまな表現の詳細をドリルダウンする。
- MDM デバイスとクラウド・デバイス: これらのデバイスでは、表現に関連付けられたプロパティーのデフォルト設定とともに、追加のセクションが自動的に表示されます。これらのデフォルトのセクションには関連するデバイス情報が含まれるため、削除できません。



文書ビュー

デバイス文書ページのタブには、以下のようなさまざまなビューが表示されます。

- **デバイス情報** - デバイスの一般的な情報が表示されます。
- **カスタム** - このデバイスに関連するカスタム・コンテンツが表示されます。
- **デプロイメント** - このデバイスのデプロイメント履歴。
- **パッチ** - このデバイスに関連するパッチ。

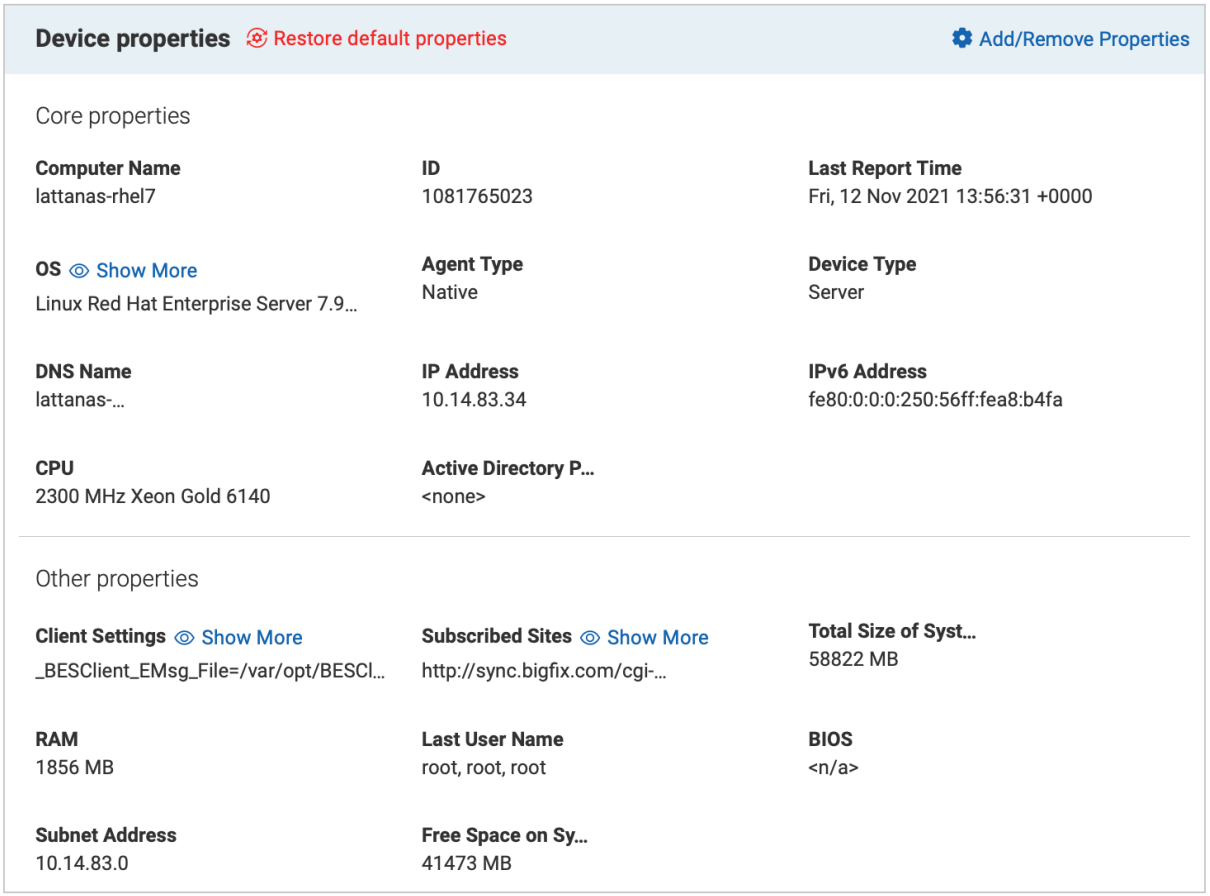
注: このタブには、「パッチ・リスト」 (（ページ） *45*)で管理されているサイトからのパッチのみが表示されます。その他のパッチは、「コンテンツ」メニューからアクセスできます。

- **ソフトウェア** - このデバイスに関連するソフトウェア。

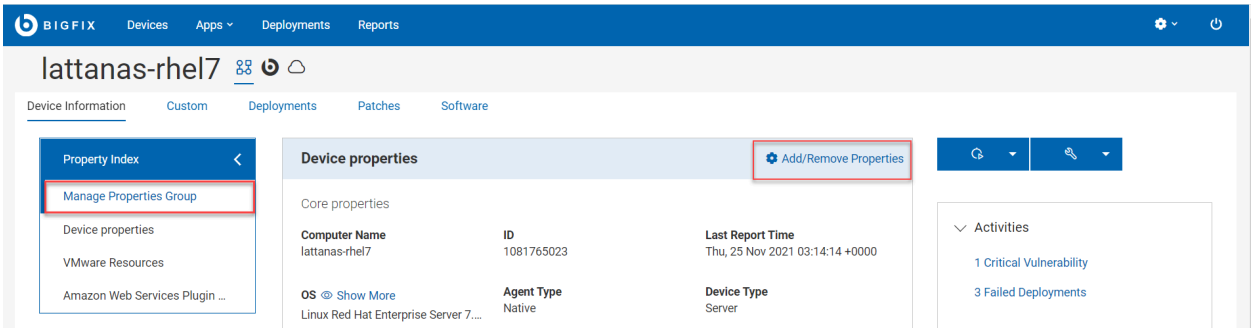
重要: オペレーターの権限設定によって表示されるビューが左右されます。例えば、カスタム・コンテンツへのアクセス権限を持たないオペレーターは、**「カスタム」**ビューを表示できません。

デバイス文書ページのレイアウトのカスタマイズ

デフォルトのビューでは、「プロパティー・インデックス」の下にプロパティー・グループが表示され、「デバイス・プロパティー」ボックスの中に一連のプロパティーが表示されます。



デバイス文書の相関ビューでは、**「プロパティー・グループの管理」**または**「プロパティーの追加/削除」**を使用して、プロパティー・インデックスとデバイスのプロパティーの表示をカスタマイズできます。

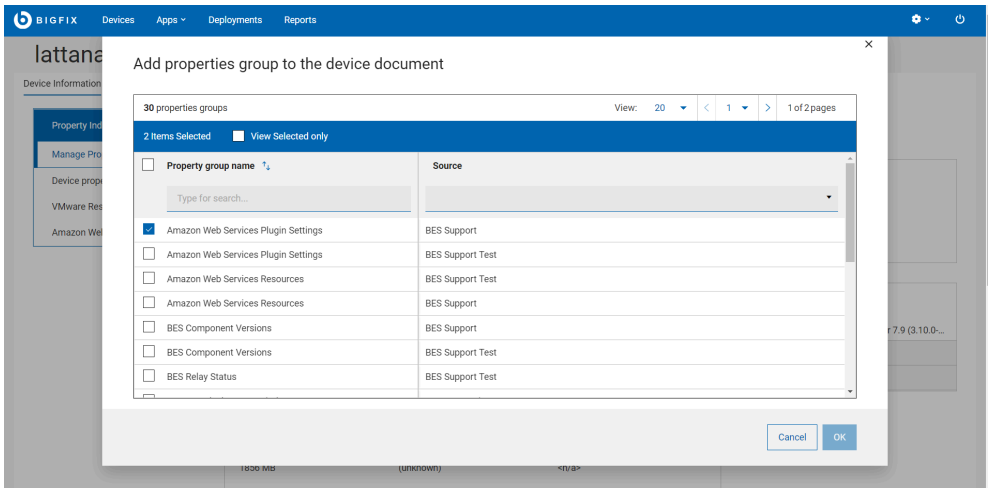


変更は、関連付けのタイプに関係なく、すべてのデバイスに適用されます。

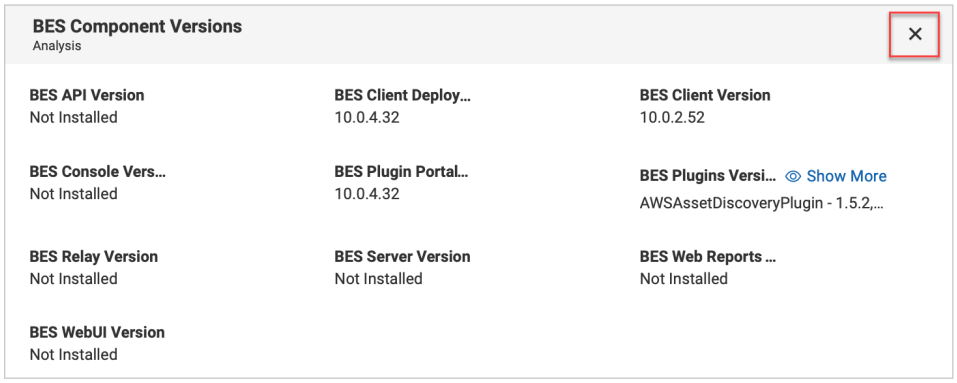
プロパティー・グループの管理

このリンクをクリックすると、「プロパティー・インデックス」の下に表示されるデフォルトのプロパティー・グループを変更できます。プロパティー・グループはいくつでも追加できます。追加されたプロパティー・グループは、「**プロパティー・インデックス**」ボックスに追加されます。「プロパティー・インデックス」を展開または縮小して、サイド・ナビゲーションを表示できます。プロパティー・グループをクリックすると、そのプロパティー・グループに自動的にスクロールして詳細を確認できます。

- プロパティー・グループの追加: プロパティー・グループを追加するには、**「プロパティー・グループの管理」**リンクをクリックし、プロパティー・グループの横にあるチェック・ボックスを選択して、「OK」をクリックします。

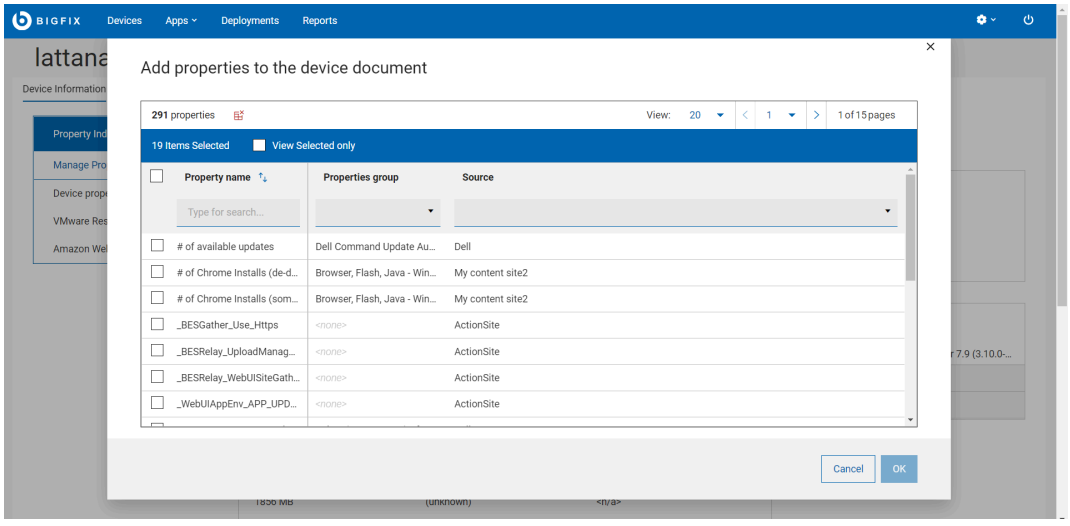


- プロパティー・グループの削除: プロパティー・グループを削除するには、そのボックスの右上にある「X」をクリックし、「OK」をクリックして確定します。



プロパティーの追加/削除

このリンクをクリックして使用可能なプロパティーのリストを表示し、デバイスのプロパティー・ビューに追加/削除させるものを選択または選択解除します。ここから、カスタム・プロパティーを追加または削除することもできます。デフォルト表示に戻るには、**「デフォルト・プロパティーを復元」**をクリックします。確定すると、デフォルトのビューがリセットされます。



アクションのトリガー

デバイス文書ページから、デバイスに関連するアクションをトリガーできます。「アクション」ボタンをクリックすると、デバイスのタイプとユーザーの権限に基づいてオプションが表示されます。例えば、MDM をサブスクライブしていないクラウド・デバイスの場合、ドロップダウンに「MDM アクションのデプロイ」は表示されません。

- デプロイ:  ボタンをクリックして、カスタム・コンテンツ、パッチ、プロファイル、ソフトウェア、または MDM アクションをデプロイします。
- 管理:  ボタンをクリックして、エージェントの更新またはインストールを送信します。
- 構成:  ボタンをクリックして、照会の発行、ファイルの送信、このデバイスへのメッセージ送信を行います。

重要: デバイス文書ページの相関ビューからアクションをトリガーすると、相関デバイスが対象となり、相関エンジンによってアクションは適切な表現にディスパッチされます。

アクティビティー

デバイス文書ページの「アクティビティー」セクションには、デバイスに該当する重大な脆弱性と失敗したデプロイメントのリンクが表示されます。リンクをクリックすると、関連するパッチまたはデプロイメントの事前フィルター済みリストが表示されます。

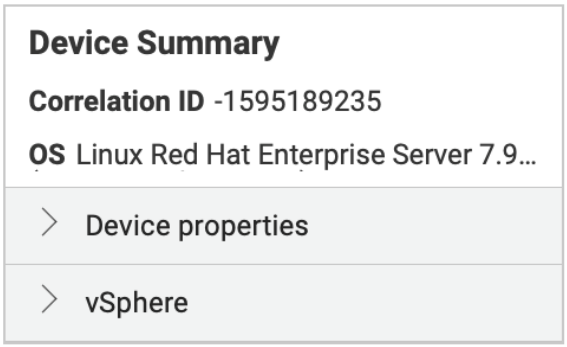
- **重大な脆弱性** - 重大でこのデバイスに適用可能な事前フィルター済みの「パッチ」タブに移動します。
- **失敗したデプロイメント** - デプロイメント状況によって事前フィルター済みの「デプロイメント」タブが表示されます。

デバイスの要約

デバイス文書の 「デバイスの要約」セクションには、デバイスに関係する最も関連性の高いプロパティの要約が表示されます。

相関デバイス

デバイスが相関している場合は、以下の情報が表示されます

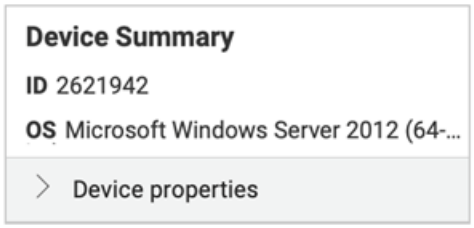


- 相関 ID
- OS
- 展開または縮小表示ができる「デバイス・プロパティー」セクションでは、以下の詳細を確認できます。
    - 要約に残しておくと便利なプロパティーの固定設定
- クラウドまたは MDM セクション (特定のソース、AWS、MDM などに関連する名前が付けられている)
    - 特定の表現によって報告された値が入力された、マスター表現と同じプロパティーの固定リスト

例えば、ロック・プロパティーは、マスター表現では「はい」、セカンダリー表現では「いいえ」という値を表示します。

非相関デバイス

デバイスが相関していない場合は、 「デバイスの要約」セクションに、デバイスの ID、OS、デバイスのプロパティーが表示されます。



ファイルの送信

ファイル・システムから、ファイルのアップロード、リスト化、削除、複数のデバイスへの送信を実行できます。

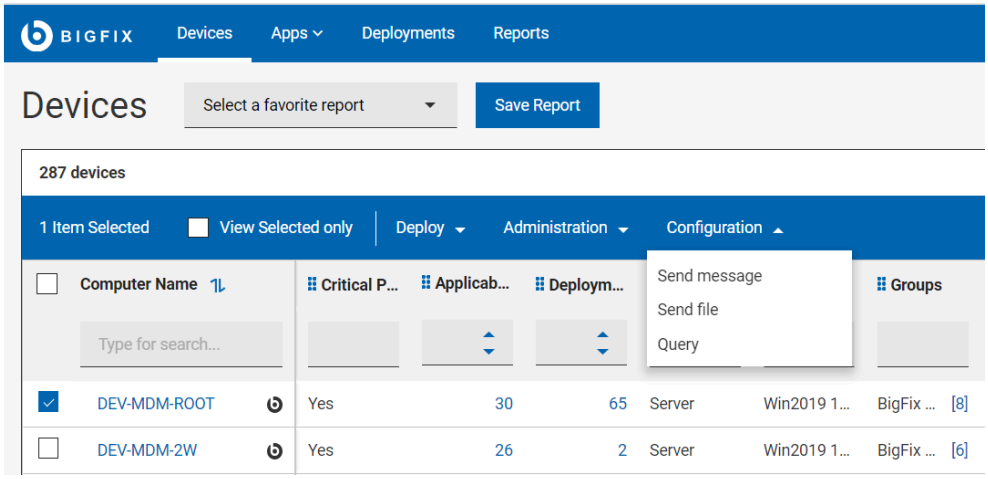
- オペレーターには以下の権限が必要です。
  - アクションの作成が可能
  - カスタム・コンテンツ
- SWD を実行する必要があり、オペレーターには SWD へのアクセス権が必要です。

このセクションでは、ファイルのアップロード、対象デバイスへのファイル送信、リストからのファイルの削除を行う方法を説明します。

ファイルのアップロード

新しいファイルをサーバーにアップロードするには:

1. **「デバイス」**ページで、1 つ以上のデバイスを選択します。**「構成」**をクリックして**「ファイルの送信」**を選択します。



「ファイル」ページには、すでにユーザーがアップロードしたファイルのリストが表示されます。

2. **「アップロード」**をクリックし、アップロードするファイルを選択して**「開く」**をクリックします。
   - ファイルのアップロードが開始し、アップロードの状態が進行状況バーに表示されます。
   - アップロードをキャンセルする場合は、進行状況バーの横にある赤色の x アイコンをクリックします。

ファイルがアップロードされると、ファイルのリストが更新され、アップロードされたファイルを対象デバイスに送信できるようになります。

注: Microsoft Edge ブラウザーを使用してファイルをアップロードする場合は、MS Edge バージョン 18.18218 以降を使用するようにしてください。以前のバージョンの Microsoft Edge では、進行状況バーにファイルのアップロード状態が表示されませんが、ファイル・リストはアップロードされたファイルで更新されます。

ファイルがアップロードされたら、デフォルト・パスに保存されます。デフォルト・パスを変更するには:

a. デフォルト・パスを変更するファイルの **DEFAULT_PATH** のリンクをクリックします。
b. **「宛先ファイル・パス」**ウィンドウで以下の操作を行います。

i. 任意のパスを入力します。
ii. 必要に応じて、**「ファイルが対象に既に存在する場合は上書きします」**のオプションを選択します。

c. **「OK」**をクリックします。

指定したパスが宛先パスとして設定されます。

ファイルの送信

ファイルを選択して、1 つ以上の選択デバイスに送信できます。

前提条件: ファイルの送信に必要な権限は、アクションの作成とカスタムの作成です。

ファイルを 1 つ以上のデバイスに送信するには:

1. **「デバイス」**（*（ページ） 22)* ページで、デバイスのリストからファイルを送信する宛先デバイスを 1 つ以上選択します。

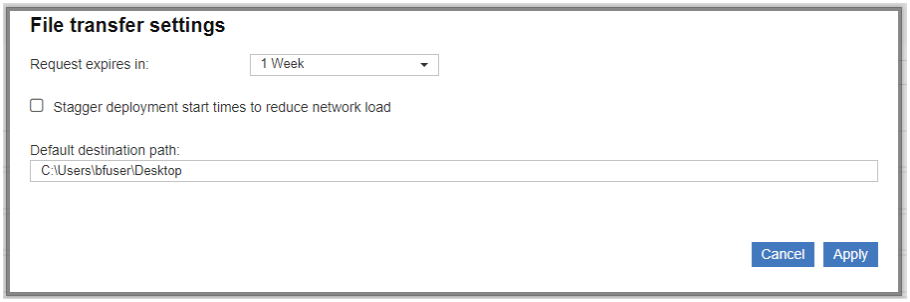
重要:
- 少なくとも 1 つの宛先デバイスを選択します。
- 複数のデバイスを選択する場合は、同じオペレーティング・システムを選択します。

2. **「その他」**をクリックして**「ファイルの送信」**をクリックします。
3. ファイルのリストから、転送するファイルを選択します。

重要: 一度に送信できるファイルは 1 つのみです。

注: ファイルは、アップロード日、ファイル名、ファイル・サイズで検索、ソートできます。

a. **「対象デバイス」** - 選択したデバイスの合計数が表示されます。デバイスの選択を変更するには、このボタンをクリックします。
b. **設定** – ファイル転送の設定を定義するには、このボタンをクリックします。



- **要求の期間** - ファイルを宛先デバイスに転送できる期間をドロップダウン・リストから選択します。この期間を過ぎると、ファイルの転送リクエストの期限が切れ、ファイルを転送できなくなります。
- **間隔を置いてデプロイメントを開始 (ネットワーク負荷を軽減するため)**– ネットワーク負荷を削減する場合はこのオプションを選択します。
- **デフォルト宛先パス** - 選択したすべてのデバイスでファイルを送信するデフォルトの宛先パスを指定します。

4. **「送信」**をクリックします。

転送が成功すると、ファイルは宛先デバイスのデフォルト・パス・セットで利用可能になります。

Delete (削除)

サーバーからファイルを削除するには、ファイルのリストから 1 つ以上のファイルを選択して **「削除」** をクリックします。

注: ファイルが削除されるとき、ファイルのリファレンスのみが削除されます。

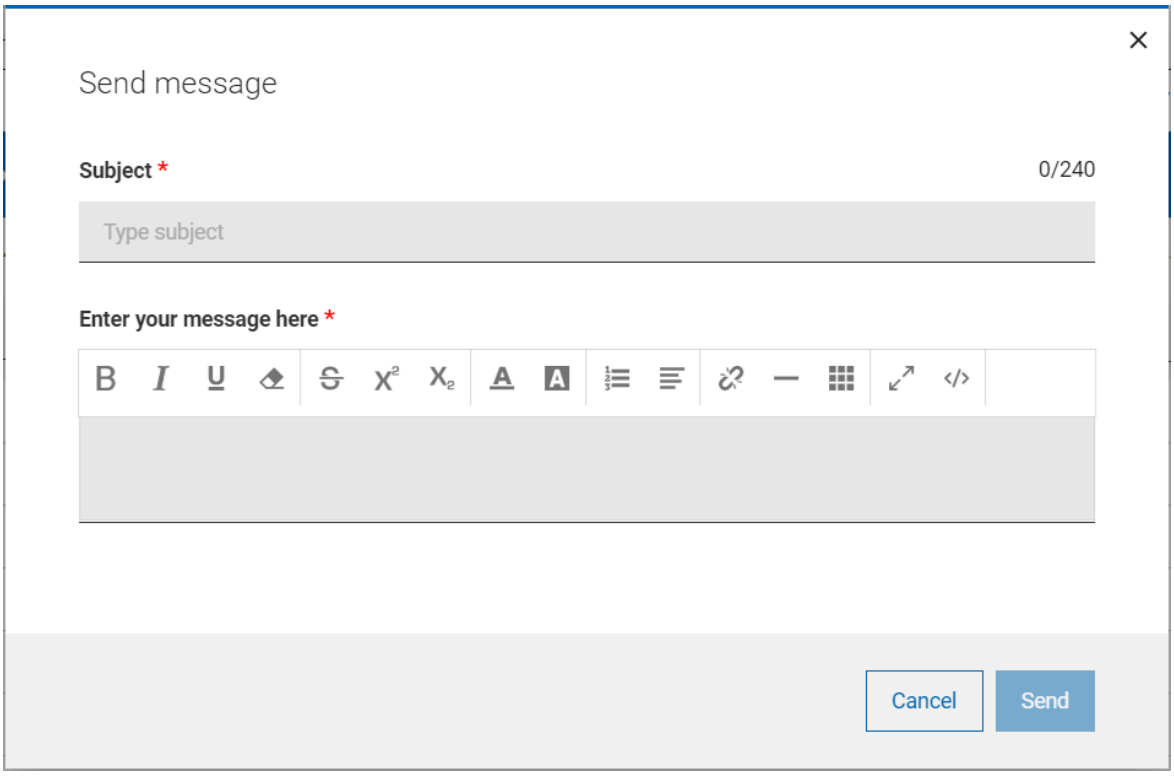
デバイスへのメッセージの送信

「メッセージの送信」機能を使用すると、複数の選択デバイスにショート・メッセージの通知を送信できます。ユーザーがメッセージを読んだかどうかを確認でき、指定日数が経過すると対象デバイスから自動的にメッセージを削除するよう設定することもできます。

- オペレーターには以下の権限が必要です。
  - アクションの作成が可能
  - カスタム・コンテンツ
- SWD を実行する必要があり、オペレーターには SWD へのアクセス権が必要です。
- 対象デバイスには SSA 3.1.0 以降がインストールされていることと、「メッセージ」タブ設定が有効になっている必要があります。

メッセージ通知を選択した対象デバイスに送信するには、以下の手順を実行します。

1. **「デバイス」** タブを開きます。
2. **「デバイス」** ページで、デバイスのリストからメッセージを送信するデバイスを 1 つ以上選択します。
3. **「構成」** をクリックして、ドロップダウン・メニューから **「メッセージの送信」** を選択します。
4. **「メッセージの送信」** ウィンドウで、件名とメッセージを該当セクションに入力します。



注:

- 件名には最大 240 文字を入力できます。
- コンテンツは、ツールバーの書式設定オプションを使用して書式設定できます。
- HTML コードをエディターにコピーして貼り付けたり、メッセージを HTML コードとして保存したりできます。

5. **「送信」**をクリックします。
   - メッセージを送信すると成功メッセージが表示され、送信したメッセージに関連するアクションが作成されます。対象デバイスに SSA 3.1.0 以降がインストールされていない場合、メッセージは配信されず、このアクションのステータスは関連なしになります。
   - ユーザーがメッセージを読むと、アクションのステータスが完了になります。これにより、オペレーターはメッセージがエンド・ユーザーによって読まれたかどうかを確認できます。

- 指定した日数の経過後、対象デバイスのユーザーの「SSA メッセージ」タブからメッセージを自動的に削除するには、メッセージの有効期限を Web UI サーバーを介して _WebUIAppEnv_NOTIFICATION_EXPIRATION_DAYS を設定します。

第 4 章. パッチ入門

「パッチ」画面を使用して、パッチのリスト、特定のパッチの検索、およびパッチの詳細情報 (既知の問題、脆弱なデバイス、およびデプロイメントなど) の表示を行います。

パッチ・リスト

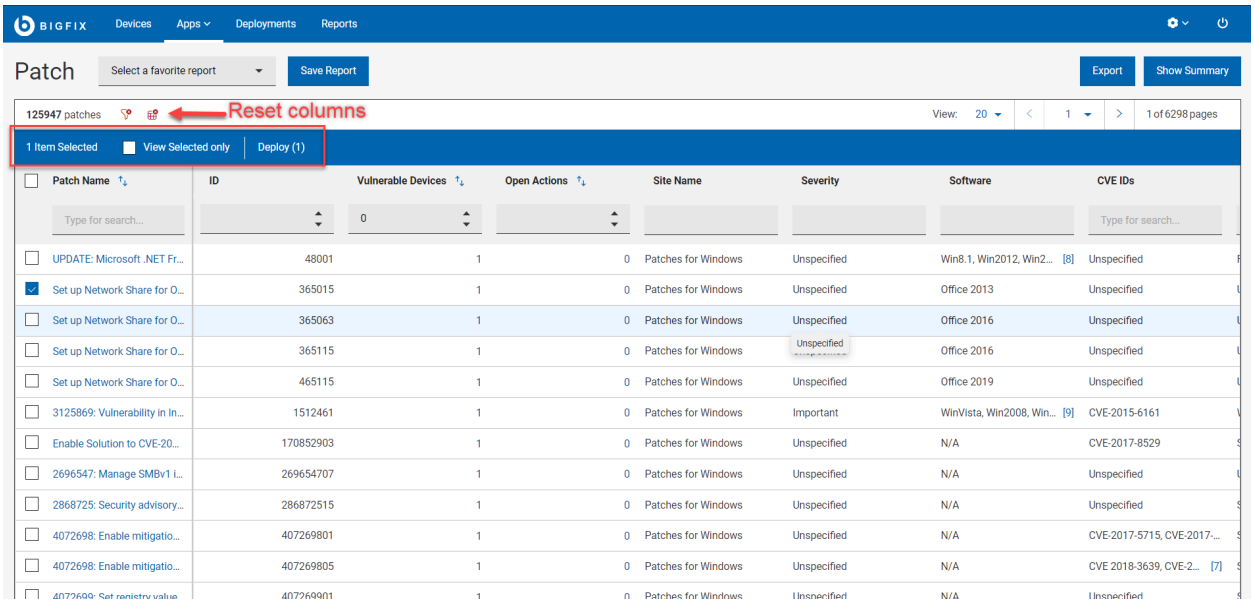
すべてのパッチのリストを表示し、カスタマイズされたパッチ・レポートを作成すると、パッチング・インテリジェンスの入手、パッチに関する迅速な決断、パッチ・コンプライアンスのレポート、リスクの伝達が可能になります。レポート内のリンクを使用して、不足しているパッチをダウンロード、インストールすることもできます。

「パッチ」ページにアクセスするには、BigFix WebUI メイン・ページで **「アプリ」 > 「パッチ」**をクリックします。

オペレーター権限設定、接続済みデバイス、サイト割り当てによって、コンテンツのリストが影響を受けます。

グリッド・ビューを使用すると、テーブル内のパッチのリストを素早く表示できます。パッチ名をクリックすると、パッチの詳細 (概要、脆弱なデバイス、デプロイメント) に移動します。**「パッチ」**ページのすべての列には、検索またはフィルタリングのオプションが用意されています。列の追加、削除、およびサイズ変更を行うことができます。**「列のリセット」**をクリックして、デフォルトのビューに戻ることもできます。

結果の絞り込みとデータ・グリッド機能のカスタマイズは、デバイス・ページと似ています。詳しくは、「グリッド表示 (（ページ） 6)」を参照してください。



- **アクション・バー:** データ・グリッドから 1 つ以上のパッチを選択すると、アクション・バーが有効になります。
  - **選択済み項目のみを表示:** 選択したパッチのみを表示するには、このボックスにチェック・マークを付けます。
  - **デプロイ: 「デプロイ」** をクリックして「アクションの実行」ダイアログに移動します。このダイアログで、パッチをデプロイできます。括弧内の数値は、選択されたパッチの数を示します。
- ヘッダー内のフィルターを使用して、結果を絞り込むことができます。
  - 「脆弱なデバイス」フィールドに値を入力して、任意の数のデバイスで必要とされるパッチを表示します。
  - 未処理アクションのフィールドに値を入力して、未処理アクションを含むパッチを表示します。
  - このフィルターを使用して、ID によってパッチを識別します。
  - サイト名 - WebUI には、次のサイトからのパッチのみが表示されます。
    - Windows 2008 I 用 ESU パッチ適用アドオン
    - Windows 7 用 ESU パッチ適用アドオン
    - Amazon Linux 2 向けパッチ
    - CentOS 6 向けパッチ
    - CentOS 6 プラグイン R2 向けパッチ
    - CentOS 7 向けパッチ

- CentOS 7 プラグイン R2 向けパッチ
- CentOS 8 向けパッチ
- Debian 7 向けパッチ
- Mac OS X 用パッチ
- Patches for Oracle Linux 6
- Patches for Oracle Linux 7
- Patches for Oracle Linux 8
- RHEL5 拡張サポート用のパッチ
- RHEL 7 向けパッチ
- RHEL 8 向けパッチ
- RHEL8 拡張サポート用のパッチ
- SLE 11 ネイティブ・ツール向けパッチ
- SLE 12 ネイティブ・ツール向けパッチ
- SLE 12 on System Z 向けパッチ
- SLE 12 PPC64LE 向けパッチ
- SLE15 向けパッチ
- SLE 15 on System Z 向けパッチ
- Ubuntu 1404 向けパッチ
- Ubuntu 1604 向けパッチ
- Ubuntu 1804 向けパッチ
- Ubuntu 2004 向けパッチ
- Windows 用パッチ
- Windows アプリケーションの更新
- Mac アプリケーションの更新

◦「重要度」フィルターを使用して、最も深刻な脅威用のパッチまたは特定の脅威レベル用のパッチを表示します。パッチの重要度は、BigFix ではなく、パッチのベンダー (Microsoft など) によって割り当てられます。

- 重大
- 重要
- 中
- 低
- 不明 - パッチにベンダー指定のレーティングがありません。

- ソフトウェア・フィルターを使用して、特定のソフトウェアで使用可能なパッチを表示します。
  - CentOS
  - Debian
  - OracleLinux
  - Red Hat Enterprise Linux
  - SUSE
  - Ubuntu
  - 未指定
  - Windows (NET Core ランタイム、CoreAdobe Acrobat、Adobe Flash Player、Adobe Reader、Adobe Shockwave、Google Chrome、GoToMeeting、ImgBurn、Microsoft Edge、Mozilla Firefox、Notepad++、Nullsoft、Oracle、Real Networks、Skype、Webex Meetings、Winamp、Winzip、Zoom)
  - Mac OS
- CVE IDフィルターを使用して、共通脆弱性と暴露でパッチを検索します。
- 「カテゴリー」フィルターを使用して、特定のタスクに関連付けられたパッチを表示します。
  - 監査 – 修正不能で、管理者の確認を要する条件を検出するために使用される BigFix パッチのタイプです。
  - バグ修正 – 1 つ以上のバグを修正する変更を適用します。
  - 構成 – 構成の問題を解決する変更を適用します。
  - 機能拡張 – 新機能を提供する変更を適用します。
  - その他 - 未指定のパッチに変更を適用します。
  - セキュリティー – 脆弱性を解決するためのソフトウェア変更を適用します。
  - サービス・パック – インストール済みのソフトウェアにパッチを適用します。更新、修正、または機能拡張の一式が単一のインストール可能

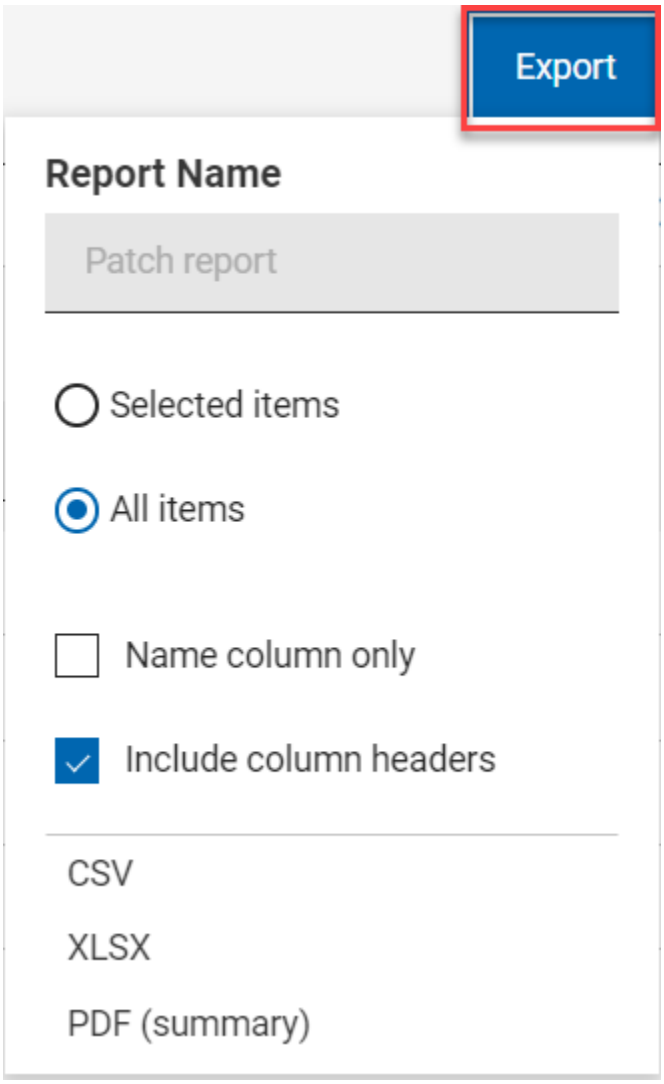
パッケージで提供されます。通常は既存のファイルの更新に使用されますが、バグの修正、セキュリティー・ホールの修復、または新機能の追加にも使用できます。

- **「リリース日」**フィールドを使用して最新パッチを表示します。日付範囲を指定して、特定の期間中に発行されたパッチを確認します。

- **レポートの保存**
  - レポートを将来の参照のために保存し、必要に応じて編集、更新、または削除します。詳しくは、「レポート (（ページ） *16)*」を参照してください。
- **要約の表示**
  1. **「パッチ」**ページで、必要なフィルターを選択します。
  2. **「要約を表示」** をクリックします。フィルターされたすべてのパッチの要約をグラフやテーブルとして表示できます。グラフ上の調べたいエリアにカーソルを合わせると、そのデータ・ポイントとパーセンテージ・データの詳細が表示されます。文字が切り詰められたラベルにカーソルを合わせると、ツール・ヒントにすべてのテキストが表示されます。フィルターを変更するか、検索テキストを入力すると、該当する情報がレポートに動的に表示されます。
     - **リリース日ごとの重大度**: パッチのリリース日から一定期間の重大度レベルごとのパッチの総数を表示します。
     - **OS ファミリーごと**: すべてのオペレーティング・システムに適用可能なパッチを表示します。テーブルは OS 名のアルファベット順にソートされています。
     - **カテゴリーごと**: カテゴリーごとのパッチ数を表示します。
- **エクスポート:**

フィルターされたレポートは `.csv`、`.xlsx`、または `.pdf` の形式でエクスポートできます。

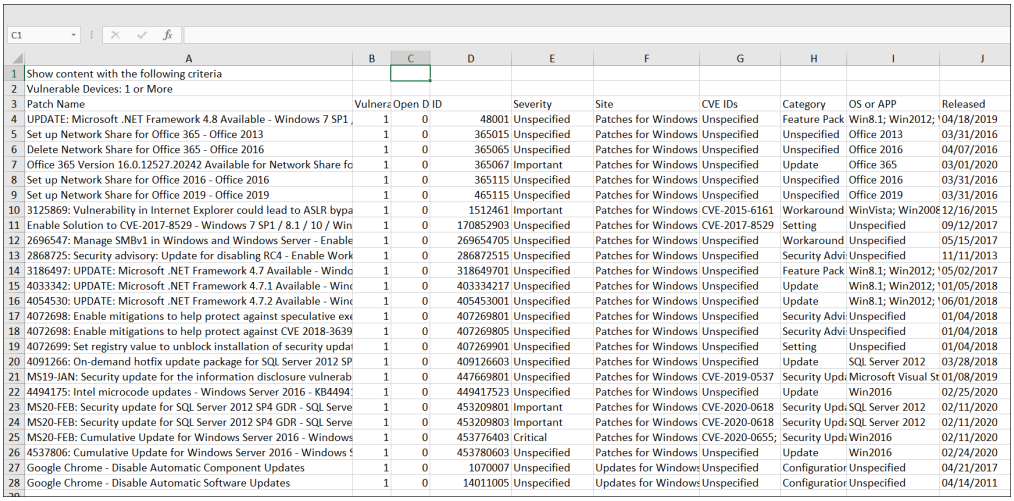
1. **「パッチ」**ページで、必要なフィルターを選択します。
2. **「エクスポート」**をクリックします。



3. **「選択された項目」**オプションを使用すると、フィルターされた結果から項目を選択してエクスポートできます。**「すべての項目」**を使用すると、フィルター処理されたリストからすべての項目をエクスポートできます。目的のオプションを選択します。
4. 名前列のみ: フィルターされた項目の名前のみをエクスポートする場合は、このオプションを選択します。
5. 列ヘッダーを含める: 項目のすべてのデフォルトの列の詳細をエクスポートする場合は、このオプションを選択します。

注: デフォルトの列以外の列を表示している場合は、名前列のみをエクスポートできます。

6. エクスポート先のファイル形式 (CSV、XLSX、PDF) を選択します。
   - デフォルトでは、レポートは「ダウンロード」フォルダーにダウンロードされ、デフォルトのファイル名 (Device_Report_mm_dd_yyyy_username) が付けられます。ブラウザー内でダウンロード設定を変更すると、ファイル名やダウンロードの保存先を変更できます。レポートを保存して後で参照したり、利害関係者と共有したりできます。
   - PDF 形式を選択した場合、数値データを含む `.csv` ファイルとデータの表示形式を含む `.pdf` ファイルを含む `.zip` ファイルがダウンロードされます。
   - エクスポートされたパッチ・レポートには、フィルターと検索条件を適用した後に表示されるパッチの主な詳細が含まれます。これらの詳細には、パッチ名、脆弱なデバイス、重大度、CVE ID、さらにすべてのパッチを展開したときに画面に表示される他のすべての詳細情報が含まれます。以下はサンプル・レポートです。

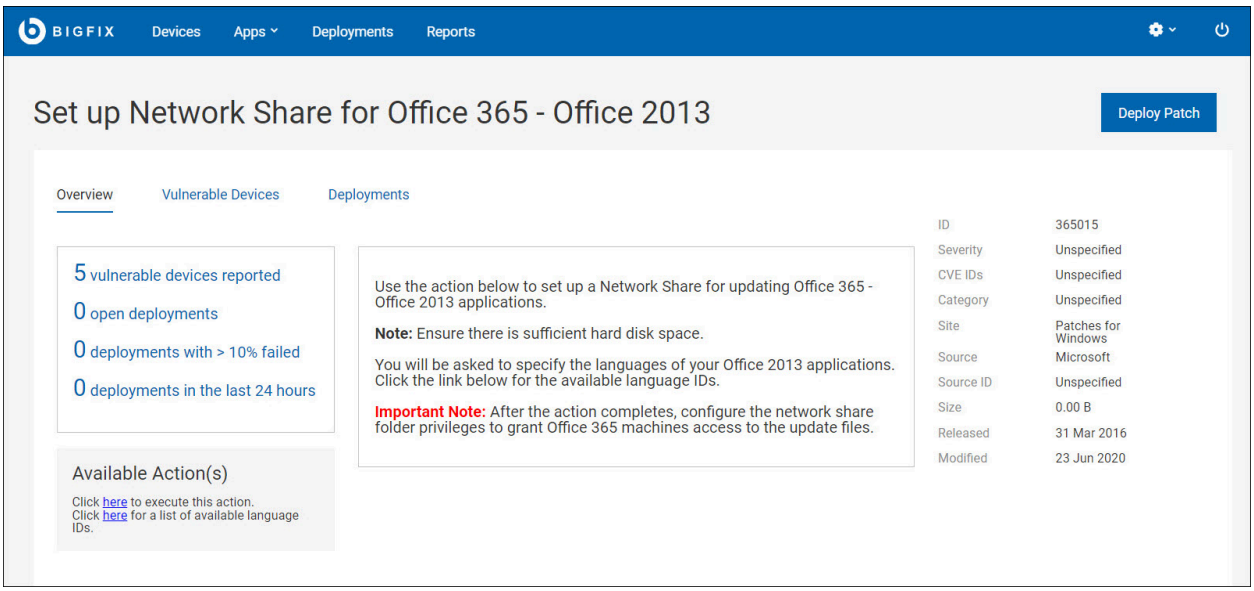


	A	B	C	D	E	F	G	H	I	J
1	Show content with the following criteria									
2	Vulnerable Devices: 1 or More									
3	Patch Name	Vulnera	Open D	ID	Severity	Site	CVE IDs	Category	OS or APP	Released
4	UPDATE: Microsoft .NET Framework 4.8 Available - Windows 7 SP1	1	0	48001	Unspecified	Patches for Windows	Unspecified	Feature Pack	Win8.1; Win2012;	04/18/2019
5	Set up Network Share for Office 365 - Office 2013	1	0	365015	Unspecified	Patches for Windows	Unspecified	Unspecified	Office 2013	03/31/2016
6	Delete Network Share for Office 365 - Office 2016	1	0	365065	Unspecified	Patches for Windows	Unspecified	Unspecified	Office 2016	04/07/2016
7	Office 365 Version 16.0.12527.20242 Available for Network Share fo	1	0	365067	Important	Patches for Windows	Unspecified	Update	Office 365	03/01/2020
8	Set up Network Share for Office 2016 - Office 2016	1	0	365115	Unspecified	Patches for Windows	Unspecified	Unspecified	Office 2016	03/31/2016
9	Set up Network Share for Office 2019 - Office 2019	1	0	465115	Unspecified	Patches for Windows	Unspecified	Unspecified	Office 2019	03/31/2016
10	3125869: Vulnerability in Internet Explorer could lead to ASLR bypa	1	0	1512461	Important	Patches for Windows	CVE-2015-6161	Workaround	WinVista; Win2008	12/16/2015
11	Enable Solution to CVE-2017-8529 - Windows 7 SP1 / 8.1 / 10 / Win	1	0	170852903	Unspecified	Patches for Windows	CVE-2017-8529	Setting	Unspecified	09/12/2017
12	2696547: Manage SMBv1 in Windows and Windows Server - Enable	1	0	269654705	Unspecified	Patches for Windows	Unspecified	Workaround	Unspecified	05/15/2017
13	2868725: Security advisory: Update for disabling RC4 - Enable Work	1	0	286872515	Unspecified	Patches for Windows	Unspecified	Security Advi	Unspecified	11/11/2013
14	3186497: UPDATE: Microsoft .NET Framework 4.7 Available - Windo	1	0	318649701	Unspecified	Patches for Windows	Unspecified	Feature Pack	Win8.1; Win2012;	05/02/2017
15	4033342: UPDATE: Microsoft .NET Framework 4.7.1 Available - Winc	1	0	403334217	Unspecified	Patches for Windows	Unspecified	Update	Win8.1; Win2012;	01/05/2018
16	4054530: UPDATE: Microsoft .NET Framework 4.7.2 Available - Winc	1	0	405453001	Unspecified	Patches for Windows	Unspecified	Update	Win8.1; Win2012;	06/01/2018
17	4072698: Enable mitigations to help protect against speculative exe	1	0	407269801	Unspecified	Patches for Windows	Unspecified	Security Advi	Unspecified	01/04/2018
18	4072698: Enable mitigations to help protect against CVE 2018-3639	1	0	407269805	Unspecified	Patches for Windows	Unspecified	Security Advi	Unspecified	01/04/2018
19	4072699: Set registry value to unblock installation of security updat	1	0	407269901	Unspecified	Patches for Windows	Unspecified	Setting	Unspecified	01/04/2018
20	4091266: On-demand hotfix update package for SQL Server 2012 SP	1	0	409126603	Unspecified	Patches for Windows	Unspecified	Update	SQL Server 2012	03/28/2018
21	MS19-JAN: Security update for the information disclosure vulnerab	1	0	447669801	Unspecified	Patches for Windows	CVE-2019-0537	Security Upd	Microsoft Visual St	01/08/2019
22	4494175: Intel microcode updates - Windows Server 2016 - KB4494	1	0	449417523	Unspecified	Patches for Windows	Unspecified	Update	Win2016	02/25/2020
23	MS20-FEB: Security update for SQL Server 2012 SP4 GDR - SQL Serve	1	0	453209801	Important	Patches for Windows	CVE-2020-0618	Security Upd	SQL Server 2012	02/11/2020
24	MS20-FEB: Security update for SQL Server 2012 SP4 GDR - SQL Serve	1	0	453209803	Important	Patches for Windows	CVE-2020-0618	Security Upd	SQL Server 2012	02/11/2020
25	MS20-FEB: Cumulative Update for Windows Server 2016 - Windows	1	0	453776403	Critical	Patches for Windows	CVE-2020-0655;	Security Upd	Win2016	02/11/2020
26	4537806: Cumulative Update for Windows Server 2016 - Windows S	1	0	453780603	Unspecified	Patches for Windows	Unspecified	Update	Win2016	02/24/2020
27	Google Chrome - Disable Automatic Component Updates	1	0	1070007	Unspecified	Updates for Windows	Unspecified	Configuratior	Unspecified	04/21/2017
28	Google Chrome - Disable Automatic Software Updates	1	0	14011005	Unspecified	Updates for Windows	Unspecified	Configuratior	Unspecified	04/14/2011

パッチ文書

パッチの説明、脆弱なデバイス、デプロイメント履歴を確認するには、そのパッチ名をクリックします。関連付けられたビューへのリンクを使用して、パッチの詳細を掘り下げます。

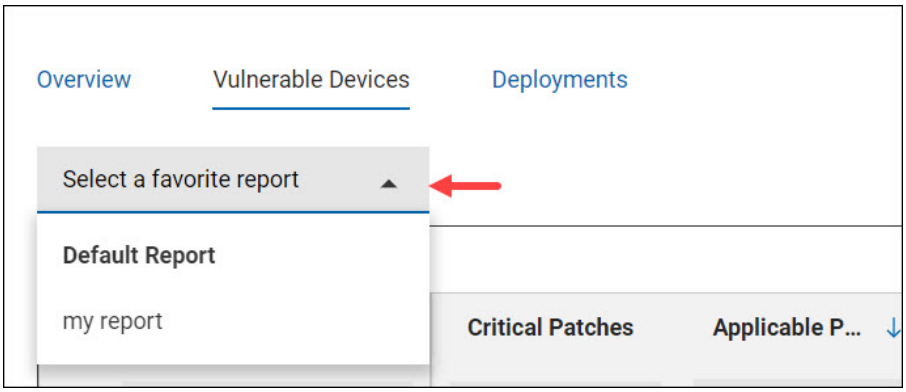
コンテンツ文書の「メモ」と「重要」に特別の注意を払います。これらの記載には、そのコンテンツに関連付けられた既知の問題などの有益な情報が含まれています。



パッチ文書の各ビューは以下のとおりです。

- 概要 - メタデータ、使用可能なアクション、ベンダー・リンクなど、パッチの詳細な説明。
- 脆弱なデバイス - 対象となる関連デバイスのリスト。
- デプロイメント - パッチ・デプロイメント履歴。

「**脆弱なデバイス**」と「**デプロイメント**」 タブで保存されているレポートをロードできます。ドロップダウンを使用して、レポートを選択します。



「実行可能なアクション」セクション内の情報は、BigFix データベースから直接入手されるため、オプションとフォーマット設定が異なる可能性があります。多くの場合、ベンダーのリリース・ノートへのリンクが含まれます。例えば、「ここをクリックして、Windows XP SP3 のリリース・ノートを表示」などです。

第 5 章. パッチ・ポリシー入門

パッチ・ポリシーは 1 つのパッチ・リストを定義する基準一式、つまり、特定のエンドポイント・セットのパッチ適用基準に適合する Fixlet の集合です。

「パッチ・ポリシー」アプリケーションを使用すると、全社で確実に継続的にパッチを適用できます。さまざまなマシン・グループのパッチ適用スケジュールを作成し、それぞれに異なるデプロイメント動作を割り当てます。パッチのタイミング、頻度と所要時間、事前キャッシュ、再試行の動作を設定します。再開が保留された場合は、間隔を置いて開始、エラーのバイパス、デバイス所有者への通知を行います。

組織内のパッチ適用サイクルとセキュリティー・ガイドラインに適合するパッチ適用戦略を実装します。パッチ・ポリシーを使用して、組織の継続的なセキュリティーとコンプライアンスのプロセスを確立し維持します。パッチ・ポリシーは現在、サポートされるパッチ・サイト (（ページ） 46)に記載されているサイトをサポートしています。

要件

- BigFix Platform バージョン 9.5.5 以降。
- BigFix WebUI がインストール済みで、実行中。
- 該当するすべての BigFix Patch サイトへの登録。

BigFix console で、デプロイメントに関連するパッチ・サイトをすべて有効化し、すべてのコンピューターから有効にしたサイトを登録します。

パッチ・ポリシーの概要

パッチ・ポリシー・アプリケーションを開くには、BigFix WebUI の**「アプリ」**メニューで**「パッチ・ポリシー」**を選択します。

パッチ・ポリシーを作成するには、以下の手順を実行します。

1. ポリシー名を入力し、ポリシーに組み込むパッチのタイプを選択します。例えば、オペレーティング・システム更新の重要なサービス・パックを含むポリシーを作成します。
2. デプロイメントのタイミング、頻度、動作を含め、このポリシーのロール・アウト・スケジュールを作成します。
3. ポリシー対象の選択: パッチの適用対象となるデバイス。
4. ポリシーをアクティブにします。

   このプロセスについて詳しくは、『パッチ・ポリシーの作成 (（ページ） 70)』を参照してください。

ポリシーを常に最新状態に保つ

ポリシー基準を満たす新規パッチが使用可能になると、パッチ・ポリシー・アプリケーションから通知が送付されます。「ポリシー・リスト」でポリシー名の横にあるデルタ・アイコンは、パッチ・コンテンツが追加または変更されていることを知らせています。新規のコンテンツを含めるために、ポリシーを更新します。ポリシーを常に最新状態にしておくには、ポリシーを手動で更新するか、自動最新表示オプションを使用します。

除外

除外しなければ、ポリシーへの組み込み基準に適合してしまうパッチを除外できます。または手動組み込みを使用したカスタム・アプリケーションで、問題の原因となるパッチを除外します。または動的除外を設定し、Microsoft Office の更新をすべて、Windows の更新ポリシーから除外します。設定した除外は、削除するまで有効のままとなります。パッチ・ポリシーには、監査用パッチ、問題のあるパッチ、またはデフォルト・アクションのないパッチは決して組み込まれません。

ポリシー・ベースのパッチ適用結果をモニターするには、WebUI の「デプロイメント」ビューを使用します。詳しくは、「デプロイメント入門 (（ページ） 209)」を参照してください。

権限とパッチ・ポリシー

BigFix のマスター・オペレーター (MO) には、すべてのパッチ・ポリシー機能に対するフル・アクセス権限があります。MO は、ポリシーを作成、編集、削除、アクティブ化、および中断し、パッチのロールアウトとスケジュールを管理し、新しいパッチがリリースされ

たときにポリシーを更新できます。マスター以外のオペレーター (NMO) は、ポリシーを追加、編集、または削除できます。NMO は、関連する権限を持っている場合に、既存のスケジュールに対象を追加することや、スケジュールから対象を削除することもできます。

パッチ・ポリシー・カテゴリー

以下の表は、パッチ・ポリシーの外部コンテンツ・カテゴリーと Fixlet カテゴリーの間のマッピングを示しています。

WebUI パッチ・ポリシー・カテゴリー	**Fixlet カテゴリー**
BUG FIX	バグ修正 バグ修正アドバイザリー バグ
ENHANCEMENT	定義の更新 定義の更新 Feature Pack Hotfix 更新 更新 製品拡張アドバイザリー ENHANCEMENT 推奨 オプション アップグレード
SERVICE PACK	ロールアップ サービスパック 更新ロールアップ
SECURITY	きわめて重要な更新

WebUI パッチ・ポリシー・カテゴリー	Fixlet カテゴリー
	重要なアップデート セキュリティ セキュリティー・アドバイザリー セキュリティー Hotfix セキュリティー設定 セキュリティーの更新 セキュリティー更新 SECURITY 必須

実行動作

次の表は、**「パッチ前およびパッチ後」コンテンツを使用する場合**と**「パッチ前およびパッチ後」コンテンツを使用しない場合**のパッチ・ポリシーの動作を示しています。

表 1. パッチ・ポリシーの実行動作

「パッチ前およびパッチ後」コンテンツの構成	**MAG 順序の実行は順番に実行されます (MAG1、MAG2、MAG3 など)**	**スケジュールの構成時に使用できる「強制的に再起動」オプションの使用**	**実行動作**
「パッチ前およびパッチ後」コンテンツを**使用する**場合	あり	再起動は、最後の MAG 実行の終了時にのみ適用されます。	MAG のシーケンスは、パッチ Fixlet が関連していない場合でも、すべての対象デバイスで実行されます。これは、関連する場合、事前タスク/ポスト・

表 1. パッチ・ポリシーの実行動作 (続く)

「パッチ前およびパッチ後」コンテンツの構成	**MAG 順序の実行は順番に実行されます (MAG1、MAG2、MAG3 など)**	**スケジュールの構成時に使用できる「強制的に再起動」オプションの使用**	**実行動作**
			タスクまたはポスト・アクションの再起動も実行されることを意味します。
「パッチ前およびパッチ後」コンテンツを**使用しない**場合	No[1]	再起動は、最後に実行される MAG が不明なため、各 MAG の実行後に適用されます。	各 MAG は、デバイスが MAG 内の 1 つ以上の Fixlet に適用可能な場合にのみ、対象デバイスで実行されます。

注:

スケジュールでターゲットを定義したオペレーターが管理する 1 つ以上のエンドポイントに関連する場合は、MAG に Fixlet が含まれます。

1. **「パッチ前およびパッチ後」コンテンツを使用しない場合**: MAG は、必ずしもエンドポイントで順序どおりに実行されるわけではありません。MAG は、エンドポイントに関連するようになると順番に実行されます。

注:

「プロパティー別にターゲット設定する」、**「グループ別にターゲット設定する」**、または**「デバイス別にターゲット設定する」**を介してパッチ・ポリシーで発

行された MAG アクションは、MAG の発行時に対象となっているデバイスに関連する Fixlet のみで構成されます。該当する Fixlet がない場合、MAG は発行されません。詳しくは、「サーバー設定 (（ページ）　　)」を参照してください。

オペレーティング・システムの更新

次の表に、Fixlet サイトとパッチ・ポリシーで使用可能な選択項目間のマッピングを示します。

Amazon Linux

表 2. Amazon Linux の OS バージョンと Fixlet サイト名

OS バージョン	Fixlet サイト名
Amazon Linux 2	Amazon Linux 2 向けパッチ
Amazon Linux 2 with Graviton	Patches for Amazon Linux 2 Graviton

Rocky Linux

表 3. Rocky Linux の OS バージョンと Fixlet サイト名

OS バージョン	Fixlet サイト名
Rocky Linux 8	Patches for Rocky Linux 8

CentOS

表 4. CentOS の OS バージョンおよび Fixlet サイト名

OS バージョン	Fixlet サイト名
CentOS 6	CentOS 6 プラグイン R2 向けパッチ
CentOS 7	CentOS 7 プラグイン R2 向けパッチ
CentOS 8	CentOS 8 向けパッチ

Debian

表 5. Debian の OS バージョンと Fixlet サイト名

OS バージョン	Fixlet サイト名
Debian 7	Debian 7 向けパッチ
Debian 11	Debian 11 向けパッチ

Mac OS X

表 6. Mac OS X の OS バージョンと Fixlet サイト名

OS バージョン	Fixlet サイト名
任意のパッチはサイトから動的にフィルタリングされます	Mac OS X 用パッチ

Oracle Linux

表 7. Oracle Linux の OS バージョンおよび Fixlet サイト名

OS バージョン	Fixlet サイト名
Oracle Linux 6	Patches for Oracle Linux 6
Oracle Linux 7	Patches for Oracle Linux 7
Oracle Linux 8	Patches for Oracle Linux 8

Red Hat Enterprise Linux

表 8. Red Hat Enterprise Linux の OS バージョンと Fixlet サイト名

OS バージョン	Fixlet サイト名
Red Hat Enterprise 5	RHEL 5 ESU 向けパッチ

表 8. Red Hat Enterprise Linux の OS バージョンと Fixlet サイト名 (続く)

OS バージョン	Fixlet サイト名
Red Hat Enterprise 6	• RHEL 6 ネイティブ・ツール向けパッチ • RHEL RHSM 6 on System z 向けパッチ • RHEL 6 ESU 向けパッチ
Red Hat Enterprise 7	• RHEL 7 向けパッチ • RHEL 7 ppc64le 向けパッチ • RHEL 7 ppc64be 向けパッチ • RHEL RHSM 7 on System z 向けパッチ • RHEL 7 ESU 向けパッチ
Red Hat Enterprise 8	• RHEL 8 向けパッチ • RHEL 8 ESU 向けパッチ • RHEL 8 ppc64le 向けパッチ
Red Hat Enterprise 9	• RHEL 9 向けパッチ

SUSE Linux Enterprise

表 9. SUSE Linux Enterprise の OS バージョンおよび Fixlet サイト名

OS バージョン	Fixlet サイト名
SLE 11	SLE 11 ネイティブ・ツール向けパッチ
SLE 12	SLE 12 向けパッチ
SLE 12 PPC64LE	SLE 12 ppc64le 向けパッチ
SLE 12 System z	SLE 12 on System z 向けパッチ (Patches for SLE 15 on System z)

表 9. SUSE Linux Enterprise の OS バージョンおよび Fixlet サイト名 (続く)

OS バージョン	Fixlet サイト名
SLE 15	SLE15 向けパッチ
SLE 15 System z	SLE 15 on System z 向けパッチ (Patches for SLE 15 on System z)

Ubuntu

表 10. Ubuntu の OS バージョンおよび Fixlet サイト名

OS バージョン	Fixlet サイト名
Ubuntu 14.04	Ubuntu 1404 向けパッチ
Ubuntu 16.04	Ubuntu 1604 向けパッチ
Ubuntu 18.04	Ubuntu 1804 向けパッチ
Ubuntu 20.04	Ubuntu 2004 向けパッチ
Ubuntu 22.04	Ubuntu 2204 向けパッチ

Windows

表 11. Windows の OS バージョンおよび Fixlet サイト名

OS バージョン	Fixlet サイト名
選択された OS バージョンのパッチは、サイトから動的にフィルタリングされます	• Enterprise Security • Windows 向けパッチ (ドイツ語) • Windows 向けパッチ (フランス語) • Windows 向けパッチ (ポーランド語)

表 11. Windows の OS バージョンおよび Fixlet サイト名 (続く)

OS バージョン	Fixlet サイト名
	• Windows 向けパッチ (イタリア語) • Windows 向けパッチ (スペイン語) • Windows 向けパッチ (チェコ語) • Windows 向けパッチ (ブラジル・ポルトガル語) • Windows 向けパッチ (日本語) • Windows 向けパッチ (簡体字中国語) • Windows 向けパッチ (韓国語) • Windows 向けパッチ (トルコ語) • Windows 向けパッチ (ハンガリー語) • Windows 向けパッチ (オランダ語) • Windows 向けパッチ (繁体字中国語) • Windows 向けパッチ (ノルウェー語) • Windows 向けパッチ (フィンランド語) • Windows 向けパッチ (スウェーデン語) • Windows 向けパッチ (ギリシャ語) • Windows 向けパッチ (デンマーク語)

表 11. Windows の OS バージョンおよび Fixlet サイト名 (続く)

OS バージョン	Fixlet サイト名
	• Windows 向けパッチ (ヘブライ語) • Windows 向けパッチ (ロシア語) • Windows 7 ESU 向けパッチ • Windows 2008 ESU 向けパッチ

オペレーティング・システム・アプリケーションの更新

次の表に、OS、さまざまなサイト名、アプリケーションを含む**オペレーティング・システム**・アプリケーションの更新を示します。

Mac OS X および Windows の OS アプリケーションの更新

表 12. Mac OS X および Windows の Fixlet サイト名とアプリケーションの更新

OS	Fixlet サイト名	アプリケーション数
Mac OS X	Mac OS X 用パッチ	• Java • iTunes • Safari
Windows	• Enterprise Security • Windows 向けパッチ (ドイツ語) • Windows 向けパッチ (フランス語)	詳しくは、「システム要件 (（ページ）　　)」を参照してください。

表 12. Mac OS X および Windows の Fixlet サイト名とアプリケーションの更新 (続く)

OS	Fixlet サイト名	アプリケーション数
	• Windows 向けパッチ (ポーランド語) • Windows 向けパッチ (イタリア語) • Windows 向けパッチ (スペイン語) • Windows 向けパッチ (チェコ語) • Windows 向けパッチ (ブラジル・ポルトガル語) • Windows 向けパッチ (日本語) • Windows 向けパッチ (簡体字中国語) • Windows 向けパッチ (韓国語) • Windows 向けパッチ (トルコ語) • Windows 向けパッチ (ハンガリー語)	

表 12. Mac OS X および Windows の Fixlet サイト名とアプリケーションの更新 (続く)

OS	Fixlet サイト名	アプリケーション数
	• Windows 向けパッチ (オランダ語) • Windows 向けパッチ (繁体字中国語) • Windows 向けパッチ (ノルウェー語) • Windows 向けパッチ (フィンランド語) • Windows 向けパッチ (スウェーデン語) • Windows 向けパッチ (ギリシャ語) • Windows 向けパッチ (デンマーク語) • Windows 向けパッチ (ヘブライ語) • Windows 向けパッチ (ロシア語)	

表 12. Mac OS X および Windows の Fixlet サイト名とアプリケーションの更新 (続く)

OS	Fixlet サイト名	アプリケーション数
	• Windows 7 ESU 向けパッチ • Windows 2008 ESU 向けパッチ	

サード・パーティーの更新

次の表に、OS、さまざまなサイト名、アプリケーション/発行者を含むサード・パーティーの更新を示します。

Mac OS X および Windows 用のサード・パーティーの更新

表 13. Mac OS X および Windows の Fixlet サイト名とアプリケーション/発行者の更新

OS	Fixlet サイト名	アプリケーション/発行者
Mac OS X	Mac アプリケーションの更新	• Adobe Acrobat • Adobe Air • Adobe Flash • Adobe Reader • Adobe Shockwave • Google Chrome • GoToMeeting • Microsoft • Mozilla Firefox • Webex • ズーム

表 13. Mac OS X および Windows の Fixlet サイト名とアプリケーション/発行者の更新 (続く)

OS	Fixlet サイト名	アプリケーション/発行者
Windows	• Windows アプリケーションの更新 • 拡張パッチ • 拡張 Windows アプリケーションの更新	詳しくは、システム要件 (（ページ）　　) を参照してください。

重大度マッピング

次の表は、**パッチ・ポリシーの重大度**カテゴリーと**Fixlet の重大度フィールド**カテゴリー間のマッピングを示しています。

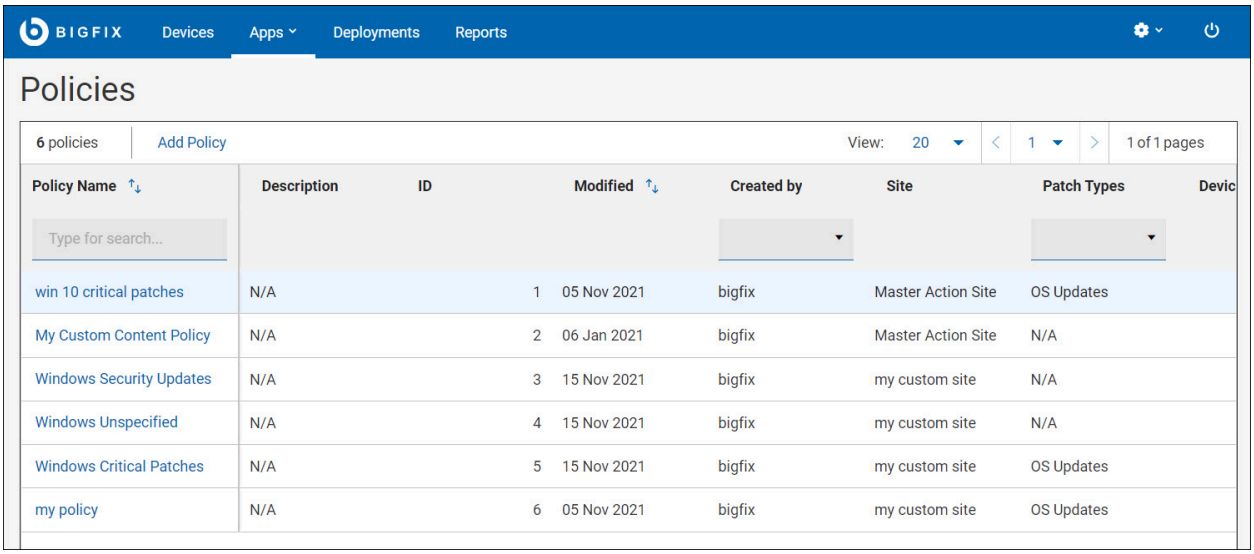
表 14. パッチ・ポリシーの重大度と Fixlet の重大度フィールド

パッチ・ポリシーの重大度	Fixlet の重大度フィールド
CRITICAL	重大、必須、高
IMPORTANT	重要、推奨
管理	管理、中
低	低、オプション、無視可能
未指定	未指定、該当なし、および空の値

パッチ・ポリシー・リスト

使用可能なポリシーがグリッド・ビューにリストされます。それぞれの列で検索、ソート、フィルター・オプションを使用すると、ポリシーがすばやく見つかります。ポリシー名をクリックして、そのデバイスの文書を開きます。**「ポリシーの追加」**ボタンをクリックして、新規ポリシーを作成します。

重要: マスター以外のオペレーター (NMO) がパッチ・ポリシー・アプリケーションのさまざまなアクションを実行するには、関連する権限が必要です。権限の詳細については、 ((ページ)　　)を参照してください。



期限切れパッチ

ポリシーは、新しいパッチがある場合、またはそのポリシーのパッチが変更、または置き換えられた場合にも期限切れになります。新しい項目の数が**「パッチの更新」** 列にリストされます。

新しいコンテンツを含めるために、ポリシーを更新します。アクティブな期限切れパッチは動作し続けますが、あまり効果的ではありません。例えば、毎日午後 3 時に実行される新しいポリシーを作成すると、実行初日にパッチは指定されたターゲットにデプロイされます。2 日目に新規のパッチが利用可能となり、ポリシーが期限切れとなった場合、3 日目以降、ポリシーは実行されますが、ポリシーは既にパッチがデプロイされていることを認識しているため、何もしません。ポリシーは更新され次第、新規パッチをデプロイします。

新しいコンテンツにより置き換え済のパッチはデプロイされなくなります。

以下のリストは、グリッド・ビュー内の個々の列を理解するのに役立ちます。

- パッチ: このポリシー内のパッチ数
- デバイス: 対象のコンピューターとコンピューター・グループの数
- OS: ポリシー内のパッチのオペレーティング・システム
- パッチ・タイプ: OS の更新、アプリケーションの更新、またはサード・パーティー製アプリケーションの更新
- 状況: アクティブまたは中断状態
- パッチの更新: 作成日時、または最終更新日時より後に Fixlet が変更された数
- 次回の更新: 次回の自動最新表示予定日 (有効な場合)
- 「サイト」: パッチ・ポリシーを含むカスタム・サイト

ポリシー状況: アクティブまたは中断状態

パッチ・ポリシーには次の 2 種類の状況があります。アクティブまたは中断状態ポリシーを更新、新規スケジュールを追加、またはその他の変更を追加するには、アクティブ・ポリシーを中断します。対象をポリシーに追加する際は、ポリシーを中断する必要はありません。新規のポリシーは、アクティブ化されるまでは中断状態のままになります。

パッチ・ポリシーの作成

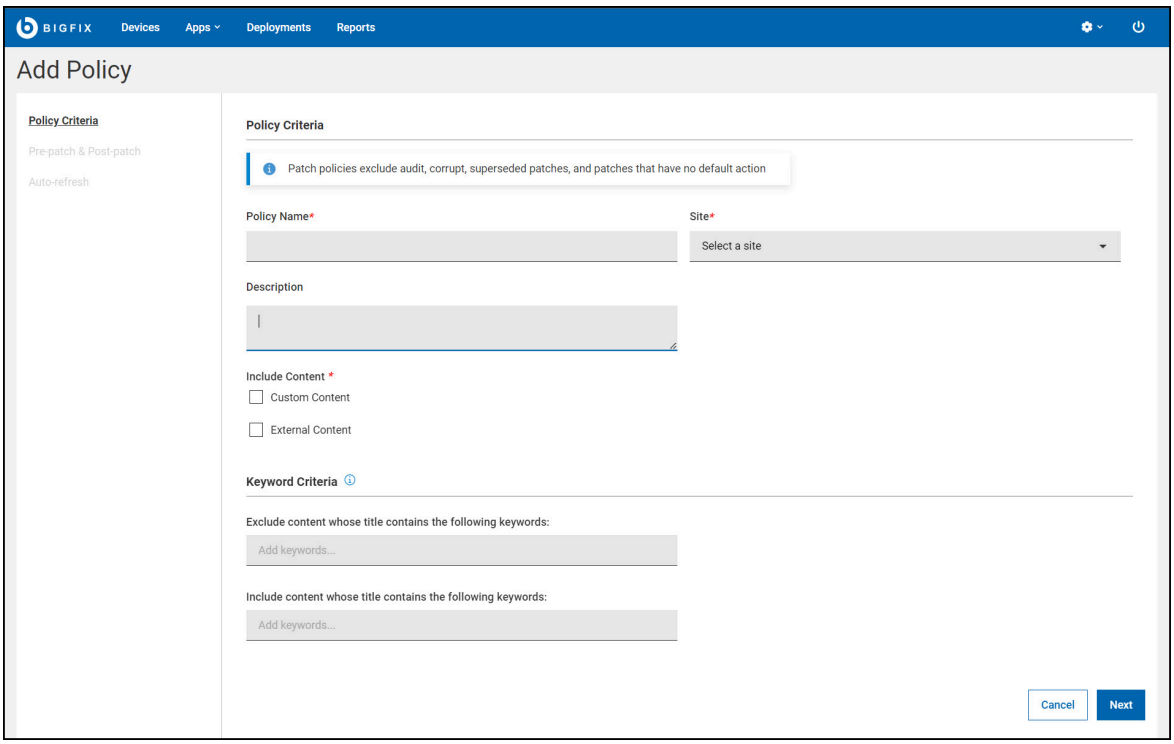
このページでは、パッチ・ポリシーを作成し、組み込むパッチを選択し、デプロイメント・オプションを設定し、対象を指定するための手順を詳しく示します。

アプリケーションを開くには、WebUI の**「アプリケーション」**メニューで**「パッチ・ポリシー」**を選択します。パッチ・ポリシー・タスクの要約を確認するには、「パッチ・ポリシー運用」 (（ページ） *92)*を確認します。

1. **「ポリシー」**ページで、**「ポリシーの追加」**をクリックします。
   「ポリシーの追加」ページが表示されます。

   注: ポリシーを追加、編集または削除するには、マスター以外のオペレーター (NMO) に「ポリシーの作成/編集」および「ポリシーの削除」の権限が必要です。権限の詳細については、WebUI 権限サービス (（ページ）)を参照してください。NMO は「ポリシーの作成/編集」の権限を持っていても、マスター・アクション・サイトに保存されたポリシーの定義を編集すること

はできません。現在、NMO はマスター・アクション・サイトにアクセスできず、自分のカスタム・サイトにのみアクセスできます。



2. 「ポリシー基準」ページで、次の情報を入力します。

   ポリシー名

   新しいポリシー名を入力します。

   サイト

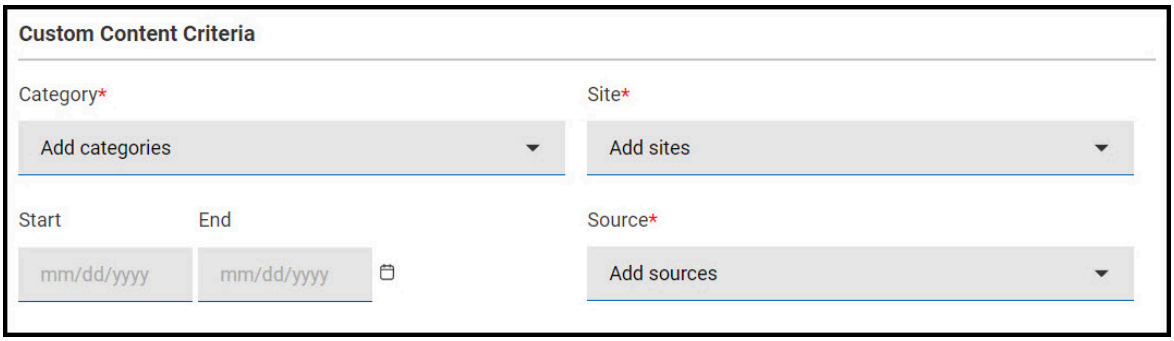
   ドロップダウンから**「マスター・アクション・サイト」**または**「カスタム・サイト」**を選択し、ポリシーとそのスケジュールを保存します。

   説明

   説明を入力します。

3. 次の 2 種類のコンテンツを含めることができます。カスタム・コンテンツまたは外部コンテンツ

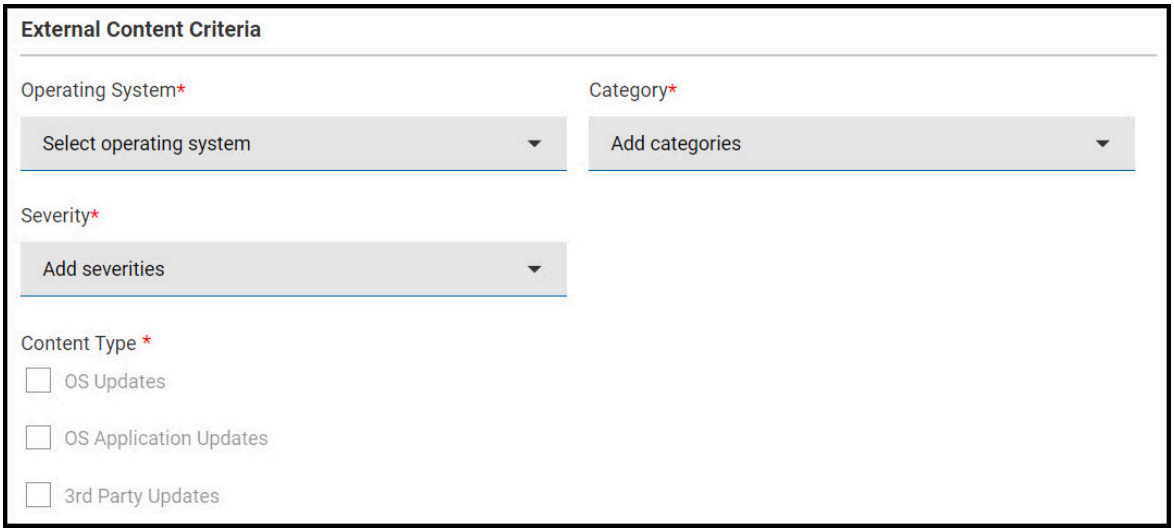
   カスタム・コンテンツ:



a. カスタム・サイトの Fixlet を含めるには、このオプションをオンにします。
b. **「カスタム・コンテンツ基準」**で、ドロップダウンから、新しいポリシーに含める必要がある**「カテゴリー」**、**「サイト」**、**「開始日/終了日」**、**「ソース」**日付を選択します。

注: ポリシーに含めるには、カスタム Fixlet には、上記のフィールドを含める必要があります。

外部コンテンツ:



a. 外部サイトの Fixlet を含めるには、このオプションをオンにします。
b. **「外部コンテンツ基準」**で、**「オペレーティング・システム」**、**「カテゴリー」**、**「重要度」**、**「コンテンツ・タイプ」**を選択します。

- オペレーティング・システム (1 つ選択): Amazon Linux、CentOS、Mac OS X、Oracle Linux、Red Hat Enterprise Linux、SUSE Linux Enterprise、Ubuntu、Windows。
- カテゴリー: バグ修正、機能拡張、セキュリティー。
- 重大度: きわめて重要、重要、中、低、未指定。
- コンテンツタイプ: OS の更新、OS アプリケーションの更新、サード・パーティーの更新。

注: パッチ・ポリシーを作成するときには、次の点を確認してください。
- Fixlet にはデフォルト・アクションが必要です。デフォルト・アクションがない場合、Fixlet はパッチ・ポリシーに含まれません。
- パッチ・ポリシーは、デフォルト・アクションを持つ Fixlet のみを検出します。
- タスクは検出されません。

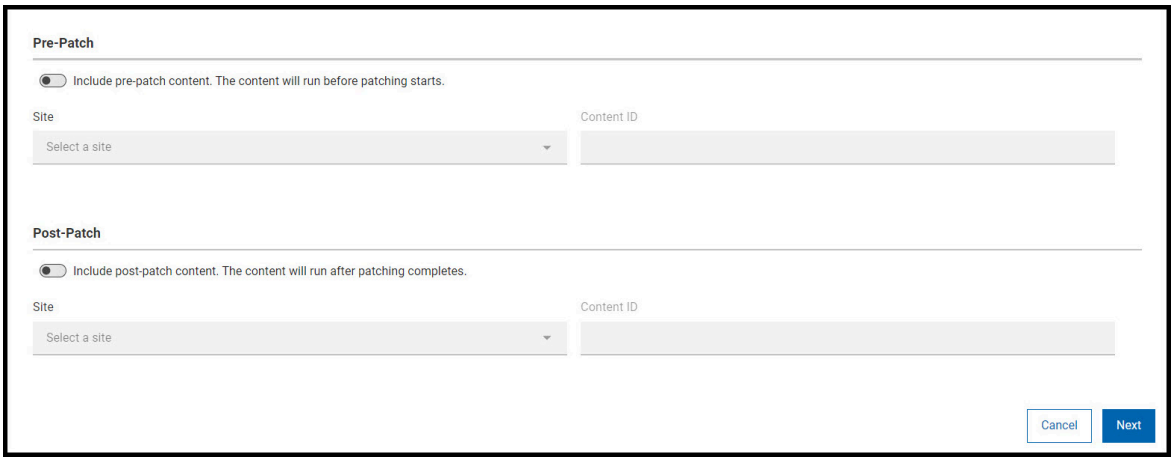
4. 必要に応じて、**キーワード条件**でパッチの除外または包含を指定します。パッチのタイトルから抜粋したキーワードまたはフレーズを入力し、**Enter** キーを押して追加します。これらのフィールドでは大文字と小文字が区別されないため、大文字と小文字の違いは無視できます。キーワードまたはフレーズを追加/削除するには、 アイコンと アイコンを使用します。

   注: 100,000 個以上の Fixlet など、ポリシーに多数の項目を含めると、パッチ・ポリシーのパフォーマンスが低下する可能性があります。物事をスムーズに実行するためには、より小さなポリシーを作成することをお勧めします。

5. **「次へ」**をクリックして、新規ポリシーの**「パッチ前およびパッチ後」**動作を構成します。**前/後コンテンツを使用する場合**および**前/後コンテンツを使用しない場合**について詳しくは、実行動作 (（ページ） 57)を参照してください。

   注: 「パッチ前およびパッチ後」コンテンツの設定は必須ではありません。パッチ前コンテンツとパッチ後コンテンツのいずれか、あるいはその両方を

設定できます。新規パッチ・ポリシーで「パッチ前およびパッチ後」コンテンツが不要な場合は、**「次へ」**をクリックして、この手順をスキップできます。



a. **切り替えスイッチ**をクリックして、「パッチ前」または「パッチ後」を有効化します。

注: デフォルトでは「パッチ前」と「パッチ後」は無効になっています。

b. ドロップダウン・メニューから**「サイト」**を選択します。

注: カスタム・サイトのみを選択できます。

c. **「コンテンツ ID」**を入力します。Fixlet またはタスクの名前は、コンテンツ ID の下に表示されます。

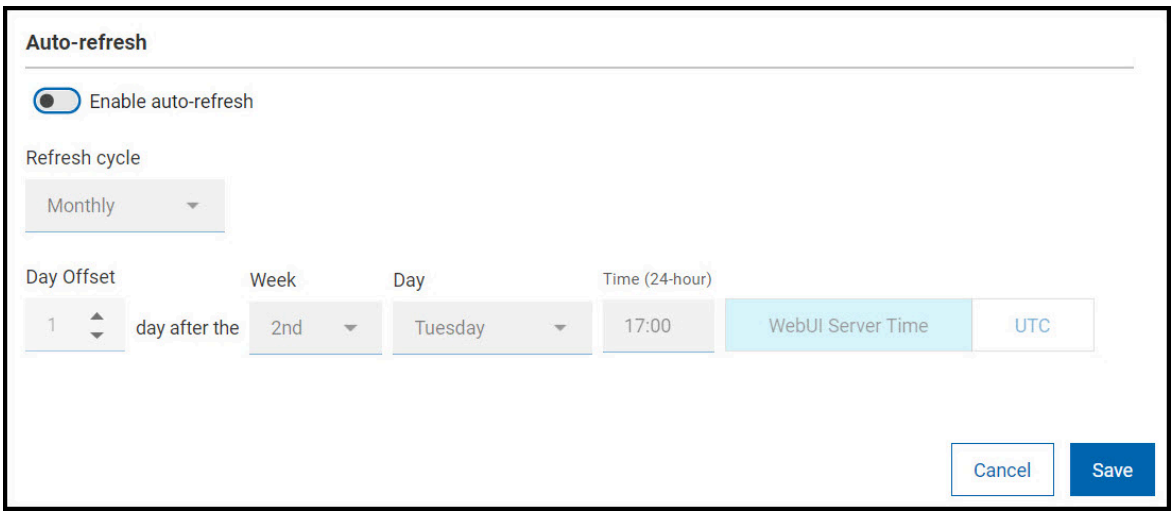
注:「コンテンツ ID」フィールドに入力できるのは、単一の **Fixlet** または**タスク**のみです。

注:

「パッチ前」または「パッチ後」を選択した場合、以下の動作が適用されます。

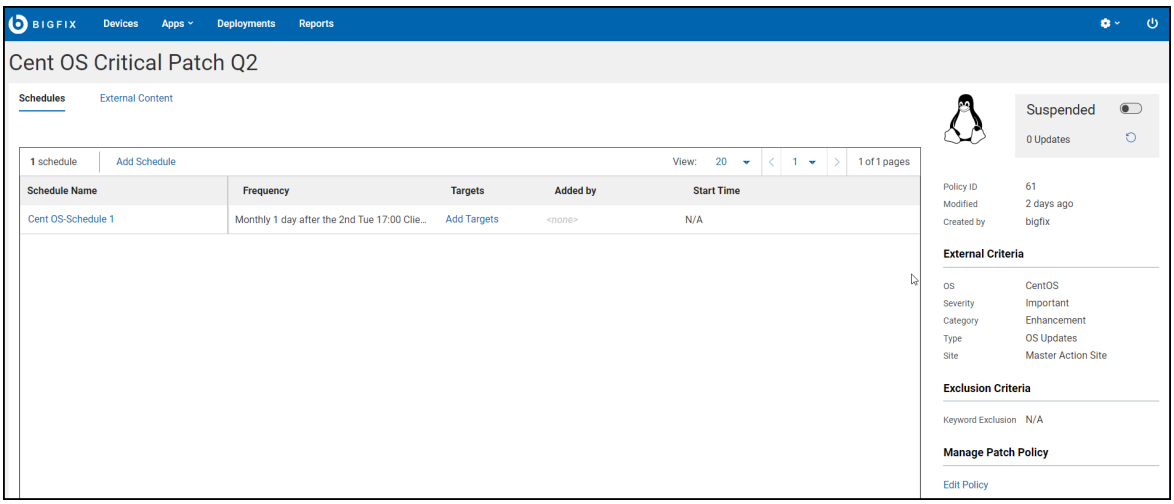
- 結果として得られるポリシー・アクションに含まれる Fixlet が 200 以下の場合、デバイスがポリシー内の事前タスク、ポスト・タスク、またはパッチ Fixlet のいずれかに適用可能であれば、ポリシー・アクションは対象デバイスで実行されます。
- 結果として得られるポリシー・アクションに含まれる Fixlet が 200 を超える場合、ポリシー・アクションは、ポリシー内のパッチ Fixlet に適用可能なデバイスだけでなく、すべての対象デバイスで実行されます。また、「提案」や「強制的に再起動」などの設定は、有効化されている場合、対象となるすべてのデバイスで実行されます。

6. **「次へ」**をクリックして、新規ポリシーの自動最新表示の動作を設定します。
7. 新規パッチの内容をポリシーに自動的に組み込むには、オプションの自動最新表示機能を使用します。更新のタイミングと頻度を制御するには、更新間隔を設定します。自動最新表示はデフォルトで無効にされています。



- 更新サイクル (毎日、毎週、毎月) または具体的な日付 (曜日または毎月何日) と時刻 (時間)。
- 日のオフセット: オプションの「経過日数」コントロールを使用して、火曜日パッチのような月次イベントに対する自動最新表示の更新をスケジュールします。月の第 2 火曜日は第 2 週にあることが多いですが、いつもそうとは限りません。(例えば、2018 年の 8 月の火曜日パッチは 14 日でした。)「経過日数」オプションを使用して、日付が月によって異なるイベントの更新を調整します。
- タイムゾーン: タイム・ゾーン (WebUI サーバー時間または UTC) を選択します。

8. ポリシー設定を保存し、ポリシー文書を表示するには、**「保存」**をクリックします。



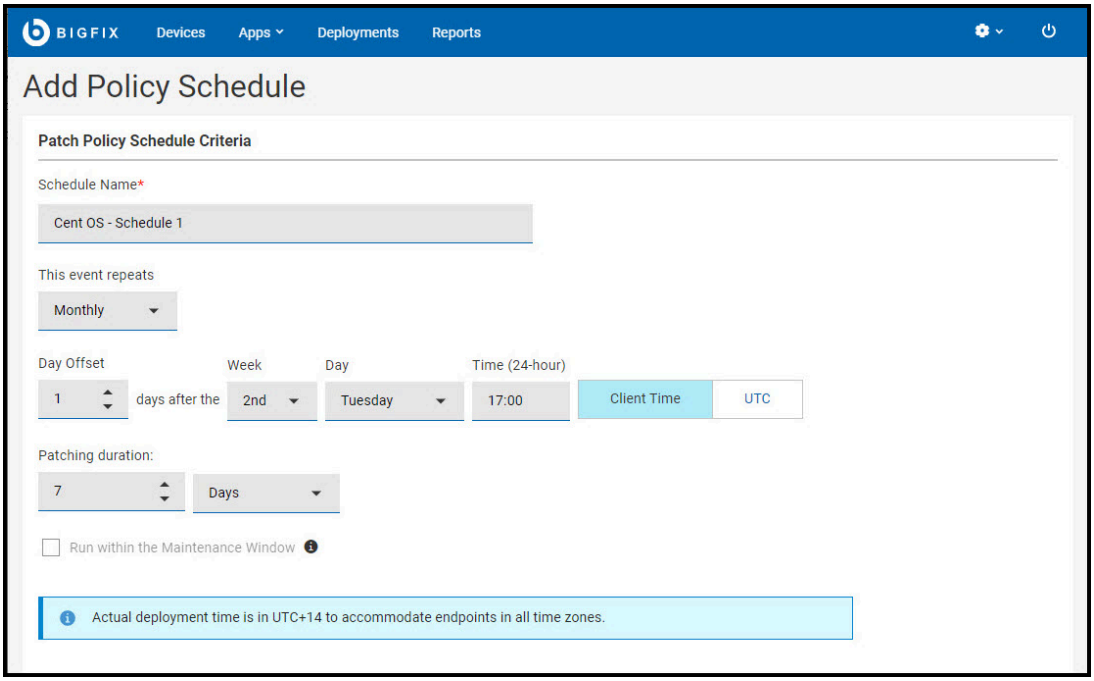
左上のポリシー名の下に**「スケジュール」**タブと**「コンテンツ」**(外部/カスタム) タブが表示されます。ポリシーの要約が右側に表示されます。確定したポリシー・スケジュールは、左側に表示されます。**「ポリシーの編集」**コントロールは右下に表示されます。**「追加者」**列には、スケジュールに対象を追加したオペレーターが表示されます。「プロパティー別にターゲット設定する」の場合は、条件を設定していたオペレーターが表示されます。

注: 「ポリシーの削除」アクションを使用して 、ポリシーを削除できます。ポリシーを削除するには**「ポリシーの編集」**をクリックし、「ポリシーの編集」ページで**「ポリシーの削除」**をクリックします。

9. **「スケジュールの追加」**ボタンをクリックして、ポリシーのデプロイメントのタイミング、動作、対象を設定します。1 つのポリシーは、それぞれ固有のデプロイメント・オプションと対象を持った、複数のスケジュールを保有できます。スケジュールのないポリシーは、デプロイされません。
   スケジューリングをすることでパッチの適用が予測でき、エラーを最小限にとどめるのに役立ちます。さらに、コンプライアンス監査時に、作業環境が会社のセキュリティー・ポリシーを確実に満たしているようにします。一部のベンダーは定期的なパッチ・リリース・スケジュールに従っており、このスケジュールに合わせてポリシー・スケジュールを調整できます。本番環境にデプロイする前にテスト環境にポリシーをロール・アウトすることをおすすめします。テスト、QA、実稼働の各ステージには、それぞれ独自のタイミングと所要時間を指定して別個のパッチ・ロールアウトを定義することを検討してください。

   注: NMO がスケジュールの追加、編集、削除を実行するには「スケジュールの作成/編集」および「スケジュールの削除」の権限が必要です。権限の詳細については、WebUI 権限サービス ((ページ)　　)を参照してください。NMO がスケジュールの追加、編集、削除を実行するには、ポリシーを保存するサイトへの書き込みアクセス権も必要です。

a. スケジュール名を入力して、デプロイメント間隔を設定します。



i. これは繰り返しイベントです (毎日、毎週、毎月) の (曜日または各月の第何日)。
ii. 経過日数: オプションの「経過日数」コントロールを使用して、火曜日パッチのような月次イベントに対するパッチ適用をスケジュールします。月の第 2 火曜日は第 2 週にあることが多いですが、いつもそうとは限りません。(例えば、2018 年の 8 月の火曜日パッチは 14 日でした。)「経過日数」オプションを使用して、日付が月によって異なるイベントのパッチ適用を調整します。
iii. 時刻 (開始時刻)
iv. タイムゾーン: プロセスを開始するときは、各エンドポイントが存在する場所の夜間メンテナンス期間にパッチの適用を開始するなど、各地のタイム・ゾーンに合わせたクライアント時刻を使用します。すべてのタイム・ゾーンのすべてのエンドポイントで同時に動作させる場合は、UTC 時刻を使用します。

- クライアント時刻 - 各エンドポイントのローカル時刻。BigFix agent がインストールされたデバイスの時刻です。
- 協定世界時 - 協定世界時 (UTC) は、時計と時刻を世界共通に調整するときに使用する世界標準時刻です。

注: 「クライアント時刻」を指定すると、ポリシーの開始時刻は UTC+14 タイム・ゾーンで指定された時刻に開始されます。詳細。「デプロイメント時刻 (（ページ） *86)*」を参照してください。

v. パッチ所要時間 (分、時間、または日数。最大 30 日間)。ポリシーに沿って応答のない対象デバイスに対しパッチのインストールを試みる時間の長さ。

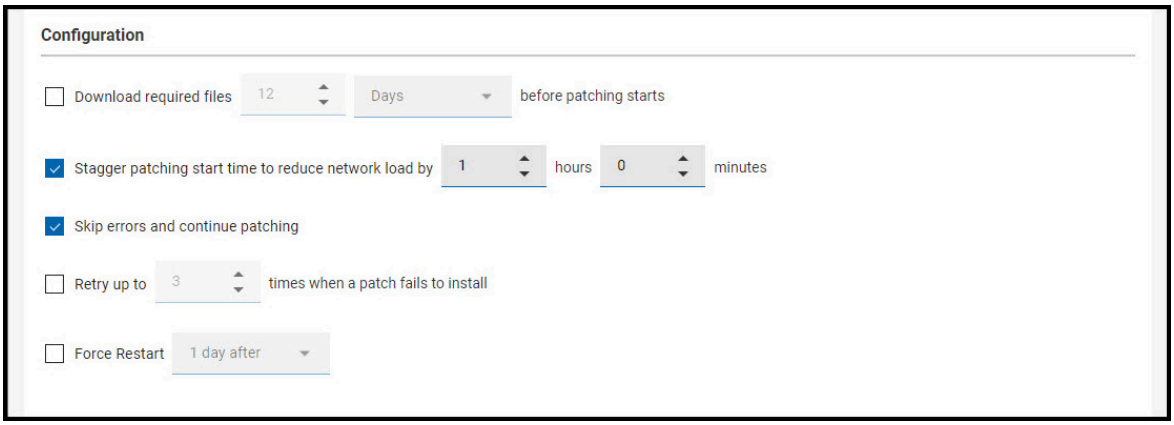
vi. 実行期間: メンテナンス・ウィンドウ - このオプションを使うと、保守作業中にパッチ・ポリシーを実行できます。メンテナンス・ウィンドウ・ダッシュボードを使って、BigFix で実行される保守作業をスケジュールできます。

注: この機能を使用するには、メンテナンス・ウィンドウのグローバル・プロパティーが存在している必要があります。

メンテナンス・ウィンドウのグローバル・プロパティーを作成するには、次の手順に従います。

1. BigFix console から、**「ツール」 > 「管理プロパティー」**に移動します。
2. BES サポート・サイトの**「メンテナンス・ウィンドウ」**プロパティーを選択し、**「カスタム・コピーの作成」**をクリックして、**「OK」**をクリックします。

10. デプロイメントとデプロイメント後の動作を設定します。



- 事前キャッシュ: パッチ適用の開始前に、必要なファイルをダウンロードするには、最大 5 日間の範囲で分数、時間数、または日数を指定します。
- ネットワーク負荷を減らすなどの目的で、パッチ適用の開始時刻をずらします。分数または時間数を設定します (無制限)。
- パッチ・エラーをバイパスしパッチ適用を続行します。パッチ・ポリシーは複数のアクション・グループ (MAG) となります。MAG は順番に実行され、最初にアクションに失敗した時点で停止します。失敗を無視して次のアクションに進めるには、「パッチ・エラーのバイパス」オプションを使用します。MAG のオプションが先行するアクションに依存しない場合は、このオプションを使用します。ポリシーと複数のアクション・グループ (MAG) のプロセスについて詳しくは、『デプロイ済みポリシーのモニタリング (（ページ） 91)』を参照してください。
- 最大 *n* 回再試行 (回数無制限)。ハードドライブのスペース不足などが原因でデバイスにパッチをインストールできない場合は、再試行の値と次の再試行までの待機期間を設定します。
    - 試行間隔 *n* (分数、時間数。最大 30 日間) でインストールを試行します。
    - インストールするには、デバイスのリブートが完了するまでお待ちください。

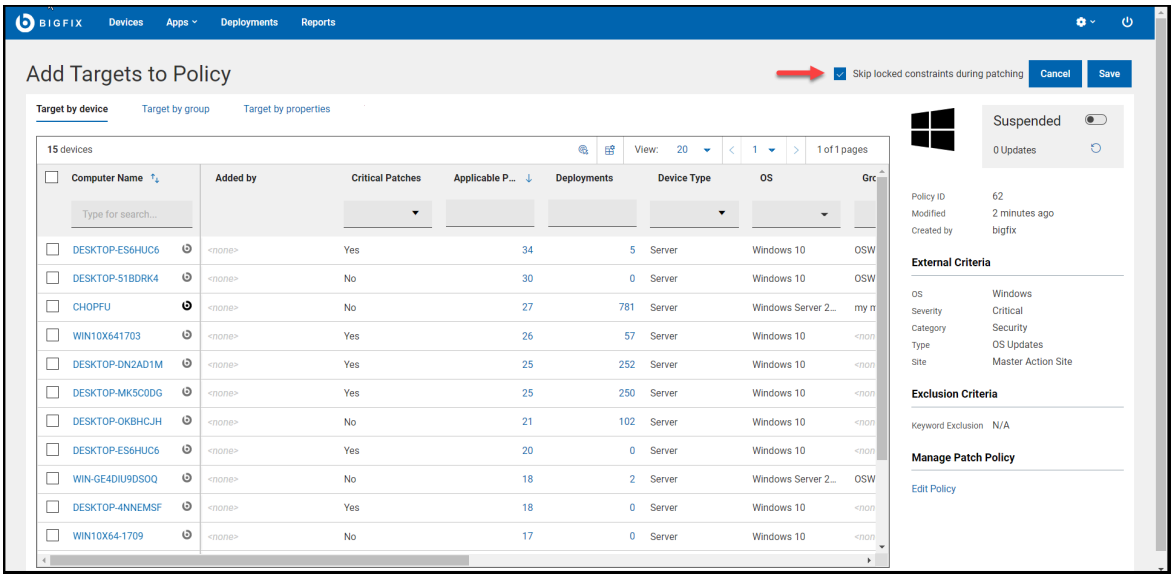
注: 複数の MAGS をパッチ前アクションおよびパッチ後アクションと組み合わせて使用すると、再試行が機能しないことがあります。

- 強制的に再起動 - 完了時に再起動を強制します。再起動が必要になると、デバイス所有者に通知し、デバイス所有者にとって都合の良い時間に再起動するオプションを提供します(1 日、7 日、15 日)。デフォルトのメッセージを使用するか、独自のメッセージを入力します。

11. スケジュールを提案として送信するには、**提案**機能を使用します。提案機能を使うと、オペレーターは、必要に応じてスケジュールを受け入れることができるようになります。

a. **「これを提案として送信」**にチェックを入れます。
b. 必要に応じて**「提案があることをユーザーに通知」**にチェックを入れます。
c. **「提案の説明」**を入力します。

12. **「保存」**をクリックすると、スケジュールが保存され、ポリシー文書に戻ります。
13. 新規スケジュールは、リスト一番上に表示されます。**「ターゲットの追加」**をクリックします。

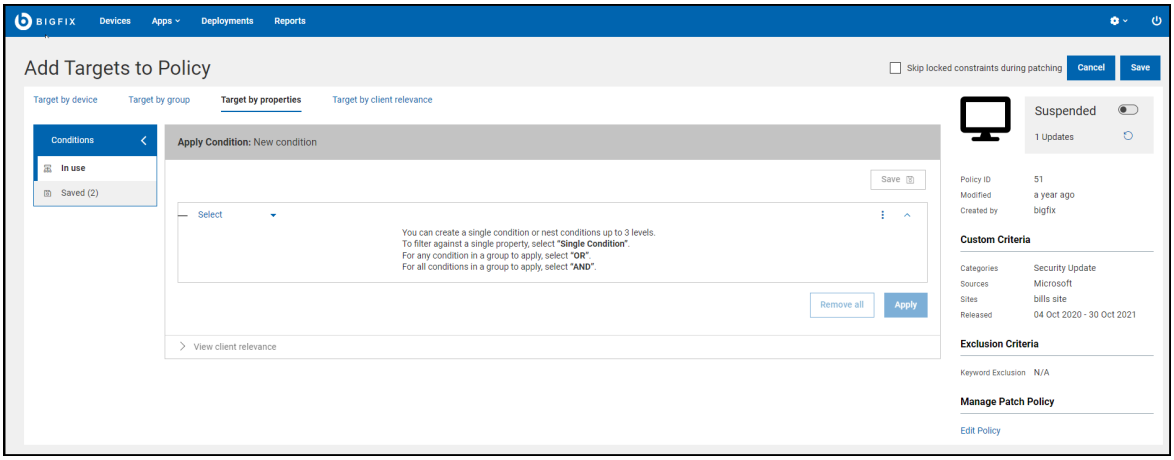


パッチ適用中ロック状態になる制約をスキップ: この機能を使用して、デバイスのロックを解除することなく、ロックされたデバイスにパッチをデプロイします。このオプションは、コンソール・ロックまたはロック解除の権限を持つオペレーターのみが使用でき、そのオペレーターによって追加されたターゲットにのみ適用されます。ロック権限の詳細については、「**ロック可能** - ローカル・オペレーターの追加」を参照してください。

注: NMO が自分で作成した対象を追加または削除するには「独自の対象の追加/削除」の権限が必要です。NMO が他のオペレーターが作成した対象を削除するには「他のオペレーターの対象の削除」の権限が必要です。NMO は許可された数のデバイスのみを対象とすることができ、制限を超えることはできません。違反した場合、WebUI アプリケーションはエラー・メッセージを表示し、NMO はそれ以上進めません。権限の詳細については、WebUI 権限サービス ((ページ))を参照してください。NMO が対象を追加/削除するには、ポリシーを保存するサイトへの読者権限が必要です。

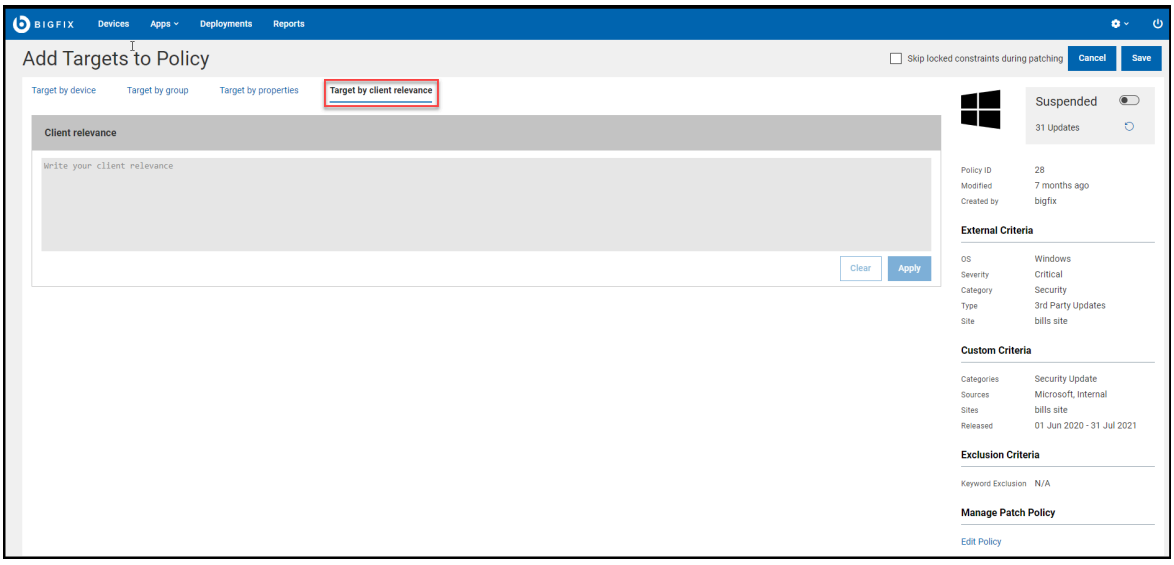
14. **「デバイス別にターゲット設定する」**タブまたは**「グループ別にターゲット設定する」**タブで、デバイスまたはコンピューター・グループを選択します。または**「プロパティー別にターゲット設定する 」**を使用してプロパティー条件のセットを定義できます。それらの条件に一致するデバイスにポリシーが発行されます。単一のスケジュールに複数のターゲット設定方法を混在させることはできません。対象のないスケジュールはデプロイされません。デバイスをチェックして選択または選択解除しま

す。**「適用可能なパッチ」**と**「デプロイメント」**列の数値は、そのデバイスに関連付けられたパッチとデプロイメント情報の数です。パッチ・ポリシー・アプリケーションに戻るには、ご使用のブラウザーの**「戻る」**ボタンを使用します。



「プロパティー別にターゲット設定する」では、対象とするエンドポイントの必要条件を定義できます。**「プロパティー別にターゲット設定する」** は、スケジュールごとに１人のオペレーターに制限されます。そのスケジュールでは、ポリシーが発行されるのはそのオペレーターが所有するエンドポイントだけです。

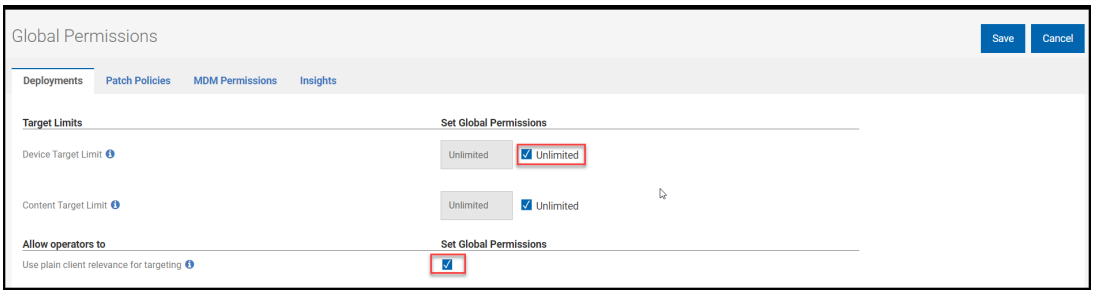
「クライアントの関連度別にターゲット設定する 」では、ポリシーのターゲットを決定するカスタム関連度を作成できます。例えば、特定のファイルのバージョンを確認できます。ポリシー・アクションは動的にターゲット設定されます。複数のターゲット設定方法を同時に選択することはできません。**「クライアントの関連度別にターゲット設定する」**は、スケジュールごとに１人のオペレーターに制限されます。そのスケジュールでは、ポリシーが発行されるのはそのオペレーターが所有するエンドポイントだけです。



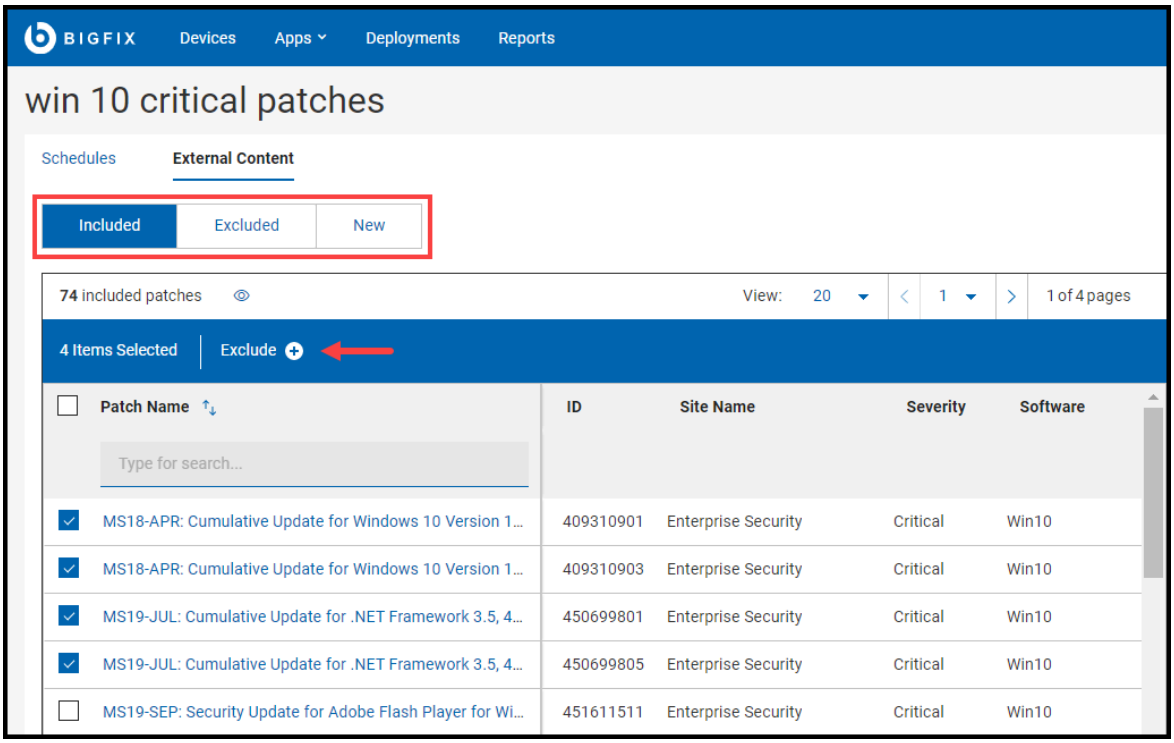
NMO が、特定のスケジュールに**「プロパティー別にターゲット設定する」**または**「クライアントの関連度別にターゲット設定する」**を設定した場合、以下のオペレーターのみがターゲット設定方法を編集したり**「デバイス別にターゲット設定する」**または**「グループ別にターゲット設定する」**に変更したりできます。

- **「プロパティー別にターゲット設定する」**または**「クライアントの関連度別にターゲット設定する」**を設定していた元の NMO
- マスター・オペレーター (MO)。

注: 「プロパティー別にターゲット設定する」または**「クライアントの関連度別にターゲット設定する」**タブは、「デバイスの対象の上限」権限が**「無制限」**に設定されている NMO にのみ表示されます。**「クライアントの関連度別にターゲット設定する」**タブを表示するには、NMO は**「ターゲット設定に標準のクライアント関連度を使用します」**をクリックする必要があります。権限の詳細については、WebUI 権限サービス ((ページ))を参照してください。



15. **「保存」**をクリックすると、対象が保存され、パッチ・ポリシー文書に戻ります。
16. **「コンテンツ」** (外部/カスタム) タブをクリックすると、新規パッチをポリシーに含めたり追加したりできるほか、ポリシーから新規パッチを除外できます。



    a. 除外するパッチを選択します。
    b. **「除外」**をクリックします。
17. 準備ができたら、**「アクティブ化」**トグル・ボタンをクリックしてポリシーをアクティブに切り替え、パッチの適用を開始します。ポリシーをアクティブ化すると、ポリシーのスケジュールもそれぞれアクティブ化されます。パッチのデプロイメント

を停止するには、随時アクティブなポリシーを中断します。ポリシーを更新するには、**「ポリシーの更新」**アイコンをクリックします。
ポリシー・ベースのパッチ適用動作をモニターするには、WebUI の「デプロイメント」ビュー (（ページ） *209)*を使用します。

注:

ポリシー・スケジュールで 「クライアント時刻」を指定した場合、ポリシーをアクティブ化すると、ポリシーの開始時刻は UTC+14 タイム・ゾーンで指定されたクライアント時刻になります。これは、すべてのタイム・ゾーンのクライアントが、指定された時刻にポリシーを受信できるようにするためです。

WebUI では、ポリシーがアクティブ化されると、ブラウザー時刻に開始時刻が表示されます。

- クライアント時刻 = ポリシーを受信するエンドポイントの時刻。
- ブラウザー時刻 = ブラウザーが存在するマシン上の時刻。

以下の計算で、UTC+14 時刻からブラウザーの時刻に変換できます。

- (ブラウザー時刻での) Start_time = <specified_client_time> - 14 時間 + <utc_hour_offset_for_browser_timezone> 時間

例

各エンドポイントのタイムゾーンで午前 5 時にポリシーを実行したいため、クライアント時刻に午前 5 時を指定しました (PST 午前 5 時、EST 午前 5 時、IST 午前 5 時など)。つまり、ポリシー・アクションは UTC+14 タイム・ゾーンで午前 5 時に発行されますが、クライアントのローカル時間で午前 5 時になるまで、クライアント・エンドポイントでポリシーは実行されません。

ブラウザーが太平洋夏時間 (PDT) にあるとします。PDT は UTC-7 であるため、UTC オフセットは -7 です。

開始時間 (PDT) = 午前 5 時～14 時間 + (-7 時間) = 午前 5 時～21 時間 = 午前 8 時 (PDT)。

ブラウザーがインド標準時 (IST) にあるとします。IST は UTC+5:30 なので、UTC オフセットは +5:30 です。

IST の開始時刻 = 午前 5 時 ～ 14 時間 + (5 時間 30 分) = 午前 5 時 ～ 8 時間 30 分 = 20 時 30 分 (IST) または午後 8 時 30 分 (IST)。

注: 事前キャッシュが選択されている場合、ポリシーの発行時間は、事前キャッシュ・セクションで指定された時間によってオフセットされます。

例えば、パッチ適用開始の 1 時間前に事前キャッシュを設定した場合、アクションは午後 8 時 30 分 (IST) ではなく午後 7 時 30 分 (IST) に発行されます。

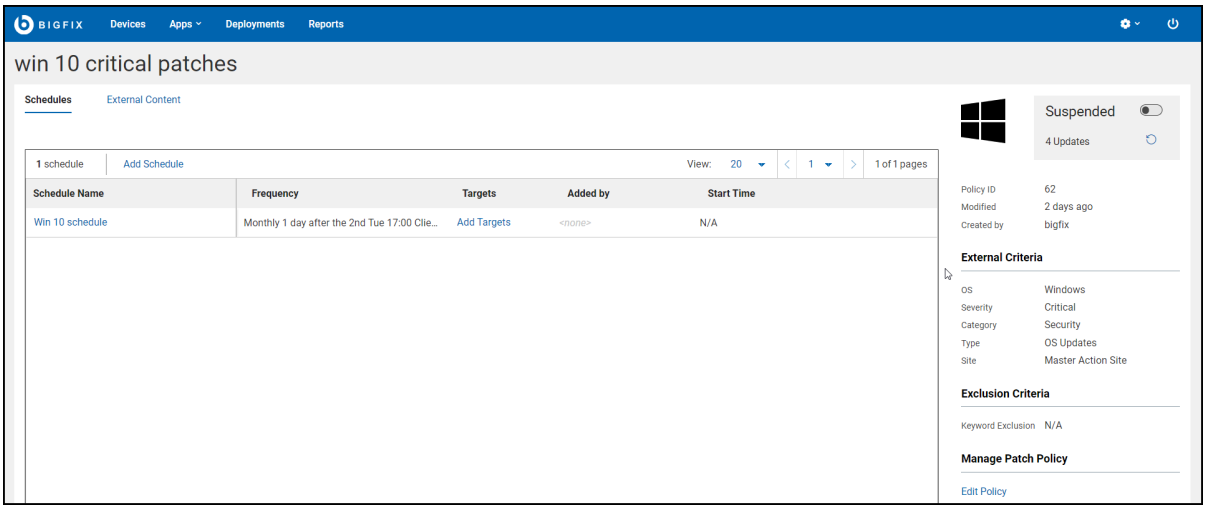
パッチ・ポリシー文書

ポリシー設定を確認、管理するには、パッチ・ポリシー文書を使用します。ポリシー情報はページの右側に表示されます。

- ステータス - アクティブまたは中断状態。
- 更新 - 使用できるパッチ更新の数。
- ポリシー ID - このポリシーの一意の ID。
- OS、重要度、カテゴリー、タイプ - 組み込み基準。
- サイト - ポリシーが保存されるサイトの名前。
- 次の更新 (アクティブなポリシー) - 次の自動最新表示時刻 (有効な場合)。
- 変更日 - 前回ポリシーが変更された時間。
- ソース: オペレーター名。
- 更新済み - 最後にポリシーが更新された日付。
- キーワードの除外 - タイトルにキーワードが含まれるコンテンツは除外される。

「スケジュール」タブ

「スケジュール」タブでは、ポリシー・スケジュールのリストが作成順に表示されます。「要約」ページに表示するスケジュール名をクリックします。



- 名前 - スケジュール名
- 頻度 - デプロイメントの間隔。
- 対象 - 対象デバイスとコンピューター・グループの数。リンクをクリックすると、対象のリストが表示されます。スケジュールに対象がない場合、**「対象の追加」**コントロールが表示されます。リンクをクリックして追加してください。
- 追加者 - この列には、スケジュールに対象を追加していたオペレーターが表示されます。「プロパティーに応じて対象を指定」の場合は、条件を設定していたオペレーターが表示されます。
- 次回のデプロイメント - スケジュールの複数のアクション・グループが BigFix のルート・サーバーに発行される時刻。ポリシーが各地で確実に正しい時刻に実行されるように、後ですべてのタイム・ゾーンのエンドポイントに対応できるよう調整されます。

右側のパネルの切り替えスイッチを使用して、ポリシーを **アクティブ化/中断**します 。アクティブなポリシーを更新または編集することはできません。「スケジュール」タブのコントロールのいくつかは、ポリシーが中断されるまでは非アクティブです。

「スケジュール」タブのコントロール:

- **スケジュールの追加**
- **アクティブ化/中断**
- **ポリシーの更新**

- **ポリシーの編集**
- **Delete (削除)**

注: マスター以外のオペレーター (NMO) がポリシーをアクティブ化または中断するには「ポリシーのアクティブ化/中断」の権限が必要で、ポリシーを更新するには「ポリシーの更新」の権限が必要です。権限の詳細については、WebUI 権限サービス (（ページ）　　)を参照してください。NMO がポリシーをアクティブ化/中断または更新するには、ポリシーを保存するサイトへの書き込みアクセス権も必要です。

「スケジュールの要約」ページ

スケジュールをどれか 1 つクリックすると、スケジュールの要約とコントロールが表示されます。スケジュールを変更するには、スケジュールのポリシーを中断する必要があります。対象を追加または削除する場合、ポリシーの中断は不要です。

- 事前キャッシュのダウンロード - ポリシー・パッチが事前キャッシュされた時刻
- 間隔を置いて開始 - ネットワーク負荷を減らすためにパッチ適用時間をずらす時間の長さ
- エラーをバイパス - 複数のアクション・グループ (MAG) の失敗を無視し、次のアクションに進むパッチ・ポリシーと MAG のプロセスについて詳しくは、『デプロイ済みポリシーのモニタリング (（ページ） *91)*』を参照してください。
- 失敗時に再試行 - パッチのインストールが失敗したとき再試行する回数と再試行の間隔
- 強制的に再起動 - 完了時の強制再起動と、強制再起動までの待機時間

「スケジュールの要約」のコントロール:

- **ターゲットの追加/編集**
- **スケジュールの編集**
- **Delete (削除)**

コンテンツ (カスタム/外部) タブ

選択したポリシーのパッチが表示されます。監査用パッチ、問題のあるパッチ、パッチ・ポリシーにデフォルト・アクションが組み込まれていないパッチ。置き換えられたパッチにはフラグが付与されますが、デプロイはされません。これらのパッチは、ポリシーが更新されるとパッチ・リストから削除されます。

ポリシーからパッチを個別に除外するには、タイトルの左にある**「除外」**チェック・ボックスを選択します。コンピューター・グループ (マニュアル・グループまたは動的グループ) を使用して対象に設定されているデバイスは、個別には除外できません。

フィルター:

- 含む - 組み込まれているパッチが表示されます。
- 除外 - 動的除外と手動の除外を含め、除外されたパッチが表示されます。
- 新規 - ポリシーが更新されるとポリシーに追加されるパッチが表示されます。
- 適用可能なパッチ - ログイン・ユーザーが操作権限を持つデバイスに関連付けられたパッチのリスト。例えば、NMO には、Windows マシンへのパッチ適用は認められていますが、Linux マシンへのパッチ適用は認められていません。Windows と Linux の両方のパッチを含むポリシーを閲覧するとき:
  - 「適用可能なパッチ」チェック・ボックスが選択されているとき、NMO には Windows のパッチのみが表示されます。
  - 「適用可能なパッチ」チェック・ボックスが選択されていないとき、NMO には Windows と Linux の両方のパッチが表示されます。
  - 無制限の権限を持つマスター・オペレーター (MO) には、**「適用可能なパッチ」**フィルターが選択されているかどうかに関係なく同じパッチが表示されます。

コンテンツ (カスタム/外部) タブのコントロール:

- **アクティブ化/中断**
- **ポリシーの更新**
- **ポリシーの編集**
- **Delete (削除)**

注: ポリシー文書のボタンは、それぞれの権限が NMO に付与されている場合にのみ表示されます。

デプロイ済みポリシーのモニタリング

ポリシー・ベースのパッチ適用動作をモニターするには、WebUI の「デプロイメント」(（ページ） 209)ビューを使用します。

複数のアクション・グループを操作する

ポリシーとは、複数の Fixlet とスケジュールを 1 つのパッケージにまとめたものです。スケジュールの示す時刻に、ポリシー基準を満たすパッチがすべて収集され、BigFix 複数のアクション・グループ (MAG) が作成されます。特定のデバイスに関連するパッチがない場合、個別アクションは一切実行されません。

単一ポリシーに数百個のパッチが含まれることがあり、その MAG に数百個のコンポーネントが含まれることがあります。パフォーマンスを向上するため、1 つのポリシーに含まれるパッチの数が 200 を超える場合には、いくつかの複数のアクション・グループに分割されます。

複数のアクション・グループ (MAG) のデフォルトの動作:

- ネットワーク負荷を軽減するために、デプロイメントの開始時刻を1 時間以上遅延させます。
- 各試行について 1 時間ごとに 3 回再試行します。
- デフォルト・アクションを使用します。
- 2 日 (48 時間) で期限切れになります。
- 対象を設定する方法は、対象のタイプが a) 静的エンドポイント、b) マニュアル・コンピューター・グループ、c) 自動コンピューター・グループのどれかによって異なります。

注: MAG で「再起動を強制」オプションが選択されている場合、パッチ前アクションとパッチ後アクションが有効になっていない限り、各アクションの後にシステムが再起動します。

パッチ・ポリシー運用: タスクのリファレンス

このページでは、パッチ・ポリシー操作の概要を示します。変更のためにアクティブ・ポリシーを中断した場合、変更後にパッチを再度アクティブ化し、パッチを再開します。

ポリシーの追加 (（ページ） 92)

ポリシーのアクティブ化 (（ページ） 93)

ポリシーの中断 (（ページ） 93)

ポリシーの更新 (（ページ） 93)

ポリシーの編集 (（ページ） 93)

ポリシーへのスケジュールの追加 (（ページ） 94)

ポリシーのスケジュールの編集 (（ページ） 94)

スケジュールへの対象の追加 (（ページ） 94)

スケジュールからの対象の削除 (（ページ） 95)

ポリシーのスケジュールの削除 (（ページ） 95)

ポリシーからの個別パッチの除外 (手動除外) (（ページ） 95)

ポリシーからのパッチ・タイプの除外 (動的除外) (（ページ） 96)

自動最新表示の有効化 (（ページ） 96)

自動最新表示スケジュールの調整 (（ページ） 96)

自動最新表示の無効化 (（ページ） 96)

ポリシーの追加

1. ポリシー・リストで、**「ポリシーの追加」**をクリックします。
2. ポリシー名と説明を入力します。
3. ドロップダウンから「サイト」を選択します。
4. ポリシーの包含条件を選択します。重要度、カテゴリー、OS、コンテンツ・タイプ。
5. 動的除外を追加し、必要に応じて自動更新オプションを設定します。**「保存」**をクリックします。

6. ポリシー文書で、**「スケジュールの追加」**をクリックします。
7. スケジュール名を入力してください。デプロイメントの頻度、動作、提案のオプションを選択します。**「保存」**をクリックします。
8. ポリシー文書で、新規スケジュール用に**「対象の追加」**のリンクをクリックします。
9. **「追加者」**にオペレーターが表示されていることを確認します。
10. **「デバイス別ターゲット」**、**「グループ別にターゲット設定する」**、**「プロパティー別にターゲット設定する」**、**「クライアントの関連度別にターゲット設定する」**のいずれかのタブからパッチ対象を選択します。**「保存」**をクリックします。
11. ポリシー文書で、**「アクティブ化」**の切り替えボタンをクリックします。

ポリシーのアクティブ化

1. ポリシー・リストからポリシー文書を開きます。
2. **「アクティブ化」**の切り替えボタンをクリックします。

ポリシーの中断

1. ポリシー・リストからポリシー文書を開きます。
2. **「中断」**の切り替えボタンをクリックします。

ポリシーの更新

1. ポリシー・リストからポリシー文書を開きます。
2. ポリシーがアクティブ状態の場合は、**「中断」**の切り替えボタンをクリックします。
3. **「今すぐ更新」**アイコンをクリックします。

ポリシーの編集

1. ポリシー・リストからポリシー文書を開きます。
2. ポリシーがアクティブ状態の場合は、**「中断」**の切り替えボタンをクリックします。
3. **「ポリシーの編集」**リンクをクリックします。
4. 必要な変更を行い、**「保存」**をクリックします。

ポリシーの削除

1. ポリシー・リストからポリシー文書を開きます。
2. ポリシーがアクティブ状態の場合は、**「中断」**の切り替えボタンをクリックします。
3. **「ポリシーの編集」**リンクをクリックします。
4. **「削除」**をクリックします。

ポリシーへのスケジュールの追加

1. ポリシー・リストからポリシー文書を開きます。
2. ポリシーがアクティブ状態の場合は、**「中断」**の切り替えボタンをクリックします。
3. **「スケジュールの追加」**をクリックします。
4. スケジュール名を入力し、スケジュールと実行オプションを設定します。**「保存」**をクリックします。
5. スケジュールの**「対象の追加」**リンクをクリックします。
6. **「デバイス別にターゲット設定する」**、**「グループ別にターゲット設定する」**、**「プロパティー別にターゲット設定する」**、**「クライアントの関連度別にターゲット設定する」**のいずれかのタブで、追加するデバイスまたはグループを選択します。**「保存」**をクリックします。

ポリシーのスケジュールの編集

1. ポリシー・リストからポリシー文書を開きます。
2. ポリシーがアクティブ状態の場合は、**「中断」**の切り替えボタンをクリックします。
3. 編集するスケジュールの名前をクリックします。
4. **「スケジュールの編集」**をクリックします。
5. 変更を行い、**「保存」**をクリックします。

スケジュールへの対象の追加

1. ポリシー・リストからポリシー文書を開きます。
2. スケジュールの「対象」リンクをクリックします。

3. **「デバイス別にターゲット設定する」**、**「グループ別にターゲット設定する」**、**「プロパティー別にターゲット設定する」**、**「クライアントの関連度別にターゲット設定する」**のいずれかのタブで、追加するデバイスまたはグループを選択します。**「保存」**をクリックします。

スケジュールからの対象の削除

1. ポリシー・リストからポリシー文書を開きます。
2. スケジュールの「対象」リンクをクリックします。
3. **「デバイス別ターゲット」**、**「グループ別にターゲット設定する」**、**「プロパティー別にターゲット設定する」**、**「クライアントの関連度別にターゲット設定する」**のいずれかのタブで、削除するデバイスまたはグループを選択します。**「保存」**をクリックします。

ポリシーのスケジュールの削除

1. ポリシー・リストからポリシー文書を開きます。
2. ポリシーがアクティブ状態の場合は、**「中断」**の切り替えボタンをクリックします。
3. 対象デバイスまたはグループをすべて削除します。
    a. スケジュールの「対象」リンクをクリックします。
    b. **「デバイス別ターゲット」**、**「グループ別にターゲット設定する」**、**「プロパティー別にターゲット設定する」**、**「クライアントの関連度別にターゲット設定する」**のいずれかのタブで、**「すべて選択解除」**を選択します。**「保存」**をクリックします。
4. 「スケジュール」タブで、**「スケジュール」**をクリックします。
5. **「スケジュールの編集」**をクリックします。
6. **「削除」**をクリックします。

ポリシーからの個別パッチの除外 (手動除外)

1. ポリシー・リストからポリシー文書を開きます。
2. ポリシーがアクティブ状態の場合は、**「中断」**の切り替えボタンをクリックします。
3. **「コンテンツ」**タブをクリックします。

4. 「**含む**」をクリックし、除外するパッチを選択します。
5. **「除外」**ボタンをクリックします。

ポリシーからのパッチ・タイプの除外 (動的除外)

1. ポリシー・リストからポリシー文書を開きます。
2. ポリシーがアクティブ状態の場合は、**「中断」**の切り替えボタンをクリックします。
3. **「ポリシーの編集」**をクリックします。
4. **「除外」**フィールドにキーワードまたはフレーズを入力し、**Enter** キーを押します。これを必要なだけ繰り返します。除外キーワードでは大文字と小文字は区別されません。
5. **「保存」**をクリックします。

自動最新表示の有効化

1. ポリシー・リストからポリシー文書を開きます。
2. ポリシーがアクティブ状態の場合は、**「中断」**の切り替えボタンをクリックします。
3. **「ポリシーの編集」**をクリックします。
4. **「自動最新表示の有効化」**の切り替えボタンをクリックして、更新の時間と頻度を設定します。
5. **「保存」**をクリックします。

自動最新表示スケジュールの調整

1. ポリシー・リストからポリシー文書を開きます。
2. ポリシーがアクティブ状態の場合は、**「中断」**の切り替えボタンをクリックします。
3. **「ポリシーの編集」**をクリックします。
4. 自動最新表示の時間と頻度を調整します。
5. **「保存」**をクリックします。

自動最新表示の無効化

1. ポリシー・リストからポリシー文書を開きます。
2. ポリシーがアクティブ状態の場合は、**「中断」**ボタンをクリックします。

3. **「ポリシーの編集」**をクリックします。
4. **「自動最新表示の無効化」**をクリックします。
5. **「保存」**をクリックします。

第 6 章. IVR 入門

Insights for Vulnerability Remediation (IVR) アプリケーションを使用して、すべての脆弱性のリストを表示し、脆弱性を修復して、カスタマイズされた IVR レポートを作成します。

WebUI IVR を開始する前に、ご使用の環境が以下の前提条件を満たしていることを確認してください。

- IVR スキーマが設定されていること
- IVR スキーマの最小バージョンは 1.4 であること
- IVR データフローが実行され、Insights と相関のあるデータが存在すること
- Insights ETL の実行

CVE ベースの Fixlet 相関

Fixlet と脆弱性を相関付ける場合、相関プロセスでは脆弱性に関連する CVE のみに焦点を当てるため、脆弱性の名前は無視されます。例えば、「CenTos SSL の脆弱性」という名前の脆弱性は、CVE と一致する場合、Windows の Fixlet に関連付けられる可能性があります。

Rapid7 および CSV ファイル・インポート用の置き換えチェーンの追跡:

- パッチ適用サポート・サイトへの登録が必要です
- 置き換えチェーンの追跡は、Windows 英語版パッチ・サイトの Fixlet コンテンツにのみ適用されます
- ある CVE に対して、Fixlet 相関プロセスは CVE と一致する Fixlet を特定し、置き換えチェーンを追跡し、脆弱性を修正する最新の Fixlet を返そうとします

IVR リスト

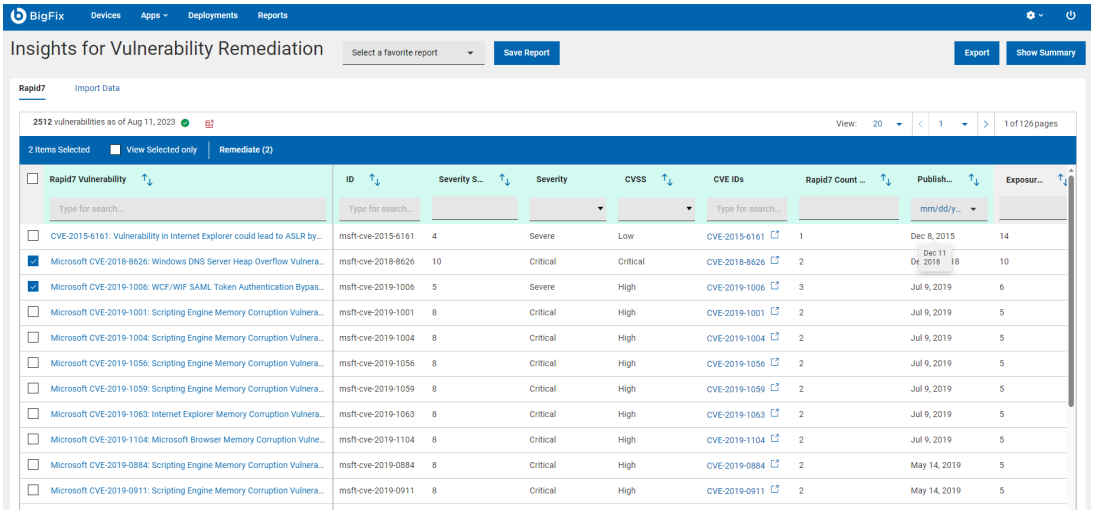
WebUI の BigFix Insights for Vulnerability Remediation (IVR) アプリケーションは、すべての脆弱性の簡単な要約をデータ・グリッド形式で提供します。このアプリケーションを使用して、脆弱性を修復し、カスタム IVR レポートを作成できます。

「IVR」ページにアクセスするには、WebUI メイン・ページで **Apps > IVR** をクリックします。

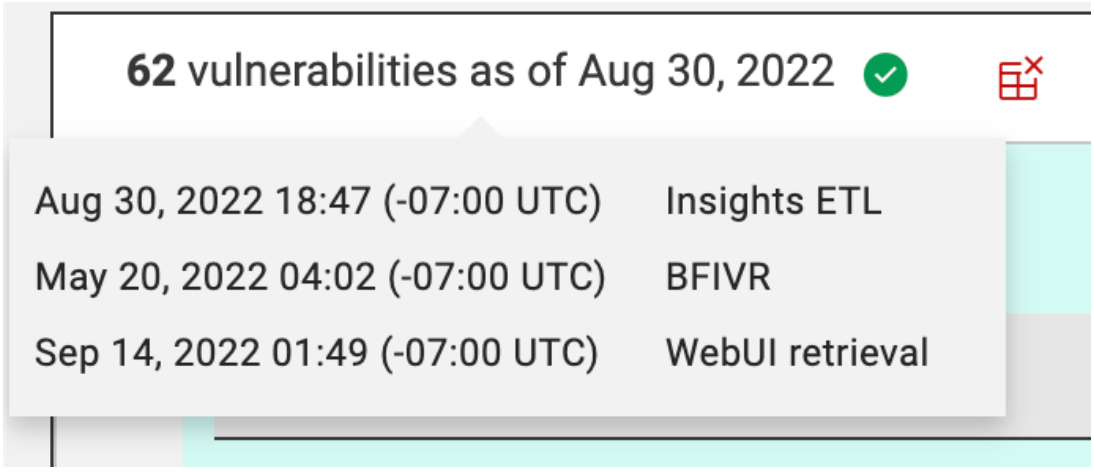
オペレーター権限設定、接続済みデバイス、サイト割り当てによって、リストのコンテンツが制御されます。グリッド表示を使用すると、テーブル内の脆弱性のリストを表示できます。脆弱性名をクリックすると、脆弱性の詳細 (概要、脆弱なデバイス、デプロイメント) に移動します。各列には、検索またはフィルターのオプションがあります。

結果の絞り込みとデータ・グリッド機能のカスタマイズは、デバイス・ページと似ています。詳しくは、「グリッド表示 (（ページ） 6)」を参照してください。

図 1. IVR アプリ - 概要



脆弱性リストの件数にマウス・カーソルを移動すると、最新の **WebUI 取得**時に更新された日時が表示されます。



脆弱性リストの件数の日付は、 **Insights ETL** または **BFIVR** のいずれかの新しいほうの日付を示します。最初に Insights ETL を完了させ、次に IVR ETL を実行して、最新の情報を取得することをお勧めします。

- **Insights ETL** は、**Insights ETL** が正常に完了した最新の日時です。これらは、Insights で設定されるスケジュールによって決まります。Insights ETL をスケジュールする方法について詳しくは、『**リンク**』を参照してください。
- **BFIVR** は、 **IVR ETL** が正常に完了した最新の日時です。これらは、 **IVR** のデプロイメント時に設定されるスケジュールによって決まります。IVR ETL スケジューリングについて詳しくは、『**リンク**』を参照してください。
- **WebUI 取得** は、ブローカーから **IVR** データを取得した最新の日時です。デフォルトでは、WebUI は IVR ブローカーを介して毎日データの取得を試みます。取得の頻度を変更できる IVR 設定を表示するには、『リンク』を参照してください。これは、WebUI が **Insights ETL** および **BFIVR** の日時を最新のメトリックで更新する時でもあります。

IVR アプリには、以下の要素が含まれています。

- **アクション・バー:** データ・グリッドから 1 つ以上の脆弱性を選択すると、アクション・バーが有効になります。
  - **選択済み項目のみを表示:** このチェック・ボックスを選択すると、選択した脆弱性のみが表示されます。
  - **修復:** **「修復」**をクリックすると、**「アクションの実行」ダイアログ**に移動します。このダイアログで脆弱性を修復できます。括弧内の数値は、選択された脆弱性の数を示します。詳しくは、「アクションの実行: デプロイ・シーケンス (（ページ） *184)*」を参照してください。
- **フィルター**

注: IVR グリッド・ビューのフィルターは、緑色と灰色で表示されます。緑色は、Qualys/Tenable/Rapid 7 からの情報であることを示しています。灰色

は、BigFix Enterprise (BFE) データベースからの情報であることを示しています。

ヘッダーにあるフィルターを使用して、結果を絞り込むことができます。

- **VPR スコア**: 脆弱性優先順位の評価スコア。
- **VPR**: 脆弱性優先順位の評価。
- **重大度**: 脆弱性の重大度。
- **CVSS**: 共通脆弱性評価システム。
- **CVE IDs**: CVE ID フィルターを使用して、共通脆弱性と暴露で脆弱性を検索します。
- **公開済み (Published)**: 公開日。
- **スキャナー・カウント**: Tenable/Qualys/Rapid 7 カウント - Tenable/Qualys/Rapid 7 が相関 BigFix コンテンツで識別した脆弱なデバイスの数を示します。

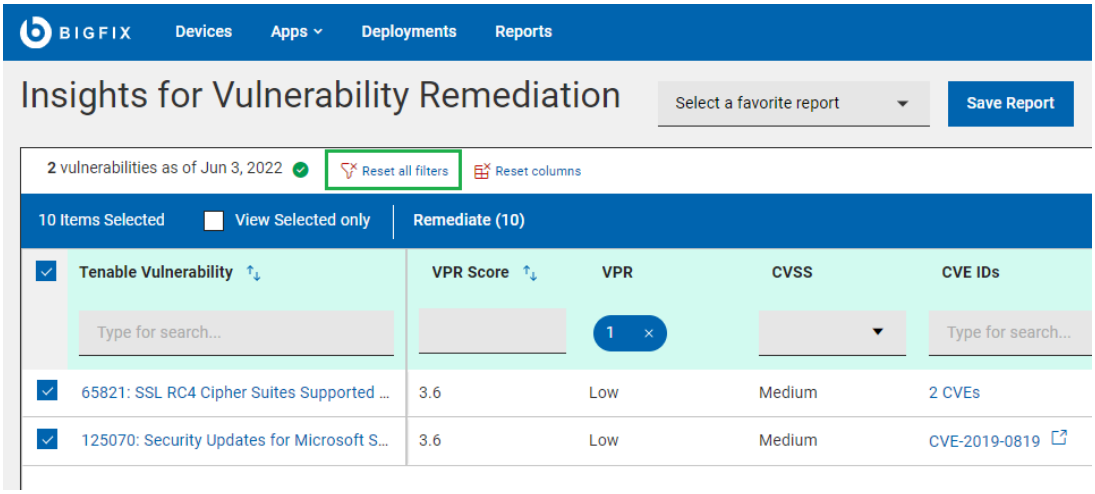
  注: 2つの条件下で、グリッドは脆弱性を示すことがあります。
  - スキャナー・カウントは、 0 より大きい必要があります。
  - オペレーターには、その脆弱性に関連付けられている Fixlet の少なくとも 1 つを表示する権限が必要です。

- **暴露数**: 関連付けられた BigFix コンテンツに適用可能なデバイスの合計。

  注: 暴露数は、一意の数ではありません。これは、Fixlet ごとに適用可能なすべてのデバイスの合計です。

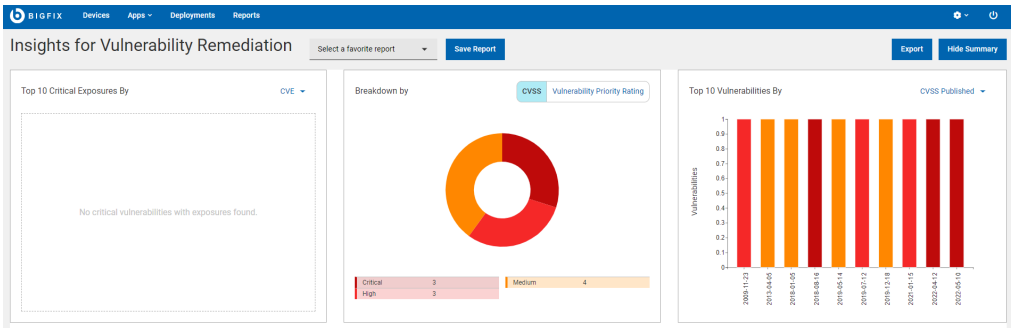
- **製品 / ファミリー**

すべての選択済みフィルターをクリアするには、**「すべてのフィルターのリセット」**をクリックします。



- **レポートの保存**
  - レポートを参照のために保存し、必要に応じて編集、更新、または削除します。詳しくは、「レポート (*(ページ) 16)*」を参照してください。
- **要約の表示:**
  1. **「IVR」**ページで、必要なフィルターを選択します。
  2. **「要約を表示」** をクリックします。フィルターされたすべての脆弱性の要約をグラフやテーブルとして表示できます。グラフの上にカーソルを移動すると、データ・ポイントとパーセンテージの詳細が表示されます。文字が切り詰められたラベルにカーソルを合わせると、ツール・ヒントにすべてのテキストが表示されます。フィルターを変更するか、検索テキストを入力すると、該当する情報がレポートに動的に表示されます。

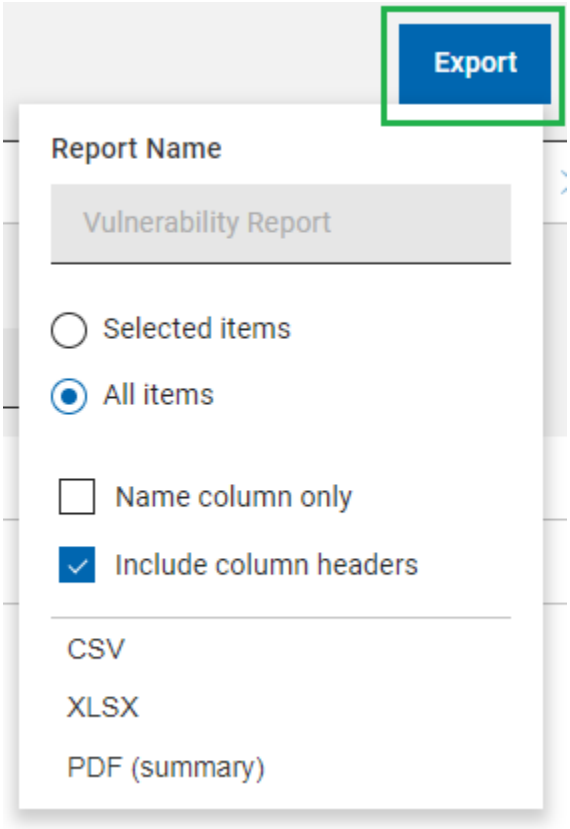
- **CVE/脆弱性 ID 別のきわめて重要な暴露の上位 10 個**
- **CVSS/脆弱性優先順位の評価別の分類**
- **CVSS 公開日/脆弱性優先順位の評価公開日別の脆弱性の上位 10 個**



- **エクスポート:**

  フィルターされたレポートは `.csv`、`.xlsx`、または `.pdf` の形式でエクスポートできます。

  1. **「IVR」**ページで、必要なフィルターを選択します。
  2. **「エクスポート」**をクリックします。



3. **「選択された項目」**オプションを使用すると、フィルターされた結果から項目を選択してエクスポートできます。**「すべての項目」**をクリックすると、フィルター処理されたリストからすべての項目をエクスポートできます。
4. フィルターされた項目の名前のみをエクスポートするには、**「名前列のみ」**をクリックします。
5. 項目のすべてのデフォルト列の詳細をエクスポートするには、「**列ヘッダーを含める**」をクリックします。

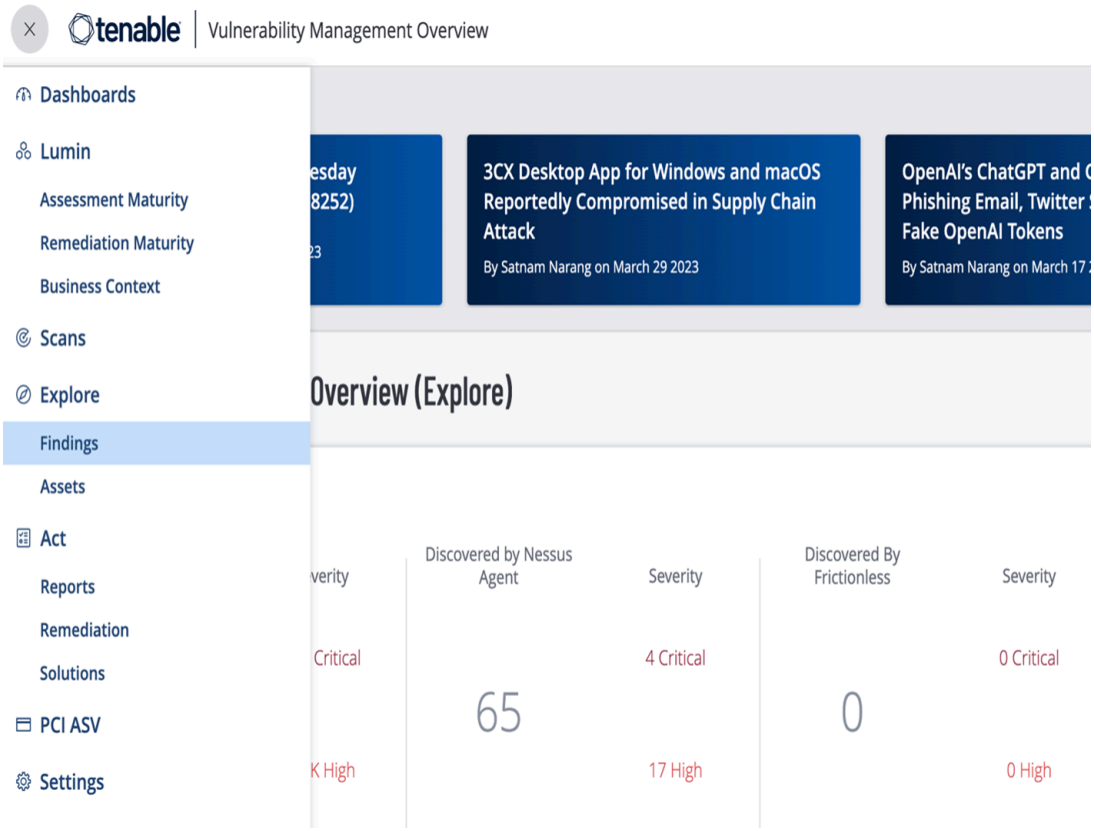
   注: デフォルトの列以外の列を表示している場合は、名前列のみをエクスポートできます。

6. エクスポートするデータのファイル形式 (CSV、XLSX、または PDF) を選択します。
   - デフォルトでは、レポートは次のデフォルトのファイル名を持つ `Downloads` フォルダーに保存されます。`Device_Report_mm_dd_yyyy_username`。ブラウザーでダウンロード設定を変更すると、ファイル名やダウンロードの保存先を変更できます。レポートを保存して後で参照することや、利害関係者と共有することができます。
   - PDF 形式を選択した場合、`.zip` ファイルがダウンロードされます。このファイルには、数値データを含む `.csv` ファイルと、データの表示形式を含む `.pdf` ファイルが含まれています。
   - エクスポートされた IVR レポートには、フィルターと検索条件を適用した後に表示される脆弱性の主な詳細が含まれます。これらの詳細には、脆弱性名、脆弱なデバイス、重大度、CVE ID、およびすべての脆弱性を展開したときに画面に表示される他のすべての詳細情報が含まれます。

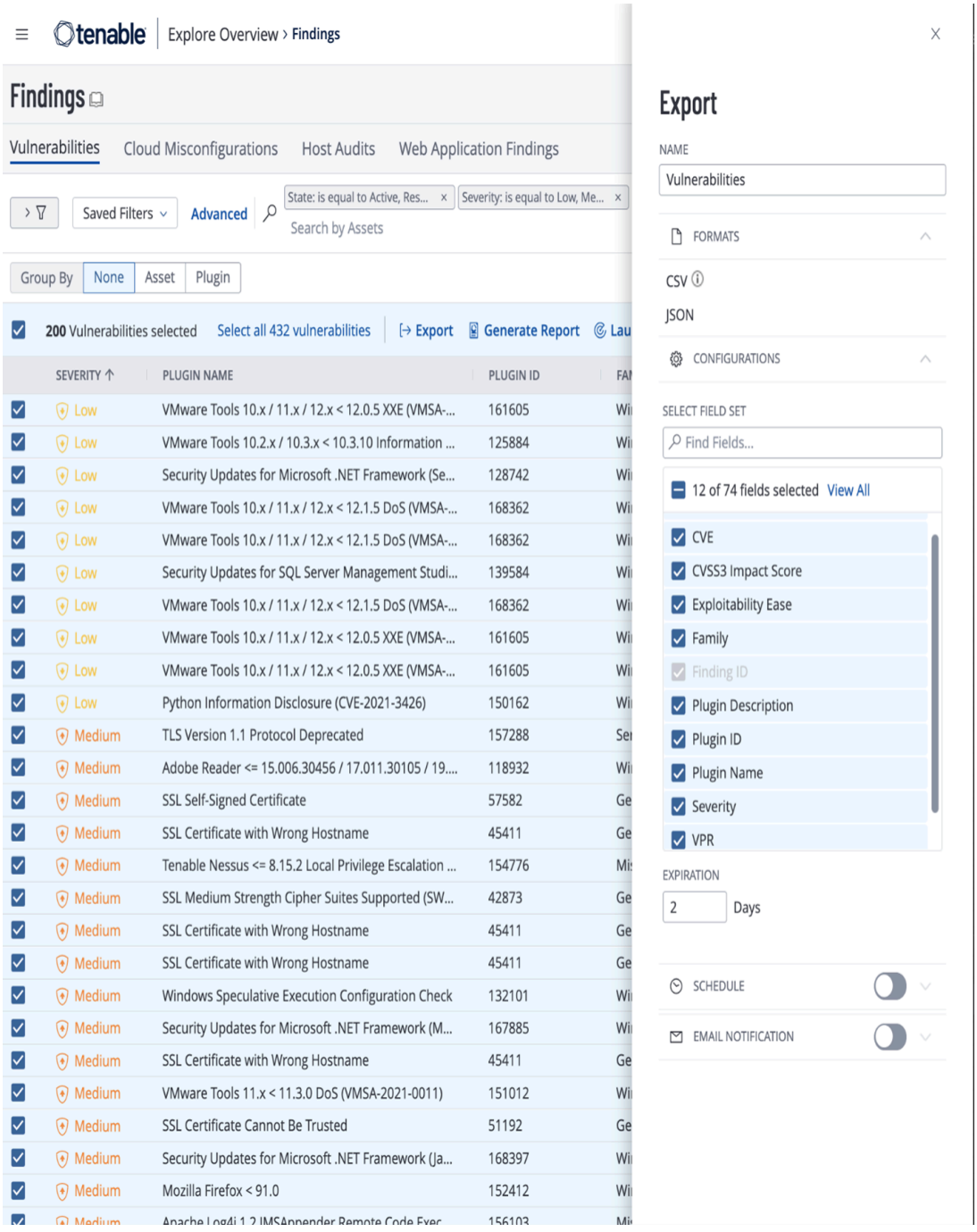
- **IVR インポート用の CSV ファイルのエクスポート**

  Tenable:

1. サイドバーを開き、Explore ヘッダーの下にある「検出結果」をクリックします。



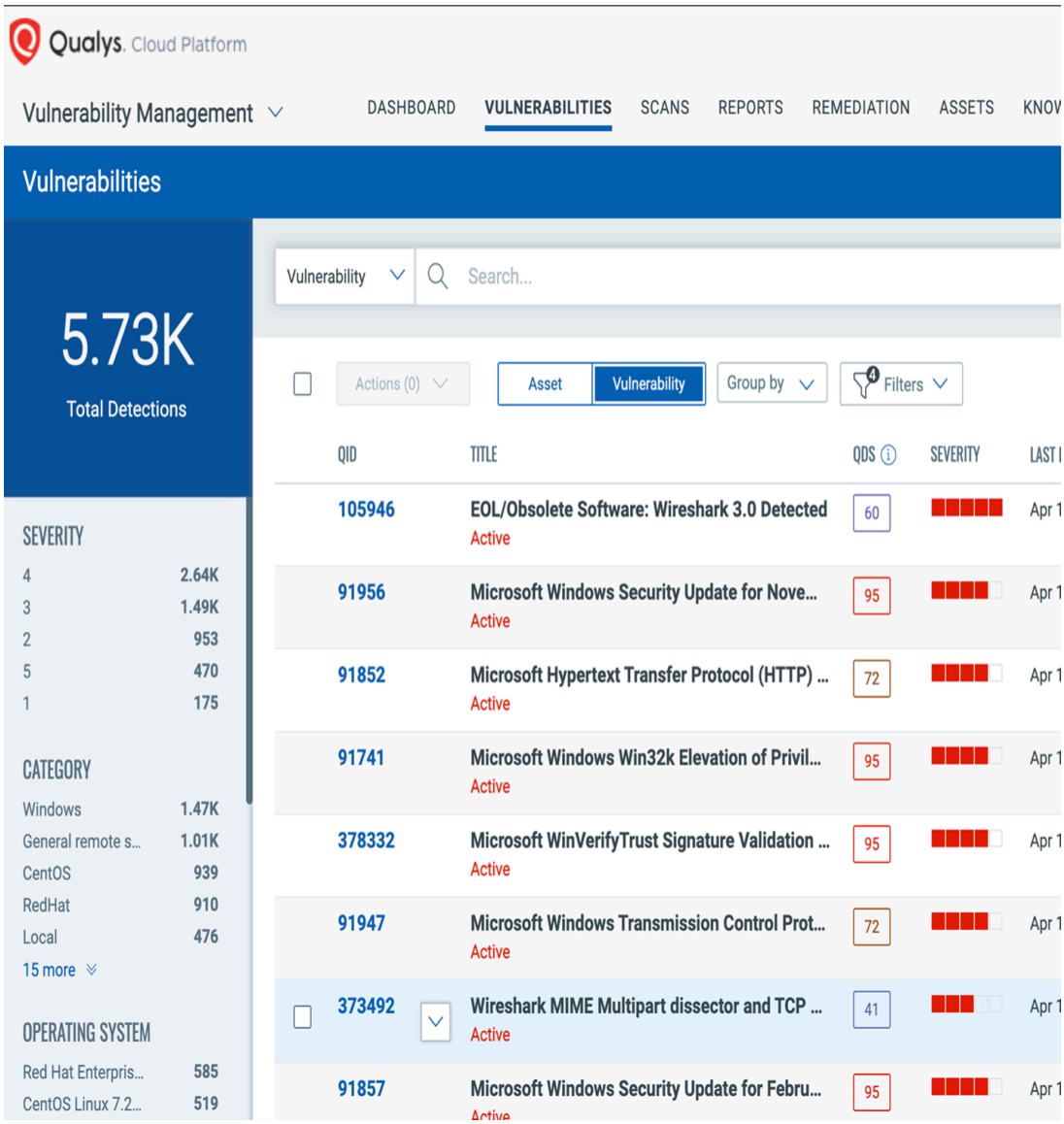
2. 必要なフィルターをテーブルに適用します。**「グループ化」**オプションが**「なし」**に設定されていることを確認します。準備ができたら、**「エクスポート」**をクリックします。



3. **「構成」**で、以下のフィールドを選択します。資産 ID、CVSS3 影響評価、悪用可能性軽減、ファミリー、プラグインの説明、プラグイン ID、プラグイン名、重大度、VPR、公開された脆弱性。

Qualys:

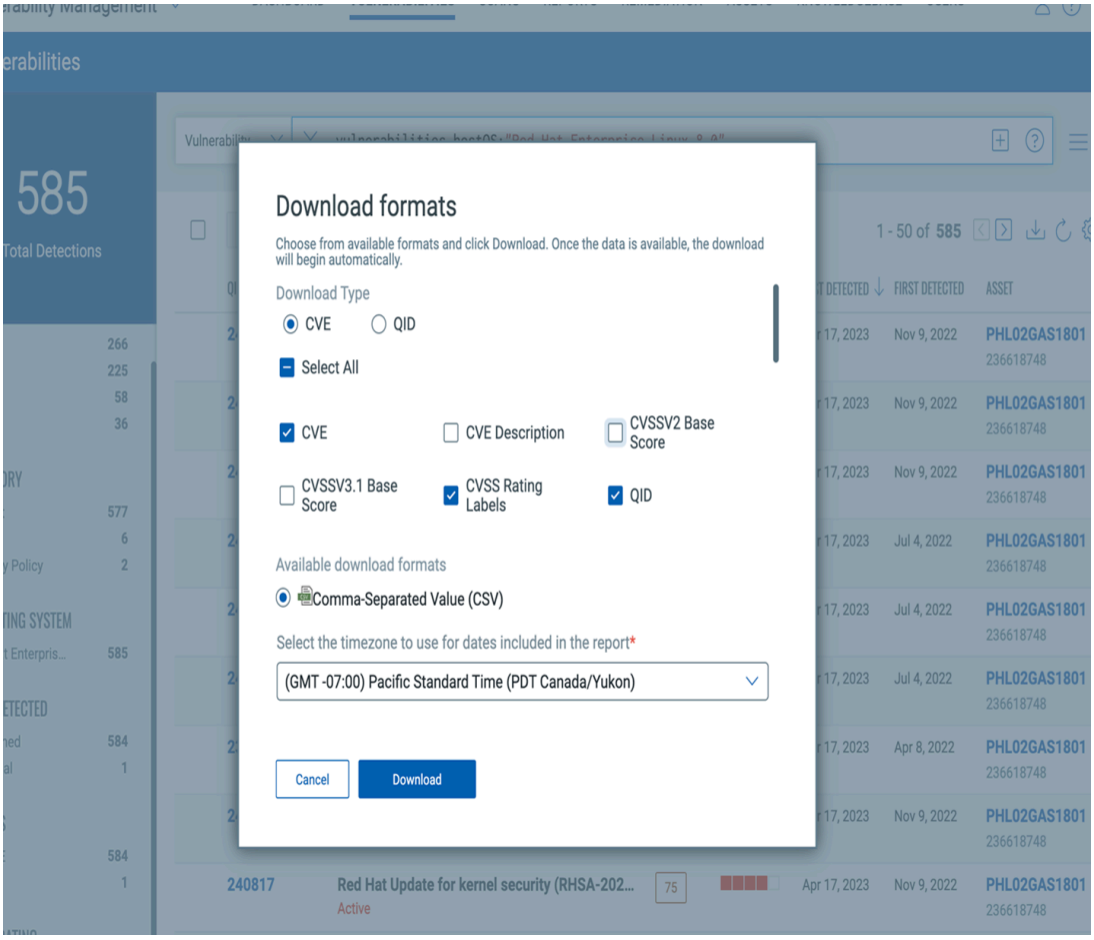
1. **「脆弱性」**に移動し、必要なフィルターを適用します。**「脆弱性」**が選択されていることを確認します。**「グループ化」**ではオプションを選択しないようにします。



2. ダウンロード・アイコンをクリックします。ダウンロード・ポップアップが表示されたら、**ダウンロード・タイプ**として **CVE** を選択します。

   「すべて選択」を選択するか、次のフィールドを個別に選択します。CVE、CVSS レーティング・ラベル、QID、タイトル、KB 重大度、重大度、CVSS レーティング・ラベル、CVE、ソリューション、資産 ID、公開日、脅威、カテゴリー。

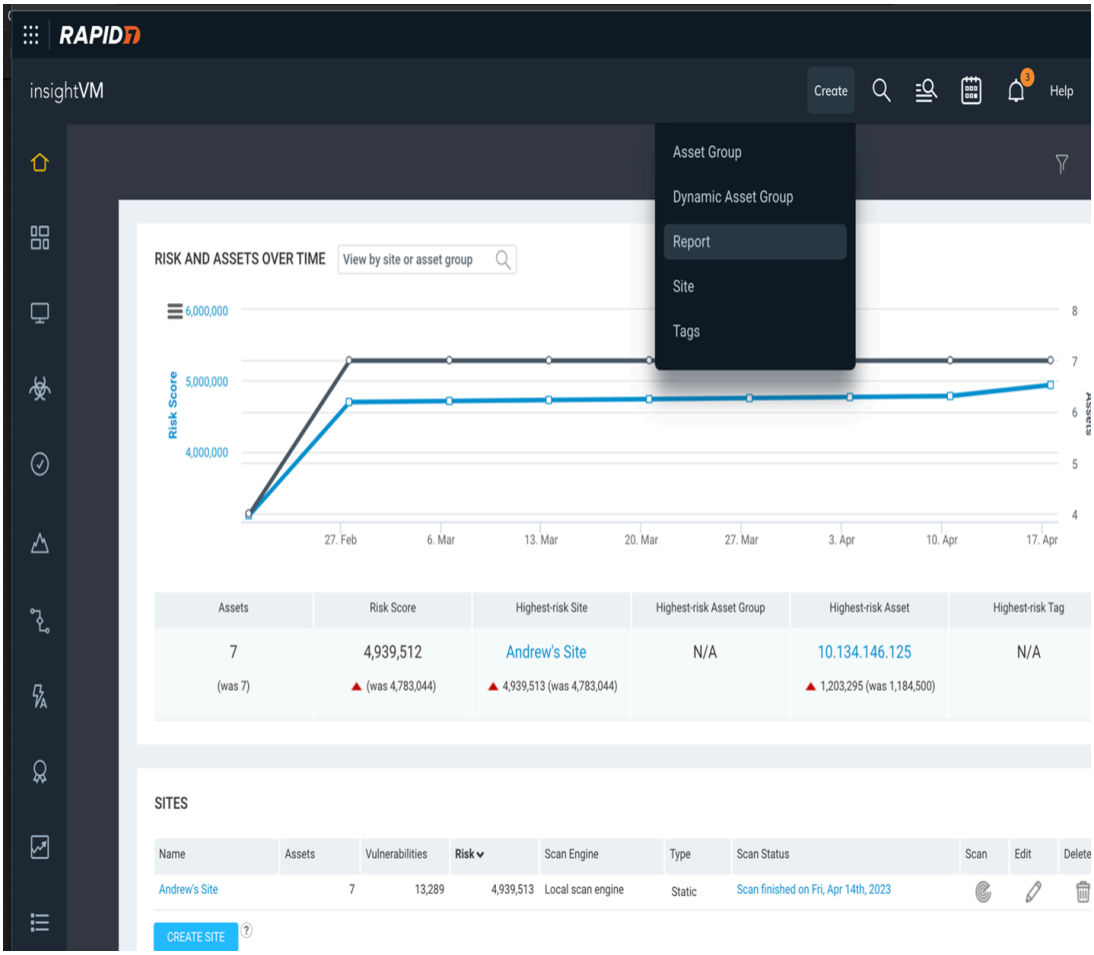
3. **「ダウンロード」**をクリックします。



注: エクスポートされた CVE が UTF-16 形式であると思われる場合は、Excel でファイルを開き、UTF-8 形式の CSV として保存しなおします。

Rapid 7:

1. Rapid 7 Scanner に移動し、**「作成」** > **「レポート」**をクリックします。



2. 「レポート・テンプレートの管理」をクリックし、「新規」をクリックします。
3. テンプレートの名前と説明を入力します。テンプレート・タイプに「エクスポート (CSV 形式)」を選択します。**「コンテンツ」**で、次のフィールドを選択します。脆弱性タイトル、脆弱性タグ、脆弱性の重大度、脆弱性の公開日、脆弱性 ID、 脆弱性の説明、脆弱性 CVSS スコア、脆弱性 CVE ID、資産 ID
4. **「保存」**をクリックします。
5. 「レポートの作成」を選択します。「テンプレート」で、作成したレポート・テンプレートを選択します。ファイル形式として CSV を選択し、必要に応じて範囲を設定します。
6. 「保存してレポートを実行」をクリックします。

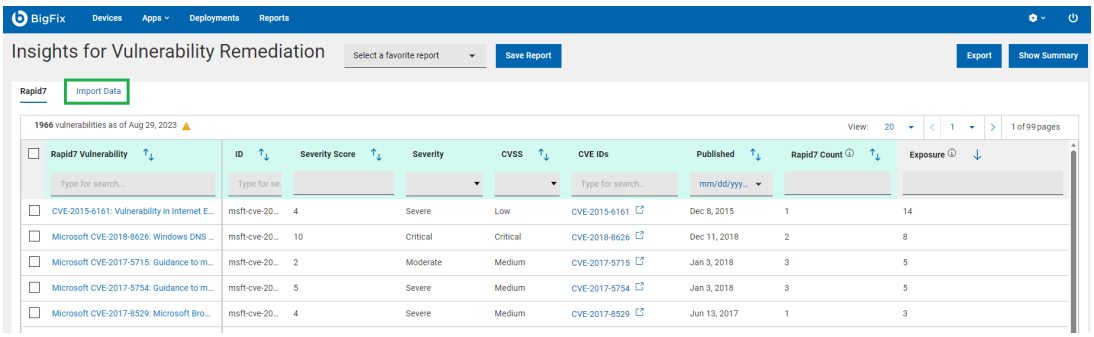
- **IVR への CSV 形式レポートのインポート: データのインポート**
  IVR アプリを使用すると、Qualys、Tenable、Rapid 7、または汎用レポートを CSV 形式で IVR に直接インポートできます。

  注: データ・インポートは、IVR アプリにアクセスできるすべてのユーザーが使用できます。WebUI IVR プラットフォームでは、一度に 1 つの CSV ファイルのインポートがサポートされていることに注意してください。WebUI IVR のすべてのユーザーは、役割や権限に関係なく、インポートした CSV レポートの管理責任を共有します。つまり、どの IVR ユーザーでも、インポートした CSV レポートを表示および削除できます。

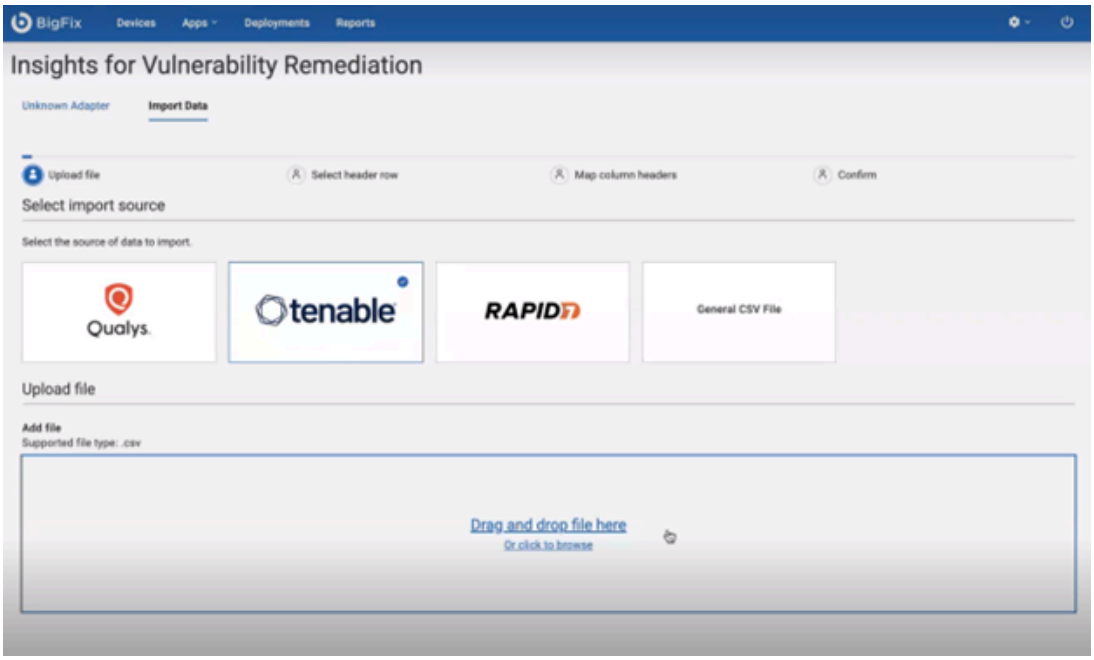
  注: データのインポートでは、Insights を設定して既存の IVR アダプターを実行する必要はありません。WebUI IVR 環境内で Insights を設定していても、インポートするデータが Insights データベースに自動的に入力されることはありません。

レポートを CSV 形式でインポートするには:

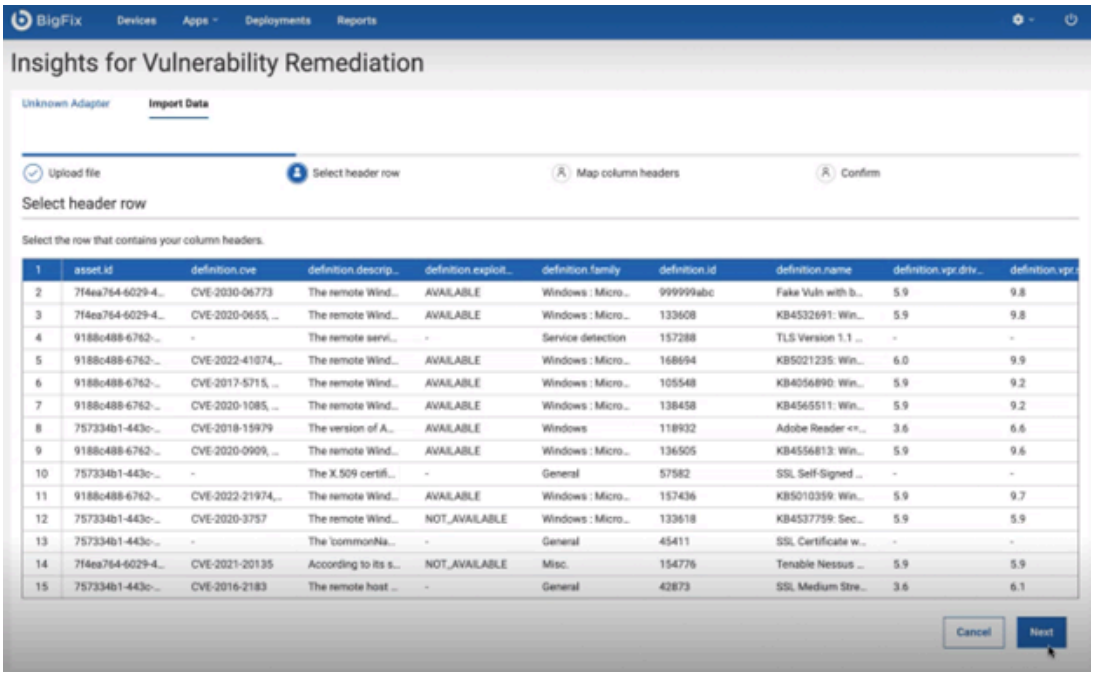
1. IVR アプリで**「データのインポート」**タブを選択します。



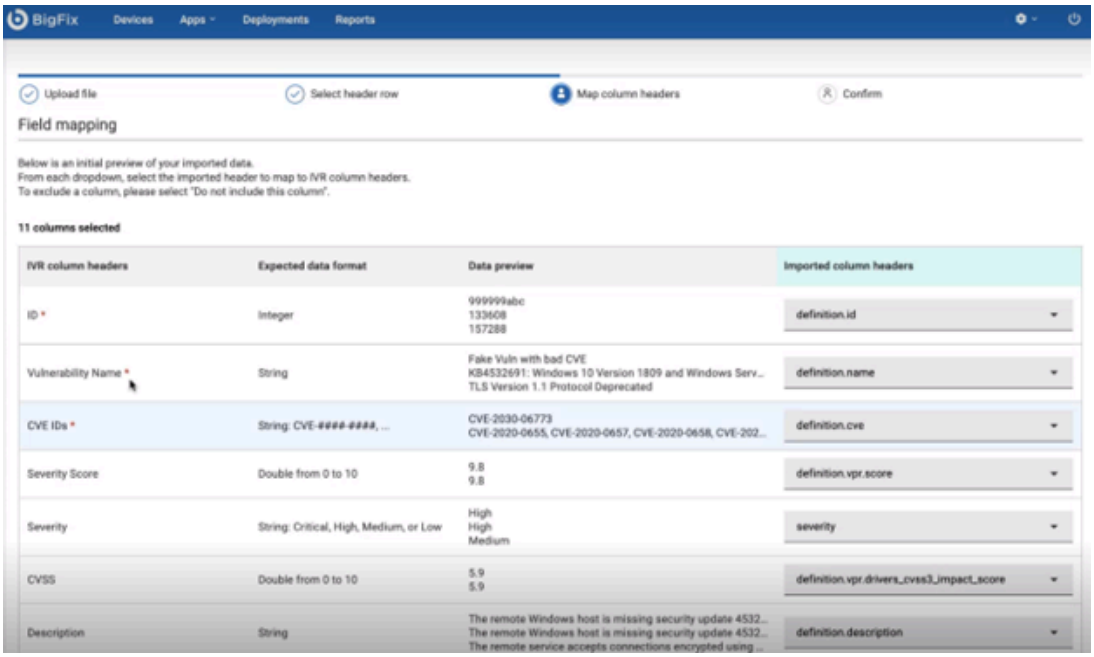
2. インポート元(Qualys、Tenable、Rapid 7、または汎用 CSV ファイル) を選択し、ファイルをアップロードします。IVR アプリがインポート・プロセスを開始します。



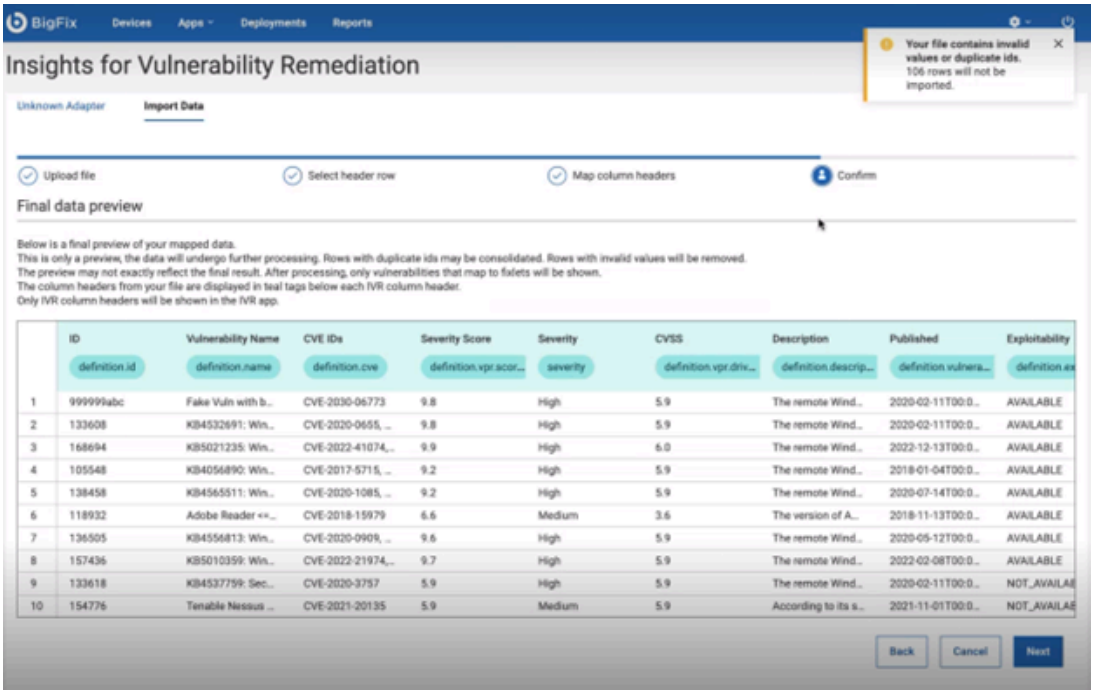
3. 列ヘッダーを含むヘッダー行を選択します。



4. 列ヘッダーをマッピングします。各ドロップダウンから、インポートしたヘッダーを選択して IVR 列ヘッダーをマッピングします。列を除外するには、ドロップダウン・リストから「この列を含めない」を選択します。



5. IVR アプリには、インポートしたデータの概要が確認用に表示されます。インポートを完了する前に、情報が正確であることを確認します。「次へ」をクリックしてください。



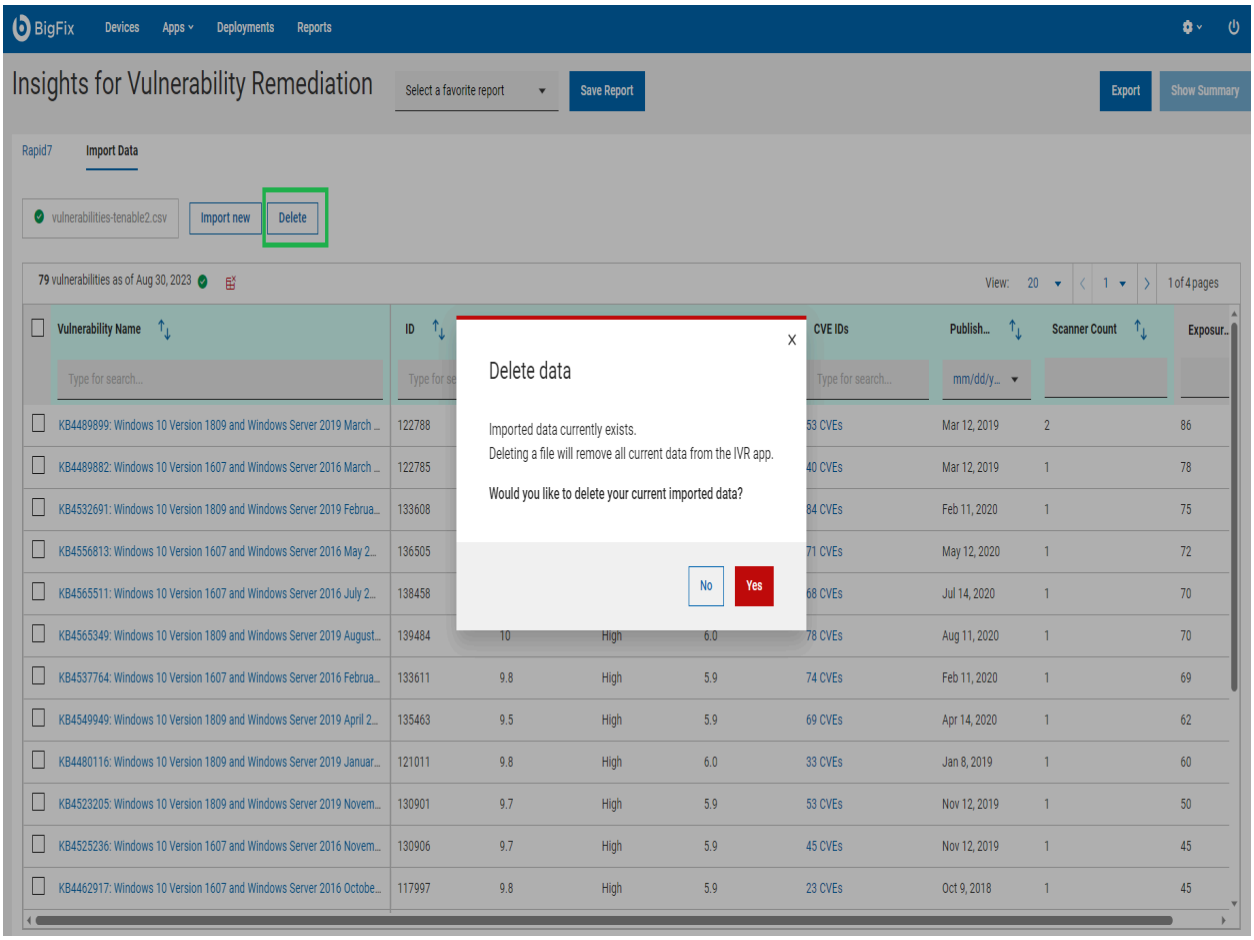
6. 確認すると、IVR アプリは脆弱性レポートをデータベースに統合します。インポートしたデータは、IVR システム内での分析およびレポート用にアクセスできるようになります。

   注: ID が重複した行は統合され、値が無効な行は削除される場合があります。相関する Fixlet が 1 つもない脆弱性は、リストに含まれません。CSV ファイルの無効な行は、IVR サイトのアプリ・フォルダーの **app\app\server\server-files** フォルダーに記録されます。このログ・ファイルの名前は次のとおりです。`IVR_CSV_INVALID_ROWS" Example path: C:\Program Files (x86)\BigFix Enterprise\BES WebUI\WebUI\sites\WebUI IVR Development_13783_324_1693266938\ivr-app\app\server\server-files`。

WebUI IVR では、インポートした脆弱性が Fixlet にマッピングされます。相関関係にある要素がバックグラウンドで進行中でも、脆弱性を選択して修正できます。1 つの Fixlet にもマッピングできなかった脆弱性 ID のリストは、デバッグ・ログに記録されます。CSV ファイル内の特定の行が無効とマークされる理由の追加情報は、次のファイルで見つかる場合があります。`<Program Files>\BigFix Enterprise\BES WebUI\WebUI\sites\WebUI IVR_XXXXX_XXXXXXXXX\IVR_CSV_INVALID_ROWS`。

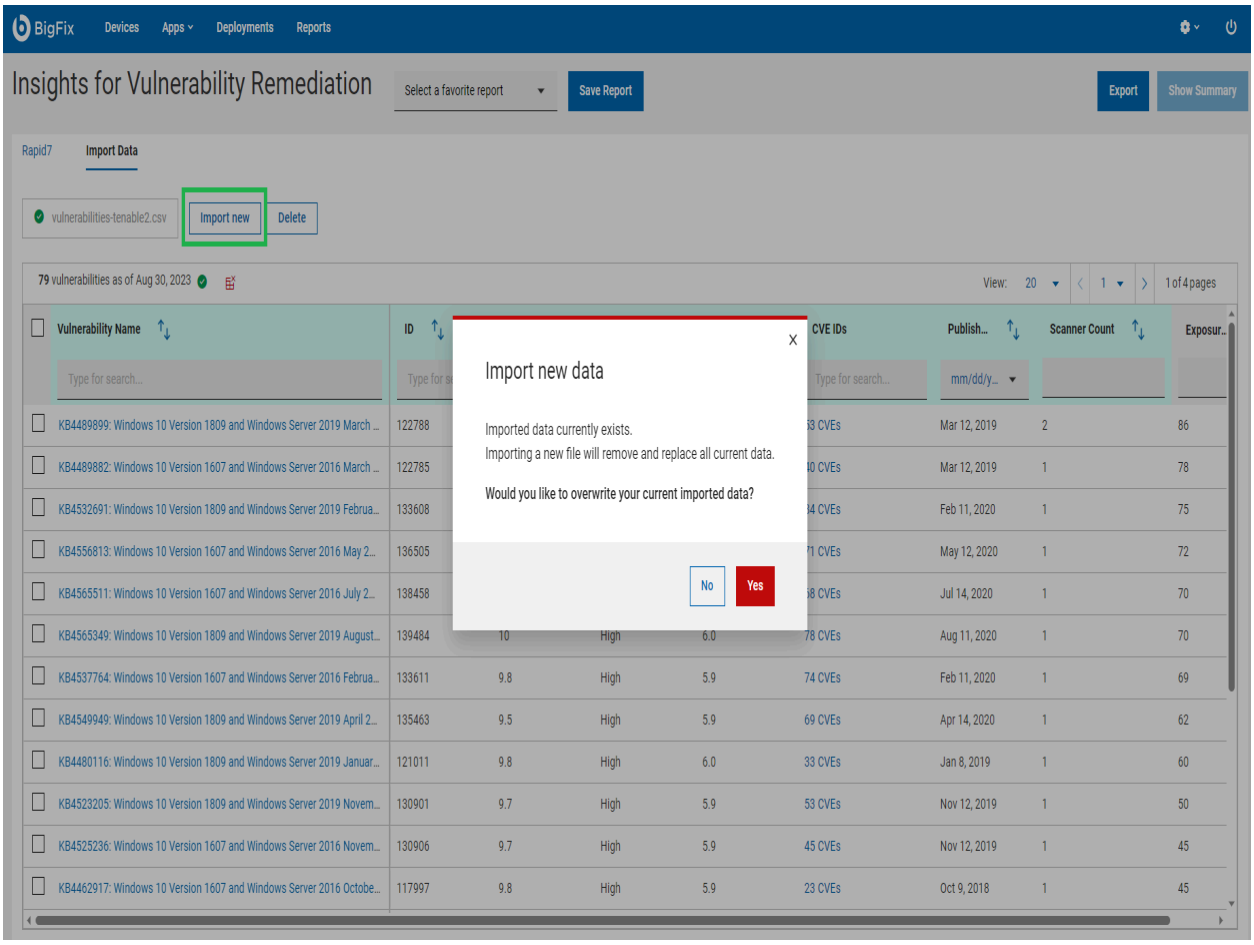
- **CSV レポートの削除**

レポートを削除するには、**「削除」**をクリックして削除を確定します。ファイルを削除すると、現在のデータはすべて IVR から削除されます。



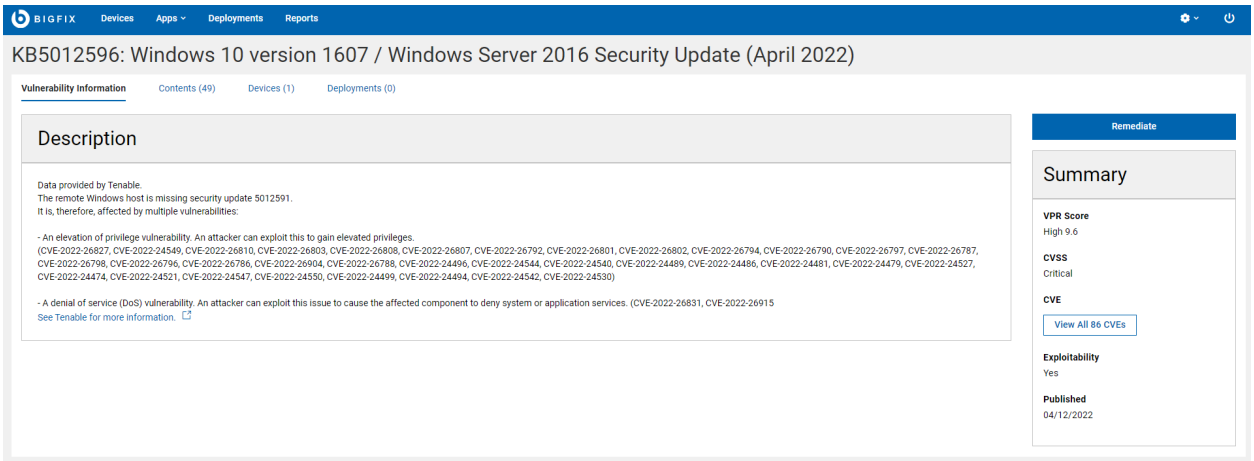
- **新しい CSV レポートのインポート**

新しいレポートをインポートするには、**「新規インポート」**をクリックします。新しいファイルをインポートすると、現在のデータはすべて削除されて置換されます。



IVR 文書

BigFix Insights for Vulnerability Remediation (BFIVR) 文書では、脆弱性、脆弱なデバイス、デプロイメント履歴の詳細の説明を確認できます。関連付けられたビューへのリンクを使用すると、脆弱性の詳細を確認できます。



IVR 文書には、以下のビューが含まれます。

- 脆弱性情報 - 脆弱性およびベンダー・リンクの詳細な説明
- コンテンツ - 選択した脆弱性に関連付けられた Fixlet のリスト
- デバイス - 対象を絞るための関連デバイスのリスト
- デプロイメント - IVR デプロイメント履歴

要約ビュー:

- VPR スコア
- CVSS
- CVE
- 悪用の可能性
- 公開済み

便利なリンク

アクションの実行: デプロイ・シーケンス (（ページ） 184)

Rapid 7 のサポート

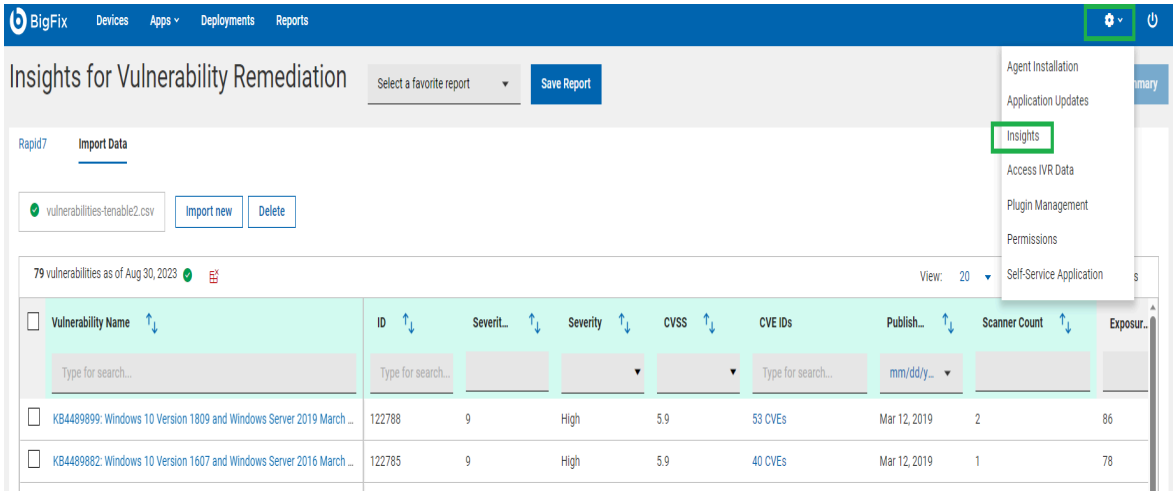
IVR と Rapid7 との統合により、BigFix は脆弱性データを取得し、それをデバイスと関連付け、CVE に基づいた修正アクションを推奨できます。また、脆弱性の重大度と暴露の日付に関する詳細なレポートを提供し、全体的な脆弱性管理を強化します。

注: Rapid 7 のサポートは、WebUI を使用して直接構成および管理します。

注: Insights に追加された新しい資産については、Insights が認識している直近の Rapid 7 スキャン日より前に検出結果データを検索することはできません。

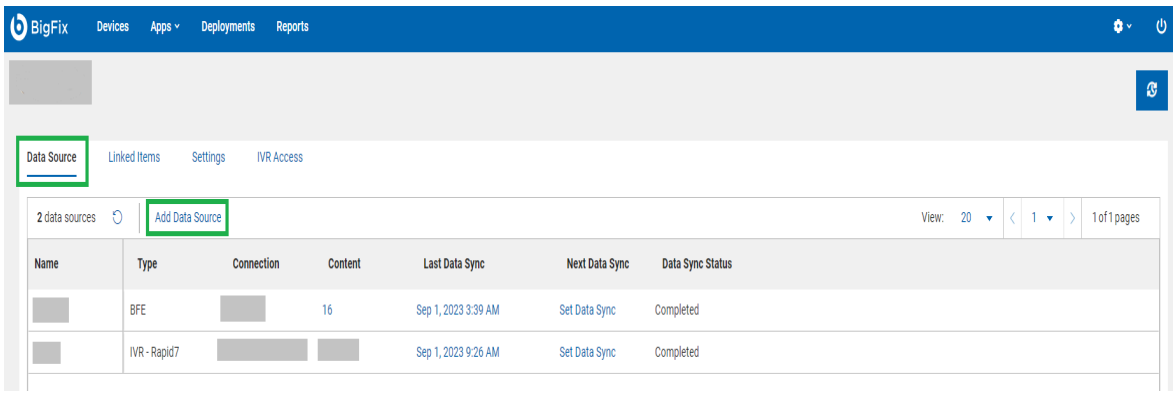
Rapid 7 データ・ソースを追加するには、次の手順を実行します。

1. WebUI アプリのナビゲーション・バーにある歯車アイコンをクリックして、「Insights」を選択します。このアクションにより、「BigFix Insights のセットアップ」ページに移動しま



す。

2. **「データ・ソース」**タブに移動し、**「データ・ソースの追加」**をクリックしま



す。

3. Rapid 7 データ・ソース・タイプを選択し、次の重要な詳細情報を入力します。
   - データ・ソースのエイリアス
   - API キー

注: API キーは、次の Rapid7 API リソースにアクセスできる必要があります。

- https://{region}.api.insight.rapid7.com/vm/v4/integration/vulnerabilities
- https://{region}.api.insight.rapid7.com/vm/v4/integration/assets

- 地域 - API エンドポイントの地域コード。地域コードの詳細については、Rapid 7 の公式ドキュメントを参照してください。
- データ開始日: スキャンのデータ取得を開始する日付
- 関連データ・ソース: データを抽出する特定のデータ・ソースを選択します
- フィルター・ストリング: このフィールドを使用して、必要に応じて脆弱性にフィルターを適用します。例えば、**{"vulnerability":"severity IN ['CRITICAL']"}** - このフィルターは重大度レベル**重大**の脆弱性のみを取得します。

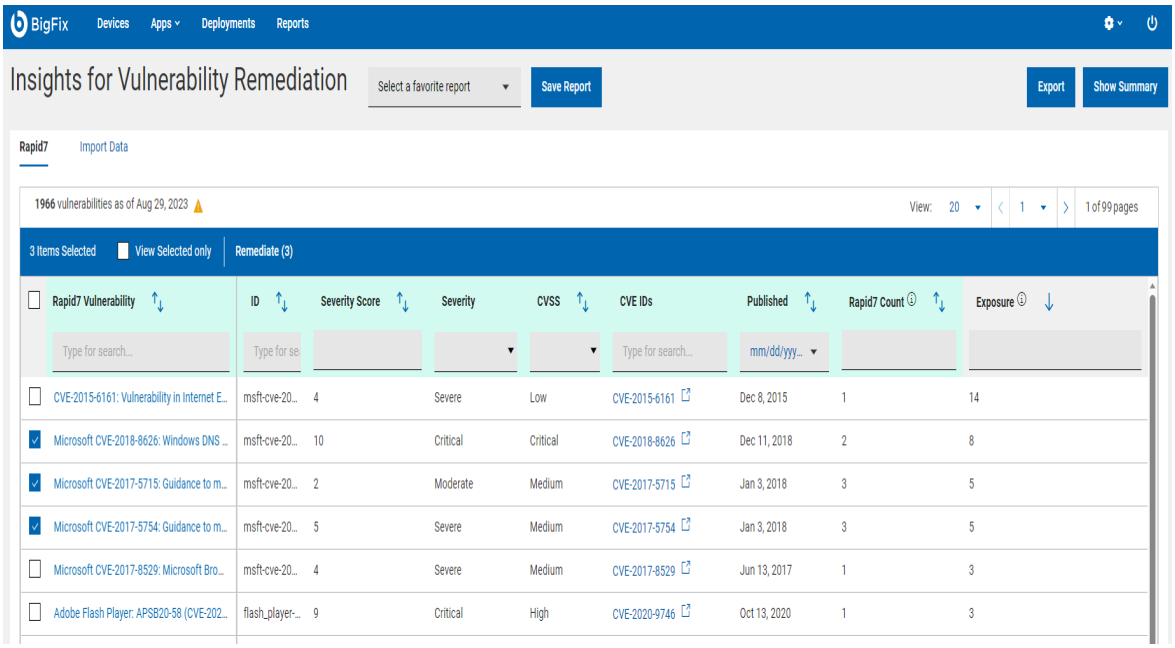
  フィルターに使用できる形式は JSON です。Rapid7 照会ビルダーで使用可能なフィルターを表示するには、Rapid 7 の公式ドキュメントを参照してください。
- プロキシー属性

4. 新しいデータ・ソースが、Rapid 7 データを Insights データベースに取り込む準備ができました。ETL プロセスを配置するには、**「ETL の設定」**をクリックします。ETL の構成方法の詳細については、「**ETL のスケジュール (（ページ）　　)**」を参照してください。

   注: BFE ETL が完了したら、Rapid 7 ETL を開始することが重要です。BigFix 環境に追加された新しいデバイスは、別のデータ同期を実行すると、Insights に統合されます。

5. 「IVR アクセス」タブに移動し、アクセス権を付与します。アクセス権を付与する方法の詳細については、「**IVR アクセス (（ページ）　　)**」を参照してください。

6. 「アプリ」に移動し、ドロップダウン・メニューから「IVR」を選択します。Rapid 7 データにアクセスできるようになりました。アクション・バーをアクティブ化するには、データ・グリッドから 1 つ以上の脆弱性を選択します。



WebUI IVR 設定

構成ファイルで変更できる BigFix Insights for Vulnerability Remediation (BFIVR) の使用可能な設定のリストをご覧ください。

設定名	デフォルト値
_WebUIAppEnv_INSIGHTS_CONFIG_PATH	<BigFix Enterprise Path>\BES WebUI\WebUI\insights_db_connection_config.

設定名	デフォルト値
_WebUIAppEnv_INSIGHT_BROKER_PORT	52318
_WebUIAppEnv_INSIGHT_BROKER_LOGGING_LEVEL	Info (情報)
_WebUIAppEnv_INSIGHTS_BROKER_CAPTURE_STDERR	0
_WebUIAppEnv_IVR_CACHE_REFRESH_TIME	デフォルトは 24 時間。最小: 5 分。値はミリ秒単位。

設定名	デフォルト値
_WebUIAppEnv_IVR_UPSERT_MAX_TIME	デフォルトは 1 時間。最小: 5 分 値はミリ秒単位。
_WebUIAppEnv_IVR_CSV_UPLOAD_SIZE_LIMIT_MB	デフォルト値は 250 です。値は ガバイト単位です
_WebUIAppEnv_INSIGHTS_IVR_NEW_DEVICES_LOOKBACK_DAYS	日

設定名	デフォルト値
_WebUIAppEnv_IVR_PROCESS_MEMORY_LIMIT_MB	128

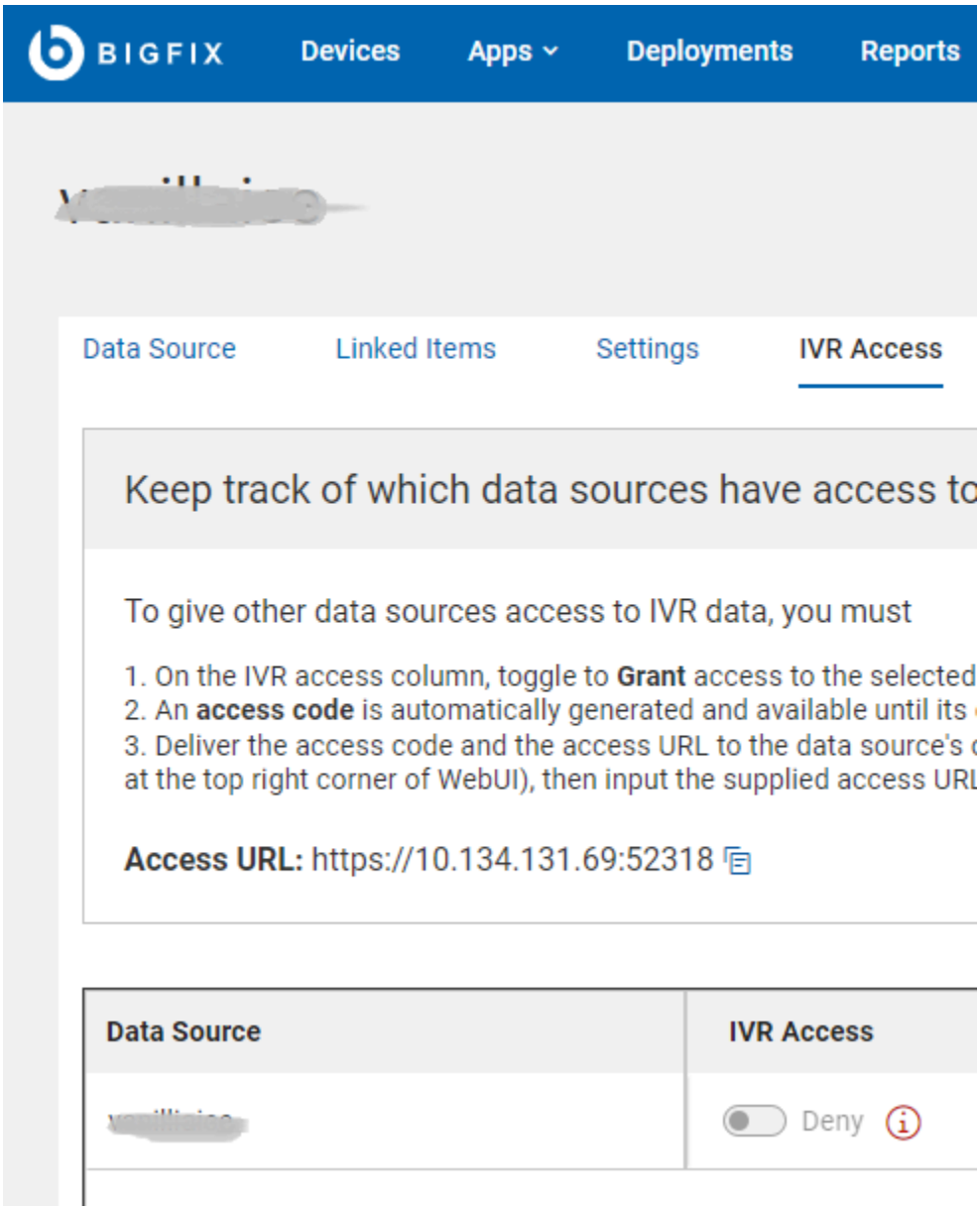
設定名	デフォルト値

IVR のトラブルシューティング

多くの場合、IVR アプリで発生するさまざまな問題をトラブルシューティングできます。

1. IVR アプリへのアクセス権限が付与されていない。

   エラー・アイコンの上にカーソルを移動すると、エラーの説明が表示されます。



考えられるエラー:

a. ご使用の環境が前提条件を満たしていない可能性があります。

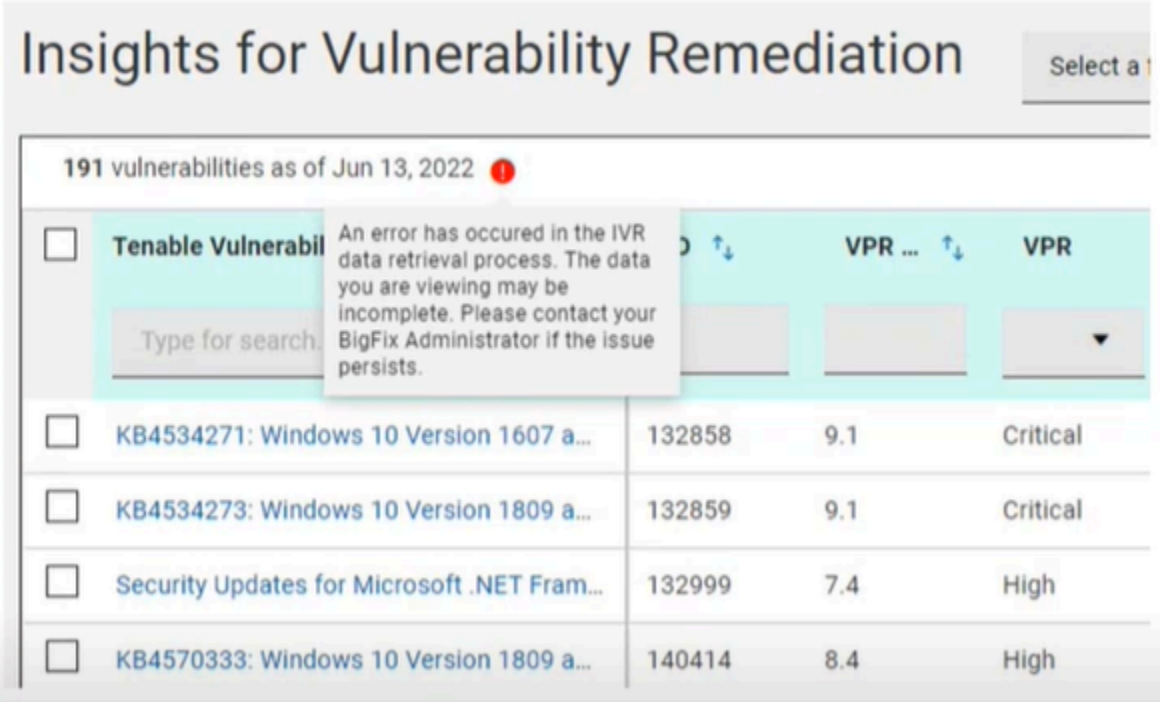
- IVR スキーマが設定されていることを確認します。
- IVR データフローが実行されていること (IVR 1.4) と、Insights に相関するデータが存在することを確認します。

注: Rapid7 では、古い IVR データフローは使用しません。IVR データフロー (IVR 1.4) が実行されているか、Rapid7 ETL プロセスが完了している必要があります。

- Insights ETL が実行中であることを確認します。

b. アクセスの許可/拒否時にエラーが発生したかどうかを確認します。
c. 自動構成中にエラーが発生したかどうかを確認します。
d. アクセス・コードの生成中にエラーが発生したかどうかを確認します。

2. データ取得プロセスで、エラーが発生した。



考えられるエラー:

a. IVR アプリケーションが insights_broker に接続しなかったか、アクセスが取り消されました。
b. ivr.log で、エラーやその他の情報を確認します。
c. プライマリー Insights サーバーの `<BigFix Enterprise Path>\BES WebUI\WebUI\sites\<WebUI Insights Folder>\insights-app\logs` フォルダーにあるブローカー・ログで、エラーについての詳細を確認します。

リリース・ノート

リリース・ノートでは、最新のアプリケーション更新など、BigFix Insights for Vulnerability Remediation の各バージョンに含まれる機能、更新、パッチについて説明しています。

IVR 3.0 - Rapid7 やカスタム CSV 取り込みを使用しているお客様

IVR 3.0 は WebUI でネイティブに使用可能で、次の新機能を搭載しています。

- IVR 用の新しいプラットフォーム、パフォーマンスの向上
- Rapid7 との IVR 統合のサポート
- BigFix で IVR 相関用の .csv ファイルをインポートする機能
- Rocky Linux 9 および Oracle Linux 9 で WebUI パッチ・ポリシーをサポート
- バグ修正
- セキュリティーの向上

Rapid7 との IVR 統合のサポート

- IVR では、IVR 3.0 で Rapid7 とのネイティブ統合がサポートされ、BigFix では Rapid7 から脆弱性情報を取得して BigFix 内のデバイスに相関してから、環境で検出された CVE に基づいて修正を提案できるようになりました。
- BigFix では、現在の環境で発覚した脆弱性、環境に現在ある脆弱性の重大度、およびさまざまな暴露の日付をレポートおよびエクスポートできます。

CSV インポート

- BigFix は、資産情報と対応する CVE を含む .csv ファイルをインポートし、それらを既存の BigFix デバイスと Fixlet に相関させることをサポートするようになりました。
- デバイスと暴露の修正は、ウィザードから簡単に選択して実行できます。

Insights Live ETL フィード

- Insights Live ETLフィード・ページは、アクティブな BFE ETL プロセスのステージとさまざまなステップを表示するように設計されています。主な目的は、ETL の問題のデバッグを支援し、進行中の ETL 操作の進捗を監視することです。
- Live ETL フィード・ページには URL 経由でのみ直接アクセスでき、WebUI で Insights にログインした後でアクセス可能になります。このページを表示する直接リンクまたはボタンはありません。
- Live ETL フィード・ページにアクセスするには、次の手順に従い、Web ブラウザーを開いて URL「https://<webui_server>/insights/live」を入力します。

更新方法

WebUI は、別の構成が行われていなければ、デフォルトで自動的に更新されます。WebUI Insights および WebUI IVR の更新は、WebUI のアプリケーション更新ページから手作業で行う必要があることに注意してください。WebUI IVR を更新すると、WebUI Insights も更新されます。詳しくは、https://help.hcl-software.com/bigfix/11.0/webui/WebUI/Admin_Guide/c_manage_application_updates.html を参照してください。

リソース

- デモ・リンク (9 月 27 日) - https://www.brighttalk.com/webcast/17964/591770?utm_source=HCLBigFix&utm_medium=brighttalk&utm_campaign=591770
- 製品ページ - https://www.hcl-software.com/bigfix/ivr-home
- マニュアル - https://help.hcl-software.com/bigfix/11.0/webui/WebUI/Users_Guide/c_get_started_with_IVR.html

第 7 章. ソフトウェア入門

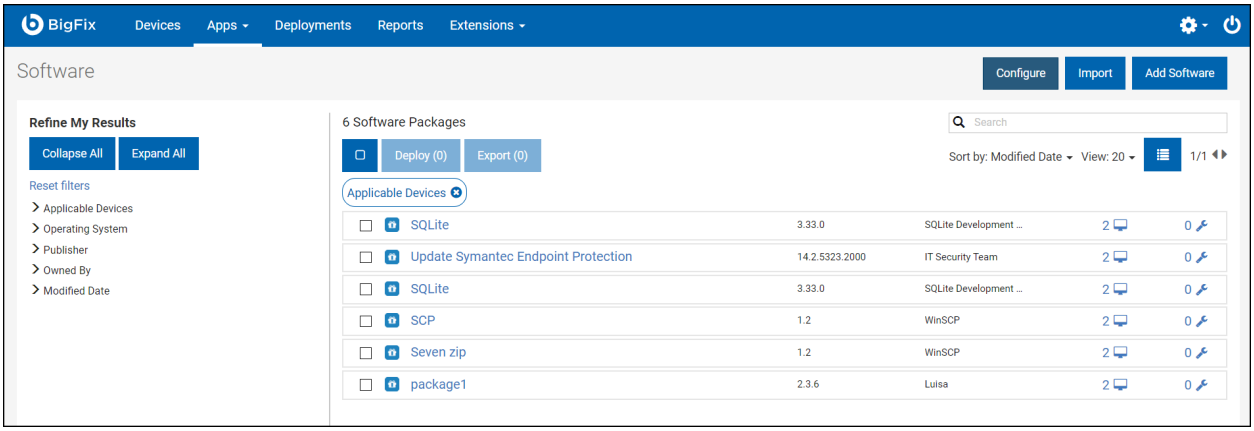
BigFix ソフトウェア・パッケージは、デバイスへのソフトウェアのインストールに使用する Fixlet のコレクションです。パッケージには、インストール・ファイル、インストール・ファイルをインストールする Fixlet、パッケージ自体に関する情報が含まれています。

ソフトウェア・パッケージのリスト、特定のソフトウェアの検索、パッケージの詳細情報の表示を行うには、ソフトウェア関連の画面を使用します。

組織のソフトウェア・アプリケーション・カタログからパッケージを追加、編集、削除するには、ソフトウェア画面を使用します。マルチ・タスク機能を使用し、複数のアクションを実行するパッケージを作成します。例えば、異なるオプションを使用して、多様な方法で単一ソフトウェアのインストールとアンインストールの両方を実行できる単体パッケージを作成します。

ソフトウェア・パッケージ・リスト

ソフトウェア・パッケージは、デバイスへのソフトウェアのインストールに使用する Fixlet のコレクションです。



- **リストのコンテンツは、オペレーターのデバイスとサイトの割り当て**、および特定のパッケージが共有されているか、または所有者によって非公開としてマークが付けられているかを反映します。
- **「ソフトウェアの追加」**リンクを使用して、**ユーザーのカタログにソフトウェアを追加**します。オペレーターにソフトウェアを追加する権限がない場合は、このリンクは表示されません。

特定の BES サーバーから、別の BES サーバーへソフトウェア・パッケージを移動するには、**「エクスポート」**と**「インポート」**機能を使用します。これらのツールは、複数の BigFix デプロイメントを実行している場合、またはバックアップをとる場合に役に立ちます。

- **エクスポート** - クリックして、BES サーバーにあるソフトウェア・パッケージを zip ファイルとしてエクスポートします。ブラウザーが、ディレクトリーを指定するよう促します。エクスポートするよう選択された複数のパッケージは、単一の zip ファイルにまとめられます。
- **インポート** - クリックして、**「エクスポート」**機能で作成されたパッケージをインポートします。パッケージをインポートする権限を持たないオペレーターには、この機能は表示されません。

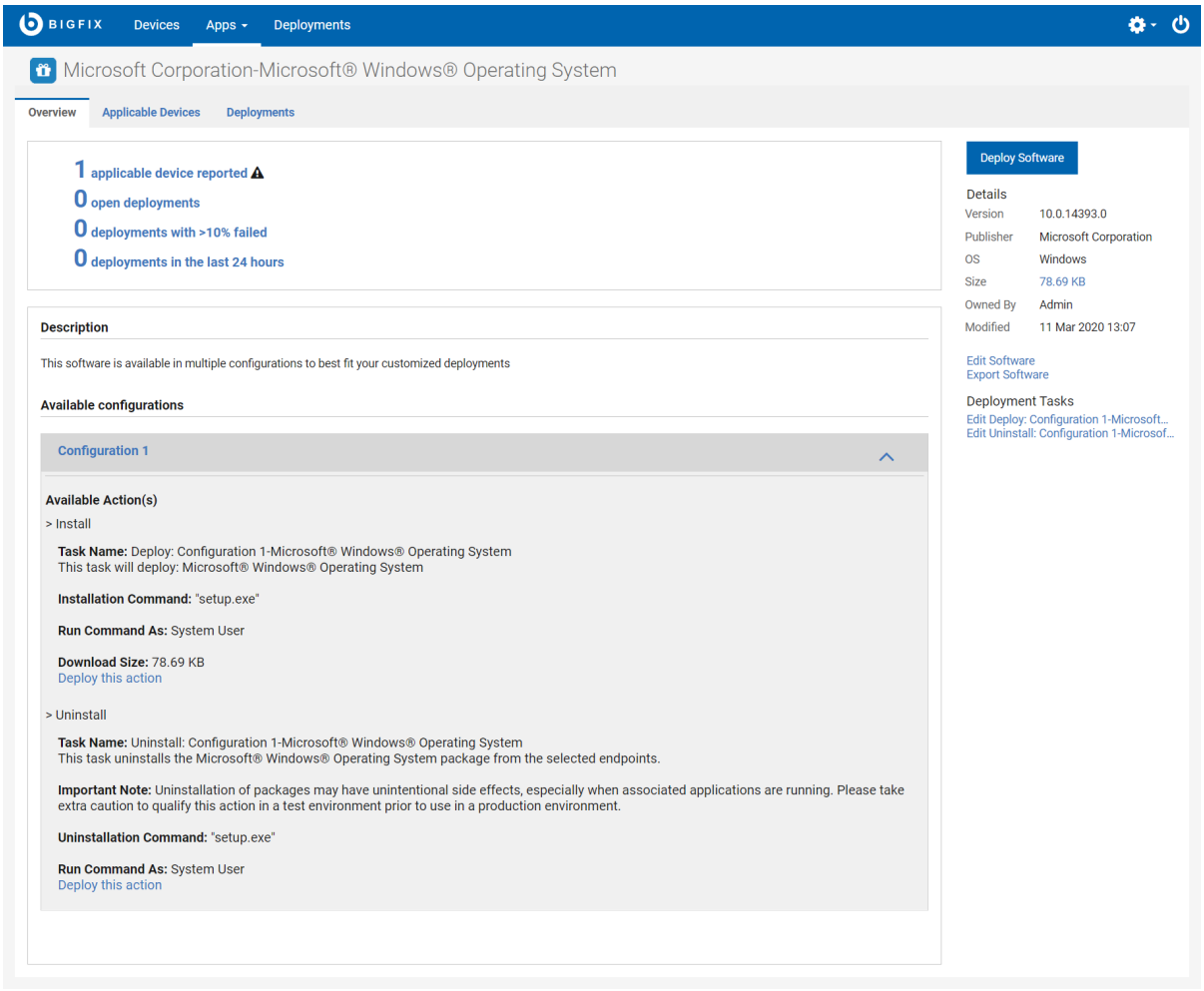
注: テキスト・ベースのファイルを含むソフトウェア・パッケージをインポートすると、失敗する場合があります。インポート・プロセスは、ファイルの SHA 値を変更でき、SHA 検証に失敗すると、インポートも失敗します。これは、BigFix プラットフォームの既知のバグです。

ソフトウェア文書

ソフトウェア・パッケージの説明、適用可能なデバイス、デプロイメント履歴を確認するには、ソフトウェア・パッケージ名をクリックします。サイドバーや関連付けられたビューにあるリンクを使用すると、パッケージの詳細を表示できます。

ソフトウェア文書ビューは以下のとおりです。

- 概要 – ソフトウェア・パッケージの詳細説明。
- 適用可能なデバイス – このソフトウェアに適格なマシン。
- デプロイメント – ソフトウェア・デプロイメント履歴。



- **「ソフトウェアのデプロイ」**をクリックして、パッケージにソフトウェアをデプロイします。
- **「ソフトウェアの編集」**リンクを使用して、ユーザーのカタログからソフトウェア・パッケージを編集または削除します。

- **「ソフトウェアのエクスポート」**リンクを使用して、パッケージをエクスポートします。
- デプロイメント・タスクのリンクをクリックして、タスクを編集します。タスクの編集について詳しくは、「カスタム・コンテンツの編集 (（ページ） *145)*」を参照してください。

ソフトウェア・カタログの操作

このセクションでは、ユーザーのカタログへのソフトウェアの追加、ソフトウェア・パッケージの編集、カタログからのパッケージの削除を行う方法を説明します。

カタログへのソフトウェアの追加に使用される権限と、ソフトウェアの編集と削除に使用される権限は、異なる方法で計算される点に注意してください。

BigFix の単一コンソール設定は、オペレーターがソフトウェアの追加権限を持つかどうかを判定します。カタログのソフトウェアを編集および削除する権限は、誰がそのソフトウェア・パッケージを所有しているか、BigFix コンソールと WebUI のどちらを使用して作成されたか、また、WebUI で作成されたパッケージが後にコンソールを使用して編集されたかどうかにも影響されます。ソフトウェア・パッケージを編集しようとして権限の問題に遭遇した場合は、BigFix 管理者にお問い合わせください。

ソフトウェア・パッケージの追加

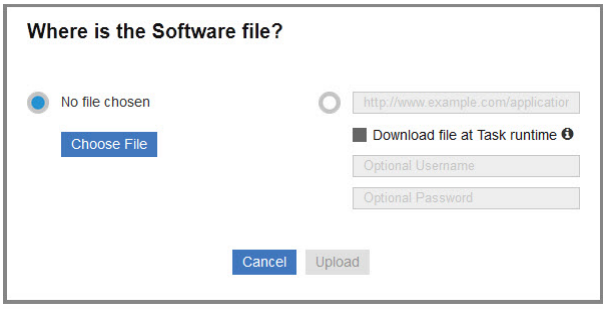
パッケージの作成と編集を簡単にするため、サポート対象のファイル・タイプに合わせて、インストール・コマンドとアンインストール・コマンドが自動的に生成されます。これらのデフォルト設定の編集や、独自設定の入力は自由に行うことができます。サポート対象外のファイル・タイプは、使用するコマンドをタイプ入力します。

- サポート対象のインストール・ファイル・タイプ:
  appv、.appx、.bat、dmg、.exe、.msi、.msp、.msu、.pkg (Mac と Solaris)、.rpm。

- サポート対象のアンインストール・ファイル・タイプ: .appv、.msi、.rpm。

ソフトウェア・パッケージの追加

1. **ソフトウェア・パッケージ・リスト**で**「ソフトウェアの追加」**をクリックして、**「ソフトウェア・パッケージのアップロード」**ダイアログを開きます。



2. ローカル・ファイルを選択するか、URL を入力してパッケージをダウンロードします。ファイルをアップロードし、BigFix サーバー上に配置します。ファイルはパッケージが削除されるまで BigFix サーバーに残ります。**「タスクの実行時にファイルをダウンロード」**ボックスにチェック・マークを付けて、パッケージがデプロイされたときにファイルをキャッシュするようにします (これはファイルを永続的に格納しない場合に役立つ代替の方法です)。
3. 「**アップロード**」をクリックします。
4. カタログ・レコードを入力します。以下を検証、入力、または選択します。
    - ソフトウェア名
    - バージョン番号
    - 公開者
    - パッケージ・アイコン - パッケージのデフォルト・アイコンを置き換えるには、**「アイコンの変更」**をクリックし、.ico または .png ファイルをアップロードします。
    - オペレーティング・システム - Linux、OS X、Solaris、Windows など。
    - カテゴリー - ソフトウェアのタイプ。既存のカテゴリーを 1 つまたは複数選択するか、新しいカテゴリー名を入力して新しいカテゴリーを作成します。
    - 説明 - パッケージの説明と、そのデプロイを担当するほかの人の役に立つ任意の指示を記述します。
    - 構成 - この場合の構成には次の 2 つの操作があります。インストールとアンインストール (任意)。

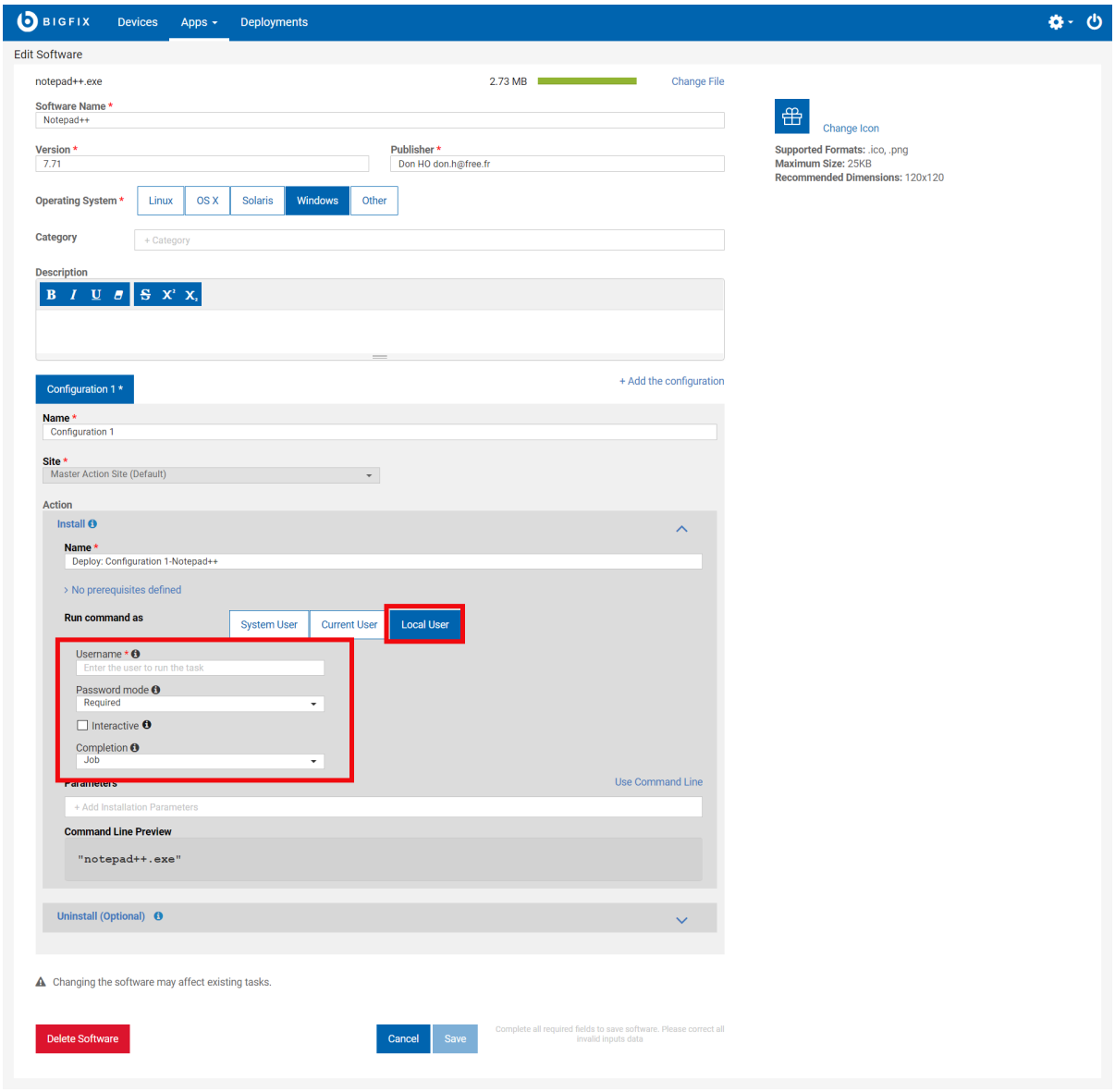
- 構成を追加するには:
  a. **「+ 構成を追加する」** をクリックします。
  b. 構成の**「名前」**を入力します。
  c. **「サイト」**リストで Fixlet が保存されている BigFix サイトを選択します。
- 構成を削除するには、削除する構成タブを選択し、**「削除」**をクリックします。構成タブが 1 つのみの場合は、**「削除」**ボタンは非表示となります。

- Windows システムの場合、システム・ユーザー、現在のユーザー、ローカル・ユーザーとしてコマンドを実行できます。BigFix クライアントで実行されるコマンドのデフォルトはシステム・ユーザーとなります (OS X、UNIX、Linux コンピューターの場合、ソフトウェアは root としてインストールされます)。場合によっては、現在のユーザーまたはローカル・ユーザーの資格情報とローカル・コンテキストを使用してインストールすることもできます。ローカル・ユーザーに関連するさまざまなパラメーターの設定方法について詳細は、ローカル・ユーザーとしてデプロイメント・コマンドの実行 (（ページ） *133)*を参照してください。
- 用意されたインストール・パラメーターのリストから選択するか、**「使用するコマンド・ライン」**をクリックしてインストール・コマンドを編集します。コマンドが正しく、完全であることを確認するため、**「コマンド・ラインのプレビュー」**を使用します。

5. **「保存」**をクリックしてパッケージを追加します。

ローカル・ユーザーとしてデプロイメント・コマンドの実行

このセクションでは、ログイン・ユーザーとは異なるローカル・ユーザーとして、コマンドを実行する際に設定できるさまざまなパラメーターについて説明します。



- **ユーザー名**: 現在ログインしているユーザーと異なるユーザーの名前です。次のいずれかの形式となります。
    1. user@ドメイン。例: 「myname@tem.test.com」
    2. ドメイン\ユーザー。例: 「TEM\myname」
- **パスワード・モード**: 認証のモードを定義します。以下のオプションを使用できます。

1. **必須**: アプリケーションはパスワードを入力するよう指示します。入力した値は安全なパラメーターとしてエージェントに渡されます。
2. **別ユーザー名を使用**: エージェントは**「ユーザー名」**で指定されたユーザー用に実行されているセッションを検索し、そのユーザーのセッションでコマンドを実行します。
3. **システム**: コマンドはローカル・システム・アカウントとして実行されます。このオプションを機能させるには、**「ユーザー名」**で指定されたユーザーがコマンド実行時にシステムにログインしている必要があります。

- **インタラクティブ**: チェック・ボックスを選択します。コマンドにより**「ユーザー名」**で指定されたユーザーのユーザー・インターフェースが開き、そのユーザーのセッションが実行されます。
- **対象ユーザー**: オプション。このオプションは**「インタラクティブ」**を選択した場合にアクティブになります。コマンドによりこのフィールドで指定したユーザーのセッションでユーザー・インターフェースが開き、そのセッションが実行されます。コマンドはプライマリー・ユーザー特権で実行しますが、コマンドが機能するには対象ユーザーがシステムにログインしている必要があります。
- **完了**: コマンドがプロセスの終了まで待機する必要があるかを指定します。
  1. **なし**: コマンドはプロセスの終了まで待機しません。コマンドが実行を開始する前に、ユーザーはシステムにログインしている必要があります。このオプションを選択すると、`SWD_Download` フォルダーが保持されます。`SWD_Download` フォルダー・クリーンアップ Fixlet をデプロイし、プロセス終了後にクライアント・コンピューターをクリーンアップします。
  2. **プロセス**: コマンドはプロセスの終了まで待機します。このオプションの場合は、指定されたユーザーがシステムにログインしている必要はありません。
  3. **「ジョブ」**: コマンドはプロセスの終了まで待機します。このオプションの場合、プロセスは独自のジョブ制御管理を実行することになっており、指定されたユーザーがシステムにログインしている必要はありません。

アンインストールの有効化

追加したソフトウェア・パッケージでアンインストール・オプションを有効にする方法を説明します。

アンインストール・オプションを有効にするには:

1. 「ソフトウェア・パッケージの追加」 (（ページ） *131)*の手順 1〜4 を完了します。
2. 「設定」タブの**「アクション」**で、**「アンインストール」**をクリックして**「オン」**を選択します。
3. **次の権限でコマンドを実行**: 利用可能なオプションを選択します。
   - システム・ユーザー
   - 現在のユーザー
   - ローカル・ユーザー
4. **「コマンド行の使用」**をクリックします。
   自動の場合: サーバーとクライアントのオペレーティング・システムが同じ場合、コマンド行の文字列は自動生成されます。そのため、この設定を保存してクライアント・マシンでアンインストール・アクションをデプロイすると、アンインストールが自動実行されます。
   手動: クライアントのオペレーティング・システムがサーバーのものと異なり (Windows クライアントと Linux サーバーなど)、2 つの異なる拡張子ファイル (*.rpm と *.msi など) をサポートしている場合は、文字列を手動で入力します。手動で入力しない場合は、この設定を保存してクライアント・マシンでアンインストール・アクションをデプロイしたあと、コンソール上でこのアクションの状態が「完了」になっていても、アンインストールは自動実行されません。
5. **「保存」**をクリックします。
   ソフトウェアをアンインストールするためのアンインストール設定が保存されます。

ホワイトリストの構成

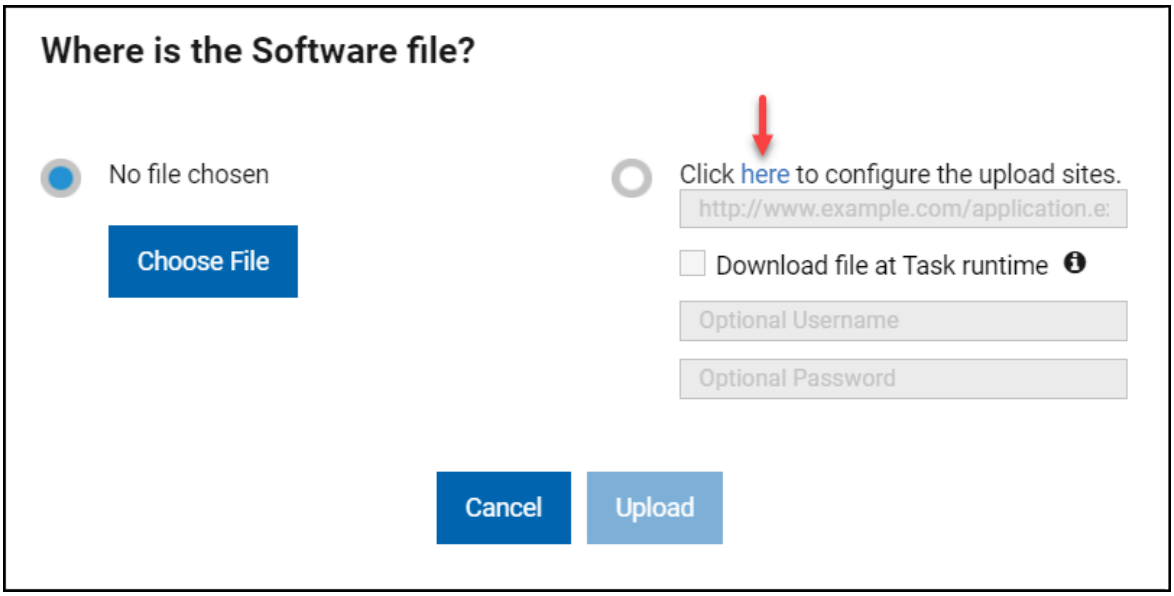
マスター・オペレーターは、ソフトウェア・パッケージをホワイトリストに登録するためのアップロード・サイトを構成できます。

注: マスター以外のオペレーターは、**ソフトウェア・パッケージ・リスト**で構成されたホワイトリストに従って許可された URL のみを使用できます (ソフトウェア・パッケージの追加 (（ページ） *131)*を参照)。

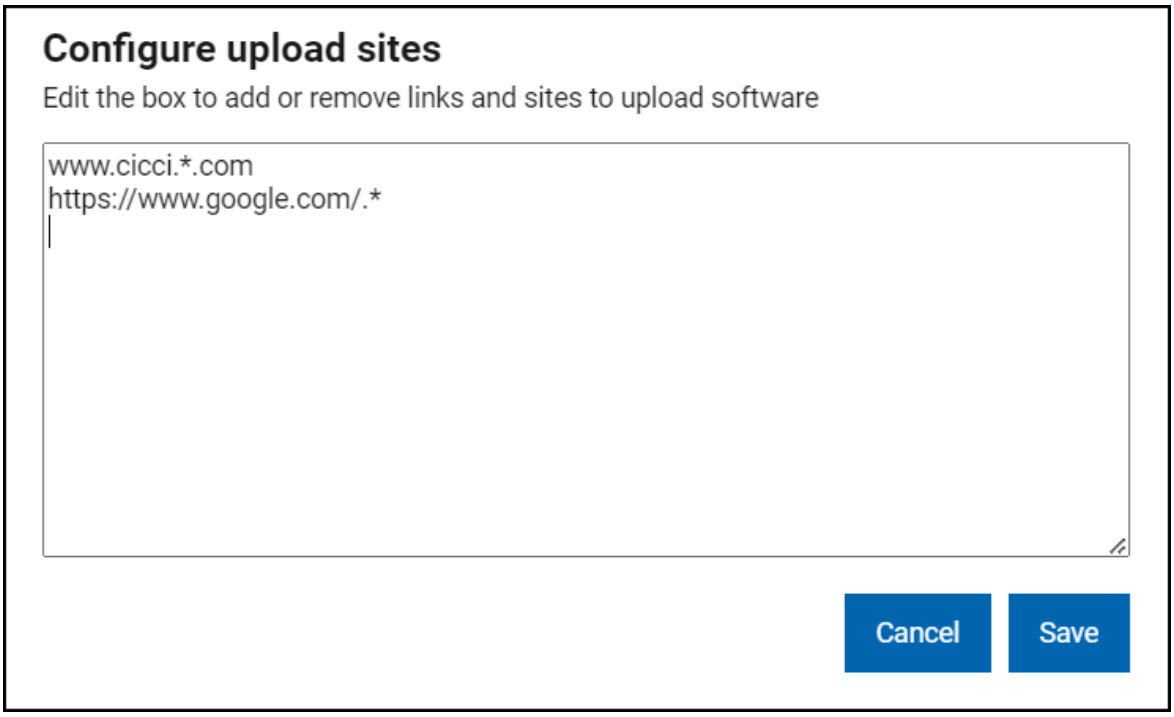
ホワイトリストの構成

サイトから SWD パッケージをアップロードするには、マスター・オペレーターが許可サイトのホワイトリストを構成する必要があります。ホワイトリストは regex 構文に従って構成できます。

1. **ソフトウェア・パッケージ・リスト**で**「ソフトウェアの追加」**をクリックして、**「ソフトウェア・パッケージのアップロード」**ダイアログを開きます。



2. **「ソフトウェア・パッケージのアップロード」**ダイアログで**ここ**をクリックします。
3. **「アップロード・サイトの構成」**ダイアログに URL を入力します。マスター・オペレーターのみがアップロード・サイトを構成できます。



4. **「保存」**をクリックしてソフトウェア・パッケージをアップロードします。

ソフトウェア・パッケージの編集

パッケージの作成と編集を簡単にするため、サポート対象のファイル・タイプに合わせて、インストール・コマンドとアンインストール・コマンドが自動的に生成されます。これらのデフォルト設定の編集や、独自設定の入力は自由に行うことができます。サポート対象外のファイル・タイプは、使用するコマンドをタイプ入力します。

- サポート対象のインストール・ファイル・タイプ:
  appv、.appx、.bat、dmg、.exe、.msi、.msp、.msu、.pkg (Mac と Solaris)、.rpm。

- サポート対象のアンインストール・ファイル・タイプ: .appv、.msi、.rpm。

ソフトウェア・パッケージの編集

1. 更新対象のソフトウェア・パッケージの文書を開きます。
2. 右側のパネルの**「ソフトウェアの編集」**リンクをクリックします。

3. パッケージ・データまたはデプロイメント・オプションに必要な変更を行います。各フィールドとフィールドのオプションについて詳しくは、『ソフトウェア・パッケージの追加 (（ページ） *131)*』を参照してください。
4. **「保存」**をクリックします。

注: ファイルや Fixlet が含まれないよう編集されたパッケージなど、SWD ダッシュボードで編集されたパッケージは、WebUIでは編集できません。

ソフトウェア・パッケージの削除

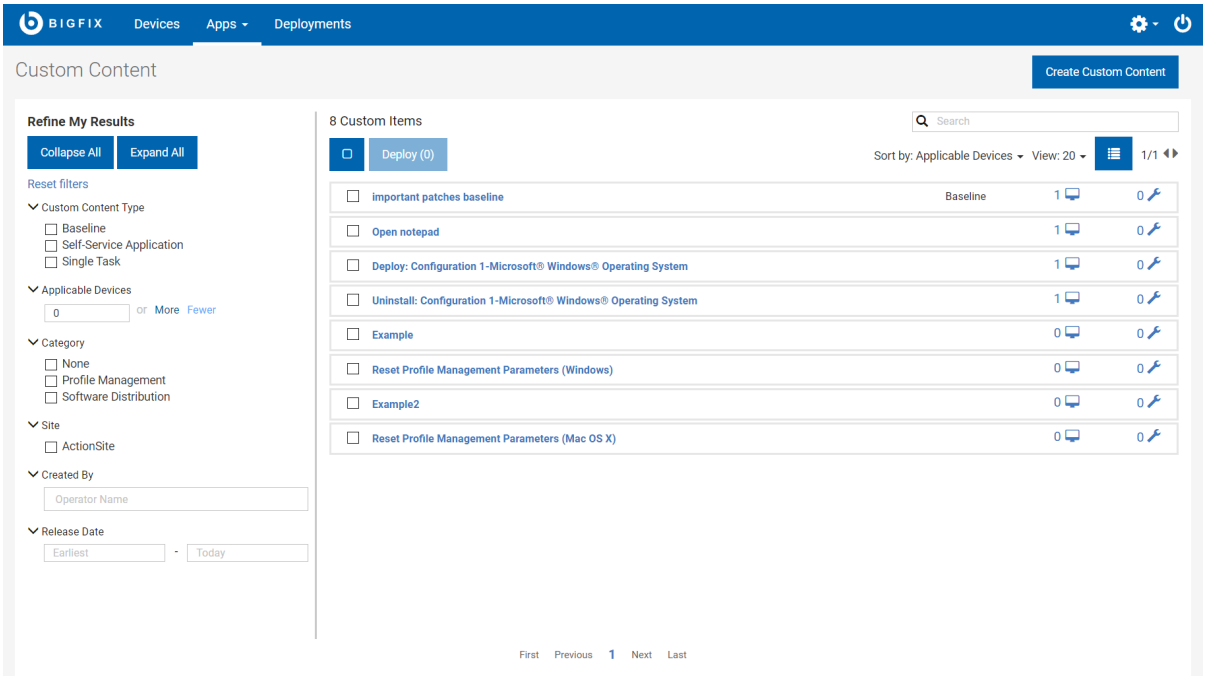
1. 削除対象のソフトウェア・パッケージの文書を開きます。
2. 右側のパネルに位置する**「ソフトウェアの編集」**リンクをクリックします。
3. ダイアログの左下隅にある**「削除」**をクリックし、表示されるプロンプトで確認します。

第 8 章. カスタム・コンテンツ入門

カスタム・コンテンツの表示、タスクの編集、適用可能なデバイスやデプロイメントなどの関連情報の表示を行うには、「カスタム・コンテンツ」ページを使用します。

カスタム・コンテンツ・リスト

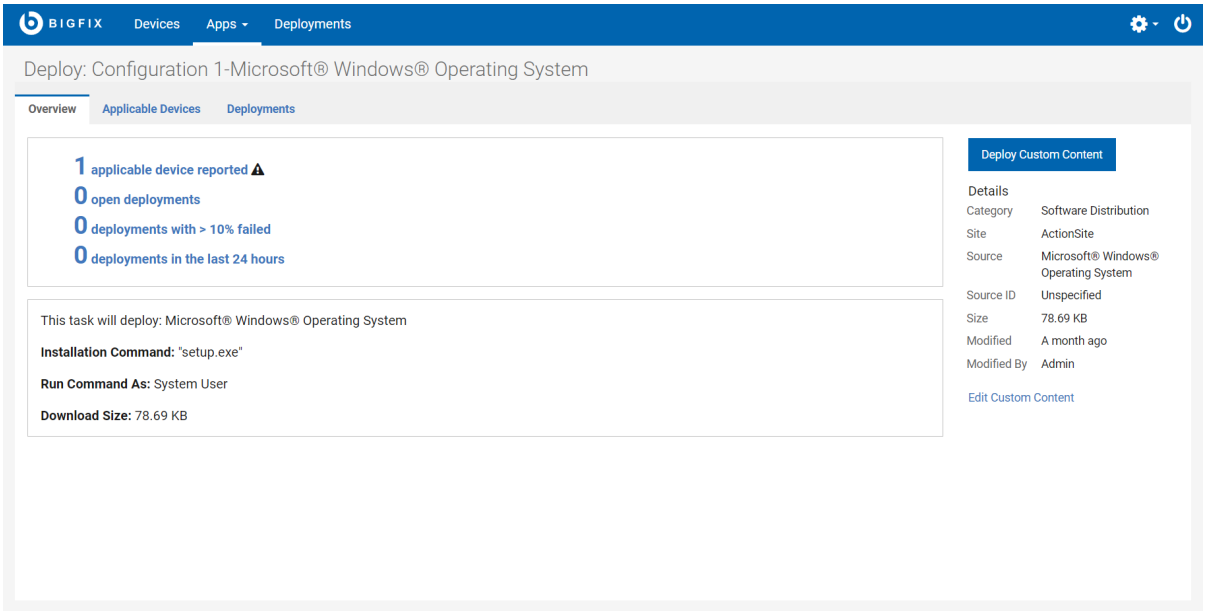
特定のタイプのコンテンツを表示するには、フィルターを使用します。タイトルをクリックして、コンテンツ文書を開きます。



共通カテゴリーには一般的に、インストール、構成、ソフトウェア配布、セキュリティーの更新、アンインストールが含まれています。サイト・フィルターは、特定のサイトに格納されたコンテンツを表示します。

カスタム・コンテンツ文書

カスタム・コンテンツの説明、適用可能なデバイスのリスト、およびデプロイメント履歴を確認するには、そのカスタム・コンテンツ名をクリックします。各リンクを使用して、関連付けられたビューで提供される詳細情報を確認します。



カスタム・コンテンツの各ビューは以下のとおりです。

- 概要 - カスタム・コンテンツの詳細な説明。
- 適用可能なデバイス - このコンテンツに適格であるマシン。
- デプロイメント - このコンテンツのデプロイメント・リスト。

カスタム・コンテンツに、例えばベースラインといった、複数アクションが含まれる場合、そのコンポーネントの名前が「概要」にリストされます。単一タスクとベースラインの違いについて詳しくは、用語集 (（ページ）　　)を参照してください。

カスタム・コンテンツの作成

「カスタム・コンテンツ」ウィザード画面を使用して、カスタム・コンテンツを作成します。

Web UI アプリケーションでは、適切な権限を持つオペレーターが新しい Fixlet コンテンツを Web UI 内に作成できます。オペレーターは、「カスタム・コンテンツの作成」ウィザードの必須フィールドに入力してカスタム・コンテンツを作成できます。「カスタム・コンテンツの作成」ウィザードの以下のフィールドは、カスタム・コンテンツの作成に必須のフィールドです。

- 名前: カスタム・コンテンツの名前を入力します。
- 関連度: 必要な関連度を入力します。
- アクション: アクション・スクリプトを入力します。
- 「サイト」: カスタム・コンテンツをデプロイするサイトを入力します。

注: すべてのフィールドが必須ではありませんが、必須以外のフィールドにも詳細を入力することをお勧めします。

カスタム・コンテンツの作成

- グローバル・ナビゲーションで「カスタム・コンテンツの作成」ページを開くには、ドロップダウンから**「アプリ」**>**「カスタム」**を選択し、**「カスタム・コンテンツの作成」**ボタンをクリックします。
- 「カスタム・コンテンツの作成」ウィザード画面で、名前を入力し、タスクの説明、関連度、アクションスクリプトを追加します。

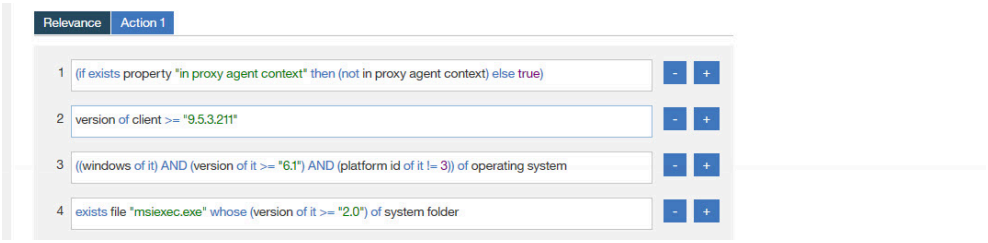
タスクの説明の追加

タスクの説明の追加は、リッチ・テキスト・フォーマット (RTF) エディターか HTML エディターを使用して行います。**「HTML エディターの使用/リッチ・テキスト・エディターの使用」**のリンクによって、これらが切り替わります。これらの 2 つのエディターは同期されていません。つまり、一方で行った変更は、他方に切り替えたときに複製されません。**「保存」**をクリックすると、アクティブなエディターのコンテンツが保存され、他のエディターで行った変更は失われます。

クロスサイト・スクリプティング攻撃から保護するために、リッチ・テキスト・エディターに入力されたテキストは、保存される前に検査されます。例えば、スタイル・タグとスクリプト・タグが削除され、URL やクラス/ID 値が変更または削除されることがあります。コンソールで作成されるコンテンツは HTML エディターで正しくレンダリングされても、リッチ・テキスト・エディターで正しくレンダリングされないこともあります。

タスクの関連度の追加

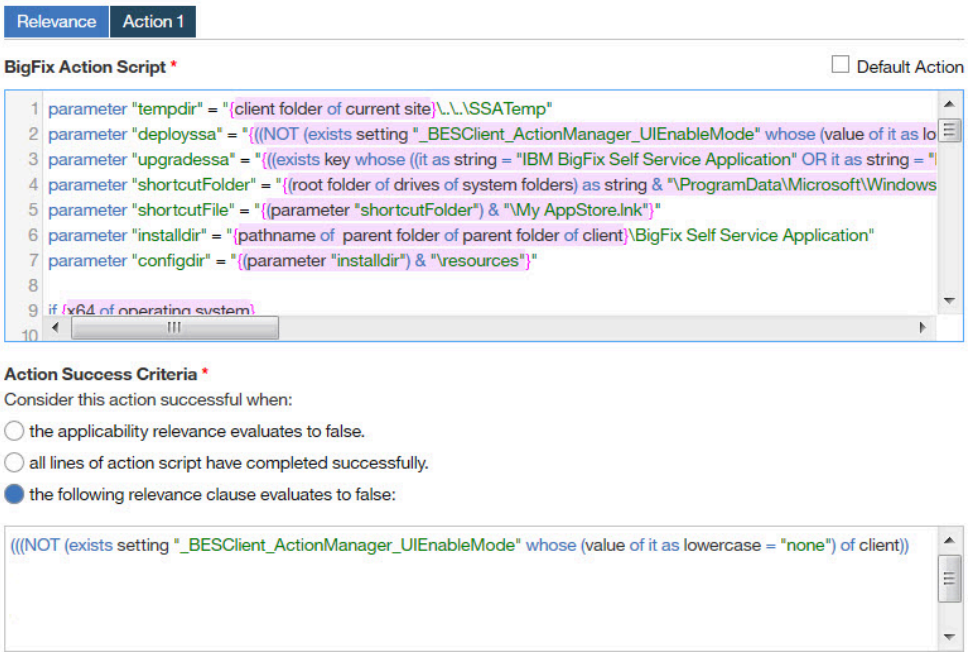
ボックス内に表示された「+」コントロールと「-」のコントロールをクリックして、句を挿入または削除します。タブ名の横のアスタリスクは、そのタブで変更が行われたことを示します。条件付き関連度のオプションを使用して BigFix コンソール内で作成された関連度に対してこのページで行われた変更は、関連句として引き続きコンソールに表示されます。



関連度の追加について詳しくは、「BigFix コンソール・オペレーター・ガイド」を参照してください。

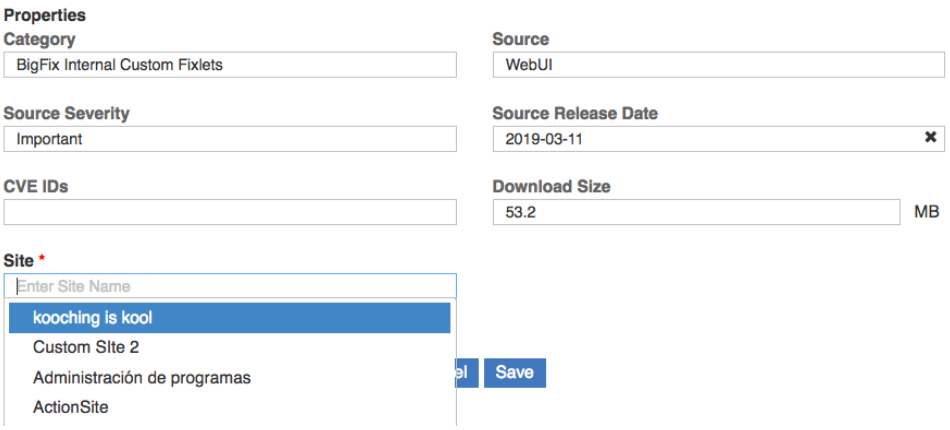
タスク・アクションの追加

「カスタム・コンテンツ・ウィザード」ページを使用してアクションを変更します。タブ名が太字のものがデフォルト・アクションです。このエディターを使用してアクションを追加または削除できません。



タスク・プロパティーの追加

「カスタム・コンテンツ・ウィザード」ページのプロパティー・フィールドを使用して、プロパティー情報を追加または変更します。タスクに適した情報を追加します。例えば、パッチ関連タスクの場合は Common Vulnerabilities and Exposures (CVE) ID などがあります。



- 「カテゴリー」- タスクのタイプ (パッチまたはソフトウェア配布など)。
- 「ダウンロード・サイズ」- タスクでファイルが配信される場合に使用 (ソフトウェアまたはパッチについて)。
- 「ソース」- 関連するファイルのソース (Microsoft からのパッチなど)。
- 「ソース・リリース日」- ソフトウェアまたはパッチがリリースされた日付。
- 「ソースの重大度」- パッチによって修正される問題に関連付けられたリスクのレベルについて記載されます。
- 「CVE ID」- パッチの CVE ID システム番号。
- サイト - カスタム・コンテンツは選択したサイトに保存されます。

重要: マスター以外のオペレーターは、自身のオペレーター・サイトと権限を持つカスタム・コンテンツ・サイトにのみ保存できます。

重要: マスター・オペレーターは、カスタム・サイトとマスター・アクション・サイトにのみ保存できます。

アイコンの追加 (オプション)

カスタム・コンテンツ・ウィザード画面では、カスタム・コンテンツに関連付けられたアイコンを追加できます。詳しくは、「カスタム・コンテンツの編集 (（ページ） *145)*」の「**アイコンの追加または変更**」セクションを参照してください。

カスタム・コンテンツの編集

カスタム・コンテンツの編集には、「タスクの編集」画面を使用します。

また、以下のことを行うことができます。

- アイコンの追加または変更。
- 関連度の編集 - 関連句の追加または削除。
- アクション・スクリプトの編集 - アクションと成功条件の追加または変更。
- タスクの削除。

「タスクの編集」ページへのリンクは、オペレーターがタスクを編集する権限を持つ場合にカスタム・コンテンツ文書とソフトウェア・パッケージ文書に表示されます。**「タスクの編集」**ページでは、現在 BigFix コンソールのフル編集機能が提供されていません。例えば、アクションを追加、スクリプト・タイプの変更、アクション設定ロックの追加の目的ではこのページを使用できません。ベースラインを編集するには BigFix コンソールを使用します。プロファイル管理アプリケーション内で作成されるタスクは、プロファイル管理アプリケーションを使用して編集する必要があります。

タスクの説明の編集

タスクの説明の編集は、リッチ・テキスト・フォーマット (RTF) エディターか HTML エディターを使用して行います。**「HTML エディターの使用/リッチ・テキスト・エディターの使用」**のリンクによって、これらが切り替わります。これらの 2 つのエディターは同期されていません。つまり、一方で行った変更は、他方に切り替えたときに複製されません。**「保存」**をクリックすると、アクティブなエディターのコンテンツが保存され、他のエディターで行った変更は失われます。

クロスサイト・スクリプティング攻撃から保護するために、リッチ・テキスト・エディターに入力されたテキストは、保存される前に検査されます。例えば、スタイル・タグとスクリプト・タグが削除され、URL やクラス/ID 値が変更または削除されることがあります。コンソールで作成されるコンテンツは HTML エディターで正しくレンダリングされても、リッチ・テキスト・エディターで正しくレンダリングされないこともあります。

タスクの関連度の編集

「タスクの編集」ページのエディターを使用して、関連度を編集します。ボックス内に表示された**「+」**コントロールと**「-」**のコントロールをクリックして、句を挿入または削除します。タブ名の横のアスタリスクは、そのタブで変更が行われたことを示します。条件付き関連度のオプションを使用して BigFix コンソール内で作成された関連度に対してこのページで行われた変更は、関連句として引き続きコンソールに表示されます。

関連度の編集について詳しくは、『BigFix コンソール・オペレーター・ガイド』を参照してください。

タスク・アクションの編集

「タスクの編集」ページのエディターを使用して、アクションを変更します。タブ名が太字のものがデフォルト・アクションです。このエディターを使用してアクションを追加または削除できません。

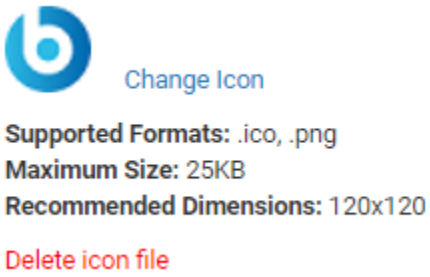
タスク・プロパティーの編集

「タスクの編集」ページのプロパティー・フィールドを使用して、プロパティー情報を追加または変更します。タスクに適した情報を追加します。例えば、パッチ関連タスクの場合は Common Vulnerabilities and Exposures (CVE) ID などがあります。

- 「カテゴリー」- タスクのタイプ (パッチまたはソフトウェア配布など)。
- 「ダウンロード・サイズ」- タスクでファイルが配信される場合に使用 (ソフトウェアまたはパッチについて)。
- 「ソース」- 関連するファイルのソース (Microsoft からのパッチなど)。
- 「ソース・リリース日」- ソフトウェアまたはパッチがリリースされた日付。
- 「ソースの重大度」- パッチによって修正される問題に関連付けられたリスクのレベルについて記載されます。
- 「CVE ID」- パッチの CVE ID システム番号。

アイコンの追加または変更

「タスクの編集」画面では、カスタム・コンテンツに関連付けられたアイコンを追加または変更できます。



注: 他のアプリケーション (SSAなど) では、アイコン形式に関しては要件がより厳しい場合があります。特定のアプリケーションでカスタム・コンテンツを使用する必要がある場合は、アプリケーションのドキュメントを参照してください。

第 9 章. BigFix Query 入門

BigFix Query 機能を使用して、エンドポイントから専用の照会チャネル経由でデータを取得します。この場合、各リレーの使用可能なメモリーは標準の BigFix 処理への影響を最小限に抑えます。

BigFix Query を使用すると、以下のことを行えます。

- 個別のコンピューター、マニュアル・コンピューター・グループ、動的コンピューター・グループを照会する
- 関連度を作成し、照会の作成に使用する
- BES サイトから関連度を検索する
- コンテンツを開発時、関連式をテストする
- 照会結果をコンマ区切り値 (CSV) ファイルにエクスポートする
- カスタム照会のライブラリーを作成し、コレクションは非公開のままにするか、他のユーザーと共有する

ユーザーおよび役割

マスター・オペレーターは照会をホストするカスタム・サイトを作成し、BigFix Query オペレーターとコンテンツ作成者へのアクセス権を割り当てます。これにより、コンテンツ作成者はカスタム・サイトに照会を保存し、照会をカテゴリーごとにグループ化し、オペレーターが照会を使用できるようにします。

コンテンツ作成者

コンテンツ作成者は BigFix Query を使用して以下のタスクを実行できます。

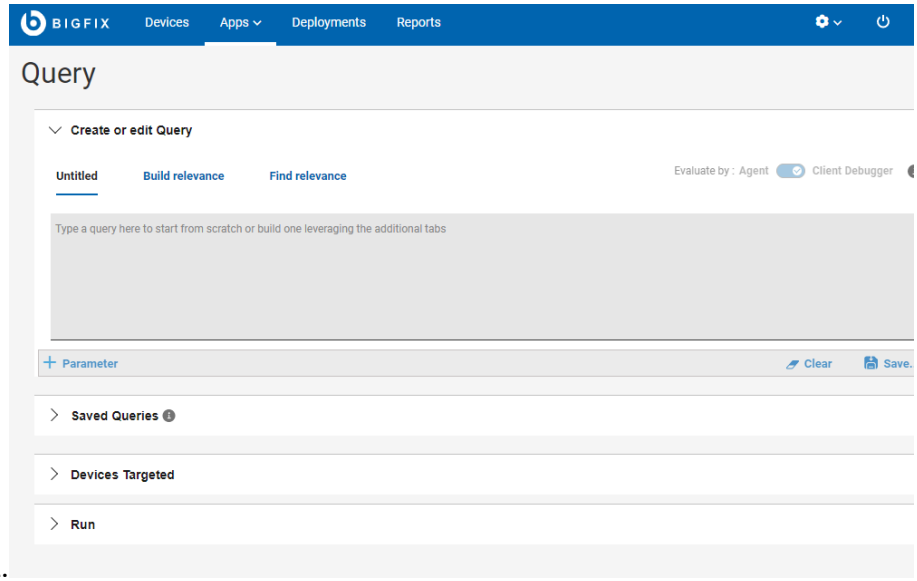
- システムとローカル照会を選択または選択解除して、照会をフィルターする
- オペレーター・サイトでサンプル照会のロード、非表示、削除、再ロードを実行する
- 照会をカスタマイズし、独自の照会を作成する
- 関連度を作成し、照会の作成に使用する
- BES サイトから関連度を検索する

- 新しいサイトに、または新しい名前で照会を保存し、オペレーターがその照会にアクセスできるようにする
- 対象デバイスを選択およびフィルターして照会を実行する
- **「表示の実行に切り替え」**をクリックして照会の関連式で使用されるパラメーター値を入力する
- 照会結果を参照し、結果を `.csv` ファイルに保存する
- 照会結果からデバイス文書を開き、調査するか、フィックスを適用する
- 照会を実行しエージェントまたはローカルの QnA による評価を行うように設定する
- 収集する照会結果のデフォルトのタイムアウト値を変更する
- 最後に実行された 5 件の照会の結果を結果タブに表示する

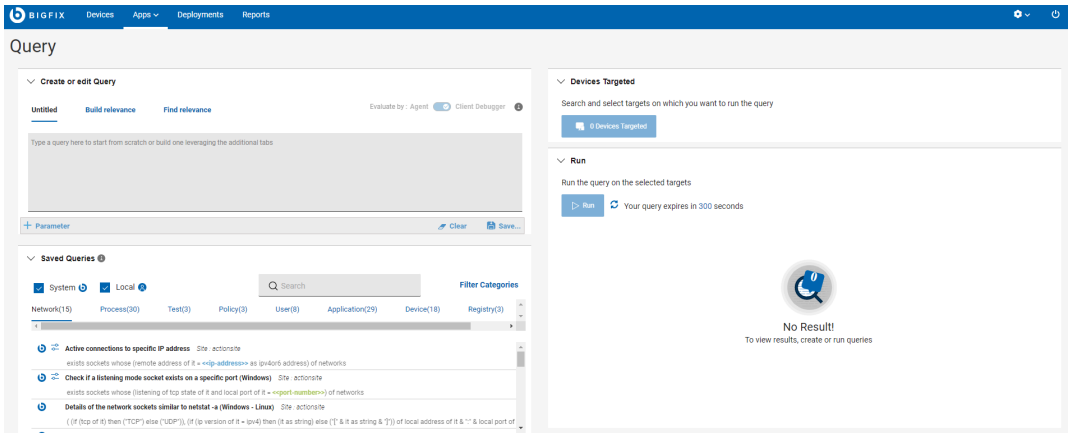
照会アプリの解像度は、1024 x 768 (最小) ～ 1920 x 1080 (最大) です。以下は、コンテンツ作成者またはマスター・オペレーターの、各解像度での照会エディターのメイン・ページの例です。

解像度 1024 x 768

図

2. 

解像度 1920 x 1080



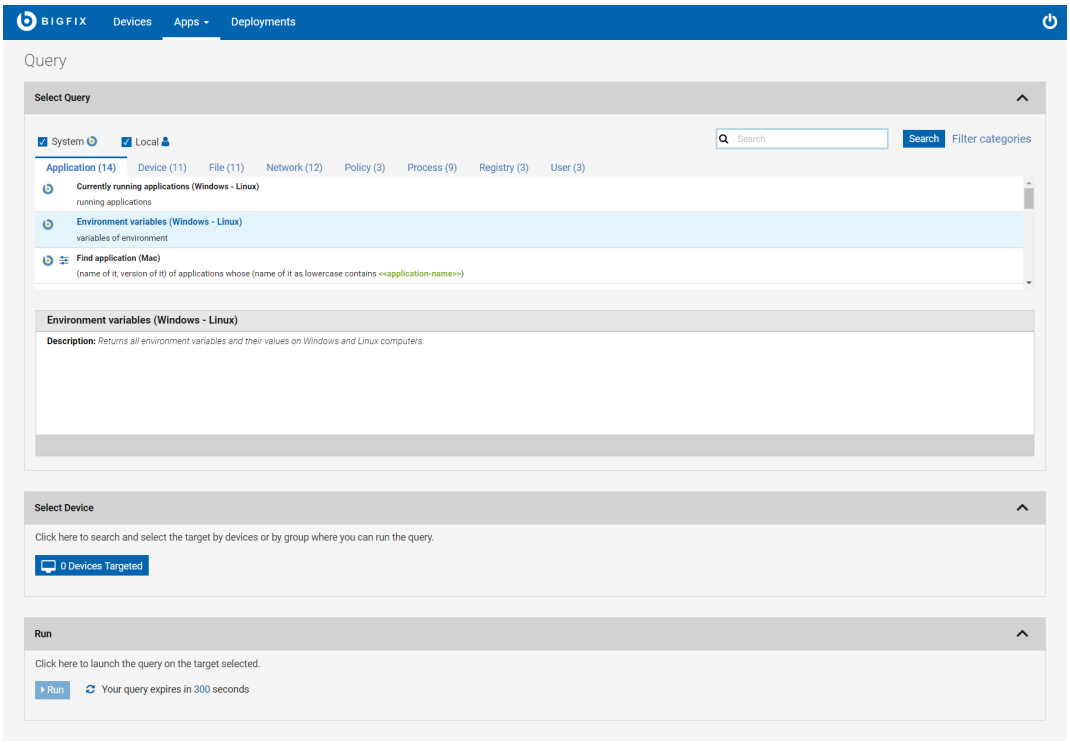
オペレーター

オペレーターは BigFix Query を使用して以下のタスクを実行できます。

- コンテンツ作成者が共有している照会を参照する
- 照会をフィルター、検索、選択する
- 照会の説明を参照する
- 対象デバイスをフィルター、選択する
- 照会を実行する
- 照会を実行しエージェントまたはローカルの QnA による評価を行うように設定する
- 照会の関連式で使用されるパラメーター値を入力する
- 最後に実行された 5 件の照会の結果を結果タブに表示する
- 収集する照会結果のデフォルトのタイムアウト値を変更する
- 照会結果を参照し、必要な権限があれば結果を CSV ファイルに保存する
- 照会結果からデバイス文書を開き、調査するか、フィックスを適用する

オペレーターは照会の作成または削除はできません。また関連式を参照することもできません。

次の画像は、マスター以外のオペレーターのメインの「照会」編集ページを示しています。

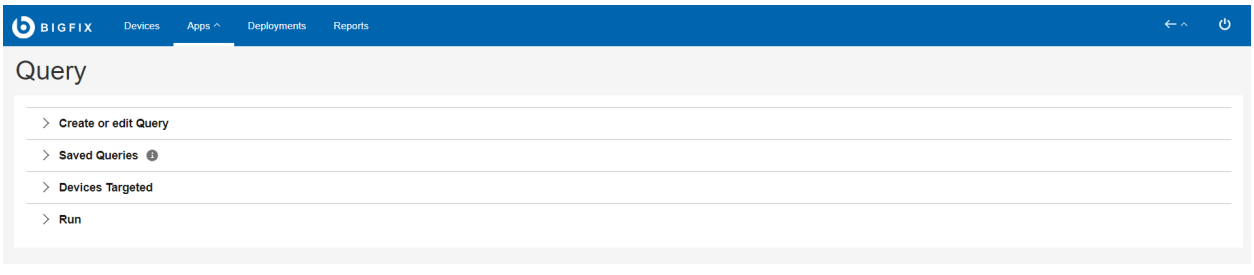


エディターとカスタム照会の使用方法についての詳細は、照会の作成 (（ページ） 160)を参照してください。

BigFix Query を使用できる各種タイプのユーザーについては、BigFix Query の権限 (（ページ）)を参照してください。

アコーディオンについて

BigFix Query ページのセクションは、デバイスからデータを取得するタスクがより把握できるようアコーディオンで整理されています。拡大または縮小で表示方法を変更します。



- **照会の作成または編集**: このセクションでは、照会の参照、編集、作成ができます。このセクションには、以下のタブがあります。
  - タイトルなしタブ (（ページ） *163)*
  - 関連度の作成 (（ページ） *165)*
  - 関連度の検索 (（ページ） *179)*
- **保存された照会**: このセクションでは、保存されたローカルの照会とカスタムの照会を確認できます。BigFix で用意されたすべての照会 (システム照会) と、オペレーターが保存した照会 (ローカル照会) が表示されます。関連コンテンツ全般を検索するには、関連度の検索 (（ページ） *179)* タブで検索を実行します。
  - システム
  - ローカル
  - 照会タイプ別にフィルタリング (システムまたはローカル)
  - Search (検索)
  - カテゴリーのフィルタリングによる検索結果の絞り込み
- **デバイスを対象として設定**: このセクションでは、ターゲット/エンドポイントの選択ができます。このセクションの 「デバイスを対象として設定」ボタンを有効にするには、ターゲットで実行する照会を選択します。「デバイスを対象として設定」ボタンをクリックし、ターゲット・デバイスを選択します。デバイスのデータがグリッドで表示されます。このグリッドで使用可能なフィルターと検索オプションを使用し、識別されたデバイスから必要なものを選択して照会を実行できます。
  - デバイス別にターゲット設定する
  - グループ別にターゲット設定する

注: 照会の要求に応答できるのは、BigFix アイコン が表示されているデバイスのみです。

- **実行**: このセクションでは、選択したターゲットで照会を実行 (（ページ） *156)*できます。取得結果はグリッドで表示されます。このセクションの「実行」ボタンを有効にするには、照会とターゲット・デバイスを選択します。

検索について

「検索」機能を使用すると、照会を検索できます。

基本の検索を行うには、検索するストリングを入力し、**「Enter」**をクリックします。これで照会のタイトルに指定のストリングを含む照会のリストがハイライトで表示されます。

注: 「id」、「start」、「false」などの検索文字列を使用して深い検索を行うと、検索は タグの属性にも基づくため、検索結果にはパラメーターを含むすべての照会が含まれます。

フィルターについて

照会結果は、作成タイプやカテゴリーに基づいてフィルタリングすることもできます。

作成タイプに基づくフィルタリング:

- **「システム」**チェック・ボックスを選択すると、データベースからロードされるサンプル照会のみが表示されます。
- **「ローカル」**チェック・ボックスを選択すると、カスタム照会のみが表示されます。

注:

- サンプル照会とカスタム照会両方を表示するには、**「システム」**と**「ローカル」**チェック・ボックス両方を選択します。
- **「システム」**と**「ローカル」**チェック・ボックス両方をクリアした場合、照会アプリはサンプル照会とカスタム照会両方を表示します。

カテゴリーに基づくフィルタリング:

1. 検索ストリングを入力し、**「フィルター・カテゴリー」**をクリックします。
2. リストからカテゴリーを選択し、検索結果を絞り込みます。

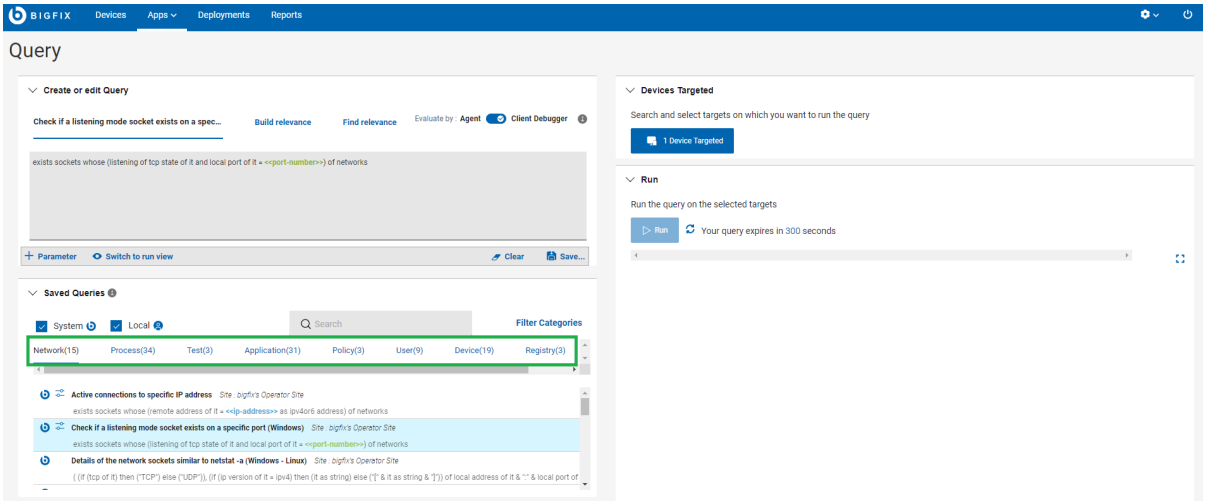
   注: すべてのカテゴリーはデフォルトで選択されます。検索結果を絞り込むには、必要のないカテゴリーのチェック・ボックスをクリアします。

3. **「保存」**をクリックして、今後の検索のために選択結果を保存します。

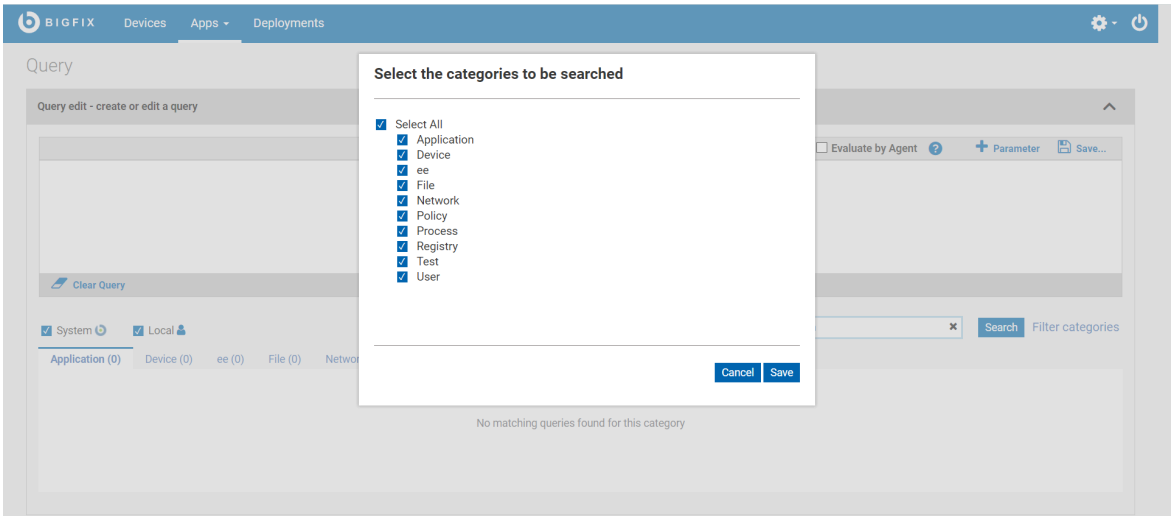
照会のタイトル、関連式、またはその両方に指定のストリングを含む照会のリストが表示されます。

カテゴリーについて

カテゴリーを使って、コンテンツ作成者はニーズに基づき照会をグループ化できます。コンテンツ作成者は、カテゴリーの作成、カテゴリーへのデータの取り込み、カテゴリーの削除を実行できます。オペレーターはカテゴリーの表示または非表示のみ操作できます。



- カテゴリータブはアルファベット順で左から右に、1 行ずつ表示されます。照会のタイトルは、カテゴリーごとにアルファベット順にリストされます。
- 各照会は少なくとも 1 つのカテゴリーに保存する必要があり、各カテゴリーには異なるサイトでホストされる照会を含められます。
- カテゴリーを削除するには、コンテンツ作成者がそのカテゴリー内の照会をすべて削除する必要があります。
- カテゴリーを作成するには、コンテンツ作成者は照会を保存する際に、カテゴリー名を指定する必要があります。
- カテゴリーで照会をフィルターするには、「フィルター・カテゴリー」をクリックし、求めるカテゴリーを選択し、「保存」をクリックします。選択したカテゴリーに関連する照会のみ表示されます。



照会とサイトについて

それぞれの照会はそのタイトルと照会をホストしているサイト名の組み合わせで、一意に識別されます。この 2 つの値のどちらかを変更した場合、照会のコピーが自動的に作成されます。照会のコピーを別のサイト内に作成した場合、その後の更新は各コピーに個別に適用する必要があります。

照会を保存できるのは、マスター・オペレーターによって割り当てられたアクセス可能なサイトのみです。こういったサイトは次のいずれかに当てはまります。

- マスター・オペレーターが作成し、オペレーターに共有しているカスタム・サイト。
- オペレーター・サイト (コンテンツ作成者がマスター・オペレーターでない場合)。

注: 既存の照会は BigFix Query の現行リリースには自動的にはインポートされません。ただし、これらの照会は引き続きダッシュボード変数として使用できます。https://developer.bigfix.com/rest-api/api/dashboardvariable.htmlページで説明されているように、REST API ダッシュボード変数リソースを使用してアクセスできます。

BigFix Query 詳細については、以下のリンクを参照してください。

- BigFix Query の使用によるクライアント情報の取得
- BigFix Query の要件
- BigFix Query の制約事項
- BigFix Query を使用できるユーザー
- WebUI からの BigFix Query の実行方法
- BigFix による BigFix Query リクエストの管理方法

サンプル照会の実行

システム照会は BigFix アイコンでマークが付けられているサンプル照会です。コンテンツ作成者は、オペレーター・サイトでのサンプル照会のロード、非表示、削除、再ロードを実行できます。

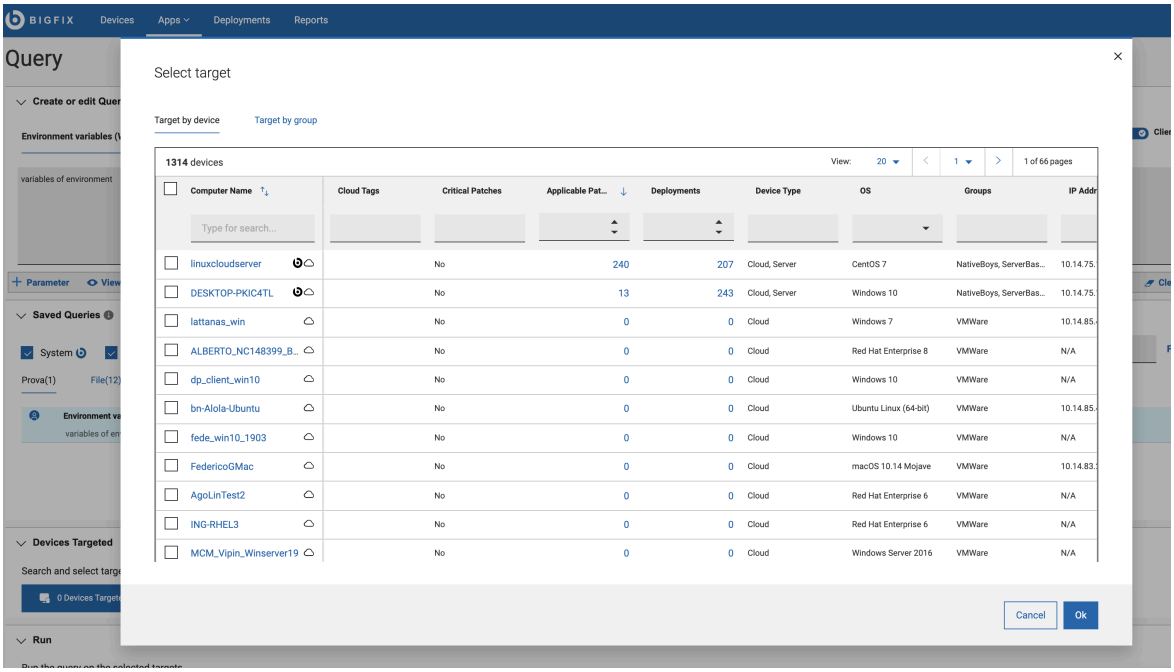
サンプル照会は BigFix から提供され、アプリケーション、ファイル、デバイス、ネットワーク、プロセス、レジストリー、ポリシー、ユーザーに特化しています。

注: 複数のコンテンツ作成者が、同じ名前とカテゴリーを持つ照会を別のサイトに保存した場合、アプリケーションによって照会の複数のインスタンスが作成されます。

サンプル照会を実行するには、以下の手順を実行します。

1. 「カテゴリー」 (（ページ） *154)*タブをクリックします。
2. 照会リストから照会を選択して、エディターに表示します。検索およびフィルター機能を使用して、特定の照会を見つけることもできます。

3. 照会にパラメーターがある場合、パラメーター値を入力するか、デフォルト値を受け入れます (デフォルト値が指定されている場合)。実行時にパラメーター値を指定するには「オペレーター・ビュー」を使用する必要があります。詳しくは、「照会のパラメーターの管理 ((ページ) 182)」を参照してください。
4. **「デバイスを対象として設定」**セクションで、**「デバイスを対象として設定」**をクリックして対象リストを開きます。表示する対象リストを選択するには、**「デバイス別ターゲット」**または**「グループ別ターゲット」**をクリックします。

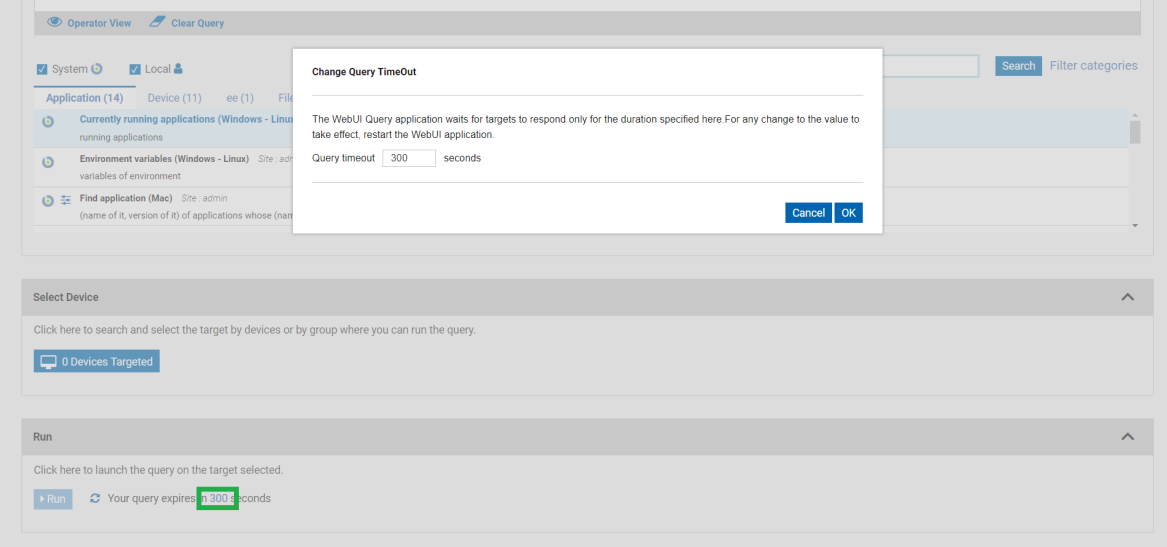


5. 照会を実行する対象デバイスを 1 つ以上選択します。
   - 個々のデバイスまたはグループを選択できます。対象は、ユーザーの権限ごとにリスト表示されます。マスター・オペレーターには、すべてのデバイスおよびグループが表示されます。マスター以外のオペレーターには、完全なリストのサブセットが表示される可能性があります。ソート、検索、フィルタリング ((ページ) 2)機能を使用すると、対象デバイスをすばやく見つけることができます。
     - 特定のデバイスまたはグループを探すには、名前列の**「検索」**フィールドに名前を入力します。
     - フィルターを使用して、特定のプロパティーを持つデバイスを見つけます。

デバイスまたはグループの選択が完了したら、**「OK」**をクリックして、エディターに戻ります。**「対象デバイス」**ボタンに、選択したデバイスの合計数が表示されます。

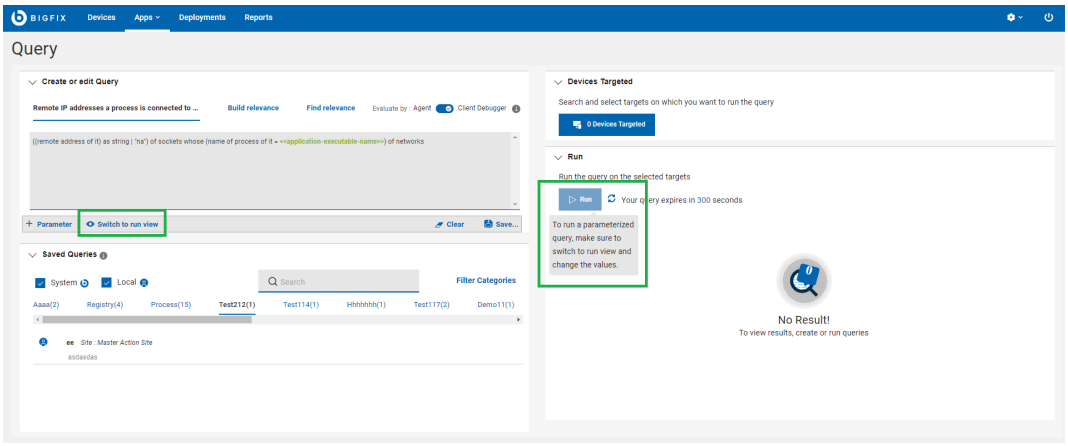
注: 照会と対象を組み合わせる際は、簡潔かつ範囲が限定されている照会が最も効率的であることを考慮してください。範囲の広い照会は大規模なデータ・セットを返し、より多くのリソースを使用するため、クエリのパフォーマンスに影響を与えます。

6. サーバーが結果を取り出すのにかかるポーリング時間に制限をかけるには、照会タイムアウトを設定します。デフォルト時間は 300 秒で、最大制限は 900 秒です。デフォルト時間を変更するには、デフォルト時間のリンクをクリックし、**「照会タイムアウトの変更」**ポップアップに必要な秒数を入力します。より広範囲な照会では、指定されたポーリング時間に到達するとサーバーは結果のポーリングを停止します。



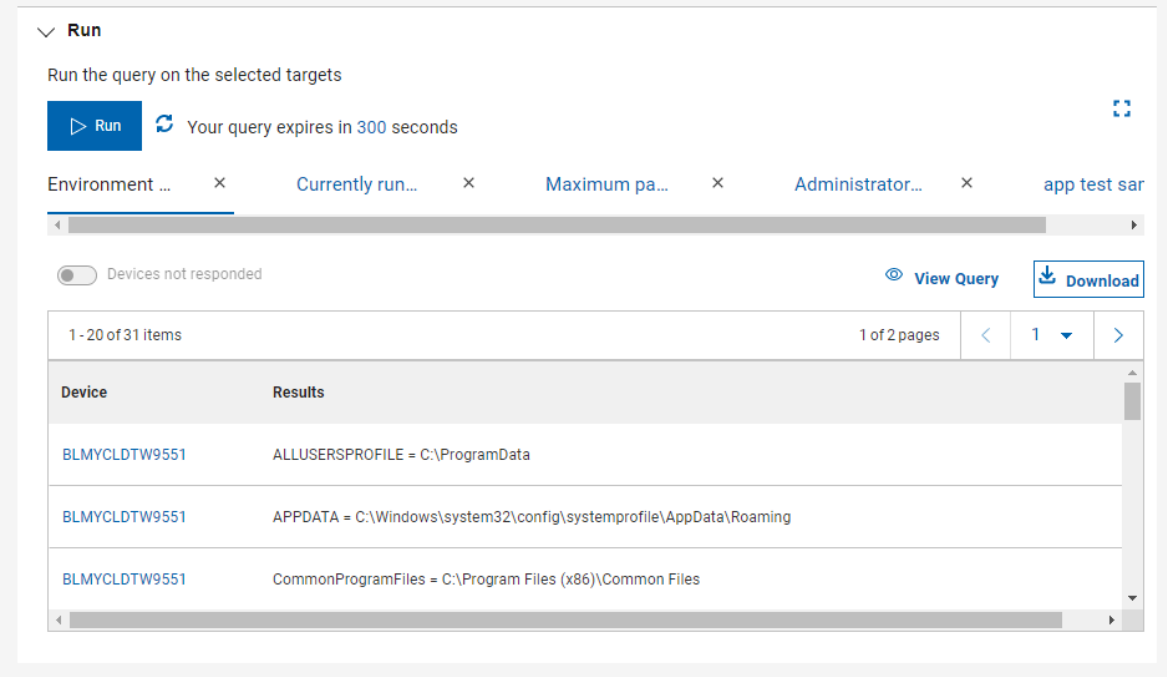
7. 照会を実行するには、**「実行」**をクリックします。照会をキャンセルするには、結果のロード中にキャンセルできます。

注: パラメーター化された照会を実行するには、必ず実行ビューに切り替えて値を変更してくださ



い。

8. 結果を確認します。デバイスはリアルタイムに報告され、設定された制限時間内にクライアントが報告すると、新着がリストに追加されます。



- フルスクリーン・モードに切り替えて、結果をさらに表示するには、**「展開」**アイコンをクリックします。アイコンを再度クリックするか、**Esc** キーを押すと、フルスクリーン・モードが終了します。
- リストの左隅に、行の総数と、これまでに報告されたデバイスの数が表示されます。
- 結果ページの総数を表示し、ページ番号を選択するか、< 前へ > および <次へ> のナビゲーション・ボタンを使用してページ間を移動できます。
- 最近実行した 5 つの照会のレポートを表示できます。照会の詳細を表示するには、「 View Query 」のアイコンをクリックします。
- レポートを選択し、**「ダウンロード」**ボタンをクリックして、レポートを `.csv` ファイルとしてダウンロードします。
- 時計のアイコンをクリックすると、最近実行した 10 件の照会のタイトルが表示されます。
- 結果をコンマ区切り値 (.csv) 形式でファイルに保存するには、**「ダウンロード」**ボタンをクリックします。

照会の作成

ローカル/カスタム照会の操作コンテンツ作成者により作成された照会は、ローカル/カスタム照会として、オペレーター・アイコンでマークが付けられています。コンテンツ作成者は、オペレーター・サイトでローカル照会の作成、ロード、非表示、削除、再ロードを実行できます。

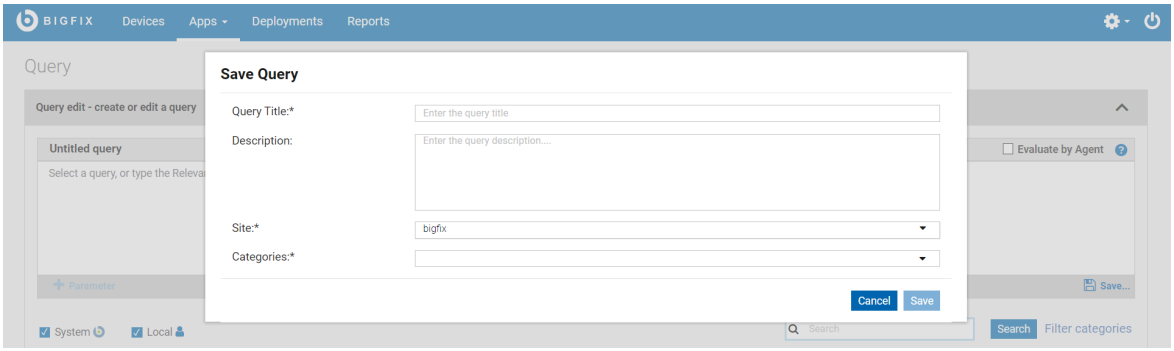
照会の作成または編集

コンテンツ作成者は、新規照会を以下の方法で作成できます。

- 関連度の作成 (（ページ） *165)* タブで関連式を作成し、照会として保存します。
- 関連度の検索 (（ページ） *179)* タブで既存の関連式を検索し、 の照会エディターで使用します。 タイトルなしタブ (（ページ） *163)*
- 照会エディターで関連式を入力し、保存します。
- 既存の照会のコピーを作成し、必要に応じて編集し、別の名前で保存するか、別の場所に保存します。

照会を作成または編集するには:

1. タイトルなしタブ (（ページ） *163)*で、「ビューの編集」 (（ページ） *149)*モードになっていることを確認します。
2. 照会エディターに関連式を入力します。
   a. 既存の照会を編集するには、カテゴリーの下にある希望する照会を選択します。これにより、エディターに照会のタイトルと関連式が表示され、それを編集できます。**「照会のクリア」**をクリックして、新しく関連式を入力することもできます。
   b. 関連度の作成 (（ページ） *165)*タブから関連式を作成するか、 関連度の検索 (（ページ） *179)*タブから既存の関連式を検索し、照会エディターにコピーして貼り付けることができます。
3. 必要に応じて、パラメーターを関連式に追加します。パラメーターについて詳しくは、以下を参照してください。 照会のパラメーターの管理 (（ページ） *182)*
4. **「保存」**をクリックします。



   a. 照会を説明するタイトルを入力します。

> **注:** 照会タイトルの推奨文字数は、最大 23 文字です。照会タイトルがそれより長い場合、タイトル・タブでの表示が一部切り捨てられます。

   b. アクセスが許可されており、照会をホストするサイトを選択します。
   c. 照会に対して少なくとも 1 つのカテゴリーを指定します。

- 複数のカテゴリーを指定した場合、照会は指定されたすべてのカテゴリーに表示されます。
- 「カテゴリー」フィールドに新規名を入力すると、新規カテゴリーが作成されます。

d. **「保存」**をクリックします。

注:

- 照会エディターでの関連式の作成は、Relevance language を使った BigFix コンソールでの Fixlets 作成に似ています。照会の作成に際しては、Relevance language に対する知識を有していることが推奨されます。Relevance language について詳しくは、「BigFix Developer」を参照してください。ただし、Relevance language について十分な知識がない場合でも、関連度の作成 (（ページ） *165)*タブでフィルターを正しく使用すれば関連式は作成可能です。
- 適用範囲が制限されている簡潔な照会が最も効率的に実行されます。大規模なデータ・セットを返す、対象範囲の広い照会は、多くのリソースを消費し、パフォーマンスに影響します。コンソール内での効率の悪い関連度に関する問題が、照会エディターでも発生する可能性があります。

既存の照会のコピーの作成

照会はそのタイトルと保存されているサイトによって一意的に識別されます。照会のコピーを作成するには、照会のタイトルまたはサイトを変更します。

注: 複数のコンテンツ作成者が同じ名前とカテゴリーを持つ照会を別のサイトに保存した場合、マスター・オペレーターにはカテゴリーの下に同じ照会の複数のインスタンスが表示される場合があります。

照会を最後に編集したユーザーを表示するには、照会のオペレーター・アイコンにカーソルを合わせます。

照会の削除

照会を削除するには、照会を選択して、その隣にある**「照会の削除」**アイコンをクリックします。

注:

- オペレーターは照会を削除できません。
- マスター・オペレーター/コンテンツ作成者はカスタム照会のみ削除でき、システム照会は削除できません。

クライアントのコンテキストの使用

コンテンツ作成者は**「エージェントによる評価」**フラグを有効化することによって、特定の照会を保存し、クライアントのコンテキストを使用できます。**「エージェントによる評価」**フラグを有効にして照会を実行することによって、クライアントからの正確なデータ取得につながります。

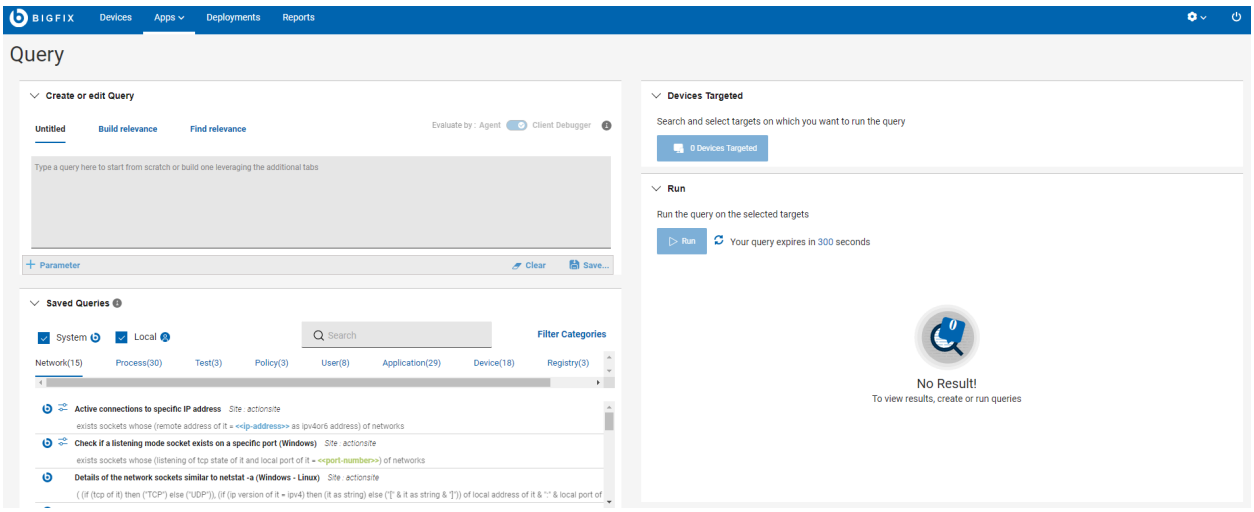
デフォルトでは、照会はクライアント・デバッガーによって評価されます。これは、`_WebUIAppEnv_USE_CLIENT_CONTEXT` クライアント設定で変更できます。この設定が 1 となっている場合、**「エージェントによる評価」**フラグは有効化されています。各照会の値を上書きできるのは、コンテンツ作成者のみです。**「エージェントによる評価」**フラグを有効化し、個別の照会を保存できます。これによりオペレーターはクライアントのコンテキストを使用できるようになります。

注: 「エージェントによる評価」フラグは BigFix プラットフォームのバージョン 9.5.13 以降でのみ使用できます。

タイトルなしタブ

Query アプリにログインすると、最初の表示は次のようになります。照会を選択していない場合、「照会の作成または編集」セクションのタブは、タイトルなしタブとして表示されます。保存された照会を選択すると、このタブには選択した照会のタイトルが表示されます。

注: 「照会」タブのレイアウトはデバイスの解像度に応じて異なります。サポートされている解像度について詳しくは、 こちらのリンク ((ページ)　　)を参照してください。

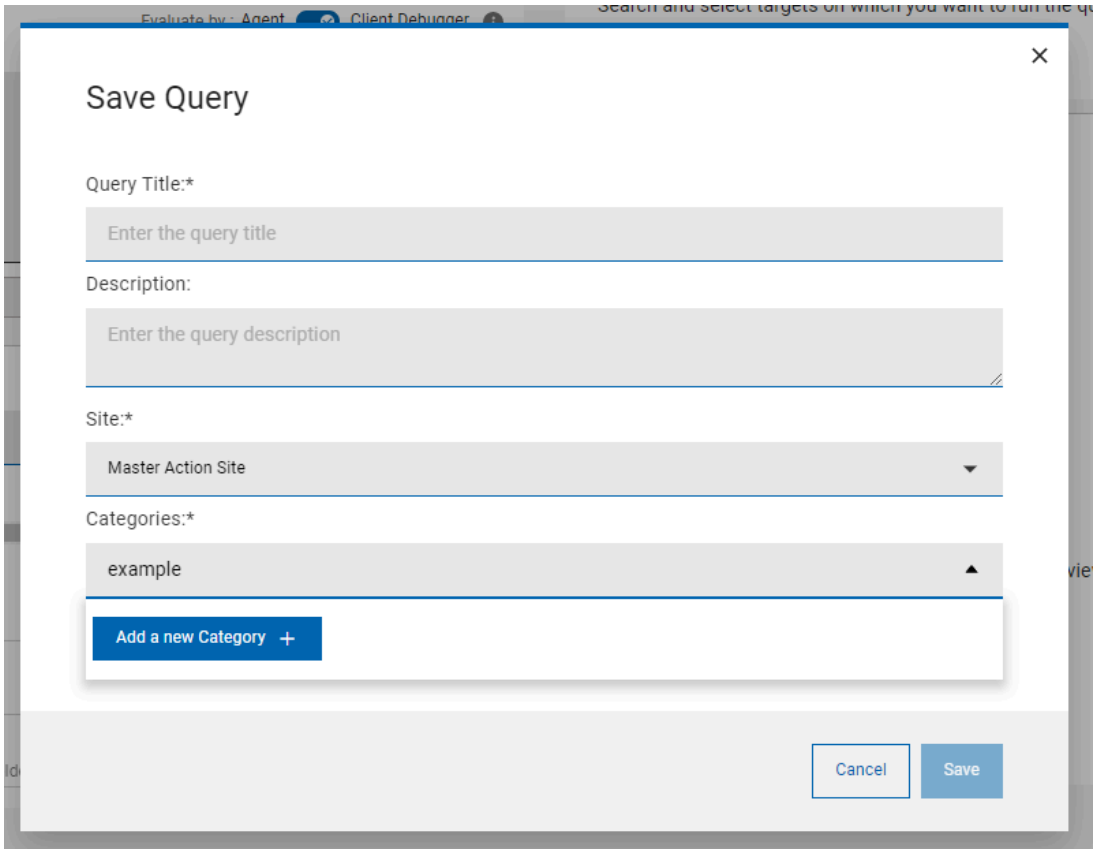


管理者やマスター・オペレーター、またはコンテンツ作成者としてログインした場合、このタブでは以下の機能が表示されます。

- **パラメーター**: 照会にパラメーターを追加するには、このボタンをクリックします。パラメーターの管理に関する詳細は、「照会のパラメーターの管理 ((ページ) 182)」を参照してください。
- **表示**: これは「オペレーター・ビュー」と「ビューの編集」を切り替えるときに役立つ切り替えボタンです。管理者がパラメーター化された照会を実行して、照会にパラメーターの値を入力する場合、管理者は「オペレーター・ビュー」に切り替える必要があります。
- **クリア**: 照会エディターで関連度ステートメントをクリアするには、このボタンをクリックします。
- **保存**: 新しい照会を保存するか、既存の照会の更新を保存するには、このボタンをクリックします。新しい照会を保存するときは、次のフィールドへの入力を求められます。
    - 照会のタイトル。
    - 説明

◦ サイト

◦ カテゴリー。新しいカテゴリーを作成するには**「新しいカテゴリーの追加」**ボタンをクリックします。



- **評価者: エージェント・クライアント・デバッガー** ((ページ) *163*): **「エージェントにより評価」**フラグを有効にして照会を実行することによって、クライアントからの正確なデータ取得につながります。
- **編集**: 「オペレーター・ビュー」に切り替えているときに、このボタンをクリックすると「編集」ビューに戻ります。

オペレーターとしてログインした場合、照会の説明のみを表示でき、関連式は表示できません。また、上記のボタンは無効になっています。オペレーターとしてパラメーター化された照会を実行する場合は、このタブからパラメーターの値を入力できます。

関連度の作成

コンテンツ作成者は、照会アプリの 「関連度の作成」タブで簡単に関連式を作成できます。

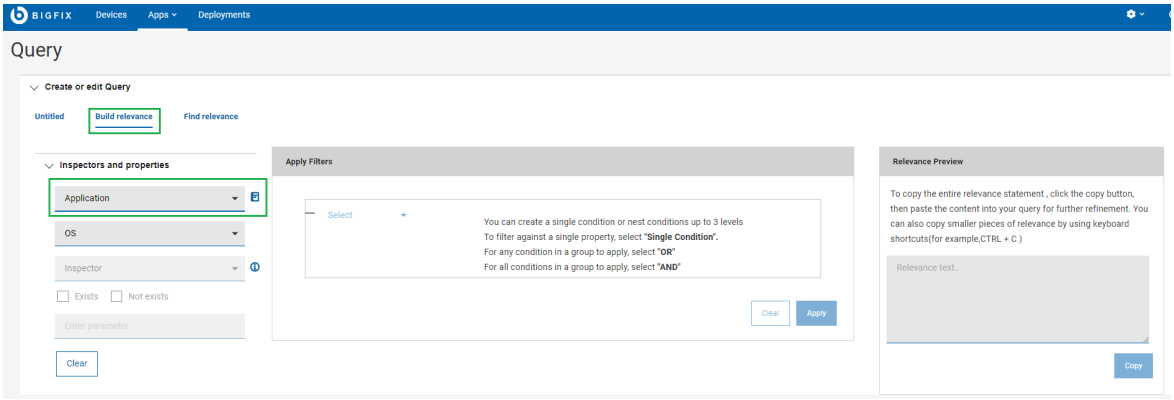
インスペクターとプロパティーを選択してフィルターを適用すると、関連式を作成できます。「コピー」をクリックしてこの関連式をコピーし、照会エディターに貼り付けると、新しい照会を作成できます。

関連式の作成

注: ご使用のデバイスの解像度によっては、照会タブのレイアウトが異なる場合があります。サポートされている解像度について詳しくは、 こちらのリンク ((ページ) *148)*を参照してください。

「関連度の作成」タブから関連式を作成するには、以下の手順を実行します。

1. WebUI のメイン・ページから、**「アプリケーション」 > 「照会」**をクリックします。
2. **「照会の作成または編集」** セクションで、**「関連度の作成」**をクリックします。
3. **「インスペクターとプロパティー」**セクションで、以下の手順を実行します。



a. 最初のドロップダウンから、インスペクターのタイプを選択します。

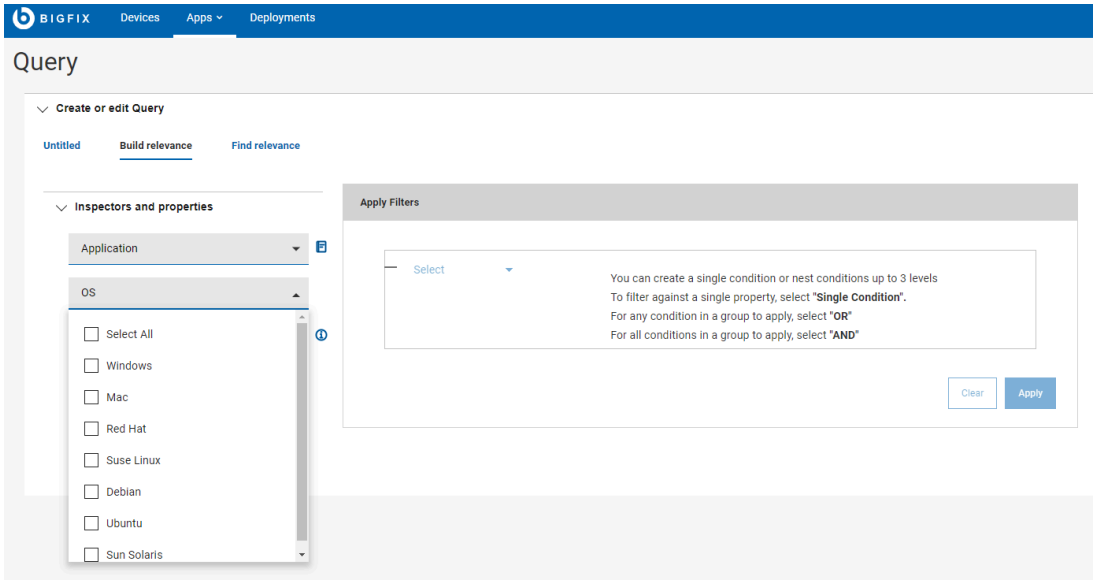
インスペクターについて詳しくは、 アイコンをクリックしてください。関連式を作成する際のインスペクターの意味について理解できます。

現在サポートされているインスペクター・タイプ:

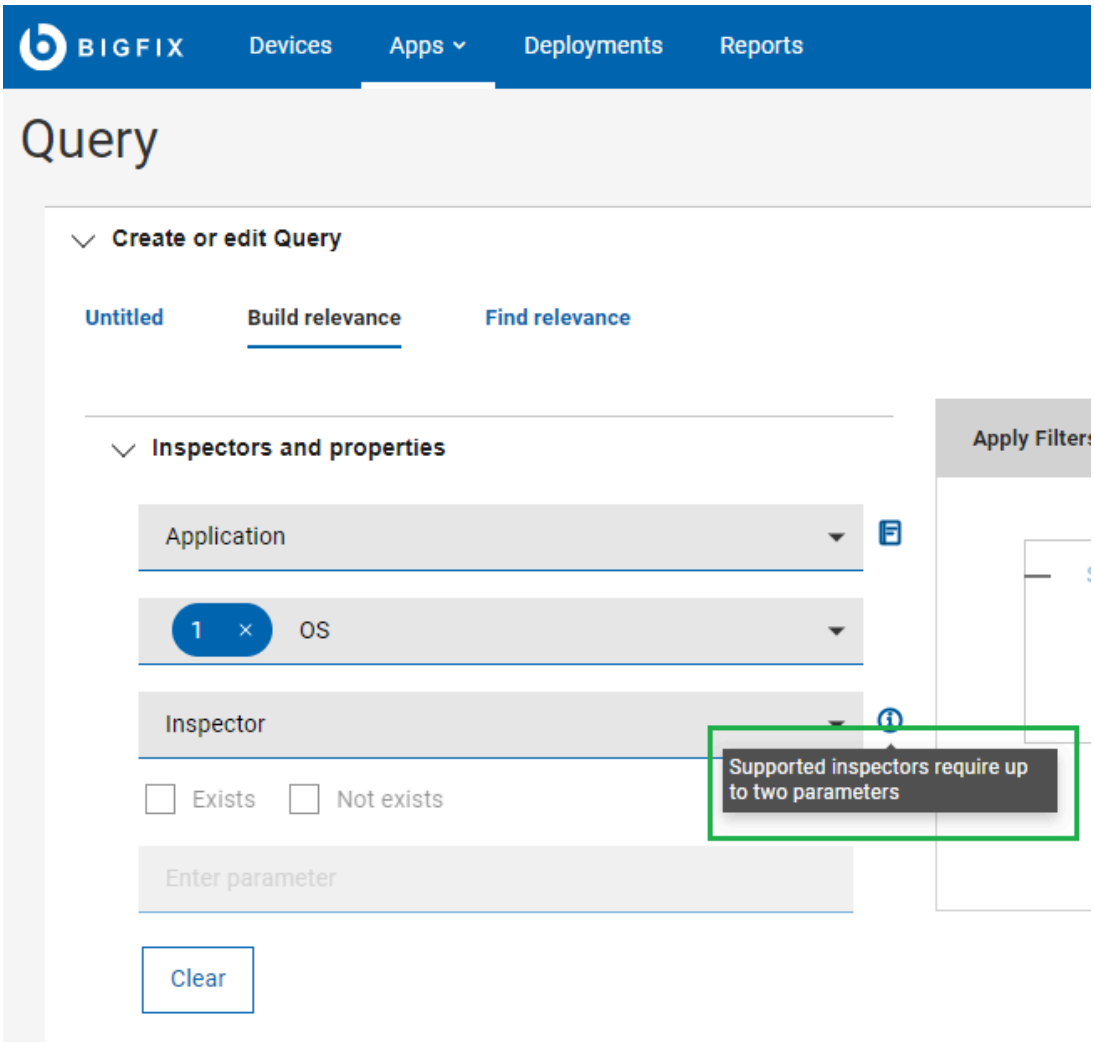
- アクティブなデバイス
- アプリケーション
- ドライブ
- ファイル

- フォルダー
- 言語
- ネットワーク IP インターフェース
- オペレーティング・システム
- プロセス
- プロセッサー
- RAM
- レジストリー・キー
- 実行中のタスク
- スケジュールされたタスク
- サービス
- User (ユーザー)

b. 2 番目のドロップダウンから、オペレーティング・システムを選択します。1 つまたは複数のオペレーティング・システムを選択できます。

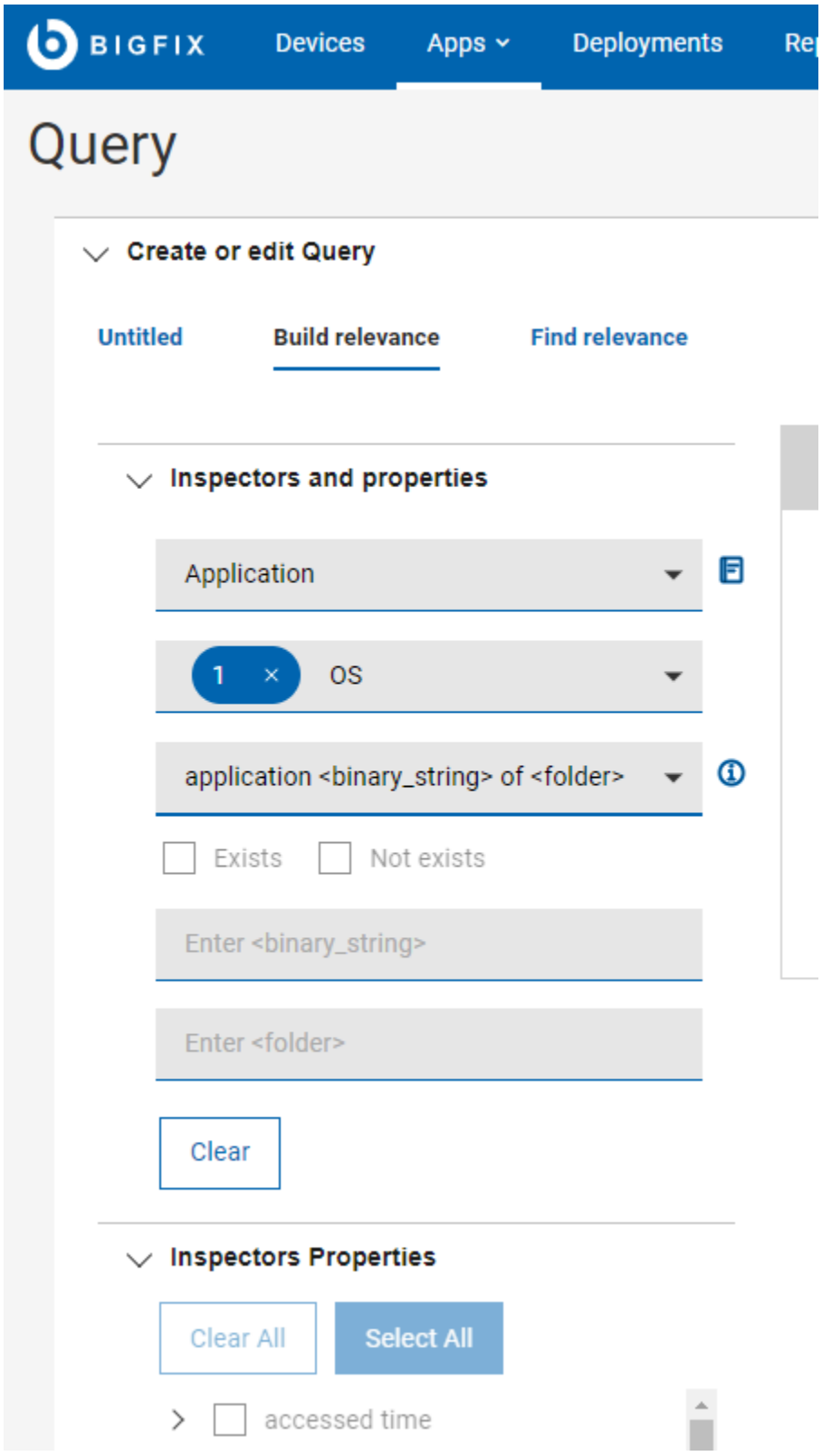


c. 選択したインスペクター・タイプとオペレーティング・システムに基づいて、適用できるインスペクターだけが表示されます。3 番目のドロップダウンから、インスペクター値を選択します。



- 選択したインスペクターがパラメーター化されている場合は、「パラメーターの入力」テキスト・ボックスにパラメーターの値を **入力** できます。

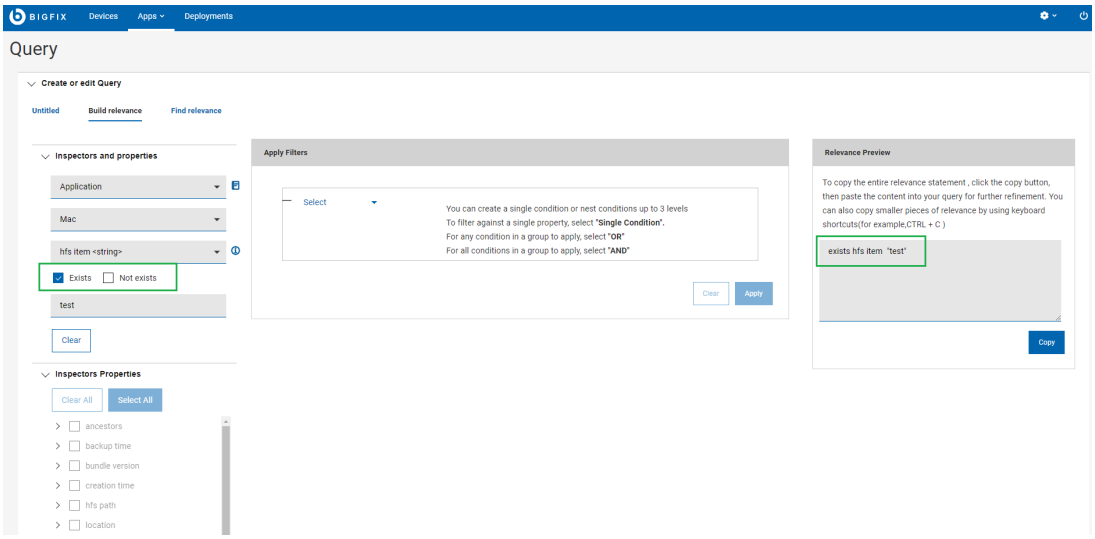
> **注:** 現在、最大 2 つのパラメーターを持つインスペクターがサポートされています。


BIGFIX
Devices
Apps
Deployments
Query
Create or edit Query
Untitled
Build relevance
Find relevance
Inspectors and properties
Application
1
OS
application <binary_string> of <folder>
Exists
Not exists
Enter <binary_string>
Enter <folder>
Clear
Inspectors Properties
Clear All
Select All
accessed time

- 選択したインスペクターがパラメーター化されていない場合、**「パラメーターの入力」**テキスト・ボックスは無効になります。

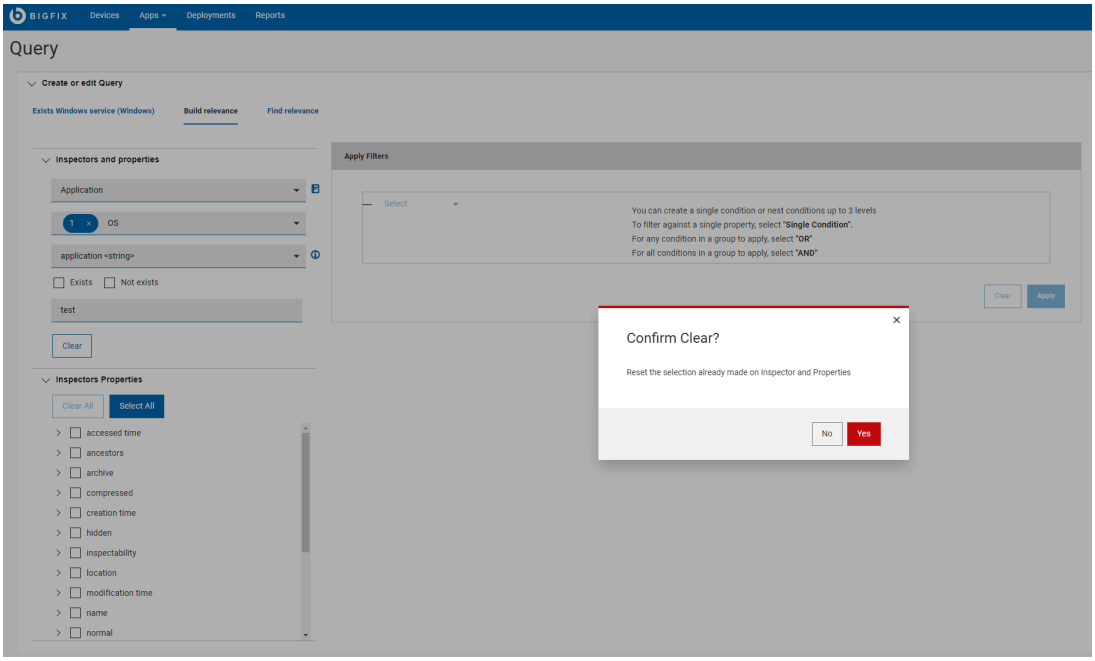
d. **「存在します」**および**「存在しません」**のキーワードは「関連度の作成」で使用できます。関連度の作成は、3 つのセクションで構成されています。
   - 「インスペクターとプロパティー」セクション: インスペクターに対して「存在します/存在しません」を追加します
   - 「インスペクターのプロパティー」セクション: インスペクターのプロパティーに対して「存在します/存在しません」を追加します
   - 「フィルターの適用」セクション: フィルターに対して「存在します/存在しません」を追加します

いずれかのチェック・ボックスを選択すると、以下の図のように「フィルターの適用」が有効になり、「インスペクターのプロパティー」が無効になりま



す。

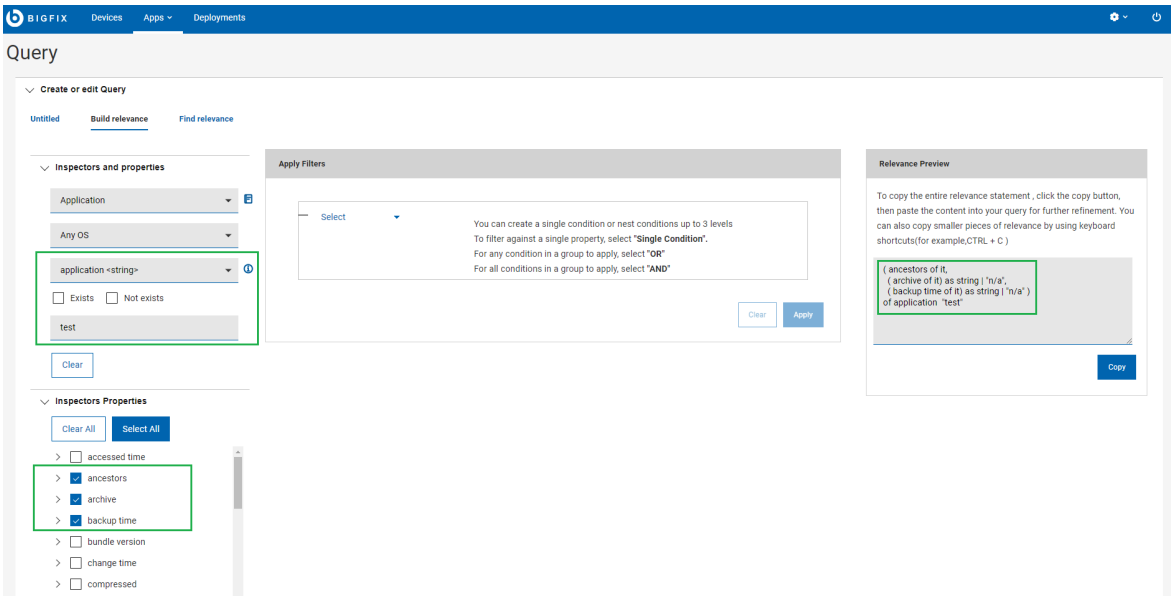
e. パラメーターを削除するには、**「クリア」**ボタンをクリックして実行しま



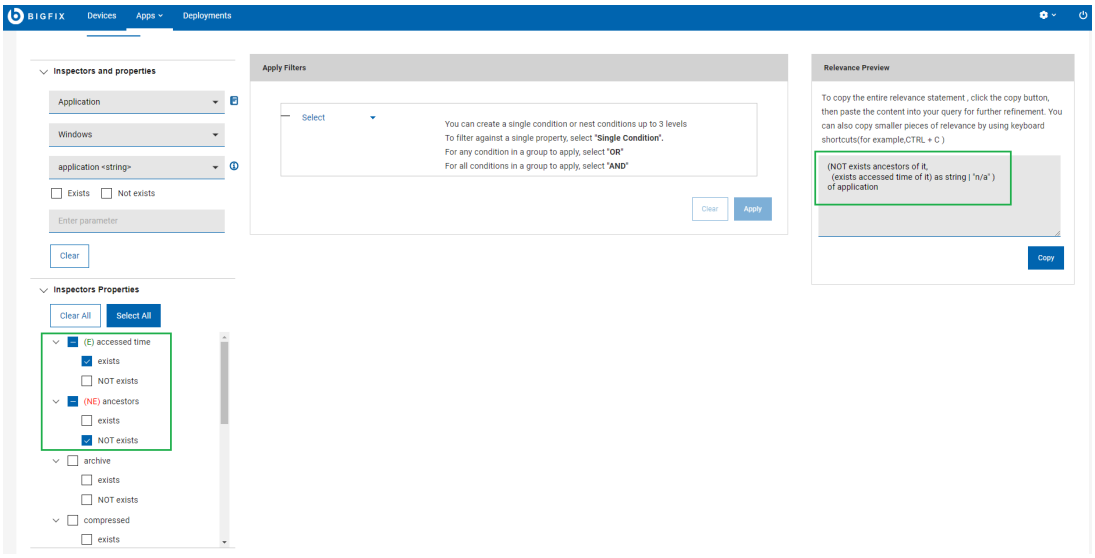
す。

4. 選択したインスペクター値に基づいて、**「インスペクターのプロパティー」** のリストにデータが取り込まれます。「関連度の作成」から返すプロパティーを選択します。

注: 「インスペクターのプロパティー」のドロップダウン・リストは**「存在します」** または **「存在しません」** のチェック・ボックスが選択されていない場合にのみ使用できます。



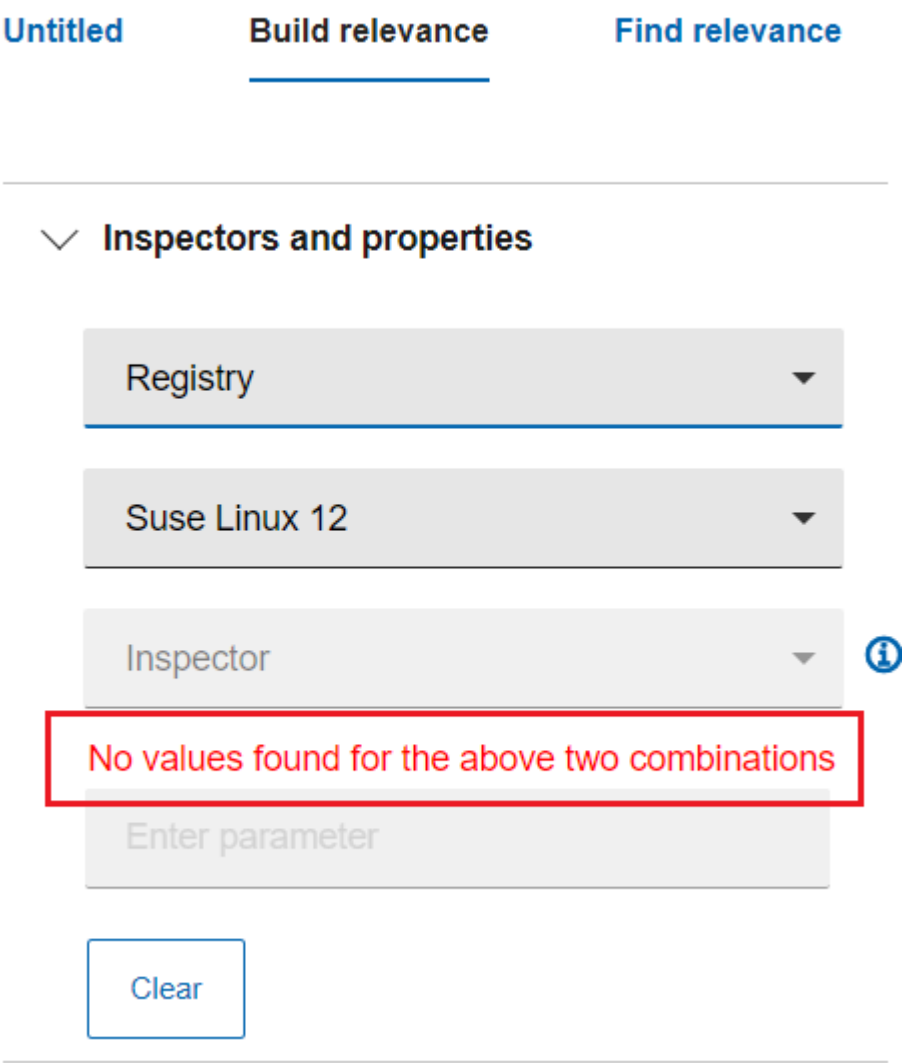
- 各プロパティーには **「存在します」** と **「存在しません」** のオプションがあります。**「存在します」** または **「存在しません」** を選択すると、プロパティーの横に **「E」** (存在します) または **「NE」** (存在しません) が表示されます。



- すべてのプロパティーを選択するには、**「すべて選択」**をクリックします。
- 選択したすべてのプロパティーをクリアするには、**「すべてクリア」**をクリックします。

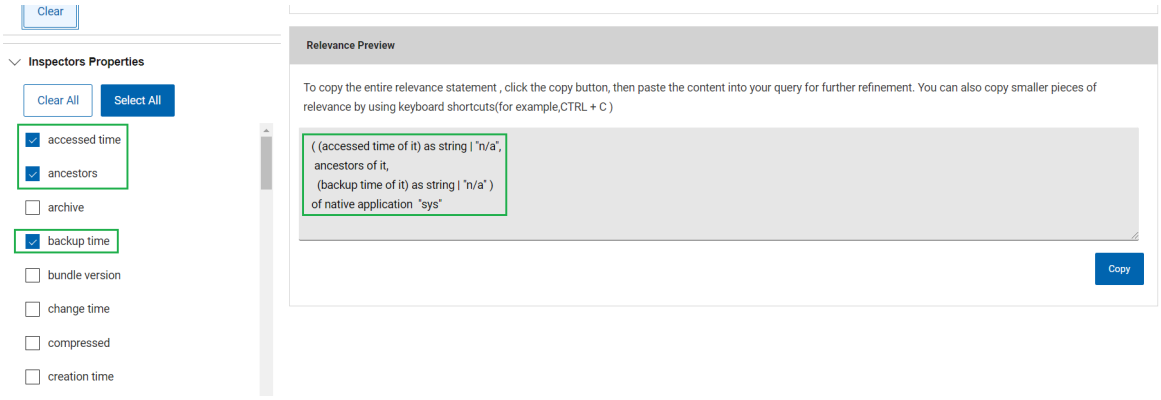
注:

- インスペクター・タイプまたはオペレーティング・システムの選択を変更すると、新しいインスペクター値が取得されます。したがって、インスペクターのプロパティーが新しく生成されます。
- 選択したインスペクター・タイプとオペレーティング・システムの組み合わせに関連するインスペクター値がない場合、以下のメッセージが表示されます。

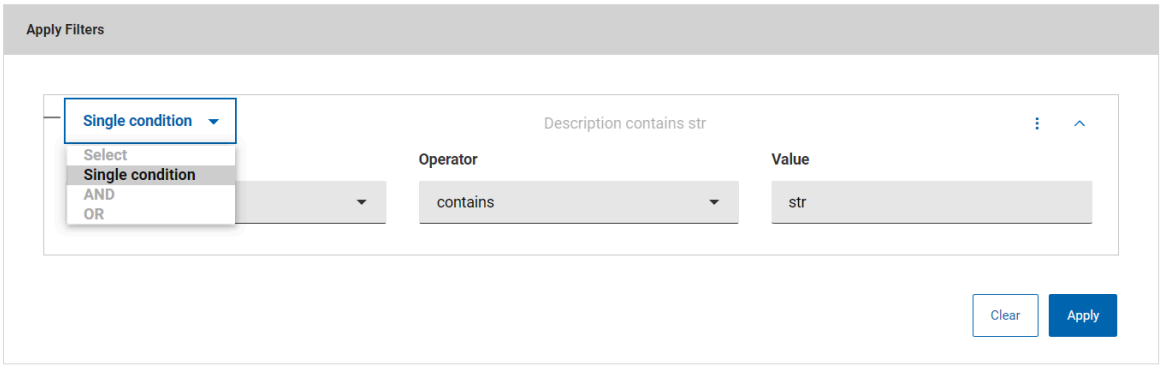


注: インスペクター・パラメーターが正確に入力されたかどうかを検証する機能はありません。

5. 「インスペクターのプロパティー」でチェック・ボックスを選択します。**「関連度のプレビュー」**ボックスで、選択したインスペクターとプロパティーから作成された関連式を確認できます。



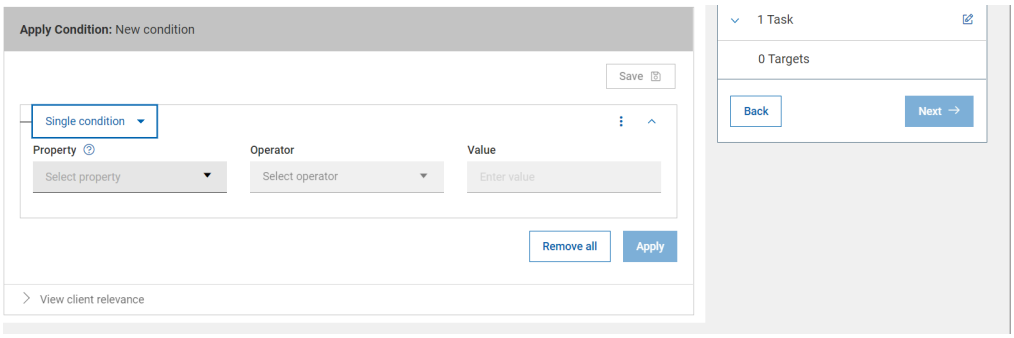
6. **フィルターの適用**関連式は、条件を組み合わせて検索をフィルタリングして作成することもできます。1 つの条件またはネストされた条件を**最大 3 つのレベルまで**作成できます。



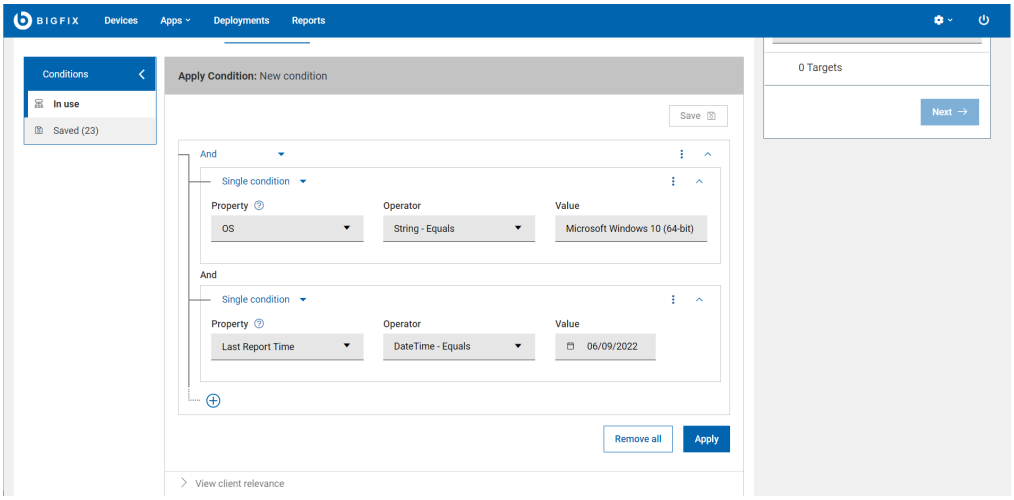
選択したインスペクターとプロパティーに条件を追加して関連式を作成するには、以下の手順を実行します。

a. **「フィルターの適用」**セクションから、以下を選択します。

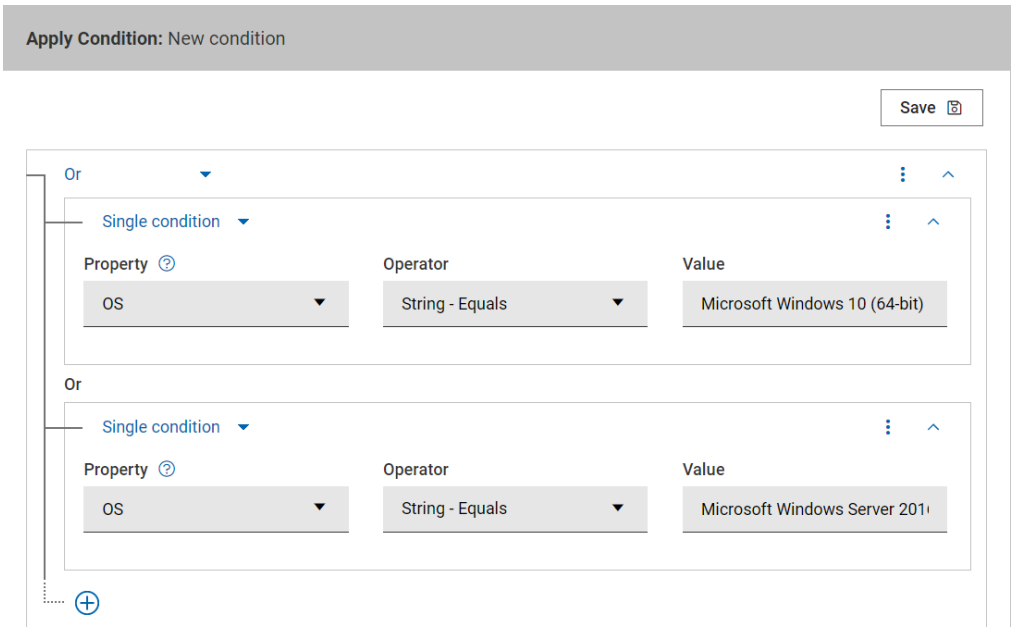
- **「単一の条件」**: 単一の条件を定義して、単一のプロパティーをフィルタリングします。



- **AND**: 複数の条件を定義して、指定した**すべて**の条件を一致させます。



- **OR**: 複数の条件を定義して、指定した**いずれか**の条件を一致させます。



右上隅の 3 点ドットのメニュー ( ) を使用すると、条件の**追**加または削除ができます。

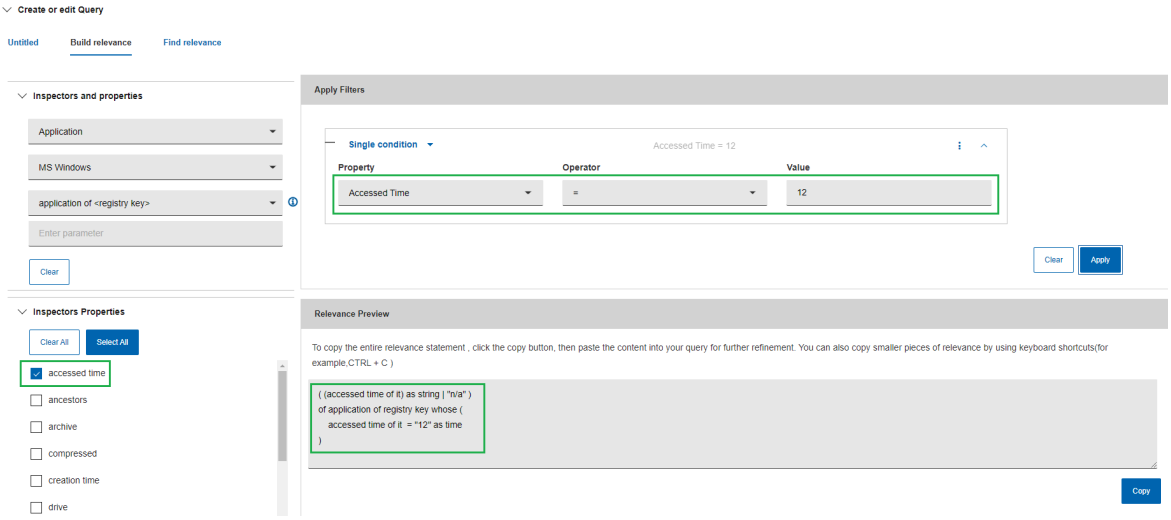
注: プロパティー値によっては、フィルター条件で使用可能な演算子の数が異なる場合があります。

- 整数値に使用できる演算子: =、<、>、>=、<=、存在します、存在しません
- ブール値に使用できる演算子: =、存在します、存在しません
- 時刻の値に使用できる演算子: =、次を含む、次の値で始まる、存在します、存在しません
- ストリング値に使用できる演算子: =、次を含む、次の値で始まる、存在します、存在しません

b. **「適用」**をクリックします。

「関連度のプレビュー」ボックスで、選択したインスペクターとプロパティーとフィルターを適用して作成された関連式を確認できます。**「コピー」**をクリックしてこ

の関連式をコピーし、照会エディターに貼り付けると、新しい照会を作成できます。フィルターをクリアするには、**「クリア」**ボタンをクリックします。ポップアップ・ウィンドウで**「はい」**をクリックしてクリアを実行します。

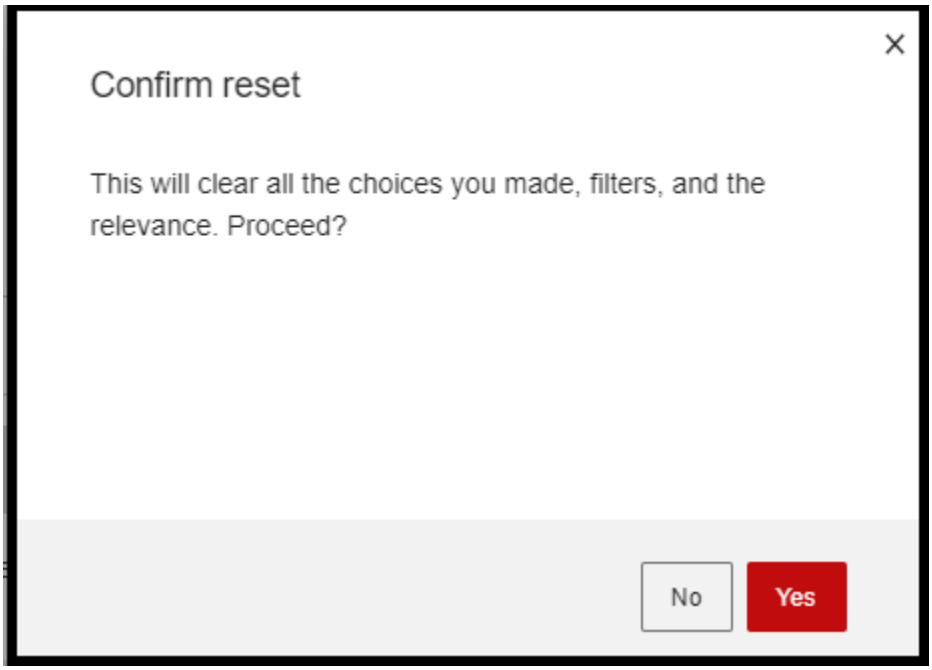


注: 最終的に完成した関連度の構文が正確かどうかを検証する機能はありません。

関連式のクリア

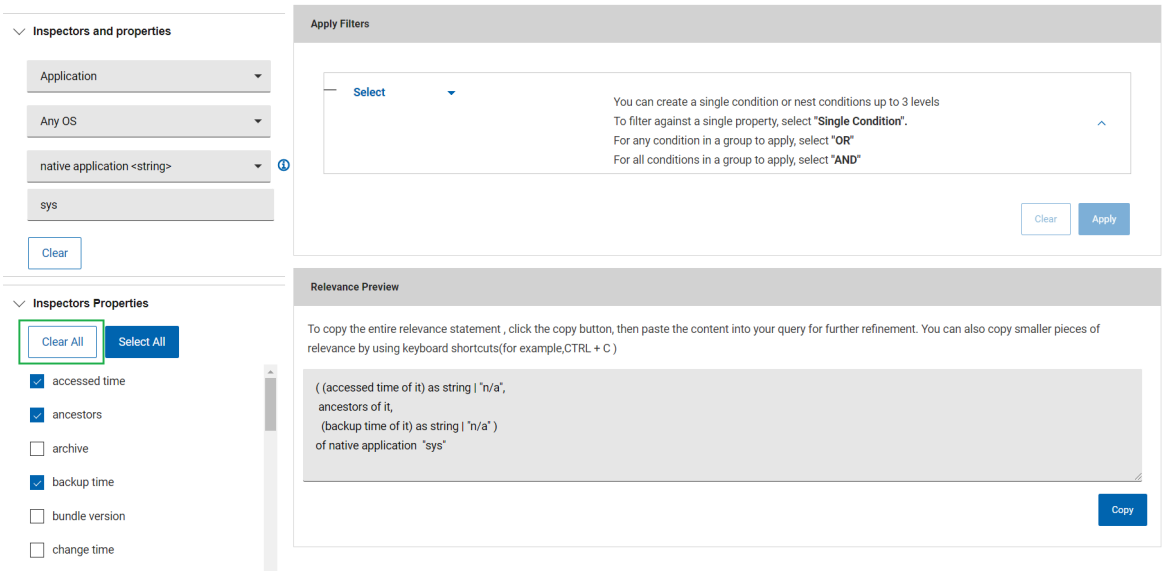
関連式をクリアするには、プレビュー・ボックスで以下の手順を実行します。

- **「関連度のプレビュー」**ウィンドウの**「リセット」**ボタンをクリックします。表示されたポップアップ・ウィンドウで**「はい」** をクリックするとリセットが実行されます。



注:「リセット」ボタンをクリックすると、関連度のプレビュー、インスペクター・プロパティー、フィルターの適用がクリアされます。

- **「インスペクターのプロパティー」**のチェック・ボックスの選択を解除します。
- **「すべてクリア」**ボタンをクリックすると、すべてのインスペクターのプロパティーが削除され、関連度のプレビュー画面から関連文が削除されます。



関連度の検索

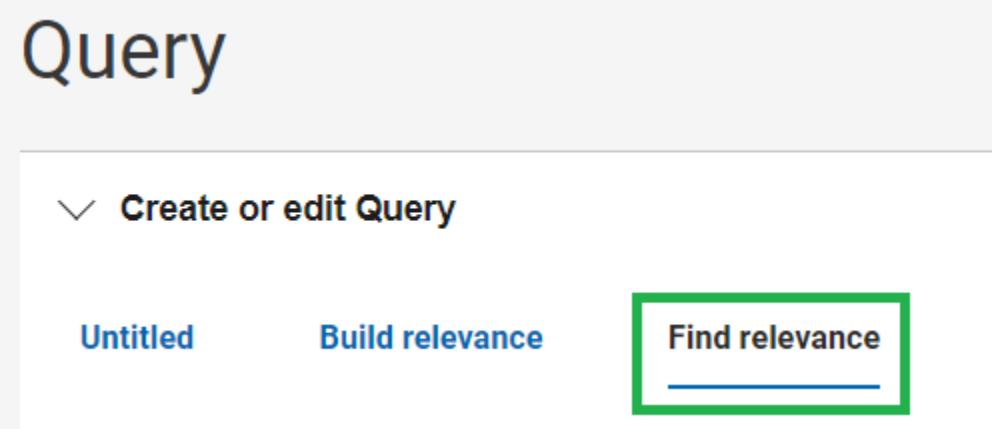
「関連度の検索」タブから、BES サーバーから関連度コンテンツを取得できます。マスター・オペレーター/コンテンツ作成者は、キーワードを使用して、BES サーバーからプロパティーまたは Fixlet とタスクを検索できます。

重要:「関連度の検索」を表示して作業するには、Web レポートが稼働している必要があります。

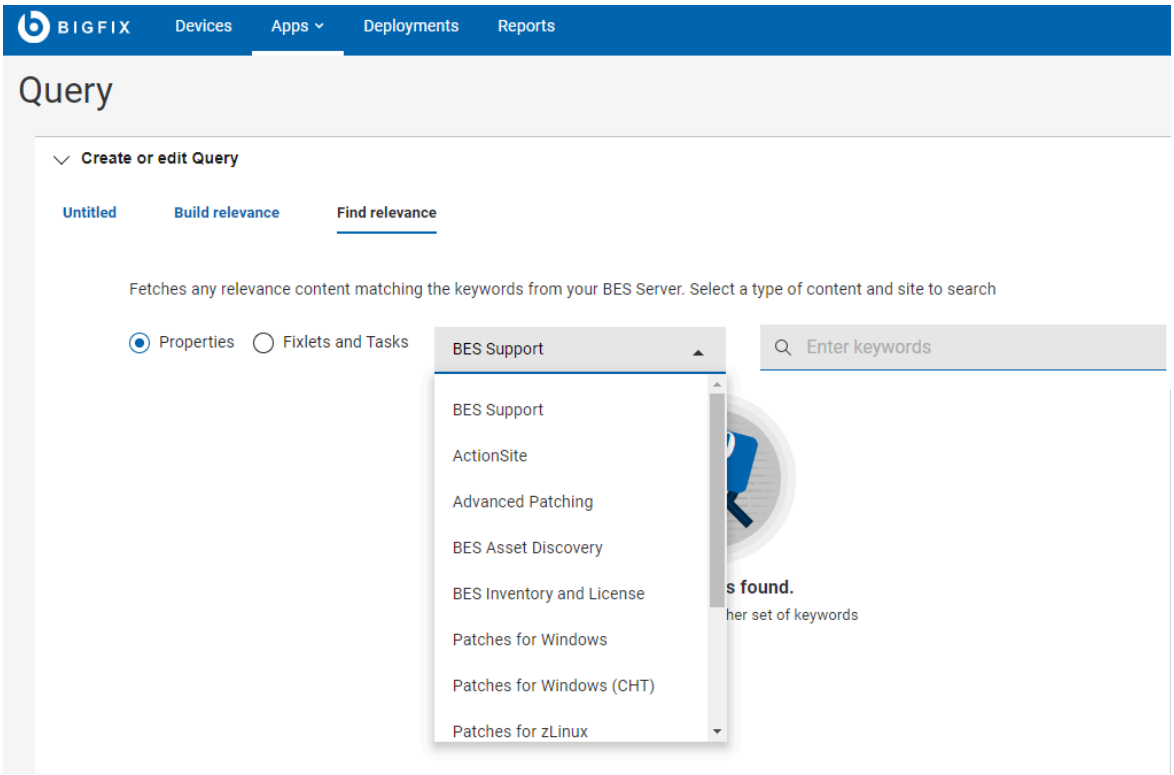
注:「照会」タブのレイアウトはデバイスの解像度に応じて異なります。サポートされている解像度について詳しくは、 こちらのリンク ((ページ)　　)を参照してください。

関連度を見つけるには、次を実行します。

1. 照会エディターで、 **「関連度の検索」**タブに移動します。



2. **「プロパティー」**または**「Fixlet とタスク」**を選択します。
3. ドロップダウン・リストから**「サイト」**を選択します。デフォルトでは、サイトは BES サポートに設定されています。検索にはカスタム・サイトが含まれます。

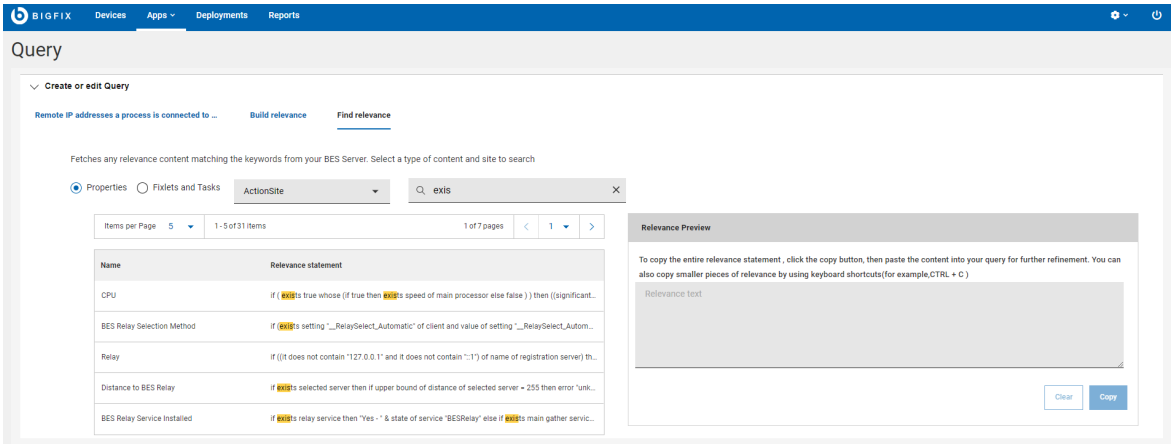


注: ドロップダウンで使用可能なサイトは、コンテンツ作成者が表示する資格を持つすべての使用可能な外部 BigFix サイトと、オペレーターがマスター・オペレーターの場合は ActionSite です。

4. 検索ボックスに任意のキーワードを入力し、**「Enter」**キーを押して結果を表示します。一致するすべての**「Fixlet とタスク」** または**「プロパティー」**(選択されたもの)が関連度ステートメントとともに結果セットに表示され、指定されたストリングが強調表示されます。

   「関連度プレビュー」を表示するには、関連する行をクリックします。

   「関連度プレビュー」テキスト・ボックスから関連度ステートメントをコピーし、照会エディターの**「タイトルなし」**タブに貼り付けて、新規照会として保存することや、照会を実行することもできます。

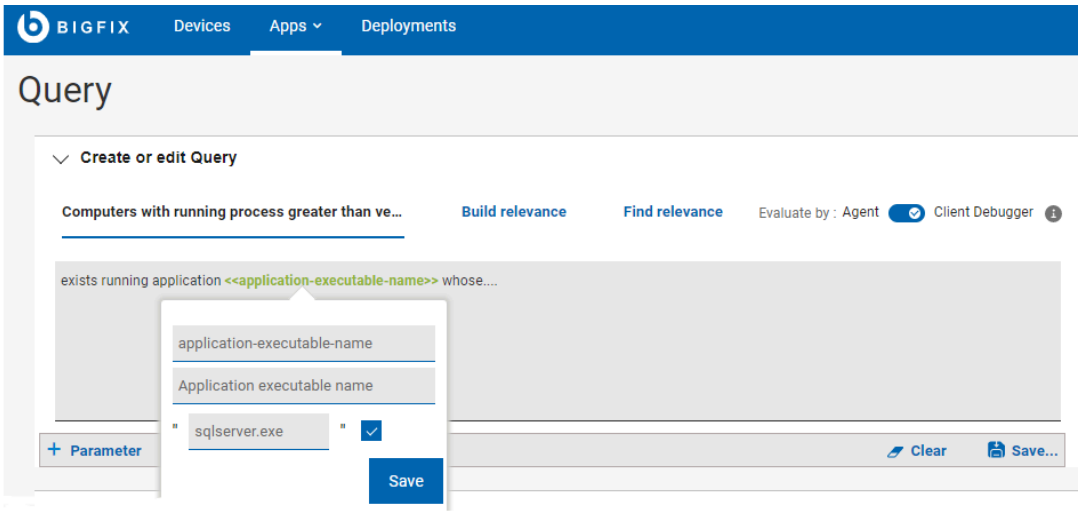


注: プロパティーが分析に属する場合、**「プロパティー」**の「名前」列は次の形式になります。*(name_of_the_analysis) name_of_the_property*。それ以外の場合は、単純にプロパティーの名前になります。**「Fixlet とタスク」**の場合は、常に Fixlet/タスクの名前になります。

照会のパラメーターの管理

コンテンツ作成者はパラメーターを照会に追加し、実行時にカスタマイズできます。オペレーターは、照会を実行するときにパラメーターに値を割り当てるよう求められますが、関連式は表示できません。

- パラメーターを追加するには、以下のステップを実行してください。
  1. 照会エディターで、**「+ パラメーター」**ボタンを有効化できるよう、編集ビューになっていることを確認します。
  2. 照会エディターで関連式のパラメーターを追加するポイントにカーソルを置き、**「パラメーター」**をクリックします。

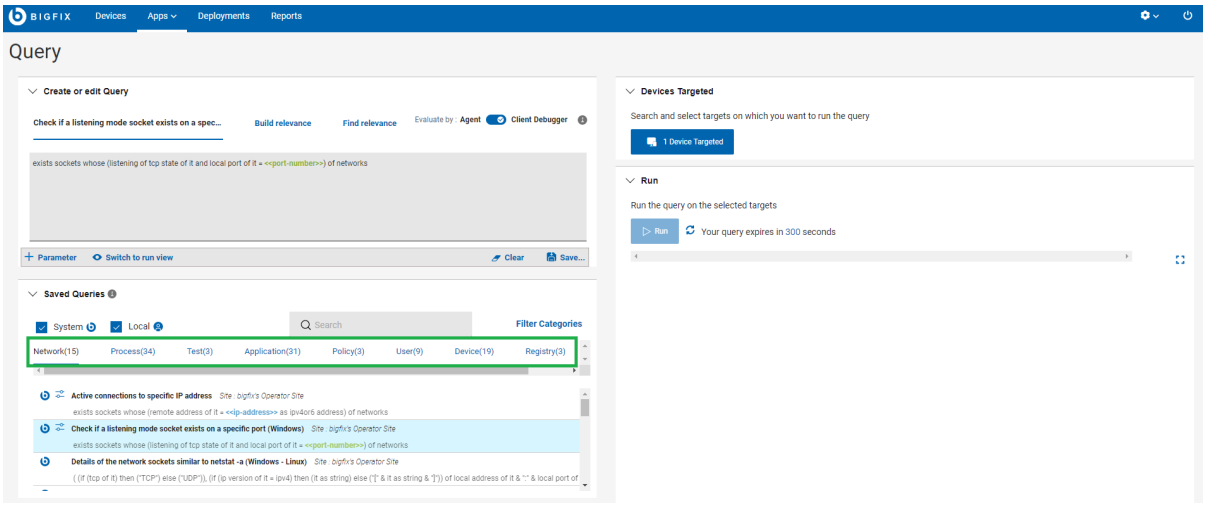


  3. **「パラメーター ID」**、**「パラメーター・ラベル」**、**「デフォルト値」**を入力し、**「保存」**をクリックします。

  パラメーターが関連式に追加されます。
- パラメーターを再使用するには、以下のステップを実行してください。
  1. **「+ パラメーター」**をクリックし、再使用するパラメーター ID を入力します。パラメーター・ラベル・フィールドとデフォルト値フィールドは自動的に入力されます。
  2. パラメーターを関連式に挿入するには、**「保存」**をクリックします。
- パラメーター定義を表示するには、照会エディター内のパラメーターをクリックします。

- 照会からパラメーターを削除するには、照会エディターでパラメーターを選択し、Backspace キーまたは Delete キーを押します。
- デフォルト値のないパラメーターに、実行時にコンテンツ作成者として値を割り当てるには、**「オペレーター・ビュー」**をクリックします。

以下のグラフィックは、パラメーターが設定された照会が「編集」ビューでどのようにコンテンツ作成者に表示されるかを示しています。



オペレーターが照会を選択したときに表示される内容を確認するには、 

をクリックします。

「編集ビュー」に戻るには、 

をクリックします。

第 10 章. アクションの実行: デプロイ・シーケンス

デプロイとは、アプリケーション、モジュール、更新、パッチなどのコンテンツを 1 つ以上のエンドポイントにディスパッチすることを意味します。例えば、ソフトウェアをデプロイすることで、対象となるエンドポイントにソフトウェアをインストールします。BigFix WebUI を使用すると、コンテンツと対象デバイスを構成して、デプロイメントを作成し、デプロイメント状況をモニターできます。デプロイメントの作成に必要なすべてのステップ、プロセス、アクティビティーを含むワークフローを総称して「デプロイ・シーケンス」といいます。

デプロイ・シーケンスの要約

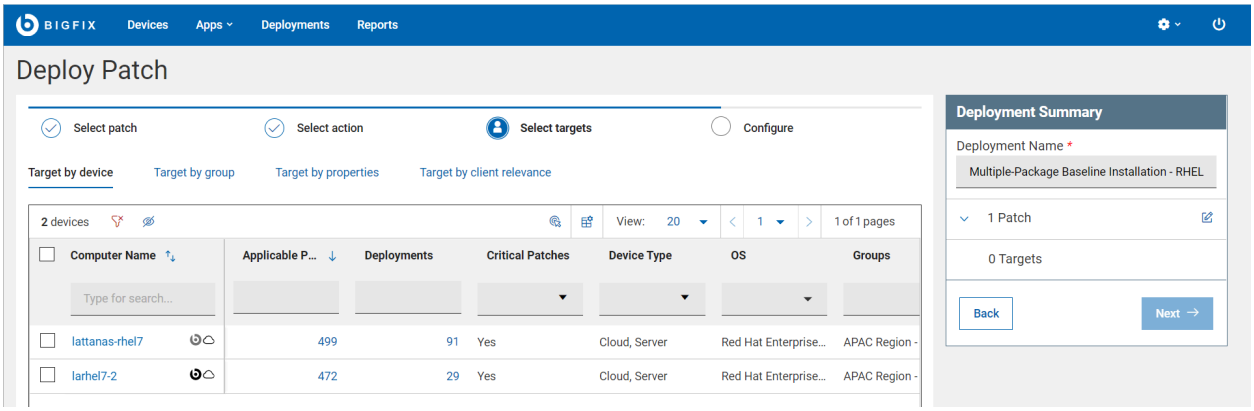
エントリー・ポイントに従ってシーケンスの変更をデプロイします。

例えば、デバイス・リストからデプロイメントを開始する場合、シーケンスは次のようになります。

1. 対象デバイスを選択します。
2. カスタム・コンテンツ、MDM アクションまたはポリシー、パッチ、ソフトウェア、プロファイルなどのコンテンツを選択します。
3. アクションを選択します。
4. デプロイメント・オプションを構成します。
5. 確認してデプロイします。

コンテンツ・ページ (パッチ・ページなど) からデプロイメントを開始する場合、シーケンスは次のようになります。

1. パッチ (またはその他のコンテンツ) を選択します。
2. アクションを選択します。
3. 対象デバイスを選択します。
4. デプロイメント・オプションを構成します。
5. 確認してデプロイします。



- 「デプロイ・シーケンス」ウィザードは、すべてのアクションが異なるタブで構成されています。いつでも別のタブに移動できます。
  - は、現在のアクションを示します
  - は、完了したアクションを示します
  - は、完了していないアクションを示します。

「デプロイメントの要約」には、デプロイメントの全体的な要約が表示されます。選択したターゲット、コンテンツ、アクション、構成に関する、すべての詳細が表示されます。「編集」ボタンをクリックすると、いつでも選択内容を変更できます。「次へ」ボタンで、シーケンスの次のステップに移動できます。要件に従ってすべてのステップが完了すると、 「デプロイ」ボタンが有効になります。「デプロイ」ボタンが無効になっている場合は、選択内容を確認して編集し、問題を修正してください。

プロンプト、状況情報、選択の各集計が「デプロイメントの要約」セクションに表示されます。ステータス・バーには、デプロイ・シーケンスの進行状況が表示されます。一部のオプションでは組み込みのヘルプ (疑問符 (?) のアイコン) が使用可能です。

- **対象の上限**管理者は一度にデプロイできるコンテンツの量、同時にデプロイまたは照会できるデバイス数を制限できます。この上限を超えると、許容範囲内に選択数を減らすまでメッセージが表示され続けます。“「デプロイメントあたり *3* 台というデバイス上限を超えました」など、このメッセージには対象の上限が含まれています。”

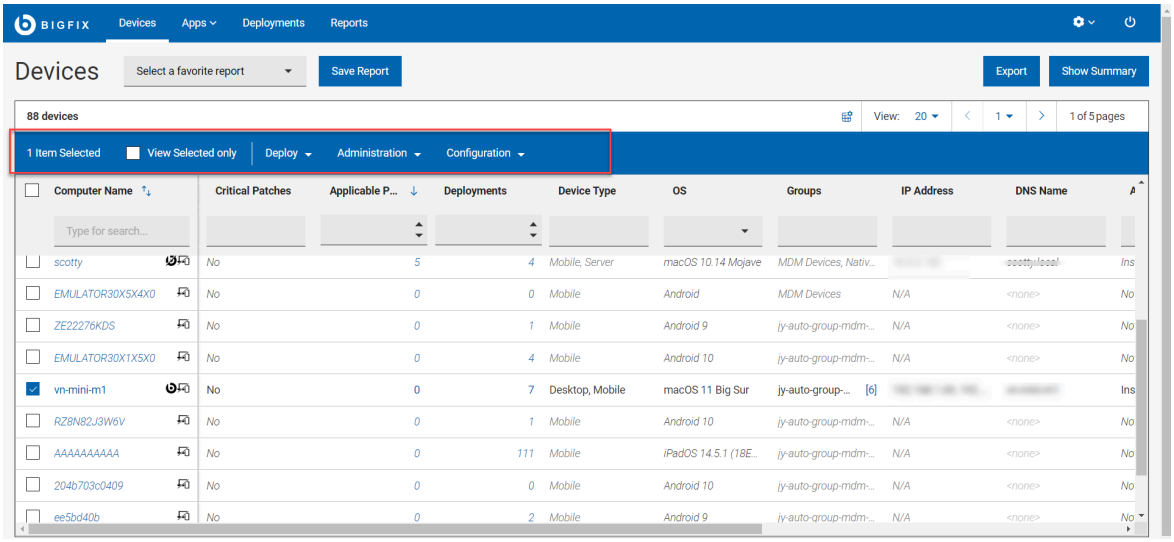
  注: ターゲット制限が定義されている場合、影響を受けるマスター以外のオペレーター (NMO) は、「グループ別にターゲット設定する」オプションを使用してアクションをデプロイできません。

- **すべてのコンテンツをデプロイできるわけではありません。**デプロイ不能コンテンツ (監査アクションなど) を選択した場合は、それをデプロイメントから削除するよう求めるプロンプトが表示されます。
- **デフォルト・アクションがない** - デフォルト・アクションのないコンテンツを選択した場合は、デフォルト・アクションを選択するよう求めるプロンプトが表示されます。
- **アクション・パラメーターが必要** - パラメーターが必要なコンテンツを選択した場合は、パラメーターの入力を求めるプロンプトが表示されます。

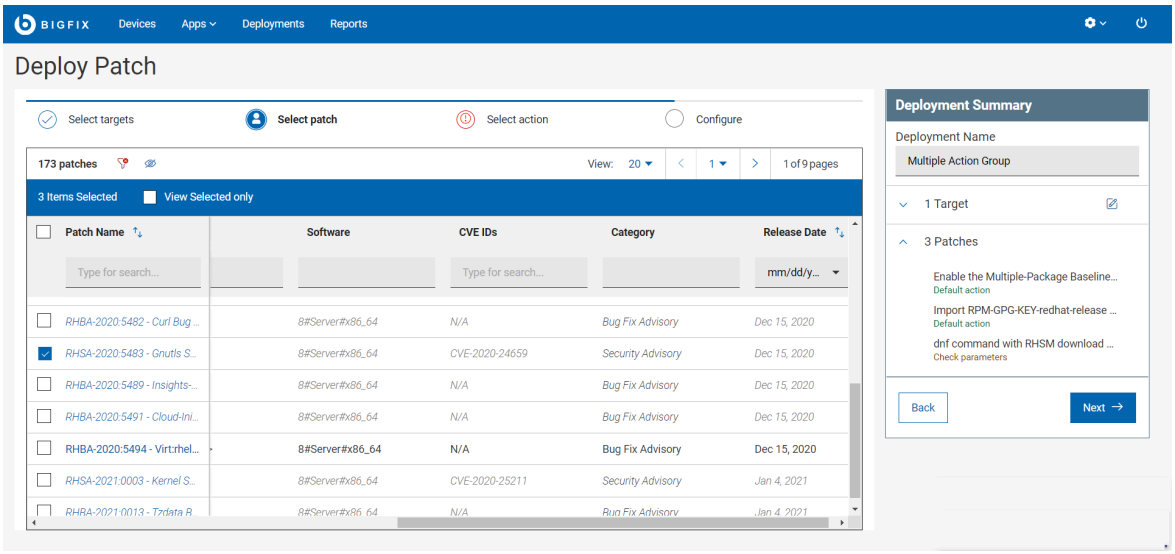
デプロイ手順

このセクションでは、デバイスにコンテンツをデプロイする手順について説明します。

1. デプロイメント用のデバイスまたはコンテンツを選択すると、青色のアクション・バーが表示されます。

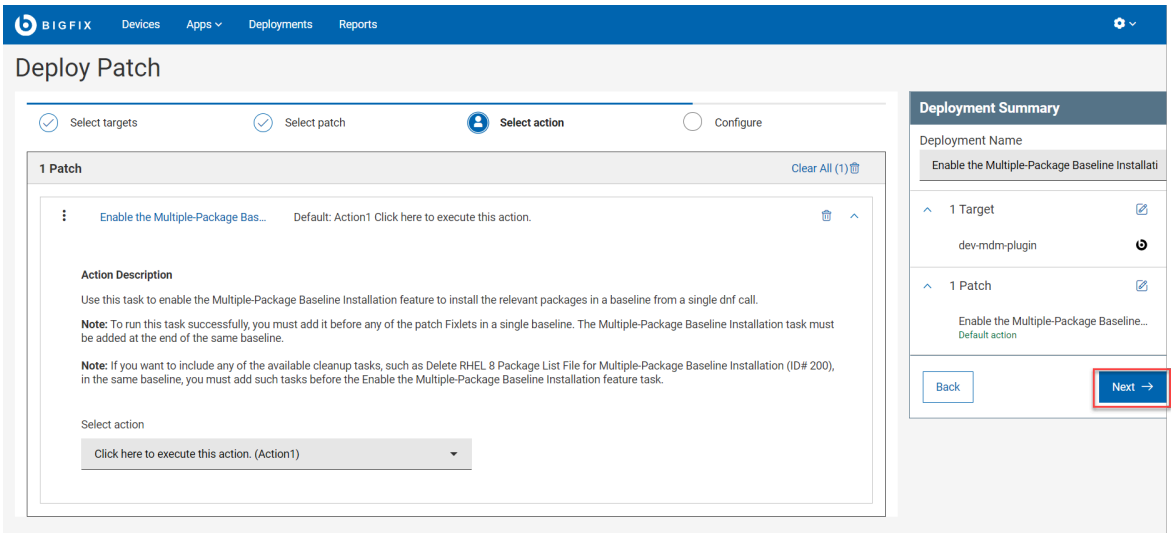


2. 対象コンテンツまたは対象デバイスをそれぞれ選択し、**「次へ」**をクリックします。



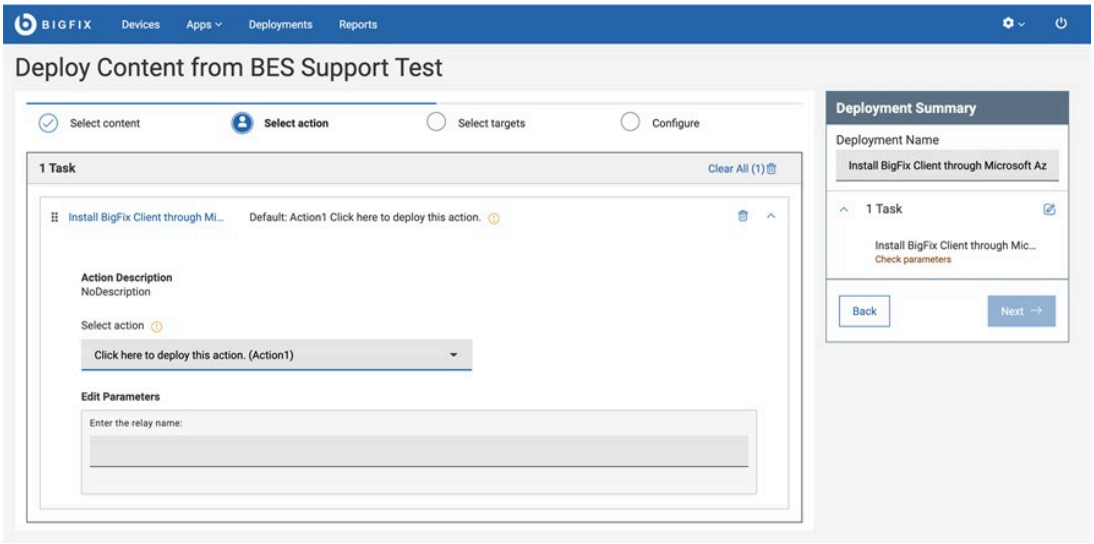
- リスト・ビュー、フィルター、検索ツールを使用し、必要な記録を見つけてください。
- デバイスと文書をレビューして、それらの効果を必ず理解してください。
- あるいは、ソフトウェア文書 (（ページ） *129*)で説明されているように、アクションをソフトウェア文書から直接デプロイできます。

3. 「アクションの選択」タブには、の作業中のアプリケーションに応じて、「タスク」、「パッチ」、「ソフトウェア」と表示されます。展開して詳細説明が表示するには、キャレット記号をクリックします。



4. 「決定が必要」プロンプトまたは「デプロイ不能」プロンプトが表示される場合は、1 つ以上のアクションで入力が必要です。
   - 1 つまたは複数のアクションで注意が必要

   a. **「選択」**アクション・リンク (タスク、パッチ、ソフトウェア) をクリックして「決定」ダイアログを開きます。



注: 複数のアクション・グループは、個々のアクションをクリックしてドラッグすると、順序を変更できます。これは、従来の BigFix® コンソールでは実行できない BigFix® WebUI の機能です。

i. 欠落しているデフォルト・アクションをすべて指定します。
- デフォルト・アクションのない、複数のアクションを持つ Fixlet の場合: ドロップダウン・リストからアクションを選択します。例えば、アプリケーションのインストールとアンインストールの両方で単一ソフトウェア・パッケージが使用される可能性があります。
- デフォルト・アクションのない、単一アクションの Fixlet の場合:
  1. コンテンツ文書をレビューします。Fixlet® 作成者は、「注意して続けてください」と言っています。Notes®、警告、既知の問題に細心の注意を払い、情報に基づいた意思決定を行ってください。
  2. アクションを削除するには、そのアクション名の横にある「x」をクリックします。アクションをデプロイするには、ドロップダウン・リストから「ここをクリックして、適用プロセスを開始」を選択します。

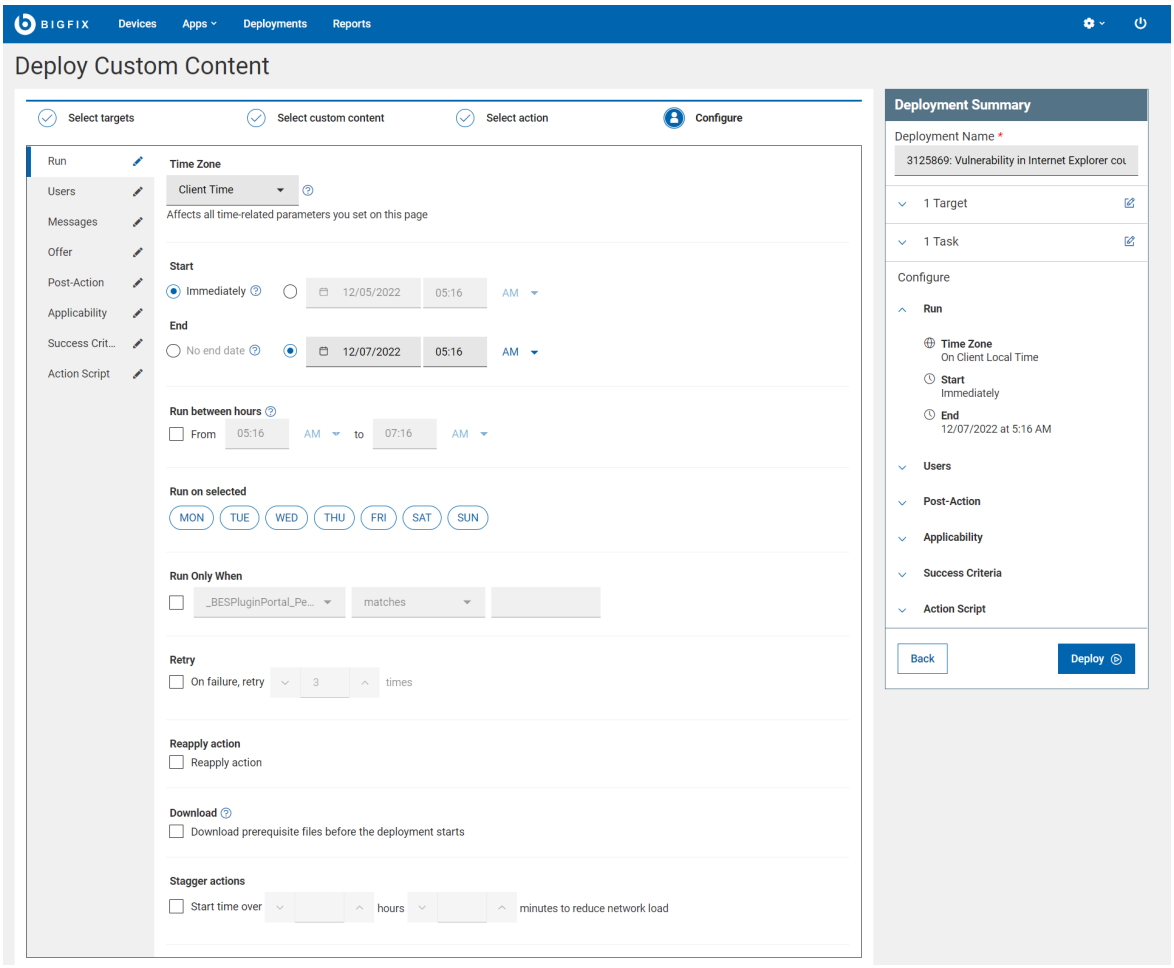
ii. 必要に応じてアクション・パラメーターを入力します。
1. ドロップダウン・リストに表示されているアクションを選択し、**「パラメーターの入力」**リンクを表示します。
2. **「パラメーターの入力」**をクリックし、パス名やサービス名などの必要情報を入力します。

iii. 監査パッチや置き換えられたパッチなどのデプロイ不能アクションをすべて削除します。

b. **「適用」**をクリックして、デプロイ・シーケンスに戻ります。

c. **「次へ」**をクリックして「構成」ページを開きます。

5. デプロイメントの構成オプションを選択して**「次へ」**をクリックします。各オプションの説明については、「構成オプション」（（ページ） *199)*を参照してください。



6. 「デプロイメントの要約」から選択した内容を確認します。何らかの調整が必要な場合には、**「編集」**アイコンを使用します。

> **注:** 「デプロイ」ボタンは、正確かつ互換性を持つデータがすべてのステップにある場合にのみ有効になります。それ以外の場合は無効となり、デプロイメントを続行するには確認および修正をする必要があります。

7. **「デプロイ」**をクリックします。
8. デプロイメント・リスト (（ページ） *209)* からのデプロイメント結果をモニターします。

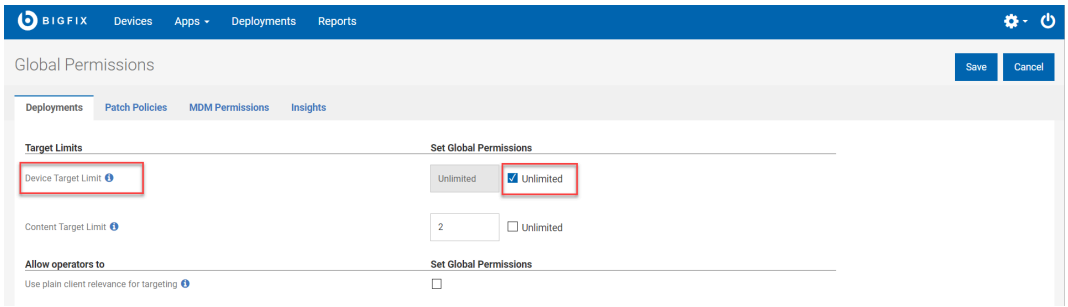
ターゲットの選択

WebUI を介してパッチまたはコンテンツをデプロイするために、複数の方法でターゲットを選択できます。

「デプロイメント・シーケンス」ウィザードで、現在のアクションが**「ターゲットの選択」**の場合、ターゲットの選択方法に対応する以下のタブが表示されます。

- **デバイス別にターゲット設定する**。デバイス・グリッドから対象デバイスを選択します。
- **グループ別にターゲット設定する**。対象デバイスの 1 つ以上のグループを選択します。
- **プロパティー別にターゲット設定する**。BigFix プロパティーに基づいて定義された 1 つ以上の条件を満たす特定の対象デバイスのセットのみを動的にフィルターして選択します。手順については、『デバイスのプロパティー別ターゲット設定 ((ページ) 192)』を参照してください 。

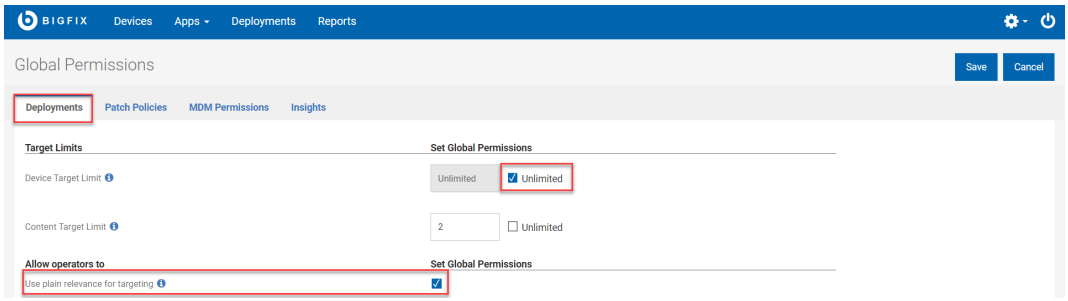
  重要: このタブは、「グローバル権限」またはユーザーに割り当てられた役割の権限で `Device Target Limit` の権限が `unlimited` に設定されているユーザーにのみ表示されます。



- **関連度別にターゲット設定する**。ターゲット設定には、信頼できるクライアントの関連度を使用します。手順については、『デバイスの関連度別ターゲット設定 ((ページ) 198)』を参照してください 。

  重要: このタブは、「グローバル権限」またはユーザーに割り当てられた役割の権限で、以下の権限が有効になっているユーザーにのみ表示されます。

- `Device Target Limit` を `Unlimited` に設定します。
- 「オペレーターに次を許可」が `Use plain relevance for targeting`



関連情報

構成オプション (（ページ） *199)*

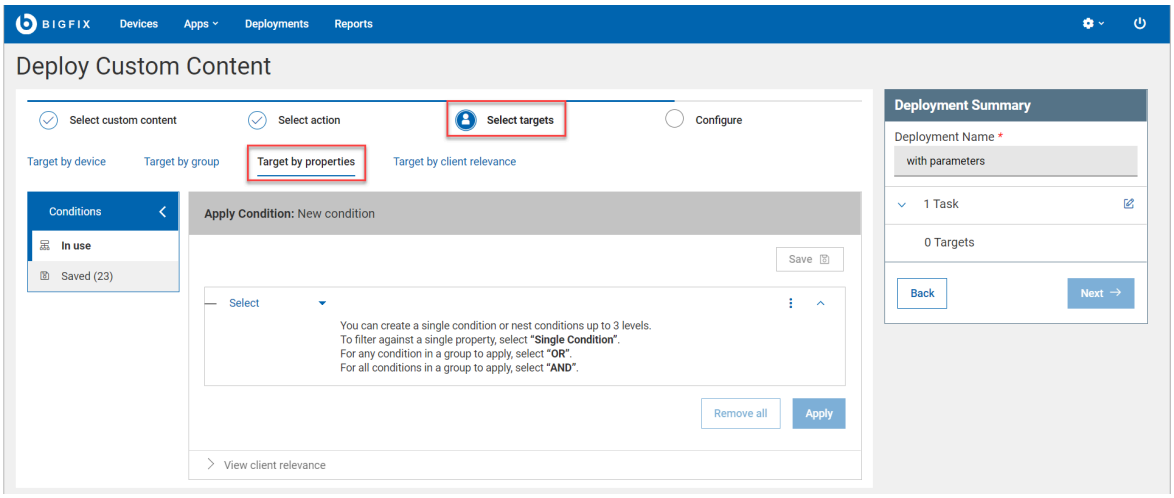
デバイスのプロパティー別ターゲット設定

BigFix プロパティーに基づいて、デバイスを動的にフィルタリングして、1 つ以上の定義済み条件を満たす特定の対象デバイスのセットを選択できます。

予約済みプロパティー (BigFix に既存のもの) およびカスタム・プロパティー (ユーザーが作成するもの) を使用して、プロパティー別にターゲット設定する条件を作成できます。単一の条件を定義することも、AND および OR ステートメントを使用してネストされた条件を作成することもできます。

次のように条件を定義します。

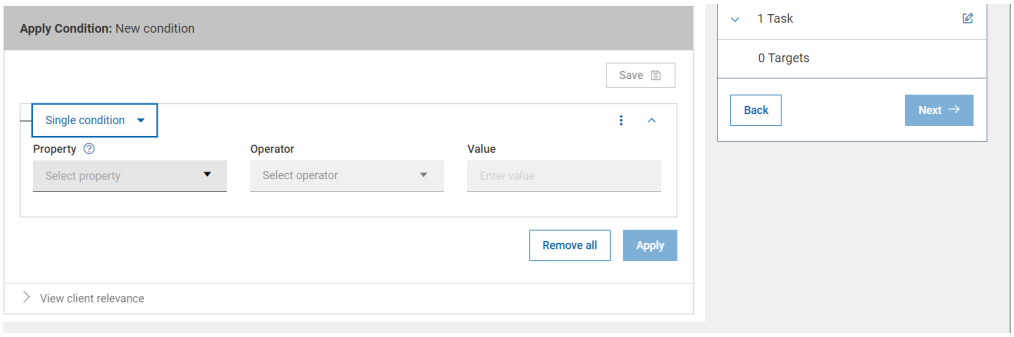
1. デプロイ・シーケンスの**「ターゲットの選択」**アクションで、**「プロパティー別にターゲット設定する」**タブを選択します。



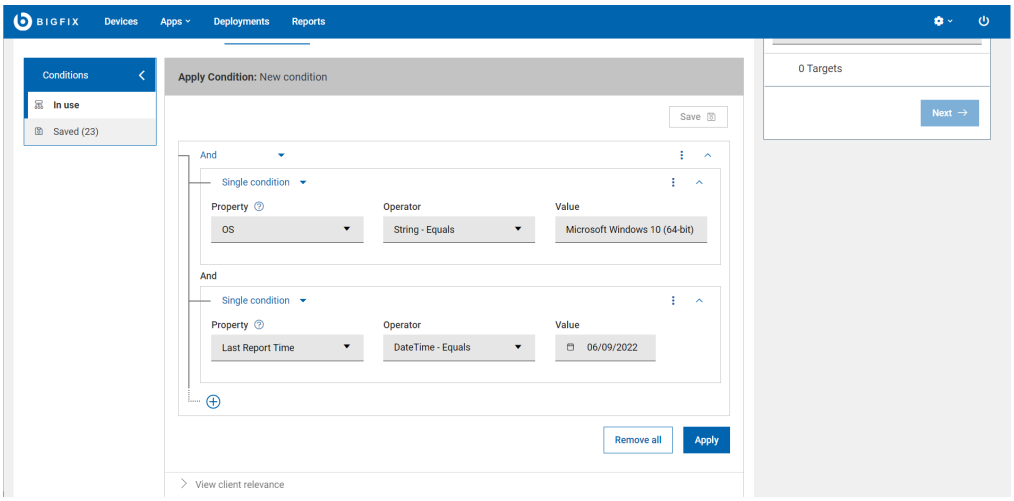
2. **「適用条件」**をクリックします。単一の条件を定義するか、または AND 演算子と OR 演算子を使用して条件を組み合わせて、プロパティーに基づいてターゲットをフィルタリングできます。
3. 条件を追加する手順は次のとおりです。

    a. **「適用条件」** セクションから**「選択」**メニューを開きます。次のメニュー・オプションが表示されます。

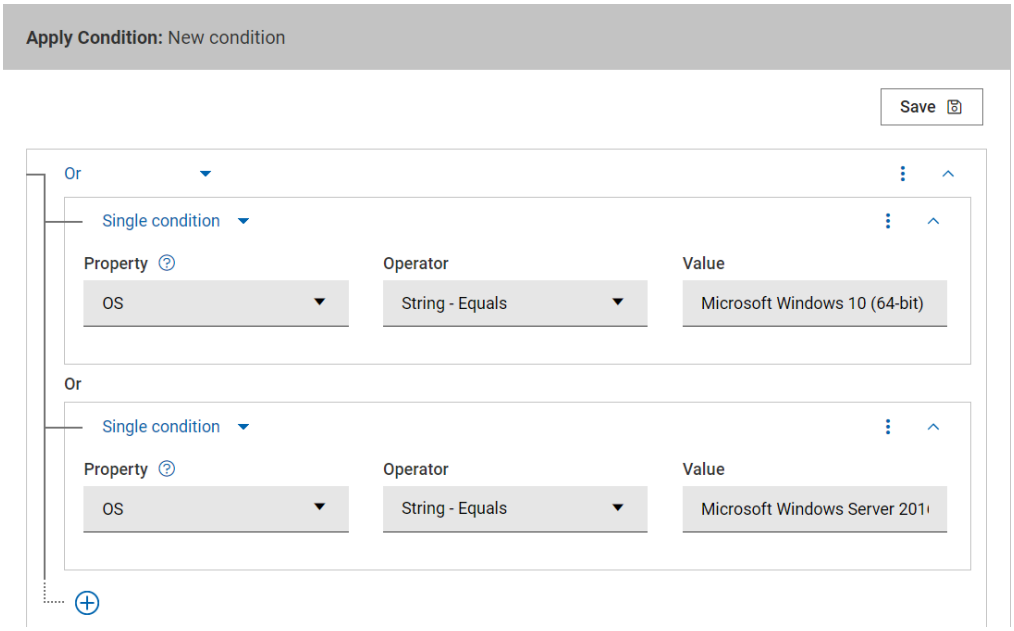
    - **単一の条件**: 単一のプロパティーでフィルタリングする単一の条件を定義するには、このオプションを選択します。



    - **および**: 指定する**すべての**条件に一致しなければならない複数の条件を定義するには、このオプションを選択します。

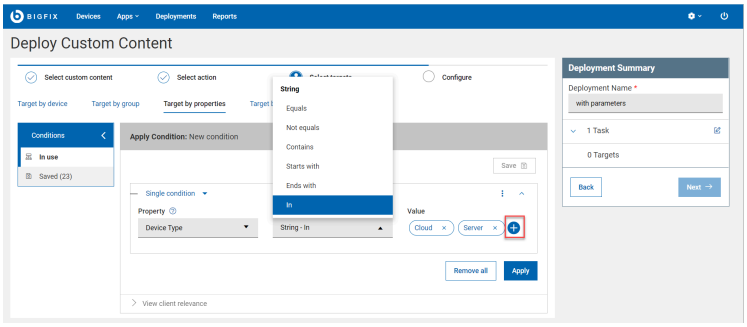


- **または**: 指定する**条件のいずれか**に一致したとき成立する複数の条件を定義するには、このオプションを選択します。



注: 演算子メニュー項目は、他のメニュー項目とは異なる働きをします。

- **演算子**:
  - 選択した **プロパティー**に応じて、動的に**演算子**オプションが表示されます。
  - 対象演算子を使用すると、値のリストを追加できます。**+** 記号をクリックして、リストに値を追加します。



  - 同じレベルであれば条件を必要な数だけ持つことができますが、ネストされた条件は最大 3 つまで指定できます。
  - データベースにまだ存在しない値を持つ条件を定義することもできます。
- **「プロパティー」**メニューにプロパティーがリストされていない場合は、**「プロパティーの追加」**をクリックしてプロパティーを選択し、**「追加」**をクリックします。
- 右上隅の 3 つの点が並んだメニュー を使用して、条件の追加、クリア、または削除ができます。
- すべての条件を削除するには**「すべて削除」**をクリックします。

4. **「適用」**をクリックします。このボタンは、条件を正しく定義した後にのみ使用できます。

- 「デプロイメントの要約」セクションには、適用可能なデバイスの総数が表示されます。

  注: 対象の見積もりには Fixlet の関連度は含まれません。プロパティーの組み合わせと一致するもののみが含まれます。

- セッションの関連度を使用するには、Web レポートがインストールされアクティブになっている必要があります。BigFix は、データベース内の情報に基づいて、条件に一致するデバイスの数を動的に評価して見積もるためです。**「次へ」**ボタンは、**「適用」**ボタンをクリックして、BigFix が対象の見積もりを完了した後にのみ有効になります。この見積もりによって、誤って不要なデプロイメントまたは大規模なデプロイメントを送信するのを防ぐことができます。

  注:「オペレーターがターゲット設定に標準の関連度を使用できるようにする」権限を持っている場合、Web レポートがインストールされていない場合や一時的に使用できないときに、プロパティー別にターゲット設定するときのターゲットの評価をバイパスできます。

5. **オプション: 「クライアントの関連度の表示」**をクリックすると、定義された条件の関連度ステートメントを表示できます。
6. **保存**: 定義済みの条件を保存して後で再利用するには、**「保存」**をクリックし、「条件の保存」ウィンドウで次の手順を実行します。

   a. **「条件名」**に、保存する条件の名前を入力します。

   b. **「共有モード」**で、次のいずれかのオプションを選択します。
      - **プライベート**: 自分だけで使用するためにこの条件を保存するには、このオプションを選択します。
      - **パブリック**: 保存した条件を他のユーザーと共有するには、このオプションを選択し、ラベルを入力して[これはチェックマークですか ?]記号をクリックします。

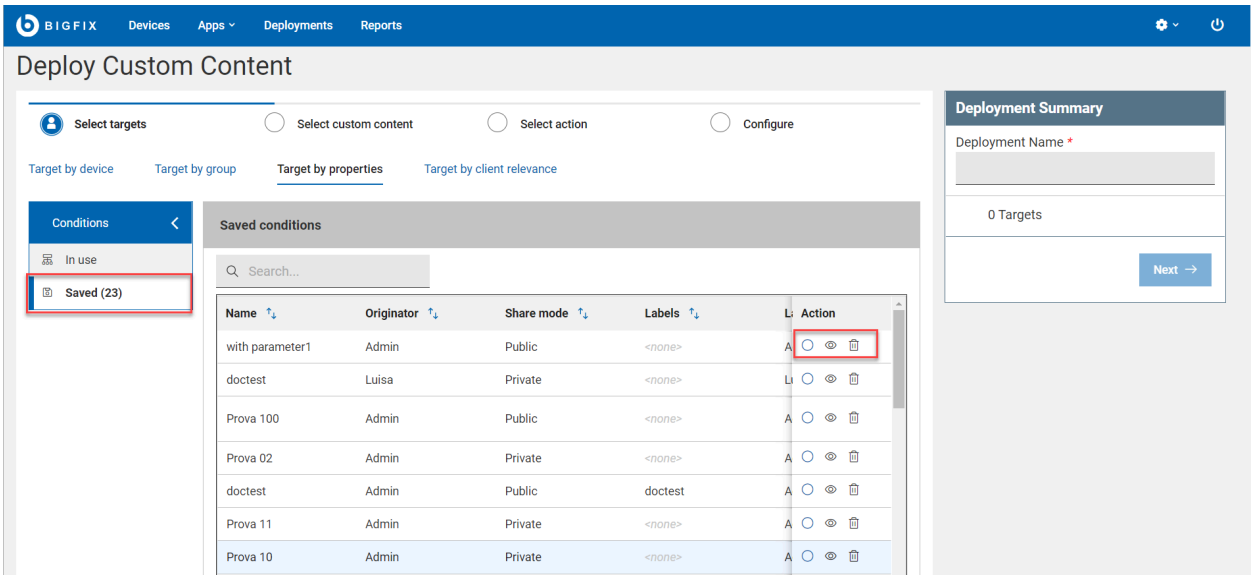
c. **オプション:** 別のラベルを追加するには、**プラス**アイコン (+) をクリックします。

d. **「OK」**をクリックします。

保存された条件にアクセスするには、**「条件」 > 「保存済み」**をクリックします。 [クリック・パスは名詞や場所ではありません。]パスの要素は、他動詞「クリックする」または「選択する」の目的語です]。保存された条件には、以下の制限が適用されます。

- 誰でもプライベート条件またはパブリック条件を保存できます。
- マスター・オペレーターのみが、すべての保存された条件への全アクセス権限を持ちます。
- 別のユーザーが作成した条件で使用される 1 つ以上のプロパティーの権限を持っていない場合、その条件を再使用することはできません。その場合、エラー・メッセージが表示されます。
- プライベート条件またはパブリック条件を削除する権限を持っていない場合、**削除**アイコンは無効になります。
- マスター・オペレーターまたはオリジネーターのみが、パブリックとして保存された条件を削除できます。

条件を選択すると、その詳細を読み込んで表示したり、クライアントの関連度を表示したり、削除したりできます。保存された条件は、名前、ラベル、オリジネーター、最終変更者で検索することもできます。



このウィンドウで使用できるオプションは次のとおりです。

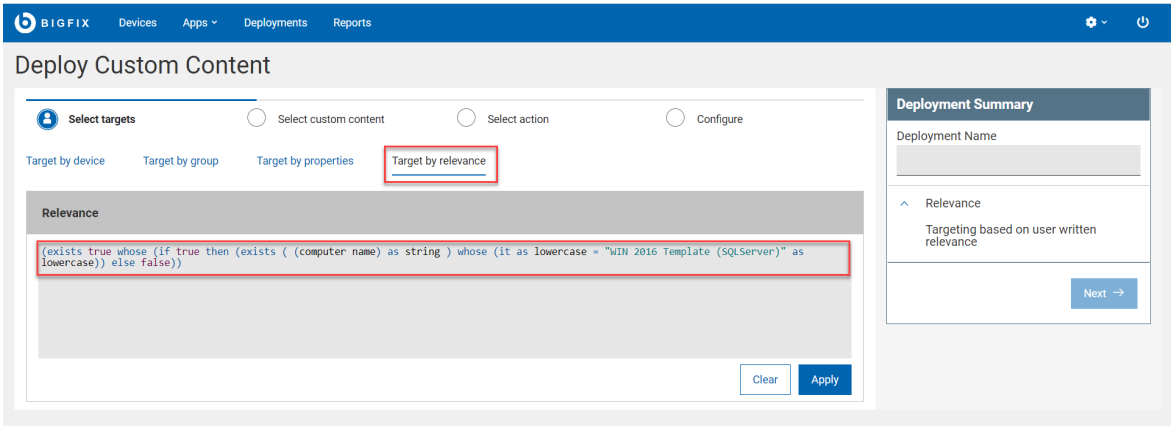
- **ロード**: クリックするとフィルターが読み込まれます。
- **クライアント関連度の表示**: クリックすると、対応するクライアントの関連度がウィンドウに表示されます。
- **削除**: フィルターを削除するにはこれをクリックし、確認ウィンドウで**「削除」**をクリックします。

> **注:** プライベートフィルターまたはパブリックフィルターを削除する権限を持っていない場合、**「削除」**アイコンは無効になります。

デバイスの関連度別ターゲット設定

標準のクライアント関連度を使用してターゲット設定を行うには、**関連度別にターゲット設定する**タブを使用します。関連度別にターゲット設定するタブでは、構文の強調表示のみが表示されます。ターゲット数の評価は行われません。
関連度ステートメントを使用してデバイスをターゲット設定する手順は、次のとおりです。

1. デプロイ・シーケンスで、**「ターゲットの選択」**アクションの**関連度別にターゲット設定する**タブを開き、関連度ステートメントを入力します。



注:

- ここで「プロパティー別にターゲット設定する」ビルダーが生成する関連度をコピーして貼り付けたり、変更したりできます。
- 関連度ステートメントのテキスト・ボックスでは、構文の強調表示が使用されます。ここに記述する関連度ステートメントは評価されません。関連度ステートメントの正しい書き方に関する詳細は、『Relevance ガイド』を参照してください。

2. **「適用」**をクリックします。

構成オプション

構成オプションを使用すると、デプロイメント・オプションを設定できます。使用可能なオプションは、BigFix 管理者による構成方法によって決まります。

左側のペインに構成カテゴリーを表示し、使用可能な構成を設定できます。各構成について詳細を確認するには、 アイコンをクリックします。「デプロイメントの要約」には設定したすべての構成の要約が表示され、デプロイの前に確認できます。デプロイメント・オプションを以下に示します。

実行

タイム・ゾーン、時刻、日付、曜日などを設定します。

- **タイム・ゾーン**:#クライアント時刻または UTC 時刻を選択できます。クライアント時刻は、BigFix クライアントのデバイスのローカル時刻です。協定世界時 (UTC) は、世界的に時計や時刻を規制する主要標準です。この選択は、すべての時間関連パラメーターに影響します。
- **開始**時刻と**終了**時刻の設定:#デプロイメントが特定の時刻に開始または終了するようスケジュールを設定し、ネットワークの負荷やデバイスの所有者の手間などを軽減します。複数のタイム・ゾーンにまたがってスケジューリングする場合、自身のタイム・ゾーンに対して過去の時間にアクションが開始するようにスケジュールを入力できます。このオプションでは、デプロイ・ボタンのクリック直後にデプロイメントが**すぐに**始まります。「終了日なし」オプションを選択すると、有効期限が設定されていない無期限のデプロイメントが作成され、継続的に稼働し、エンドポイントが要件を満たしているかのチェックが行われます。詳しくは、用語集 (（ページ）　　) を参照してください。
- **次の時間の間に実行**:#アクションを実行できる期間を定義します。この機能は、他の条件がすべて有効な場合にのみ、指定時刻に開始されます。
- **次の日に実行**:#一週間のうち 1 日以上の曜日を選択し、デプロイを定期的に実行します。
- **すべてのメンバー・アクションを実行**: このオプションは、複数のアクションがある場合にのみ表示されます。複数のアクション・グループ内のアクションは、順番に実行され、失敗した最初のアクションで停止します。失敗を無視し、次のアクションへと進むように MAG に指示するには、このオプションを選択します。MAG のアクションが先行するアクションに依存しない場合、このオプションを使用します。

  注: このオプションは、複数のアクションがある場合にのみ表示されます。

- **指定の場合のみ実行** 条件を設定する場合にのみチェック・ボックスを選択します。ドロップダウン・リストから条件を選択し、条件の値を指定します。

- **再試行**: このチェック・ボックスを選択すると、デプロイメントが失敗した場合に再試行するタイミングを設定できます。
- **アクションの再適用**:#このチェック・ボックスを選択すると、アクションを再適用するタイミングを設定できます。
- **ダウンロード:**#このチェック・ボックスを選択すると、開始時刻スケジュールに関係なくデプロイメント・ファイルを随時ダウンロードできます。デプロイメント前に、デプロイメント関連ファイルをベンダーのサーバーから BigFix サーバーに転送することで、それらのファイルを事前キャッシュします。ジョブのこの部分を最初に実行することで、大容量のファイルを処理する場合や、メンテナンス・ウィンドウが狭い場合に時間を節約できます。
- **ネットワーク・ロードを削減するため、デプロイメントを遅延**: 間隔を時間と分で入力します。

ユーザー

アクションを実行する前にログオン・ユーザー (または指定されたユーザーのグループ) が存在することが必要かどうかを指定できます。

- **アクションの実行**:#このオプションを選択すると、デプロイメントをログイン状況に応じて実行できます。
- **ユーザーの選択**: デプロイメントをすべてのユーザー、ローカル・セッションのユーザー、グループ内のユーザーに対して実行する必要がある場合に選択します。グループを選択するには、グループ名を入力して「挿入」をクリックします。

Messages

ターゲット・クライアントに表示する情報メッセージと、ユーザーによる操作のオプションを指定します。

- **アクションの実行前**: このオプションを選択すると、デプロイメントを実行する前にターゲット・コンピューターにメッセージを表示できます。
- **アクションの実行中**: このオプションを選択すると、デプロイメントの実行中にターゲット・コンピューターにメッセージを表示できます。

通知の送信

デプロイメントが失敗した場合または完了した場合に E メール・アラートをトリガーします。1 人以上の受信者を**「宛先:」**フィールドに入力し、複数のアドレスをコンマで区切ります。

- 失敗時に送信 - しきい値 (1〜250,000) を入力し、指定した数のデバイス上でデプロイメントが失敗した場合に 電子メールを受信します。
- 完了時に送信 - すべての対象でデプロイメントが完了した際に電子メールを受信するには、このボックスにチェック・マークを付けます。注: コンピューター・グループを対象としている場合にはこの通知オプションは使用できません。

オファー

この構成により、デバイス所有者がアクションを容認または拒否し、デプロイメントの実行タイミングを制御できるようにします。例えば、アプリケーションをインストールするかインストールしないか、またはインストールを日中ではなく夜間に実行するかどうかなどです。「提案」として設定されたアクションは、該当するマシン上のクライアント UI の提案リストで使用可能になります。ユーザーは利用可能な提案のリストを閲覧し、興味のある提案を適用できます。提案は、「ユーザー」タブで選択されたユーザーと、クライアント提案 UI が有効になっているマシンにのみ表示されます。構成するには、**「これを提案として送信」**チェック・ボックスを選択し、提案の説明を

入力します。**提案について通知を受ける**ように設定すると、提案がある場合に通知を受信できます。

注: 提案を無期限デプロイメントとして送信しないでください。無期限の提案は、ソフトウェアのオプションを完全に削除できないなど、デバイス所有者に問題を生じさせる可能性があります。

提案のオプション:

- **「ソフトウェア配信クライアント」**ダッシュボードに対してのみ - デバイスでクライアント UI が有効になっており、Self-Service Application が無効の場合に、ソフトウェア提案をクライアント UI の「ソフトウェア配信クライアント」ダッシュボードに表示します。Self-Service Application が有効になっている場合、すべての提案はそこに表示されます。
- **使用可能な提案があることをユーザーに通知** - 新規提案が使用可能であるという通知をエンドポイントに含めます。
- **提案の説明** - 表示されたボックスにアクションの説明を入力します。この説明はユーザーに対して表示されます。フォント、サイズ、スタイル、番号付け、およびフォーマット設定を変更して、説明をカスタマイズできます。提案に複数のアクションが含まれている場合、デフォルトで各コンポーネントの名前が含まれています。

ポスト・アクション

アクションのフォローアップ動作を指定します。

- **何もしない**: アクションの実行後に何もしない場合、このオプションを選択します。
- **コンピューターの再起動**: アクションの実行後にコンピューターを再起動する場合、このオプションを選択します。

- **再起動する前にプロンプトを出す**: アクティブなユーザーに対してメッセージを表示します。デフォルトのメッセージを送信するか、テキスト・ボックスにメッセージのタイトルとテキストを入力します。
- **ユーザーに再起動の取り消しを許可する**: デプロイメント後にユーザーが再起動をキャンセルできるようにします。
- ドロップダウンから日数、時間、分のいずれかの期限を設定し、期限がきたら自動的に再始動するか、ユーザーが承認するまでアクション・メッセージを上部に表示するかのオプションを選択します。

- **コンピューターをシャットダウンする**: アクションの実行後にコンピューターをシャットダウンする場合、このオプションを選択します。
  - **シャットダウン前にプロンプトを出す**: コンピューターをシャットダウンする前に、アクティブなユーザーにメッセージを表示します。デフォルトのメッセージを送信するか、テキスト・ボックスにメッセージのタイトルとテキストを入力します。
  - **シャットダウンのキャンセルを許可する:** デプロイメント後にユーザーがシャットダウンをキャンセルできるようにします。
  - ドロップダウンから日数、時間、分のいずれかの期限を設定し、期限がきたら自動的にシャットダウンするか、ユーザーが承認するまでアクション・メッセージを上部に表示するかのオプションを選択します。

適用の関連度

このタブは、コンソールの次のダイアログからでも使用できます。

- アクションの実行
- マルチアクションの実行
- 「コンピューター設定の編集」

Fixlet アクションの関連度を判断するために使用する基準を指定します。

- **元の Fixlet またはタスク・メッセージの関連度が真になった場合**。このオプションを選択し、デフォルト・アクションに設定された関連式を確認します。元の関連式を使用することを強く推奨します。ただし、カスタマイズしてニーズに合わせることもできます。
- **次のカスタム関連度が true と評価された場合**: このオプションを選択し、ニーズに即して既存の関連式を変更するか、新規の関連式を指定します。

成功条件

アクションを正常とみなす条件を定義します。以下のいずれかのオプションを選択します。

- **適用の関連度が false として評価された場合**

  これがデフォルトの成功条件です。この場合、アクションを適用可能にした Relevance ステートメントが TRUE でなくなることが求められます。Relevance ステートメントが問題を通知し、アクションがその問題を修正するので、成功を確立するには通常はこれで十分です。
- **アクション・スクリプト内のすべての行が正しく完了した場合**

  成功かどうかを、アクション・スクリプトのすべてのステップが完了したかどうかに応じて判断できます。
- **次のカスタム関連度が false と評価された場合**

  特殊な Relevance 句を使用して、アクションがその目標を達成したことを確認できます。この場合、画面のテキスト・ボックスが編集可能になり、新しい Relevance 句を作成したり、既存の Relevance 句を修正したりできます。

アクション・スクリプト

一般的に、Fixlet またはタスクに付属のアクション・スクリプトの使用をお勧めします。ただし、環境やビジネス・ニーズに合わせてアクション・スクリプトを調整すると便利な場合もあります。**「アクションの実行」**ダイアロ

グの**「アクション・スクリプト」**タブを使用して、アクション・スクリプトを変更できます。このダイアログには以下の 2 つのオプションがあります。

- **元の Fixlet またはタスク・メッセージから**

  ほとんどの Fixlet アクションではこれがデフォルトで、推奨されるオプションです。
- **カスタム・アクション・スクリプトから**

  以下のオプションのいずれかを選択し、既存のスクリプトを変更するか、テキスト域に新規スクリプトを入力することができます。このスクリプトに使用するアクション・スクリプトのタイプを選択します。
  - **BigFix アクション・スクリプト**

    これは、アクションの BigFix 標準スクリプト言語です。アクション言語について詳しくは、BigFix Developer Web サイト (*https://developer.bigfix.co m*) の「*Action Script Language*」セクション (https://developer.bigfix.com/action-script/) を参照してください。
  - **AppleScript**

    これはコンピューター・リソースを制御するための Apple のスクリプト言語です。
  - **SH**

    アクションは、Linux または UNIX または bsd シェルによって実行されるシェル・スクリプトです。
  - **PowerShell**

    バージョン 10.0.4 以降では、BigFix は PowerShell スクリプトも実行できます。

「アクション・スクリプト」テキスト・ボックスに記述したスクリプトを、選択した Windows クライアントで実行できます。このスクリプトは、Windows オペレーティング・システムによってデフォルトでインストールされている PowerShell 上の C:\Windows\System32\WindowsPowerShell\v1.0 ディレクトリー (使用可能な場合) または C:\Windows\SysWOW64\WindowsPowerShell\v1.0 で実行されます。

スクリプトは、デフォルトで **-ExecutionPolicy Bypass** オプションを使用して実行されます。このオプションを使用しないようにするには、『List of settings and detailed descriptions』ページの「Miscellaneous」セクションで説明されている `_BESClient_PowerShell_DisableExecPolicyBypass` クライアント設定を使用します。

非表示モードで実行されるため、ユーザー操作を必要とする PowerShell スクリプト、ポップアップ・ウィンドウまたはダイアログ・ボックスの表示はサポートされないため、アクションが実行状態のままになるか、スクリプトがログ・ファイルにエラーを表示する可能性があります。

注: デフォルトでは、アクションを元に戻すことはできません。使用するアクションは、小さい規模でテストしてからネットワーク全体に適用するようにしてください。

実行前後のスクリプト

このオプションは、ベースラインをデプロイするときに使用可能になります。アクション・スクリプトは、BigFix アクション・スクリプト、AppleScript、SH、PowerShell (（ページ） *206)* で記述できます。

- **実行前**: この複数のアクション・グループの実行前に実行するスクリプトを記述します。
- **実行後**: この複数のアクション・グループの実行後に実行するスクリプトを記述します。

第 11 章. デプロイメント入門

BigFix デプロイメントのモニターおよび完了の確認をするには、「デプロイメント」ビューを使用します。

デプロイメント・リスト

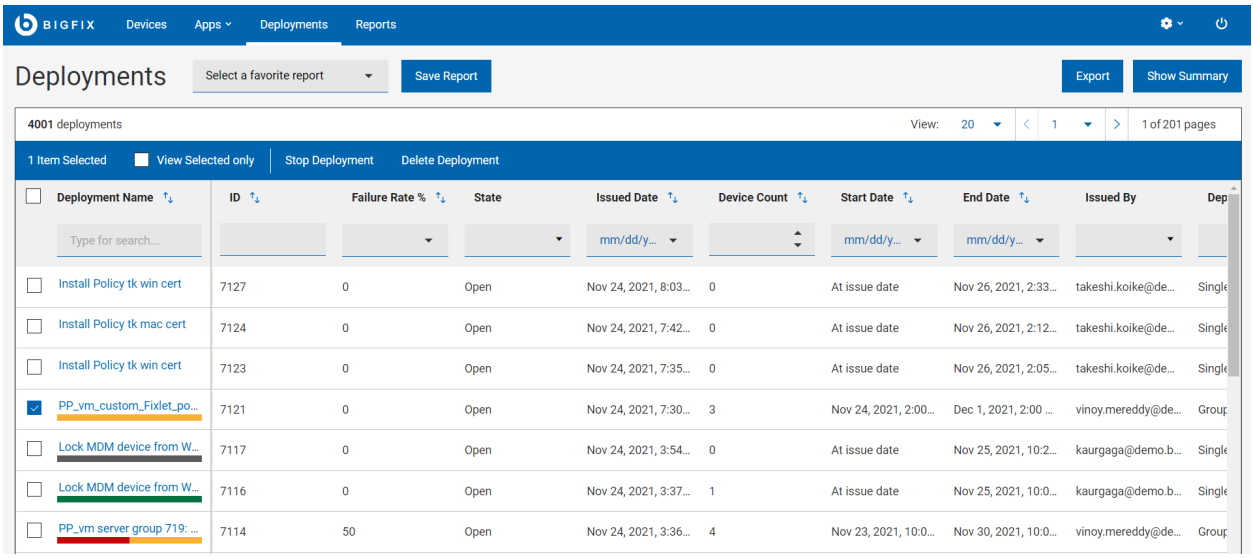
すべてのデプロイメントのリストを表示し、カスタマイズされたデプロイメントの要約レポートを作成して各デプロイメントの詳細情報を確認します。

「デプロイメント」ページにアクセスするには、WebUI のメイン・ページから**「デプロイメント」**を選択します。

WebUI デプロイメント画面には、権限の設定にかかわらず、すべてのデプロイメントのリストが表示されます。オペレーターは、すべてのデプロイメントを表示できますが、実行できるアクションは引き続き権限によって制御されます。例えば、WebUI パッチ画面にアクセスできないオペレーターにも、すべてのパッチ・デプロイメントが表示されますが、このオペレーターは実行中のパッチ・デプロイメントを停止できません。

WebUI は、WebUI、BigFix コンソール、BES サポートなどの外部サイトから開始されたアクションをすべて表示します。

以下のイメージは、デフォルトの列の順序で表示されたデプロイメント・データ・グリッドを示しています。デフォルトでは、データは「発行日」に基づいて降順にソートされます。列を並べ替えない場合、このビューはカスタマイズできません。



デプロイメントの管理

デプロイメントを管理するには、リストから 1 つ以上のデプロイメントを選択します。青いバーが表示されます。ユーザー権限に応じて、以下のアクションを実行できます。

- デプロイメントの停止 (（ページ） *219)* (`Open` の状態)。
- デプロイメントの削除 (`Expired` または `Stopped` の状態)。

デプロイメント・ステータス・バー

デプロイメントの名前のセルには、各デプロイメントの デプロイメント状況 (（ページ） 217) の概要を簡単に示す色付きのバーも表示されます。

結果の絞り込み

- **ソート順:** リストを以下の基準で並べ替えできます。
  - デプロイメント名
  - ID
  - 失敗率
  - 発行日
  - デバイス・カウント
  - 開始日
  - 終了日
- **フィルター**: デプロイメント・データをフィルタリングするには、目的の列のテキスト・フィールドをクリックし、検索ストリングを入力します。または目的の列のリストからオプションを選択します。
  - 検索を高速化するには、フィルターを組み合わせます。
    - **デプロイメント名**: 入力された検索ストリングを含むデプロイメントをフィルタリングします。
    - **ID**入力された ID の番号を含むデプロイメントをフィルタリングします。
    - **失敗率 (%)** : デプロイメントを、指定した失敗率でフィルタリングします。

- **状態**: 期限の切れた、開いている、または停止したデプロイメントすべてにフィルタリングします。
- **発行日**: 日、週、月、四半期、または特定の日付または日付範囲内に発行されたデプロイメントをフィルタリングします。
- **デバイス・カウント** : 適用可能なデプロイメント、または指定された最小デバイス数で発行されたデプロイメントをフィルタリングします。
- **開始日**: 日、週、月、四半期、または特定の日付または日付範囲内に開始するすべてのデプロイメントをフィルタリングします。
- **終了日**: 日、週、月、四半期、または特定の日付または日付範囲内に終了するすべてのデプロイメントをフィルタリングします。
- **発行者**: ログイン中のユーザーまたは指定したユーザーによって発行されたデプロイメントにフィルタリングします。
- **デプロイメント・タイプ**: 単一のコンテンツ (Fixlet、ソフトウェア、タスク) またはグループ (複数のアクション・グループ、ベースライン) を対象とするすべてのデプロイメントをフィルタリングします。
- **動作**: ユーザー・メッセージを含むデプロイメント、オファー・タイプのデプロイメント、無期限のデプロイメント、エンドポイントを再起動するデプロイメントなどの特定の動作でデプロイメントをフィルタリングします。
- **アプリケーション・タイプ**: 特定のアプリケーション・タイプに属するデプロイメントにフィルタリングします。
- **ソース・サイト**: 特定のサイトに属するすべてのデプロイメントをフィルタリングします。

注: デフォルトでは、最大 5 つのフィルターを組み合わせて同時に処理できます。フィルターの最大数を超えると、パフォーマンスに影響します。デフォルト値は、`_WebUIAppEnv_MAX_FILTERS_NUMBER` の設定を使用して構成できます。

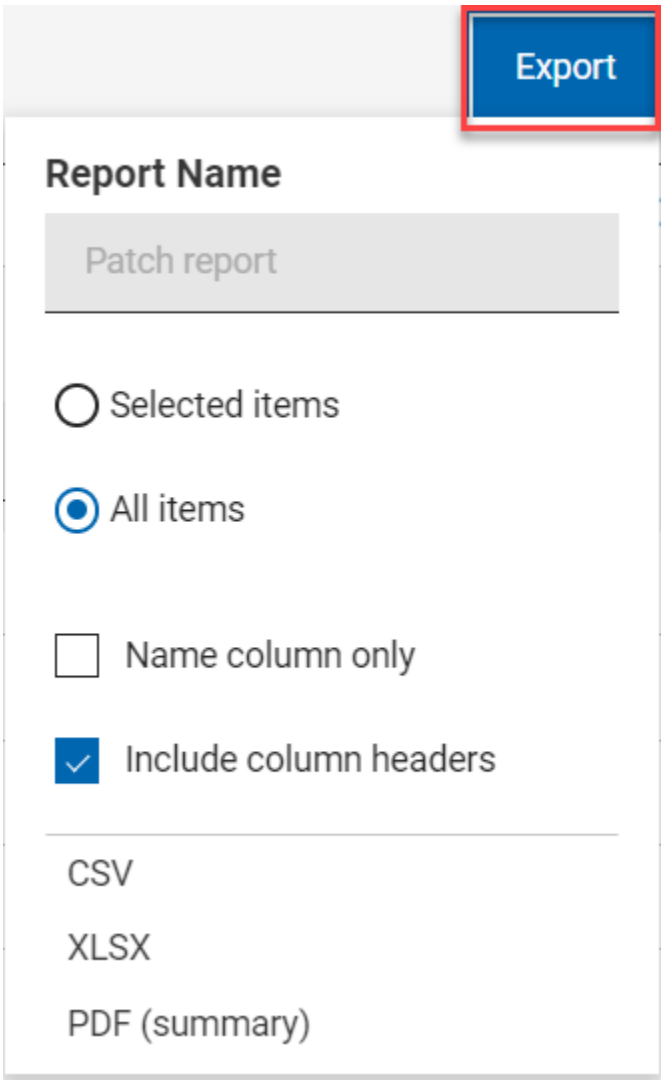
◦ すべての選択済みフィルターをクリアするには、「すべてのフィルターのリセット」をクリックします。

デプロイメント・レポート

- **レポートの保存**: レポートを将来の参照のために保存し、必要に応じて編集、更新、または削除します。詳しくは、「レポート (（ページ） *16)*」を参照してください。
- **要約の表示:**
  1. **「デプロイメント」**ページで、必要なフィルターを選択します。
  2. **「要約を表示」** をクリックします。デプロイメント・データをグラフやテーブルとして表示できます。グラフ上の調べたいエリアにカーソルを合わせると、そのデータ・ポイントとパーセンテージ・データの詳細が表示されます。文字が切り詰められたラベルにカーソルを合わせると、ツール・ヒントにすべてのテキストが表示されます。フィルターを変更するか、検索テキストを入力すると、該当する情報がレポートに動的に表示されます。
  3. **デプロイメント日ごとのデプロイメント状態**: デプロイメント総数とデプロイメント開始日以来の一定期間のデプロイメント状態を表示します。
  4. **失敗率 (%)**: デプロイメント総数とさまざまなカテゴリーにおける 0〜100 の失敗率を表示します。
  5. **アプリケーション・タイプごと**: デプロイメント総数と各アプリケーション・タイプを表示します。
- **エクスポート:**

  フィルターされたレポートは `.csv`、`.xlsx`、または `.pdf` の形式でエクスポートできます。

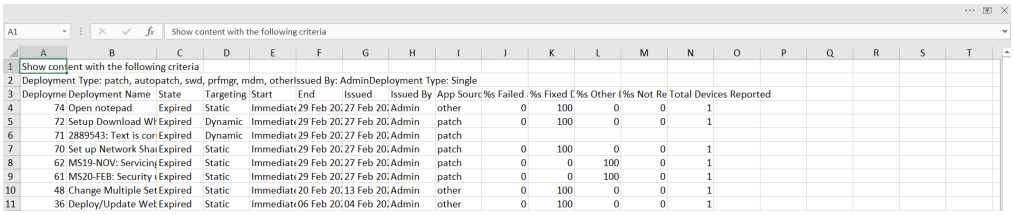
  1. **「デバイス」**ページで、必要なフィルターを選択します。
  2. **「エクスポート」**をクリックします。



3. **「選択された項目」**オプションを使用すると、フィルターされた結果から選択した項目をエクスポートできます。**「すべての項目」**を使用すると、フィルター処理されたリストからすべての項目をエクスポートできます。最適なオプションを選択してください。
4. 名前列のみ: フィルターされた項目の名前のみをエクスポートする場合は、このオプションを選択します。
5. 列ヘッダーを含める: 項目のすべてのデフォルトの列の詳細をエクスポートする場合は、このオプションを選択します。

注: デフォルトの列以外の列を表示している場合は、名前列のみをエクスポートできます。

6. エクスポート先のファイル形式 (CSV、XLSX、PDF) を選択します。
   - デフォルトでは、レポートは「ダウンロード」フォルダーにダウンロードされ、デフォルトのファイル名 (Device_Report_mm_dd_yyyy_username) が付けられます。ブラウザー内でダウンロード設定を変更すると、ファイル名やダウンロードの保存先を変更できます。レポートを保存して後で参照したり、利害関係者と共有したりできます。
   - PDF 形式を選択した場合、数値データを含む `.csv` ファイルとデータの表示形式を含む `.pdf` ファイルを含む `.zip` ファイルがダウンロードされます。
   - エクスポートされたデプロイメント・レポートには、フィルターや検索条件を介して選択したデプロイメントに関する主な情報が含まれます。これらの情報には、デプロイメント ID、デプロイメント名、デプロイメントの状態、さらにすべてのデプロイメントを展開したときに画面に表示されるその他の詳細情報が含まれます。以下はサンプル・レポートです。



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
1	Show content with the following criteria																			
2	Deployment Type: patch, autopatch, swd, prfmgr, mdm, other							Issued By: Admin	Deployment Type: Single											
3	Deployme	Deployment Name	State	Targeting	Start	End	Issued	Issued By	App Sourc	%s Failed	%s Fixed	%s Other	%s Not Re	Total Devices Reported						
4	74	Open notepad	Expired	Static	Immediat	29 Feb 20;	27 Feb 20;	Admin	other	0	100	0	0	1						
5	72	Setup Download WI	Expired	Dynamic	Immediat	29 Feb 20;	27 Feb 20;	Admin	patch	0	100	0	0	1						
6	71	2889543: Text is cor	Expired	Dynamic	Immediat	29 Feb 20;	27 Feb 20;	Admin	patch											
7	70	Set up Network Sha	Expired	Static	Immediat	29 Feb 20;	27 Feb 20;	Admin	patch	0	100	0	0	1						
8	62	MS19-NOV: Servicing	Expired	Static	Immediat	29 Feb 20;	27 Feb 20;	Admin	patch	0	0	100	0	1						
9	61	MS20-FEB: Security (	Expired	Static	Immediat	29 Feb 20;	27 Feb 20;	Admin	patch	0	0	100	0	1						
10	48	Change Multiple Set	Expired	Static	Immediat	20 Feb 20;	13 Feb 20;	Admin	other	0	100	0	0	1						
11	36	Deploy/Update Wel	Expired	Static	Immediat	06 Feb 20;	04 Feb 20;	Admin	other	0	100	0	0	1						

デプロイメント文書

デプロイメントのデプロイメント状況、動作 (構成で設定)、対象の情報を表示するには、そのデプロイメント名をクリックします。関連付けられたビューへのリンクを使用して、デプロイメントの詳細を掘り下げます。

デプロイメント文書の各ビューは以下のとおりです。

- 概要 – 状況、動作、対象など、選択したデプロイメントの詳細説明。
- デバイス結果 - 対象の状況 – 各エンドポイント上のデプロイメントの状況。
- コンポーネント結果 – 複数のアクションを持つコンテンツ用。対象デバイス上の各コンポーネントのデプロイメントの状況が成功率で表される。

注: パフォーマンス上の理由から、アクションに 200 を超える項目が含まれている場合、各コンポーネントのデプロイメント状況は取得されません。

デプロイメントのモニタリング: 状態、状況、結果

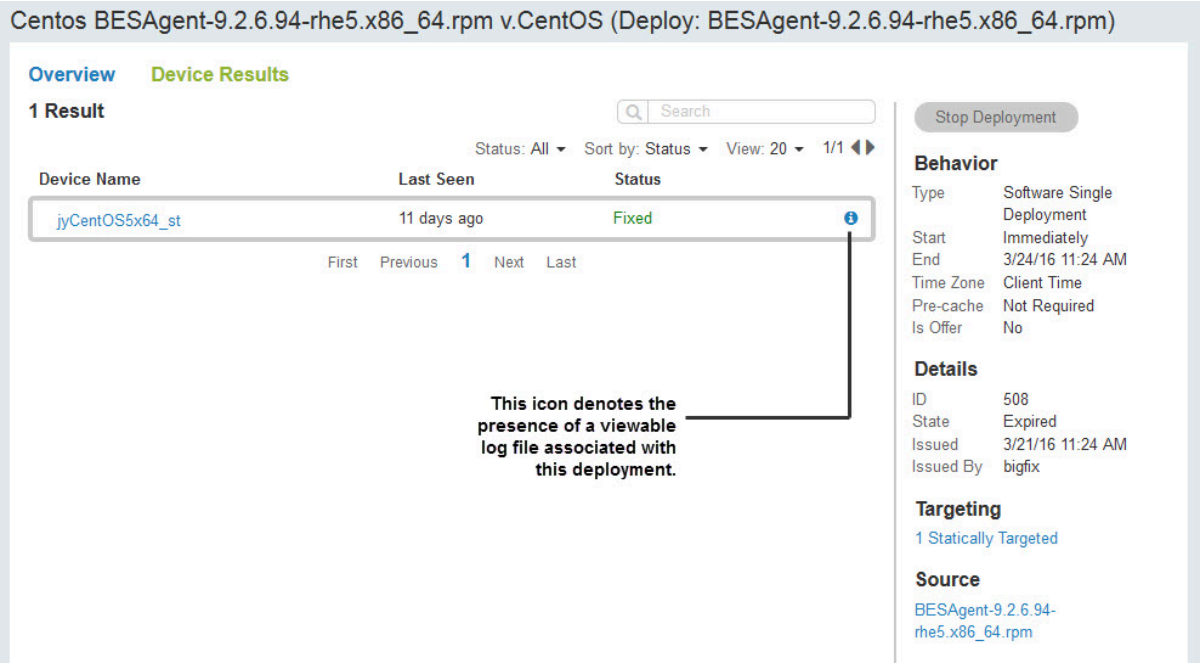
デバイス結果、デプロイメント状況、デプロイメント状態の間の違いを理解して、デプロイメント結果を正しく解釈してください。

デバイス結果

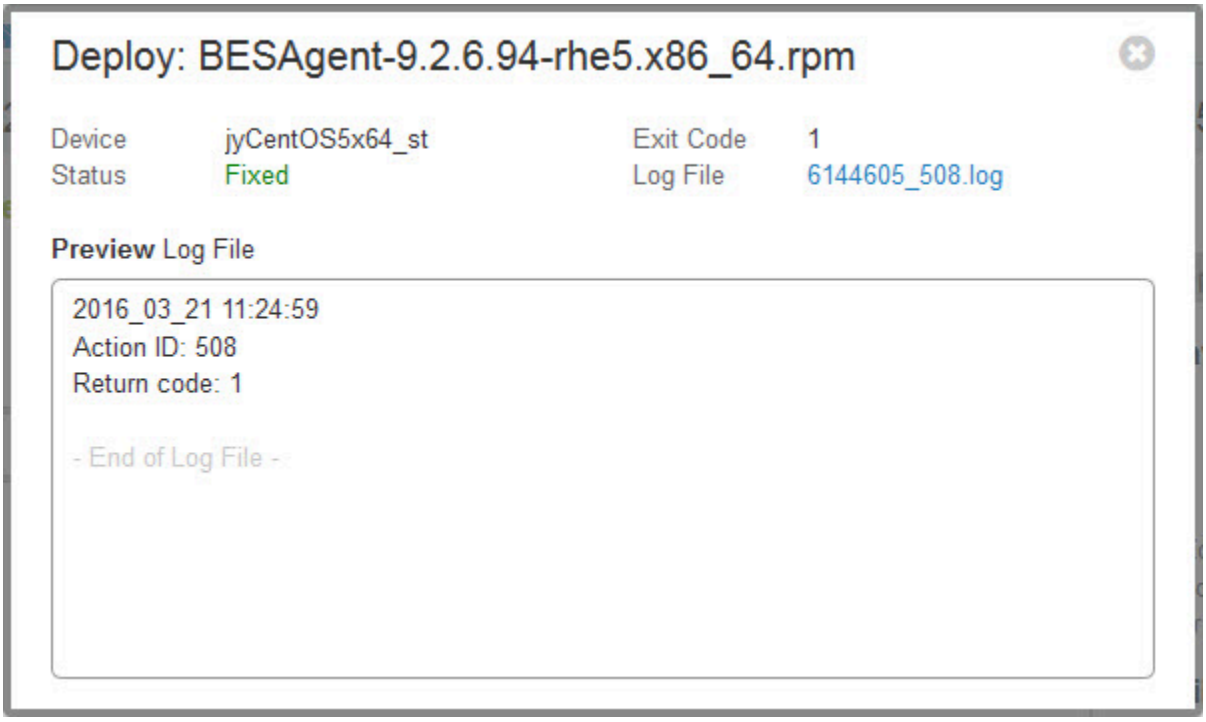
デバイス結果は、特定のエンドポイントでのデプロイメントの状態について説明します。さまざまな BigFix デバイス結果コードがあります。WebUI で見られる最も一般的なコードは、以下のとおりです。

- 修正済みまたは完了 - デプロイメントはこのデバイス上で正常終了しました。
- 失敗 - デプロイメントはこのデバイス上で失敗しました。
- 再起動の保留中 - 最終的な成功が示唆されています。
- 関連なし - アクションはこのデバイスに関連していません。
- 実行中
- 評価中
- ダウンロードの保留中

ソフトウェア・デプロイメントには、関連付けられたログ・ファイルがある場合があります。このログは、「デバイス結果」画面で参照できます。表示可能なログ・ファイルの存在は、アイコンによって表示されます。ログ・ファイルはソフトウェアのデプロイメントにのみ使用できます。



ログ・アイコンをクリックして、関連付けられているログ・データを表示します。ログ・ファイル名をクリックすると、完全なログをダウンロードできます。

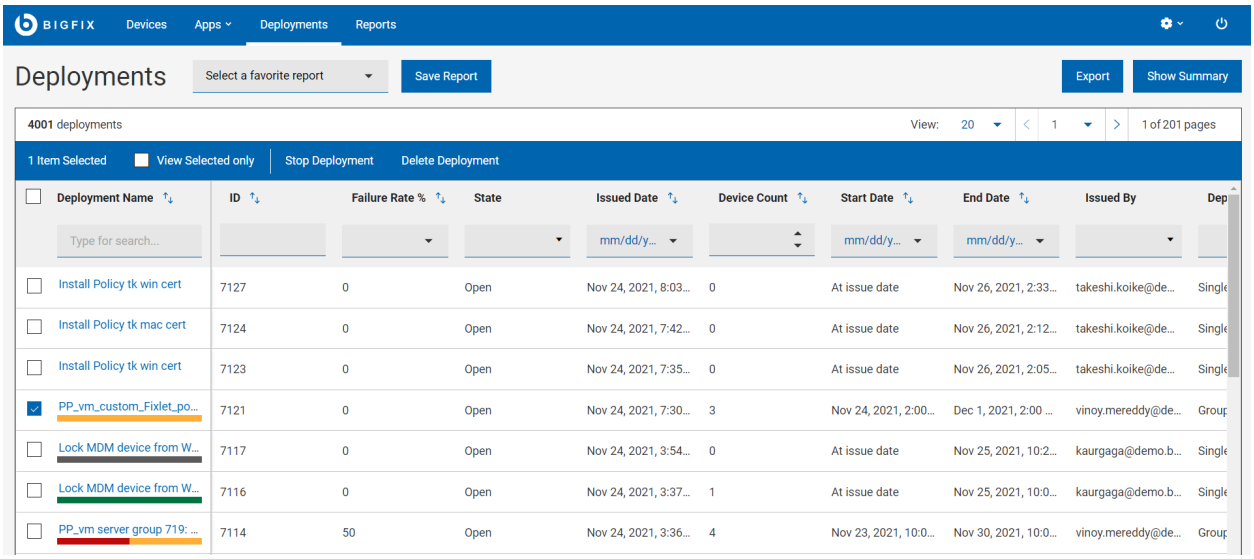


注: ログ・ファイルは、ソフトウェア・デプロイメントに関してのみ表示できます。さらに、BigFix WebUI 内でログ・ファイルを表示するには、現在のユーザーは従来の BigFix コンソール内のソフトウェア配信サイトをサブスクライブして、ソフトウェア配信サイトの分析 11 をアクティブにする必要があります。

デプロイメント状況

デプロイメント状況はデバイス結果を使用して表現されます。

- 単一のアクションを持つデプロイメントの場合、デプロイメント状況は各対象デバイスの累積のデプロイメント状況であり、成功率で表されます。
- 複数のアクションを持つデプロイメントの場合、デプロイメント状況は各対象デバイスの各コンポーネントの累積のデプロイメント状況であり、成功率で表されます。



- 緑 - 修正済み (パッチ)、または完了済み (ソフトウェア、カスタム・コンテンツ) デプロイメント。
- 灰色 - まだレポートされていない、または関連なし。
- 赤 - エラーのあるデプロイメントと失敗したデプロイメント。

- 黄 - 再起動の保留中、実行中、評価中、ダウンロードの保留中など、その他すべての状態。
- ステータス・バーなし – 関連デバイスなし。

デプロイメント状態

デプロイメント状態は、エンドポイント上で実行するデプロイメントの適格性について説明します。デプロイメント状況の計算には関連しません。

デプロイメント状態には以下の 3 つの値があります。

- 進行中 - デプロイメントは、エンドポイントで実行される資格があります。
- 有効期限切れ - デプロイメントは、すべてのタイム・ゾーンですべての有効なエンドポイントの終了時刻が経過したため、もう実行する資格がありません。アクションのデフォルトの有効期限は 2 日です。
- 停止 - デプロイメントは、オペレーターまたは管理者によって停止されたため、もう実行する資格がありません。

要約: デバイス結果は、特定のデバイスの特定のデプロイメントの結果です。デプロイメント状態は、実行するデプロイメントの適格性について説明します。デプロイメント状況は、対象エンドポイントでのデプロイメントの累積結果を提供します。

複数のアクションを持つデプロイメントの評価

グループまたはベースラインを伴うものなど、複数のアクションを持つデプロイメントの状態を正確に把握するには、個々のコンポーネントの状況を確認してください。つまり、デプロイメント・グループの状況が 100 % 未満の場合には、その内のどのコンポーネントがまだ完了していないのかを確認してください。

1. デプロイメント・リストを開きます。
2. 「デプロイメント・タイプ」フィルターを使用して、グループ・デプロイメントのリストを表示します。
3. 必要なデプロイメントを選択し、その文書を開きます。
4. **「コンポーネント結果」**をクリックします。

注: パフォーマンス上の理由から、アクションに 200 を超える項目が含まれている場合、各コンポーネントのデプロイメント状況は取得されません。

デプロイメントの停止

すべてのデプロイメントが最初から正常に完了するわけではありません。必要に応じて、任意のデプロイメント・リストまたは文書ビューにある**「デプロイメントの停止」**ボタンを使用してデプロイメントを終了します。

デプロイメントが停止する理由には、以下があげられます。

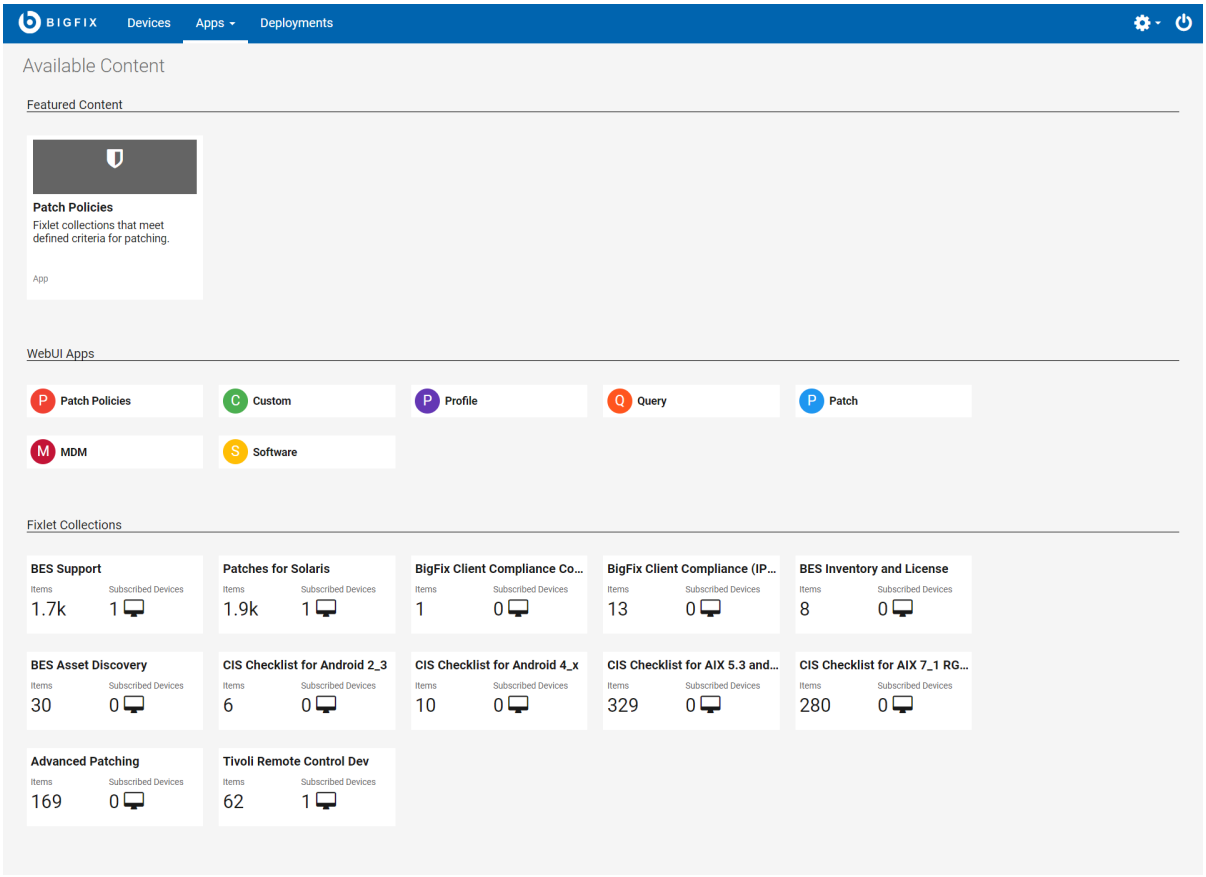
- 多くのデバイスで失敗が確認され始めた。
- 対象デバイスでブルー・スクリーンが表示され始めた。
- ベースライン (または Fixlet) を更新したため、古い方を停止する必要がある。

デプロイメントの問題を診断して修正するには、BigFix 管理者によって提供されたデプロイメント・ビューおよびカスタム・ツールを使用します。デプロイメント・ビューやカスタム・ツールを使用して、デプロイメントが失敗した原因と、問題が発生した際の効果的な解決策を見つけます。デプロイメントが失敗する理由には、以下があげられます。

- コンピューターがオフラインである。
- コンピューターが再構築中であるか、イメージの再作成中である。
- コンピューターのディスクの空き容量が不足している。
- コンピューターが BigFix 更新サーバーと通信していない。
- BigFix agent がコンピューター上で実行されていない。
- いくつかの依存ソフトウェアがコンピューター上で欠落している。

第 12 章. コンテンツ・アプリケーション入門

コンテンツ・アプリケーションは、BigFix サイトで Fixlet、タスク、およびベースラインを処理するために使用します。標準の WebUI ツールでコンテンツの検索、フィルター処理、デプロイができます。



注:

- 「コンテンツ・アプリケーション」に表示されるサイトは、サブスクライブ済みのサイトと、ログインしているユーザーに付与されている権限によって異なります。
- また、WebUI アプリケーションにまだ関連付けられていないサイトも一覧表示されます。

「おすすめのコンテンツ」セクションでは、新規サイト、新規アプリケーション、新機能を搭載したアプリケーションが強調表示されています。「WebUI アプリケーション」セクションでタイルをクリックすると、WebUI アプリケーションが開きます。オペレーターは、「コンテンツ・アプリケーション」で許可されるサイトのホワイト・リストのサイトを閲覧できます。マスター・オペレーターは、WebUI アプリケーション・コレクションに含まれないサイトもすべて閲覧できます。

注: Fixlet の中にはデプロイできないものもあります。次のような Fixlet をデプロイするときは「コンテンツ・アプリケーション」を使用しないでください。

- アクションを実行するかアクションを保護する JavaScript など、JavaScript を含むか使用している
- セッション関連度を使用している
- 特殊なコンソール API を使用している

該当する Fixlet は実行されませんが、デバイスで問題の存在を知らせるレポートの返すようになるまでは、問題があることを示す情報 (エラーなど) が表示されません。デプロイできる Fixlet かどうかが不明確な場合は、想定外の動作を防ぐため、該当する Fixlet を BigFix コンソールで実行します。

オペレーター・アクセス

以下のリストは、オペレーターのタイプによって実行できるアクティビティーをまとめたものです。

- マスター以外のオペレーターは、WebUI アプリケーションの BES サポートにアクセスできません。マスター・オペレーターのみを対象としています。
- マスター・オペレーターは外部サイトをすべて参照できますが、表 1 に記載の以下 2 つのサイトは除きます。
- マスター以外のオペレーターは表示できる外部サイトにのみアクセスできます。表 2 に記載のアクセス可能なホワイトリスト・サイトを参照してください。

表 15. マスター・オペレーターがアクセスできない外部サイトのリスト

サイト ID	サイト名
8361	OS Deployment およびベア・メタル・イメージ
8363	OS Deployment およびベア・メタル・イメージ・ベータ

表 16. マスター以外のオペレーターがアクセスできるホワイトリスト・サイトのリスト

サイト ID	サイト名
12249	拡張パッチ
3107	BES Asset Discovery
3073	BigFix クライアント・コンプライアンス (IPSec フレームワーク)
3043	BigFix クライアント・コンプライアンス構成
9287	BigFix ラボ

サイト ID	サイト名
8253	BitLocker 管理 (ラボ)
11316	AIX 5.3 および 6.1 の CIS チェックリスト
11316	AIX 5.3 および 6.1 の CIS チェックリスト
11522	AIX 7.1 - RG03 の CIS チェックリスト
12070	Apache HTTP Server 2.2 (Linux) の CIS チェックリスト
12391	CentOS Linux 6 の CIS チェックリスト
12410	CentOS Linux 7 の CIS チェックリスト
11535	Linux の DB2 の CIS チェックリスト
11536	DB2 (Windows) の CIS チェックリスト
15106	Internet Explorer 10 の CIS チェックリスト
12337	Internet Explorer 11 の CIS チェックリスト
12339	Mac OS X 10.10 の CIS チェックリスト
12354	Mac OS X 10.11 の CIS チェックリスト

サイト ID	サイト名
12425	Mac OS X 10.12 の CIS チェックリスト
11313	Mac OS X 10.6 の CIS チェックリスト
12389	Mac OS X 10.8 の CIS チェックリスト
11566	MS IIS 7 の CIS チェックリスト
12509	MS IIS 8 の CIS チェックリスト
11568	MS SQL Server 2005 の CIS チェックリスト
11570	MS SQL Server 2008 R2 の CIS チェックリスト
11574	MS SQL Server 2012 DB Engine の CIS チェックリスト
11539	Oracle Database 11-11g R2 (Linux) の CIS チェックリスト
11540	Oracle Database 11-11g R2 (Windows) の CIS チェックリスト
11537	Oracle Database 9i-10g (Linux) の CIS チェックリスト

サイト ID	サイト名
11538	Oracle Database 9i-10g (Windows) の CIS チェックリスト
12373	Oracle Linux 6 の CIS チェックリスト
12364	Oracle Linux 7 の CIS チェックリスト
11318	RHEL 5 の CIS チェックリスト
11366	RHEL 6 の CIS チェックリスト
12181	RHEL 7 の CIS チェックリスト
12187	SLES 10 の CIS チェックリスト
12518	SLES 11 の CIS チェックリスト
11317	Solaris 10 の CIS チェックリスト
11526	Solaris 11 - RG03 の CIS チェックリスト
12465	SUSE 12 の CIS チェックリスト
12453	Ubuntu 12.04 LTS Server の CIS チェックリスト

サイト ID	サイト名
12439	Ubuntu 14.04 LTS Server の CIS チェックリスト
12429	Ubuntu 16.04 LTS Server の CIS チェックリスト
12288	の CIS チェックリスト
11356	Windows 2003 DC の CIS チェックリスト
11358	Windows 2003 MS の CIS チェックリスト
13083	Windows 2008 DC - RG03 の CIS チェックリスト
13085	Windows 2008 MS - RG03 の CIS チェックリスト
13075	Windows 2008 R2 DC の CIS チェックリスト
13077	Windows 2008 R2 MS の CIS チェックリスト
12064	Windows 2012 DC の CIS チェックリスト
12066	Windows 2012 MS の CIS チェックリスト
12057	Windows 2012 R2 DC の CIS チェックリスト
12061	Windows 2012 R2 MS の CIS チェックリスト

サイト ID	サイト名
12469	Windows 2016 DC の CIS チェックリスト
12471	Windows 2016 MS の CIS チェックリスト
11491	Windows 7 の CIS チェックリスト
12093	Windows 8 の CIS チェックリスト
15107	Windows 8.1 の CIS チェックリスト
11360	Windows XP の CIS チェックリスト
9342	Client Manager Builder
8151	Application Virtualization の Client Manager
75	Client Manager for Endpoint Protection
9318	TPMfOSD の Client Manager
11035	AIX 5.1 の DISA STIG チェックリスト
11036	AIX 5.2 の DISA STIG チェックリスト
11434	AIX 53 - RG03 の DISA STIG チェックリスト

サイト ID	サイト名
11436	AIX 61 - RG03 の DISA STIG チェックリスト
11354	AIX 7.1 の DISA STIG チェックリスト
11040	HPUX 11.11 の DISA STIG チェックリスト
11460	HPUX 11.23 - RG03 の DISA STIG チェックリスト
11462	HPUX 11.31 - RG03 の DISA STIG チェックリスト
11458	Internet Explorer 10 - RG03 の DISA STIG チェックリスト
12068	Internet Explorer 11 - RG03 の DISA STIG チェックリスト
11454	Internet Explorer 8 - RG03 の DISA STIG チェックリスト
11456	Internet Explorer 9 - RG03 の DISA STIG チェックリスト
12309	Mac OS X 10.10 の DISA STIG チェックリスト
12427	Mac OS X 10.11 の DISA STIG チェックリスト
12225	Mac OS X 10.8 の DISA STIG チェックリスト

サイト ID	サイト名
12346	Mac OS X 10.9 の DISA STIG チェックリスト
12497	Oracle Linux 6 の DISA STIG チェックリスト
11042	RHEL 3 の DISA STIG チェックリスト
11043	RHEL 4 の DISA STIG チェックリスト
11430	RHEL 5 - RG03 の DISA STIG チェックリスト
11440	RHEL 6 RG03、CentOS Linux 6 RG03 の DISA STIG チェックリスト
12412	RHEL 7、CentOS Linux 7 の DISA STIG チェックリスト
11432	Solaris 10 - RG03 の DISA STIG チェックリスト
12281	Solaris 11 の DISA STIG チェックリスト
11045	Solaris 8 の DISA STIG チェックリスト
11046	Solaris 9 の DISA STIG チェックリスト
11048	SUSE 10 の DISA STIG チェックリスト

サイト ID	サイト名
11059	SUSE 11 の DISA STIG チェックリスト
11058	SUSE 9 の DISA STIG チェックリスト
12289	Windows 10 の DISA STIG チェックリスト
11141	Windows 2003 DC の DISA STIG チェックリスト
11142	Windows 2003 MS の DISA STIG チェックリスト
11143	Windows 2008 DC の DISA STIG チェックリスト
11144	Windows 2008 MS の DISA STIG チェックリスト
11145	Windows 2008 R2 DC の DISA STIG チェックリスト
11146	Windows 2008 R2 MS の DISA STIG チェックリスト
11575	Windows 2012 DC の DISA STIG チェックリスト
11577	Windows 2012 MS の DISA STIG チェックリスト
12467	Windows 2016 の DISA STIG チェックリスト
11140	Windows 7 の DISA STIG チェックリスト

サイト ID	サイト名
11564	Windows 8 の DISA STIG チェックリスト
11147	Windows Vista の DISA STIG チェックリスト
11148	Windows XP の DISA STIG チェックリスト
11120	Internet Explorer 7 の FDCC チェックリスト
11123	Windows Vista の FDCC チェックリスト
11124	Windows Vista ファイアウォールの FDCC チェックリスト
11121	Windows XP の FDCC チェックリスト
11122	Windows XP ファイアウォールの FDCC チェックリスト
13013	IBM License Reporting (ILMT)
8506	MaaS360 モバイル・デバイス管理
12380	管理対象脆弱性
8150	パッチ・サポート
8102	電源管理
15105	QRadar の脆弱性

サイト ID	サイト名
8110	Remote Control
6113	SCM レポート作成
9188	ソフトウェア配信
8032	Tivoli Endpoint Manager for Software Usage Analysis v1.3
9072	Trend Common Firewall
9095	Mac の Trend Core Protection Module
11119	Internet Explorer 7 の USGCB チェックリスト
11113	Internet Explorer 8 の USGCB チェックリスト
12106	RHEL 5 の USGCB チェックリスト
11110	Windows 7 の USGCB チェックリスト
11112	Windows 7 Energy の USGCB チェックリスト
11111	Windows 7 ファイアウォールの USGCB チェックリスト
11116	Windows Vista の USGCB チェックリスト
11114	Windows Vista Energy の USGCB チェックリスト

サイト ID	サイト名
11115	Windows Vista ファイアウォールの USGCB チェックリスト
11118	Windows XP の USGCB チェックリスト
11117	Windows XP ファイアウォールの USGCB チェックリスト
8346	Virtual Endpoint Manager
5040	Windows システムの脆弱性
9112	Windows 7 移行
9173	Windows 販売サイト
8232*	Mac アプリケーションの更新
5095*	Windows アプリケーションの更新

重要: *これらのサイトからのコンテンツは、**「パッチ」**アプリケーションで利用可能です。

第 13 章. Extension Management アプリケーション入門

BigFix Extension Management アプリケーションを使用すると、現在使用可能な製品で提供されている機能を超えて WebUI 機能を拡張できます。WebUI にアドホック拡張機能を追加することで、現在製品によって処理されていない特定のユース・ケースに対応できます。

拡張機能の開発

このリリースでは、ニーズに合わせたインターフェースのカスタマイズを迅速化するために、拡張機能の開発は HCL 担当者に限定されています。この機能の今後のリリースでは、HCL が提供するパブリック・ツールキットを使用して、組織が独自に拡張機能を開発できるようになります。

プロセス・フローの概要

カスタマイズされた拡張機能を開発して管理するための手順の概要は、次のとおりです。

1. 組織は HCL 担当者に連絡してビジネス要件を定義し、HCL 内の適切なチームと連携して拡張機能を開発します。
2. HCL チームは、WebUI の拡張機能を開発して、お客様の要求に対応するために WebUI で使用できない新機能を追加し、外部サイトに公開するか、拡張ファイルを共有することによって拡張機能を配布します。
3. WebUI 管理者は、WebUI の Extension Management の機能を有効にします。
4. 組織からの WebUI ユーザー (必要なカスタム・サイトに対する読み取り/書き込み権限を持つマスター・オペレーターまたはコンテンツ作成者) は、拡張アプリケーション・ファイル (`*.webui`) を受信またはダウンロードしてカスタム・サイトにインストールします。
5. 拡張機能がインストールされると、「Extension Management」の WebUI からアクセスできるようになります。適切なサイト・アクセス権と権限を持つユーザーは、それらの権限を他のアプリケーションとシームレスに連携して使用し、WebUI から拡張機能を管理できます。

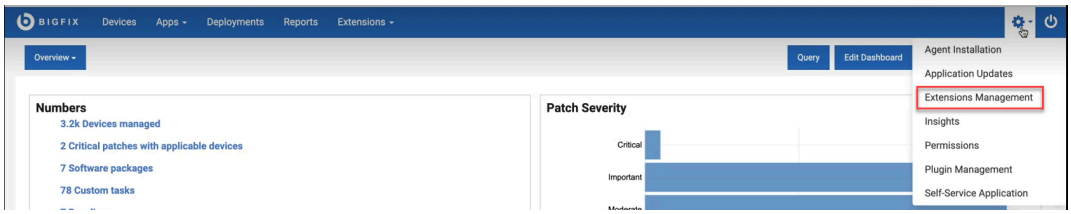
Extension Management へのアクセス

デフォルトでは、Extension Management は WebUI に追加されません。追加するには、WebUI 管理者に連絡してサーバー設定 `_WebUIAppEnv_ENABLE_EXTENSIONS_MANAGEMENT` (（ページ）) を構成してください。サーバー設定の変更を有効にするには、構成後に WebUI を再起動します。

ユーザーおよび役割

マスター・オペレーターとコンテンツ作成者

マスター・オペレーターとコンテンツ作成者は、Extension Management アプリケーションをインストール、管理、および使用できます。



拡張機能アプリケーションは、次のように管理できます。

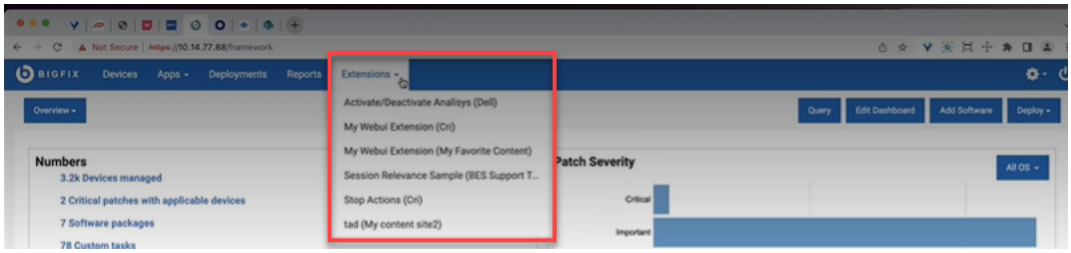
- HCL 担当者の指示に従って、外部サイトまたは拡張ファイル (`*.webui`) から新しい拡張子をインストールします。
- 拡張機能を起動する
- 拡張機能を修復する
- 拡張機能を更新する
- 拡張機能を検索、ソート、フィルタリング、およびナビゲートする
- 古くなった拡張機能をアンインストールまたは削除する

注:

- マスター・オペレーターは、すべてのカスタム・サイトにアクセスできるため、組織で使用可能なすべての拡張機能を管理できます。コンテンツ作成者は、拡張機能にアクセス可能なサイト内で使用可能な拡張機能のみを管理できます。
- 外部サイトは、マスター・オペレーターとコンテンツ作成者の両方の読み取り専用サイトであり、外部サイトから拡張機能を削除することはできません。

マスター以外のオペレーター

NMO (マスター以外のオペレーター) は、カスタム・サイトにインストールされている拡張機能を表示できます。NMO は「拡張機能」メニューから拡張機能アプリケーションを起動して操作できます。NMO は、拡張機能に対して管理アクションを管理または実行することはできません。



:

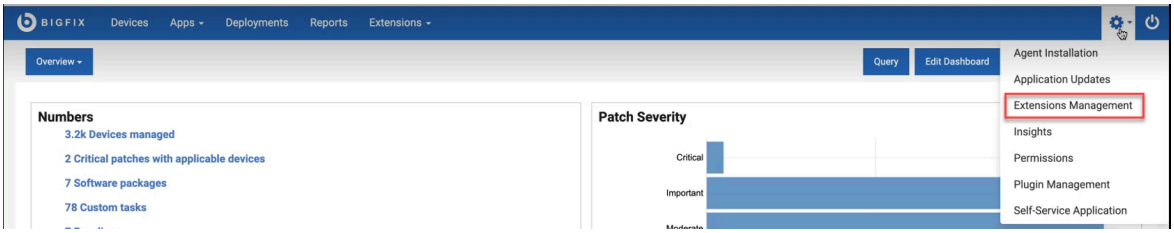
サイトからの拡張機能のインストール

このページでは、外部サイトから拡張機能をインストールする方法について説明します。

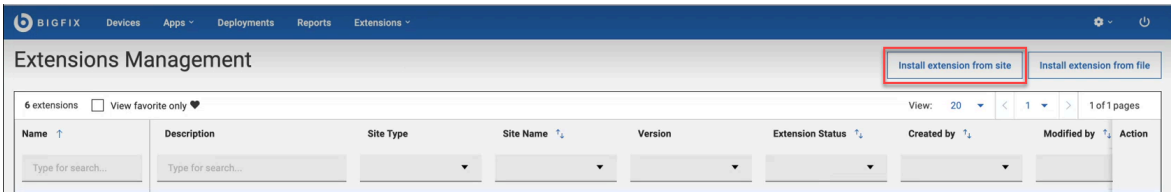
- このタスクを実行するには、マスター・オペレーターまたはコンテンツ作成者で、必要なカスタム・サイトの読み取り/書き込みアクセス権が必要です。
- 外部サイトで拡張機能が使用可能になっていることを確認します。

外部サイトから拡張機能をインストールするには、次の手順を実行します。

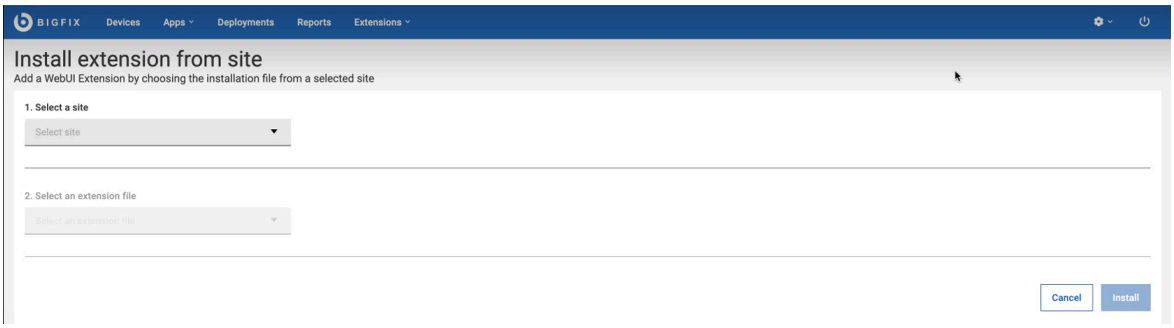
1. 適切な資格情報を使用して WebUI にログインします。
2. メニュー・バーから設定をクリックし、**「Extensions Management」**を選択します。



3. Extension Management のページで**「サイトから拡張機能をインストール」**をクリックします。



4. 以下のページが表示されます。



ドロップダウンから:

a. 拡張機能ファイルが使用可能なサイトを選択します。

> **注:** アクセス権があるサイトのみが表示されます。

b. 拡張機能ファイルを選択します。選択したサイトに公開されている、すべての拡張機能が表示されます。

5. **「インストール」**をクリックします。
6. 拡張機能が正常にインストールされると、Extension Management のページに表示されます。

関連情報

拡張に対する作業 (（ページ） 239)

拡張機能の更新 (（ページ） 242)

拡張機能のアンインストール (（ページ） 245)

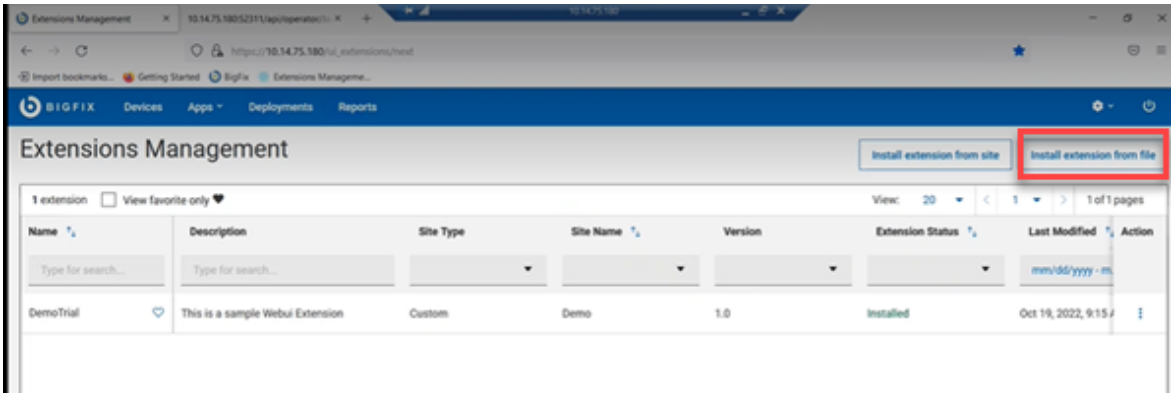
ファイルからの拡張機能のインストール

このページでは、ファイルから拡張機能をインストールする方法について説明します。

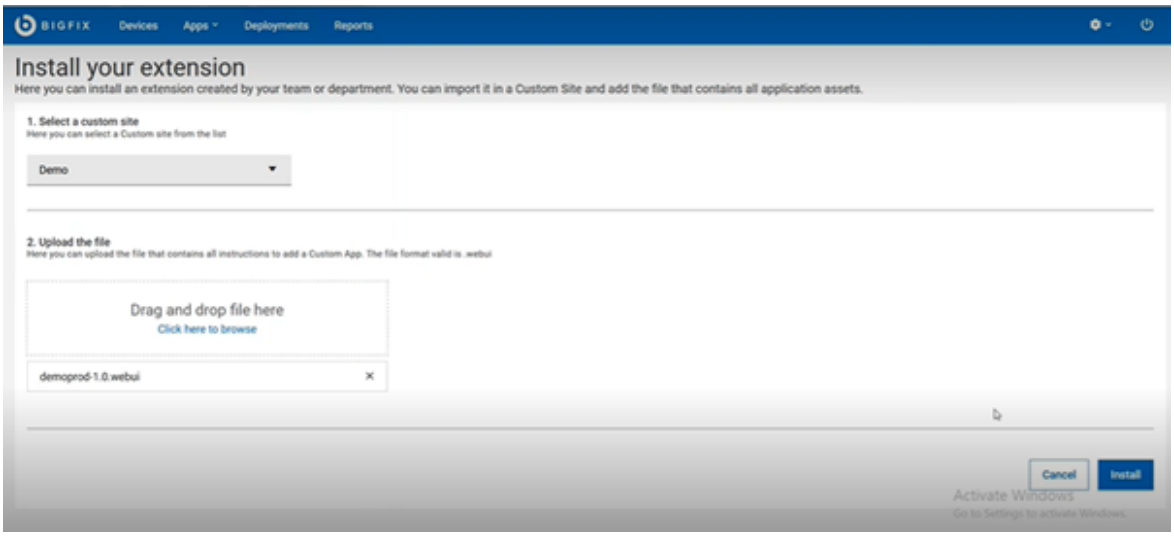
このタスクを実行するには、マスター・オペレーターまたはコンテンツ作成者で、カスタム・サイトの読み取り/書き込みアクセス権が必要です。

ファイルから拡張機能をインストールするには、次の手順を実行します。

1. 適切な資格情報を使用して WebUI にログインします。
2. メニュー・バーの**「Extension Management」**をクリックします。
3. **「ファイルから拡張機能をインストール」**をクリックします。



4. 拡張機能をインストールするカスタム・サイトを選択します。
5. カスタム・アプリを追加するためのすべての指示が含まれているファイルをアップロードします。有効なファイル形式は `.webui` です。



6. **「インストール」**をクリックします。
7. 拡張機能が正常にインストールされると、成功メッセージが表示され、拡張機能が Extension Management グリッドにリストされます。

関連情報

拡張に対する作業 (（ページ） *239)*

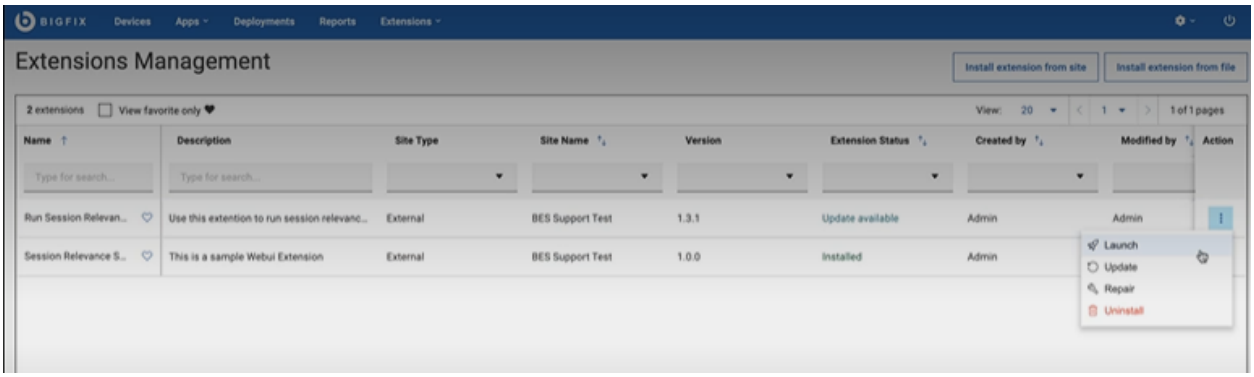
拡張機能の更新 (（ページ） *242)*

拡張機能のアンインストール (（ページ） *245)*

拡張に対する作業

このページでは拡張機能の操作方法について説明します。

拡張機能は、インストール後に Extension Management グリッドにリストされます。

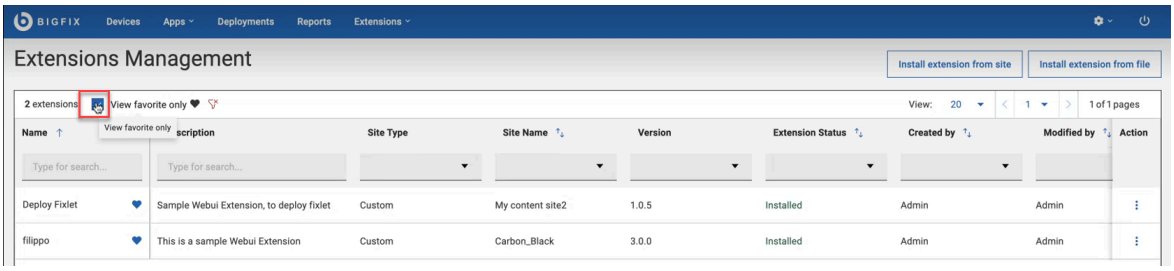


「アクション」列の下のメニューから、次のアクションを実行できます。

- **Launch (（ページ） *241)***: 拡張機能をインストールしたら、その拡張機能を起動して操作できます。
- **更新** (（ページ） *242)*: 外部サイトで新しいバージョンが利用可能になった場合は、拡張機能を更新します。詳しくは、リンク (（ページ） *242)*を参照してください。
- **修復**: 拡張機能アプリケーションの拡張機能ステータスが「修復」と表示される場合は、拡張機能アプリケーション・ファイルに修復が必要です。「修復」リンクをクリックして、アプリケーションが意図したとおりに動作するように拡張機能の修復と再インストールを行います。
- **アンインストール (（ページ） *245)***: 不要になった拡張機能はアンインストールできます。

Extensions Management グリッドからは、次のアクションも実行できます。

- **お気に入り**: お気に入りアイコン をクリックし、拡張機能をお気に入りとしてマークします。「お気に入りのみ表示」チェックボックスをオンにすると、グリッドには、お気に入りとしてマークされた拡張機能のみが表示されます。



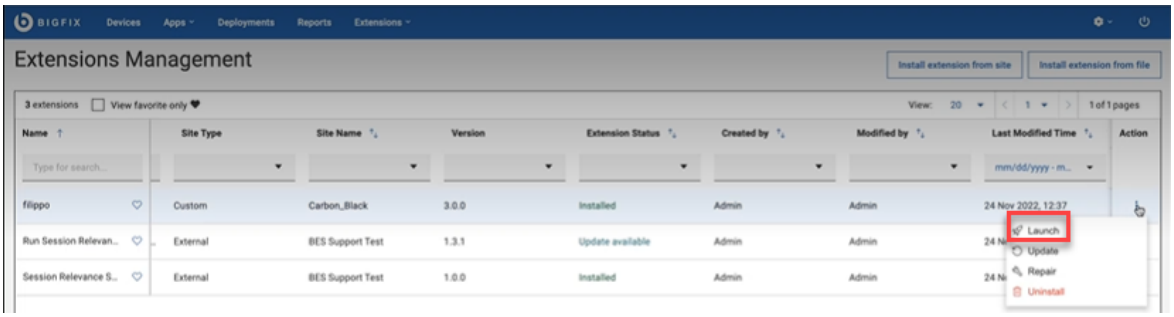
- **フィルター**: 拡張機能は、「名前」、「説明」、「サイト・タイプ」、「サイト名」、「バージョン」、「拡張機能ステータス」、「作成者」、「変更者」、「最終変更時刻」でフィルタリングできます。テキストで検索するか、列の下のオプションを選択して、必要なデータをフィルタリングできます。
- **ソート**: 拡張機能は、「名前」、「サイト名」、「拡張機能ステータス」、「作成者」、「変更者」、「最終変更時刻」の各列ごとにソートできます。
- **ページ付けと移動**：「表示」ドロップダウンから数値を選択して、1 ページに表示できる拡張機能の数を設定できます。左右の矢印を使用して、ページ間を移動できます。

Launch

マスター・オペレーターまたはコンテンツ作成者としてサインインしている場合は、次の方法で拡張機能を起動できます。

- 「拡張機能」メニューから拡張機能を直接起動します。「拡張機能」メニューには、すでにインストールされているすべての拡張機能アプリケーションのリストが表示されます。ここから拡張機能を起動すると、関連する拡張機能アプリケーションが同じページで開きます。ここから拡張機能アプリケーションを 1 つずつ操作できます。

- **「アクション」**サブメニューから拡張機能アプリケーションを起動します。これを行うには、「アクション」列で、目的の拡張機能のメニュー・アイコンをクリックし、「起動」を選択します。拡張機能アプリケーションが新しいウィンドウで開きます。1 つ以上の拡張機能を開くことができ、すべての拡張機能アプリケーションは新しいタブで開きます。



NMO としてサインインしている場合、アクセス可能なサイトにインストールされている拡張機能アプリケーションは「拡張機能」メニューの下に表示されます。拡張機能アプリケーションを選択して、そこから直接起動できます。

関連情報

拡張機能の更新 (（ページ） *242)*

拡張機能の更新

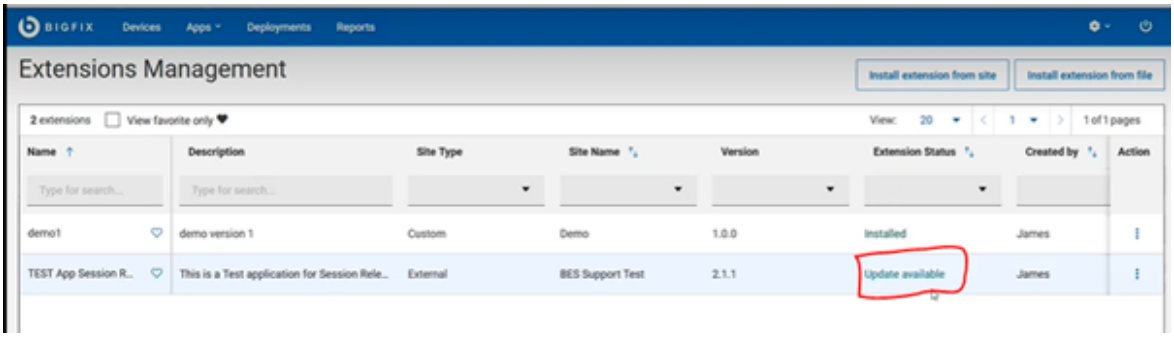
新しいバージョンの拡張機能が使用可能になったら、拡張機能を更新できます。

始める前に: このタスクを実行するには、マスター・オペレーターまたはコンテンツ作成者で、必要なカスタム・サイトの読み取り/書き込みアクセス権が必要です。

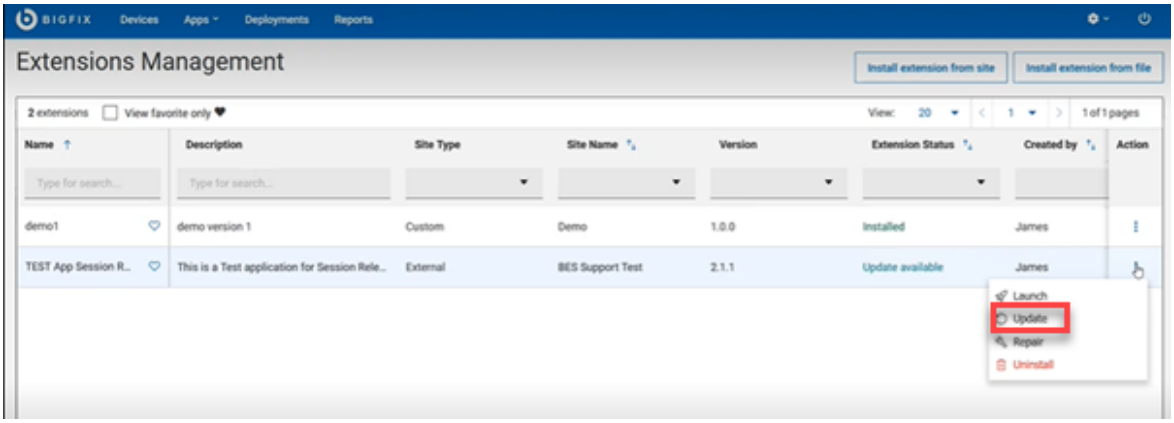
外部サイトからの更新

「サイトからインストール」オプションを使用して拡張機能をインストールした場合、その拡張機能の新しいバージョンが個々の外部サイトに公開されると、拡張機能ステータスは「更新が利用可能」ステータスが表示されます。拡張機能を更新するには、次の手順を実行します。

1. 利用可能な更新の**拡張機能ステータス**を確認します。

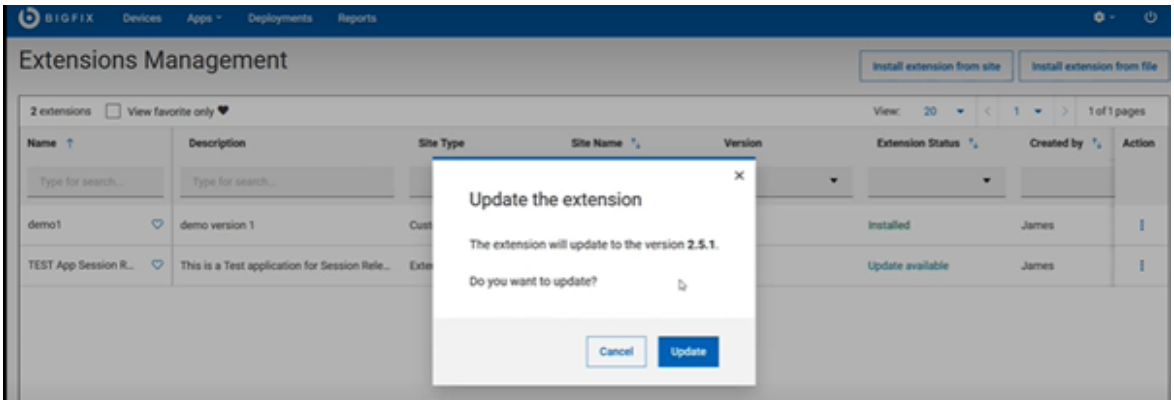


2. **「更新が利用可能」**リンクをクリックして更新します。または、拡張機能に対応する**「アクション」**列の下にあるメニュー・アイコンをクリックして、**「更新」**を選択することもできます。



注: サイトからインストールした拡張機能の場合、ドロップダウンの「更新」オプションが有効になるのは、拡張機能ステータスに「更新が利用可能」と表示される場合のみです。

3. 更新を確認します。

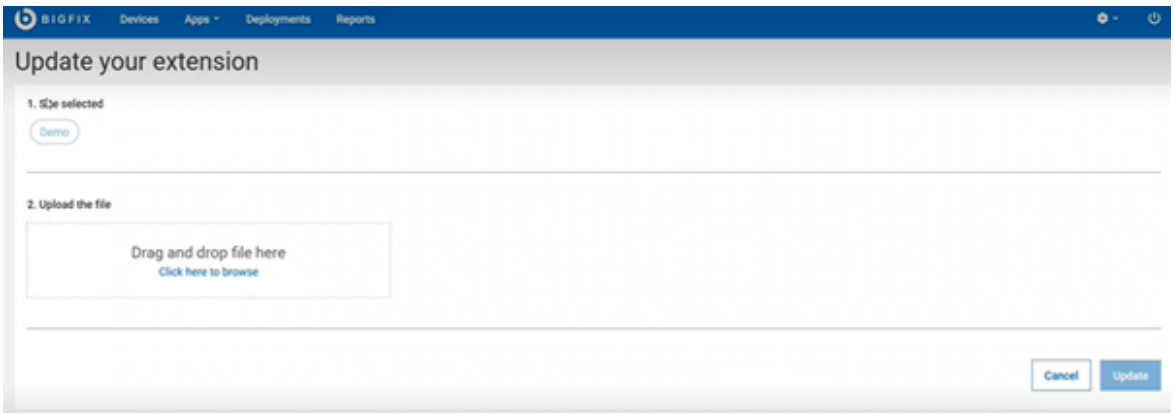


成功メッセージが表示され、拡張機能ステータスが「インストール済み」に変更されます。

カスタム・サイトからの更新

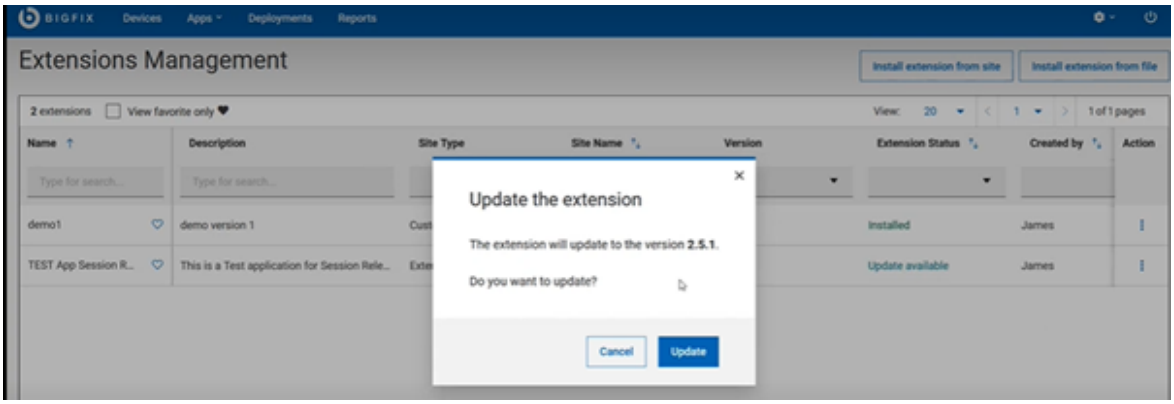
「ファイルから拡張機能をインストール」オプションを使用して拡張機能をインストールした場合は、カスタム・サイトにアップロードされた拡張機能ファイルに移動して、拡張機能を新しいバージョンに更新できます。これを行うには、次の手順を実行します。

1. 拡張機能に対応する**「アクション」**列の下にあるメニュー・アイコンをクリックして、**「更新」**を選択します。
2. 「拡張機能の更新」ページで、新しいバージョンの拡張機能ファイルをドラッグ・アンド・ドロップするか、「参照するにはここをクリック」リンクをクリックして、カスタム・サイトから新しいバージョンの拡張機能ファイルを探します。



注: 「選択したサイト」では、拡張機能の最初のインストール元だったサイトが自動的に選択されて表示されます。この表示は、拡張機能の更新中には変更できません。

3. 更新を確認します。



拡張機能ステータスがインストール済みに変更されました。

拡張機能のダウングレード

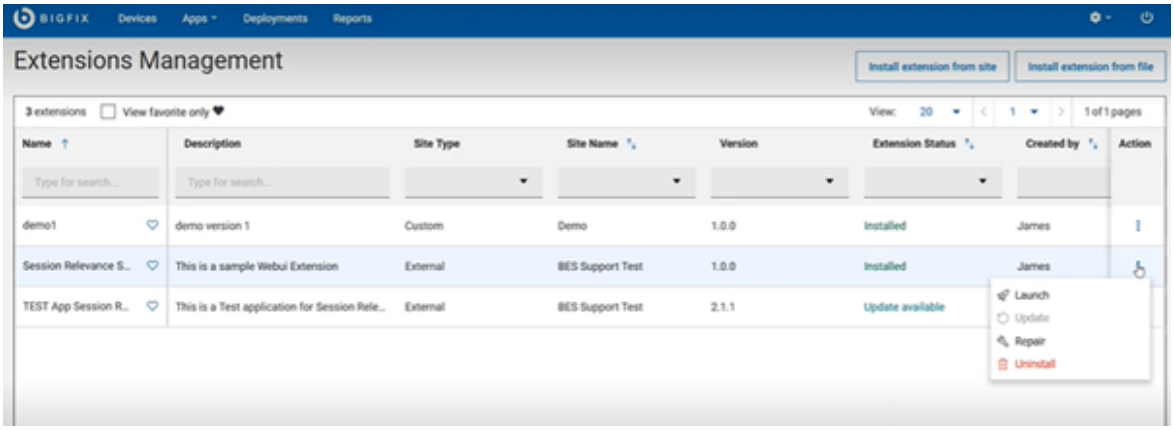
拡張機能は、現在のバージョンから古いバージョンにダウングレードすることもできます。これを行うには、拡張機能の更新中に、必要に応じて外部サイトまたはカスタム・サイトから、古いバージョンの拡張機能ファイルを選択します。

拡張機能のアンインストール

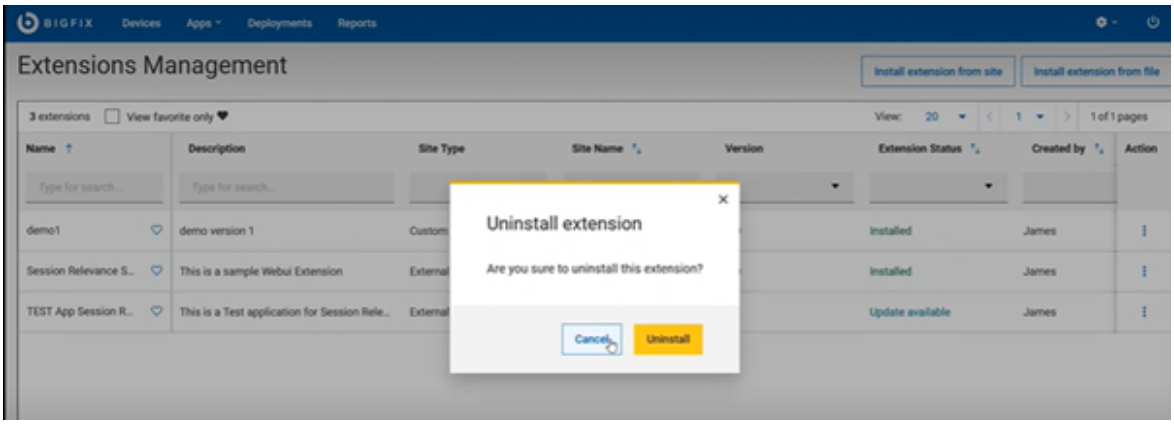
不要になった拡張機能はアンインストールできます。

拡張機能をアンインストールするには、次の手順を実行します。

1. 「Extension management」ページで、アンインストールする拡張機能に対応するドロップダウン・メニューをクリックし、メニューから**「アンインストール」**を選択します。



2. ポップアップ・ウィンドウで**「アンインストール」**をクリックし、アンインストールの実行を確定します。



注: カスタム・サイトから拡張機能をアンインストールする場合は、そのサイトにアップロードされた拡張機能ファイルを削除することもできます。

第 14 章. Modern Client Management と BigFix Mobile

このセクションでは、BigFix Modern Client Management (MCM) と BigFix Mobile について説明し、MCM の概念、用語、機能について理解します。MDM 管理対象エンドポイントの完全なライフサイクルを管理するための詳細な手順をここに記載しています。

概要

- BigFix は、すべてのエンドポイントを動的に可視化するエージェント機能をエンドポイント管理に提供します。BigFix WebUI は、BigFix エージェントがインストールされていない最新のデバイスを管理するだけでなく、BigFix エージェントがインストールされている従来のデバイスも簡単に管理できます。BigFix エージェントは、エンドポイントへのダウンロード、パッチ、構成、その他のコンテンツをリアルタイムで開始し、アクションを開始して、継続的に自己評価とポリシー適用を実行します。BigFix では、Windows、macOS、iOS、Android エンドポイントをエージェント不要で管理することもできます。
- オンプレミス MDM のアーキテクチャー概要やその他の詳細情報については、「オンプレミス・デプロイメント」を参照してください。
- BigFix は、エンドポイントを効果的に管理するための重要なアクションとすぐに使用可能なポリシーを提供することにより、Windows、macOS、iOS、iPadOS、Android を実行する企業所有のデバイスや BYOD デバイスの管理を拡張します。

BigFix MCM

BigFix MCM を使用すると、MDM 技術を活用して、Windows や macOS の OS を搭載した最新のラップトップに管理機能を拡張できます。

BigFix Mobile

BigFix Mobile は、エンドポイント管理を iOS、iPadOS、Android デバイスに拡張します。

前提条件

詳しくは、『前提条件および要件』を参照してください。

機能の概要

Modern Client Management と BigFix Mobile では、次の方法を用いてお使いの環境の最新のクライアントの管理を促進します。

デバイス登録

BigFix MCM は、組織のニーズに基づいて、異なるオペレーティング・システムを搭載するデバイスのさまざまな登録方法をサポートします。詳しくは、『デバイス登録』を参照してください。

MCM ダッシュボード

BigFix Modern Client Management ダッシュボード (（ページ） 250) では、以下が提供されます。

- 環境内の MCM 管理対象デバイスと、MCM デプロイメント全体の正常性に関する情報。
- デバイスの管理、デバイスのセキュリティー、デバイスの暗号化における、あらゆる側面の統計情報をすばやく確認。
- 報告デバイスと非報告デバイスの数、成功したアクションと失敗したアクションの数など、重要な統計に関する通知。
- 登録されたデバイスの総数、各オペレーティング・システムを搭載するデバイスの数、モバイルやデスクトップなどのデバイス・タイプに関する概要。
- 日次タスク、ヘルプ情報、サポート・チケットを作成するリンクへの迅速なアクセス。

BigFix agent をデプロイ (MCM のみ)

MCM を使用すると、WebUI を介して、登録済みの macOS または Windows デバイスに BigFix agent をデプロイできます。登録済み MCM デバイスに BigFix エージェントもインストールされている場合は、両方の管理機能を利用でき、ユーザーにはデバイスの 1 つの統合された表現が表示されます。これらの相関デバイスでは、BigFix エージェントと MDM API の両方からのアクションを使用できます。

デバイスのインベントリー (MCM および BigFix Mobile)

MCM and BigFix Mobile では、情報がネイティブ BigFix エージェント、MDM、クラウド・インスタンスのいずれかから取得されたものであっても、重要なデバイス情報をデバイスのリスト (（ページ） 22)に表示できます。

注: マスター以外のオペレーターが WebUI でモバイル関連コンテンツにアクセスするには、モバイル・サイト (BESUEM Mobile) に対するアクセス権が必要です。

デバイスの簡易表現 (MCM および BigFix Mobile)

WebUI では、ネットワーク上の各デバイスがアイコンで表示されます (ネイティブ 

、クラウド 

、または MDM 

)。エンドポイントに複数の表現がある場合は、複数のアイコンが表示されます。複数の表現があるデバイスは、相関デバイスと呼ばれます。

デバイス管理 (MCM および BigFix Mobile)

MCM and BigFix Mobile は、macOS や Windows などの最新のデスクトップや、Android、iOS、iPadOS などのモバイル・デバイスの管理に役立つ追加の機能とポリシーを備えています。ロック、ワイプ、再起動、シャットダウンなどのアクションをサポートします。ポリシーと呼ばれる BigFix 成果物に取り込まれた機能を適用できます。

デバイス・セキュリティー

MCM and BigFix Mobile は、管理対象デバイスへのセキュリティー・ポリシーの適用を容易にします。これにより、IT 管理者は、すべての管理対象デバイスでパスワードや制限などを適切に設定できます。

アプリケーション管理 (MCM および BigFix Mobile)

MCM を使用すると、MDM サーバーでアプリケーションを事前にステージングして、ポリシー・グループを介して macOS エンドポイントと Windows エンドポイントにアプリケーションを配布できます。BigFix Mobile では、Play

Store および App Store から基本的なストア・アプリケーションを配布できます。

ポリシー管理 (MCM および BigFix Mobile)

BigFix MCM and BigFix Mobile では、Apple (macOS、iOS、iPadOS)、Windows、Android デバイス全体に共通のパスコード・ポリシーと制限ポリシーを設定できます。組織やデバイスのオペレーティング・システムに適したカスタム・ポリシーをアップロードすることもできます。さまざまなオペレーティング・システムで使用可能なポリシーのリストについては、『ポリシーの管理 (（ページ） *382)*』を参照してください。

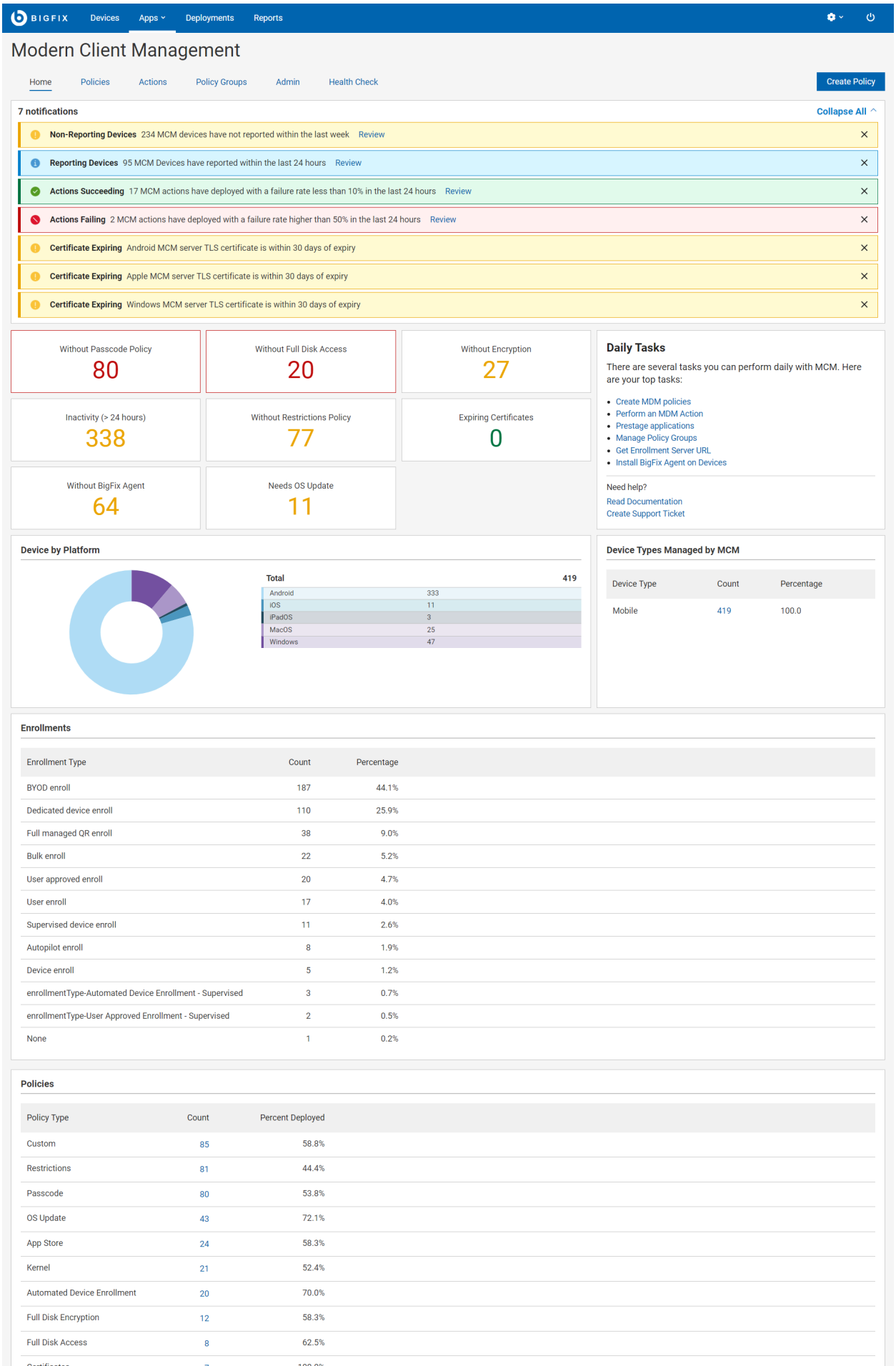
必要なライセンス

- BigFix MCM、BigFix Lifecycle、BigFix Compliance のライセンスを使用して、MDM API および WebUI でラップトップを管理できます。
- BigFix でモバイル・デバイスを管理するには、BigFix Mobile のライセンスが必要です。

Modern Client Management ダッシュボード

MCM ダッシュボードは、MCM アプリケーションのホーム・ページです。このダッシュボードでは、MDM が管理するデバイスのデバイス管理、デバイス・セキュリティー、デバイス暗号化などのあらゆる情報を確認できます。

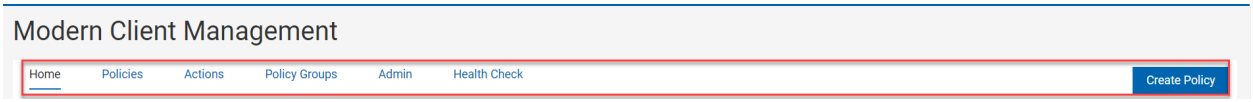
MCM ダッシュボードを表示するには、WebUI メイン・ページから**「アプリケーション」** > **「MCM」**をクリックします。


BIGFIX
Devices
Apps
Deployments
Reports
Modern Client Management
Home
Policies
Actions
Policy Groups
Admin
Health Check
Create Policy
7 notifications
Collapse All
Non-Reporting Devices 234 MCM devices have not reported within the last week Review
Reporting Devices 95 MCM Devices have reported within the last 24 hours Review
Actions Succeeding 17 MCM actions have deployed with a failure rate less than 10% in the last 24 hours Review
Actions Failing 2 MCM actions have deployed with a failure rate higher than 50% in the last 24 hours Review
Certificate Expiring Android MCM server TLS certificate is within 30 days of expiry
Certificate Expiring Apple MCM server TLS certificate is within 30 days of expiry
Certificate Expiring Windows MCM server TLS certificate is within 30 days of expiry
Without Passcode Policy
80
Without Full Disk Access
20
Without Encryption
27
Inactivity (> 24 hours)
338
Without Restrictions Policy
77
Expiring Certificates
0
Without BigFix Agent
64
Needs OS Update
11
Daily Tasks
There are several tasks you can perform daily with MCM. Here are your top tasks:
Create MDM policies
Perform an MDM Action
Prestage applications
Manage Policy Groups
Get Enrollment Server URL
Install BigFix Agent on Devices
Need help?
Read Documentation
Create Support Ticket
Device by Platform
Total 419
Android 333
iOS 11
iPadOS 3
MacOS 25
Windows 47
Device Types Managed by MCM
Device Type Count Percentage
Mobile 419 100.0
Enrollments
Enrollment Type Count Percentage
BYOD enroll 187 44.1%
Dedicated device enroll 110 25.9%
Full managed QR enroll 38 9.0%
Bulk enroll 22 5.2%
User approved enroll 20 4.7%
User enroll 17 4.0%
Supervised device enroll 11 2.6%
Autopilot enroll 8 1.9%
Device enroll 5 1.2%
enrollmentType-Automated Device Enrollment - Supervised 3 0.7%
enrollmentType-User Approved Enrollment - Supervised 2 0.5%
None 1 0.2%
Policies
Policy Type Count Percent Deployed
Custom 85 58.8%
Restrictions 81 44.4%
Passcode 80 53.8%
OS Update 43 72.1%
App Store 24 58.3%
Kernel 21 52.4%
Automated Device Enrollment 20 70.0%
Full Disk Encryption 12 58.3%
Full Disk Access 8 62.5%

重要: MCM ダッシュボードで予期されるデータを表示するには、正常性チェック (（ページ） *264)* ですべての分析がアクティブ化されていることを確認します。

ナビゲーション・バー

ナビゲーション・バーは、MCM アプリケーション全体のページの上部に表示されます。ナビゲーション・バーを使用して、どの機能ページにも簡単に移動できます。



- ホーム - アプリケーションの任意のページから「ホーム」タブをクリックすると、MCM ダッシュボード・ページに移動します。
- ポリシー (（ページ） *382)* - このタブから、ポリシーを作成および管理できます。
- アクション (（ページ） *460)* - このタブから、ロック、ワイプ、再起動、シャットダウン、ポリシーの削除など、デバイスの MCM アクションを開始できます。
- ポリシー・グループ (（ページ） *386)* - このタブから、ポリシー・グループを作成および管理できます。
- 管理者 - このタブから、 MCM コンポーネントの設定 (（ページ） *273)*、インストーラーとアプリの事前ステージング、登録設定の構成、リカバリー・キーの設定を実行できます。
- 正常性チェック (（ページ） *264)* - このタブから、ご使用の環境内の異なるオペレーティング・システムのすべての MCM コンポーネントの状況をモニターできます。
- **「ポリシーの作成」**ボタンをクリックすると「ポリシー (（ページ） *382)*」ページが開き、ポリシー・タイプのリストが表示されます。オペレーティング・システムやポリシーの作成要件に応じて、ポリシー・タイプをクリックできます。

概要

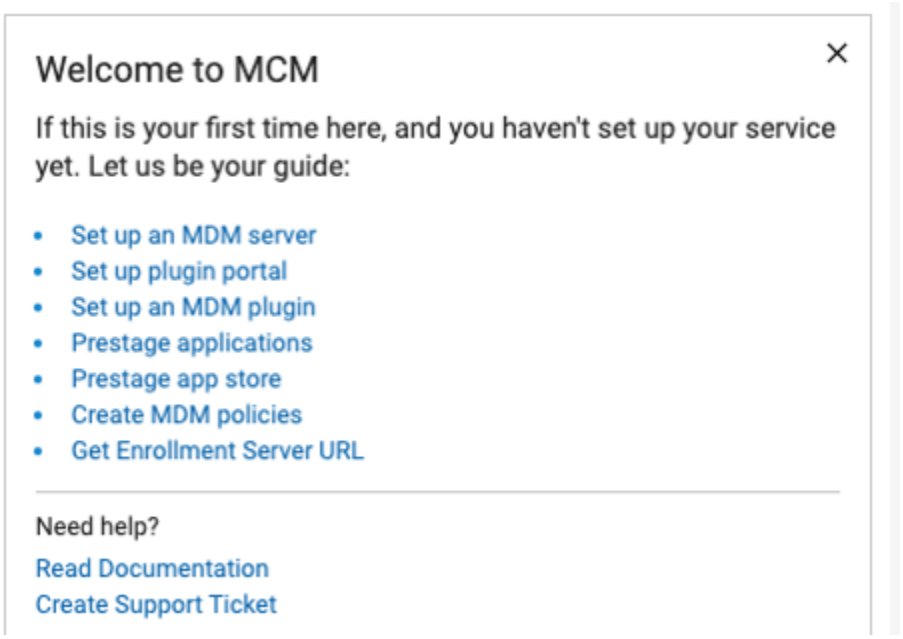
ダッシュボードには、さまざまな情報と統計が表示されます。ダッシュボードの各セクションの統計は、ログインしているユーザーのアクセス許可とデプロイメントの全体的な

ライセンス・レベルに応じて異なります。例えば、BigFix Mobile のライセンスを持たない組織には、iOS、iPadOS、または Android デバイスに関連するデータは表示されません。また、BigFix コンソールで構成されたデバイスの所有権に応じて、マスター・オペレーターとマスター以外のオペレーターに表示される数は異なります。

ダッシュボードでクリック可能な統計項目をクリックすると、その特定の項目のフィルターされたリストが表示され、その項目のリストに対して必要なアクションを実行できます。

MCM へようこそ

このセクションでは、初心者のマスター・オペレーター向けに、MDM サーバーおよびその他の管理タスクを設定するためのクイック・リンクを紹介します。MCM の資料ページにアクセスしてヘルプ情報を確認することや、ここからサポート・チケットを作成することもできます。

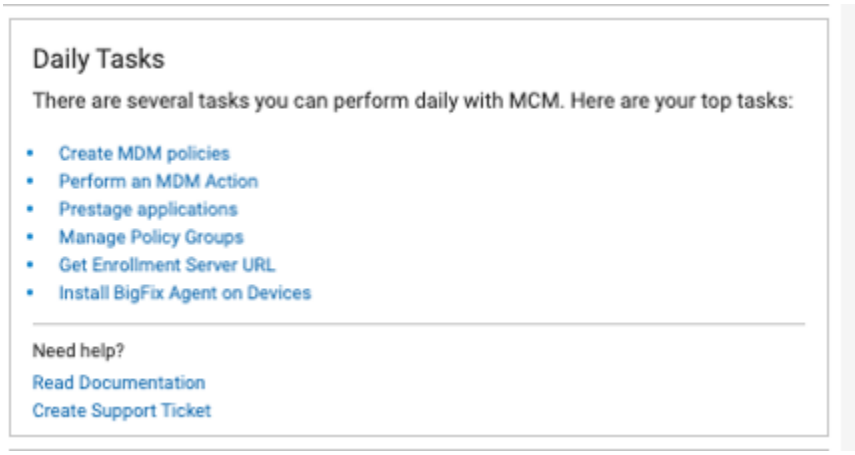


日次タスク

マスター・オペレーターが「MCM へようこそ」を閉じると、今後 MCM ダッシュボードにアクセスする時には「日次タスク」が表示されるようになります。このセクションでは、デバイス管理のタスクへのクイック・リンクを紹介します。MCM 管理ガイドにアクセス

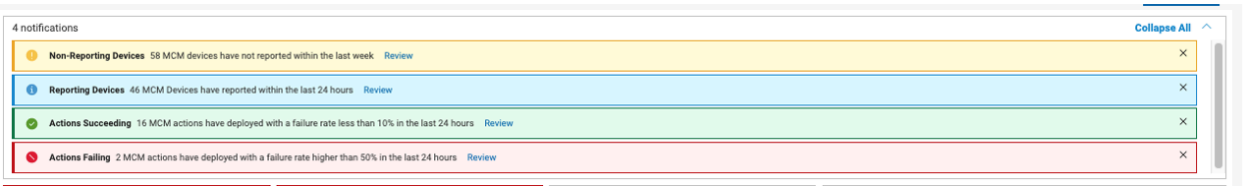
してヘルプ情報を確認することや、ここからサポート・チケットを作成することもできます。

注: MCM ダッシュボードにアクセスするマスター以外のオペレーターには、「日次タスク」タイルのみが表示されます。



通知

「通知」セクションには、MDM デプロイメント全体についての簡単な情報、警告、アラートが表示されます。



以下が表示されます。

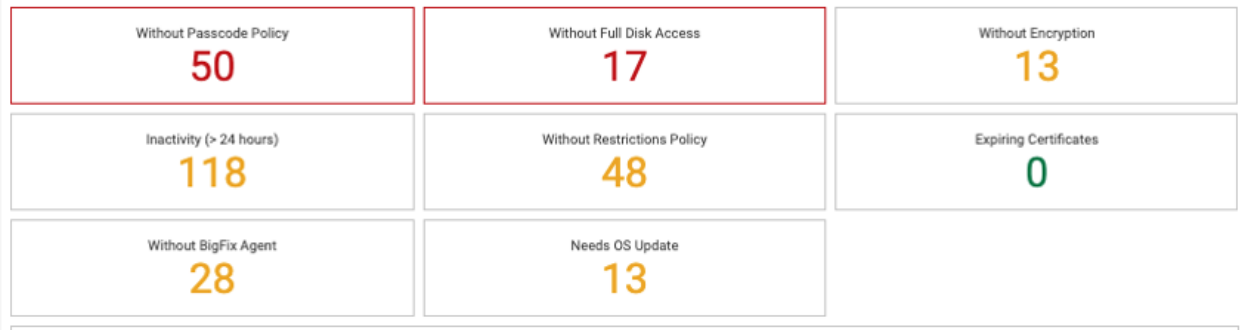
- 24 時間以内に報告された MDM デバイス
- 24 時間以内に報告されなかった MDM デバイス
- 最近成功したデプロイメント (24 時間で失敗が 10% 未満)

- 最近失敗最近失敗したデプロイメント (24 時間で失敗が 50% 超)
- さまざまな MDM 証明書に関する警告とエラー (証明書の有効期限が 30 日以内の場合の警告、証明書の有効期限が切れた場合のエラー)。以下の証明書が評価されます。
    - Apple プッシュ証明書
    - 認証 CA 証明書
    - 認証証明書
    - TLS 証明書

通知の横にある**「確認」**リンクをクリックして、その通知に固有のデバイスのフィルターされたリストを表示します。**「すべて縮小」**トグルをクリックすると、通知セクションを展開または縮小できます。

数値タイル

ダッシュボードのウィジェットは、管理対象デバイスに適用されるポリシーに関する概要を提供します。



以下の方法でデプロイされたポリシーをカウントしています。

- ポリシー (（ページ） *382)*を介して個別にデプロイされたポリシー
- ポリシー・グループ・アクションを介し、デバイスを対象にしてデプロイされたポリシー
- ポリシー・グループを介して登録時にデプロイされたデフォルト・ポリシー

以下の数値タイルがダッシュボードに表示されます。

- **パスコード・ポリシーなし** - パスコード・ポリシー (（ページ） *446)* が適用されていないデバイスの数。MDM 環境にある、異なる OS のデバイスがすべてカウントされます。
- **フル・ディスク・アクセスなし** - フル・ディスク・アクセス (（ページ） *435)* ポリシーが適用されていない macOS デバイスの数。
- **暗号化なし** - ディスク暗号化ポリシー (（ページ） *431)* ポリシーが適用されていない macOS デバイスと Windows デバイスの数。
- **非アクティブ (> 24 時間)** - 相関デバイスを含め、24 時間以上MDMに報告されなかったデバイスの数。
- **制限ポリシーなし** - 制限ポリシー (（ページ） *451)* が適用されていないデバイスの数。MDM 環境にある、異なる OS のデバイスがすべてカウントされます。
- **期限が切れる証明書** - 30 日以内に証明書の有効期限が切れるように設定されている macOS/iOS/iPadOS デバイスの数。このウィジェットでは、デバイス証明書の有効期限が既に切れているデバイスの数もカウントされます。

  注:
  - デバイス証明書の有効期限が切れているデバイスは、MDM に再登録して、MDM に再び適切に報告する必要があります。
  - Apple 登録証明書を更新するには、該当するデバイスで BESUEM の Fixlet 3000 を実行します。Fixlet 3000 は、有効期限が近づくと関連するすべてのデバイスに適用される、無期限のポリシー・アクションとして実行できます。

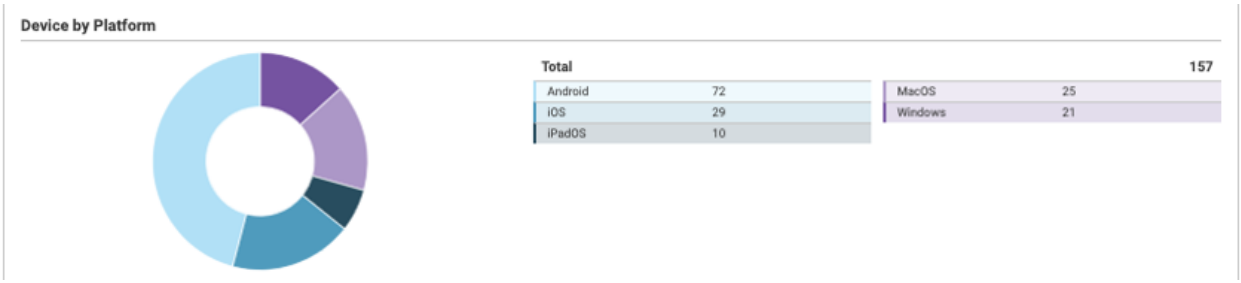
- **BigFix エージェントなし** - BigFix agent がインストールされていない macOS デバイスと Windows デバイスの数。
- **OS の更新が必要な Apple デバイス** - OS の更新が必要な Apple デバイスの数。

注: 現時点では、これは iOS/iPad の数にのみ制限されています。

プラットフォームによるデバイス

このセクションには、MCM および BigFix Mobile に登録されているデバイスの総数が表示されます。円グラフと、登録済みデバイスのオペレーティング・システムの分類を示すテーブルが表示されます。

円グラフまたはテーブルの各行をクリックすると、選択した MDM オペレーティング・システムでフィルターされたデバイスのリストが表示されます。



MCM によって管理されるデバイス・タイプ

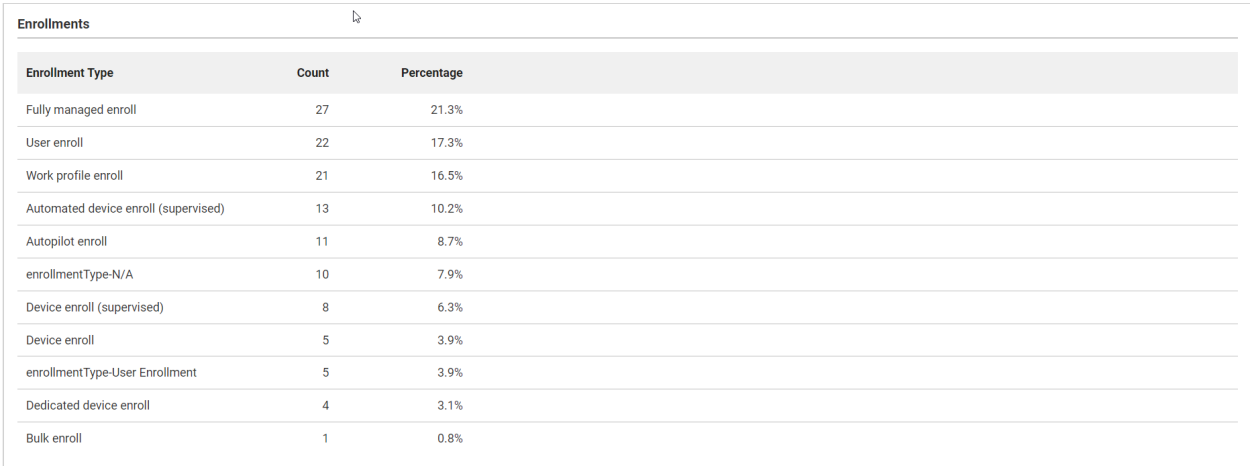
このセクションには、ご使用の環境内の MCM および BigFix Mobile によって管理されている各デバイス・タイプのデバイスの総数が表示されます。また、パーセンテージのデータも表示されます。

デバイス・タイプに対応するカウントをクリックすると、そのデバイス・タイプでフィルターされたデバイスのリストが表示されます。

登録

このセクションには、すべての登録タイプごとの登録総数と、登録全体におけるそれぞれのパーセンテージが表示されます。

登録タイプに対応するカウントをクリックすると、その登録タイプに登録済みのデバイスでフィルターされたリストが表示されます。



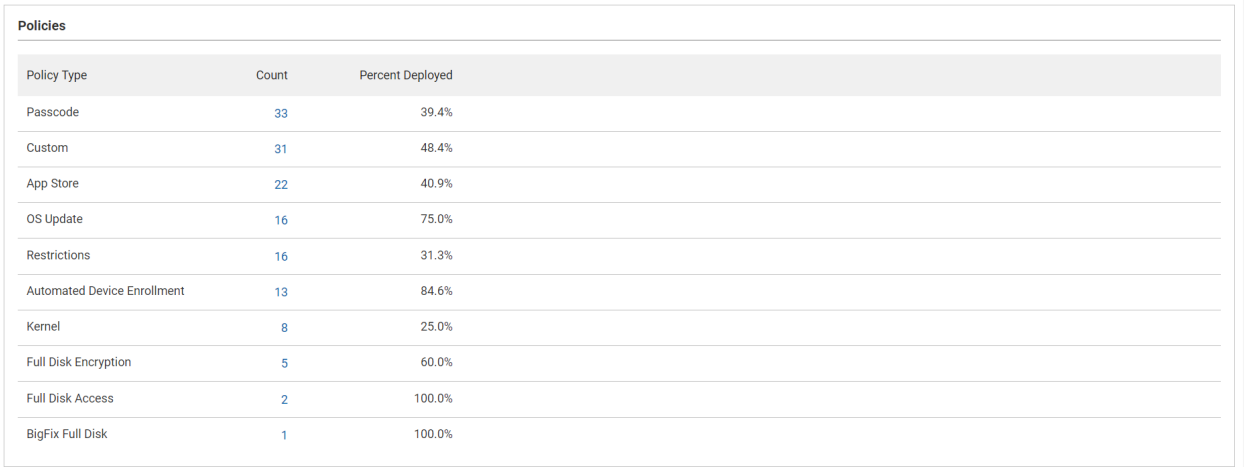
Enrollments

Enrollment Type	Count	Percentage
Fully managed enroll	27	21.3%
User enroll	22	17.3%
Work profile enroll	21	16.5%
Automated device enroll (supervised)	13	10.2%
Autopilot enroll	11	8.7%
enrollmentType-N/A	10	7.9%
Device enroll (supervised)	8	6.3%
Device enroll	5	3.9%
enrollmentType-User Enrollment	5	3.9%
Dedicated device enroll	4	3.1%
Bulk enroll	1	0.8%

ポリシー

このセクションには、作成されたポリシーの総数と、すべてのポリシー・タイプでデプロイされたポリシーのパーセンテージが表示されます。

ポリシー・タイプに対応するカウントをクリックすると、そのポリシー・タイプでフィルターされたポリシーのリストが表示されます。



Policies

Policy Type	Count	Percent Deployed
Passcode	33	39.4%
Custom	31	48.4%
App Store	22	40.9%
OS Update	16	75.0%
Restrictions	16	31.3%
Automated Device Enrollment	13	84.6%
Kernel	8	25.0%
Full Disk Encryption	5	60.0%
Full Disk Access	2	100.0%
BigFix Full Disk	1	100.0%

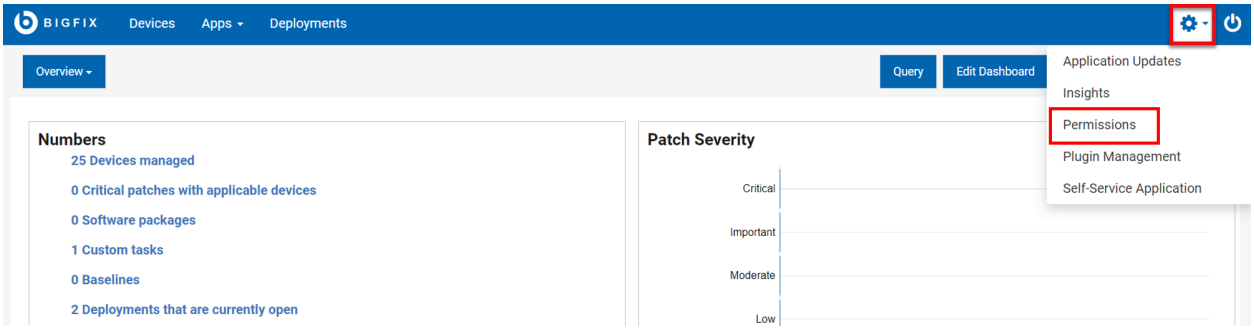
関連情報

MCM および BigFix Mobile コンポーネントのインストールと管理 - オンプレミスのみ (（ページ） 273)

MCM の役割と権限

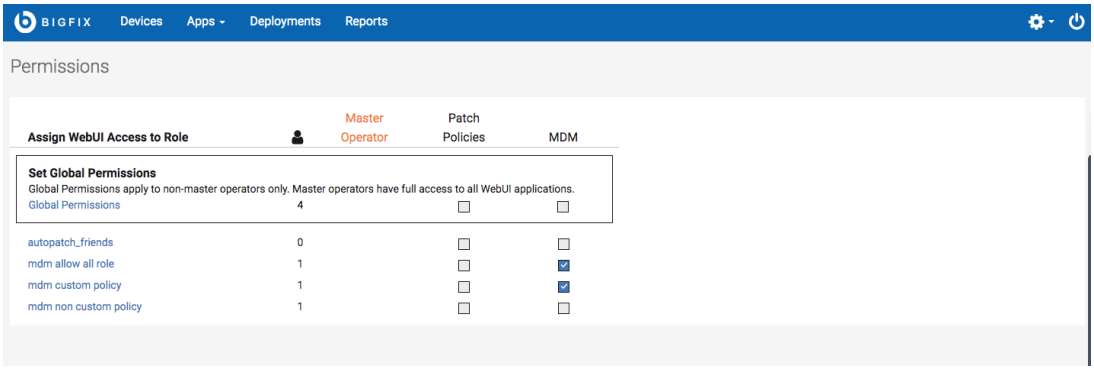
WebUI 権限サービスを使えば、WebUI MDM でのユーザーとユーザーグループの権限と設定をさらに細かく制御できるようになります。

「権限」ページに移動するには、マスター・オペレーターが歯車アイコンをクリックし、ドロップダウン・メニューから「権限」を選択します。

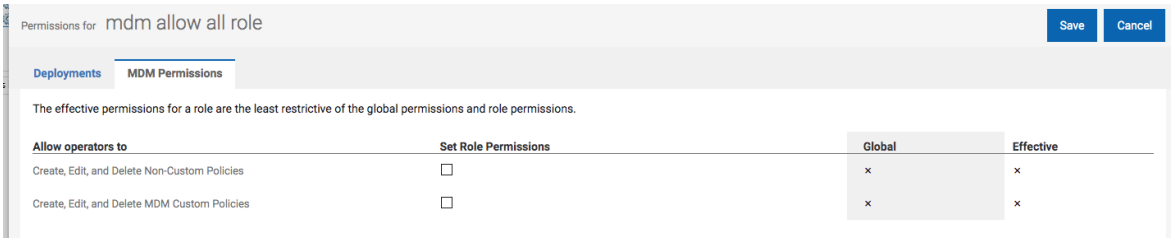


マスター・オペレーターは、MDM を使用して、権限と設定サービス (PPS) で次の 2 つの設定を行うことができます。

1. ユーザーの役割に基づく MCM アプリケーションの表示を設定する
    - 例えば、「mdm すべての役割の許可」と「mdm カスタム・ポリシー」の役割を持つユーザーは、MCM アプリケーションを表示できますが、これらの役割ではないユーザーは、MCM アプリケーションにアクセスできません。



2. 特定の MCM 権限の設定



    - 「非カスタム・ポリシーの作成、編集、削除」権限により、ユーザーは WebUI がネイティブにサポートするポリシー (パスコード・ポリシー、カーネル・ポリシー、証明書ポリシー、制限ポリシー、およびフル・ディスク・アクセス・ポリシー) を変更できます。
    - 「MCM カスタム・ポリシーの作成、編集、削除」権限により、ユーザーは独自に定義してアップロードするカスタム・ポリシーを変更できます。

WebUI の権限は、ユーザーの権限が役割の権限とグローバル権限の組み合わせであるという、コンソールの権限と同じように機能します。例: ユーザーが 4 つの異なる役割の一部であり、そのうちの 1 つだけが MCM 固有の権限にアクセスできる場合、そのユーザーは MCM にアクセスできます。ユーザーが MCM 固有の権限を持つ役割の一部ではないが、MCM のグローバル権限が設定されている場合、そのユーザーは役割を介したアクセス権を持っていないにもかかわらず、MCM にもアクセスできます。

関連情報

ポリシーの管理 (（ページ） 382)

デバイスのインベントリー

MDM にデバイスが登録されると、デバイスは WebUI に報告され、**「デバイス」**ページに表示されます。BigFix WebUI の「デバイス」ページを使って、すべてのデバイスのリストを確認できます (権限レベルによります)。デバイス・リストには、MCM によって管理されるデバイスを含む、BigFix 環境にあるすべてのデバイスが表示されます。

注:

- デバイス名の横にある、ラップトップおよび携帯電話のアイコン 

は、デバイスが MDM で管理されていることを示しています。MDM アクション、MDM ポリシー、クライアントの更新を送信、BigFix エージェントのデプロイは、これらのデバイスにのみデプロイできます。
- マスター以外のオペレーターが WebUI でモバイル関連コンテンツにアクセスするには、モバイル・サイト (BESUEM Mobile) に対するアクセス権が必要です。
- デバイス名の横にある BigFix アイコン 

は、デバイスが BigFix ネイティブ・エージェントで管理されていることを示しています。クライアントの更新を BigFix ネイティブ・エージェント・デバイスに送信することもできます。
- デバイス名の横にあるクラウド・アイコン 

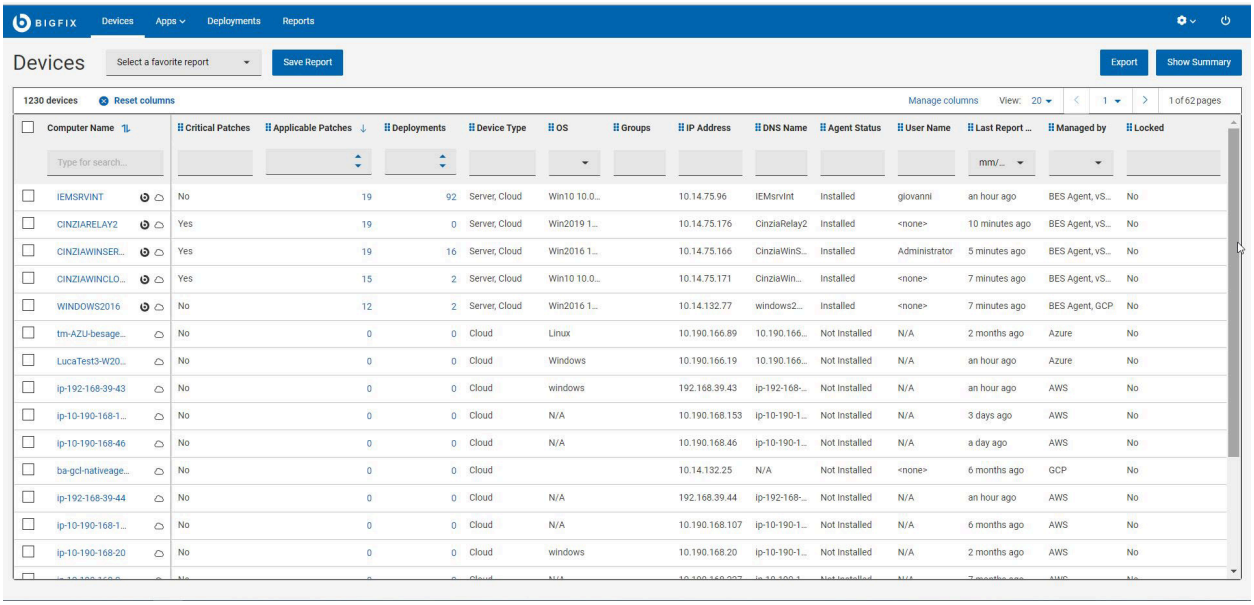
は、デバイスがクラウドで管理されていることを示しています。
- デバイス名の横に 2 つ以上のアイコン 

が表示されている場合は、デバイスは相関関係にあり、複数の方法で管理できることを示しています。

MDM では、追加のデプロイメント・オプションが「デプロイ」ドロップダウン・メニューに表示されます。マスター以外のオペレーターがこのドロップダウン・メニューを表示するには、「アクションの作成が可能」権限を持っている必要があります。ユーザー権限について詳細は、「BigFix プラットフォーム」ガイドを参照してください。

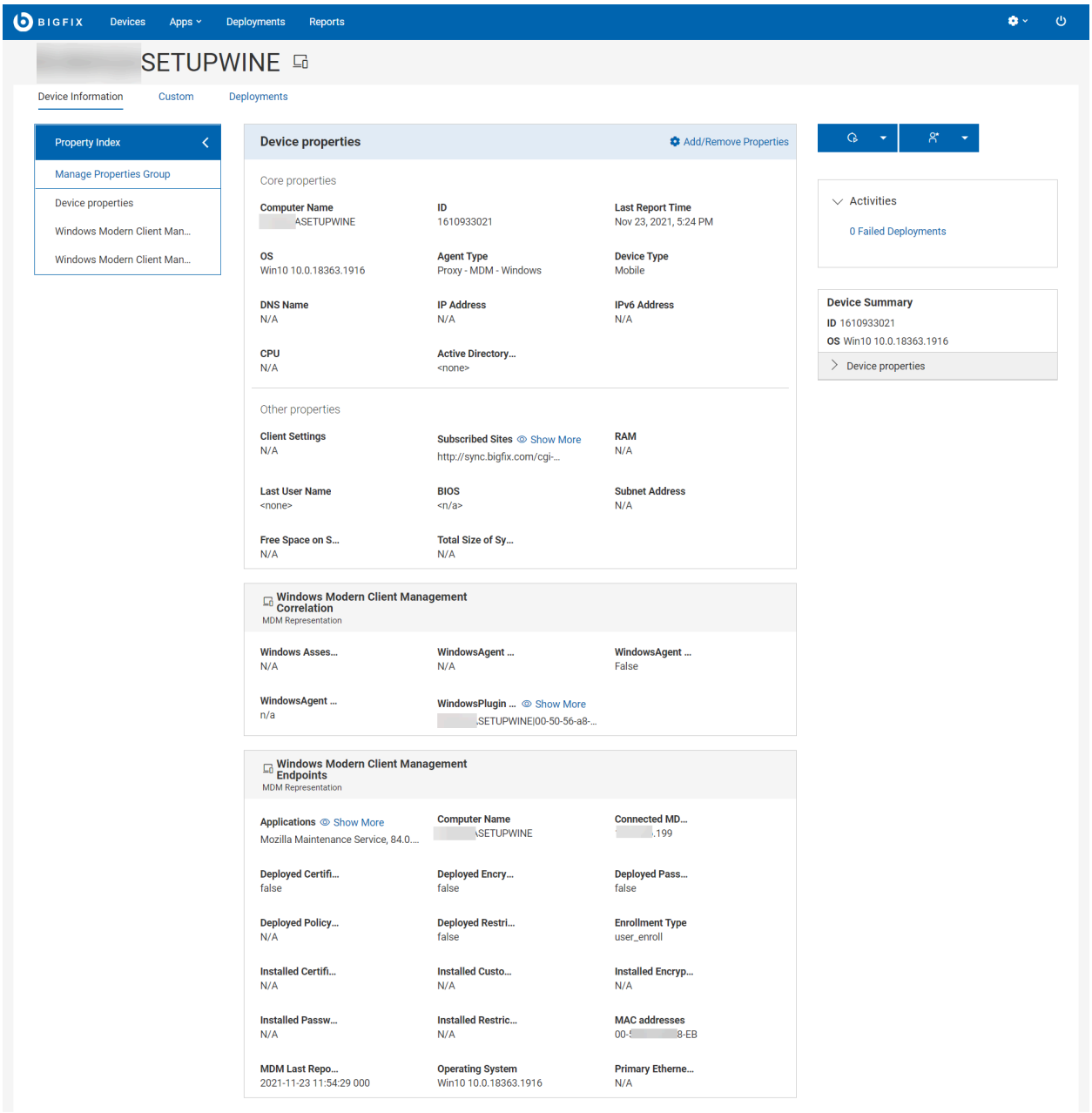
WebUI MDM アプリケーションの表示設定が可能なユーザー (（ページ） 259)には、WebUI MDM で使用できる次のオプションがあります。

- MDM アクションのデプロイ: ユーザーは、ロック、ワイプ、再始動などの MDM 固有のアクションをデプロイできます。
- MDM ポリシーのデプロイ: ユーザーは MDM ポリシーをデプロイして、パスワード設定をロックダウンしたり、該当する場合は、MCM 登録済みデバイスに対するカーネルまたはフル・ディスク・アクセスの例外、制限ポリシー、証明書ポリシーを追加したりできます。
- MDM ポリシー・グループのデプロイ: ユーザーは、MDMポリシーとアプリケーションのセットを選択した MDM エンドポイントにデプロイできる MDM ポリシー・グループをデプロイできます。
- BigFix エージェントのデプロイ: ユーザーは BigFix エージェントを BigFix エージェントがデプロイされていない MDM デバイスにデプロイできます。
- MDM 登録と MDM 登録解除: ユーザーがデバイスを MDM に登録および MDM から登録を解除できるようにします。



デバイス・リストのデバイスをクリックすると、デバイスのプロパティー、状況、関連コンテンツ項目、デプロイメント履歴を含むデバイス文書が表示されます。さらに、デバイスが MDM デバイスまたは MDM 表記のある相関デバイスであれば、MDM デバイスに関する追加の分析情報も確認できます。

注: デバイスが相関関係にある場合、デバイス文書は異なるデバイス・レポートを生成します。それには IP アドレス、名前、オペレーティング・システム名、分析など共通のプロパティーが含まれます。BigFix は MDM からのプロパティー情報を上書きして、ネイティブ・エージェントからのプロパティーを表示します。デバイス・タイプといった一部のフィールドについて、BigFix WebUI はさまざまなデバイス・レポートの集約を表示します。



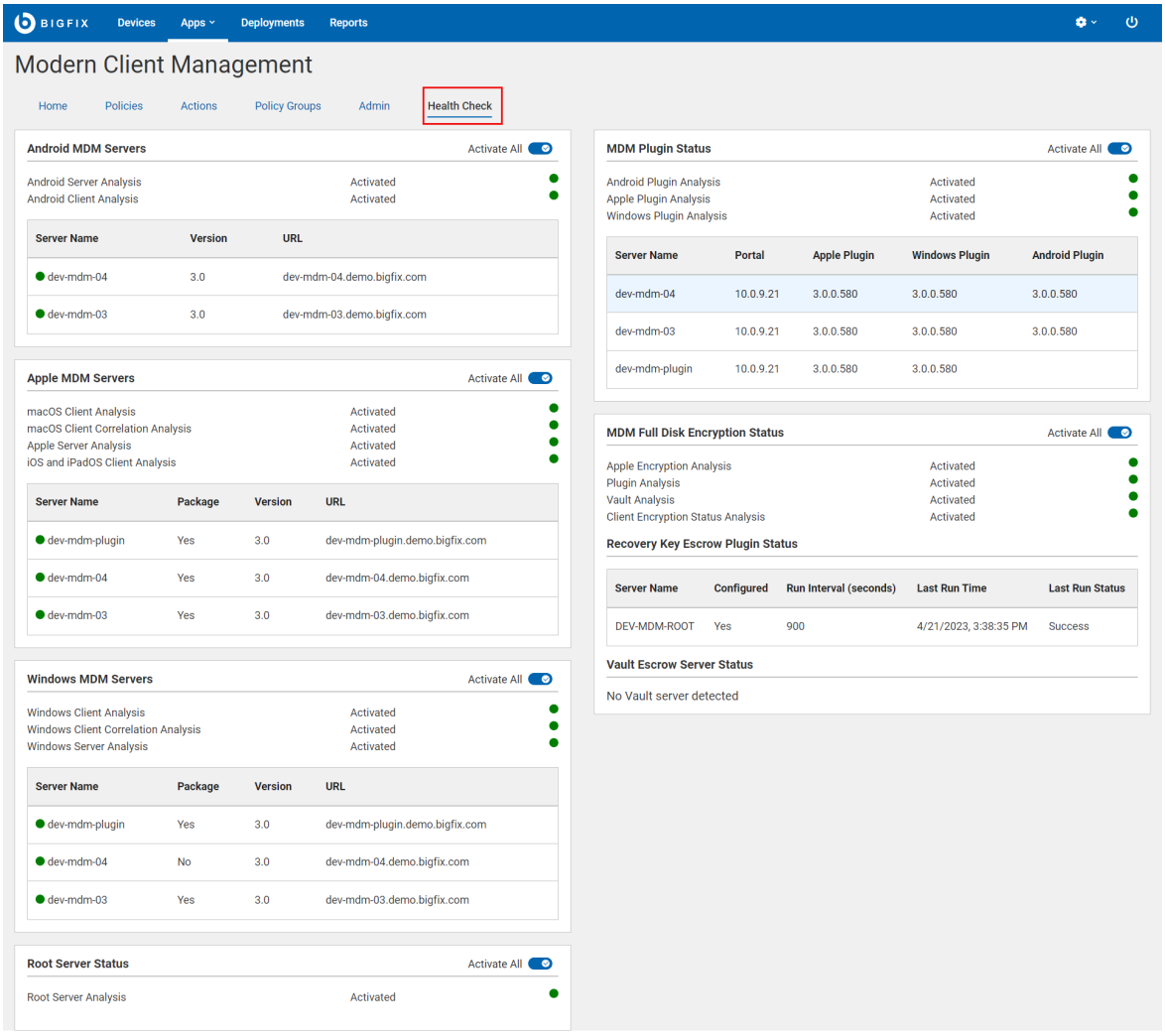
正常性チェック

マスター・オペレーターとして、MCM アプリケーションの「正常性チェック 」ページを使用して、MCM デプロイメントの正常性を監視します。

注: この機能は、マスター以外のオペレーターには適用されません。

「正常性チェック」ページにアクセスするには:

1. マスター・オペレーターとして WebUI にログインします。
2. WebUI のメイン・ページから、**「アプリケーション」 > 「MCM」**を選択します。
3. Modern Client Management ホーム・ページで、**「正常性チェック」**をクリックします。「正常性チェック」ページは以下のように表示されます。



このページは、重要な正常性インジケーターを追跡するために、以下のようにさまざまなセクションに編成されています。

- **Android MDM サーバー**
- **Apple MDM サーバー**

- **Windows MDM サーバー**
- **ルート・サーバーの状況**
- **MDM プラグイン・ステータス**
- **MDM フル・ディスク暗号化の状況**

活動化状況に応じて、**「すべてアクティブにする」**または**「すべて非アクティブにする」**トグル ボタンをクリックして、関連するすべての BESUEM/BESUEM Mobile 分析をアクティブ化または非アクティブ化します。アクティブにすると、関連する分析の横に緑色のチェック・マークが表示されます。

重要: MCM アプリが期待どおりに機能するように、すべての分析がアクティブ化されていることを確認します。

Android MDM の状況

- サーバー名: 検出された Android MDM サーバーのリストが表示されます。Android MDM サーバーがない場合は、「サーバーが検出されませんでした」と表示されます。Android MDM サーバーのセットアップについては、「BigFix Android MDM サーバーのインストール (（ページ）283)」を参照してください。
- バージョン: インストールされている Android MDM サーバーの現在のバージョンが表示されます。

Apple MDM サーバー

- サーバー名: 検出された Apple MDM サーバーのリストが表示されます。Apple MDM サーバーがない場合は、「サーバーが検出されませんでした」と表示されます。Apple MDM サーバーの設定については、『Apple 用の BigFix MDM サービスのインストール (（ページ）279)』を参照してください。
- パッケージ: BigFix Agent macOS インストーラー・パッケージが MDM サーバーで事前にステージングされているかどうかを示します。これは、MDM 経由で OSX デバイスに BigFix agent を正常にデプロイする

ために必要です。パッケージが正しく事前にステージングされている場合、ユーザーには緑色のチェック・マークが表示されます。パッケージが見つからず、パッケージを追加する場合は、『macOS BigFix インストーラーの事前ステージ (（ページ） *355)*』を参照してください。

- バージョン: インストールされている Apple MDM サーバーの現在のバージョンが表示されます。
- URL: 構成されたサーバーの MDM URL を表示します。 サーバーの URL が検出されない場合は、サーバーが正しくセットアップされていることを確認します。サーバーを設定するには、『Apple 用の BigFix MDM サービスのインストール (（ページ） *279)*』を参照してください。

Windows MDM サーバー

- サーバー名: 検出された Windows サーバーのリストが表示されます。Windows サーバーがない場合は、「サーバーが検出されませんでした」と表示されます。Windows MDM サーバーの設定については、『Windows 用の BigFix MDM サービスのインストール (（ページ） *276)*』を参照してください。
- パッケージ: BigFix エージェント Windows .msi インストーラー・パッケージが MDM サーバーで事前にステージングされているかどうかを示します。これは、MDM 経由で Windows デバイスに BigFix agent を正常にデプロイするために必要です。パッケージが正しく事前にステージングされている場合、関連するサーバーには緑色のチェック・マークが表示されます。パッケージが見つからず、パッケージを追加する場合は、『Windows BigFix インストーラーの事前ステージ (（ページ） *357)*』を参照してください。
- バージョン: インストールされている Windows MDM サーバーの現在のバージョンが表示されます。
- URL: 構成されたサーバーの MDM URL を表示します。 サーバーの URL が検出されない場合は、サーバーが正しくセットアップされていることを確認します。サーバーをセットアップするには、「BigFix Windows MDM サーバーのインストール (（ページ） *276)*」を参照してください。

ルート・サーバーの状況

この解析では、BES サーバーをチェックして、作成された PPKG ファイルがあるかどうかを確認します。

注: BES サーバーで作成された PPKG は自動的に MDM サーバーに移動され、PPKG アクションが実行されるときに MDM サーバーによって使用されます。

MDM プラグイン・ステータス

インストールされているすべてのプラグイン・ポータル名、バージョン、およびインストールされている Apple MDM プラグイン、Windows MDM プラグイン、Android プラグインのバージョンのリストを表示します。コンポーネントがインストールされていない場合は、「なし」と表示されます。

MDM フル・ディスク暗号化の状況

MDM フル・ディスク暗号化の状況が表示されます。

- FDE 分析がアクティブ化されているかどうかが表示されます。
- リカバリー・キー・エスクロー・プラグインの状況: リカバリー・キー・エスクロー・プラグインが構成されているかどうかが表示されます。構成されている場合は、サーバーとプロンプトが表示される時間間隔が表示されます。構成されていない場合は、構成できるリンクが表示されます。
- Vault エスクロー・サーバーの状況: Vault エスクロー・サーバーが構成されているかどうかが表示されます。構成されている場合は、Vault エスクロー・サーバーの名前が表示されます。

関連資料

正常性チェックで MDM プラグイン・ステータスが正しく表示されない (（ページ）)

対象デバイスを選択します。

WebUI を使用して、MCM コマンドを実行するための条件を満たす特定の対象デバイスのグループを簡単にフィルタリングおよび選択できます。これらのコマンドには、コンポーネントのインストールや更新、アクション、ポリシー、ポリシー・グループのデプロイなどのタスクが含まれます。

デバイス・リスト (（ページ） 22) および「ターゲットの選択」リストにアクセスすると、ネットワーク内のすべての関連デバイスの完全なリストが表示されます。

デバイス・タイプ、オペレーティング・システム、IP アドレスなどのさまざまなフィルターを利用して、選択範囲を絞り込むことができます。目的のフィルターを適用すると、リストは動的に更新され、指定した条件を満たすデバイスのみが表示されます。これにより、MCM コマンドの実行に適した対象デバイスを簡単に識別できます。

さらに、WebUI には、デバイスの選択を微調整するための追加オプションが用意されています。プロパティー列を追加または削除したり、フィルター済みリストを保存したり、保存されたリストを使用してアクションを迅速化したりすることで、データ・グリッドをカスタマイズできます。詳しくは、「デバイス・リスト (（ページ） 22)」を参照してください。これらの機能を利用することで、MCM コマンドを実行するための要件に合った対象デバイスを効率的かつ効果的に選択できます。

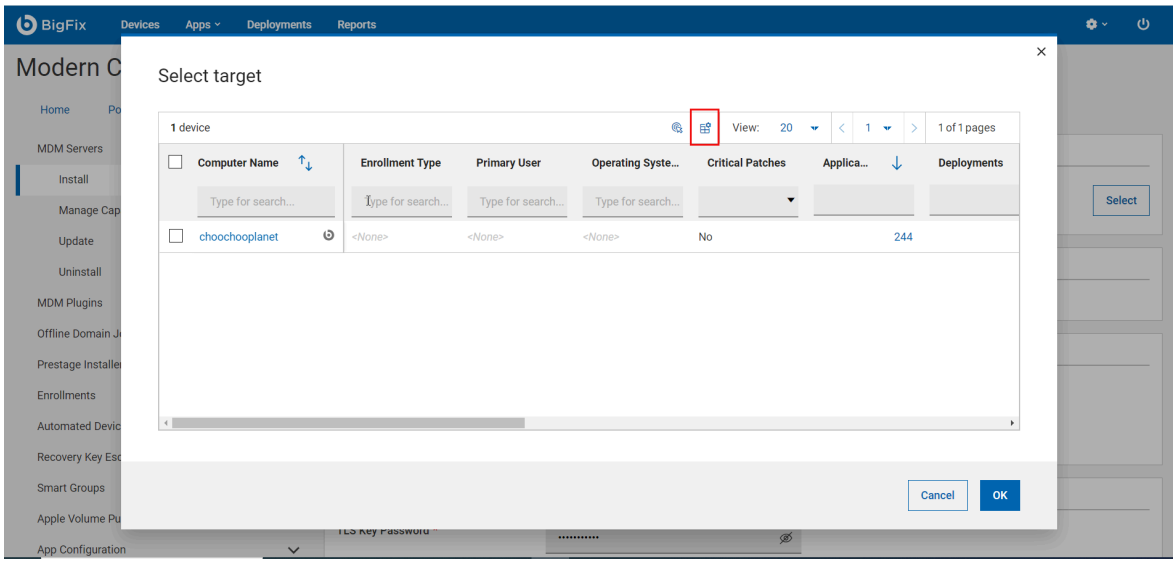
プライマリー・ユーザー・フィルターと登録タイプ・フィルターの追加

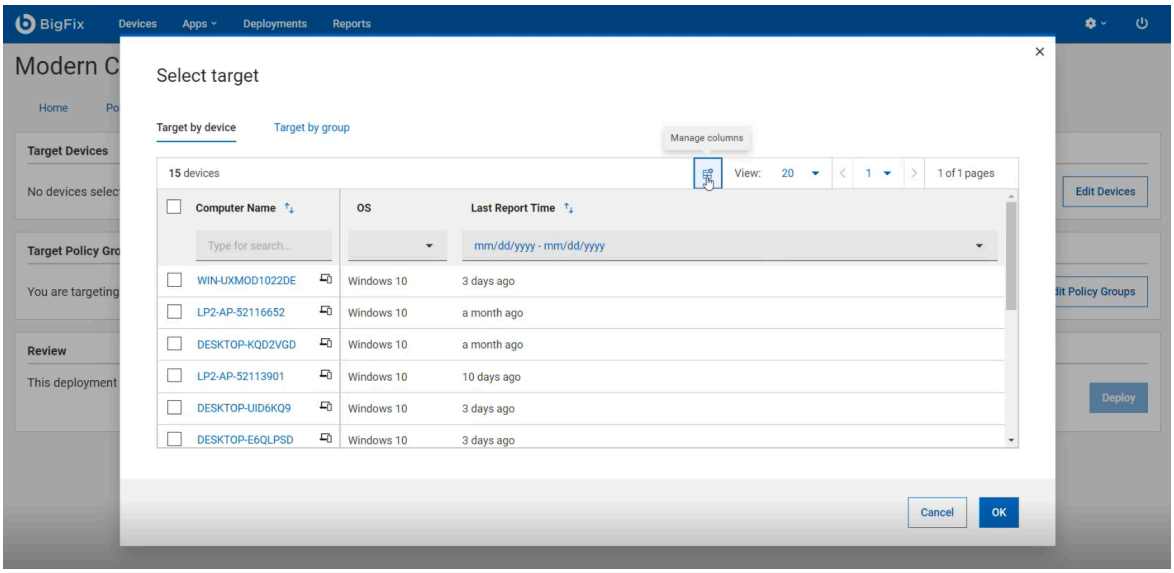
WebUI では、フィルターを追加してプライマリー・ユーザーと登録タイプに基づいてデバイスを対象にすることができます。これらのフィルターを追加すると、WebUI では、iOS、iPadOS、macOS、Android、Windows を含むすべての MCM 登録デバイスが分析され、ネットワーク内のすべてのデバイスのプライマリー・ユーザーと登録タイプが表示されます。グリッド上のデータに基づいて特定のデバイスをさらに検索、フィルタリングして対象とし、MDM タスクを実行できます。

- 外部プロパティー分析 (`BESUEM` および `BESUEM Mobile`) がアクティブになっていることを確認してください。手順については、「コンテンツ・サイトのサブスクライブ」を参照してください。

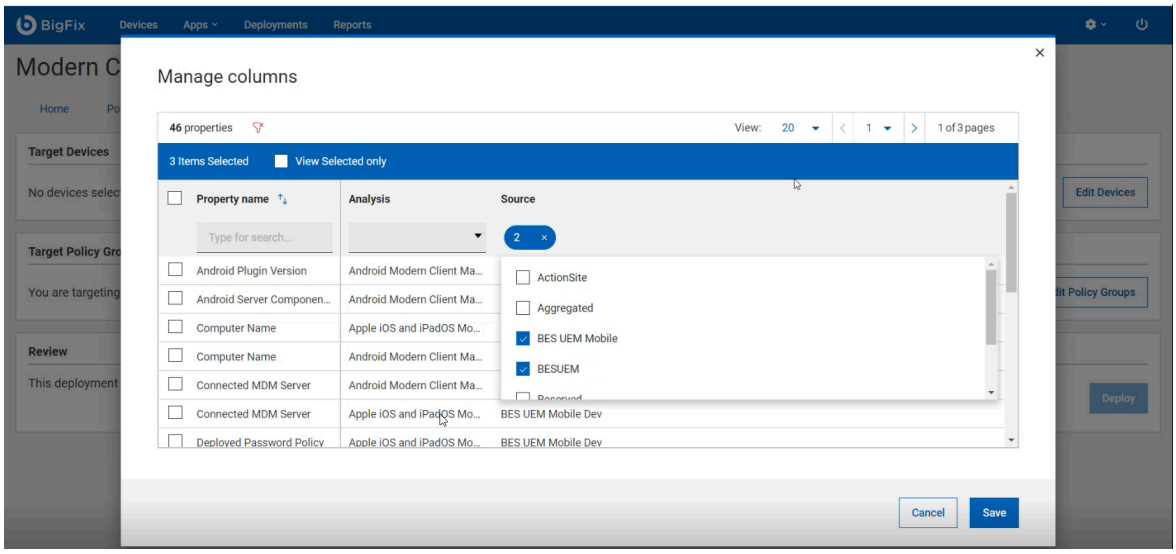
プライマリー・ユーザー列と登録タイプ列をデバイス・リスト (（ページ） *22)*およびデバイス別ターゲット・グリッドに追加します。

1. 「デバイス」ページからターゲットを選択するか、「デバイス別ターゲット」ページから、列の管理アイコンをクリックしま

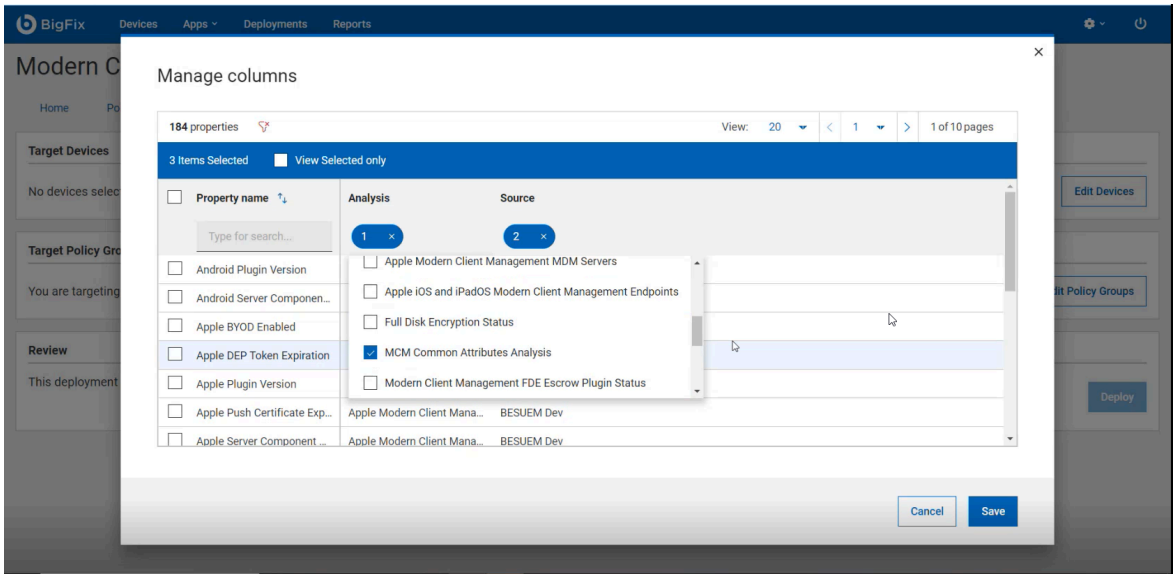




2. 「列の管理」画面の**「ソース」**で、`BESUEM Mobile` と `BESUEM` を選択しま



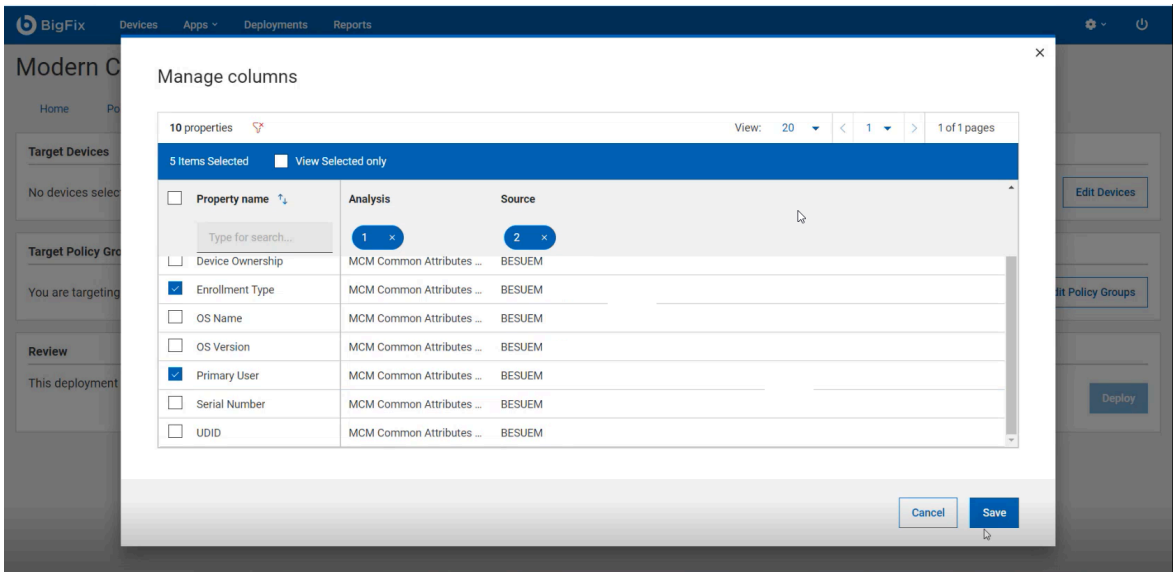
3. **「分析」**リストから、`MCM Common Attributes Analysis` を選択しま



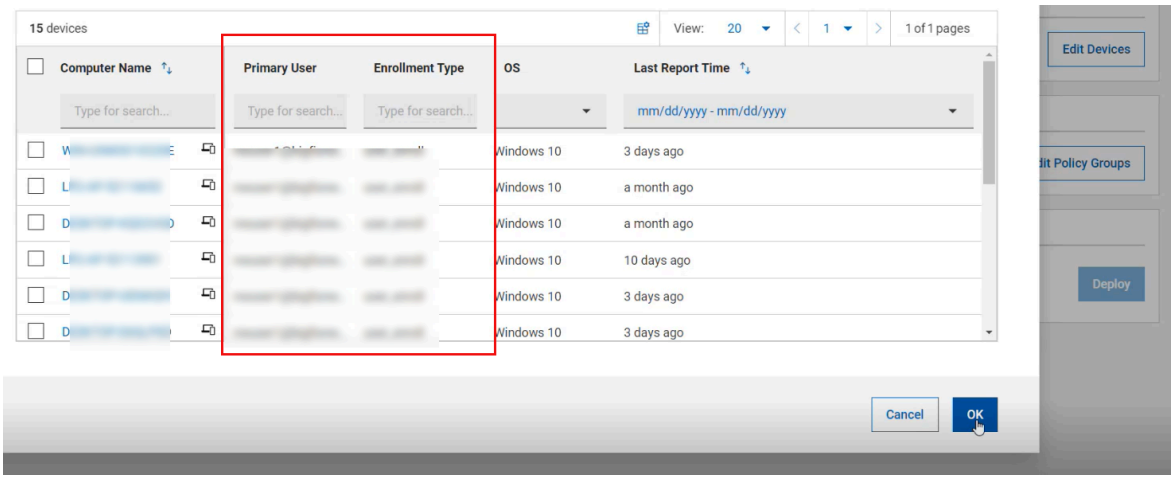
す。

す。

4. **「プロパティー」**の `Enrollment Type` および `Primary User` を選択しま



5. **「保存」**をクリックします。選択したプロパティーがデータ・グリッドの列として追加されます。



注: 「デバイス別ターゲット」ページでプロパティーを追加するときは、ページを開くたびに列を有効にする必要があります。ターゲット・デバイスのページを再度開くと、以前のターゲット・デバイスの選択が有効になります。

データ・グリッドには、検索機能によってプライマリー・ユーザー列と登録タイプ列が追加されます。プライマリー・ユーザーまたは登録タイプは、文字列を使用して検索できます。

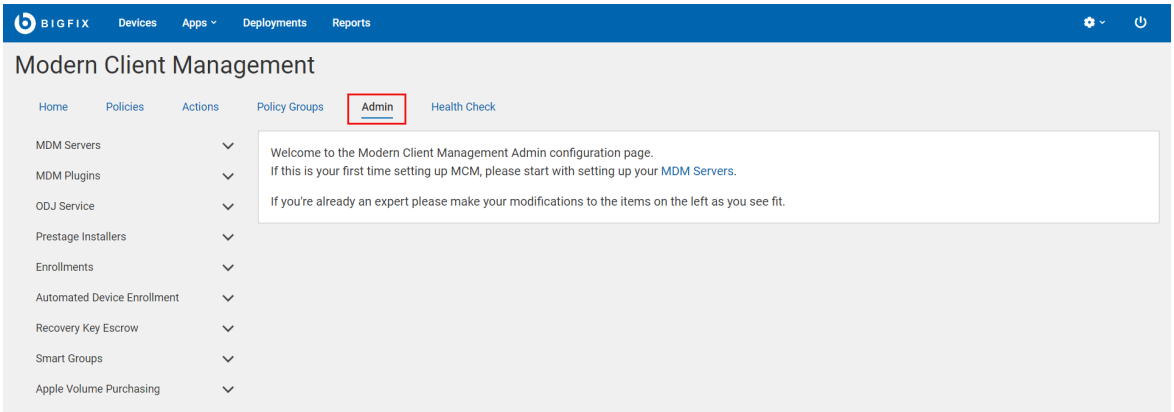
MCM および BigFix Mobile コンポーネントのインストールと管理 - オンプレミスのみ

オンプレミス MDM では、MDM サーバーのセットアップを 1 回だけ実行する必要があります。MDM オンプレミスを適用する前に、必要なハードウェアとソフトウェアをセットアップしておく必要があります。BigFix WebUI を使用して環境をセットアップします。

前提条件、セットアップ手順、その他の情報の詳細については、『インストールおよび設定ガイド』の「オンプレミス・デプロイメントのセットアップ」セクションを参照してください。

BigFix WebUI を使用して MDM コンポーネントを設定および管理する方法は、次のとおりです。

- 自分がマスター・オペレーター (MO) であることを確認します。
- WebUI のメイン・ページで、**「アプリケーション」 > 「MCM」**をクリックし、「Modern Client Management」ページで**「管理者」**をクリックします。



MDM サーバーのインストール

MDM サーバーのインストール: Windows™、Apple®、または Android MDM サーバーのスタンドアロン・バージョンをインストールできます。MDM サーバーに機能を追加して、

これらのオペレーティング・システムの組み合わせを管理することもできます。MDM サーバーをインストールする前に、次の操作を行います。

- Docker Engine、Docker Compose、OpenSSL をインストールします。
- BES クライアントを MDM サーバーのインストール先コンピューターにインストールします。これは、WebUI または Fixlet を使用して MDM サーバーをインストールする必要があるためです。

注: MCM v3.0 では、MDM サーバーのインストール時に LDAP を設定する必要がありません。これは、「機能の管理」画面で設定できます。これにより、MDM サーバーのインストール後に ID サーバーと認証方法を選択するオプションが提供されます。

機能の管理

コンポーネントが 1 つしかインストールされていない MDM サーバー (Windows、Apple、または Android) の場合は、コンポーネントを追加できます。識別情報サービスを構成することもできます。「MDM サーバー機能の管理 (（ページ） 288)」を参照してください。

MDM プラグインのインストール

MDM プラグインのインストール: MDM サーバーと BigFix プラグイン・ポータル間の接続をセットアップするには、MDM プラグインのインストールが必要です。MDM プラグインは、REST API およびクライアント証明書を使用した AMQP プロトコルを介して MDM サーバーと通信します。MDM プラグインは、Apple、Windows、Android デバイスを管理するために使用できます。

MDM プラグインをインストールする前に:

- サーバー・ホストがプラグイン・ポータル・バージョン 10.0.2 以降を実行していることを確認します。

注:

- MDM プラグインの任意のバージョンをインストールするには、プラグイン・ポータル v10.0.2 以降が必要です。
- 最新の MDM バージョンのすべての機能を機能させるには、プラグイン・ポータル v10.0.8 以降が必要です。

- BigFix agent バージョン 10.0.2 以降がローカルで実行されていることを確認します。BigFix クライアントのインストールの詳細については、「BigFix コンポーネントのインストール」をご覧ください。
- 必要な (具体的には CA 証明書からの) 資格情報、クライアント証明書、BESAdmin.sh から生成されたクライアント・キーがあることを確認してください。詳細については、「MDM SSL 証明書」をご覧ください。
- Apple、Windows、Android サーバー用のさまざまな形式の CA TLS 証明書と MDM プッシュ資格情報があることを確認します。

サーバーとクライアントの資格情報の管理

特定の MDM サーバーと安全に通信するために、クライアント・アプリケーション (MDM プラグイン、WebUI、ID サービス) に適切なサーバー証明書とクライアント証明書とキーのセットが必要です。これらの証明書とキーは、BESAdmin を使用して生成し、MDM サーバーのインストール時にアップロードできます。初期インストール後、これらの資格情報を追加、変更、または削除する場合は、WebUI を使用して実行できます。サーバーおよびクライアントの資格情報を追加、更新、または削除する方法について詳しくは、以下を参照してください。

- 資格情報の追加 (（ページ） *302*)
- 資格情報の更新 (（ページ） *304*)
- 資格情報の削除 (（ページ） *305*)

Update (更新)

必要に応じて MDM サーバーとプラグインを更新します。「MDM コンポーネントの更新 (（ページ） 297)」を参照してください。

アンインストール

WebUI からいつでも MDM コンポーネントをアンインストール (（ページ） 298)できます。MDM コンポーネントをアンインストールすると、登録済みデバイスの一部またはすべてを管理する機能が削除される点に注意してください。

Windows 用の BigFix MDM サービスのインストール

WebUI を使用して Windows に MDM サービスを提供するために、BigFix MDM Service for Windows をインストールする方法について説明します。

この手順は、MDM サーバーに MDM サービスを初めてインストールする場合のものです。MDM サービスのいずれかをすでにインストールしている場合は、MDM サーバー機能の管理 (（ページ） *288)* オプションを使用して追加の MDM サービスを追加します。一部の構成はすべての MDM サービスに共通であり、インストールされている MDM サービスごとに再指定すべきではありません。

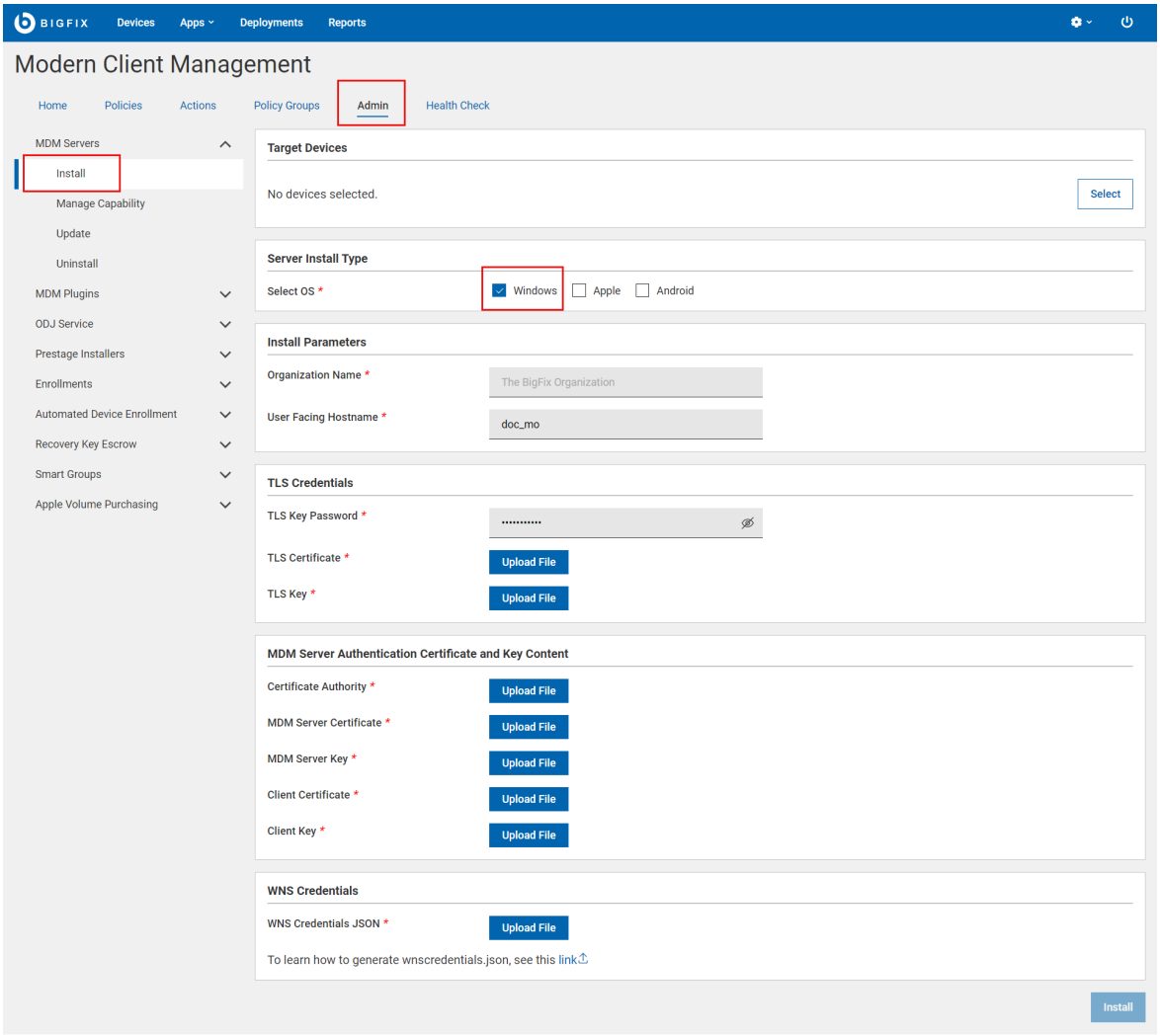
BigFix MDM Service for Windows をインストールするには、次の前提条件を満たす必要があります。

- WebUI 経由でこのタスクを実行するには、マスター・オペレーターでなければなりません。
- `wnscredentials.json` ファイルをアップロードする準備が整っている必要があります。このファイルを作成するためのワークフローについては、『 (（ページ） *)*』を参照してください。
- 信頼できる CA TLS 証明書が必要です。
- 特に CA 証明書からの資格情報、クライアント証明書、BESAdmin.sh から生成されたクライアント・キーが必要です。詳細については、「MDM SSL 証明書」をご覧ください。

BigFix MDM Service for Windows をインストールするには、次の手順を実行します。

1. WebUI のメイン・ページから、**「アプリケーション」 > 「MCM」**を選択します。
2. 「Modern Client Management」ページで、**「管理者」**をクリックします。

3. 「管理者」ページで、**「MDM サーバー」**の左側のナビゲーションから、**「インストール」**を選択します。



4. ターゲット・デバイスの選択**「選択」**をクリックし、MDM サーバーをインストールする、適切なターゲットを選択します。
5. サーバーのインストール・タイプ: 「OS の選択」で**「Windows」**を選択して、Windows デバイスを管理します。
6. インストール・パラメーター:
    - **組織名**: 文字列を入力してください。デバイスの登録中にここに入力した組織名が、エンド・ユーザーに表示されます。
    - **ユーザー向けホスト名**: 無線登録の場合、ユーザーが MDM に登録するためにアクセスできるサーバーのホスト名です。値は、インター

ネットからアクセス可能な有効な FQDN にする必要があります。例えば、`mdmserver.deploy.bigfix.com` です。

注: `https://` ここには含めないでください。

7. TLS 資格情報: MDM サーバーの TLS 証明書とキー・ファイルをアップロードします。
   a. TLS キー・パスワード: TLS キーを復号化するには、TLS キーの暗号化時に使用したパスワードを入力します。
   b. TLS 証明書: 「ファイルのアップロード」をクリックし、場所を参照して TLS `.crt` ファイルを選択します。
   c. TLS キー: 「ファイルのアップロード」をクリックし、場所を参照して、保存済みの暗号化された `mdmserver.key` を選択します。「BigFix MDM サーバー TLS 証明書コンテンツ」を参照してください。
8. MDM サーバー認証証明書とキー・コンテンツ: MDM サーバーの認証証明書とキー・ファイルをアップロードします。
   a. **「認証局」**の場合は、「ファイルのアップロード」をクリックし、ファイルの場所を参照して、`ca.cert.pem` ファイルを選択します。
   b. **「MDM サーバー証明書」**の場合は、「ファイルのアップロード」をクリックし、ファイルの場所を参照して、`server.cert.pem` ファイルを選択します。
   c. **「MDM サーバー・キー」**の場合は、「ファイルのアップロード」をクリックし、ファイルの場所を参照して、`server.key` ファイルを選択します。

      ヒント: `.pem` ファイルと `.key` ファイルの生成方法の詳細については、「MDM SSL 証明書」を参照してください。

   d. **「クライアント証明書」**の場合は、「ファイルのアップロード」をクリックし、`client.cert.pem` ファイルに移動して選択します。
   e. **「クライアント・キー」**の場合は、「ファイルのアップロード」をクリックし、`client.key` ファイルに移動して選択します。
9. WNS 資格情報オペレーティング・システムとして Windows を選択すると、このフィールドが表示されます。「ファイルのアップロード」をクリックし、ファイルの場所を参照して、`wnscredentials.json` ファイルを選択します。

ヒント: `wnscredentials.json` ファイルを生成する方法について詳しくは、『(（ページ）)』を参照してください。

10. **「インストール」**をクリックします。

結果: このアクションは、次のアクティビティーを完了します。

1. MDM のインストールに必要な一連の docker イメージを software.bigfix.com からダウンロードします。
2. サーバーが実行されるプラグイン証明書および TLS 証明書を含むサービスと証明書をインストールします。
3. 必要なすべての構成を適用します。

関連情報

TLS 証明書の更新 (（ページ）)

Apple 用の BigFix MDM サービスのインストール

WebUI を使用して BigFix MDM Service for Apple をインストールする方法について説明します。

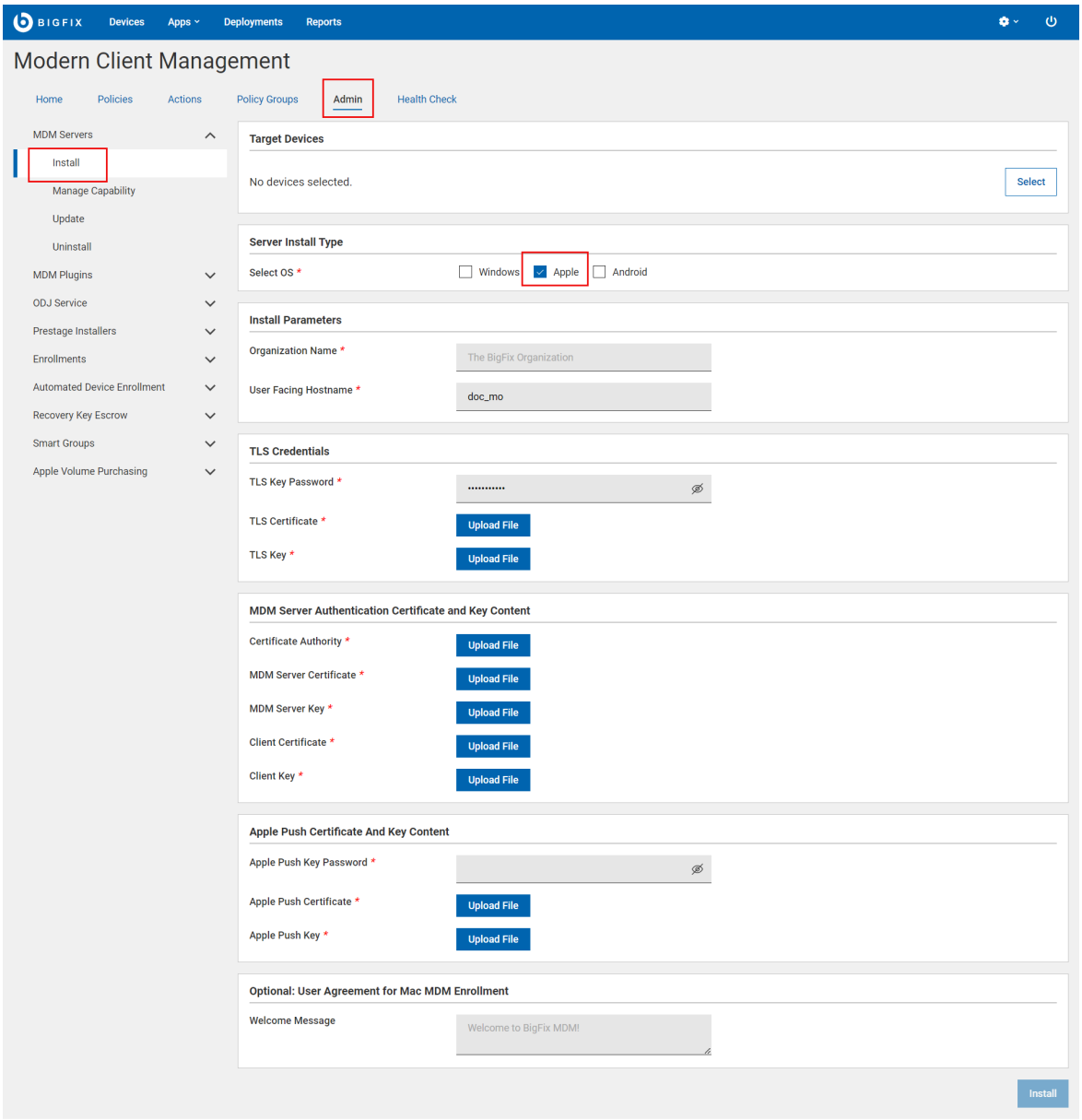
この手順は、MDM サーバーに MDM サービスを初めてインストールする場合のものです。MDM サービスのいずれかをすでにインストールしている場合は、MDM サーバー機能の管理 (（ページ） *288)* オプションを使用して追加の MDM サービスを追加します。一部の構成はすべての MDM サービスに共通であり、インストールされている MDM サービスごとに再指定すべきではありません。

BigFix MDM Service for Apple をインストールするには、次の前提条件を満たす必要があります。

- この MDM サーバーのデプロイメントには、HCL ベンダーの署名プロセスを通じて取得され、Apple によって処理された Apple プッシュ通知証明書 (（ページ）　　) PEM ファイルが必要です。
- 必要な証明書とキーが必要です。「MDM SSL 証明書」をご覧ください。
- MDM サーバー・ターゲットで実行されている BigFix エージェント・バージョン 10.0.2 以降が必要です。
- WebUI 経由でこのタスクを実行するには、マスター・オペレーターでなければなりません。

Apple エンドポイント用の BigFix MDM サーバーをインストールするには、次の手順を実行します。

1. WebUI のメイン・ページから、**「アプリケーション」 > 「MCM」**を選択します。
2. 「Modern Client Management」ページで、**「管理者」**をクリックします。
3. 「管理者」ページで、**「MDM サーバー」**の左側のナビゲーションから、**「インストール」**を選択します。
4. ターゲット・デバイスの選択**「選択」**をクリックし、MDM サーバーをインストールする適切なターゲットを選択します。
5. サーバーのインストール・タイプ: 「OS の選択」で、**「Apple」**を選択します。



6. インストール・パラメーター:
   - 組織名: 文字列を入力してください。デバイスの登録中にここに入力した組織名が、エンド・ユーザーに表示されます。
   - ユーザー向けホスト名: 無線登録の場合、ユーザーが MDM に登録するためにアクセスできるサーバーのホスト名です。値は、インター

ネットからアクセス可能な有効な FQDN にする必要があります。例えば、`mdmserver.deploy.bigfix.com` です。

注: `https://` ここには含めないでください。

7. TLS 資格情報: MDM サーバーの TLS 証明書とキー・コンテンツの詳細を入力します。
   a. TLS キー・パスワード: TLS キーを復号化するには、TLS キーの暗号化時に使用したパスワードを入力します。
   b. TLS 証明書: 「ファイルのアップロード」をクリックし、場所を参照して TLS `.crt` ファイルを選択します。
   c. TLS キー: 「ファイルのアップロード」をクリックし、場所を参照して、保存済みの暗号化された `mdmserver.key` を選択します。「BigFix MDM サーバー TLS 証明書コンテンツ」を参照してください。
8. MDM サーバー認証証明書とキー・コンテンツ: MDM サーバーの認証証明書とキー・ファイルをアップロードします。
   a. **「認証局」**の場合は、「ファイルのアップロード」をクリックし、ファイルの場所を参照して、`ca.cert.pem` ファイルを選択します。
   b. **「MDM サーバー証明書」**の場合は、「ファイルのアップロード」をクリックし、ファイルの場所を参照して、`server.cert.pem` ファイルを選択します。
   c. **「MDM サーバー・キー」**の場合は、「ファイルのアップロード」をクリックし、ファイルの場所を参照して、`server.key` ファイルを選択します。

      ヒント: `.pem` ファイルと `.key` ファイルの生成方法の詳細については、「MDM SSL 証明書」を参照してください。

   d. **「クライアント証明書」**の場合は、「ファイルのアップロード」をクリックし、`client.cert.pem` ファイルに移動して選択します。
   e. **「クライアント・キー」**の場合は、「ファイルのアップロード」をクリックし、`client.key` ファイルに移動して選択します。
9. Apple プッシュ証明書とキー・コンテンツ:

- Apple プッシュ・キー・パスワード: 「APN 証明書の生成」で説明されているように、プッシュ証明書秘密鍵の暗号化に使用した秘密鍵パスフレーズを入力します。
- Apple プッシュ証明書: 「ファイルのアップロード」をクリックし、ファイルの場所を参照して、`Push PEM` ファイルを選択します。
- Apple プッシュ・キー: 「APN 証明書の生成」の手順 2 で説明されているように、「ファイルのアップロード」をクリックしてファイルの場所を参照し、暗号化された `Push key` ファイルを選択します。

10. Mac MDM 登録のユーザー契約: これはオプションです。MDM への登録を受け入れる前にユーザーに表示される、ウェルカム・メッセージ・テキストを入力します。ここに入力したメッセージは、登録プロセスを通じて Apple デバイスの登録を続行することを受け入れるためにエンド・ユーザーに表示されます。これにより、組織はデバイス登録の使用条件をデバイスのユーザーに通知または警告できます。このメッセージには、例えば、デバイスまたはヘルプデスクの連絡先情報のリモート管理を許可する警告が含まれます。
11. **「インストール」**をクリックします。

結果: このアクションは、次のアクティビティーを完了します。

1. MDM のインストールに必要な一連の docker イメージを software.bigfix.com からダウンロードします。
2. サーバーが実行されるプラグイン証明書、TLS 証明書、および Apple プッシュ証明書を含むサービスと証明書をインストールします。
3. 必要なすべての構成を適用します。

関連情報

TLS 証明書の更新 (（ページ）　　)

Android 用 BigFix MDM サービスのインストール

WebUI を使用して BigFix MDM Service for Android をインストールする方法について説明します。

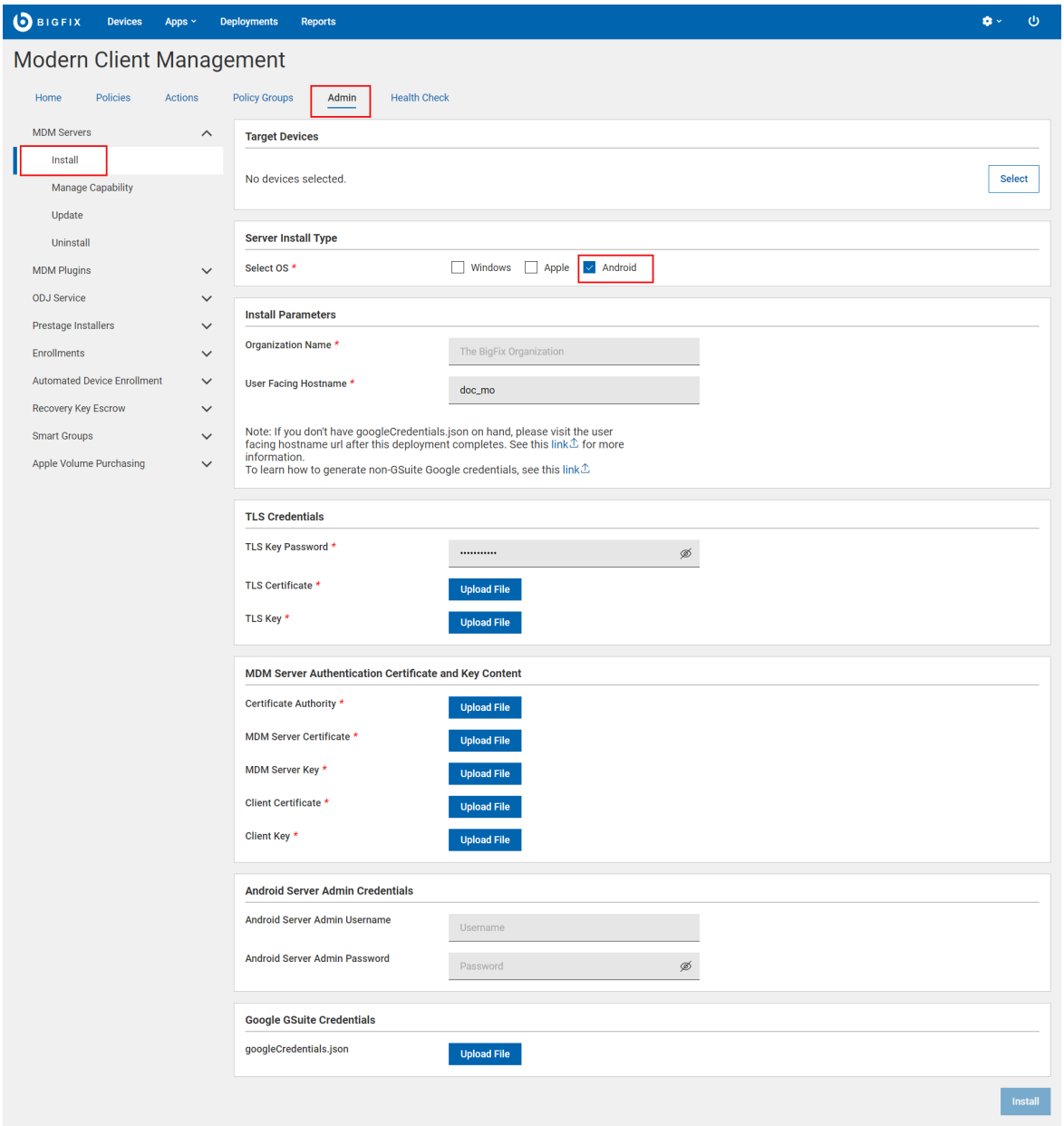
この手順は、MDM サーバーに MDM サービスを初めてインストールする場合のものです。MDM サービスのいずれかをすでにインストールしている場合は、MDM サーバー機能の管理 (（ページ） *288)* オプションを使用して追加の MDM サービスを追加します。一部の構成はすべての MDM サービスに共通であり、インストールされている MDM サービスごとに再指定すべきではありません。

Android エンドポイント用の BigFix MDM サーバーをインストールするには、次の前提条件を満たす必要があります。

- 必要な証明書とキーが必要です。『BigFix プラグインおよび MDM SSL 証明書とキー (（ページ）)』を参照してください。
- MDM サーバー・ターゲットで実行されている BigFix エージェントが必要です。
- WebUI 経由でこのタスクを実行するには、マスター・オペレーターでなければなりません。

Android エンドポイント用の BigFix MDM サーバーをインストールするには、次の手順を実行します。

1. WebUI のメイン・ページから、**「アプリケーション」 > 「MCM」**を選択します。
2. 「Modern Client Management」ページで、**「管理者」**をクリックします。
3. 「管理者」ページの左側のナビゲーションで、「MDM サーバー」の下にある**「インストール」**を選択します。
4. ターゲット・デバイスの選択**「選択」**をクリックし、MDM サーバーをインストールする適切なターゲットを選択します。
5. サーバーのインストール・タイプ: 「OS の選択」で「Android」を選択します。



6. インストール・パラメーター:
    - 組織名: 文字列を入力してください。デバイスの登録中に、ここに入力した組織名が、残りのプロファイル情報と共にユーザーに表示されます。
    - ユーザー向けホスト名: 無線登録の場合、ユーザーが MDM に登録するためにアクセスできるサーバーのホスト名です。無線登録の場合、ユーザーが MDM に登録するためにアクセスできるサーバーのホスト名です。値は、イ

ンターネットからアクセス可能な有効な FQDN にする必要があります。例えば、`mdmserver.deploy.bigfix.com` です。

注: `https://` ここには含めないでください。

一部の Android 管理構成もここで行われます。「Managed Google Play アカウント エンタープライズに登録する (（ページ）　　)」を参照してください。

7. TLS 資格情報: MDM サーバーの TLS 証明書とキー・コンテンツの詳細を入力します。
   a. TLS キー・パスワード: TLS キーを復号化するには、TLS キーの暗号化時に使用したパスワードを入力します。
   b. TLS 証明書: 「ファイルのアップロード」をクリックし、場所を参照して TLS `.crt` ファイルを選択します。
   c. TLS キー: 「ファイルのアップロード」をクリックし、場所を参照して、保存済みの暗号化された `mdmserver.key` を選択します。「BigFix MDM サーバー TLS 証明書コンテンツ」を参照してください。
8. MDM サーバー認証証明書とキー・コンテンツ: MDM サーバーの認証証明書とキー・ファイルをアップロードします。
   a. **「認証局」**の場合は、「ファイルのアップロード」をクリックし、ファイルの場所を参照して、`ca.cert.pem` ファイルを選択します。
   b. **「MDM サーバー証明書」**の場合は、「ファイルのアップロード」をクリックし、ファイルの場所を参照して、`server.cert.pem` ファイルを選択します。
   c. **「MDM サーバー・キー」**の場合は、「ファイルのアップロード」をクリックし、ファイルの場所を参照して、`server.key` ファイルを選択します。

      ヒント: `.pem` ファイルと `.key` ファイルの生成方法の詳細については、「MDM SSL 証明書」を参照してください。

   d. **「クライアント証明書」**の場合は、「ファイルのアップロード」をクリックし、`client.cert.pem` ファイルに移動して選択します。
   e. **「クライアント・キー」**の場合は、「ファイルのアップロード」をクリックし、`client.key` ファイルに移動して選択します。

9. G Suite 以外のアカウントの場合は、Android サーバー管理者資格情報が必要です。G-Suite アカウントの場合は、Google Gsuite 資格情報が必要です。

   注: Android サーバー管理者資格情報または Google Gsuite 資格情報のいずれかが必要です。両方は必須ではありません。両方を入力しようとすると UI が停止します。

   Android サーバー管理者の資格情報:

   a. Android サーバー管理者のユーザー名: ストリングを入力して管理 UI ユーザー名を設定します。
   b. Android サーバー管理者のパスワード: ストリングを入力して管理 UI パスワードを設定します。

      重要: アプリケーションのセキュリティーを向上するために、強力で複雑なパスワード (例えば、長いほど安全性が高まるので長さが 12 文字以上で、大文字、小文字、数字、句読点、特殊記号を組み合わせたもの) を設定します。

   `googlecredentials.json` ファイルを生成する方法について詳しくは、『Managed Google Play アカウント エンタープライズに登録する ((ページ))』を参照してください。

   または

   Google GSuite 資格情報: 「ファイルのアップロード」をクリックし、ファイルの場所を参照して、`googlecredentials.json` ファイルを選択します。
10. **「インストール」**をクリックします。

結果: このアクションは、次のアクティビティーを完了します。

1. MDM のインストールに必要な一連の docker イメージを software.bigfix.com からダウンロードします。
2. サーバーが実行されるプラグイン証明書および TLS 証明書を含むサービスと証明書をインストールします。
3. 必要なすべての構成を適用します。

関連情報

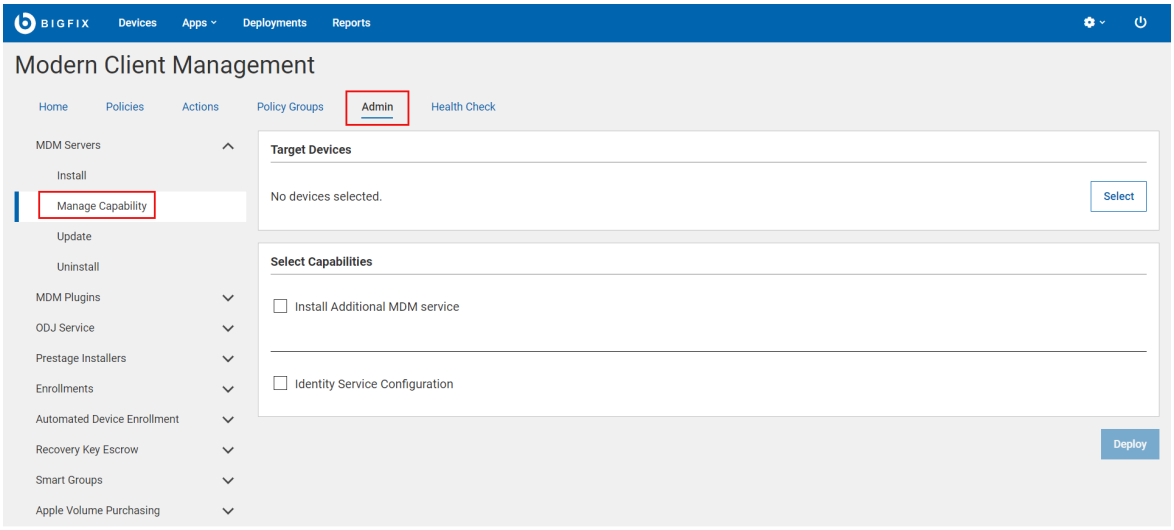
TLS 証明書の更新 (（ページ）　　)

MDM サーバー機能の管理

このトピックでは、Windows、Apple、Android などの追加の MDM サービスをインストールし、ID サービスを構成する方法について説明します。

3 つすべての MDM コンポーネントがインストールされていない MDM サーバー (Windows、Apple または macOS) の場合は、不足しているコンポーネントを追加できます。例えば、Windows MDM サーバーは、このワーク・フローを使用して Apple MDM または Android MDM サーバーの機能を追加できます (その逆も実行できます)。この画面を使用して、組織の ID サービスで使用される認証方式を構成することもできます。

1. WebUI のメイン・ページから、**「アプリケーション」 > 「MCM」**を選択します。
2. 「Modern Client Management」ページで、**「管理者」**をクリックします。
3. 「管理者」ページで、**「MDM サーバー」 > 「機能の管理」**を選択します。以下のページが表示されます。



4. **「選択」**をクリックして、追加の MDM サービスをインストールしたり、ID サービスを構成したりする MDM サーバーを選択します。MDM サーバーにデプロイするオプションを 1 つ以上選択する必要があります。
5. **追加の MDM サービスのインストール**

   a. 「機能の選択」セクションで、**「追加の MDM サービスのインストール」**チェックボックスをオンにします。

   b. オペレーティング・システムを選択します。

   - Windows

     WNS 資格情報オペレーティング・システムとして Windows を選択すると、このフィールドが表示されます。「ファイルのアップロード」をクリックし、ファイルの場所を参照して、`wnscredentials.json` ファイルを選択します。

     ヒント: `wnscredentials.json` ファイルを生成する方法について詳しくは、『 (（ページ）)』を参照してください。

   - Apple
     - Apple プッシュ証明書とキー・コンテンツ:
       - Apple プッシュ・キー・パスワード: Apple プッシュ・キー・パスワードを入力します。
       - Apple プッシュ証明書: 「ファイルのアップロード」をクリックし、ファイルの場所を参照して、`Push PEM` ファイルを選択します。
       - Apple プッシュ・キー: 「ファイルのアップロード」をクリックし、ファイルの場所を参照して、`Push key` ファイルを選択します。MDM サーバーの Apple プッシュ証明書を取得する方法については、APN 証明書の生成 (（ページ）)を参照してください。
     - Mac MDM 登録のユーザー契約: これはオプションです。エンド・ユーザー契約のようこそメッセージ・テキストを入力します。ここに入力したメッセージは、登録プロセスを通じて Apple デバイスの登録を続行することを受け入れるためにエンド・ユーザーに表示さ

れます。これにより、組織はデバイスの登録条件をデバイス・ユーザーに通知または警告できます。このメッセージには、例えば、デバイスまたはヘルプデスクの連絡先情報のリモート管理を許可する警告が含まれます。

- Android
  - G Suite 以外のアカウントの場合は、Android サーバー管理者資格情報が必要です。G-Suite アカウントの場合は、Google G-Suite 資格情報が必要です。

    注: Android サーバー管理者資格情報または Google Gsuite 資格情報のいずれかが必要です。両方は必須ではありません。両方を入力しようとすると UI が停止します。

    Android サーバー管理者の資格情報:
    - Android サーバー管理者のユーザー名: ユーザー名を入力してください。
    - Android サーバー管理者のパスワード: パスワードを入力してください。

    `googlecredentials.json` ファイルを生成する方法について詳しくは、『Managed Google Play アカウント エンタープライズに登録する (（ページ）　　)』を参照してください。

    または

    Google GSuite 資格情報: 「ファイルのアップロード」をクリックし、ファイルの場所を参照して、`googlecredentials.json` ファイルを選択します。

6. **ID サービスの設定**

   a. 「機能の選択」セクションで、**「ID サービスの設定」**チェックボックスをオンにします。選択できる ID サービス・オプションが表示されます。

   b. ID サービスの選択

- 認証なし: 認証が不要な場合は、このオプションを選択します。これにより、ユーザーの資格情報を使用して身元を確認することなく、誰でも MCM サービスに登録できるようになります。
- AD/OpenLDAP
  - SAML 有効化: これはオプションです。SAML 認証の構成 (（ページ）) を使用可能にするには、このチェックボックスを選択します。

    注: MCM v3.0 では、Okta がサポートされます。Okta 固有の設定に関する手順を以下に示します。

    - SAML 資格情報: 次の形式で、発行者および signOnUrl 情報を含む JSON ファイルをアップロードします。

      ```
      { "issuer" : "http://www.okt.......ndV5d7",
      "signOnUrl" :
       "https://dev-12345............WIBUg5d7/aln7rix...
      ..FK5d7" }
      ```

      注: `.json` ファイルの作成方法について詳しくは、ステップ 2: SAML 資格情報ファイルの作成 (（ページ）)を参照してください。

    - SAML Identity Provider 証明書: ダウンロードした `okta.cert` ファイルをアップロードします ステップ 3: Okta サーバーから SAML 識別情報 プロバイダ証明書をダウンロード (（ページ）)
  - LDAP URL: これは必須です。有効な形式は https://<server>:<port> です。LDAP URL 形式の詳細については、「https://ldap.com/ldap-urls/」を参照してください
  - LDAP 基本 DN: これは必須です。有効な形式「dc=example,dc=org」

注: 複数のベース DN の構成はサポートされていません。

- LDAP バインド・ユーザー: これは必須です。サーバーにバインドするためのルート・ポイント。例えば、CN=LdapCreds,DC=mydomain,DC=mycompany,DC=com."user@example.o
- LDAP バインド・パスワード: これは必須です。文字列を入力してください。

• Azure AD

- SAML 有効化: これはオプションです。SAML 認証登録 (（ページ）*291)*を有効にするには、このチェックボックスをオンにします。
- Azure の資格情報: これは必須です。次の形式で Azure AD 資格情報を含む .`json` ファイルをアップロードします。

```
{ "client_id": "06b6d920-xxxx-xxxx-xxxx-73792306xxxx",
  "tenant_id": "31ac2431-xxxx-xxxx-xxxx-6215b1c2xxxx",
  "client_secret":
 "d7bc6b2e-xxxx-xxxx-xxxx-b5c681e5xxxx"
 }
```

この情報の取得方法については、Azure AD の登録と構成にある BigFix Wiki のドキュメントを参照してください。

7. **「デプロイ」**をクリックします。

注: 「デプロイ」ボタンが有効になるのは、選択した機能に必要なすべてのパラメーターがエラーなしで指定された場合のみです。

対象となる MDM サーバーの既存の機能の上に、選択したオペレーティング・システムの機能が追加されます。認証方式と ID サービスが設定されます。

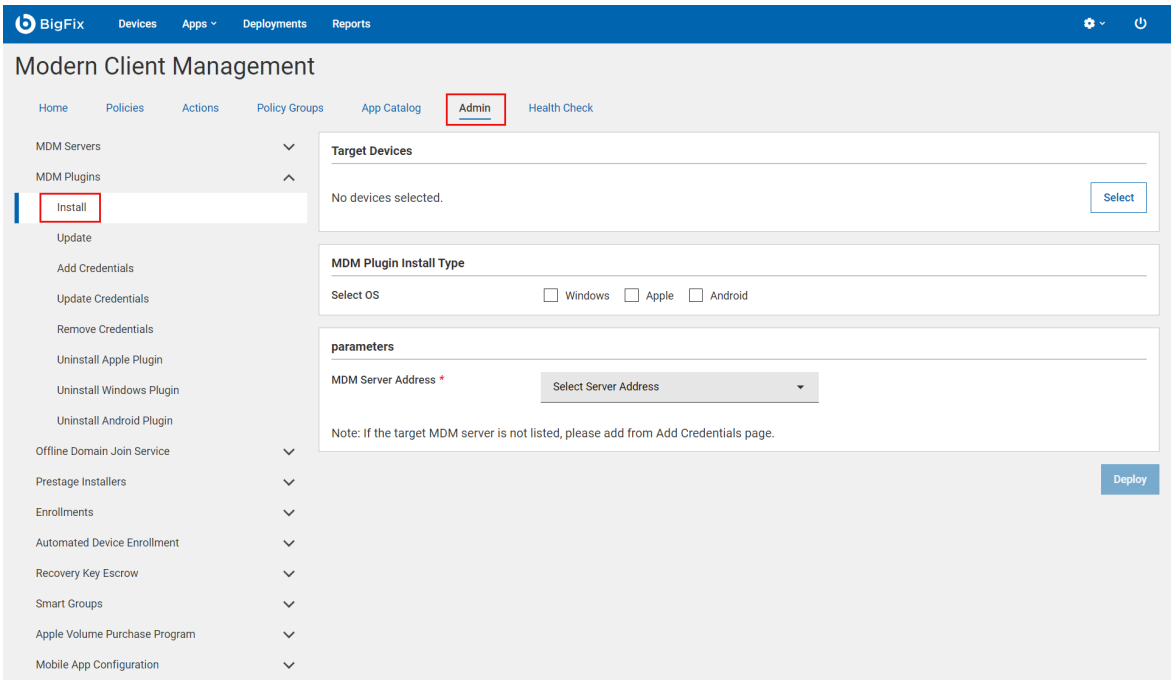
Windows 用の MDM プラグインのインストール

サポートされている MDM プラグイン (Windows、Apple、Android) をプラグイン・ポータル (Windows または Linux) にデプロイするには、以下の手順を実行します。

ターゲット・サーバー・ホストは、BigFix クライアントが実行され、プラグイン・ポータルがインストールされている必要があります。

MDM プラグインを Windows または Linux のプラグイン・ポータルにインストールするには、次の手順を実行します。

1. WebUI のメイン・ページから、**「アプリケーション」 > 「MCM」**を選択します。
2. 「Modern Client Management」ページで、**「管理者」**をクリックします。
3. 「管理者」ページで、**「MDM プラグイン」**の左側のナビゲーションから、**「インストール」**をクリックします。



4. 「対象デバイス」セクションで、**「選択」**をクリックし、MDM プラグインをインストールする Windows または Linux のプラグイン・ポータルを選択します。
5. MDM の**「プラグインのインストール・タイプ」**で、オペレーティング・システムとして Windows を選択します。

注: 複数のオペレーティング・システムを選択し、選択したオペレーティング・システムの MDM プラグインを同時にインストールできます。

6. 「パラメーター」の下の**「MDM サーバー・アドレス」**ドロップダウンから、Windows 用の BigFix MDM サービスのインストール (（ページ）)で入力したものと同じ MDM サーバーのホスト名または IP アドレスを選択します。このオプションを選択すると、プラグイン・ポータルは、DMZ 内にある選択した MDM サーバーとの接続を確立できます。
7. **「デプロイ」**をクリックします。

インストールに成功すると、MDM プラグイン・ファイルは次の場所にあります。

- Windows – `C:\Program File (x86)\BigFix Enterprise\BES Plugin Portal\Plugins`
- Linux
  - 2 進数 – `/opt/BESPluginPortal/Plugins`
  - データ・ファイル – `/var/opt/BESPluginPortal`

登録済みの Windows エンドポイントを管理 (（ページ） *368)*できるようになりました。

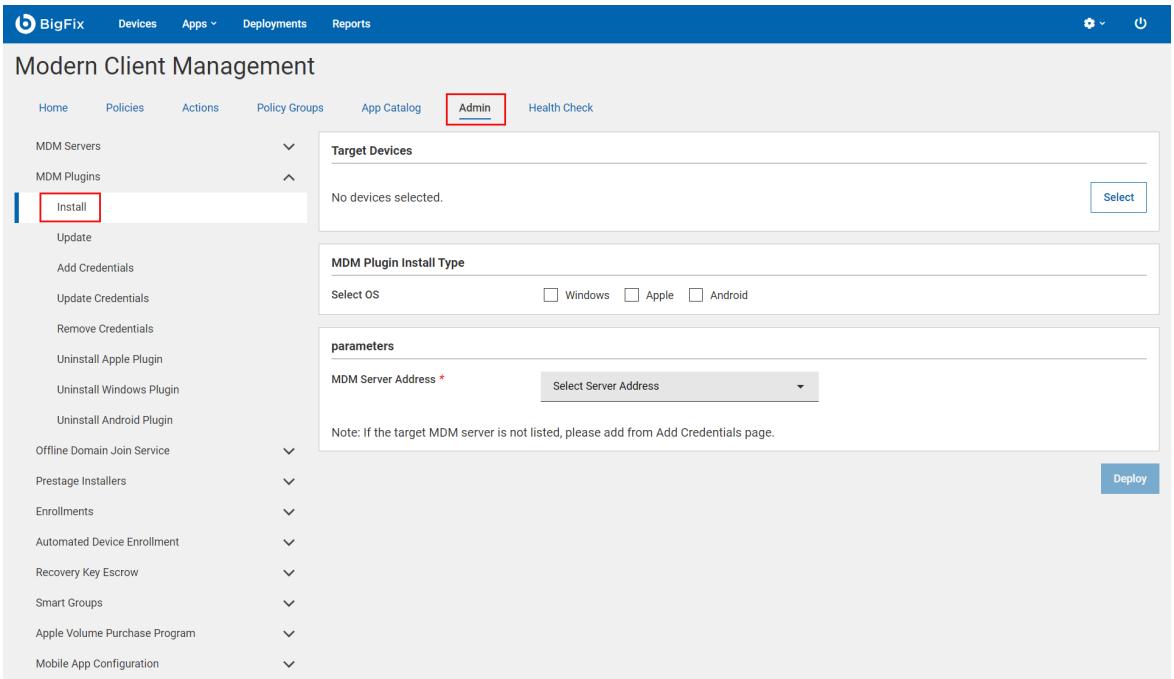
Apple 用の MDM プラグインのインストール

Windows または Linux のプラグイン・ポータルに MDM プラグインをデプロイして Apple デバイスを管理する方法について説明します。

ターゲット・サーバー・ホストは、BigFix クライアントが実行され、プラグイン・ポータルがインストールされている必要があります。

Apple 用の MDM プラグインをデプロイするには、次の手順に従います。

1. WebUI のメイン・ページから、**「アプリケーション」 > 「MCM」**を選択します。
2. 「Modern Client Management」ページで、**「管理者」**をクリックします。
3. 「管理者」ページで、「MDM プラグイン」の左側のナビゲーションから、**「インストール」**をクリックします。



4. 「対象デバイス」セクションで、**「選択」**をクリックし、MDM プラグインをインストールする MDM サーバーを選択します。
5. 「MDM プラグインのインストール・タイプ」で、オペレーティング・システムとして Apple を選択します。

   注: 複数のオペレーティング・システムを選択し、選択したオペレーティング・システムの MDM プラグインを同時にインストールできます。

6. 「パラメーター」の下の**「MDM サーバー・アドレス」**ドロップダウンから、Apple 用の BigFix MDM サービスのインストール (（ページ） 279)で入力したものと同じ MDM サーバーのホスト名または IP アドレスを選択します。このオプションを選択すると、プラグイン・ポータルは、DMZ 内にある選択した MDM サーバーとの接続を確立できます。

インストールに成功すると、MDM プラグイン・ファイルは次の場所にあります。

- Windows – `C:\Program File (x86)\BigFix Enterprise\BES Plugin Portal\Plugins`
- Linux

- 2 進数 – `/opt/BESPluginPortal/Plugins`
- データ・ファイル – `/var/opt/BESPluginPortal`

登録した Apple エンドポイントを管理 (（ページ） *368)*できるようになりました。

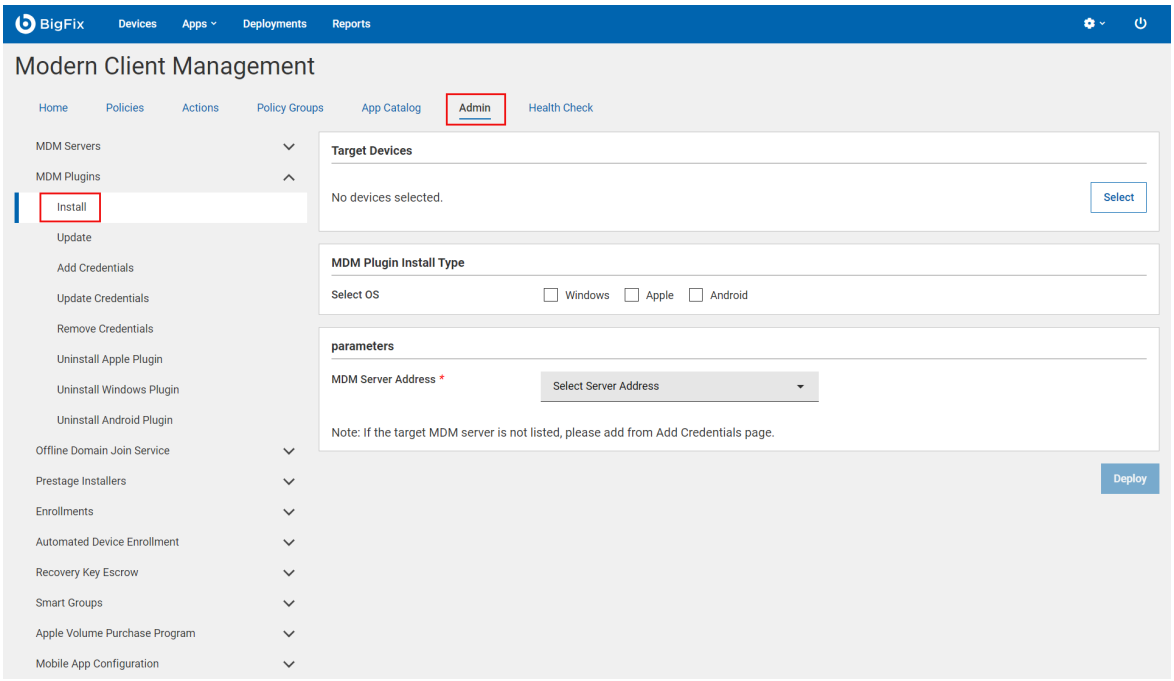
Android 用の MDM プラグインのインストール

Android プラグイン・ポータルでサポートされている MDM プラグインをデプロイする方法について説明します。

ターゲット・サーバー・ホストは、BigFix クライアントが実行され、プラグイン・ポータルがインストールされている必要があります。

Android 用の MDM プラグインをインストールするには、次の手順を実行します。

1. WebUI のメイン・ページから、**「アプリケーション」 > 「MCM」**を選択します。
2. 「Modern Client Management」ページで、**「管理者」**をクリックします。
3. 「管理者」ページで、「MDM プラグイン」の左側のナビゲーションから、**「インストール」**をクリックします。



4. 「対象デバイス」セクションで、**「選択」**をクリックし、MDM プラグインをインストールする MDM サーバーを選択します。
5. 「MDM プラグインのインストール・タイプ」で、オペレーティング・システムに Android を選択します。

   注: 複数のオペレーティング・システムを選択し、選択したオペレーティング・システムの MDM プラグインを同時にインストールできます。

6. 「パラメーター」の下の**「MDM サーバー・アドレス」**ドロップダウンから、Android 用 BigFix MDM サービスのインストール (（ページ）)で入力したものと同じ MDM サーバーのホスト名または IP アドレスを選択します。このオプションを選択すると、プラグイン・ポータルは、DMZ 内にある選択した MDM サーバーとの接続を確立できます。
7. **「デプロイ」**をクリックします。

インストールに成功すると、MDM プラグイン・ファイルは次の場所にあります。

- Windows – `C:\Program File (x86)\BigFix Enterprise\BES Plugin Portal\Plugins`
- Linux
  - 2 進数 – `/opt/BESPluginPortal/Plugins`
  - データ・ファイル – `/var/opt/BESPluginPortal`

これで、登録済みの Android エンドポイントを管理 (（ページ） *368)*できます。

MDM コンポーネントの更新

MDM コンポーネントを更新する方法について説明します。

始める前に:

- WebUI 経由でこのタスクを実行するには、マスター・オペレーターでなければなりません。
- MDM プラグインを最新バージョンに更新するには、プラグイン・ポータルのバージョン 10.0.2 以降が必要です。

MDM サーバーの更新

MDM サーバーを更新するには、次の手順を実行します。

1. WebUI のメイン・ページから、**「アプリ」 > 「MCM」**をクリックします。
2. 「Modern Client Management」ページで、**「管理者」**をクリックします。
3. 「管理者」ページの左側のナビゲーションで、「MDM サーバー」の下の**「更新」**をクリックします。
4. 「対象デバイス」セクションで**「デバイスの編集」**をクリックします。更新が必要な使用可能なサーバーの一覧が表示されます。必要なサーバーを選択し、**「OK」**をクリックします。
5. 選択したサーバーの数を確認し、**「デプロイ」**をクリックします。WebUI は対象のサーバーで更新プログラムを実行します。

MDM プラグインの更新

MDM プラグインを更新するには:

1. WebUI のメイン・ページから、**「アプリ」 > 「MCM」**をクリックします。
2. 「Modern Client Management」ページで、**「管理者」**をクリックします。
3. 「管理者」ページの左側のナビゲーションで、「MDM プラグイン」の下の**「更新」**をクリックします。
4. 「対象デバイス」セクションで**「デバイスの編集」**をクリックします。更新が必要な使用可能なデバイスの一覧が表示されます。必要なデバイスを選択し、**「OK」**をクリックします。
5. 選択したサーバーの数を確認し、**「デプロイ」**をクリックします。WebUI は対象のサーバーで更新プログラムを実行します。

MDM コンポーネントのアンインストール

MDM コンポーネントをアンインストールする方法について説明します。

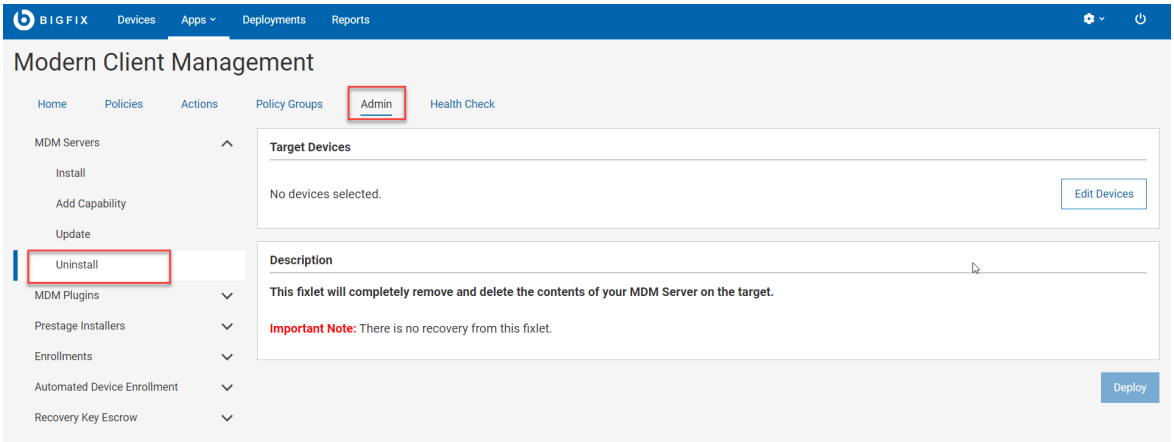
始める前に: WebUI 経由でこのタスクを実行するには、マスター・オペレーターでなければなりません。

MDM サーバーのアンインストール

MDM サーバーをアンインストールすると、サーバーから BigFix MDM が削除され、そのサーバーから MDM サービスを使用できなくなります。MDM サーバーをアンインストールすると復旧する方法はありません。MDM デバイスを登録し、再び適切にレポートできるようにするには、MDM を再インストールする必要があります。

MDM サーバーをアンインストールするには、次の手順を実行します。

1. WebUI のメイン・ページから、**「アプリ」 > 「MCM」**をクリックします。
2. 「Modern Client Management」ページで、**「管理者」**をクリックします。
3. 「管理者」ページの左側のナビゲーションで、「MDM サーバー」の下の**「アンインストール」**をクリックします。



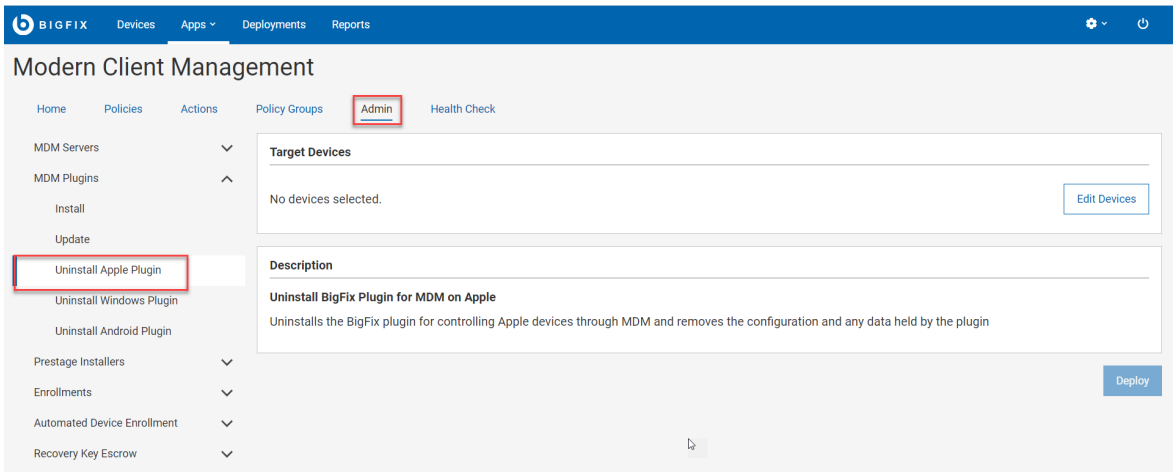
4. **「デバイスの編集」**をクリックし、アンインストールする MDM サーバーを選択します。
5. **「デプロイ」**をクリックします。

Apple 用 MDM プラグインのアンインストール

Apple 用 MDM プラグインをデバイスからアンインストールすると、そのサーバーから Apple デバイスを管理できなくなります。

アンインストールするには:

1. WebUI のメイン・ページから、**「アプリ」 > 「MCM」**をクリックします。
2. 「Modern Client Management」ページで**「管理者」**をクリックします。
3. 「Modern Client Managemen」ページの左側のペインで、「MDM プラグイン」の下の**「Apple プラグインのアンインストール」**をクリックします。



4. **「デバイスの編集」**をクリックし、MDM プラグインをアンインストールするサーバーを選択します。
5. **「デプロイ」**をクリックします。

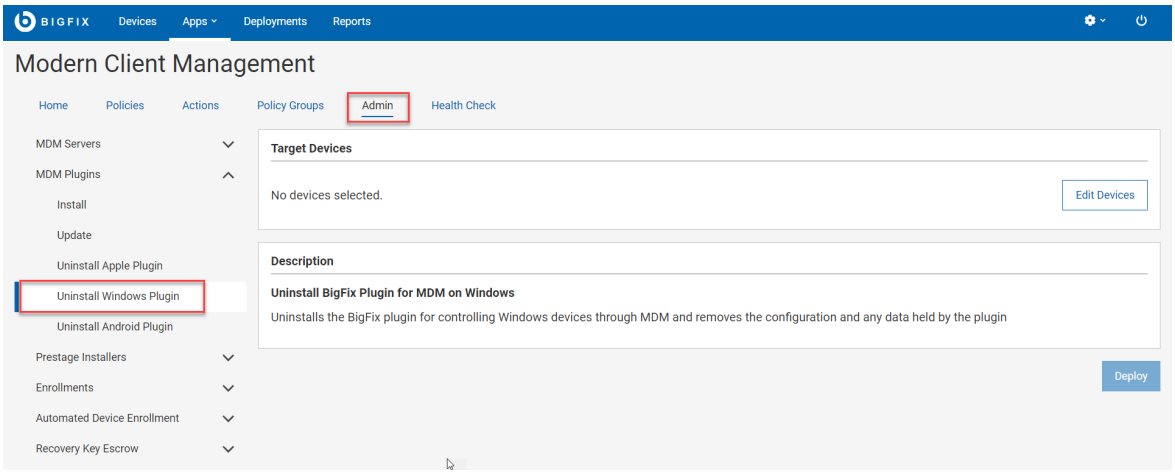
Windows 用 MDM プラグインのアンインストール

Windows 用の MDM プラグインをアンインストールすると、そのプラグイン・ポータルから Windows デバイスを管理できなくなります。

アンインストールするには:

1. WebUI のメイン・ページから、**「アプリ」 > 「MCM」**をクリックします。
2. 「Modern Client Management」ページで、**「管理者」**をクリックします。

3. 「Modern Client Management」ページの左側のペインで、「MDM プラグイン」の下の**「Windows プラグインのアンインストール」**をクリックします。



4. **「デバイスの編集」**をクリックし、Windows MDM プラグインをアンインストールするデバイスを選択します。
5. **「デプロイ」**をクリックします。

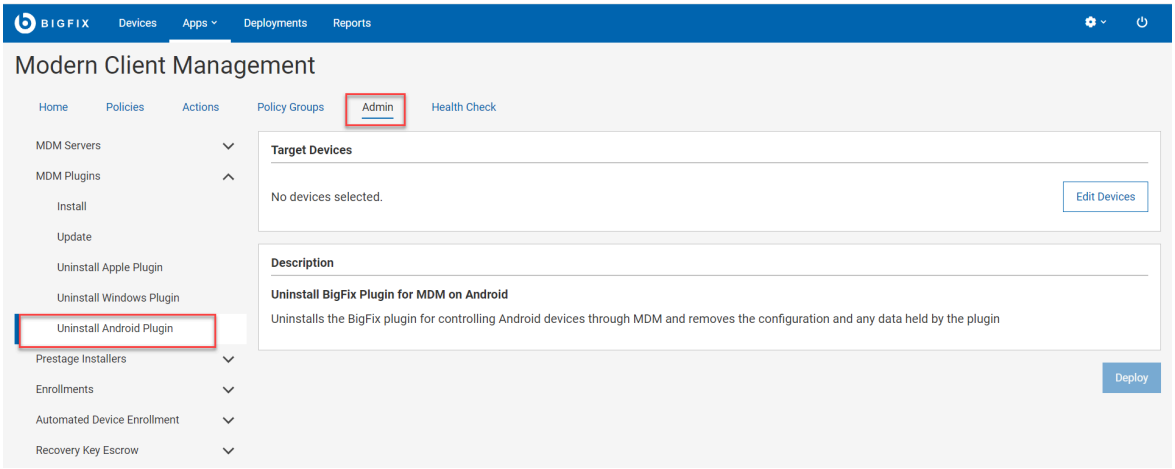
Android 用 MDM プラグインのアンインストール

Android 用の MDM プラグインをアンインストールすると、そのプラグイン・ポータルから Android デバイスを管理できなくなります。

アンインストールするには:

1. WebUI のメイン・ページから、**「アプリ」 > 「MCM」**をクリックします。
2. 「Modern Client Management」ページで、**「管理者」**をクリックします。

3. 「Modern Client Management」ページの左側のペインで、「MDM プラグイン」の下の**「Android プラグインのアンインストール」**をクリックします。



4. **「デバイスの編集」**をクリックし、Android MDM プラグインをアンインストールするデバイスを選択します。
5. **「デプロイ」**をクリックします。

関連資料

MDM サーバー再インストール中のエラー (（ページ）　　)

資格情報の追加

最初の MDM サーバーのインストール後、追加サーバーの資格情報を追加する場合は、いつでも WebUI の**「資格情報の追加」**ページから追加できます。

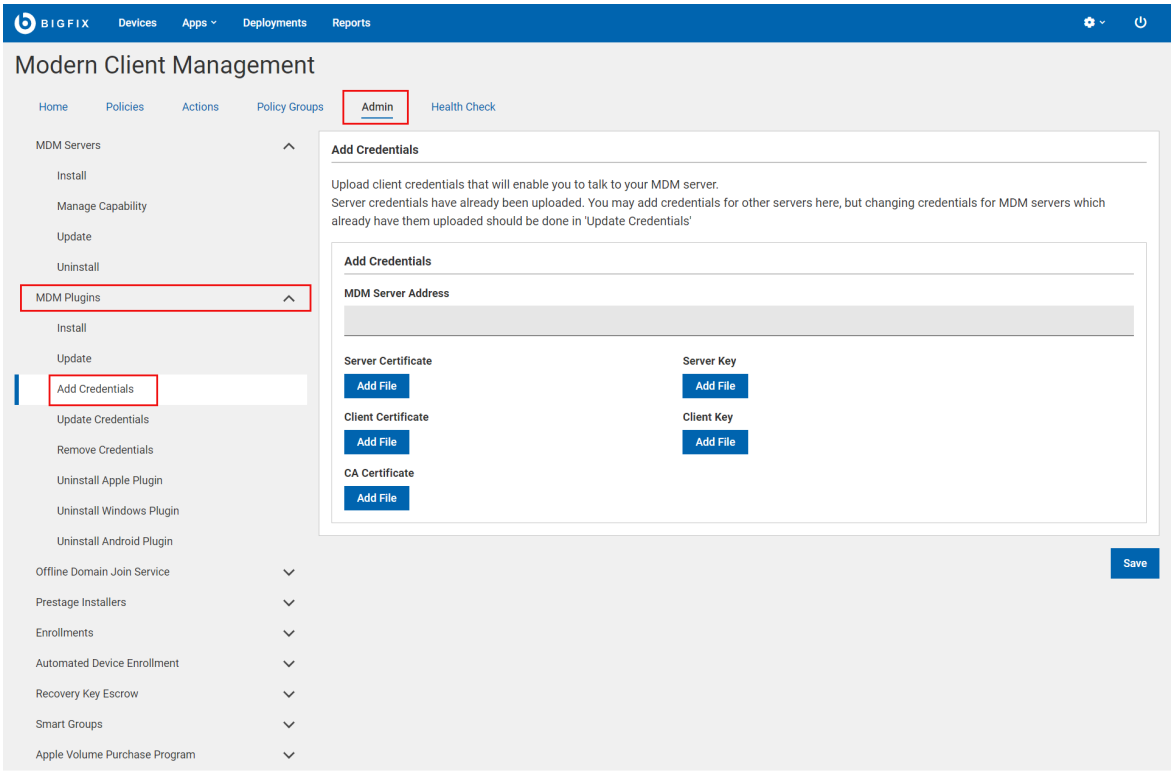
サーバーとクライアントの資格情報を追加するには、次の手順を実行します。

注:

- MCM を 2.x から 3.x にアップグレードし、WebUI と MDM サーバー間で直接接続を確立するには、BESAdmin ツール (（ページ）　　)で最初に取得して、MDM サーバーと MDM プラグインのインストール時にアップロードしたものと同じサーバー資格情報とクライアント資格情報をアップロードする必要があります。

- 初期設定に MDM サービス (Windows MDM、Android MDM、Apple MDM) を追加する場合は、新しい資格情報のみをアップロードします。
- 以前追加された既存の資格情報を更新するには、資格情報の更新 ((ページ) 304) に進みます。

1. MCM の「管理者」ページで、**「MDM プラグイン」**を展開し、**「資格情報の追加」**をクリックします。



2. **MDM サーバー・アドレス**: 資格情報を追加する MDM サーバーのアドレスを入力します。例えば、`mdmserver.deploy.bigfix.com` です。
3. アップロードする証明書またはキーの横にある**「ファイルの追加」**をクリックし、フォルダーに移動してそれぞれのファイルを選択します。

   注: 適切な証明書とキー・ファイルをアップロードします。アップロードしたファイルが一致しない場合は、エラー・メッセージが表示されます。

4. **「保存」**をクリックします。

アップロードした資格情報は WebUI に保存されます。これらの資格情報は、MDM サーバーとクライアント・アプリケーション (MDM プラグイン、WebUI) 間の通信を確立するために使用されます。

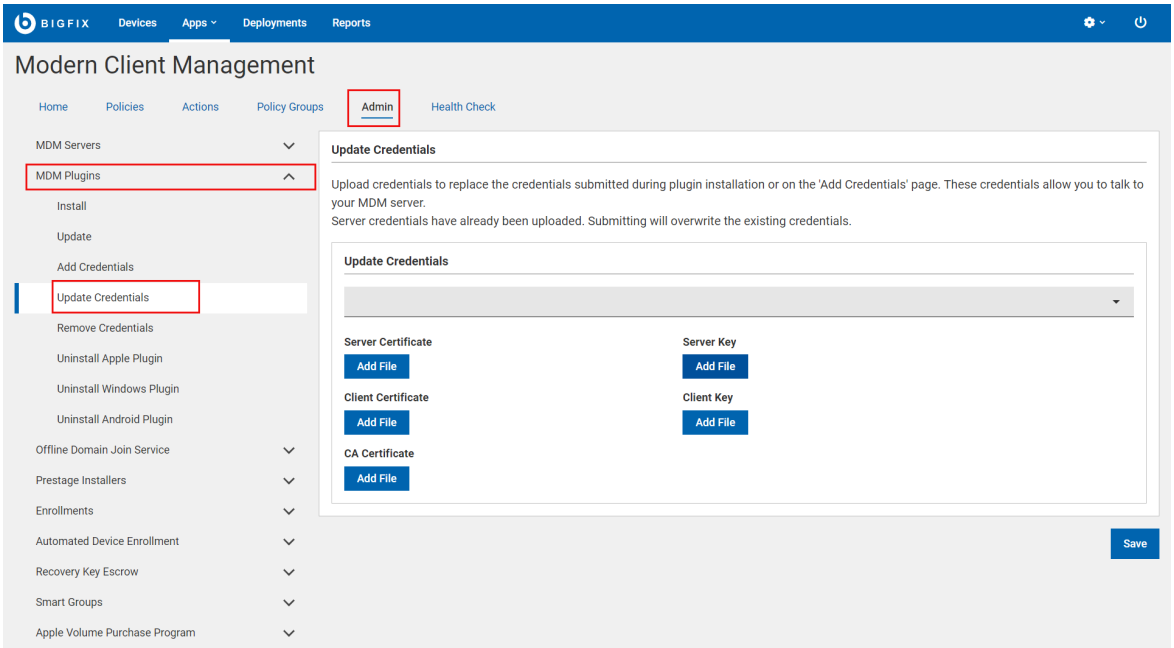
資格情報の更新

MDM サーバーの初期インストール時にアップロードしたサーバーとクライアントの資格情報、および後から「資格情報の追加」ページを介して追加した資格情報は置き換えることができます。

サーバーとクライアントの資格情報を更新するには、次の手順を実行します。

注: 資格情報をアップロードすると、以前アップロードした資格情報は上書きされます。

1. MCM の「管理者」ページで、**「MDM プラグイン」**を展開し、**「資格情報の更新」**をクリックします。



2. 「資格情報のアップロード」ドロップダウンには、お使いの環境内の MDM サーバーがリストされます。資格情報をアップロードする MDM サーバーを選択します。例えば、`mdmserver.deploy.bigfix.com` です。

3. アップロードする証明書またはキーの横にある**「ファイルの追加」**をクリックし、フォルダーに移動してそれぞれのファイルを選択します。

   注: 適切な証明書とキー・ファイルをアップロードします。アップロードしたファイルが一致しない場合は、エラー・メッセージが表示されます。

4. **「保存」**をクリックします。

以前アップロードした資格情報は、資格情報ストア内で、今回アップロードした資格情報に置き換わります。

注: 資格情報ストアにアップロードしても、これらの資格情報はさまざまなサーバーに自動的には再デプロイされません。

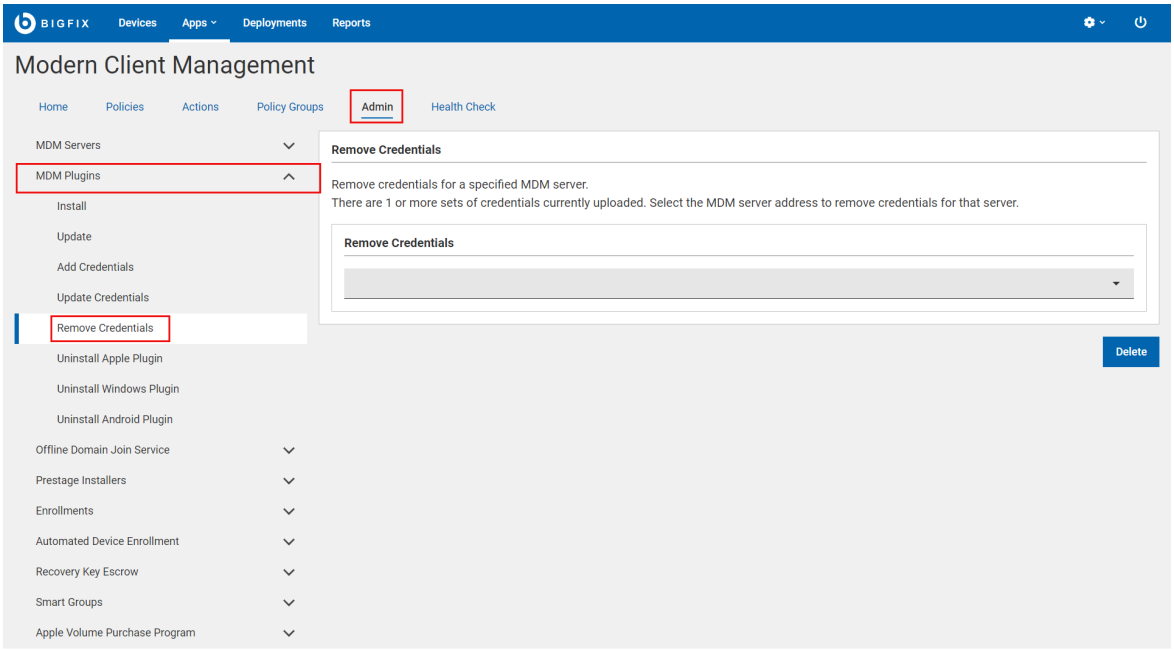
資格情報の削除

以前アップロードしたサーバーとクライアントの認証情報は、WebUI の**「資格情報の削除」**ページから削除できます。

MDM サーバーの資格情報を削除するには、次の手順を実行します。

注: 資格情報を削除すると、MDM サーバーと WebUI、MDM プラグイン、ID サービスなどの他のクライアント・アプリケーションとの通信を確立できなくなります。接続を再確立するには、資格情報を再度アップロードする必要があります。

1. MCM の「管理者」ページで、**「MDM プラグイン」**を展開し、**「資格情報の削除」**をクリックします。



2. **「資格情報の削除」**ドロップダウンから、資格情報を削除する MDM サーバーを選択します。
3. **「削除」**をクリックします。

選択した MDM サーバーのすべての資格情報が削除されます。ブラウザーを更新して、関連 MDM サーバーを「資格情報の削除」ドロップダウンから削除します。

ODJ サービスのインストールと管理

Offline Domain Join (ODJ) サービスは「アドオン」サービスであり、MDM サーバーの初期インストールの完了後に WebUI を介してインストールされます。

ODJ service、前提条件、および ODJ service インストール準備のための初期セットアップについて詳しくは、ドメイン参加のインストールと構成 (（ページ）　　) を参照してください。

ODJ service アーキテクチャと登録フローについて詳しくは、オフライン・ドメイン参加サービスを使用した Autopilot 登録 (（ページ）　　) を参照してください。

インストール

WebUI を使用して ODJ service をインストールする方法について説明します。

ODJ サービスをインストールするには、次の要件を満たす必要があります。

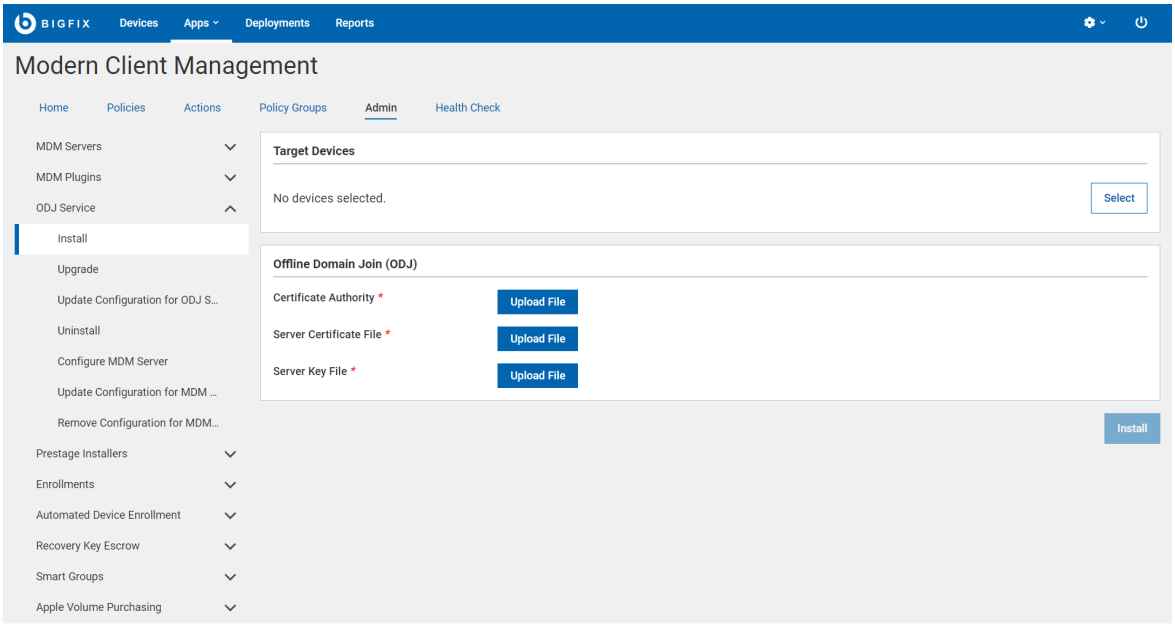
- WebUI 経由でこのタスクを実行するには、マスター・オペレーターでなければなりません。
- ODJ service をインストールする必要があるターゲットは、Windows 10 以降を実行している必要があります。
- BESclient は、ターゲットの Windows デバイスにインストールする必要があります。
- ターゲット・デバイスは Active Directory (AD) に既に接続されている必要があります。

注: 詳しくは、「ハイブリッド・ドメイン参加の前提条件 ((ページ))」を参照してください。

Windows ターゲットに ODJ service をインストールするには、次の手順を実行します。

1. WebUI のメイン・ページから、**「アプリケーション」 > 「MCM」**を選択します。
2. 「Modern Client Management」ページで、**「管理者」**をクリックします。

3. 「管理者」ページで、**「ODJ サービス」**の左側のナビゲーションから、**「インストール」**を選択しま



4. **「選択」**をクリックします。適格な Windows デバイスが一覧表示されます。ODJ service をインストールするターゲットを選択します。
5. ODJ サーバー用に作成した適切な証明書ファイルをアップロードします。「ODJ および MDM SSL 証明書とキー (（ページ）)」を参照してください。
   a. 「認証局」の場合は、**「ファイルのアップロード」**をクリックし、ファイルの場所を参照して、`ca.cert.pem` ファイルを選択します。
   b. サーバー証明書ファイルの場合は、**「ファイルのアップロード」**をクリックし、ファイルの場所を参照して、`server.cert.pem` ファイルを選択します。
   c. サーバー・キー・ファイルの場合は、**「ファイルのアップロード」**をクリックし、ファイルの場所を参照して、`server.key` ファイルを選択します。
6. **「インストール」**をクリックします。
す。

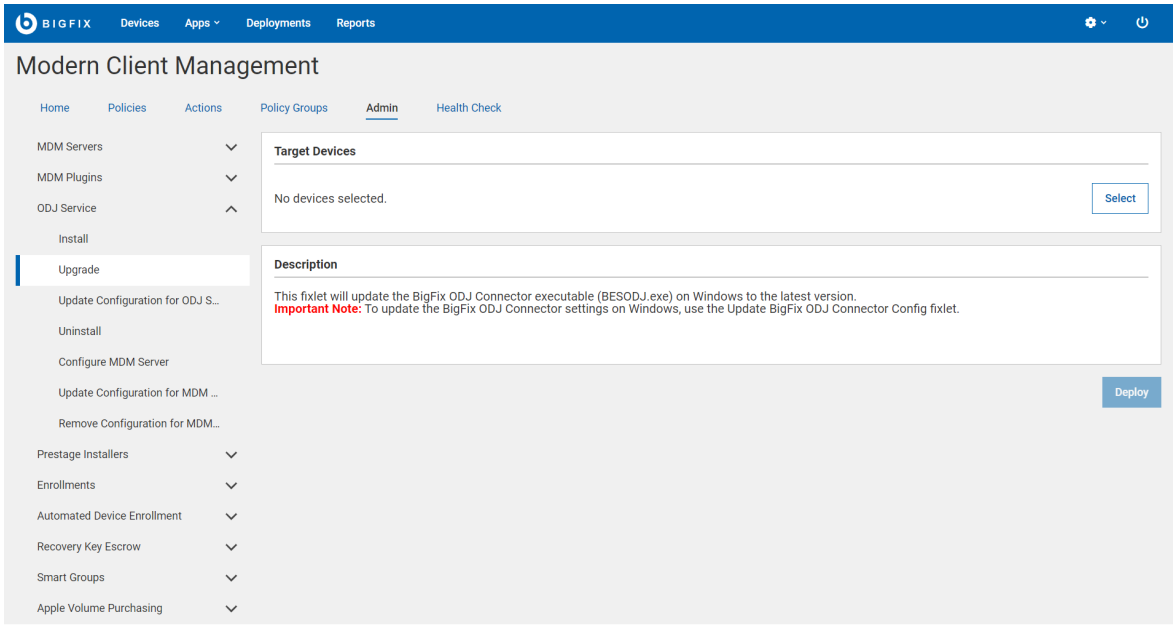
このアクションは、ターゲットの Windows マシンに ODJ service をインストールします。

アップグレード

ODJ service の新しいバージョンがリリースされたら、アップグレードが必要になります。

ODJ service を最新バージョンにアップグレードするには、次の手順を実行します。

1. WebUI のメイン・ページから、**「アプリ」 > 「MCM」**をクリックします。
2. 「Modern Client Management」ページで、**「管理者」**をクリックします。
3. 「管理者」ページの左側のナビゲーションで、「ODJ サービス」下の**「アップグレード」**をクリックします。



4. 「対象デバイス」セクションで**「選択」**をクリックします。「ターゲットの選択」ページには、古いバージョンの ODJ サービスがインストールされている Windows デバイスのリストが表示されます。ターゲットを選択し、**「OK」**をクリックします。
5. 選択したターゲットの数を確認し、**「デプロイ」**をクリックします。

このアクションは、ODJ serviceを入手可能な最新バージョンに更新します。

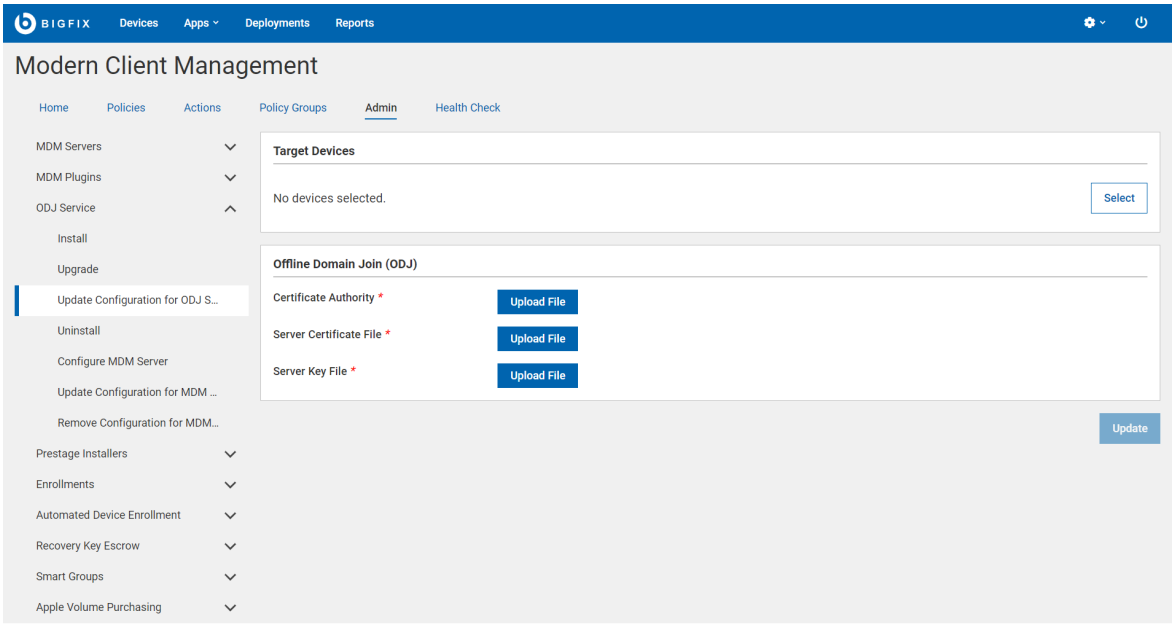
ODJ サービスの構成の更新

ODJ サービスを更新する方法について説明します。

ODJ サーバー証明書を置き換える場合は、ODJ の構成を更新することで、その証明書を置き換えることができます。これを行うには、次の手順を実行します。

1. WebUI のメイン・ページから、**「アプリ」 > 「MCM」**を選択します
2. 「Modern Client Management」ページで、**「管理者」**をクリックします。

3. 「管理者」ページで、**「ODJ サービス」**の左側のナビゲーションから、**「ODJ サービスの構成の更新」**を選択しま



4. **「選択」**をクリックして、ODJ サービスがインストール済みで更新が必要なターゲット Windows マシンを選択します。
5. ODJ サーバー用に作成した適切な証明書ファイルをアップロードします。「ODJ および MDM SSL 証明書とキー (（ページ）)」を参照してください。
   a. 「認証局」の場合は、**「ファイルのアップロード」**をクリックし、ファイルの場所を参照して、`ca.cert.pem` ファイルを選択します。
   b. サーバー証明書ファイルの場合は、**「ファイルのアップロード」**をクリックし、ファイルの場所を参照して、`server.cert.pem` ファイルを選択します。
   c. サーバー・キーの場合は、**「ファイルのアップロード」**をクリックし、ファイルの場所を参照して、`server.key` ファイルを選択します。
6. **「更新」**をクリックします。
す。

このアクションにより、選択した Windows マシンの ODJ サービスが更新されます。

アンインストール

ODJ service をアンインストールする方法について説明します。

WebUI 経由でこのタスクを実行するには、マスター・オペレーターでなければなりません。

ODJ service をアンインストールすると、ターゲットの Windows マシンからサービスが削除されます。削除されたターゲット・マシンから ODJ service を使用することはできなくなります。

ODJ service をアンインストールするには、次の手順を実行します。

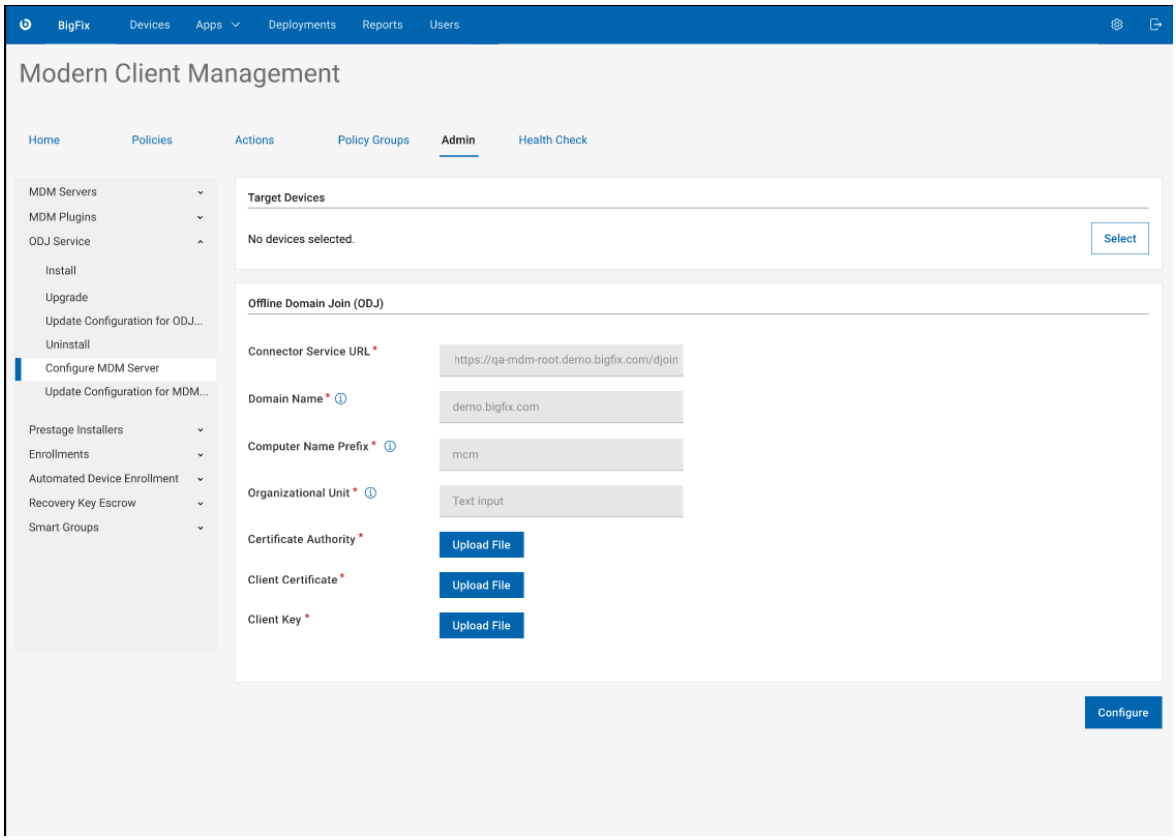
1. WebUI のメイン・ページから、**「アプリ」 > 「MCM」**をクリックします。
2. 「Modern Client Management」ページで、**「管理者」**をクリックします。
3. 「管理者」ページの左側のナビゲーションで、「ODJ サービス」下の**「アンインストール」**をクリックします。
4. 「対象デバイス」セクションで**「選択」**をクリックして、ODJ サービスを削除する 1 台以上の Windows マシンをターゲットにします。
5. **「デプロイ」**をクリックします。

選択したターゲット・マシンから ODJ サービスがアンインストールされます。ODJ service をアンインストールすると復旧する方法はありません。Autopilot が登録された Windows デバイスを再度 Active Directory に参加させるには、ODJ サービスを再インストールする必要があります。

ODJ サービス用の MDM サーバーの構成

ODJ サービスを利用するように MDM サーバーを構成する方法を説明します。

1. 「MCM 管理者」ページで、**「ODJ サービス」**の左側のナビゲーションから、**「MDM サーバーの構成」**を選択しま



2. **「選択」**をクリックして、MDM サーバーを選択します。
3. 「Offline Domain Join (ODJ)」セクションで、次の手順を実行します。
   - **コネクター・サービス URL**: URL を https://<ODJ_connector_host>/djoin の形式で指定します

     この場合、<ODJ_connector_host> は ODJ サービスをホストするサーバーのホスト名または IP アドレスです。

     例: https://172.xx.xxx.xxx/djoin、https://odj.example.com/djoin。
   - **ドメイン名**: コンピューターが参加する Active Directory (AD) ドメインの完全修飾ドメイン名 (FQDN) を指定します。
   - **コンピューター名の接頭部**: コンピューター名に適切な接頭部を指定します。コンピューター名の長さは 15 文字です。接頭部の後にランダムな文字が自動的に追加され、15 文字のコンピューター名が生成されます。

す。

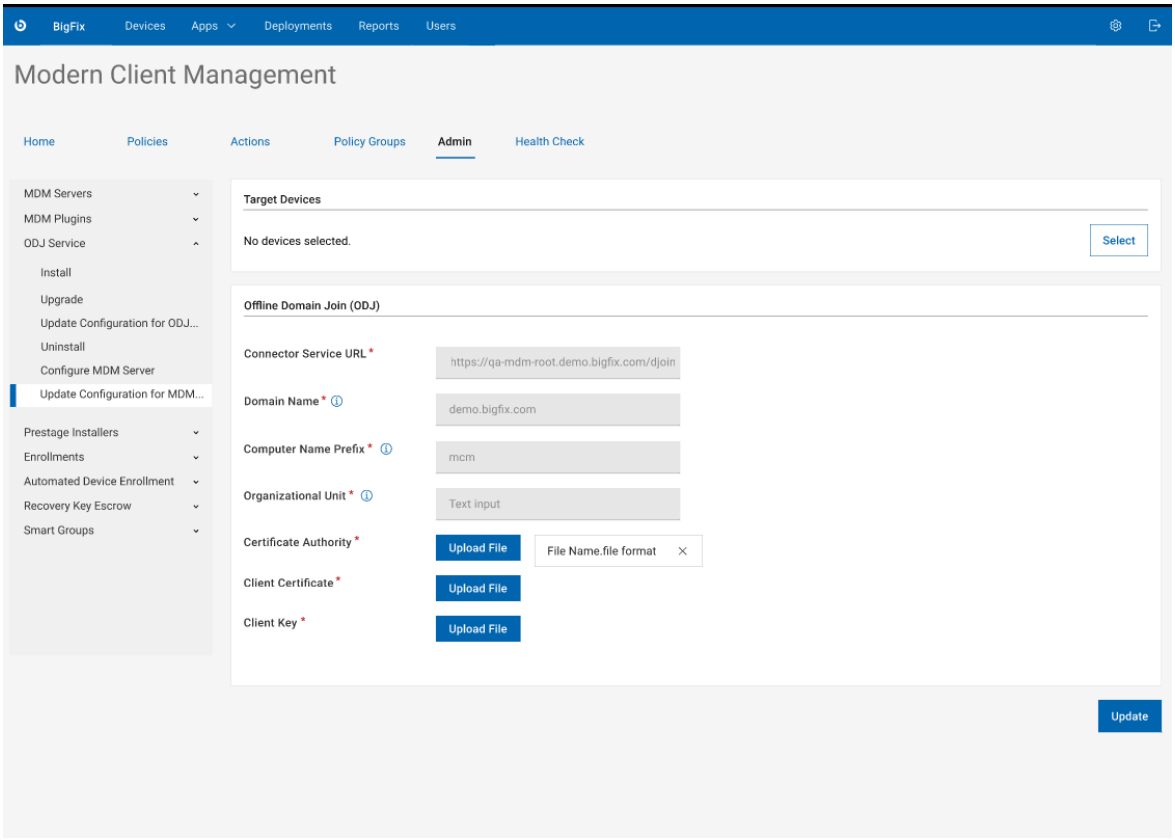
- **組織単位:** コンピューター・アカウントを作成する必要がある組織単位 (OU) の識別名を指定します。指定していない場合は、Active Directory ドメインのデフォルト OU が使用されます。
- ODJ サーバー用に作成した適切な証明書ファイルをアップロードします。「ODJ および MDM SSL 証明書とキー (（ページ）　　)」を参照してください。
  - **認証局**: **「ファイルのアップロード」**をクリックし、`ca.cert.pem` ファイルを選択します。
  - **クライアント証明書**: **「ファイルのアップロード」**をクリックし、`client.cert.pem` ファイルを選択します。
  - **クライアント・キー**: **「ファイルのアップロード」**をクリックし、`client.key` ファイルを選択します。

4. **「構成」**をクリックします。

MDM サーバーの構成の更新

MDM サーバーで以前に実行した ODJ 構成を変更して、構成を更新できます。

1. 「MCM 管理者」ページで、**「ODJ サービス」**の左側のナビゲーションから、**「MDM サーバーの構成」**を選択しま



2. **「選択」**をクリックして、MDM サーバーを選択します。
3. 「Offline Domain Join (ODJ)」セクションで、次の手順を実行します。
   - **コネクター・サービス URL**: URL を https://<ODJ_connector_host>/djoin の形式で指定します

     この場合、<ODJ_connector_host> は ODJ サービスをホストするサーバーのホスト名または IP アドレスです。

     例: https://172.xx.xxx.xxx/djoin、https://odj.example.com/djoin。
   - **ドメイン名**: コンピューターが参加する Active Directory (AD) ドメインの完全修飾ドメイン名 (FQDN) を指定します。
   - **コンピューター名の接頭部**: コンピューター名に適切な接頭部を指定します。コンピューター名の長さは 15 文字です。接頭部の後にランダムな文字が自動的に追加され、15 文字のコンピューター名が生成されます。

す。

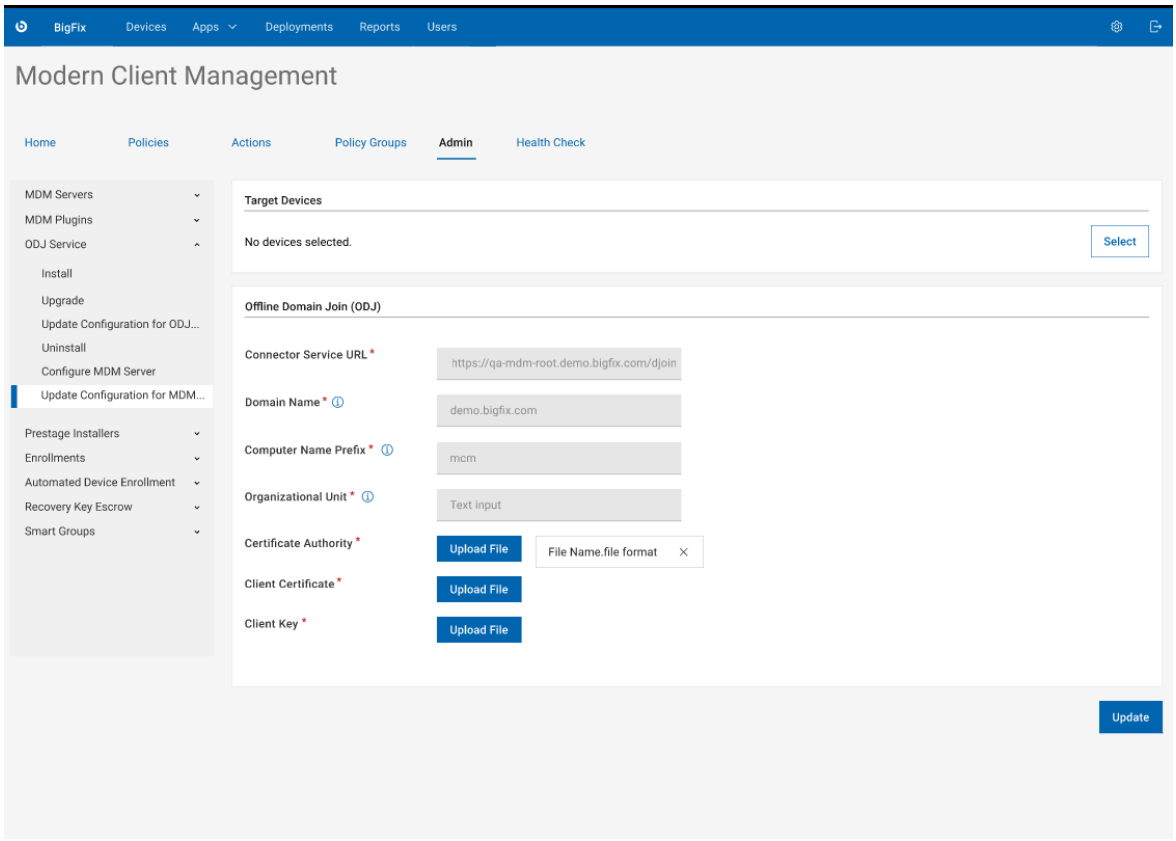
- **組織単位:** オプション。コンピューター・アカウントを作成する必要がある組織単位 (OU) の識別名を指定します。指定していない場合は、Active Directory ドメインのデフォルト OU が使用されます。
- ODJ サーバー用に作成した適切な証明書ファイルをアップロードします。「ODJ および MDM SSL 証明書とキー (（ページ）　　)」を参照してください。
  - **認証局**: **「ファイルのアップロード」**をクリックし、`ca.cert.pem` ファイルを選択します。
  - **クライアント証明書**: **「ファイルのアップロード」**をクリックし、`client.cert.pem` ファイルを選択します。
  - **クライアント・キー**: **「ファイルのアップロード」**をクリックし、`client.key` ファイルを選択します。

4. **「更新」**をクリックします。

MDM サーバーの構成の削除

MDM サーバーから ODJ 構成を削除できます。

1. 「MCM 管理者」ページで、**「ODJ サービス」**の左側のナビゲーションから、**「MDM サーバーの構成」**を選択しま



2. **「選択」**をクリックして、MDM サーバーを選択します。
3. 「Offline Domain Join (ODJ)」セクションで、次の手順を実行します。
   - **コネクター・サービス URL**: URL を https://<ODJ_connector_host>/djoin の形式で指定します

     この場合、<ODJ_connector_host> は ODJ サービスをホストするサーバーのホスト名または IP アドレスです。

     例: https://172.xx.xxx.xxx/djoin、https://odj.example.com/djoin。
   - **ドメイン名**: コンピューターが参加する Active Directory (AD) ドメインの完全修飾ドメイン名 (FQDN) を指定します。
   - **コンピューター名の接頭部**: コンピューター名に適切な接頭部を指定します。コンピューター名の長さは 15 文字です。接頭部の後にランダムな文字が自動的に追加され、15 文字のコンピューター名が生成されます。

す。

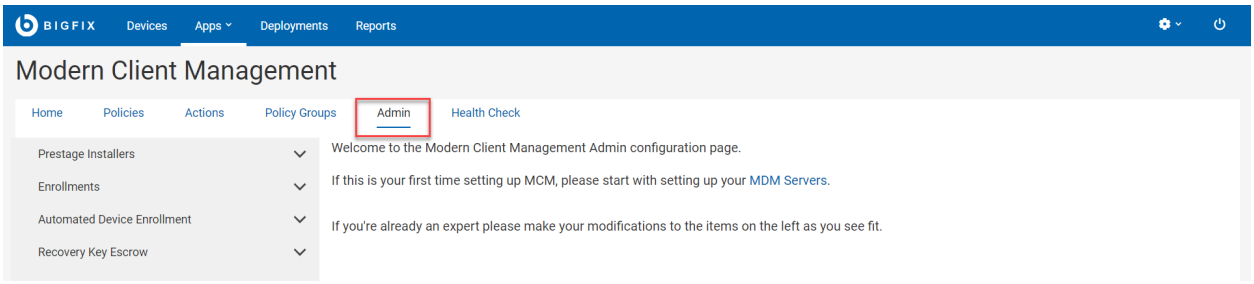
- **組織単位:** オプション。コンピューター・アカウントを作成する必要がある組織単位 (OU) の識別名を指定します。指定していない場合は、Active Directory ドメインのデフォルト OU が使用されます。
- ODJ サーバー用に作成した適切な証明書ファイルをアップロードします。「ODJ および MDM SSL 証明書とキー ((ページ))」を参照してください。
  - **認証局**: **「ファイルのアップロード」**をクリックし、`ca.cert.pem` ファイルを選択します。
  - **クライアント証明書**: **「ファイルのアップロード」**をクリックし、`client.cert.pem` ファイルを選択します。
  - **クライアント・キー**: **「ファイルのアップロード」**をクリックし、`client.key` ファイルを選択します。

4. **「更新」**をクリックします。

BigFix MCM および BigFix モバイルの構成

MCM コンポーネントをセットアップした後に追加の構成オプションを設定することにより、Windows の一括登録、macOS 用の DEP ポリシー、Windows エンドポイントおよび MacOS MDM エンドポイント用の事前ステージ・インストーラーなどの機能を有効にすることができます。

MCM を構成するには、WebUI メイン・ページから**「アプリ」 > 「MCM」**をクリックし、「最新のクライアント管理」ページで**「管理者」**を選択します。



オペレーティング・システムと登録タイプに応じて、構成オプションを表示し、以下のような構成タスクを実行します。

- macOS BigFix インストーラーの事前ステージ (（ページ） *355)*
- Windows BigFix インストーラーの事前ステージ (（ページ） *357)*
- Windows プロビジョニング・パッケージの作成 (（ページ） *337)*
- プロビジョニング・パッケージ生成ポイントの指定 (（ページ） *336)*
- Windows Autopilot のサービス利用条件の構成 (（ページ） *350)*
- 暗号化リカバリー・キー・エスクロー証明書の生成 (（ページ） *372)*
- Recovery Key Escrow プラグインのセットアップ (（ページ） *373)*
- 自動デバイス登録ポリシーの管理 (（ページ） *353)*

スマート・グループ

スマート・グループは、Active Directory グループ、ユーザー属性、およびデバイス属性に基づいて作成および管理される動的ユーザー・グループです。スマート・グループのメンバーは、管理者が手動で定義するのではなく、WebUI で動的に定義されます。ユーザーまたはデバイスが登録されているスマート・グループを使用して複数のデバイスをターゲットに設定し、アプリ、デバイス・アクセス、グループ・メンバーシップなどを管理できます。

利点

スマート・グループは、ユーザーベースの登録とデバイスのターゲット設定により、MDM 登録デバイスのスケーラブルな管理を促進します。スマート・グループを使用すると、IT 管理者は次のようなさまざまな方法でデバイスを管理できます。

スマート・グループはユーザー属性 (（ページ） 319)とデバイス属性 (（ページ） 320)に基づいてリソースへのアクセス権限を提供するために、効果的なアクセス制御システムとしても使用できます。例えば、iOS のスマートフォンを使用して、「米国」にある「エンジニアリング」部門に所属するすべてのユーザーが含まれているスマート・グループを作成し、米国に準拠した iOS のスマートフォンに適用される特定のエンジニアリング関連リソースへのアクセス権を付与できます。

スマート・グループを使用すると、ユーザーおよび属性データを保存できるユーザーを管理できます。

User の属性

ユーザー属性は、Microsoft Active Directory や LDAP (Lightweight Directory Access Protocol) ディレクトリーなど、組織のディレクトリー・サービスで管理対象情報に基づいて、エンド・ユーザーを一意に識別するのに役立ちます。ユーザー属性には、任意の英数字 ID、電子メール ID、またはさまざまなユーザー間で共有される共通属性を含めることができます。これらのユーザー属性により、認証、許可、および情報の取得が容易になります。ユーザー属性の例は次のとおりです。

- ID 情報: ユーザー名、メール・アドレス、ユーザー ID 番号、役職、部署、または場所
- アクセス資格情報: パスワード、セキュリティーに関する質問/回答、認証トークン
- 許可: アクセス権、役割、および責任

ディレクトリー・サービスに基づいて、ユーザー属性を定義し (（ページ） *324*)、スマート・グループに関連付けることができます。これにより、デバイスのグループを効率的にフィルタリングしてターゲットを設定し、次の方法で一貫して管理できます。

- アクセス制御: デバイスを特定のユーザーに関連付けることで、組織は特定のリソース、システム、またはデータに対してアクセス権を持つユーザーを制御できます。
- セキュリティー: 管理者は、ユーザーの役割に基づいてセキュリティー・ポリシーを設定でき、権限を付与された個人のみが機密情報にアクセスできるようになります。
- デバイスの構成: ユーザー属性を使用して、個々のニーズに基づいてデバイスの構成を調整できます。これにより、ユーザーは各自の役割に必要なツールと設定を確実に使用できます。
- ユーザー・エクスペリエンス: ユーザー属性に基づいてデバイスを管理することで、パーソナライズされたユーザー・エクスペリエンスを実現できます。ユーザーは、各自の役割と責任に合わせて、カスタマイズ済み設定、アプリケーション、およびアクセス権限を持つことができます。
- ポリシーの適用: デバイスを特定のユーザーに関連付けることで、IT ポリシーをより効果的に適用します。これには、ソフトウェアのインストール、更新、アンチウイルス保護、およびその他のセキュリティー対策に関連するポリシーが含まれます。

- リモート・デバイス管理: IT 管理者は、デバイスが特定のユーザーに関連付けられている場合、問題のリモート・トラブルシューティング、更新のデプロイ、およびメンテナンス・タスクの効率化を行うことができます。
- ID 管理: 適切な個人が適切なリソースにアクセスできるようにすることで、安全で効率的な IT 環境を促進します。
- 組織の変化への適応性: ユーザーが役割を変更したり、組織から脱退したりする場合、ユーザー属性に基づいてデバイスを管理することで、シームレスな移行が可能になります。デバイスのアクセスと構成は、ユーザーの状況と責任の変化を反映するよう調整できます。

- 特定のデバイス・セットに対して、パスコード・ポリシー、制限ポリシー、証明書ポリシーなどのカスタマイズされたポリシーをデプロイします。
- 特定のデバイス・セットに応じて、ロック、ワイプなどのカスタマイズ済みアクションをトリガーします。

デバイス属性

デバイス属性とは、MDM 登録デバイスに関連付けられたさまざまな特性と情報のことを指します。これらの属性には、ハードウェアの仕様、オペレーティング・システムの詳細、ネットワークの構成、およびその他の関連情報が含まれます。

MDM サーバーは、次の方法でデバイス情報を収集および更新します。

- デバイス登録: 登録プロセス中、MDM サーバーはデバイス・タイプ、モデル、シリアル番号、ハードウェア仕様などの基本的なデバイス情報を収集します。
- BigFix エージェントのインストール: BigFix エージェントは、デバイスに関する情報を収集して BigFix に送信します。
- デバイス照会: MDM サーバーは、現在の場所、インストール済みアプリケーション、またはセキュリティー設定に関する詳細をデバイスに送信する場合があります。
- プラットフォーム固有の API: MDM サーバーは、オペレーティング・システムが提供するプラットフォーム固有の API を使用して、デバイス情報を取得します。例えば、iOS デバイスでは、MDM サーバーは Apple の MDM プロトコルと API を使用してデバイスに関する情報を収集できます。

- ネットワーク通信: デバイスは、更新、ポリシー、およびその他の指示について、MDM サーバーと定期的に通信します。このような通信中、MDM サーバーはデバイスに関する情報を要求して受信できます。
- ユーザーの入力: 一部の属性には、ユーザーの入力または権限が必要な場合があります例えば、デバイスの場所を取得するには、ユーザーが位置情報へのアクセスを許可する必要がある場合があります。
- デバイスの更新: デバイス情報は、デバイスが更新されると更新されます。

これらのデバイス属性を関連付けることで、スマート・グループを作成して、特定の属性を持つデバイスのグループを一貫して構成および管理できます。これにより、ポリシーの効率的な実装、セキュリティー対策の実施、デバイス管理の合理化を、それぞれの独自の特性に基づいて実現できます。次に、スマート・グループ内のデバイス属性を関連付けてデバイス・グループを管理する例を示します。

- セキュリティー・ポリシー: スマート・グループは、デバイス・モデルとオペレーティング・システムのバージョンに基づいて定義でき、パスコード要件、暗号化設定、その他の認証ポリシーなどのセキュリティー構成をプッシュできます。
- アプリケーション管理: オペレーティング・システムと使用可能なストレージに基づいてスマート・グループを定義し、特定のアプリケーションをデバイスにプッシュしたり、互換性と組織ポリシーに基づいて特定のアプリケーションのインストールを制限したりできます。
- ネットワーク構成: ネットワーク接続に関連するデバイス属性に基づいて、Wi-Fi ポリシーをプッシュして、デバイスが承認されたネットワークに接続し、組織固有のネットワーク・ポリシーに従うようにすることができます。
- 電子メールおよび通信ポリシー: デバイス属性を使用して、電子メールと通信の設定を構成できます。これには、企業のメール・アカウントの設定と管理、VPN 構成、およびデバイス・タイプとオペレーティング・システムに基づいた通信制限の定義が含まれます。
- 更新: デバイス・タイプ、モデル、OS バージョン、ハードウェア仕様などのデバイスのインベントリーの詳細に基づき、更新を管理し、ハードウェアのアップグレードを計画できます。

- リモート・ワイプおよびロック: デバイスの紛失や盗難時、または従業員が退職した場合は、デバイス属性を使用してデバイスをリモートでワイプまたはロックできます。
- 位置ベースのポリシー: デバイスの場所に基づいて、異なるセキュリティー設定を構成できます (例: 社内と社外のセキュリティー設定を比較する場合など)。
- コンプライアンス・チェック: デバイスのコンプライアンス違反 (古い OS バージョン、セキュリティー設定が満たされていないなど) をモニターし、必要な構成を適用することで問題を自動的に修復できます。
- カスタム構成: デバイス属性に基づいてカスタム構成を作成し、組織のニーズや業界の規制に従って管理アプローチを調整できます。

ベスト・プラクティス

スマート・グループを作成するときは、次の点を検討してください。

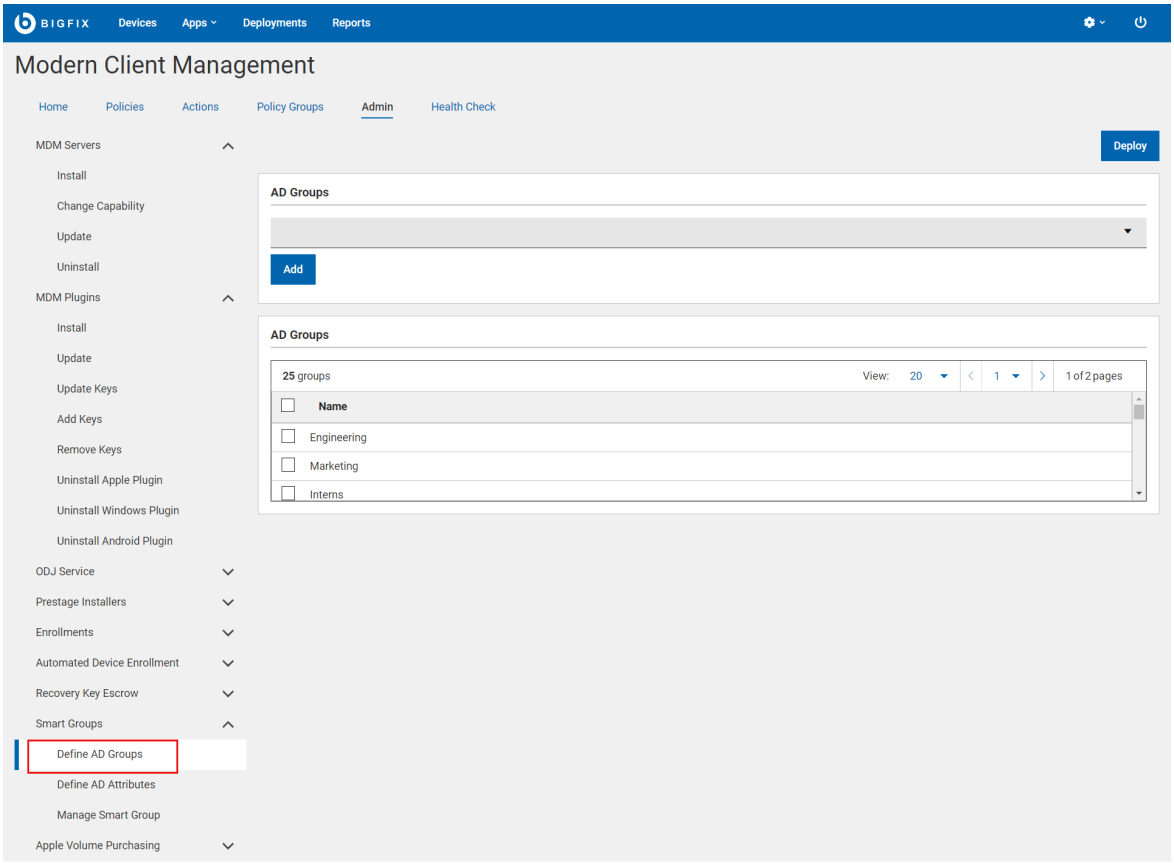
- スマート・グループを作成して、特定のポリシー・グループと関連付けられた構成に一致するために、新しい登録によって満たす必要があるユーザーまたはデバイスの条件を定義します。
- スマート・グループ名:
    - スマート・グループで定義された条件セットを反映する必要があります。
    - スマート・グループに特定のデバイスまたは特定の OS 条件を識別するデバイス条件が含まれていない限り、特定のデバイス・タイプを参照しないようにしてください。
    - スマート・グループ内で定義されていないアプリケーションやポリシーを参照しないようにしてください。
- 同じスマート・グループを任意の数のポリシー・グループに適用できます。

グループの定義

WebUI の Active Directory からユーザー・グループのサブセットを追加できます。ここで追加したグループはスマート・グループに関連付けることができ、定義したグループ名でデバイスをターゲットにすることができます。

グループ名を定義するには、以下の手順を実行します。

1. MCM の**「管理者」**ページで**「スマート・グループ」**を展開し、**「グループの定義」**をクリックします。



2. **「AD グループ」**ドロップダウン・メニューには、Active Directory のマスター・リストに含まれているグループ名がリストされます。1 つ以上のユーザー・グループを選択します。

> **注:** 検索ボックスに入力すると、これまでに入力した文字や単語に基づいて、候補またはオートコンプリート・オプションが表示されます。

3. **「追加」**をクリックします。ユーザー・グループがグリッドに追加されます。

> **注:** 最大で 64 グループまで追加できます。定義したグループのいずれかを削除すると、実際のワーキング・セットは `64 - n` 個のグループ (`n` は削除したグループの数) になります。

4. **「デプロイ」**をクリックして、グリッドに追加したすべてのユーザー・グループを MDM サーバーにデプロイします。

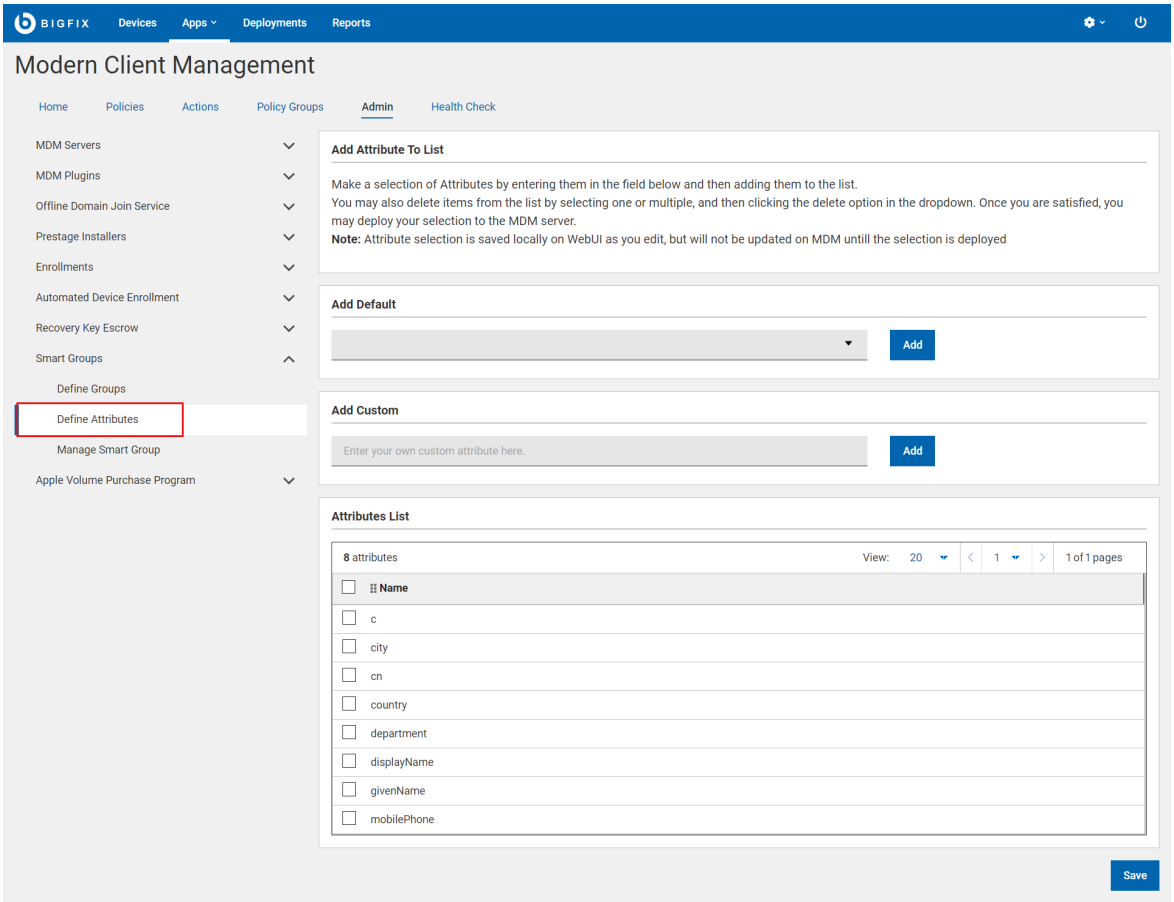
   グリッドのグループを削除してから MDM サーバーにデプロイする場合は、削除するユーザー・グループを 1 つ以上選択し、青色のアクション・バーから**「削除」**を選択します。

属性の定義

WebUI で属性を定義し、それらの属性を定義した属性ごとにターゲット・デバイスに含めることができます。

属性を定義するには、以下のステップを実行します。

1. MCM の**「管理者」**ページで**「スマート・グループ」**を展開し、**「属性の定義」**をクリックします。



2. **「デフォルトの追加」**: このドロップダウンをクリックして、サポート対象属性 (（ページ） 325)のリストを表示し、リストから属性を選択します。**「追加」**をクリックして、属性リストに追加します。

   または

   「カスタムの追加」: 文字列を入力して**「追加」**をクリックし、属性リストにカスタム属性を追加します。
3. **「保存」**をクリックして、グリッドに追加したすべての属性を MDM サーバーにデプロイします。

   グリッドの属性を削除してから MDM サーバーにデプロイする場合は、削除する属性を選択し、青色のアクション・バーから**「削除」**を選択します。

サポート対象ユーザーおよびデバイスの属性

このセクションでは、WebUI での スマート・グループ (（ページ） 318) 作成時にサポートされるユーザーおよびデバイスの属性について説明します。

デフォルト・ユーザー属性

次の表に Active Directory (AD) および Azure Active Directory (AAD) の WebUI でサポートされているデフォルトのユーザー属性 (（ページ） 319)のリストを示します。

サポート対象属性	定義	ディレクトリー・サービス
c	ユーザーの国情報を保持します。	Active Directory
cn	共通名は、ユーザーの氏名または表示名です。通常は、ユーザーを人間が読み取り可能な形式で識別するために使用されます。	Active Directory
department	ユーザーが所属する部署の名前が含まれます。	Active Directory/

サポート対象属性	定義	ディレクトリー・サービス
		Azure Active Directory
表示名	これはユーザーの表示名で、多くの場合「名姓」の形式で表示されます。	Active Directory/ Azure Active Directory
givenName	この属性には、ユーザーの名 (下の名前) が保存されます。	Active Directory/ Azure Active Directory
city	ユーザーの市区町村の名前を保持します。	Active Directory
mobilePhone	この属性には、ユーザーの携帯電話番号が保存されます。	Active Directory/ Azure Active Directory
userPrincipalName	UPN は、ユーザーのユーザー名とドメイン名で構成される代替ユーザー識別子です (例: username@domain.com)。多くの場合、ユーザー認証に使用されます。	Active Directory/ Azure Active Directory
surname	姓。ユーザーの姓 (苗字) が保存されます。	Active Directory/ Azure Active Directory
状態	ユーザーの都道府県の名前を保持します。	Active Directory/

サポート対象属性	定義	ディレクトリー・サービス
		Azure Active Directory
country	ユーザーが所在する国/地域。例: 「US」または「UK」。最大長 128。	Azure Active Directory
usageLocation	国/地域でのサービスの可用性を確認するための法的要件により、ライセンスが割り当てられるユーザーに必要です。NULL 非許容。2 文字の国/地域コード (ISO 規格3166)。例: 「US」、「JP」、および「GB」。	Azure Active Directory

カスタム・ユーザー属性

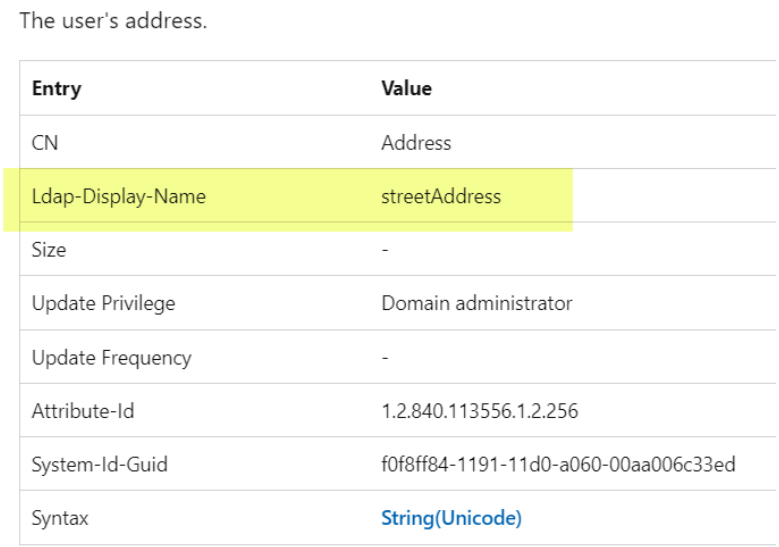
カスタム・ユーザー属性を使用すると、ユーザー・アカウントに関連付けられているデフォルトの属性セットを拡張できます。これは、デフォルト属性でカバーされていないユーザーに関する追加情報を保存する必要がある場合に便利です。カスタム・ユーザー属性を作成および管理する方法について説明します。

注:

- WebUI では**「カスタム追加」**テキスト・ボックスに入力したデータは制限も検証もされません。ディレクトリー・サービスとまったく同じスペルと形式の適切なカスタム属性を追加してください。
- WebUI では、Active Directory または Azure Active Directory で定義された標準以外のディレクトリー・サービスで定義されたカスタム属性を追加することもできます。

Active Directory

- Active Directory で定義されている属性のリストは、https://learn.microsoft.com/en-us/windows/win32/adschema/attributes-all で確認できます。
- カスタム属性を追加する場合は、属性の *Ldap-Display-Name* を入力します。例えば、ユーザー属性「Address」を追加する場合は、「カスタム追加」テキスト・ボックスに「streetAddress」と入力し、「追加」をクリックします。



The user's address.

Entry	Value
CN	Address
Ldap-Display-Name	streetAddress
Size	-
Update Privilege	Domain administrator
Update Frequency	-
Attribute-Id	1.2.840.113556.1.2.256
System-Id-Guid	f0f8ff84-1191-11d0-a060-00aa006c33ed
Syntax	String(Unicode)

Azure Active Directory

Azure Active Directory で定義されているユーザー属性のリストは、https://learn.microsoft.com/en-us/azure/active-directory-b2c/user-profile-attributes で確認できます。

デフォルト・デバイス属性

次の表に、WebUI でサポートされているデフォルトのデバイス属性 (（ページ） *320)*のリストを示します。

サポート対象属性	定義
deviceManufacturer	デバイスを設計および製造した会社の名称。例: Dell、HP、Lenovo、Apple。
deviceModel	デバイスの正確なモデル名または番号。例: iPhone 13 Pro、Lenovo ThinkPad X1 Carbon
deviceOSType	デバイスにインストールされているオペレーティング・システム (OS) のタイプまたはカテゴリー。例: Windows、macOS、Android、iOS
deviceOSVersion	デバイスにインストールされているオペレーティング・システムの特定のバージョンまたはリリース。例: iOS 15.1、Android 12
deviceOwnership	デバイスが個人または組織によって所有されているかどうかを示すデバイスの所有権状況
表示名	デバイスの識別に、通常使用される名前またはラベルを表します
serialNumber	デバイスの一意の識別番号またはコード

スマート・グループの管理

このセクションでは、スマート・グループを作成、編集、削除する方法について説明します。

- スマート・グループの作成 (（ページ） *329)*
- スマート・グループの編集 (（ページ） *332)*
- スマート・グループの削除 (（ページ） *334)*

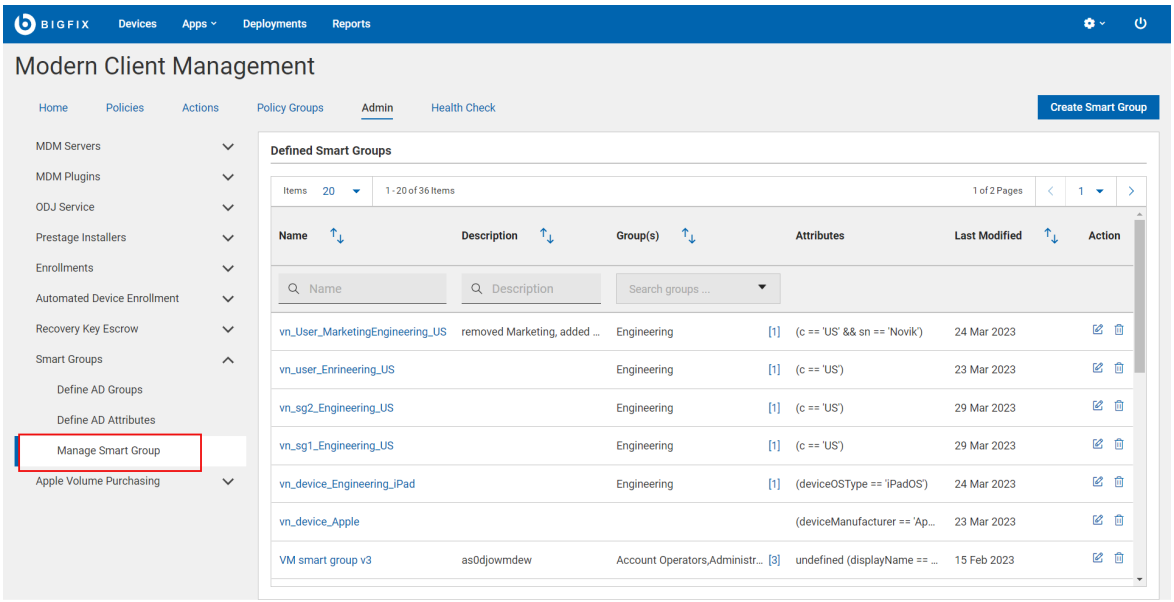
スマート・グループの作成

このトピックでは、スマート・グループの作成方法について説明します。

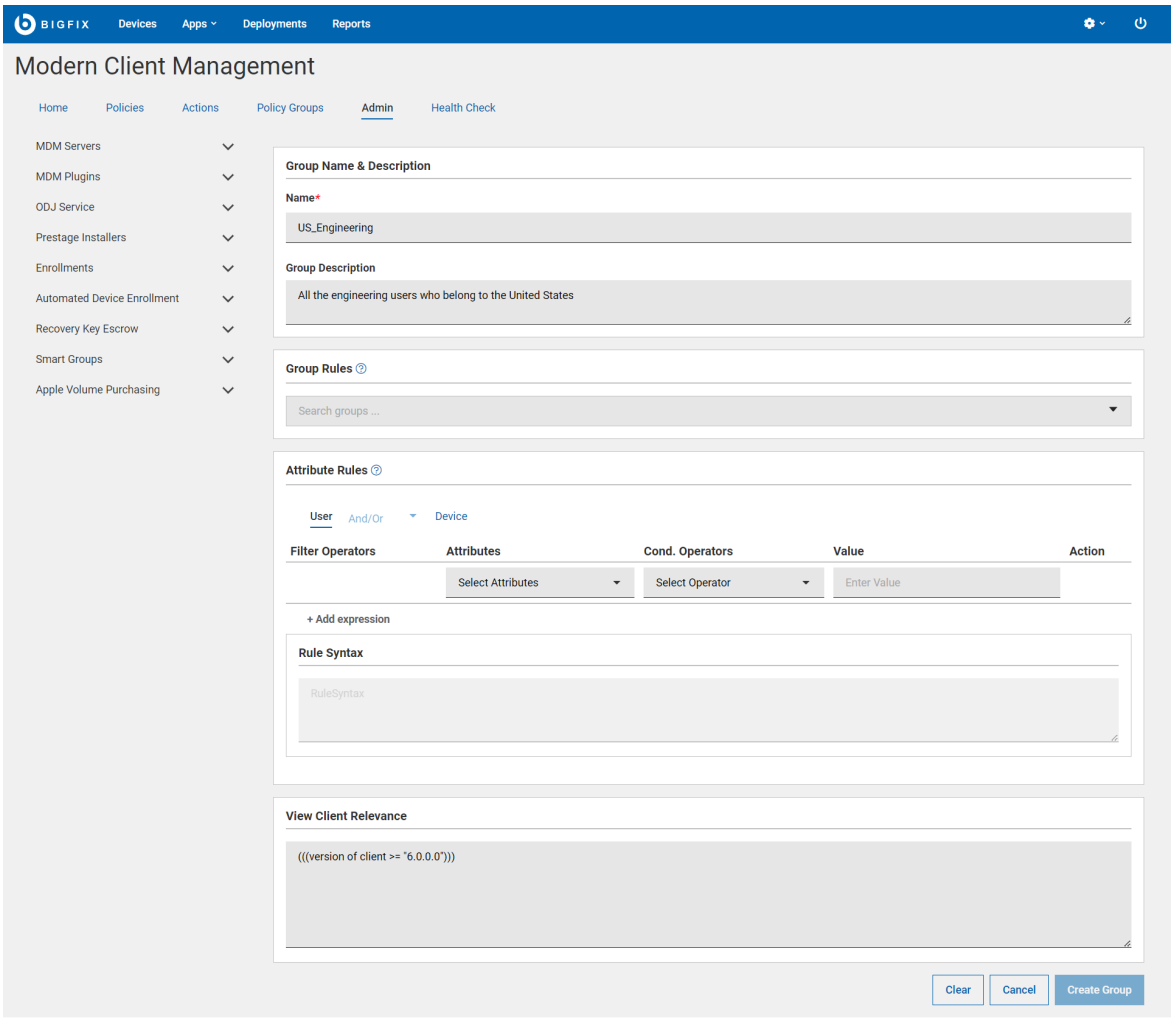
AD グループ (（ページ） *322)*と AD 属性 (（ページ） *324)*が定義済みであり、スマート・グループに関連付けることができることを確認します。

スマート・グループを作成するには、以下の手順を実行します。

1. MCM の**「管理者」**ページで**「スマート・グループ」**を展開し、**「スマート・グループの管理」**をクリックします。



2. 右上隅にある**「スマート・グループの作成」**をクリックします。
3. 次のページの**「グループ名と説明」**に次の項目を定義します。



- **名前**: これは必須フィールドです。スマート・グループの名前を入力します。
- **グループの説明**: スマート・グループの分かりやすい説明を入力します。
- **グループ・ルール**: ドロップダウンには、グループの定義 (（ページ） 322) ページで定義した最大 64 個のグループがリストされます。1 つ以上のグループを選択して、グループ・ルールを定義します。
  - リストからグループを 1 つ以上選択します。
  - ルールにグループを追加するには、  をクリックします。
  - ルールからグループを削除するには、選択したグループの横にある**「X」**をクリックします。
- **属性ルール**: 属性、条件演算子、値の組み合わせを使用して、1 つ以上のルールを定義できます。

ルールを追加し、関連式を作成するには:

- **「属性ルール」**セクションで、次の操作を実行します。
  - ユーザー属性ルールを定義するには、**「ユーザー」**タブを選択します。
  - **「論理積」/「論理和」**を選択して、ユーザー属性ルールとデバイス属性ルールの両方を含めるか、いずれかを含めます。

    注: 論理積と論理和は、1 つ以上のユーザー属性ルールまたはデバイス属性ルールを定義した後に有効になります。

  - デバイス属性ルールを定義するには、**「デバイス」**タブを選択します。
  - 属性、条件演算子、値を選択します。
  - 別のルールを追加するには、**「+ 式の追加」**をクリックします。

  例えば、"部門" = "エンジニアリング" により、部門がエンジニアリングのユーザーすべてが取得されます。

「クライアント関連度の表示」セクションには、ルール定義に応じて関連度ステートメントが動的に表示されます。

4. **「グループの作成」**をクリックしてスマート・グループを作成します。

該当するグループと属性を定義し、該当するデバイスをフィルタリングするスマート・グループが作成されました。

例: 米国エンジニアリング・ユーザーのみに「USENGINEERS」という名前のスマート・グループを作成し、USENGINEERS グループをターゲットとする「USENGINEERRESTRITIONS」という名前の制限ポリシーを追加した場合、米国内およびエンジニアリング・グループ内であると評価されるすべてのエンドポイントには、その特定の制限ポリシーが適用されます。

作成したスマート・グループを使用して、特定のデバイスをターゲットにすることができます。スマート・グループをポリシー・グループに関連付けて、特定のデバイス・セットにポリシーをデプロイすることもできます。

スマート・グループの編集

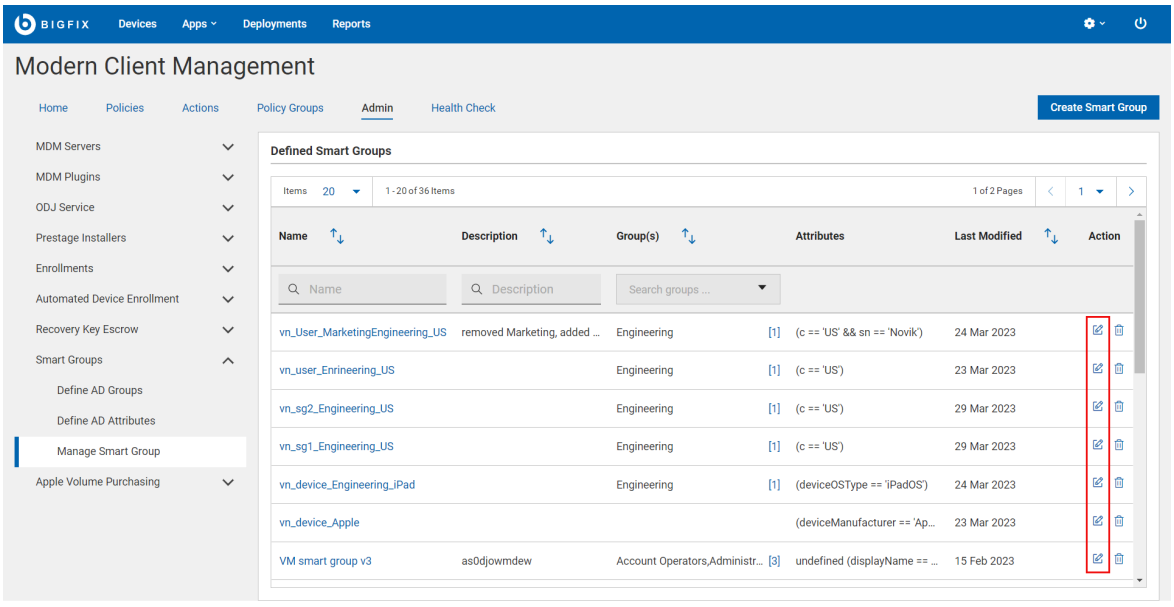
このセクションでは、作成済みスマート・グループを編集および変更する方法について説明します。

既存のスマート・グループを編集する手順は、次のとおりです。

- デバイスに割り当てられて以前関連していたポリシーまたはポリシー・グループは削除されます。
- 変更したスマート・グループのポリシーまたはポリシー・グループの割り当ては保持されます。
- ポリシーまたはポリシー・グループは、適切なポリシーが適用されたすべての関連デバイスに再適用されます。

スマート・グループを編集するには、次の手順を実行します。

1. MCM の**「管理者」**ページで**「スマート・グループ」**を展開し、**「スマート・グループの管理」**をクリックします。
2. 変更するスマート・グループの横の編集ボタンをクリックします。



3. 次の画面で、説明、グループ・ルール、属性ルールを必要に応じて変更します。クライアント関連度は、変更を加えると動的に更新されます。

注: スマート・グループ名は作成後に変更できません。

4. **「保存」**をクリックします。

スマート・グループの定義が変更され、すべてのデバイスが最新のスマート・グループの条件に基づいて再評価されます。

例:

- AWSAdmin 属性を持たないユーザーにのみポリシーを制限する属性条件を追加してスマート・グループの定義を変更し、USENGINEERS にパスコード・ポリシーをデプロイすると、AWSAdmin 属性を持たない米国エンジニアリング・ユーザーに属するデバイスにのみポリシーがデプロイされます。残りのデバイスには、このパスコード・ポリシーはデプロイされません。
- 上記の属性条件では、AWSAdmin 属性を持つ米国エンジニアのサブセットには、変更前にデプロイされた一部のポリシーが適用されなくなります。また、AWSAdmin グループに適用できない一部のポリシーは、適切なデバイスから削除されない限り、そのまま維持されます。

スマート・グループの削除

このセクションでは、スマート・グループの削除方法について説明します。

スマート・グループを削除する場合:

スマート・グループを削除するには、以下の手順を実行します。

1. MCM の**「管理者」**ページで**「スマート・グループ」**を展開し、**「スマート・グループの管理」**をクリックします。
2. 削除するスマート・グループの横の**「削除」**ボタンをクリックします。
3. 確認するには**「OK」**をクリックします。

デバイスの登録

デバイスを BigFix MCM に登録して WebUI にリストし、MDM で管理する必要があります。

BigFix MCM は、デバイスのオペレーティング・システムと組織内の要件に基づく複数の登録方法をサポートします。BigFix MCM でサポートされる、さまざまなオペレーティング・システムの登録方法については、『デバイス登録』を参照してください。

一括登録 - Windows

このセクションでは、Windows の一括登録の手順について説明します。

前提条件:

- 一括登録の対象となる Windows デバイスに BigFix agent がインストールされていることを確認します。
- BigFix コンソールから、分析 15 - `Modern Client Management Root Server Analysis` を有効にします。
- BES ルート・サーバーの `C:\Program Files (x86)\BigFix Enterprise\BES Server\Mirror Server\Config,` にある `DownloadWhitelist.txt` ファイルに、以下を追加します。

```
http://localhost.*
```

このタスクについて: 一括登録のワークフローは次のとおりです。

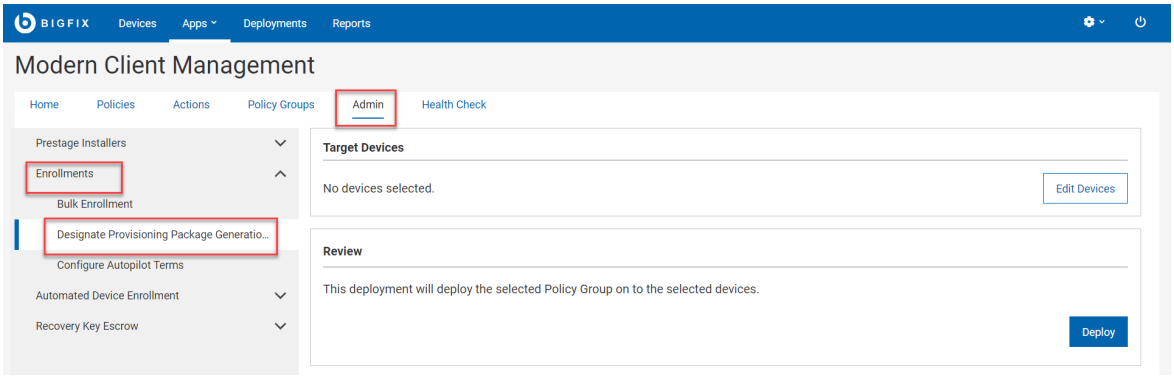
1. プロビジョニング・パッケージ生成ポイントの指定: WebUI Master operator は 1 つ以上のデバイスを指定し、Windows プロビジョニング・パッケージ (`.ppkg`) ファイルを生成します。この構成タスクは、指定された Windows エンドポイントのクライアント設定を実行して、後で MCM を登録するために使用される `.ppkg` ファイルを作成するデバイスとして指定します。
2. Windows PPKG 成果物の作成: Master operator は、ステップ 1 で指定されたエンドポイントを使用して `.ppkg` ファイルを生成します。このステップの後、`.ppkg` ファイルは MDM サーバーで使用可能になり、デプロイメントでの一括登録が容易になります。

3. 一括登録: MDM 登録アクションをトリガーした後、BigFix agent がインストールされた、対象の Windows デバイスは、事前構成された .ppkg 成果物と共に MCM に自動的に登録されます。ユーザーの操作は必要ありません。
4. プライマリー・ユーザーの割り当て: .ppkg ファイルを使用して登録した Windows デバイスのプライマリー・ユーザー名は、ユーザー割り当て (（ページ） 473) アクションを使用して適切なプライマリー・ユーザー名で上書きする必要があります。上書きしないと、登録済みのすべての Windows デバイスは、.ppkg にハードコードされたデフォルトのプライマリー・ユーザー情報を報告するため、スマート・グループ (（ページ） 318) によるユーザーおよびグループ管理を使用できなくなります。

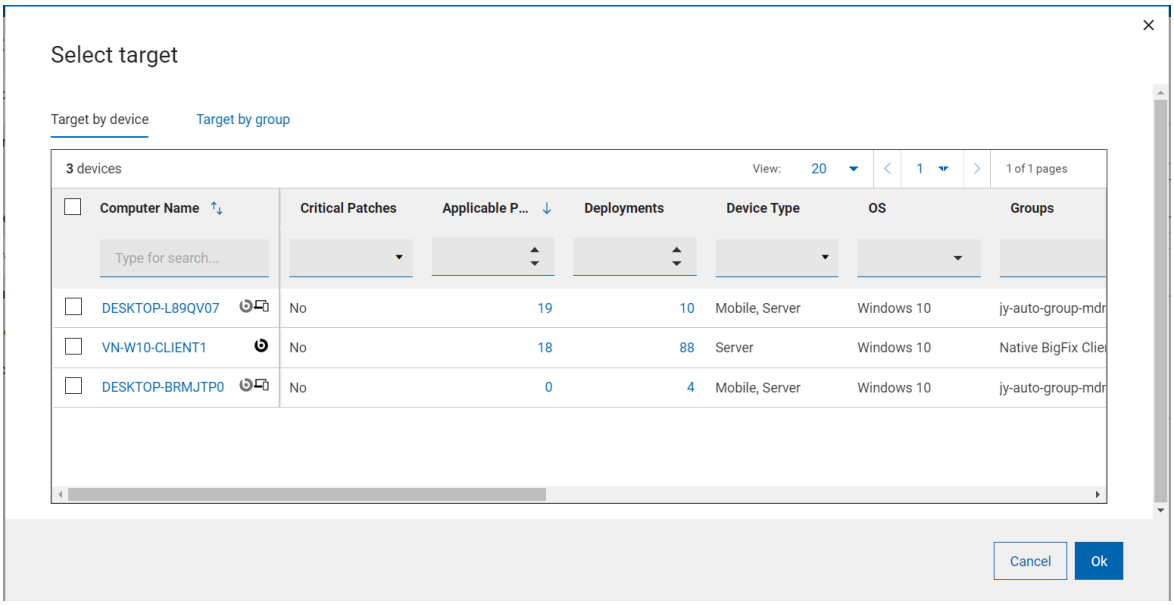
プロビジョニング・パッケージ生成ポイントの指定

デバイスを Windows プロビジョニング・パッケージ生成ポイントとして指定するには、次の操作を実行します。

1. Master operator として BigFix WebUI にログインします。
2. WebUI メイン・ページで、**「アプリ」 > 「MCM」**をクリックします。
3. 「Modern Client Management」ページで、**「管理者」 > 「登録」 > 「プロビジョニング・パッケージ生成ポイントの指定」**をクリックします。



4. 「プロビジョニング・パッケージ生成ポイントの指定」ページの「対象デバイス」セクションで、**「デバイスの編集」**をクリックします。
5. 「デバイス別ターゲット」ページで、1 つ以上のデバイスを選択して .ppkg ファイルを生成し、**「OK」**をクリックします。



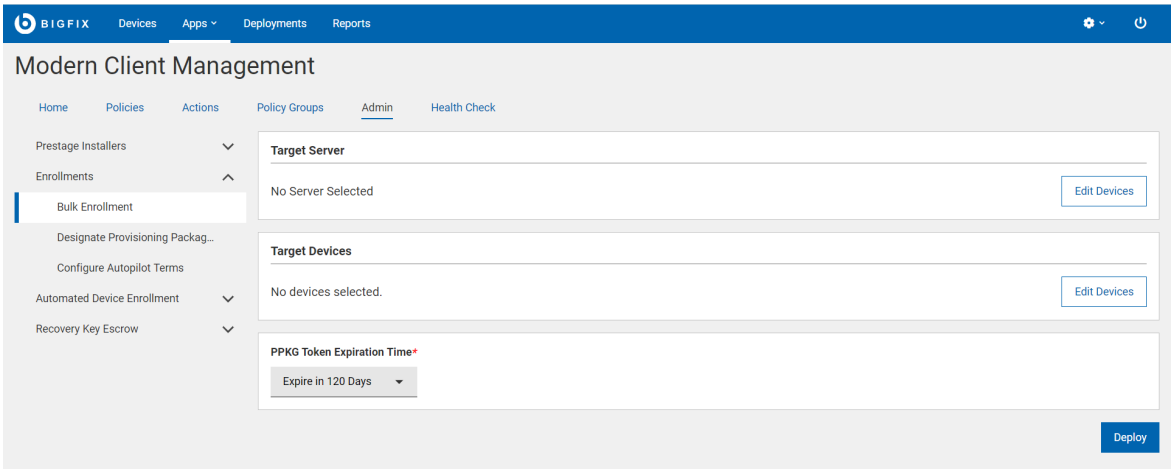
6. 「対象デバイス」セクションの情報を確認し、**「適用」**をクリックします。

結果: 選択したデバイスは、`.ppkg` ファイルを作成できる `.ppkg` 生成ポイントになります。クライアント設定 `MCM_WIN10_BULK_ENROLLMENT_ENDPOINT = 1` が対象デバイスで設定されます。

Windows プロビジョニング・パッケージの作成

Windows プロビジョニング・パッケージ (`.ppkg`) を作成し、MDM サーバーの一括登録に使用できるようにするには、次の操作を行います。

1. Master operator として WebUI にログインします。
2. **「アプリ」 > 「MCM」**をクリックします。
3. 「Modern Client Management」ページで、**「管理者」**をクリックします。
4. 「管理者」ページで、**「登録」 > 「一括登録」**をクリックします。



5. **「対象サーバー」**セクションには、このタスクが正常に完了したときに .ppkg ファイルがデプロイされた MDM サーバーが表示されます。変更を加える場合は、**「デバイスの編集」**をクリックします。
6. **「ターゲット・デバイス」**セクションには、プロビジョニング・パッケージ生成ポイントの指定 ((ページ) *336)* で指定されたデバイスの数が表示されます。変更を加える場合は、**「デバイスの編集」**をクリックします。

> **注:** ここで選択した Windows デバイスは、ArchiveNow を使用して、ルート MDM server に ppkg コンテンツをアップロードします。選択した Windows エンドポイントと ArchiveNow に関する特定のワークフローがある場合、このアクションの後に上書きされます。

7. **PPKG トークンの有効期限**: このフィールドは必須です。ドロップダウン・メニューからオプションを選択して、ppkg の有効期間を設定します。有効期限が切れると、その ppkg を Windows デバイスの登録に使用することはできません。デフォルトの有効期限は 120 日です。使用可能なオプションは次のとおりです。
    - 120 日後に期限切れ
    - 1 年後に期限切れ
    - 有効期限なし: このオプションを選択すると、ppkg は有効期限なしになります。

> **ヒント:** WebUI は内部で各 PPKG に固有のトークンを作成します。これにより、必要なときに新しい PPKG を作成してデプロイすることで、不正な

PPKG の使用を防ぐことができます。MDM サーバー上の PPKG トークンと登録デバイスが一致しない場合、登録を完了できません。

重要:

- タイムスタンプ付き PPKG を MDM サーバーにデプロイする場合は、MDM サーバーが v2.1.1 以降にアップグレードされていることを確認します。
- 有効期限なしで作成された PPKG ファイル (以前のバージョンの BigFix MCM で作成) は、MDM サーバー v2.1.1 以降では期待どおりに機能しません。したがって、PPKG を再度作成してデプロイする必要があります。

8. **「デプロイ」**をクリックします。

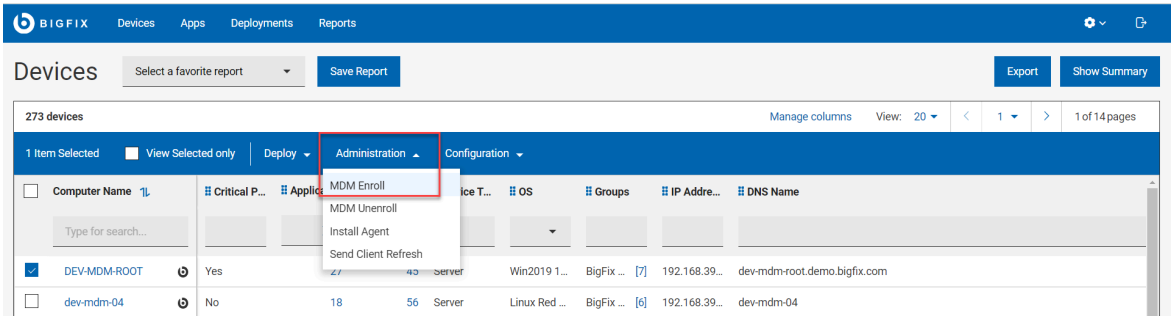
注: このプロセスが完了するまで数分かかります。プロセスを高速化するには `ppkg` を生成する Windows デバイスを数回再起動します。

結果: このアクションが完了すると、Windows `ppkg` ファイルが、ターゲットの Windows デバイスの `C:\MCMPPKG` に作成されます。

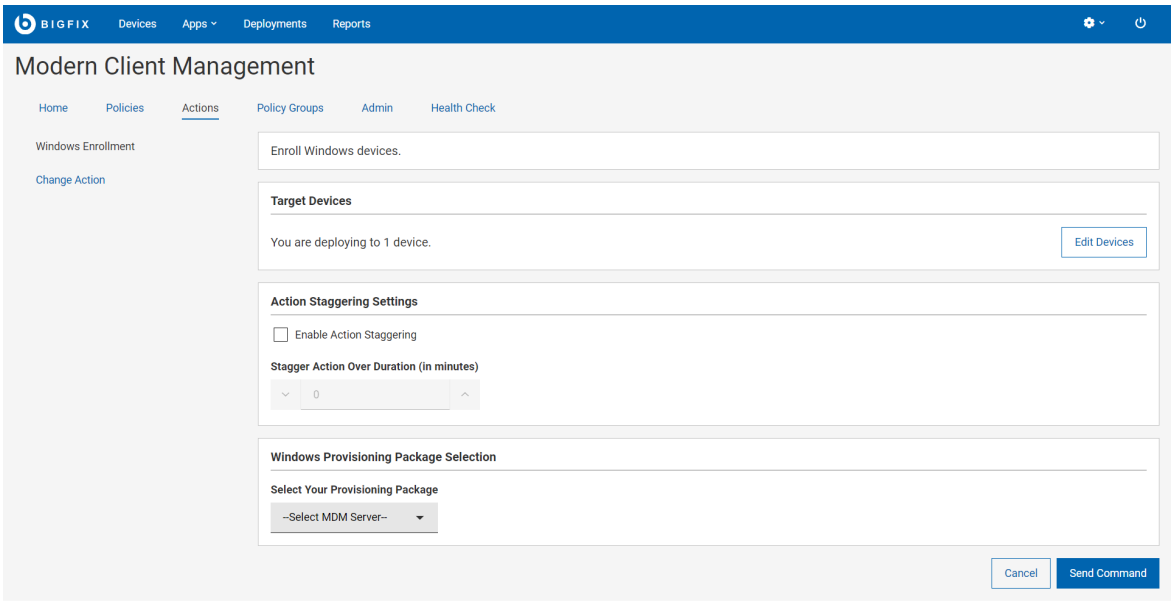
一括登録

デバイスを前のステップで作成した `.ppkg` 成果物を使用して一括で登録するには、以下を実行します。

1. BigFix WebUI にログインします。
2. 「デバイス」 (*(ページ) 22)*ページでネイティブ BigFix agent がインストールされているデバイスをフィルタリングします。これを行うには**「OS」**列で `Windows` を選択し、**「エージェント」**列で `Yes` を選択します。
3. デバイスの一覧から、一括登録するすべてのデバイスまたはサブセットを選択します。
4. **「管理」 > 「MDM 登録」**をクリックします。



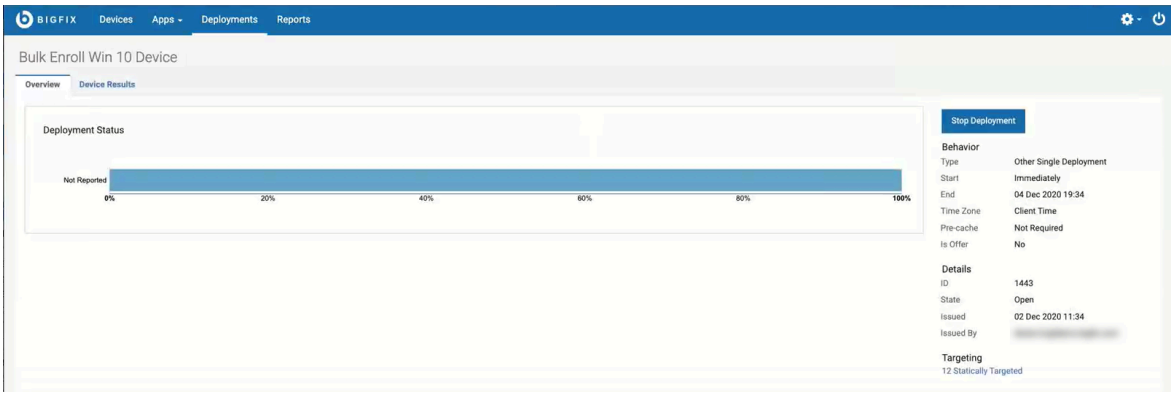
「Windows 登録」ページが表示されます。



5. 「対象デバイス」セクションに、対象デバイスの数が表示されます。対象デバイスを変更する場合は、**「デバイスの編集」**をクリックします。
6. アクションの分散設定: **「アクション分散の有効化」**を選択し、**「期間 (分) にわたってアクションを分散」**に入力します。この設定を使用すると、MDM サーバーとネットワークにかかる負荷を分散し、対象となるすべてのエンドポイントが同時に登録を試みるのを防ぐことができます。登録エンドポイントを分散することで、期間がより管理しやすくなり、新しく登録されるデバイスによって発生するトラフィックの量が正規化されます。この設定を行うと、各エンドポイントは、指定された時間間隔内で時間をランダムに選択して、登録を行います。
7. **「プロビジョニング・パッケージの選択」**で、選択したデバイスを登録する MDM サーバーを選択します。

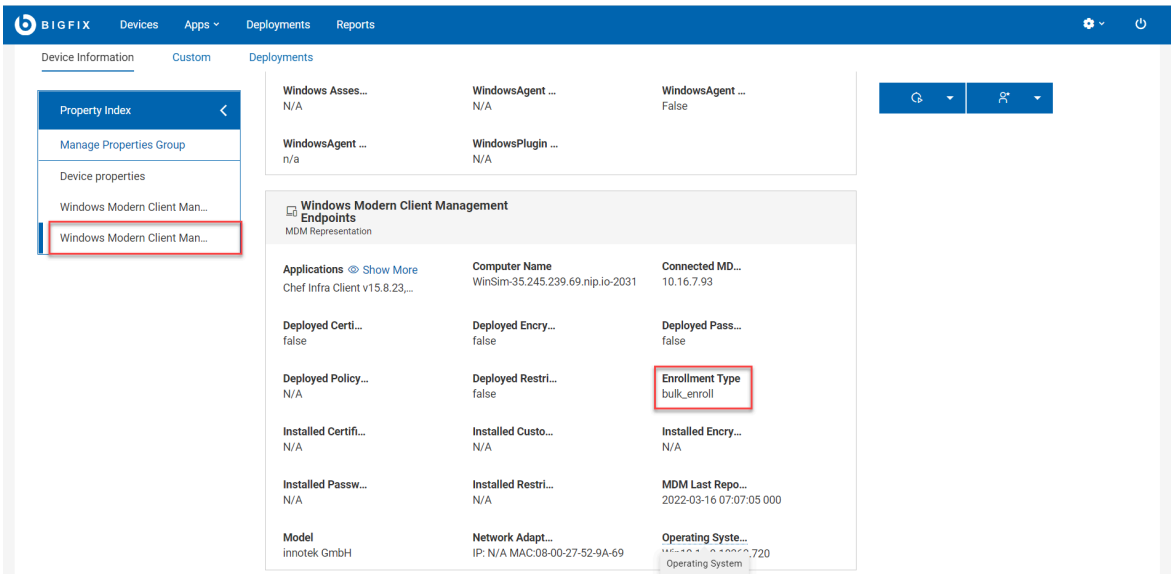
注: このドロップダウンには、Windows プロビジョニング・パッケージの作成 (（ページ） *337)* に従って PPKG がデプロイされている MDM サーバーがリストされます。

8. **「コマンドの送信」**をクリックします。
   - 選択したデバイスで MDM 登録を開始する BigFix 適用環境が生成されます。
   - 対象デバイスとデバイス結果に関する情報を含むデプロイメント文書 (（ページ） *214)*が表示されます。
   - 対象デバイスが登録プロセスを開始します。
   - 任意の時点でデプロイメントを停止するには、**「デプロイメントの停止」**をクリックします。



結果:

- アクションの実行後、ターゲットデバイスは、選択した MDM サーバーに登録されます。
- 登録済みデバイスは、デバイス・リスト (（ページ） *22)* に MDM アイコン SAMPLE_WIN とともに表示されます。
- 「デバイス・リスト」で、一括登録されたデバイスをクリックすると、「デバイス情報」ページの「Windows Modern Client Management エンドポイント」セクションで、「登録タイプ」が「bulk_enroll」と表示されます。



- デバイス・ユーザーが登録済みデバイスで構成済みのプロビジョニング・パッケージの詳細を表示するには、「設定」>「アカウント」>「職場または学校にアクセスする」>「プロビジョニング・パッケージを追加または削除する」に移動します。

  何らかの理由で一括登録を使用してこのデバイスを再度登録する場合は、次の手順を実行します。

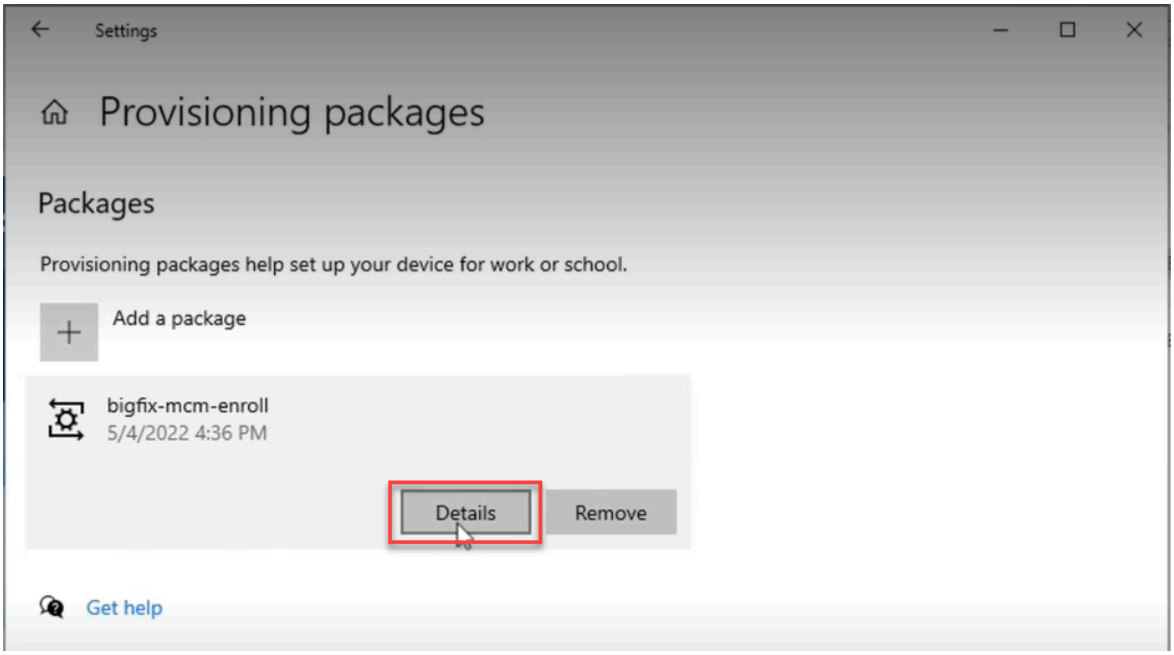
  1. デバイスでプロビジョニング・パッケージを削除します。
  2. 「設定」>「アカウント」>「職場または学校にアクセスする」で MDM プロフィールを切断します。
  3. WebUI から Windows 登録を開始します。

トラブルシューティング

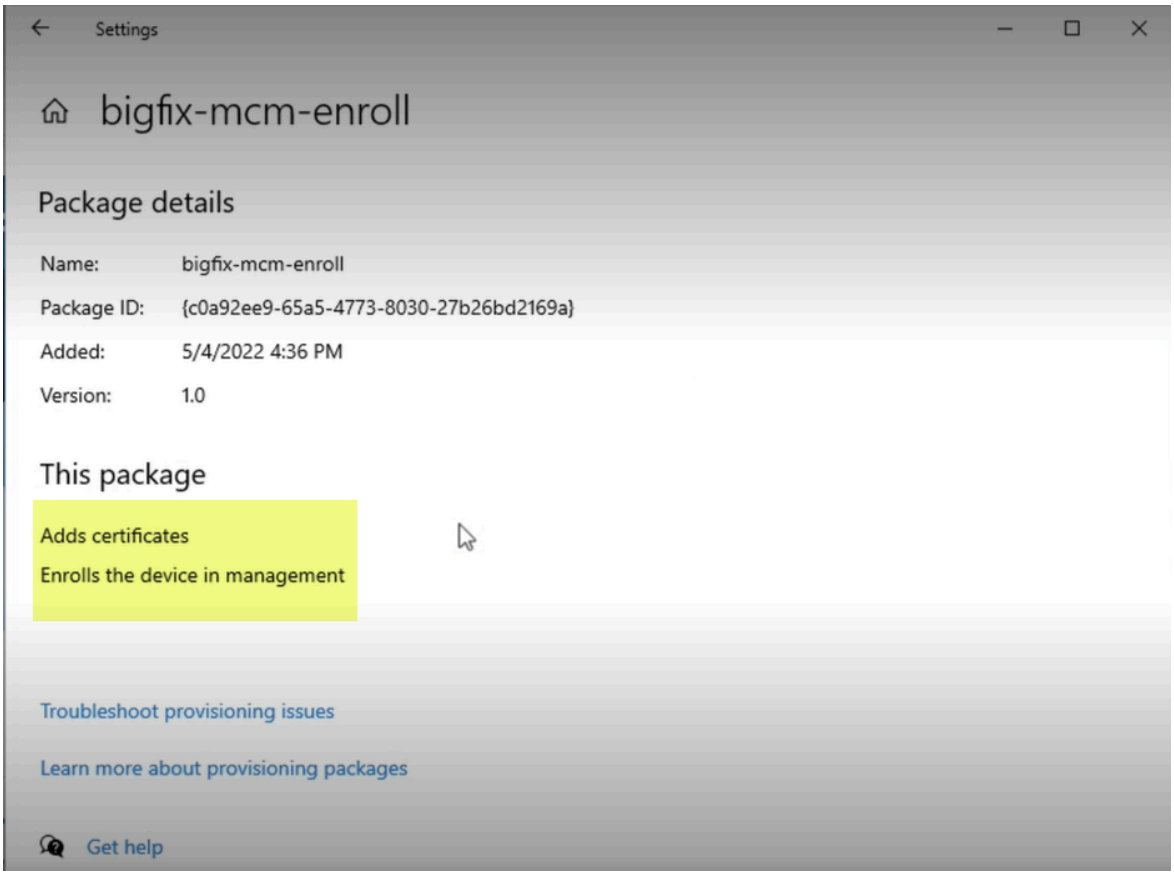
一括登録、無線 (OTA) 登録 (（ページ） 346)、または PPKG ファイルをダウンロードするための電子メールまたはリンクを介した登録 (（ページ） 347)に、`.ppkg` ファイルを使用できます。

これらのシナリオではいずれも、登録が正常に完了すると、デバイス・ユーザーは登録済みデバイスで構成済みのプロビジョニング・パッケージの詳細を表示できます。このためには、以下の手順に従います。

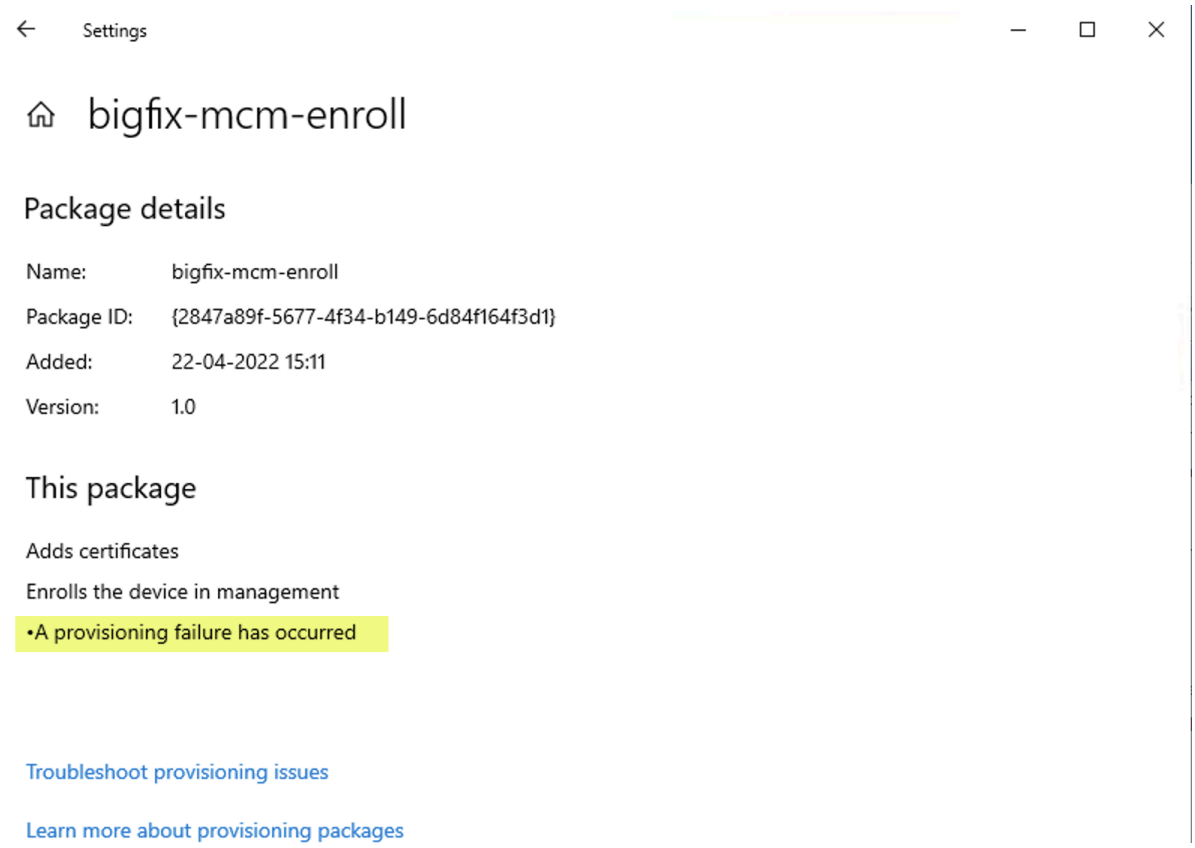
1. Windows デバイスで、**「設定」 > 「アカウント」 > 「職場または学校にアクセス」 > 「プロビジョニング・パッケージを追加または削除する」**に移動します。
2. 詳細を表示するには、プロビジョニング・パッケージをクリックし、**「詳細」**をクリックします。



構成した `.ppkg` の詳細は、例えば次のように表示されます。



失敗した場合は、次のようなエラーメッセージが表示されます。



これは .ppkg による登録がうまくいかなかったことを意味します。

.ppkg 登録が失敗する理由として次のようなものがありますが、原因はこれに限定されません。

- .ppkg の有効期限が切れている場合。設定された PPKG トークンの有効期限 (（ページ） 338)が切れている場合、各 .ppkg を使用した登録は失敗します。
- MDM サーバーとデバイス上の .ppkg が異なる場合。

管理者に連絡して、登録を続行するための適切な .ppkg ファイルを入手してください。

重要: 別の .ppkg ファイルを使用して再登録を試みる前に、その前にダウンロードしていた .ppkg ファイルをデバイスから削除するようにしてください。

ユーザーによる登録 - Windows

Windows デバイスをデバイス・ユーザーとして登録する方法については、このセクションを参照してください。

Windows プロビジョニング・パッケージが MDM サーバーに存在する場合、管理者はデバイス・ユーザーと `.ppkg` ファイルを共有して、ユーザーによる登録を通じて Windows デバイスを登録できます。

Windows プロビジョニング・パッケージを作成およびデプロイする方法については、「一括登録 - Windows (（ページ） *335*)」を参照してください。

重要: 登録の前に、Windows プロビジョニング・パッケージ (`.ppkg`) が対象デバイスに存在していないことを確認します。Windows デバイスを再登録する場合は、`.ppkg` ファイルが手動で削除されていることを確認してください。

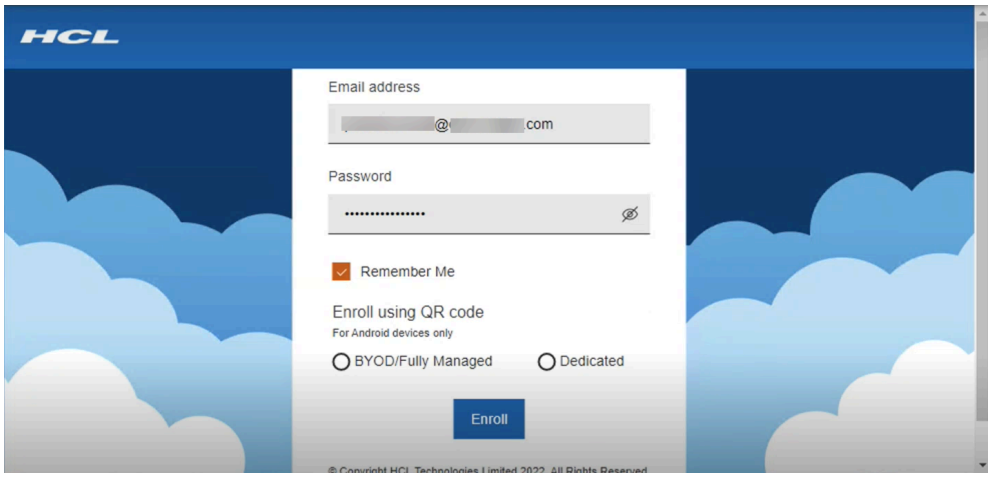
ユーザーによる登録は、以下の方法で行うことができます。

無線経由の登録:

MDM サーバーに Windows プロビジョニング・パッケージがある場合、デバイス上のユーザーが MDM サーバーの登録 URL をクリックすると、認証が成功したときに `.ppkg` ファイルが表示されます。ユーザーはこの `.ppkg` ファイルを使用して、MDMに自動的に登録できます。これを行うには、以下を実行します。

1. 前提条件 (（ページ）　　)が満たされていることを確認します。
   登録する必要がある Windows デバイスで、Web ブラウザーを起動し、MDM サーバーの URL に移動します。`ppkg` パッケージが MDM サーバーに存在し、一括登録が TRUE に設定されている場合は、次の画面が表示されます。
   - LDAP 認証がオンの場合は、資格情報の有効な AD セットに関連付けられた E メール・アドレスとパスワードを入力し、**「登録」**をクリックします。
   - LDAP 認証がオフの場合は、**「登録」**をクリックします。

   `ppkg` ファイルがダウンロードされます。



2. ダウンロードされた ppkg ファイルをクリックすると、登録プロセスが開始されます。

PPKG ファイルをダウンロードするための電子メールまたはリンクを介した登録

管理者が電子メール、ダウンロード可能なリンク、またはその他の手段を介してデバイス・ユーザーと .ppkg ファイルを共有し、デバイス・ユーザーがその .ppkg ファイルをダブルクリックした場合、MDM 登録プロファイルがエンドポイントに追加されます。

トラブルシューティングの情報については、トラブルシューティング (（ページ） 342)を参照してください。

Autopilot 登録

Windows Autopilot を使用すると、管理者は、最初の起動時に MDM に登録するように事前構成された新しいデバイスまたは工場出荷時にリセットされている Windows デバイスを自動的に登録できます。

Autopilot の構成は、Microsoft Endpoint Manager を使用して行われます。詳しくは、BigFix の Wiki ページの『Windows Autopilot 構成ガイド』を参照してください。

WebUI を使用して、Autopilot の登録に対して次の項目を構成できます。

- ポリシー・グループによるデフォルトの Windows プロファイル (（ページ） *348)*
- Windows Autopilot サービス利用条件 (（ページ） *350)*

Autopilot 登録用のデフォルト Windows プロファイルの構成

登録時に Windows エンドポイントにデプロイできる MDM サーバーでデフォルト Windows プロファイルを構成する方法について説明します。

ポリシー・グループは、登録時に MDM エンドポイントに適用できる MDM・ポリシーとアプリケーションの集合です。

Autopilot デバイスの登録時に、ポリシーのセットを適用するポリシー・グループを作成するワークフローを以下に示します。

1. アプリケーションを事前ステージングします。MDM サーバーで事前にステージングされたアプリケーションをここに示します。アプリケーションの事前ステージングの方法については、「アプリケーションの事前ステージング (（ページ）)」を参照してください。
2. カスタム・ポリシーのアップロード (（ページ） *458)*。必要に応じて、カスタム・ポリシー・コードを含む `.xml` ファイルをアップロードします。

   注: 任意で、をアップロードできます。 デバイス・ユーザーによる完全管理対象 (会社所有) デバイスの登録解除を制限するカスタム・ポリシー (（ページ） *349)*

3. 必要に応じて、他の MDM ポリシー・タイプ (パスコード・ポリシー (（ページ） *446)*、制限ポリシー (（ページ） *451)*、証明書ポリシー (（ページ） *402)* など) を作成し、ポリシーを保存します。

   注: Windows のディスク暗号化ポリシーは、現時点ではポリシー・グループの一部として使用できません。

4. ポリシー・グループを作成します。 (（ページ） *386)*

   a. OS を選択します。オペレーティング・システムに Windows を選択します。

   b. ポリシーを追加します。「+」ボタンをクリックし、必要なカスタム・ポリシーとその他の MDM ポリシーをポリシー・グループに追加します。

注: 一度に使用可能なパスコードまたは制限ポリシーは 1 つだけですが、複数の証明書ポリシーが使用可能です。

c. アプリケーションを追加します。必要な事前ステージ済みアプリケーションをポリシー・グループに追加します。

d. BigFix エージェントを追加します。

e. グループに割り当てます。「Autopilot 登録」を選択すると、デフォルト設定では、登録時にすべての Autopilot 登録済みデバイスにこのポリシー・グループがデプロイされます。

f. ポリシー・グループを保存します。

5. ポリシー・グループを選択し、ポリシー・グループを MDM サーバーにデプロイします。

デフォルトのポリシー・グループが作成され、MDM サーバーにデプロイされます。Windows ファイルが Autopilot 登録で登録されると、このポリシー・グループに追加されたポリシーとアプリケーションが登録済みデバイスにデプロイされます。

デバイス・ユーザーによる完全管理対象 (会社所有) デバイスの登録解除を制限するカスタム・ポリシー

Windows デバイス・ユーザーが完全管理対象 (会社所有) デバイスを MDM から登録解除するのを制限するには、以下のコードを使用してカスタム・ポリシー `.xml` ファイルをアップロードし、それを MDM サーバーにデプロイするポリシー・グループに追加します。

```
<Replace>
<CmdID>20</CmdID>
<Item>
<Target>
<LocURI>./Vendor/MSFT/Policy/Config/Experience/AllowManualMDMUnenrollment</LocURI>
</Target>
```

```
<Meta>
<Format>int</Format>
<Type>text/plain</Type>
</Meta>
<Data>0</Data>
</Item>
</Replace>
```

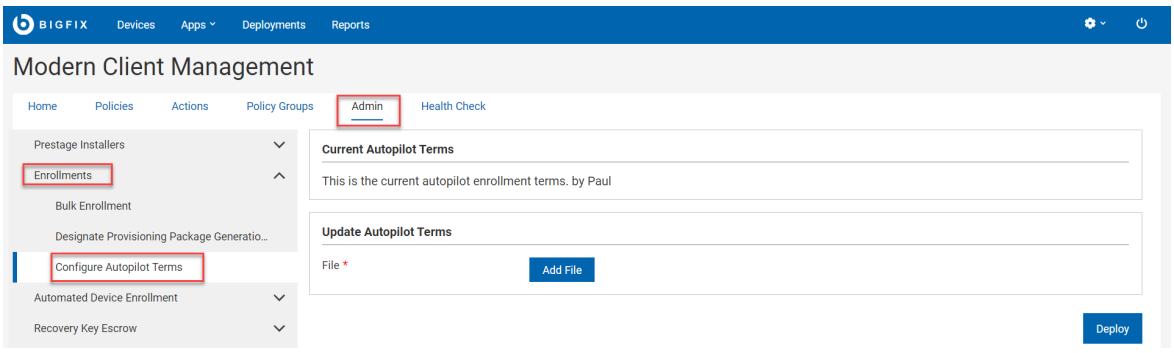
Windows Autopilot のサービス利用条件の構成

会社のロゴと利用規約を追加して、Windows Autopilot を使用して登録する際にエンド・ユーザーのご使用条件画面をカスタマイズする方法について説明します。

カスタマイズされたサービス利用条件 HTML ファイルを作成します。

注: この HTML ファイルは、エンド・ユーザーに対して特定のアクションを実行する特定のボタンを表示するために、特定の要件を満たす必要があります。プロトコル・セマンティクスの詳細については、「https://docs.microsoft.com/en-us/windows/client-management/mdm/azure-active-directory-integration-with-mdm#terms-of-use-protocol-semantics」を参照してください。これらの要件を満たしていない Autopilot のサービス条件 HTML ファイルを使用すると、ユーザーが起動時に正しく登録できなくなります。

1. WebUI のメイン・ページから、**「アプリケーション」 > 「MCM」**を選択します。
2. 「Modern Client Management」ページで、**「管理者」 > 「登録」 > 「Autopilot の条件の構成」**をクリックします。以下のページが表示されます。



3. 「Autopilot 利用条件の更新」で、**「ファイルの追加」**をクリックし、組織のカスタマイズされた利用条件を含む HTML ファイルを選択します。
4. **「デプロイ」**をクリックします。

構成されたサービス利用条件ページは、Windows Autopilot を通じてデバイスが登録されると、Windows デバイスに表示されます。

Apple 自動デバイス登録

MCM and BigFix Mobile は、Apple デバイスの登録と構成を自動化するオンライン・サービスである Apple 自動デバイス登録プログラム (DEP) をサポートしています。

Apple 自動デバイス登録を使用すると、ユーザーの介入なしに、多数の Apple デバイスを簡単に登録できます。Apple Business Manager ポータルでは、BigFix 管理者は、デバイスをどの MDM サーバーに割り当てることができるかを事前に設定し、デバイスの初期セットアップの一環としてデバイスを MCM and BigFix Mobile に自動的に登録できます。

プログラムの資格を得る方法や Apple Business Manager とのリンクなど、Apple 自動デバイス登録の詳細については、Apple のサポート・サイトを参照してください。

すべての Apple デバイスは、初期設定の一部として、Apple Business Manager にアクセスして、登録するために特定の MDM サーバーに事前に割り当てられているかどうかを確認します。Apple Business Manager は、特定のプロファイルにマップするデバイスの構成を検出すると、そのプロファイルをデバイスに送信します。デバイスは登録情報を処理し、必要な設定を行い、プロファイル内で定義された MDM サーバーにアクセスして MDM 登録を行います。Apple 自動デバイス登録プロファイルのマッピングに特定のデバイスがない場合、デバイスは、自動割り当て者としてマークされている MDM サーバーに割り当てられた自動デバイス登録プロファイルを取得します。

自動デバイス登録用の ABM または MCM サーバーの構成方法については、BigFix の Wiki ページ『DEP 用 Apple Business Manager クイック・スタート・ガイド』を参照してください。

注: すべての自動デバイス登録プロファイル構成ファイル (`.crt, .key, .enc,` および `.p7M`) は、MDM サーバー上の `/var/opt/BESUEM/certs` ディレクトリーに格納されます。

これらの構成がすべて完了したら、ユーザーが Apple デバイスの電源を入れて最初の OS セットアップを行い、インターネットに接続すると、Apple サーバーは通知を受け取り、自動デバイス登録プロファイル・アカウントを認識し、デバイスを適切な MDM サーバーにリダイレクトします。Apple デバイスのセットアップ・アシスタントは、ユーザーのアクティベーション・プロセスを支援します。

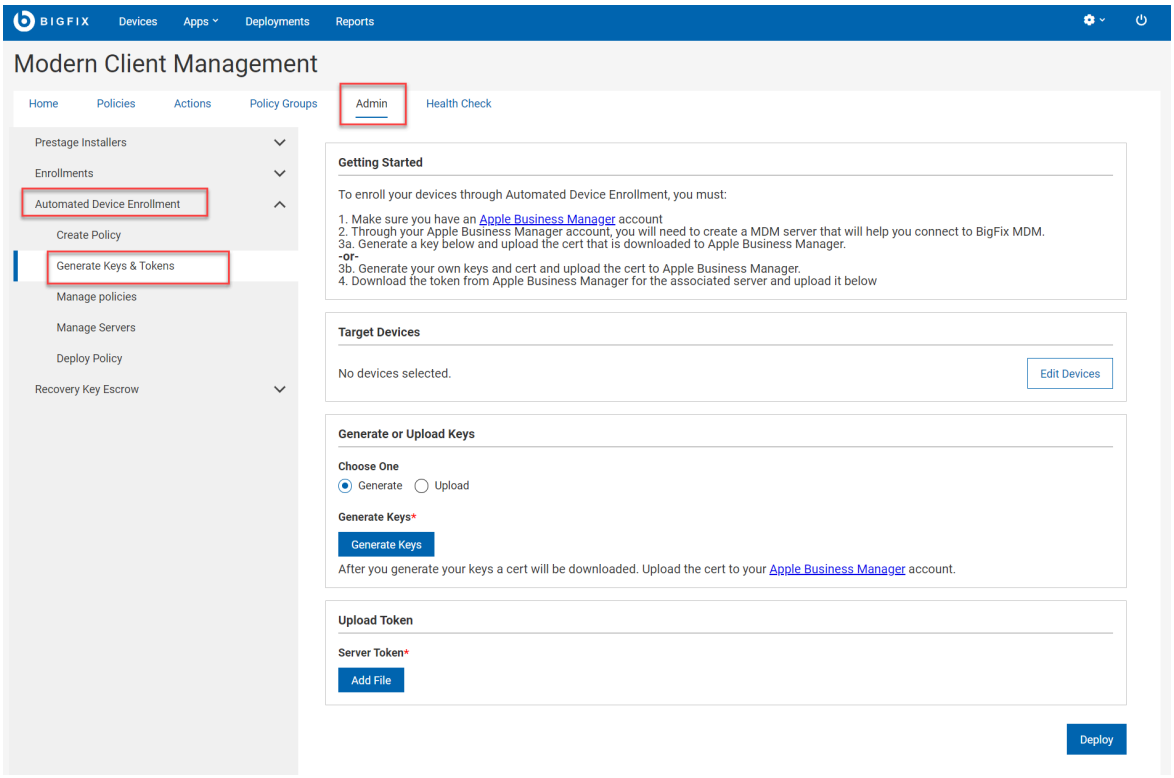
デバイスの登録後、WebUI を使用して MDM デバイスを管理 (（ページ） 368)できます。

MDM サーバー・トークンのアップロード

WebUI を介して、自動デバイス登録によって通信を確立し、Apple デバイスを登録するために、Apple Business Manager から取得したサーバー・トークン (`.p7m`) をアップロードする必要があります。

Apple Business Manager で定義する MDM サーバーの公開鍵または秘密鍵を作成するには、次の手順を実行します。

1. マスター・オペレーターとして BigFix WebUI にログインします。
2. WebUI のメイン・ページから、**「アプリ」 > 「MCM」**をクリックします。
3. 「Modern Client Management」ページで、**「管理者」 > 「自動デバイス登録」 > 「キーとトークンの生成」**をクリックします。以下のページが表示されます。



4. **「対象デバイス」**で、**「デバイスの編集」**をクリックし、Apple Business Manager で定義する MDM サーバーを選択します。
5. **「トークンのアップロード」**で、**「ファイルの追加」**をクリックし、Apple Business Manager で作成した MDM サーバー・トークン `.p7m` を参照します。
6. **「デプロイ」**をクリックします。

ターゲット MDM サーバーと Apple Business Manager の間で接続が確立されます。この MDM サーバーは、デバイスを自動的に登録できる DEP サーバーとして機能します。

次のステップ:ABM でのデバイスの割り当て (（ページ）　　)

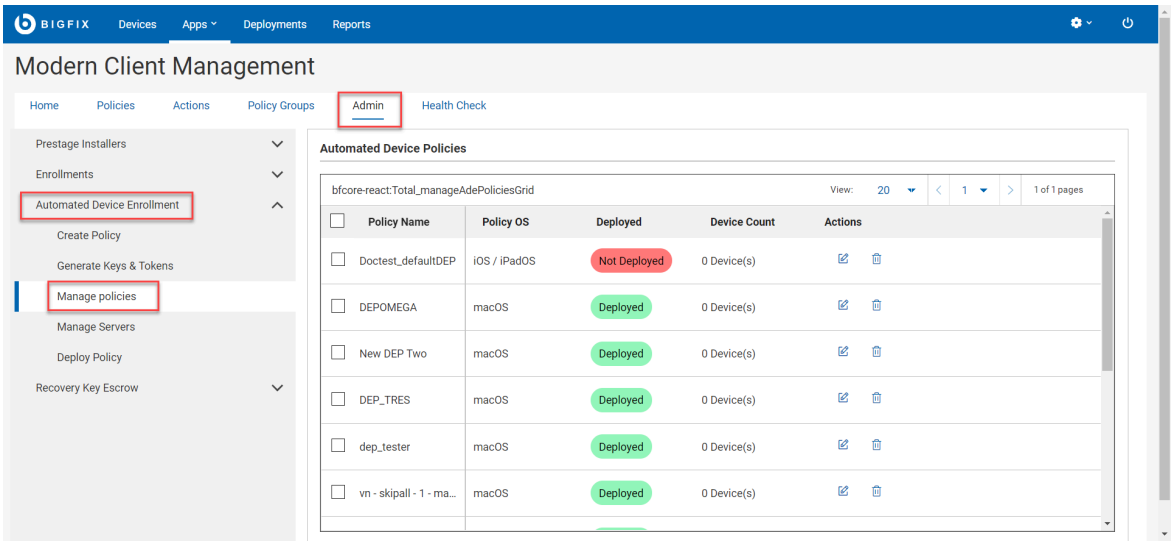
自動デバイス登録ポリシーの管理

DEP ポリシーの管理方法を説明します。

DEP ポリシーを管理するには、次の手順を実行します。

1. マスター・オペレーターとして BigFix WebUI にログインします。
2. WebUI のメイン・ページから、**「アプリ」** > **「MCM」**をクリックします。

3. 「Modern Client Management」ページで、**「管理者」 > 「自動デバイス登録」 > 「ポリシーの管理」**をクリックします。関連するすべてのポリシーを一覧で示した以下のページが表示されます。



4. ポリシーの管理:
   - ポリシーの結果リストを絞り込むには、適切なフィルターを選択します。
   - 既存のポリシーを編集するには、目的のポリシーの横にあるペン・アイコン  をクリックし、変更を加えて、 をクリックします。**「保存」**
   - ポリシーを削除するには、目的のポリシーの横にあるごみ箱アイコン  をクリックし、**「削除」**をクリックして確定します。
   - 新しいポリシーを作成 (（ページ）)するには、**「ポリシーの作成」**をクリックします。
   - DEP サーバーにポリシーをデプロイするには、リストからポリシーを選択し、**「デプロイ」**をクリックします。

アプリケーションの管理

MCM サーバーは、登録中、またはデバイスが MCM に登録された後で、、Windows、macOS、Android、Apple モバイル・デバイスに、BigFix agent やその他のアプリケーションをインストールするように構成できます。

管理者ユーザーは次のタスクを実行できます。

- Windows および macOS デバイス用の BigFix agent の事前ステージング
- Android および Apple モバイル・デバイスの管理対象構成の定義
- VPP 機能の有効化または無効化による Apple モバイル・デバイスでのアプリ管理

ログインした WebUI ユーザーは次のタスクを実行できます。

- を介したアプリの追加、削除、表示、管理 (（ページ）)
- App Store アプリ・ポリシー (（ページ）) の作成、管理、デプロイによる MCM 登録モバイル・デバイスでのアプリ管理

macOS BigFix インストーラーの事前ステージ

MDM サーバーで macOS 用 BigFix agent の最新バージョンを事前ステージしてデプロイする方法について説明します。

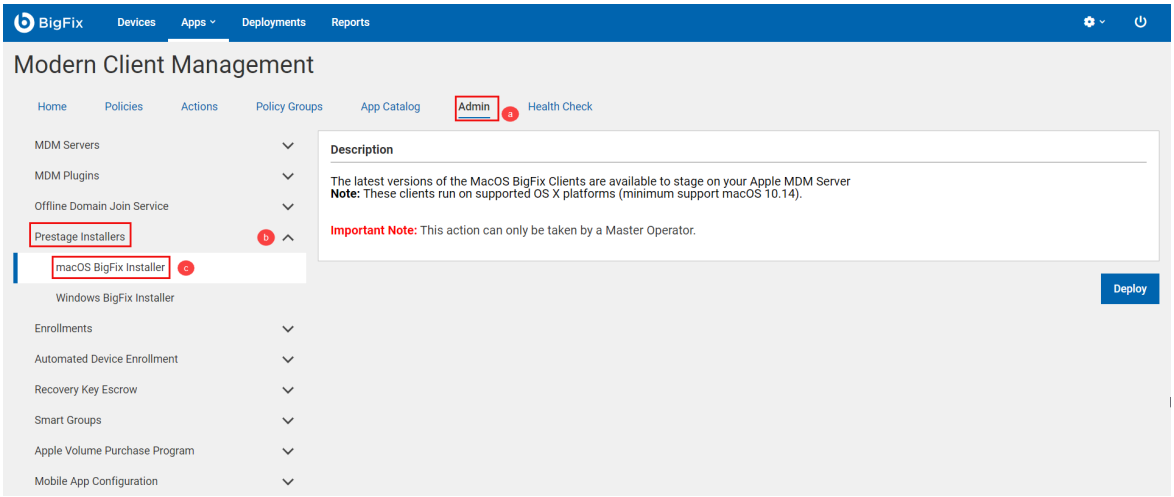
マスター・オペレーターのみが、MDM サーバーに MacOS エージェントを事前ステージできます。

BigFix インストーラー・パッケージが MDM サーバーで事前ステージされている場合、エンドポイントが MDM に登録された後、登録済みのデバイスに BES エージェントをデプロイすることもできます。

BigFix は、macOS 用 BigFix agent のリリース済みバージョンごとにインストール・パッケージを提供します。パッケージの更新バージョンが利用可能になるたびに、WebUI を使用して MDM サーバーに対してこのパッケージを事前ステージします。事前ステージされると、BigFix エージェントをデプロイするターゲットとして MacOS デバイスが選択されている場合、WebUI は「BigFix エージェントのデプロイ」アクションでデプロイできる BigFix パッケージを一覧表示します。

macOS デバイス用の BigFix インストーラーを事前ステージするには:

1. WebUI のメイン・ページから、**「アプリ」 > 「MCM」**をクリックします。
2. 「Modern Client Management」ページで、**「管理者」 > 「インストーラーの事前ステージ」 > 「macOS BigFix インストーラー」**をクリックします。以下のページが表示されます。



3. **「デプロイ」**をクリックします。

このアクションは、使用可能なすべての MDM サーバー上に macOS 用の最新の BigFix インストーラーをデプロイします。

注:

- 対象デバイス上の OS バージョンと互換性のある署名済み macOS パッケージのみが正常にインストールされます。
- また、macOS パッケージを正常にインストールするには、前提条件がある場合はその条件を満たす必要があります。例えば、macOS パッケージを Apple シリコン (M1 チップ) のデバイスにインストールするには、前提条件の Rosetta ソフトウェアをそれらのデバイスにインストールする必要があり

ます。詳しくは、https://support.apple.com/en-us/HT211861 を参照してください。

- アプリケーションが事前ステージ済みであることを MDM サーバーが認識するまでに時間がかかる場合があります。インストールできるパッケージを取り込む分析は、15 分ごとに情報が更新されます。

関連資料

BigFix エージェントのデプロイメント (（ページ）)

関連情報

MCM アクションのデプロイ (（ページ） *460)*

Windows BigFix インストーラーの事前ステージ

MDM サーバーで Windows 用 BigFix agent 最新バージョンを事前ステージしてデプロイする方法について説明します。

Windows BigFix インストーラー・パッケージが MDM サーバーで事前ステージされている場合、Windows エンドポイントが MDM に登録されると、登録済みのデバイスに BigFix エージェントをデプロイすることもできます。

始める前に: 事前ステージを行う前に、カスタム MSI パッケージを作成する必要があります。これは、Windows で BES サーバーをインストールする場合、インストーラーは BigFix agent をマストヘッド (BigFix agent の構成プロファイル) なしで `BigFix Enterprise \BES Installers\ClientMSI` フォルダーにコピーするためです。一般的な BigFix のインストールが完了すると、BigFix サーバーでベース MSI を確認できます。サイト・マストヘッドを含めることによってこの MSI パッケージをカスタマイズする必要があり、必要に応じて、インストーラー内で認証リレー情報を設定して、BigFix エージェントを WebUI を介してデプロイします。

A. カスタム BigFix エージェント MSI パッケージを準備する

カスタム BigFix エージェント MSI パッケージを準備するには、次の手順を実行します。

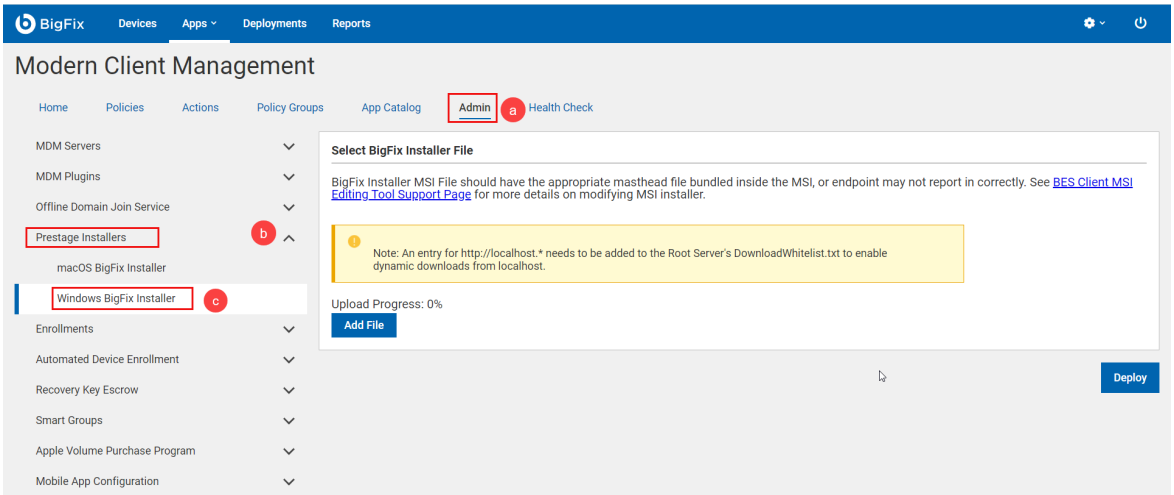
1. サーバー・コンポーネントと共にインストールされている BigFix エージェント `.msi` ファイルを見つけます(デフォルトの場所: `BES Installers\ClientMSI\BigFixAgent.msi`)。
2. `masthead.afxm` ファイルと `BigFixAgent.msi` ファイルを Windows マシン上の新しいフォルダーにコピーして、`BigFixAgent.msi` ファイルにマストヘッドを追加します。
3. `BESClientSetupMSI.exe` コマンドを実行し、インストーラーの手順に従ってマストヘッドに追加します。
4. `BigFixAgent.msi` ファイルに認証リレー `BESClientSetupMSI.exe /secureregistration <RELAY_PASSWORD> /relayserver1 http://<RELAY_HOST>:52311/bfmirror/downloads/ <TARGET_MSI>` がある場合は、必要に応じて、認証リレー・コマンドの詳細を追加します。

   結果: 事前ステージ可能なカスタマイズ済み `BigFixAgent.msi` ファイルは、選択したフォルダーにある Windows コンピューターで使用できるようになります。

B. Windows 用の BigFix インストーラーを事前ステージする

次の BigFix インストーラーを事前ステージするには、以下のステップを実行します。

1. WebUI のメイン・ページから、**「アプリ」 > 「MCM」**をクリックします。
2. 「Modern Client Management」ページで、**「管理者」 > 「インストーラーの事前ステージ」 > 「Windows BigFix インストーラー」**をクリックします。以下のページが表示されます。



3. **「ファイルの追加」**をクリックし、用意したカスタム `BigFixAgent.msi` ファイルを Windows マシンから選択します。
4. **「デプロイ」**をクリックします。

結果: このアクションは、使用可能なすべての MDM サーバー上に Windows 用の最新の BigFix インストーラーをデプロイします。事前ステージ済みの `BigFixAgent.msi` ファイルは MDM サーバー上の `/var/opt/BESUEM/packages` で確認できます。

注: アプリケーションが事前ステージ済みであることを MDM サーバーが認識するまでに時間がかかる場合があります。インストールできるパッケージを取り込む分析は、15 分ごとに情報が更新されます。

関連資料

BigFix エージェントのデプロイメント (（ページ）　　)

関連情報

MCM アクションのデプロイ (（ページ） *460)*

Apple Volume Purchase Program の有効化

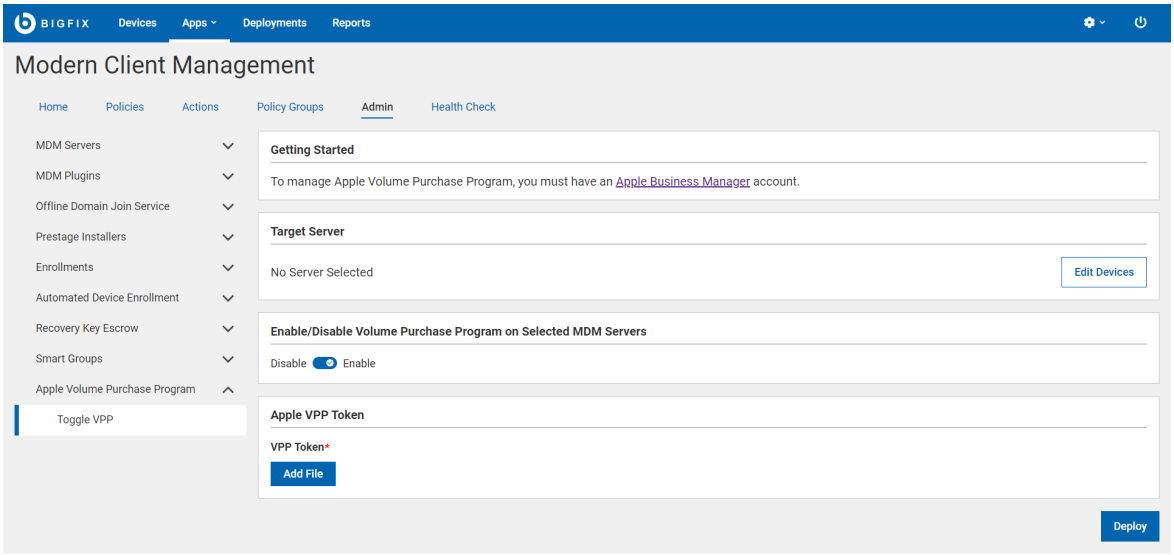
選択した MDM サーバーで、Apple Volume Purchase Program (VPP) を有効にすることができます。

Apple VPP トークンを入手する必要があります。VVPP に登録されている組織に関連付けられた Apple ID を使用して、Apple School Manager または Apple Business Manager からトークンをダウンロードします。

組織の Apple Business Manager または Apple School Manager アカウントを BigFix Mobile にリンクするには、VPP トークンが必要です。BigFix Mobile を使用して、組織内のデバイスにアプリとブックを配布します。

1. VPP を有効にするには、WebUI にマスター・オペレーターとしてログインします。
2. **「アプリ」 > 「MCM」**をクリックします。

3. **「管理者」**タブで、**「Apple Volume Purchase Program」 > 「VPP の切り替え」**を選択します。



4. **「デバイスの編集」**をクリックし、Apple VPP を有効にする MDM サーバーを選択します。
5. トグル・ボタンをクリックして VPP を有効にします。
6. **「Apple VPP トークン」**で **「ファイルの追加」**をクリックし、ダウンロードした `.vpptoken` ファイルを探します。
7. **「デプロイ」**をクリックします。

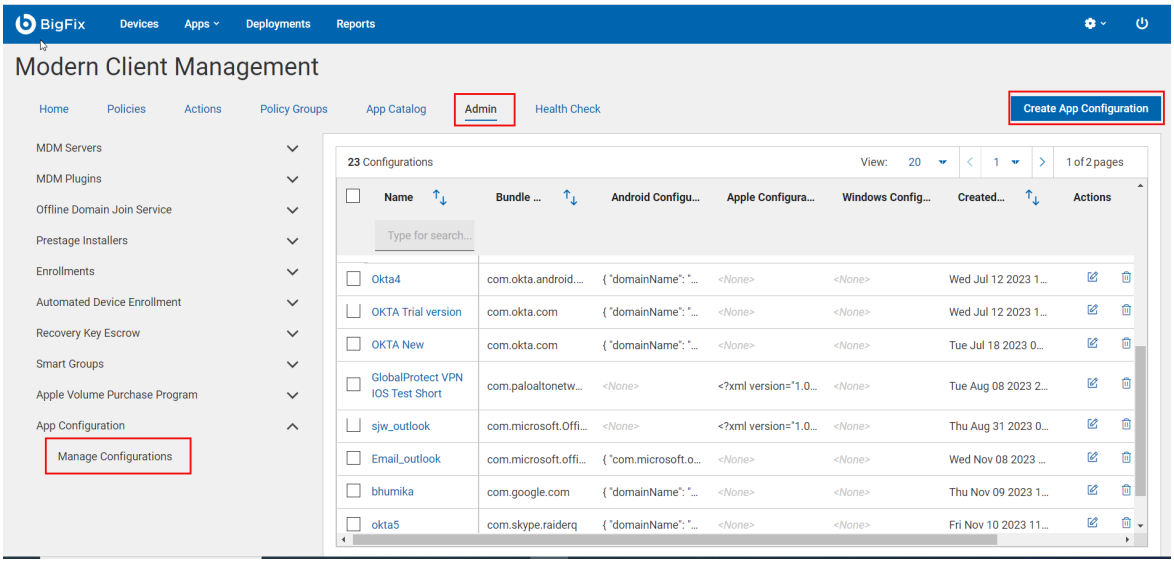
選択した MDM サーバーで VPP が有効になりました。 (（ページ）) を使用して VPP アプリを追加および配布できます。

アプリ構成

管理者ユーザーは、Android、Apple、Windows のアプリの構成設定を定義し、管理対象構成をサポートできます。

アプリ設定を構成するには、必要なアプリが (（ページ）) に追加されていることを確認します。

1. **「MCM アプリ」**ページで、**「管理」 > 「アプリ構成」 > 「設定の管理」**をクリックし、**「アプリ構成を作成」**をクリックします。



2. **「アプリ構成」**ページで次の手順を実行します。
   - 名前: アプリの名前を入力します。
   - バンドル ID/製品 ID: 必須。Android アプリと Apple アプリのバンドル ID または Windows アプリの製品 ID を入力します。

     注: Android アプリと Apple アプリのバンドル ID については、Google Play ストアまたは Apple App Store でアプリの詳細を検索してください。Windows アプリの製品 ID については、Windows ストアでアプリの詳細を検索してください。

   - 必要に応じて、Android、Apple、Windows に固有の構成設定を入力します。
     - **Android**Android アプリ構成の場合は、キーと値のペアとして JSON 形式で構成を入力します。

       例

       Okta Device Trust for Android を構成するための JSON 形式の管理対象構成:

```
 "managedConfiguration": {
 "domainName": “example.okta.com”,
 "managementHint": "3zr7Q~vw4C16FS2bH8UfS 1gJ5cL6sj~x_U9PQ"}
```

注: MDM デバッグ・ツールを使用して、Android アプリの管理対象構成を検索できます。

- **Apple**: Apple 構成の場合は、キーと値のペアで XML 形式の構成を入力します。

  例 1

  Apple モバイル・デバイス用の Outlook アプリを構成するための XML 形式の管理対象構成:

```
<?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>com.microsoft.outlook.EmailProfile.EmailAccountName</k
ey>
  <string>John Doe Email</string>
  <key>com.microsoft.outlook.EmailProfile.EmailAddress</key>
  <string>john.doe@hcl.com</string>

 <key>com.microsoft.outlook.EmailProfile.ServerHostName</key
>
  <string>outlook.office365.com</string>
  <key>com.microsoft.outlook.EmailProfile.EmailUPN</key>
  <string>john.doe@hcl.com</string>
  <key>com.microsoft.outlook.EmailProfile.AccountType</key>
  <string>SMTP</string>
```

```
 <key>com.microsoft.outlook.EmailProfile.AccountDomain</key>
  <string>hcl</string>
</dict>
</plist>
```

例 2

Apple モバイル・デバイス用の Okta Device Trust を構成するための XML 形式の管理対象構成:

```
<?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>OktaVerify.OrgUrl</key>
  <string>example.okta.com</string>
  <key>managementHint</key>
  <string><3zr7Q~vw4C16FS2bH8UfS 1gJ5cL6sj~x_U9PQ</string>
</dict>
</plist>%
```

注: 一部のアプリではリモート構成がサポートされません。アプリ構成キーについては、ソフトウェア・ベンダーの資料を参照してください。MDM デバッグ (（ページ）　　)・ツールを使用して、管理対象構成のプロパティーのリストを検索することもできます。

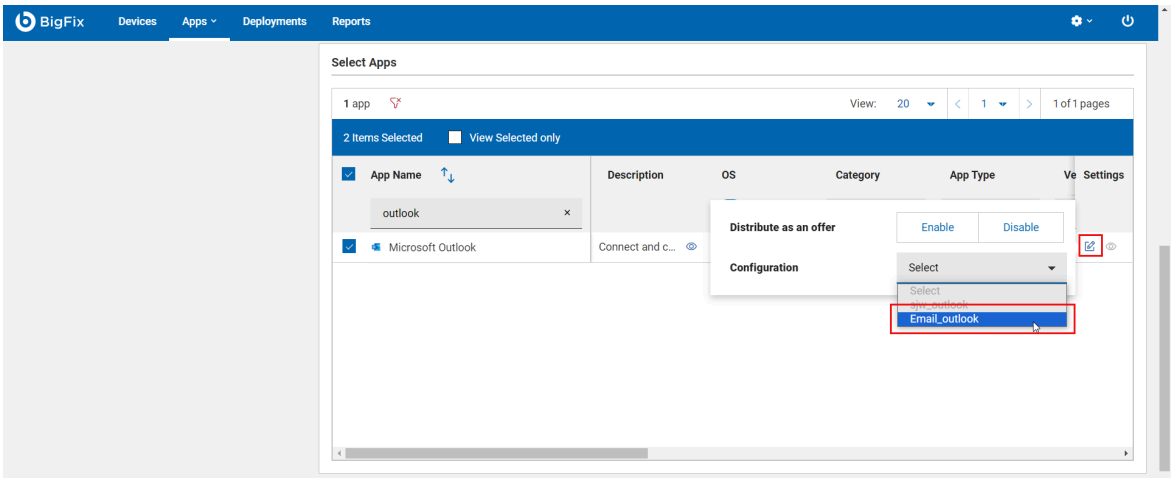
3. **「保存」**をクリックします。

注: 必須情報を入力した後でのみ、保存は有効になります。

指定されたアプリの管理対象設定が保存されます。

保存した管理対象構成を アプリ・デプロイメント・ポリシー (（ページ） 396) に含めるには、次の手順を実行します。

1. アプリ・デプロイメント・ポリシーに管理対象構成があるアプリを選択し、アプリに対応する編集ボタンをクリックします。



2. 「構成」ドロップダウンをクリックし、選択したアプリにアプリ・デプロイメント・ポリシーを使用して適用する管理対象構成の名前を選択します。

注:

- アプリ・ポリシーをデバイスにデプロイする前に、事前構成されたアプリがそのデバイスの仕事用プロファイルでインストールされて構成されていないことを確認します。
- アプリ・ポリシーのデプロイ後、アプリが登録済みターゲット・デバイスにインストールされていることを確認できます。Play ストアまたは App Store からインストールを確認できます。
- アプリ・ポリシーを使用してデプロイされたすべての管理対象プロパティーが、インストール時にサイレント・モードでアプリケーションに設定されていることを確認できます。

Android E メール・アプリの設定

登録済み Android デバイスでの E メール・アプリの構成 (（ページ　　)は、E メール・アプリにリモートで適用できる設定を定義することにより、管理対象構成を通じて行うことができます。

E メール・アプリは、他の Android アプリを配信するのと同じ方法で構成して配信することができます。アプリケーション管理 (（ページ　　) のアプリ配信ワークフローに従ってください。

E メール・アプリをカスタマイズしたり、組織の設定で事前構成したりする場合は、管理対象構成を E メール・アプリに追加できます。管理者は特定の構成を E メール・アプリにプッシュして、デバイスがユーザーの正しい E メール設定でセットアップされていることを確認できます。

E メール・アプリの管理対象構成を追加するには、キーと値のペアとして JSON 形式で構成を入力します。MDM デバッグ・ツールを使用して、Android アプリの管理対象構成を検索できます。

以下は、Android 向けの管理対象構成を使用して、E メール・アプリ設定の JSON 構成を定義する方法の例です。

- **例 1**: 企業メール・アカウントを使用して Android 用 Outlook アプリを構成するための JSON 形式の管理対象構成:

```
{
        "com.microsoft.outlook.EmailProfile.EmailAddress":
 "john.doe@hcl.com",
        "com.microsoft.outlook.EmailProfile.EmailAccountName":
 "John.Doe",
        "com.microsoft.outlook.EmailProfile.ServerHostName":
 "outlook.office365.com",
        "com.microsoft.outlook.EmailProfile.AccountDomain": "hcl"
        "com.microsoft.outlook.EmailProfile.EmailUPN":
 "john.doe@hcl.com",
        "com.microsoft.outlook.EmailProfile.AccountType": "SMTP"
```

```
      }
}
```

- **例 2 :** Gmail アカウントを使用して Android 用 Outlook アプリを構成するための JSON 形式の管理対象構成:

```
{
       "com.microsoft.outlook.EmailProfile.EmailAddress":
"john.doe@gmail.com",
       "com.microsoft.outlook.EmailProfile.EmailAccountName":
"john.doe",
       "com.microsoft.outlook.EmailProfile.ServerHostName":
"smtp.gmail.com",
       "com.microsoft.outlook.EmailProfile.AccountDomain": "gmail",
       "com.microsoft.outlook.EmailProfile.EmailUPN": "MyAccount",
       "com.microsoft.outlook.EmailProfile.AccountType": "SMTP"
     }
```

注: E メール・アプリとして Gmail を使用する場合は、認証のために Google Chrome などのブラウザー・アプリも仕事用プロファイルにデプロイしてください。

Android VPN アプリの設定

VPN アプリにリモートで適用できる管理対象構成を使用して設定を定義することにより、登録済み Android デバイス上の VPN アプリを管理 (（ページ　　)できます。

E メール・アプリは、他の Android アプリを配信するのと同じ方法で構成して配信することができます。アプリケーション管理 (（ページ　　) のアプリ配信ワークフローに従ってください。

Android 用 VPN アプリを構成するには、対象の Android VPN アプリの管理対象構成 (（ページ） 360)のパラメーターを JSON 形式で定義します。以下の基本的な例により、管理対象構成を介した Android VPN 構成 JSON の主要パラメーターについて説明します。

```
{
"portal":"xxxxx-xxx.hcl-software.com",
"username":"example@domain.com",
"password":"*********"
}
```

ここで、

- **Portal:** VPN サーバーの IP アドレスまたはドメイン。
- **username:** VPN プロファイルの一意の識別子。
- **password:** ユーザー名に関連付けられた秘密鍵。

よくある質問

一般的な問い合わせに回答します。

Android アプリのバンドル ID を確認するにはどうすればよいですか

- アプリがアプリ・カタログにある場合、バンドル ID は、 (（ページ）) ページの関連アプリの「バンドル ID」列に表示されます。
- Google Play で Android アプリを検索し、アプリをクリックしてアプリのページを開くこともできます。アプリ ID は、`?id=` の後の URL に表示されます。例えば、Outlook の URL は https://play.google.com/store/apps/details?id=com.microsoft.office.outlook で、バンドル ID は `com.microsoft.office.outlook` です。

Android アプリの管理対象構成のプロパティーを見つけるにはどうすればよいですか?

アプリが管理対象構成をサポートしている場合は、MDM デバッグ (（ページ）)・ツールを使用して管理対象構成プロパティーのリストを検索できます。

デバイスの管理

MDM にデバイスが登録されると、デバイスは WebUI に報告され、**「デバイス」**ページに表示されます。これらの MCM デバイスおよび BigFix モバイル・デバイスの表示、管理、制御には、WebUI の MCM アプリケーションを使用します。

「MCM」ページにアクセスするには、WebUI のメイン・ページから**「アプリ」 > 「MCM」**を選択します。

注: マスター・オペレーターは、 WebUI 権限 (（ページ） *259)*を使用して、ユーザーの MCM アプリケーションへのアクセスを構成できます。BigFix WebUI を介して MCM アプリケーションにアクセス可能で、「アクションの作成が可能」権限と「カスタム・コンテンツを表示可能」権限を持つユーザーのみが、ネイティブの MCM ポリシー (（ページ） *382)*を作成できます。

フル・ディスク暗号化

BigFix MCM を使用すると、Windows (BitLocker) および macOS (FileVault2) からネイティブのフル・ディスク暗号化 (FDE) テクノロジーを一元管理して、保存データを保護できます。

BigFix MCM のフル・ディスク暗号化機能について詳しくは、『フル・ディスク暗号化 (（ページ）)』を参照してください。

フル・ディスク暗号化を構成およびデプロイするためのワークフロー

1. BES サーバー・プラグイン・サービスをセットアップする (BES サポートの Fixlet 708) (（ページ）)
2. リカバリー・キー・エスクローの構成 (（ページ） *371)*
3. ディスク暗号化ポリシーの作成 (（ページ） *431)*
4. FDE ポリシーのデプロイ (（ページ） *375)*

正常性チェック

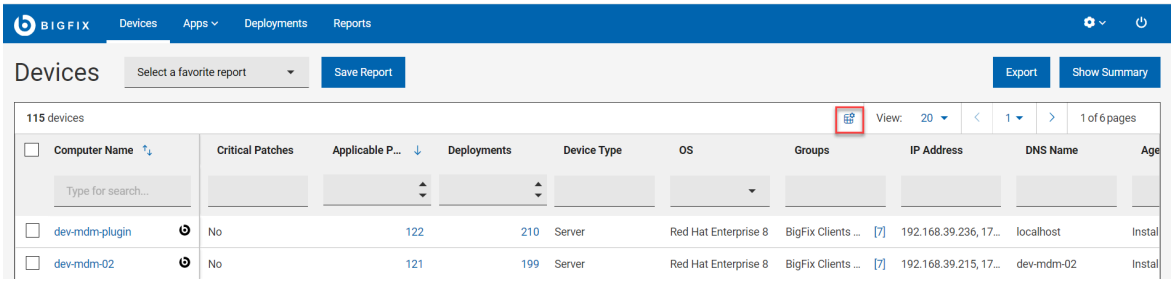
フル・ディスク暗号化を構成した後、「最新のクライアント管理」ページで MDM フル・ディスク暗号化の状況 (（ページ） 268) を表示するには、**「正常性チェック」**をクリックします。

暗号化の状況用の保存済みレポートの作成

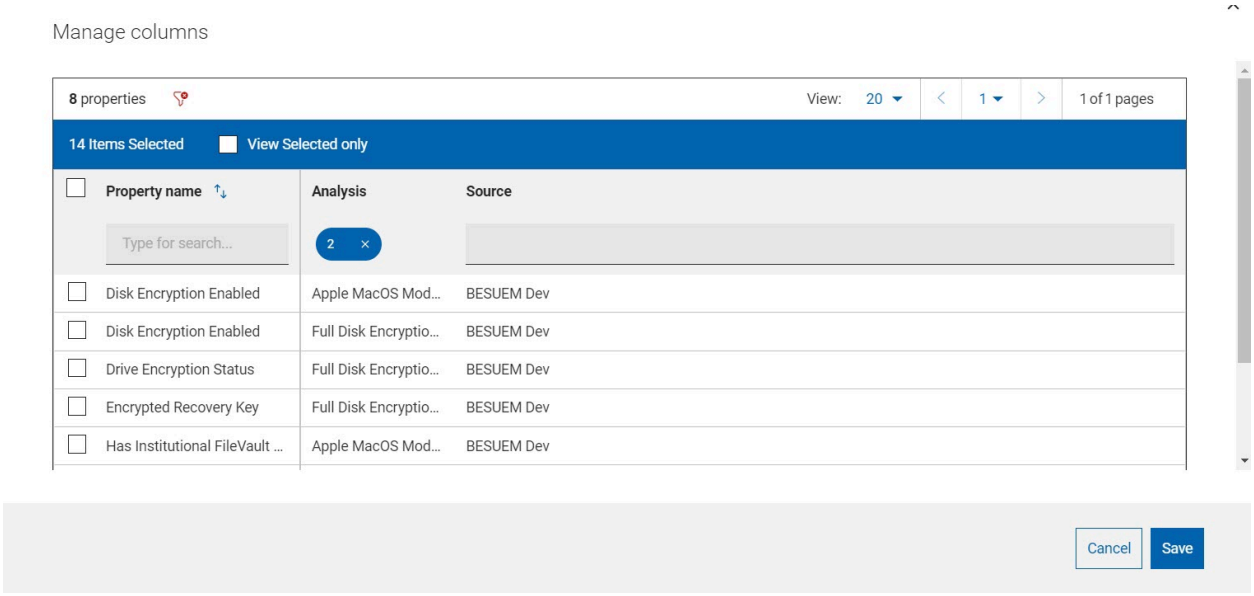
「フル・ディスク暗号化の状況」分析のプロパティーを使用すると、暗号化されていないデバイスやリカバリー・キーがないデバイスなどをフィルタリングで検索できる列を有効にできます。

「フル・ディスク暗号化」固有のデバイス・プロパティーをデバイス・データ・グリッドに含めるには、次の手順を実行します。

1. 「デバイス・リスト」 (（ページ） 22)から、「列の管理」アイコンをクリックします。



2. 「列の管理」ウィンドウで、 「プロパティー名」フィールドまたは 「分析」列でストリングで検索し、 「フル・ディスク暗号化」を選択します。



プロパティー	説明
暗号化	エンドポイントが暗号化されている場合、暗号化されたリカバリー・キーが表示されます。 **注:** エンドポイントが暗号化されているものの、リカバリー・キーが表示されていない場合は、キーの再生成の対象になっている可能性があります。
ドライブ暗号化の状況	ディスク暗号化は、システム・ドライブの全体的な暗号化の状況を示します。
ディスク暗号化の状況	ドライブ暗号化は、Windows のドライブごとの暗号化の状況と方法を示します。
TPM の状況	TPM の状況は、Windows で TPM が検出されたかどうか、および作動可能かどうかを示します。この値は「作動可能」、「作動不能」、「検出されませんでした」です

注:

- プロパティーを選択し、データグリッドの表示方法を構成した後、「デバイス・ページ」の「レポートの保存」 (（ページ） 27)をクリックして、レポートにビューを保存できます。
- レポート名とレポートの説明を入力して保存をクリックすると、グローバル・ナビゲーション・バーの「レポート (（ページ） 16)」の下のビューが使用できるようになり、後で表示および参照できます。

リカバリー・キー・エスクローの構成

キー・エスクローは、重要な暗号化キーを保管する方法です。キー・エスクローを使用することで、組織は、セキュリティー侵害、キーの紛失や忘れ、自然災害などの危機が発生した場合に、重要なキーを安全に復元できるようにすることができます。

次のシナリオでは、リカバリー・キー・エスクローが必要になります。

- デスクサイド・サポート担当者が、壊れたラップトップから新しいラップトップにディスクを移動する場合。
- 従業員の退職後に、安全に保管するために法務局にラップトップを送付する場合。
- ラップトップをリサイクルする場合。

リカバリー・キーのエスクロー構成には、以下のステップが含まれます。

1. 証明書の作成 - WebUI MDM アプリを使用してリカバリー・キーを暗号化するための証明書とキーのペアを作成します。この証明書は、Windows アクションおよび macOS エスクロー・ペイロードで使用されます。キーは、復号化のために BES サーバーのプラグイン・フォルダーに配置されます。
2. Vault の設定 – 既存の Vault サーバー (URL、アクセス キー) を指定するか、自己署名証明書を使用して Vault をデプロイすることもできます。ボールト・ディレクトリーにアクセスして、生成された非 SEAL キーとアクセス・キーを取得し、WebUI でボールト設定を構成できます。

3. エスクロー・プラグインの設定 - プラグインをデプロイするアクションをトリガーし、キーと Vault の詳細を使用して構成して、秘密鍵が BES サーバーの「アプリケーション」ディレクトリーに保管されるようにします。
4. リカバリー・キーをエスクローするための手動デバイス・タスク - リカバリー・キーが見つからないか期限切れになっている場合は、再生成して取得できます。

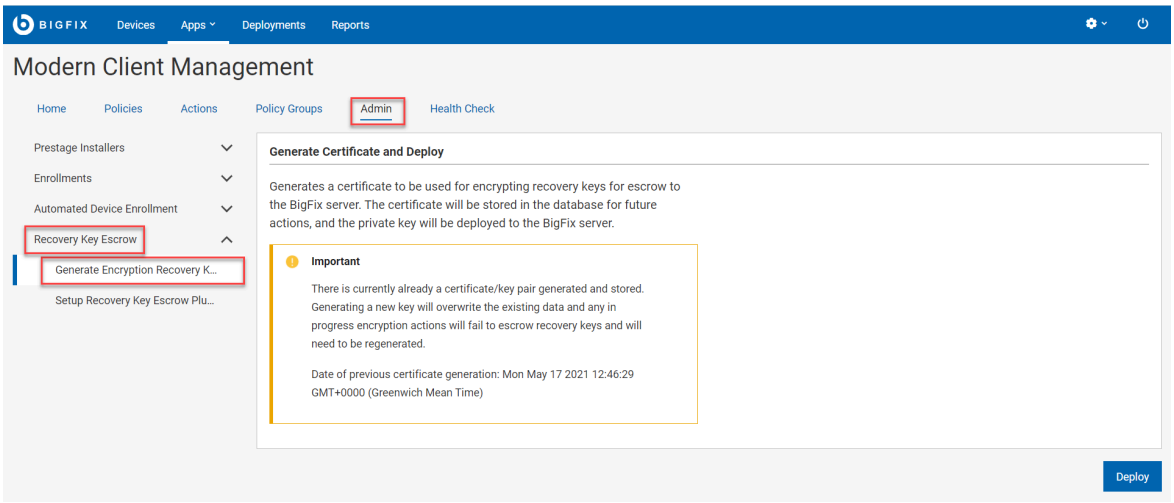
注:

- 設定の続行、起動時にパスワードを入力して暗号化処理を開始、強制再起動後の OS の起動などは、ユーザーの操作が必要になります。
- macOS では、2 次ドライブの暗号化やリムーバブル・ドライブの暗号化の適用はサポートされていません。

暗号化リカバリー・キー・エスクロー証明書の生成

証明書と鍵ペアを生成するには、以下のステップを実行します。

1. WebUI のメイン・ページから、**「アプリケーション」 > 「MCM」 > 「管理者」**をクリックします。
2. **「管理者」**ページで、**「リカバリー・キー・エスクロー」**を展開し、**「暗号化リカバリー・キー・エスクロー証明書の生成」**をクリックします。
3. 次の画面で**「導入」**をクリックします。



。

これで、リカバリー・キーの作成に使用される証明書と鍵ペアが生成され、今後のアクションのために WebUI データベースに保管されます。鍵は、Windows または macOS の暗号化ポリシーのデプロイ時に使用されます。

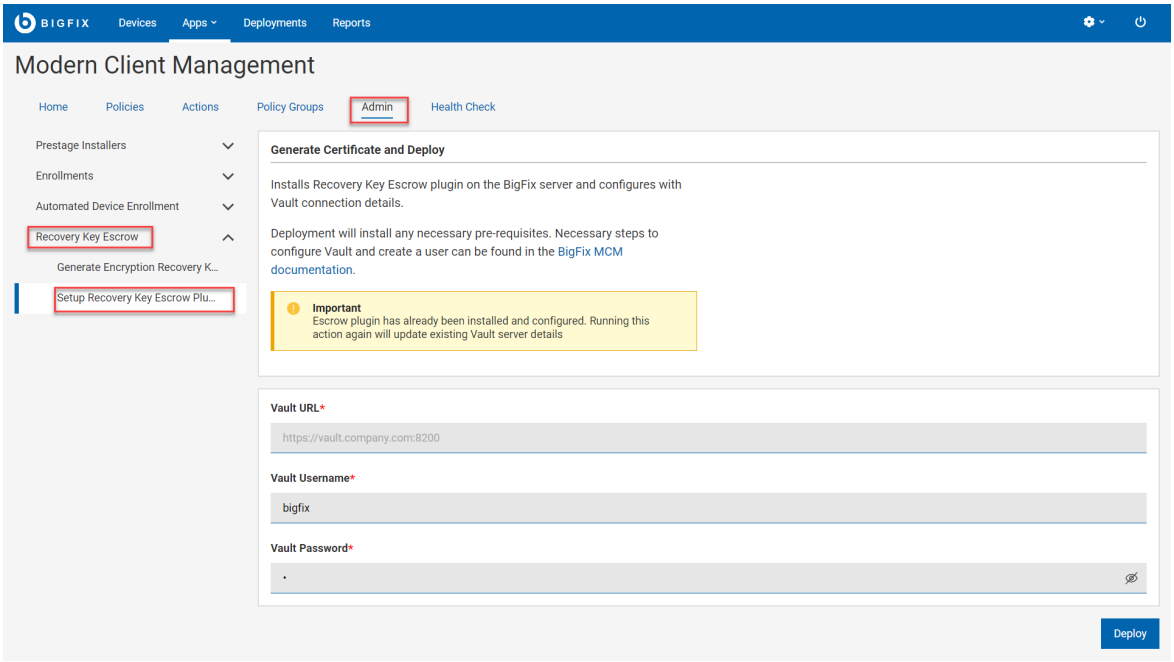
重要: このページから証明書と鍵ペアを再生成することもできます。ただし、新しいキー・セットを生成すると悪影響があります。進行中の暗号化アクションは、古い証明書を使用して暗号化するため、リカバリー・キーのエスクローに失敗します。これを回避するには、MacOS のフル・ディスク暗号化ポリシーを再デプロイすることをお勧めします。これは、今後のリカバリー・キーの更新または再生成のためにデバイスに保存されているエスクロー証明書を更新するためです。

Recovery Key Escrow プラグインのセットアップ

BES Server Plugin Service (（ページ）　　)が既にインストールされていることを確認します。

BES サーバーに暗号化プラグインをインストールするには、以下のステップを実行します。

1. WebUI のメイン・ページから、**「アプリ」 > 「MCM」**をクリックします。
2. 「Modern Client Management」ページで、**「管理者」**をクリックします。
3. 次の画面から、**「リカバリー・キー・エスクロー」 > 「Recovery Key Escrow プラグインのセットアップ」**を選択します。



4. **前に設定**した「bigfix」シークレット・エンジンへの書き込みアクセス権限を持つ**「Vault URL」**、**「Vault ユーザー名」**、「Vault パスワード」 (（ページ）)を入力します。
5. **「デプロイ」**をクリックします。

デフォルトでは、Recovery Key Escrow プラグインは、安全なシークレット・リポジトリーであるため、Vault (https://www.hashicorp.com/products/vault) と対話しようとします。正しく機能させるには、リカバリー・キーの保存と取得のために Vault を個別に構成する必要があります。詳しくは、「Vault のセットアップ (（ページ）)」を参照してください。
構成が完了すると、Vault への特定のアクセス権を持つユーザーは、適切にエスクローされたすべてのキーのリカバリー・キーを取得できます。

注: Vault へのユーザー・アクセスは、BigFix ユーザーとオペレーターとは別であり、個別に構成する必要があります。

フル・ディスク暗号化ポリシーを作成する方法については、「ディスク暗号化ポリシー (（ページ） 431)」を参照してください。

FDE ポリシーのデプロイ

作成した FDE ポリシーをデプロイするには、以下のステップを実行します。

1. 「デバイス」ページから 1 つ以上のデバイスを選択し、**「適用」 > 「MDM ポリシー」**をクリックします。
2. 「ポリシーのデプロイ」ページで、必要に応じてオプションを選択します。「デバイスをすぐに再起動する」オプションを選択すると、エンド・ユーザーの再起動動作に関係なく、エンドポイントが再起動されます。
3. Windows オプション: Windows の場合、通知の表示がデフォルトです。「通知の表示」を選択しなければ、このアクションの実行直後にエンドポイントが再起動します。

暗号化リカバリー・キーの再生成

Windows または macOS デバイスの暗号化リカバリー・キーを再生成する方法について説明します。

リカバリー・キーを再生成するには、BigFix エージェントがアクションを実行する必要があり、MDM のみで実行することはできません。Mac デバイスでは、リカバリー・キーを再生成するために、特権ユーザーのユーザー名とパスワードを入力するように求めるプロンプトが、ユーティリティーからデバイス・ユーザーに表示されます。

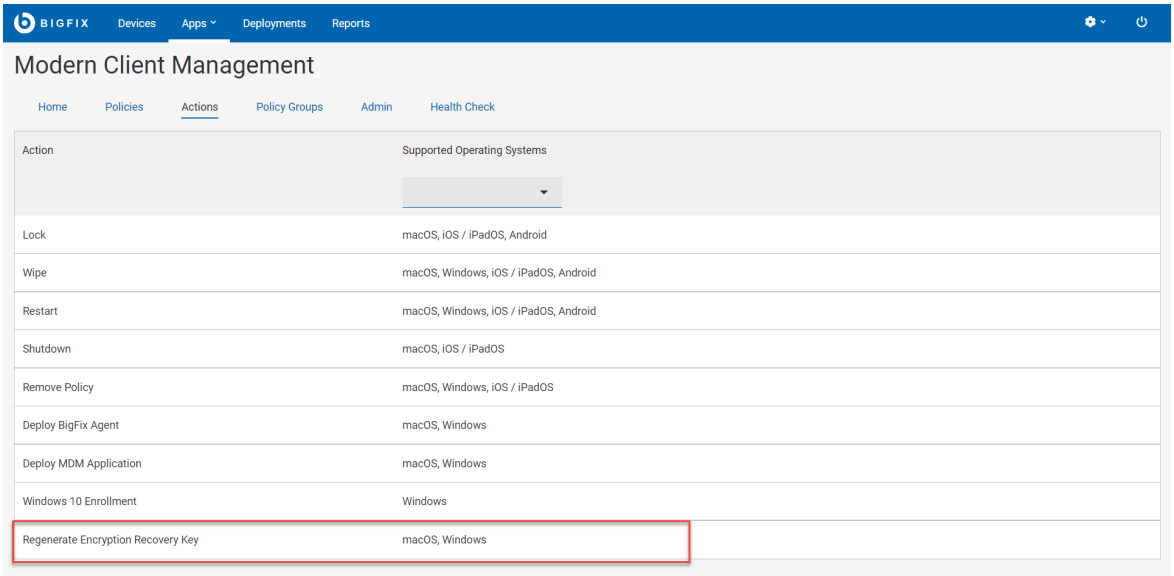
Mac デバイスでは、リカバリー・キーを再生成するために、特権ユーザーのユーザー名とパスワードを入力するように求めるプロンプトが、小規模なユーティリティからエンドユーザーに表示されます。

エスクローされたリカバリー・キーを取得するには、オペレーターまたはサポート担当者が Vault サーバー・インターフェースに直接ログインする必要があります (提供されている

Fixlet を使用して Vault を設定している場合は、作成された読み取りユーザーを使用できます)。「bigfix」シークレット・エンジンにはリカバリー・キーが含まれています。リカバリー・キーは、BigFix コンピューター ID、コンピューター名、最後にログインしたユーザーに基づいて ID で保管され、Vault インターフェースで検索できます。ボールト内のエントリー名には、リカバリー・キーがエスクローされた時点の値が含まれています。

フル・ディスク暗号化リカバリー・キーを再生成するには、次の手順を実行します。

1. WebUI で**「アプリケーション」 > 「MCM」**をクリックします。
2. 「Modern Client Management」ページで**「アクション」**をクリックします。
3. 使用可能なアクションのリストで、**「暗号化リカバリー・キーの再生成」**をクリックします。



4. 次のページで**「デバイスの編集」**をクリックして、対象の Windows または macOS デバイスを選択します。
5. 選択した内容を確認して**「適用」**をクリックします。

MCM ポリシーのデプロイ

MCM ポリシーをデプロイすると、管理者は MCM デバイスを構成および管理できます。

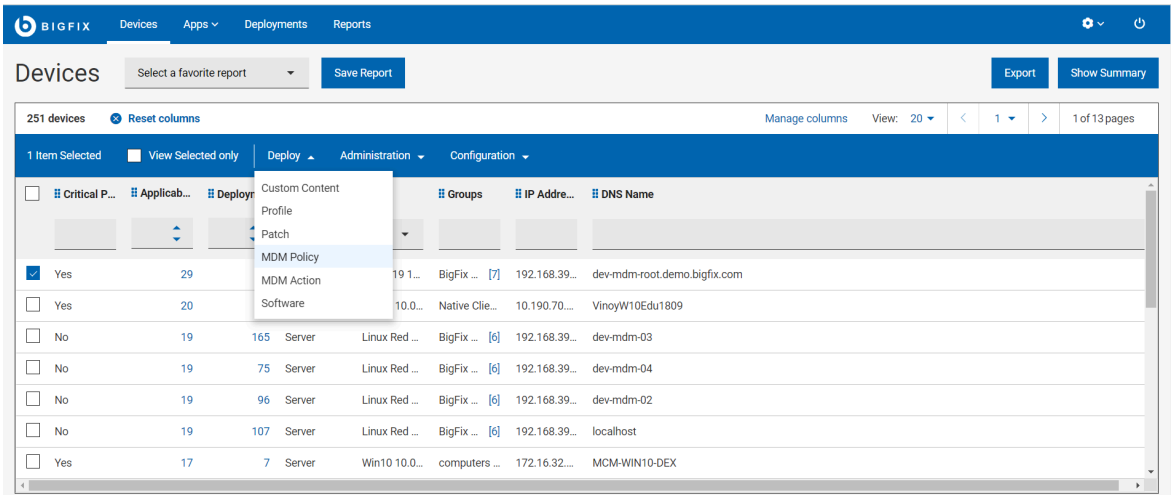
注:

- マスター・オペレーターはすべてのアクションを実行できます。次の注意事項は、マスター・オペレーター以外のユーザーにのみ適用されます。
  - BigFix WebUI 経由で MDM アプリケーションにアクセスできるユーザーのみ、MDM ポリシーをデプロイできます。マスター・オペレーターは、「WebUI 権限」 (（ページ） 259)サービスを使用してアクセス許可を構成できます。
  - マスター以外のオペレーターが「非カスタム・ポリシーの作成、編集、削除」権限を持っている場合のみ、ネイティブの MDM ポリシー (カーネル拡張、パスコード・ポリシー、証明書ポリシー、制限ポリシー、フル・ディスク・アクセス) を作成できます。
  - BigFix コンソールで「アクションの作成が可能」権限を持つユーザーのみ、MDM ポリシーをデプロイできます。これらのユーザーは、ポリシーの参照/編集/デプロイに関わる BigFix カスタム・サイトの権限も必要です。ポリシーがマスター・アクション・サイトで作成されている場合は必要ありません。権限について詳細は、「MDM 権限 (（ページ） 259)」を参照してください。
  - MDM ポリシーは MDM が管理するエンドポイントにのみデプロイできます。MDM 以外のデバイスを含むデバイス・グループに MDM ポリシーをデプロイすると失敗します。
  - WebUI はアクションが正しいデバイス・タイプに適用されていない場合、そのアクションの生成を行いません。例えば、MDM ポリシーをネイティブの BigFix エージェント・デバイスまたはクラウド・デバイスにデプロイすることを WebUI は阻止します。
  - MDM ポリシーをネイティブの BigFix 表記と MDM 表記両方の相関デバイスにデプロイしようとすると、MDM ポリシーは MDM デバイスにのみデプロイされます。

以下のステップに従い、MDM ポリシーをデプロイします。

1. **「デバイス」**リストに移動します。
2. MDM ポリシーをデプロイするデバイスを 1 つ以上選択します。
3. **「デプロイ」**ボタンをクリックします。

4. **「MDM ポリシーのデプロイ」**をドロップダウン・リストから選択します。



5. **「ポリシーの編集」**をクリックして、デプロイするポリシーを選択します。
6. **「デプロイ」**をクリックし、選択したデバイスに MDM ポリシーをデプロイします。

注: マスター以外のオペレーターは、デプロイするためにポリシーが作成されたサイトを表示できる必要があります。マスター以外のオペレーターがこのデプロイメント・ワークフローで正しい MDM ポリシーを表示できない場合は、BigFix サイト権限を確認する必要があります。

関連情報

ポリシーの管理 ((ページ) *382)*

BigFix エージェントのデプロイ

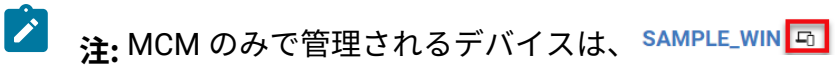
BigFix agent をデバイスにデプロイすることで、BigFix 管理者はそれらのデバイスで BigFix の全機能を使用できます。

重要: BigFix agent は、macOS および Windows デバイスにのみインストールできます。BigFix agent は、iOS、iPadOS、Android デバイスにはインストールできません。さらに、BigFix エージェントのデプロイを実行する前に、macOS および Windows の BigFix エージェントのインストール・パッケージを MDM サーバーに事前にステージングする必要があります。事前にステージングする方法については、『macOS BigFix インストーラーの事前ステージ (（ページ） 355)』および『Windows BigFix インストーラーの事前ステージ (（ページ） 357)』を参照してください。

- マスター・オペレーターは、MCM デバイスに BigFix agent をデプロイできます。
- 「WebUI を使用できます」、「アクションの作成が可能」、「カスタム・コンテンツ」権限を持つマスター以外のオペレーター (NMO) は、MCM デバイスに BigFix agent をデプロイできます。

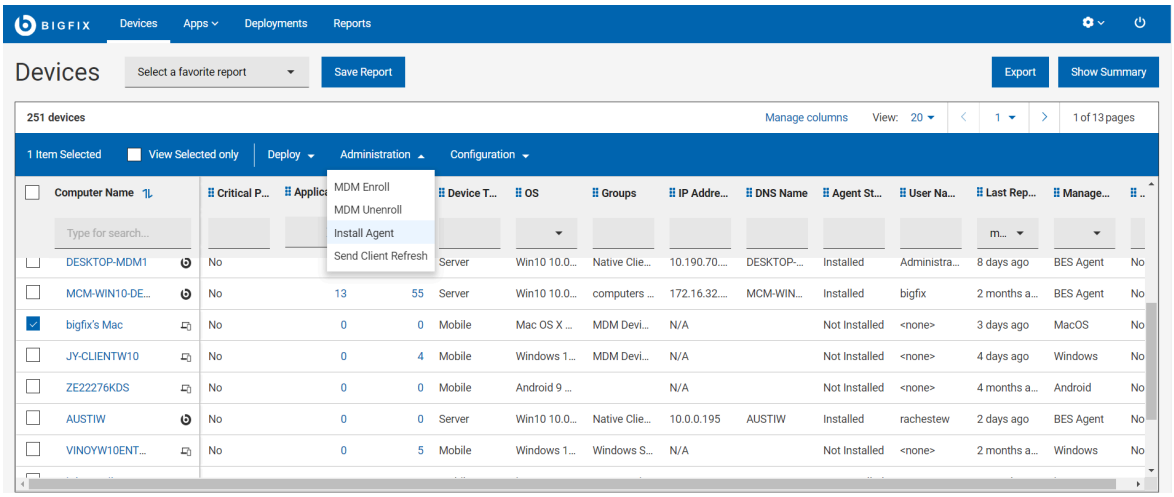
BigFix agent をデプロイするには、次の手順を実行します。

1. MCM のみで管理される macOS または Windows デバイスを 1 つ以上選択します。(デバイス・リストから、**「エージェント・ステータス」 > 「いいえ」** フィルターを使用して、BigFix agent がインストールされていないデバイスをフィルターできます。

   注: MCM のみで管理されるデバイスは、 

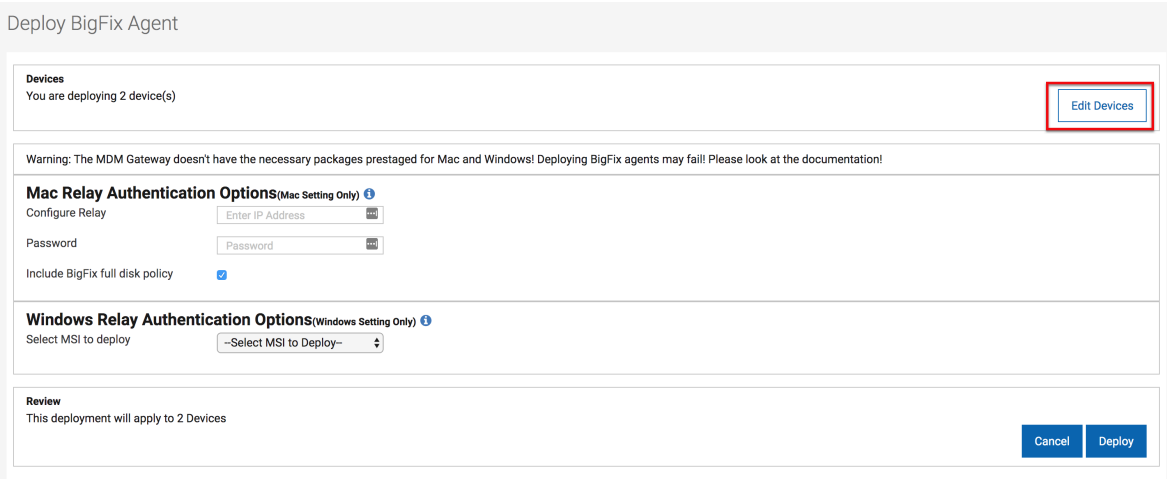
   の MCM の記号が横に表示されます。

2. 青色のアクション・バーから、**「管理」 > 「エージェントのインストール」**をクリックしま



す。

3. デバイスを追加または削除するには、**「BigFix エージェントのデプロイ」**ページで、**「デバイスの編集」**をクリックします。



4. リレー認証オプションを設定します。
    a. **Mac リレー認証オプション**: このセクションは、Mac エンドポイントが選択されている場合に表示されます。
        - **リレーの設定**: IP アドレスまたは DNS 名を入力します。
        - **パスフレーズ**: パスフレーズを入力します。
        - **BigFix フル・ディスク・ポリシーを含める**: BigFix にフル・ディスク・アクセス権を付与するには、このチェックボックスをオンにします。

b. **Windows リレー認証オプション**: このセクションは、Windows エンドポイントが選択されている場合に表示されます。
   - **デプロイする MSI の選択**: このリストから、MDM サーバーで事前にステージングした msi ファイルを選択します。

5. BigFix エージェントをデプロイするには、**「デプロイ」**をクリックします。

注:

- アクションが完了すると、MDM と BigFix エージェントの両方がデバイスを管理できるようになります。
- リレー設定時に入力した IP アドレスとパスフレーズは、MacOS MDM エンドポイントでのみ使用されます。Windows MDM デバイスの場合は、事前にステージングされ、MSI の一部として既にリレー認証がついた MSI が必要です。
- BigFix エージェントのデプロイは、BigFix エージェントのインストーラーが MDM サーバーに事前にステージングされている場合のみ機能します。BigFix WebUI には macOS の場合は 1 つ以上の .pkg ファイル、Windows™ デバイスの場合は 1 つの .msi ファイルが必要です。インストール・パッケージが MDM サーバーにない場合、ユーザーは BigFix エージェントのアクションは失敗しますという警告を受信します。WebUI は、デフォルトでは、MDM サーバーの `/var/opt/BESUEM/packages` フォルダー内の .msi ファイルと .pkg ファイルをチェックして、BigFix エージェント・パッケージが正しく事前にステージングされているかどうかを確認します。

関連資料

BigFix エージェントのデプロイメント (（ページ）)

関連情報

macOS BigFix インストーラーの事前ステージ (（ページ） *355)*

Windows BigFix インストーラーの事前ステージ (（ページ） *357)*

ポリシーの管理

BigFix WebUI を使用して、Windows、Apple (macOS/iOS/iPadOS)、Android デバイスに固有のポリシーを作成および管理できます。

ユーザーの権限と機能

MCM アプリケーションを表示するための WebUI 権限を持ち、カスタム以外のポリシーを作成、編集、および削除する機能を持つマスター・オペレーターおよびマスター以外のオペレーターは、WebUI を介して次のポリシーを管理できます。

- App Store アプリ・ポリシー (（ページ）)
- 証明書ポリシー (（ページ） *402)*
- テンプレートからカスタム (（ページ） *403)*
- ディスク暗号化ポリシー (（ページ） *431)*
- フル・ディスク・アクセス (（ページ） *435)*
- カーネル拡張ホワイトリスト (（ページ） *436)*
- キオスク・ポリシー (（ページ） *439)*
- OS の更新ポリシー (（ページ） *443)*
- パスコード・ポリシー (（ページ） *446)*
- 制限ポリシー (（ページ） *451)*
- システム拡張ホワイトリスト (（ページ） *454)*
- カスタム・ポリシー (（ページ） *458)*

カスタム・ポリシー

MDM カスタム・ポリシーを作成、編集、および削除する権限を持つユーザーには、カスタム・ポリシーを作成できる追加オプションが表示されます。

マスター・オペレーター

DEP (デバイス登録プログラム) と ディスク暗号化ポリシー (（ページ） 431) ポリシーを管理する権限を持つのは、マスター・オペレーターのみです。

マスター以外のオペレーター

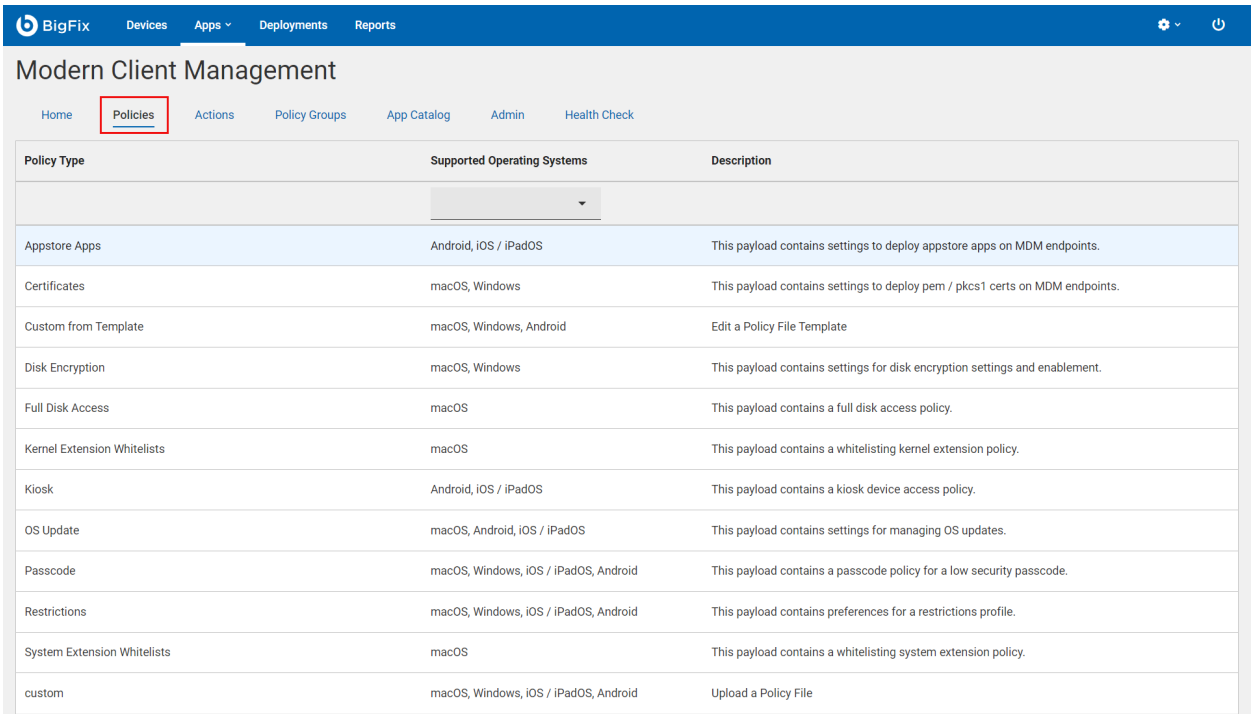
MCM と BigFix Mobile のポリシーとアクションを管理するには、マスター以外のオペレーターには次の権限が必要です。

- MCM カスタム・ポリシーおよび非カスタム・ポリシーを作成、編集、削除 (（ページ） *259)*するための適切な権限
- MCM アクションとポリシーを配置するために BigFix コンソールで設定された「Can Create Actions」および「Custom Content」権限
- マスター以外のオペレーター (NMO) が、「サイトへのポリシーの割り当て」ドロップダウン・メニューでカスタム・サイトを表示し、MDM ポリシーをリンクするには、少なくとも 1 つのカスタム・サイトに対する Writer 権限を持っている必要があります。
- NMO が BESUEM サイトのポリシーの正確なデバイス・カウントにアクセスするには、Reader 権限を持っているか、Reader 権限を持つ役割の一部である必要があります。

> **注:** カスタム・サイトを作成して権限を割り当てる方法については、「カスタム・サイトの作成」を参照してください。

WebUI で構成可能なポリシー

BigFix WebUI を使って構成できるポリシーを次に示します。



特定のポリシー・タイプは、オペレーティング・システムに固有です。各ポリシー・タイプの下には、適用されるオペレーティング・システムのロゴが表示されてユーザーに通知されます。複数のロゴが見つかった場合、それらのロゴに固有のポリシーを複数のオペレーティング・システムに適用できることを示しています。

ポリシー・タイプ	スコープ	使用可能な OS
パスコード・ポリシー (（ページ） *446)*	低セキュリティー要件のパスコード・ポリシーの作成	macOS / iOS / iPadOS、、Android
カーネル拡張ホワイトリスト (（ページ） 436)	macOS カーネルにコードを動的にロードするための、カーネル拡張ホワイトリスト・ポリシーの作成	macOS
フル・ディスク・アクセス (（ページ） *435)*	ディスク・スペースを暗号化するポリシーの作成	macOS

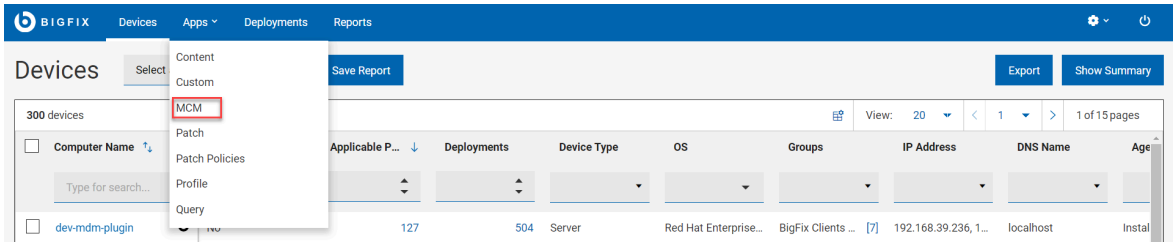
ポリシー・タイプ	スコープ	使用可能な OS
カスタム・ポリシーのアップロード (（ページ） *458)*	カスタム・ポリシーの作成	macOS / iOS / iPadOS、、Android
制限ポリシー (（ページ） *451)*	制限ポリシーの作成	macOS / iOS / iPadOS、、Android
証明書ポリシー (（ページ） *402)*	証明書ポリシーの作成	macOS、
ディスク暗号化ポリシー (（ページ） *431)*	ディスク暗号化を適用するポリシーの作成	macOS、
App Store アプリ・ポリシー (（ページ）)	MDM エンドポイントにアプリ・ストアのアプリをデプロイするポリシーの作成	iOS / iPadOS、Android
OS の更新ポリシー (（ページ） *443)*	OS 更新を管理するポリシーの作成	iOS / iPadOS、Android

注:

- 対象デバイスに同じタイプの複数の非カスタム・ポリシーをデプロイすることはできません。
- 対象デバイスに複数のカスタム・ポリシーを一度にデプロイできます。

ポリシー作成の手順:

ポリシーを作成するには、次の手順を実行します。

1. MCM アプリを開きま


す。
2. **「ポリシーの作成」**をクリックしま


す。
3. ポリシーがリストされているページで、 「サポートされるオペレーティング・システム」を選択して、選択したオペレーティング・システムでサポートされているポリシー・タイプのみを表示します。フィルターされたリストから、作成するポリシー・タイプを選択します。

ポリシー・グループ

ポリシー・グループを使用すると、ポリシー、アプリケーション、BigFix エージェントを単一のグループに結合し、MDM サーバーまたは登録済みデバイスにデプロイできます。

オペレーティング・システムに固有の登録タイプを割り当てて、MDM サーバーにデプロイすることができます。デプロイされたポリシー・グループ内のポリシーは、それらの特定のデバイスのデフォルト登録ポリシーになります。

オペレーティング・システムに固有の登録タイプを割り当て、適用可能なデバイスにデプロイして、デフォルトの登録ポリシーをオーバーライドできます。

ポリシー・グループには、以下を含めることができます。☒

- MDM ポリシー (パスコード・ポリシー (（ページ） *446)*、 制限ポリシー (（ページ） *451)*、証明書ポリシー (（ページ） *402)*、App Store アプリ・ポリシー (（ページ）)、カーネル拡張ホワイトリスト (（ページ） *436)*、フル・ディスク・アクセス (（ページ） *435)*、カスタム・ポリシー (（ページ） *458)*)

  注: OS の更新ポリシー (（ページ） *443)* iOS 向けおよび Windows 向けディスク暗号化ポリシー (（ページ） *431)*の場合、ポリシー・グループではサポートされません)

- 事前ステージングされたアプリケーション (（ページ）)
- BigFix エージェント (（ページ） 379)

始める前に: 作成、ポリシーとアプリケーションの追加、削除、デプロイなどのポリシー・グループ関連タスクを実行するには、マスター・オペレーターである必要があります。マスター以外のオペレーターは、ポリシー・グループに含めるポリシーのみを作成できます。

ポリシー・グループの処理

- ポリシー・グループの作成 (（ページ） *387)*
- ポリシー・グループのデプロイ (（ページ） *392)*
- ポリシー・グループをスマート・グループに関連付けます
- ポリシー・グループの編集 (（ページ） *395)*
- ポリシー・グループの削除 (（ページ） *395)*

ポリシー・グループの作成

ポリシー・グループを作成するには、以下のようにします。

1. BigFix WebUI のメイン・ページから、**「アプリケーション」 > 「MDM」**をクリックします。
2. Modern Client Management のホームページで、**「ポリシー・グループ」**をクリックします。
3. **「ポリシー・グループ」** ページで、 **「 ポリシー・グループの作成」**をクリックします。

4. **「ポリシー・グループの作成」** ページで、以下を実行します。
   a. **「ポリシー・グループ名」** と **「説明」** を入力します。
   b. OS を選択します。
   c. **グループに割り当てます**。このポリシー・グループを MDM サーバーにデプロイする場合、「グループに割り当て」は、このポリシー・グループ内で定義されたポリシーおよびアプリケーションを取得するために適用可能な登録デバイスのタイプを指定します。

   注: ここでグループを割り当てない場合、このポリシー・グループは、既に登録されている 1 つ以上のデバイスまたは BigFix デバイス・グループにのみデプロイできます。登録時に、デバイスは割り当てられていないポリシー・グループからポリシーとアプリケーションを取得しません。

   以下に、使用可能な登録グループを示します。

オペレーティング・システム	登録グループ
Android	• 作業プロファイル登録: このポリシー・グループを BYOD Android デバイスに割り当てます。新規登録時に、BYOD Android デバイスはこのグループに追加されたポリシーを受け取ります。 • 完全管理対象登録: このポリシー・グループを完全管理対象 Android デバイスに割り当てます。新規登録時に、フルマネージド Android デバイスは、このグループに追加されたポリシーを受け取ります。 • 専用デバイス登録: このポリシー・グループを専用 Android デバイスに割り当てます。新規登録時に、専用 Android デバイスは、このグループに追加されたポリシーを受け取ります。

オペレーティング・システム	登録グループ
	注: Android の場合、ポリシー・グループ機能を介してのみポリシーをプロビジョンできます。どのポリシー・グループにも直接追加されていない個々のポリシーを、MDM サーバーまたは登録済みデバイスに直接プロビジョニングすることはできません。
IOS	• 無線経由の登録: このポリシー・グループを、無線経由で登録されている iOS デバイスに割り当てます。新規登録時に、無線経由登録された iOS デバイスは、このグループに追加されたポリシーを受け取ります。 • ユーザー登録 (BYOD): このポリシー・グループを BYOD iOS デバイスに割り当てます。新規登録時に、BYOD iOS デバイスはこのグループに追加されたポリシーを受け取ります。 • 自動デバイス登録: このポリシー・グループを、自動デバイス登録によって登録された iOS デバイスにを割り当てます。
iPadOS	• 無線経由の登録: ポリシー・グループ内のポリシーを、無線経由で登録されているすべての iPadOS デバイスにデプロイします。新規登録時に、無線経由で登録された iPadOS デバイスは、このグループに追加されたポリシーを受け取ります。 • ユーザー登録 (BYOD): このポリシー・グループを BYOD iPadOS デバイスに割り当てます。新規登録時に、BYOD

オペレーティング・システム	登録グループ
	iPadOS デバイスはこのグループに追加されたポリシーを受け取ります。 • 自動デバイス登録: ポリシー・グループ内のポリシーを、自動デバイス登録によって登録されるすべての iPadOS デバイスにデプロイします。
macOS	• 無線経由の登録: ポリシー・グループ内のポリシーを、無線経由で登録されているすべての macOS デバイスにデプロイします。新規登録時に、無線経由で登録された macOS デバイスは、このグループに追加されたポリシーを受け取ります。 • ユーザー登録 (BYOD): このポリシー・グループを BYOD macOS デバイスに割り当てます。新規登録時に、BYOD macOS デバイスはこのグループに追加されたポリシーを受け取ります。 • 自動デバイス登録: ポリシー・グループ内のポリシーを、自動デバイス登録によって登録されるすべての macOS デバイスにデプロイします。
Windows	• 無線経由の登録: ポリシー・グループ内のポリシーを、無線経由で登録されているすべての Windows デバイスにデプロイします。 • 一括登録: ポリシー・グループ内のポリシーを、一括登録によって登録されるすべての Windows デバイスにデプロイします。 • Autopilot 登録: ポリシー・グループ内のポリシーを、Autopilot 登録によって登録されるすべての Windows デバイスにデプロイします。

5. アプリケーションまたはポリシーを追加するには、左側のナビゲーションペインで、目的の項目の横にある「+」記号をクリックします。次に、目的のポリシーまたはアプリケーション (あるいはその両方) を選択します。**「保存」**をクリックして変更を保存してから、モジュールを閉じます。
   - **ポリシーの追加**: このオプションを使用すると、ユーザーはポリシー・グループにポリシーを追加できます。リストされたポリシーは、ポリシー・グループの選択されたオペレーティング・システムによって事前にフィルタリングされます。リストからポリシーを選択し、「OK」をクリックしてそのポリシーをポリシー・グループに追加します。異なるタイプの複数のポリシーを追加できます。矛盾するポリシーを追加しないようにしてください。特定のポリシー (パスコード・ポリシー、制限ポリシーなど) の場合、そのタイプのポリシーはポリシー・グループに 1 つのみ追加できます。

     注: グループ・ポリシーを保存する前に、追加したポリシーを削除する場合は、ポリシー・リストに戻り、削除するポリシーの選択を解除します。

     重要: Android 専用デバイスの場合は、 キオスク・モード (（ページ）) 設定を持つポリシーをポリシー・グループに追加してください。それ以外の場合、専用デバイスは、フルマネージド・デバイスとして機能します。

   - **アプリケーションの追加** (macOS および Windows のみ): このオプションを使用すると、ユーザーは事前ステージングされたアプリケーションをポリシー・グループに追加できます。リストされたアプリケーションは、ポリシー・グループの選択されたオペレーティング・システムによって事前にフィルタリングされます。1 つ以上のアプリケーションを選択し、「OK」をクリックしてポリシー・グループに追加します。

     重要: このページからアプリケーションを追加できるのは、Mac ポリシー・グループと Windows ポリシー・グループのみです。Android、iOS、または iPadOS デバイスにアプリケーションを追

加するには、 を App Store アプリ・ポリシー (（ページ）) 作成し、 **「ポリシーの追加」**を介してポリシー・グループに 追加する必要があります。

- **BigFix エージェントの追加** (MCM のみ): このリストには、選択した OS で使用可能なすべての事前ステージング済み BigFix エージェント・バージョンがリストされます (Windows および macOS のみ)。

6. 現在選択されているポリシーをポリシー・グループに保存するには、右下の **「保存」** ボタンをクリックしてポリシー・グループを保存します。

注: 少なくとも 1 つのポリシーと 1 つのアプリケーションをポリシー・グループに追加していることを確認してください。アプリケーションまたはポリシーを選択せずにポリシー・グループを保存しようとすると、WebUI は少なくとも 1 つのポリシーまたはアプリケーションを追加するよう求めるプロンプトを出します。

結果: ポリシー・グループが作成され、ポリシー・グループにリストされます。作成されたポリシーがデータ・グリッドに表示されます。必要に応じてフィルタリングしてソートし、特定のポリシー・グループを見つけることができます。

ポリシー・グループのデプロイ

ポリシー・グループを MDM サーバーにデプロイして、登録時にポリシー・グループのコンテンツを適用可能なデバイスにプッシュできます。ポリシー・グループのコンテンツを、既に登録されているデバイスに直接デプロイすることもできます。

デフォルト・ポリシー - MDM サーバー上のポリシー・グループのデプロイ

ポリシー・グループを MDM サーバーにデプロイすることで、デバイスの登録時にポリシー・グループの内容が自動的に取得されます。ポリシー・グループは、特定のオペレーティング・システム (Android、iOS、iPadOS、macOS、Windows) および特定の MDM 登録タイプ (OTA、DEP、一括登録、Autopilot 登録、BYOD 登録、完全管理対象登録など) をターゲットにできます。

ポリシー・グループを MDM サーバーにデプロイするには、以下のようにします。

1. **「ポリシー・グループ」**ページから、ポリシー・グループを選択します。青いアクション・バーが表示されます。
2. **「デプロイ」**ドロップダウンから、 **「MDM サーバー上」**を選択します。
3. スマート・グループをポリシー・グループに関連付ける場合は、次のページで**「スマート・グループの編集」**をクリックし、スマート・グループ (（ページ） *318)* を選択します。
4. 選択したスマート・グループとポリシー・グループを確認し、**「デプロイ」**をクリックします。

結果:

- これにより、BigFix 環境内のすべての MDM サーバーにポリシー・グループがデプロイされます。
- MDM サーバーにポリシー・グループをデプロイするときに スマート・グループ (（ページ） *318)* を選択した場合、登録時に、MDM サーバーにデプロイされたポリシー・グループの内容が、指定したオペレーティング・システム、登録タイプ、スマート・グループ定義 (（ページ） *329)*に従って、デフォルトのポリシーとして適格なデバイスにデプロイされます。

注:

- デバイスまたは MDM サーバーに一度にデプロイできるポリシー・グループは 1 つのみです。ただし、「DMD サーバーへのポリシー・グループのデプロイ」を複数回実行することで、異なるオペレーティング・システムおよび登録グループに影響を与えるポリシー・グループをデプロイできます。特定のオペレーティング・システムと登録グループの組み合わせの最新のポリシー・グループは、登録時に有効になります。例:

- macOS の無線経由の登録ポリシー・グループ「ファースト・ポリシー・グループ」を作成して MDM サーバーにデプロイすると、新しく登録された OTA macOS デバイスは「ファースト・ポリシー・グループ」のコンテンツを取得します。☒

  。
- その後、macOS の無線経由の登録ポリシー・グループ「セカンド・ポリシー・グループ」を作成して MDM サーバーにデプロイすると、新しく登録された OTA macOS デバイスは「セカンド・ポリシー・グループ」のコンテンツを取得します。
- 「ファースト・ポリシー・グループ」と「セカンド・ポリシー・グループ」の両方を一度に選択して、MDM サーバーにデプロイすることはできません。一度にデプロイできるのは 1 つのみです。

登録済みデバイスのポリシーの更新 - ポリシー・グループ・アクション

選択したデバイスまたはデバイス・グループにポリシー・グループをデプロイすることにより、登録済み MDM デバイスのポリシーを更新できます。

注: ポリシー・グループの作成中に登録タイプを選択しない場合は、そのポリシー・グループを選択した適用可能なデバイスまたはデバイス・グループにデプロイできます。

選択した適用可能なデバイスまたはデバイス・グループにポリシー・グループをデプロイするには、以下のようにします。

1. **「ポリシー・グループ」** ページから、ポリシー・グループを選択します。青いアクション・バーが表示されます。
2. **「ポリシー・グループ・アクション」**をクリックします。

3. 「ポリシー・グループのデプロイ」ページで、 **「デバイスの編集」** をクリックして、デバイスまたはデバイス・グループを選択します。
4. 選択したポリシーとデバイスを確認し、**「デプロイ」**をクリックします。

結果: これにより、環境内のすべての MDM サーバーにポリシー・グループがデプロイされます。

重要: 専用 Android デバイス: 登録後、ポリシー・グループがデプロイされると、デプロイされたポリシー・グループ内のポリシーが以前のポリシー (存在する場合) を上書きします。

スマート・グループとポリシー・グループの関連付け

スマート・グループ (（ページ） *318)* をポリシー・グループに関連付けると、ポリシーは、スマート・グループで定義された条件 (Active Directory グループ (（ページ） *322)*のプライマリー・ユーザー・メンバーシップ、Active Directory ユーザー属性ルール、デバイス属性ルール (（ページ） *324)*など)、および OS タイプと登録タイプに基づいてデプロイされます。

注: 複数のポリシー・グループをスマート・グループに関連付けること (またはその逆) ができます。

ポリシー・グループの編集

ポリシー・グループを編集するには、ポリシー・グループの名前をクリックします。ここから、選択したポリシーとアプリケーションを変更したり、名前、説明、その他の詳細を変更したりできます。変更したポリシー・グループを保存すると、古いポリシー・グループが上書きされるため、実行する変更について確認してください。変更が完了したら、「保存」ボタンをクリックして保存し、表示ページに戻ることができます。変更を保存せずに「キャンセル」ボタンを選択して戻ることもできます。

ポリシー・グループの削除

ポリシー・グループを削除するには、以下のようにします。

1. 「ポリシー・グループ」ページから、削除するポリシー・グループを選択します。
2. 水平スクロール・バーを使用してページの右端に移動し、選択したポリシー・グループに表示されている削除アイコンをクリックします。

注: ページの右下にある赤い **「削除」**ボタンをクリックして、「ポリシー・グループの編集」ページからポリシー・グループを 削除 することもできます。

結果: 選択したポリシー・グループが削除されます。デバイス上のこのポリシー・グループを介して以前にデプロイされたポリシーは影響を受けません。

アプリ・デプロイメント・ポリシー

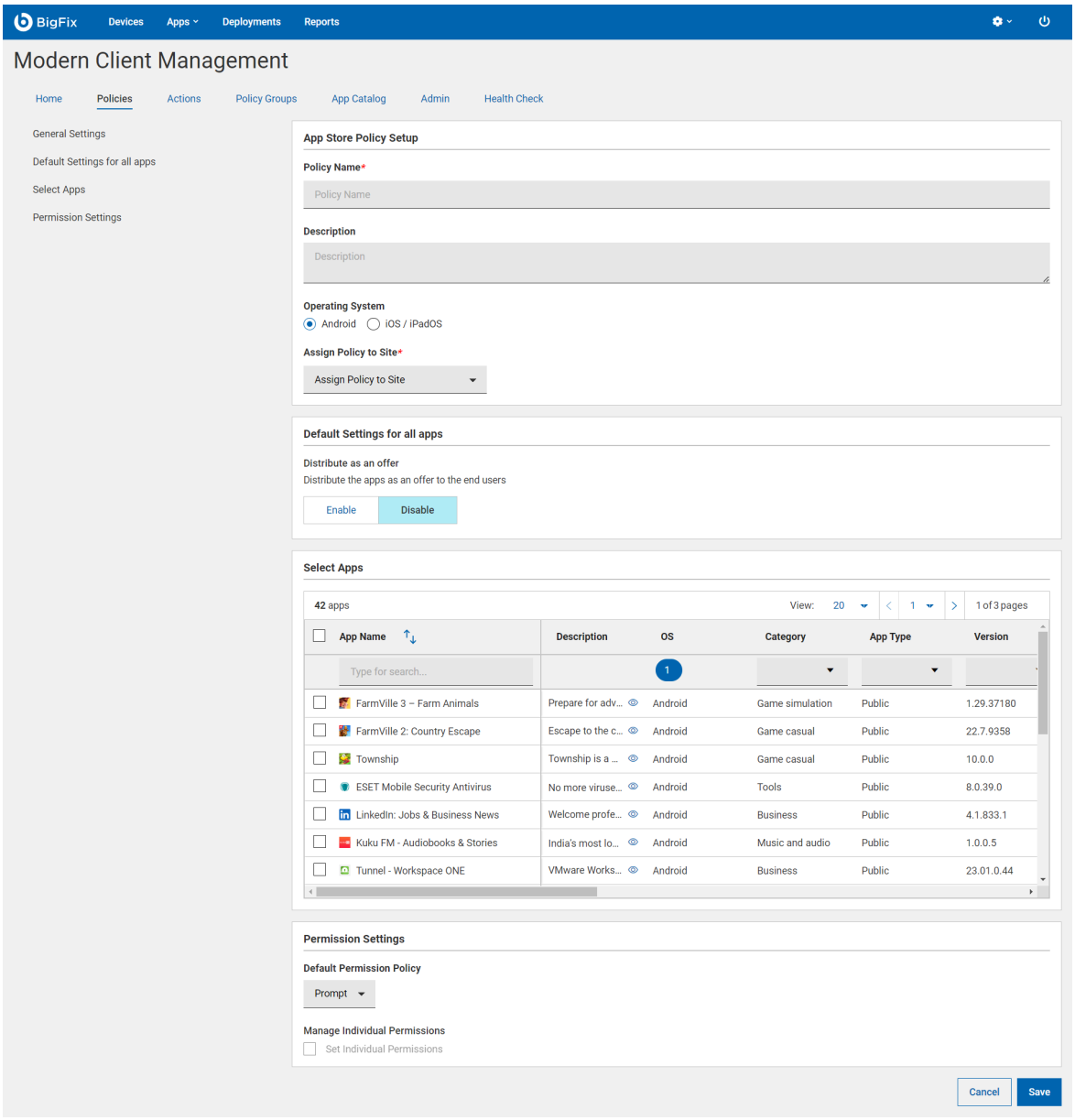
BigFix MCM では、App ストアからアプリケーションを Android、iOS、iPadOS デバイスにインストールするためのアプリケーション・ポリシーを構成できます。

アプリ・デプロイメント・ポリシーの作成前に、必要なアプリが（（ページ）　　）に追加されていることを確認します。

アプリ・デプロイメント・ポリシーの作成

アプリ・デプロイメント・ポリシーを作成するには、以下のステップを実行します。

1. BigFix WebUI にログインします。
2. **「アプリケーション」 > 「MCM」**に移動します。
3. 右上隅にある**「ポリシーの作成」**をクリックします。
4. ポリシー・タイプのリストから、**「アプリ・デプロイメント」**を選択します。以下のページが表示されます。



5. **「一般設定」**セクションで、アプリ・デプロイメント・ポリシーの名前と説明を入力します。
6. オペレーティング・システムを選択します。
7. **「サイトへのポリシーの割り当て」**ドロップダウンからサイトを選択します。
8. オペレーティング・システム固有の設定を構成します。アプリ・ポリシー内のすべて

のアプリにグローバルに権限を設定できます。必要に応じてアプリを選択し、

をクリックすることで、ポリシー内の個々のアプリの権限を設定することもできます。  アイコンの上にカーソルを合わせると、アプリの設定が表示されます。

Android

すべてのアプリのデフォルト設定:

提案として配布: 有効にすると、アプリは、アプリ・マーケットプレイス、Web サイト、直接配布などのさまざまな方法で Android デバイスにダウンロードまたはインストールできるようになります。アプリを提案としてエンド・ユーザーに配布するオプションを有効または無効にします。

許可セット

- **デフォルトの許可ポリシー**: デフォルトの許可ポリシーとして設定された許可は、アプリ・ポリシーを介してインストールされるすべてのアプリケーションにグローバルに適用されます。管理者は、管理対象 Android アプリのデフォルトのランタイム許可ポリシーを設定する際に、以下のオプションから選択できます。
  - [プロンプト] - アプリをインストールする許可を付与するようユーザーに求めるプロンプトを表示します。これはデフォルト・オプションです。デバイス・ユーザーは、アプリのインストールを許可するかキャンセルするかを選択できます。
  - 「認可」 - 管理対象アプリをユーザー介入なしでインストールするための許可を自動的に付与します。
  - 「否認」 - 許可されていないアプリのインストールを防止するための許可を自動的に拒否します。
- **個々の許可の管理**: 選択したアプリに基づいて、WebUI に許可のリストが表示されます。IT 管理者は、リモートで許可を設定して、アプリケーションがデータにアクセスしたり、デバイスを制御したりできないようにすることができます。例えば、ユーザーの連絡先、外部ストレージ、または場所を読み取る機能は、ランタイム許可です。ユーザーは、アプリケーションに対してこれらの許可を明示的に付与する必要があります。ただし、管理対象の

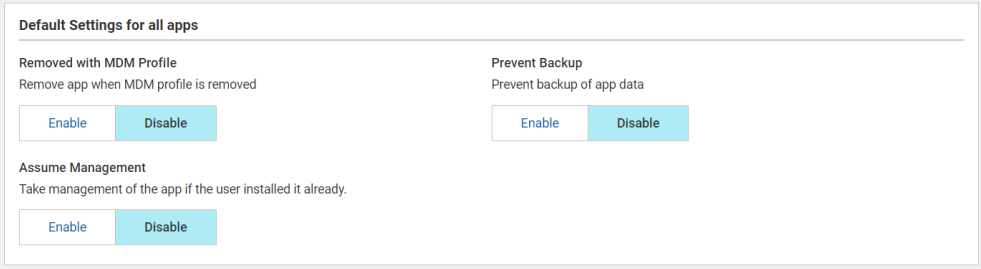
Google Play アプリケーションの場合、管理者は WebUI からこれらの許可を構成して適用できます。個々の許可に対して 「プロンプト」 、 「認可」 、 「否認」 を選択します。リストされている許可について詳しくは、Android の公式ドキュメント (https://developer.android.com/reference/android/Manifest.permission) を参照してください。

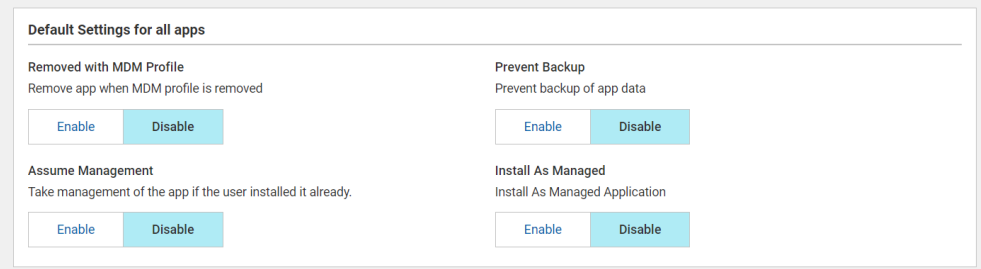
- **アプリごとに許可をカスタマイズ**: アプリごとの許可を構成する場合は、アプリを選択してアプリの編集アイコンをクリックし、個々の許可を選択します。

注: この App Store ポリシーのデプロイメントにより、このポリシーで指定されていない、過去にデプロイされた仕事用プロファイル・アプリケーションがすべて削除されます。

iOS/iPadOS

すべてのアプリのデフォルト設定: デフォルト設定として設定された許可は、アプリ・ポリシーを介してインストールされるすべてのアプリケーションにグローバルに適用されます。



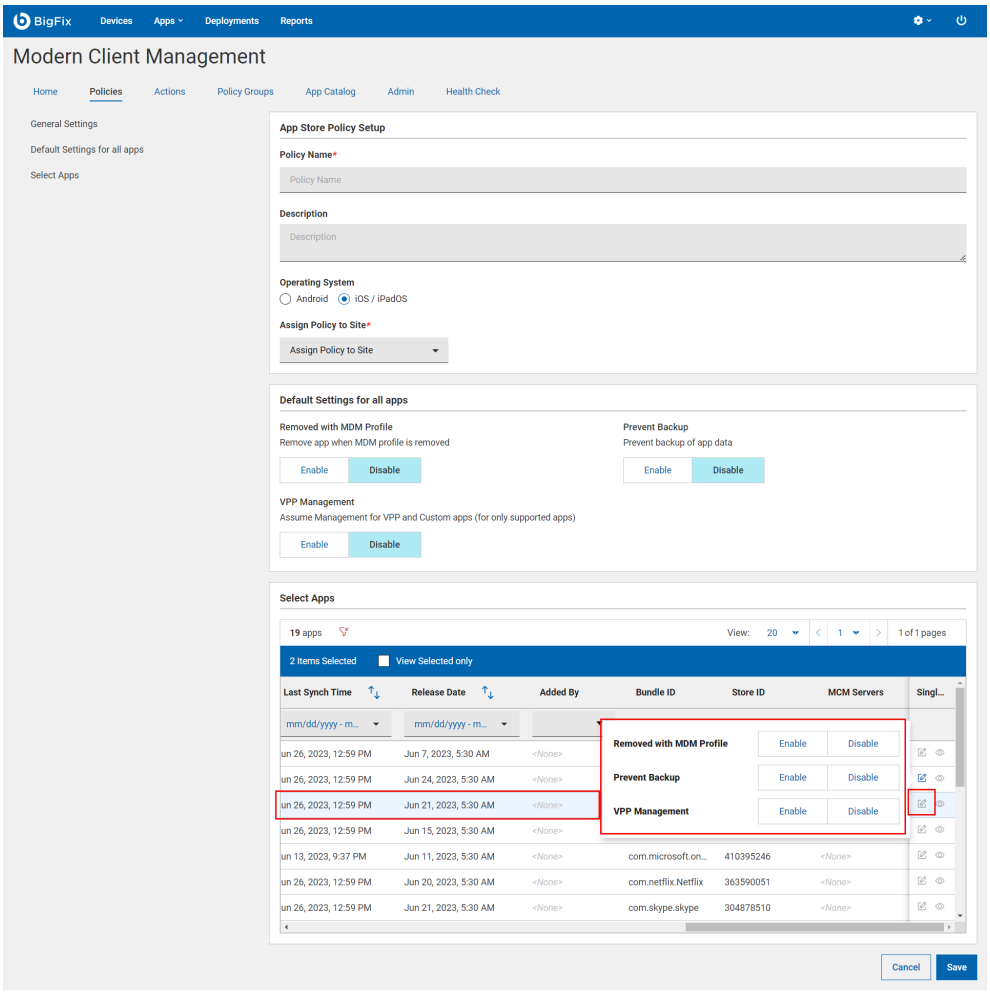


- **MDM プロファイルで削除**: MDM プロファイルが削除されたときにアプリを削除する場合は、この設定を有効にします。
- **バックアップの防止**: アプリ・データのバックアップを防止するには、この設定を有効にします。
- **管理を想定**: 有効にすると、MDM プロファイルがインストールされた場合、デバイスは管理を想定します。つまり、デバイスの設定、セキュリティー・ポリシー、アプリのインストール、その他の構成を BigFix で管理できます。

  注: このオプションは VPP アプリにのみ適用されます。監視対象 Apple デバイスにのみアプリを配布する場合は、この設定を有効にします。アプリを Apple ユーザー登録デバイスに配信する場合は、このオプションを選択しないでください。このオプションは BYOD 登録には許可されません。詳しくは、「既知の制限 ((ページ))」を参照してください。

- **管理対象としてインストール**: 有効にすると、アプリ構成プロファイルがデバイスに適用されたとき、アプリはこれらのデバイスで「管理対象」としてインストールされます。つまり、IT 管理者は、ポリシーで指定されたアプリをインストールして管理できます。IT 管理者は、macOS デバイスにアプリケーションをリモートでデプロイしてインストールしたり、特定の構成設定や環境設定をアプリケーションにプッシュしたり、セキュリティー・ポリシー、コンプライアンス要件、およびアクセス制御を適用したり、アプリケーションの使用状況を追跡したりできます。レポート用のデータを収集し、必要に応じてトラブルシューティングや更新を実行し、アプリのアップデートやパッチをインストールし、必要に応じてアプリをデバイスから削除することもできます。

個々のアプリ設定: アプリごとの設定を構成する場合は、それぞれのアプリで使用可能な編集ボタンをクリックして構成します。



9. **アプリの選択**: このグリッドには、アプリ・カタログに追加されたすべてのアプリがリストされます。目的のアプリを選択し、必要に応じて設定を構成します。
10. **「保存」**をクリックします。

アプリ・デプロイメント・ポリシーが作成され、デプロイの準備ができました。

ポリシーがデプロイされると、デバイスは、設定された許可またはアクションがデバイス・マネージャーによって実行されていることを示す通知を受け取ります。デバイス内の許可マネージャーに、適用された許可が表示されます。

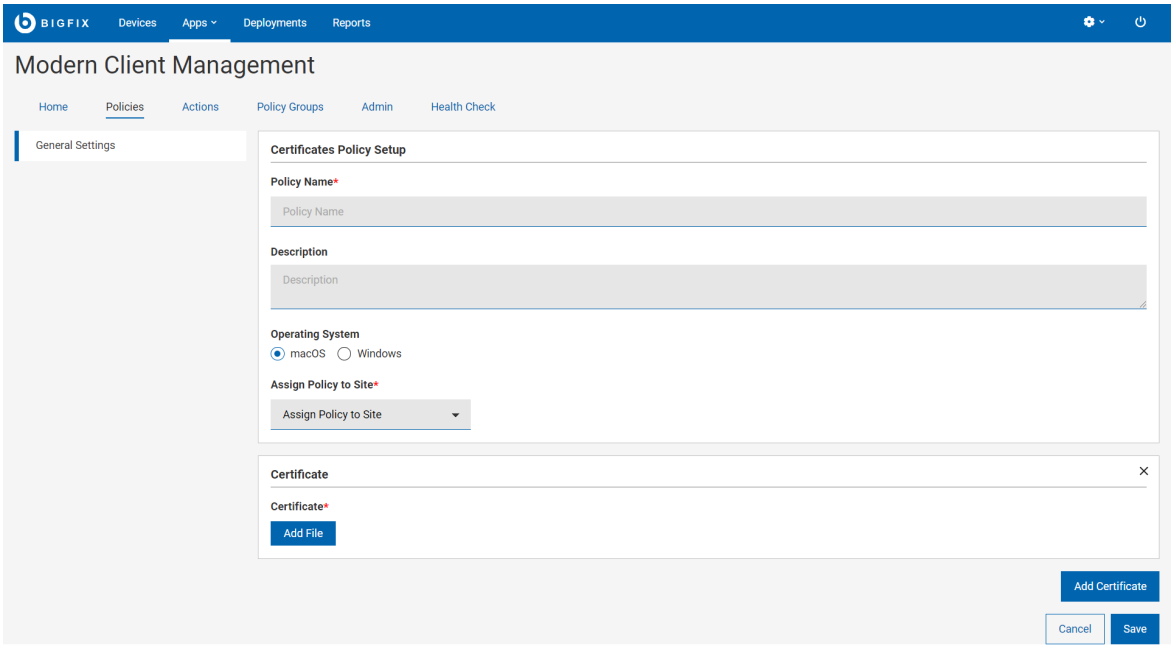
注: Android: 新しいポリシーをデプロイすると、以前にインストールされたが、新しいポリシーで指定されていないすべての作業プロファイル・アプリは削除されます。

証明書ポリシー

MDM サーバーに `.pem` および `.der` 証明書をアップロードして MDM にデプロイする方法について説明します。

証明書ポリシーを作成または編集するには、次の手順に従います。

1. WebUI のメイン・ページから、**「アプリケーション」 > 「MCM」**を選択します。
2. 「MDM」ページで、**「ポリシーの作成」**をクリックします。
3. ポリシー・タイプのリストから、**「証明書」**を選択します。以下のページが表示されます。



4. **「一般設定」**セクションで、次の操作を行います。
   a. ポリシーの名前と説明を入力します。
   b. オペレーティング・システムを選択します。オペレーティング・システムを選択すると、追加のフィールドが表示されます。
   c. **「サイトへのポリシーの割り当て」**ドロップダウンで、**「マスター・アクション・サイト」**を選択します。
5. **「証明書」**セクションで、次の操作を行います。

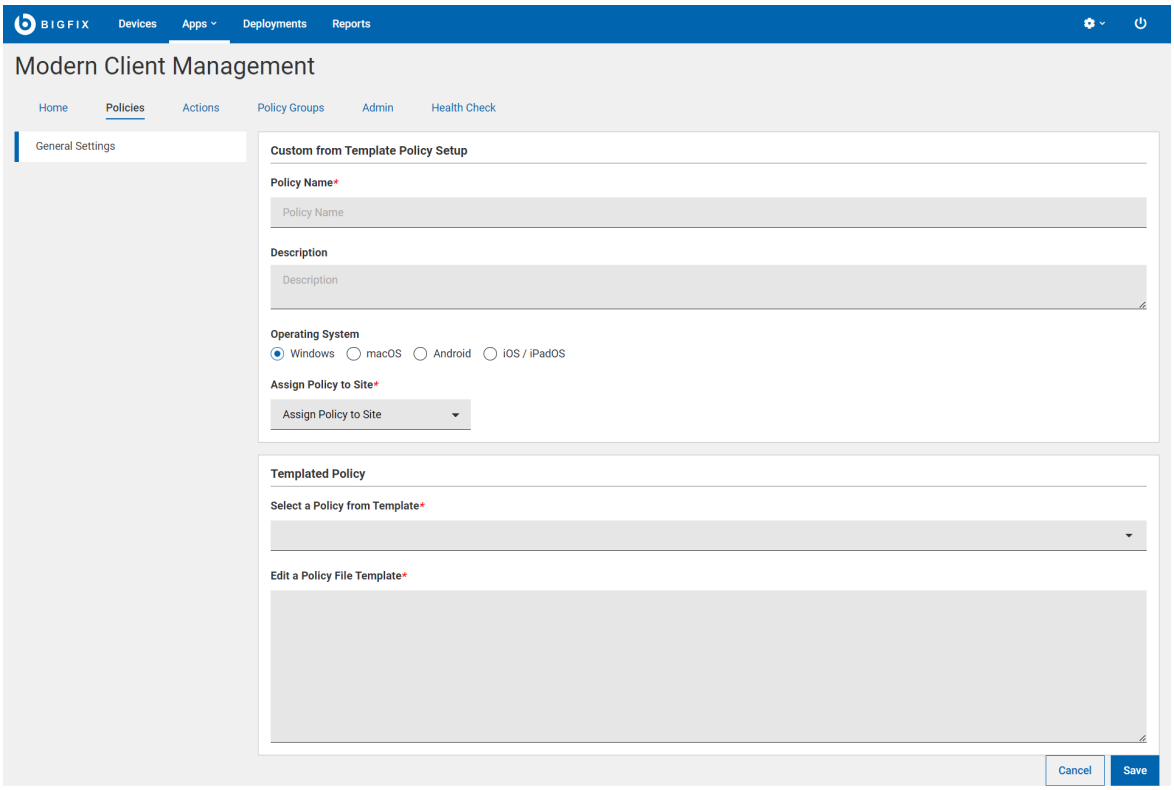
   a. オペレーティング・システムとして Windows を選択した場合は、**「証明書のタイプ」**を選択します。
   b. **「ファイルの追加」**をクリックして、`.pem` または `.der` の証明書ファイルを選択します。
6. **「証明書の追加」**をクリックして、別の証明書をアップロードします。
7. **「保存」**をクリックします。証明書ポリシーが作成されます。

テンプレートからカスタム

WebUI には、カスタム・ポリシー・テンプレートのセットが用意されており、カスタム・ポリシーとして直接保存するか、編集して保存してから、ポリシー・グループに含めることができます。

カスタム・テンプレート・ページにアクセスし、オペレーティング・システムの既存のテンプレートからカスタム・ポリシーを作成するには、次の手順を実行します。

1. MCM アプリケーションで**「ポリシーの作成」**をクリックし、**「テンプレートからカスタム」**を選択します。
2. **「一般設定」**ページで**「ポリシー名」**と**「説明」**を入力します。



3. **「オペレーティング・システム」**を選択します。選択したオペレーティング・システムに従って、該当するカスタム・ポリシー・テンプレートが**「テンプレートからポリシーを選択する」**ドロップダウンに表示されます。

   注: デフォルトのカスタム・ポリシー・サンプル・テンプレートは削除できません。

4. **「サイトへのポリシーの割り当て」**ドロップダウンから、ポリシーを割り当てるサイトを選択します。
5. 選択したポリシー・テンプレートを編集して、必要に応じてカスタマイズします。
6. **「保存」**をクリックします。
7. 保存されたカスタム・テンプレートが、**「ポリシー」**タブの下に表示されます。このカスタム・ポリシーをポリシー・グループに追加するか、必要に応じて個々のデバイスにデプロイします。

オペレーティング・システム固有のカスタム・ポリシー・テンプレートおよび変更可能なコンテンツについては、次のページを参照してください。

Windows

- Windows SCEP DeviceID テンプレート (（ページ） *405)*
- Windows SCEP Username テンプレート (（ページ） *406)*
- Windows プライベート・ファイアウォール有効テンプレート (（ページ） *407)*
- Windows パブリック・ファイアウォール有効化テンプレート (（ページ） *407)*
- Windows Offline Domain Join テンプレート (（ページ） *408)*

MacOS、iOS、iPadOS

- Apple SCEP テンプレート (（ページ） *415)*

Android

- 専用デバイスのサンプル・テンプレート (（ページ） *420)*
- アプリケーション適用サンプル・テンプレートの確認 (（ページ） *422)*
- ユーザー選択サンプル・テンプレートを使用したアプリケーションの確認 (（ページ） *423)*

Windows カスタム・ポリシー

このセクションでは、Windows カスタム・ポリシーで使用できるカスタム・テンプレートについて説明します。

Windows SCEP DeviceID テンプレート

このカスタム・テンプレートは、デバイス ID に基づいて Windows デバイスにデプロイする SCEP ポリシーを作成することができます。

Windows SCEP DeviceID テンプレートからカスタム・ポリシーを作成するには、次の手順を実行します。

1. MCM アプリケーションで**「ポリシーの作成」**をクリックし、**「テンプレートからカスタム」**を選択します。
2. **「一般設定」**ページで**「ポリシー名」**と**「説明」**を入力します。
3. **オペレーティング・システム**として Windows を選択します。
4. **「サイトへのポリシーの割り当て」**ドロップダウンから、ポリシーを割り当てるサイトを選択します。
5. **「テンプレートからポリシーを選択する」**ドロップダウンから、**「Windows SCEP DeviceID テンプレート」**を選択します。
6. **「保存」**をクリックして、カスタム Windows SCEP DeviceID ポリシーを保存します。
7. カスタム・ポリシーを適切なポリシー・グループに追加します。

注: ポリシーのデプロイ時に、必要なパラメーターが SCEP (Simple Certificate Enrollment Protocol) の構成 (（ページ）　　) に従って置き換えられます。

Windows SCEP Username テンプレート

このカスタム・テンプレートは、SCEP ポリシーを作成し、OTA 登録のデバイス・ユーザー名に基づいて Windows デバイスにデプロイすることを目的としています。

Windows SCEP Username テンプレートからカスタム・ポリシーを作成するには、次の手順を実行します。

1. MCM アプリケーションで**「ポリシーの作成」**をクリックし、**「テンプレートからカスタム」**を選択します。
2. **「一般設定」**ページで**「ポリシー名」**と**「説明」**を入力します。
3. **オペレーティング・システム**として Windows を選択します。
4. **「サイトへのポリシーの割り当て」**ドロップダウンから、ポリシーを割り当てるサイトを選択します。
5. **「テンプレートからポリシーを選択する」**ドロップダウンから、Windows SCEP Username ポリシーを選択します。

6. **「保存」**をクリックして、カスタム Windows SCEP Username ポリシーを保存します。
7. カスタム・ポリシーを適切なポリシー・グループに追加します。

注: ポリシーのデプロイ時に、必要なパラメーターが SCEP (Simple Certificate Enrollment Protocol) の構成 (（ページ）　　) に従って置き換えられます。

Windows プライベート・ファイアウォール有効テンプレート

このカスタム・テンプレートは、プライベート・ファイアウォール・ポリシーを作成して Windows デバイスにデプロイするためのものです。このポリシーを適用すると、ターゲット Windows デバイスで Windows ファイアウォールを有効にして、インバウンド接続とアウトバウンド接続を制御できます。

Windows プライベート・ファイアウォール・テンプレートからカスタム・ポリシーを作成するには、次の手順を実行します。

1. MCM アプリケーションで**「ポリシーの作成」**をクリックし、**「テンプレートからカスタム」**を選択します。
2. **「一般設定」**ページで**「ポリシー名」**と**「説明」**を入力します。
3. **オペレーティング・システム**として Windows を選択します。
4. **「サイトへのポリシーの割り当て」**ドロップダウンから、ポリシーを割り当てるサイトを選択します。
5. **「テンプレートからポリシーを選択する」**ドロップダウンから、Windows プライベート・ファイアウォール有効テンプレートを選択します。
6. 設定を変更せずに**「保存」**をクリックします。

Windows パブリック・ファイアウォール有効化テンプレート

このカスタム・テンプレートは、Windows デバイスにデプロイするパブリック・ファイアウォール・ポリシーを作成するためのものです。このポリシーを使用すると、ターゲット Windows デバイスで Windows ファイアウォールが有効になっていること、およびインバウンド接続とアウトバウンド接続を制御していることを確認できます。

Windows パブリック・ファイアウォール・テンプレートからカスタム・ポリシーを作成するには、次の手順を実行します。

1. MCM アプリケーションで**「ポリシーの作成」**をクリックし、**「テンプレートからカスタム」**を選択します。
2. **「一般設定」**ページで**「ポリシー名」**と**「説明」**を入力します。
3. **オペレーティング・システム**として Windows を選択します。
4. **「サイトへのポリシーの割り当て」**ドロップダウンから、ポリシーを割り当てるサイトを選択します。
5. **「テンプレートからポリシーを選択する」**ドロップダウンから、「Windows パブリック・ファイアウォール有効化テンプレート」を選択します。
6. 設定を変更せずに**「保存」**をクリックします。

Windows Offline Domain Join テンプレート

WebUI では、Windows 用のカスタム ODJ ポリシー・テンプレートを使用できます。他のポリシーと同様にこのテンプレートを変更してポリシー・グループに追加し、MDM サーバーにデプロイできます。このカスタム ODJ ポリシーを個々のデバイスにデプロイすることもできます。

Windows Offline Domain Join テンプレートからカスタム・ポリシーを作成するには、次の手順を実行します。

1. WebUI から、**「アプリ」 > 「MCM」**を選択します。
2. WebUI の MCM ダッシュボードが表示されます。**「ポリシーの作成」**をクリックします。
3. 使用可能なポリシー・オプションのリストから、**「テンプレートからカスタム」**を選択します。
4. 「一般設定」ページで、次の手順を実行します。
    a. **「ポリシー名」**と**「説明」**を入力します。
    b. **「オペレーティング・システム」**で、「Windows」を選択します。
    c. **「サイトへのポリシーの割り当て」**ドロップダウンから、ポリシーを割り当てるサイトを選択します。

d. **「テンプレート・ポリシー」**セクションの**「テンプレートからポリシーを選択する」**ドロップダウンで、**「Windows Offline Domain Join テンプレート」**を選択します。
e. **「保存」**をクリックして、カスタム ODJ ポリシーを保存します。

5. 「Autopilot」登録タイプを使用して Windows のポリシー・グループに保存された ODJ ポリシーを追加し、MDM サーバーにデプロイします。

Windows E メールのサンプル・テンプレート

Windows デバイスでは、ポリシーを使用して 電子メール構成を管理 (（ページ）)できます。このセクションでは、WebUI のテンプレートを使用してカスタム Windows 電子メール・ポリシーを作成する方法について説明します。

Windows 電子メール・テンプレートからカスタム・ポリシーを作成するには、次の手順を実行します。

1. WebUI から、**「アプリ」 > 「MCM」**を選択します。
2. WebUI の MCM ダッシュボードが表示されます。**「ポリシーの作成」**をクリックします。
3. 使用可能なポリシー・オプションのリストから、**「テンプレートからカスタム」**を選択します。
4. 「一般設定」ページで、次の手順を実行します。
   a. **「ポリシー名」**と**「説明」**を入力します。
   b. **「オペレーティング・システム」**で、「Windows」を選択します。
   c. **「サイトへのポリシーの割り当て」**ドロップダウンから、ポリシーを割り当てるサイトを選択します。
   d. **「テンプレート・ポリシー」**セクションの**「テンプレートからポリシーを選択する」**ドロップダウンで**「Windows 電子メール・サンプル・テンプレート」**を選択します。

   注: パラメーターを変更して基本的な電子メール・ポリシーを作成する必要はありません。Windows デバイスにこのポリシーをデプロイすると、システムは登録時に入力されたプライマリー・デバイス・ユーザー

の名前と電子メール・アドレスが取得して、ネイティブ Windows 電子メール・アプリにログインします。

e. **「保存」**をクリックして、Windows カスタム電子メール・ポリシーを保存します。

5. 保存したポリシーを Windows のポリシー・グループに追加し、MDM サーバーにデプロイします。

Windows VPN サンプル・テンプレート

Windows デバイスでは、ポリシーを使用して VPN 構成を管理 (（ページ）　　)できます。このセクションでは、WebUI のテンプレートを使用してカスタム Windows VPN ポリシーを作成する方法について説明します。

Windows VPN テンプレートからカスタム・ポリシーを作成するには、次の手順を実行します。

1. WebUI から、**「アプリ」 > 「MCM」**を選択します。
2. WebUI の MCM ダッシュボードが表示されます。**「ポリシーの作成」**をクリックします。
3. 使用可能なポリシー・オプションのリストから、**「テンプレートからカスタム」**を選択します。
4. 「一般設定」ページで、次の手順を実行します。
   a. **「ポリシー名」**と**「説明」**を入力します。
   b. **「オペレーティング・システム」**で、「Windows」を選択します。
   c. **「サイトへのポリシーの割り当て」**ドロップダウンから、ポリシーを割り当てるサイトを選択します。
   d. **「テンプレート・ポリシー」**セクションの**「テンプレートからポリシーを選択する」**ドロップダウンで**「Windows VPN サンプル・テンプレート」**を選択し、必要なパラメーターを編集します。

注: 。このサンプル・テンプレートは、EAP - MSCHAPv2 構成を使用する PPTP VPN 用です。この構成では、Windows ログオン資格情報を使用して接続を行います。EAP の構成と認証の詳細については、「ネット

ワーク・アクセス用の Extensible Authentication Protocol (EAP)」を参照してください

```
<Atomic>
<CmdID>5ed5b540-92c3-49e4-808e-01de3d9a799a</CmdID>
<Replace>
<CmdID>9b2f2603-1ae8-44b9-a80b-652540b99bf0</CmdID>
<Item>
<Target>
<LocURI>./Vendor/MSFT/VPNv2/{{VPN_PROFILENAME}}/
ProfileXML</LocURI>
</Target>
<Data>
<![CDATA[<VPNProfile>
<ProfileName>{{VPN_PROFILENAME}}</ProfileName>
<NativeProfile>
<Servers>{{VPN_SERVERHOST}}</Servers>
<Authentication>
<UserMethod>Eap</UserMethod>
<Eap>
<Configuration>
<EapHostConfig
 xmlns="http://www.microsoft.com/provisioning/EapHostConfig"><Eap
Method><Type
 xmlns="http://www.microsoft.com/provisioning/EapCommon">26</Type
><VendorId
 xmlns="http://www.microsoft.com/provisioning/EapCommon">0</Vendo
rId><VendorType
 xmlns="http://www.microsoft.com/provisioning/EapCommon">0</Vendo
rType><AuthorId
 xmlns="http://www.microsoft.com/provisioning/EapCommon">0</Autho
rId></EapMethod><Config
```

```
 xmlns="http://www.microsoft.com/provisioning/EapHostConfig"><Eap
 xmlns="http://www.microsoft.com/provisioning/BaseEapConnectionPr
opertiesV1"><Type>26</Type><EapType
 xmlns="http://www.microsoft.com/provisioning/MsChapV2ConnectionP
ropertiesV1"><UseWinLogonCredentials>true</UseWinLogonCredentials
></EapType></Eap></Config></EapHostConfig>
</Configuration>
</Eap>
</Authentication>
</NativeProfile>
<RememberCredentials>true</RememberCredentials>
</VPNProfile>]]>
</Data>
</Item>
</Replace>
</Atomic>
```

e.
- テンプレート内に示されているすべての **{{VPN_PROFILENAME}}** を VPN 接続名に置き換えます。
- テンプレートの **{{VPN_SERVERHOST}}** をサーバー名またはアドレスに置き換えます。

注: `UseWinLogonCredentials` を true に設定している場合、VPN クライアントは、ユーザーがエンドポイントにログインする Windows 資格情報を使用して、エンドポイントから VPN サーバーに接続します。

f. **「保存」**をクリックして、Windows カスタム VPN ポリシーを保存します。

5. 保存したポリシーを Windows のポリシー・グループに追加し、MDM サーバーにデプロイします。

MDM 登録 Windows デバイスにこのポリシーをデプロイすると、MCM サーバーはデバイスに VPN プロファイルを作成します。ログオン資格情報を使用して、設定された VPN サーバーとの VPN 接続を確立します。

Windows WiFi サンプル・テンプレート

登録 Windows デバイスでは、ポリシーを使用して WiFi 構成を管理 (（ページ）　　)できます。このセクションでは、WebUI のテンプレートを使用してカスタム Windows WiFi ポリシーを作成する方法について説明します。

Windows WiFi テンプレートからカスタム Windows WiFi ポリシーを作成するには、次の手順を実行します。

1. WebUI から、**「アプリ」 > 「MCM」**を選択します。
2. WebUI の MCM ダッシュボードが表示されます。**「ポリシーの作成」**をクリックします。
3. 使用可能なポリシー・オプションのリストから、**「テンプレートからカスタム」**を選択します。
4. 「一般設定」ページで、次の手順を実行します。
    a. **「ポリシー名」**と**「説明」**を入力します。
    b. **「オペレーティング・システム」**で、「Windows」を選択します。
    c. **「サイトへのポリシーの割り当て」**ドロップダウンから、ポリシーを割り当てるサイトを選択します。
    d. **「テンプレート・ポリシー」**セクションの**「テンプレートからポリシーを選択する」**ドロップダウンで**「Windows WiFi サンプル・テンプレート」**を選択し、必要なパラメーターを編集します。

```
<Add>
 <CmdID>3cd19f03-8d96-4684-bdec-9e0eede9a193</CmdID>
 <Item>
  <Target>

 <LocURI>./Vendor/MSFT/WiFi/Profile/{{SSID_NAME}}/
WlanXml</LocURI>
  </Target>
  <Data>
   <![CDATA[<WLANProfile
 xmlns="http://www.microsoft.com/networking/WLAN/profile/v1">
```

```
 <name>{{SSID_NAME}}</name>
 <SSIDConfig>
  <SSID>
   <hex>{{SSID_HEXCODE}}</hex>
   <name>{{SSID_NAME}}</name>
  </SSID>
  <nonBroadcast>false</nonBroadcast>
 </SSIDConfig>
 <connectionType>ESS</connectionType>
 <connectionMode>auto</connectionMode>
 <autoSwitch>false</autoSwitch>
 <MSM>
  <security>
   <authEncryption>
    <authentication>WPA2PSK</authentication>
    <encryption>AES</encryption>
    <useOneX>false</useOneX>
    <FIPSMode
 xmlns="http://www.microsoft.com/networking/WLAN/profile/v2">fals
e
    </FIPSMode>
   </authEncryption>
   <sharedKey>
    <keyType>passPhrase</keyType>
    <protected>false</protected>
    <keyMaterial>{{WIFI_PASSWORD}}</keyMaterial>
   </sharedKey>
   <PMKCacheMode>disabled</PMKCacheMode>
  </security>
 </MSM>
</WLANProfile>]]>
  </Data>
```

```
 </Item>
</Add>
```

- テンプレートに示されているすべての **{{SSID_NAME}}** を WiFi SSID に置き換えます。
- WiFi SSID 文字列を 16 進値に変換し、テンプレート内の **{{SSID_HEXCODE}}** を WiFi SSID の 16 進値に置き換えます。
- テンプレート内の **{{WIFI_PASSWORD}}** を実際の WiFi 共有シークレットに置き換えます。

注: 上記の設定により、基本的な WiFi ポリシーを作成できます。カスタマイズ可能なパラメーターの一覧については、Microsoft のマニュアルを参照してください。

e. **「保存」**をクリックしてカスタム WiFi ポリシーを保存します。

5. 保存したポリシーを Windows のポリシー・グループに追加し、MDM サーバーにデプロイします。

MacOS カスタム・ポリシー

このセクションでは、macOS カスタム・ポリシーで使用できるカスタム・テンプレートについて説明します。

Apple SCEP テンプレート

このカスタム・テンプレートは、Android デバイスにデプロイする SCEP ポリシーを作成するためのものです。

Apple SCEP テンプレートを使用してカスタム・ポリシーを作成するには、次の手順を実行します。

1. MCM アプリケーションで**「ポリシーの作成」**をクリックし、**「テンプレートからカスタム」**を選択します。
2. **「一般設定」**ページで**「ポリシー名」**と**「説明」**を入力します。
3. **「オペレーティング・システム」**として macOS を選択します。

4. **「サイトへのポリシーの割り当て」**ドロップダウンから、ポリシーを割り当てるサイトを選択します。
5. **「テンプレートからポリシーを選択する」**ドロップダウンから、Apple SCEP テンプレートを選択します。
6. **「保存」**をクリックして、カスタム Apple SCEP デバイス ID ポリシーを保存します。ポリシーのデプロイ時に、必要なパラメーターが SCEP (Simple Certificate Enrollment Protocol) の構成 (（ページ）) に従って置き換えられます。

ポリシーを適切なポリシー・グループに追加して、Apple デバイスにデプロイします。

Apple 電子メールのサンプル・テンプレート

Apple デバイスでは、ポリシーを使用して 電子メール構成を管理 (（ページ）)できます。専用の電子メール・クライアント・アプリ (Outlook など) または Web ベースのソリューション (Google Workspace など) を使用するように登録済みデバイスを設定できます。このセクションでは、WebUI のテンプレートを使用してカスタム Apple 電子メール・ポリシーを作成する方法について説明します。

Apple 電子メール・テンプレートからカスタム・ポリシーを作成するには、次の手順を実行します。

1. WebUI から、**「アプリ」 > 「MCM」**を選択します。
2. WebUI の MCM ダッシュボードが表示されます。**「ポリシーの作成」**をクリックします。
3. 使用可能なポリシー・オプションのリストから、**「テンプレートからカスタム」**を選択します。
4. 「一般設定」ページで、次の手順を実行します。
    a. **「ポリシー名」**と**「説明」**を入力します。
    b. **「オペレーティング・システム」**には、**macOS** または **iOS/iPadOS** を選択します。
    c. **「サイトへのポリシーの割り当て」**ドロップダウンから、ポリシーを割り当てるサイトを選択します。

d. **「テンプレート・ポリシー」**セクションの**「テンプレートからポリシーを選択する」**ドロップダウンで**「Apple 電子メール・サンプル・テンプレート」**を選択し、必要なパラメーターを編集します。

注: すべてのプレースホルダー情報に、特定の値を入力するか、リストから値を選択します。

- テンプレートの **%%** は、入力の必要があるデータのプレースホルダーを示します
- **| (垂直バー)** は、選択可能なパラメーターの選択肢を示します。

必要な設定については、「Apple デバイスのメール MDM ペイロード設定」を参照してください。

。

e. **「保存」**をクリックして、カスタム電子メール・ポリシーを保存します。

macOS または iOS/iPadOS のポリシー・グループ (（ページ） *386)*に、保存したポリシーを追加してデプロイします。MDM 登録 Apple デバイスにこのポリシーをデプロイすると、システムは登録時に入力されたプライマリー・ユーザーの名前と E メール・アドレスを取得して、電子メール・アプリにログインします。

Apple VPN サンプル・テンプレート

Apple デバイスでは、ポリシーを使用して VPN 構成を管理 (（ページ）)できます。このセクションでは、WebUI のテンプレートを使用してカスタム Apple VPN ポリシーを作成する方法について説明します。

Apple VPN テンプレートからカスタム・ポリシーを作成するには、次の手順を実行します。

1. WebUI から、**「アプリ」 > 「MCM」**を選択します。
2. WebUI の MCM ダッシュボードが表示されます。**「ポリシーの作成」**をクリックします。
3. 使用可能なポリシー・オプションのリストから、**「テンプレートからカスタム」**を選択します。

4. 「一般設定」ページで、次の手順を実行します。
    a. **「ポリシー名」**と**「説明」**を入力します。
    b. **「オペレーティング・システム」**には、**macOS** または **iOS/iPadOS** を選択します。
    c. **「サイトへのポリシーの割り当て」**ドロップダウンから、ポリシーを割り当てるサイトを選択します。
    d. **「テンプレート・ポリシー」**セクションの**「テンプレートからポリシーを選択する」**ドロップダウンで**「Apple VPN サンプル・テンプレート」**を選択し、必要なパラメーターを編集します。

    注: すべてのプレースホルダー情報に、特定の値を入力するか、リストから値を選択します。
    - テンプレートの **%%** は、入力の必要があるデータのプレースホルダーを示します
    - **| (垂直バー)** は、選択可能なパラメーターの選択肢を示します。

    必要な設定については、「Apple デバイスの VPN 設定の概要」を参照してください。

    e. **「保存」**をクリックして、カスタム VPN ポリシーを保存します。

macOS または iOS/iPadOS のポリシー・グループ (（ページ） *386)*に、保存したポリシーを追加してデプロイします。MDM 登録 Apple デバイスにこのポリシーをデプロイすると、MCM サーバーはデバイスに VPN プロファイルを作成します。ユーザーが VPN に接続すると、インストールおよび設定時に設定された VPN 資格情報が取得され、VPN 接続が確立されます。

Apple WiFi サンプル・テンプレート

Apple デバイスでは、ポリシーを使用して WiFi 構成を管理 (（ページ）)できます。このセクションでは、WebUI のテンプレートを使用してカスタム Apple WiFi ポリシーを作成する方法について説明します。

Apple WiFi テンプレートからカスタム WiFi ポリシーを作成するには、次の手順を実行します。

1. WebUI から、**「アプリ」 > 「MCM」**を選択します。
2. WebUI の MCM ダッシュボードが表示されます。**「ポリシーの作成」**をクリックします。
3. 使用可能なポリシー・オプションのリストから、**「テンプレートからカスタム」**を選択します。
4. 「一般設定」ページで、次の手順を実行します。
    a. **「ポリシー名」**と**「説明」**を入力します。
    b. **「オペレーティング・システム」**には、必要に応じて **macOS** または **iOS/iPadOS** を選択します。
    c. **「サイトへのポリシーの割り当て」**ドロップダウンから、ポリシーを割り当てるサイトを選択します。
    d. **「テンプレート・ポリシー」**セクションの**「テンプレートからポリシーを選択する」**ドロップダウンで**「Apple WiFi サンプル・テンプレート」**を選択し、必要なパラメーターを編集します。

        注: すべてのプレースホルダー情報に、特定の値を入力するか、リストから値を選択します。
        - テンプレートの **%%** は、入力の必要があるデータのプレースホルダーを示します
        - **| (垂直バー)** は、選択可能なパラメーターの選択肢を示します。

        必要な設定については、「Apple デバイスの WiFi MDM 設定」を参照してください。

    e. **「保存」**をクリックして、Apple カスタム WiFi ポリシーを保存します。

macOS または **iOS/iPadOS** 用の ポリシー・グループ (（ページ） *386)* に、保存された WiFi ポリシーを追加し、必要に応じてデプロイします。この WiFi ポリシーが MDM 登録 Apple デバイスにデプロイされると、Wi-Fi 設定はポリシーに従ってデバイス上で自動的に構成されます。

Android カスタム・ポリシー

このセクションでは、Android カスタム・ポリシーで使用できるカスタム・テンプレートについて説明します。

専用デバイスのサンプル・テンプレート

このカスタム・テンプレートは、Android デバイスにデプロイする専用デバイス・ポリシーを作成するためのものです。

専用デバイスは、デジタル・サイネージ、チケット印刷、インベントリー管理など、単一のユース・ケースを満たす企業所有のデバイスです。管理者はデバイスの使用を単一のアプリまたは少数のアプリにさらにロックダウンでき、ユーザーがそのデバイス上で他のアプリを有効にしたり、他のアクションを実行したりすることを防止できます。専用デバイスの詳細については、

「キオスク管理」を参照してください。

カスタム・テンプレートを変更してパーソナライズするには、以下の手順を実行します。

1. MCM アプリケーションで**「ポリシーの作成」**をクリックし、**「テンプレートからカスタム」**を選択します。
2. **「一般設定」**ページで**「ポリシー名」**と**「説明」**を入力します。
3. **オペレーティング・システム**として Android を選択します。
4. **「サイトへのポリシーの割り当て」**ドロップダウンから、ポリシーを割り当てるサイトを選択します。
5. **「テンプレートからポリシーを選択する」**ドロップダウンから、専用デバイス・サンプル・テンプレートを選択します。
6. このポリシー・スニペットには、アクセスが最小限の専用デバイスの推奨デバイス設定が含まれています。*packageName* と *installType* を編集して、このポリシーによってインストールする必要があるアプリケーションをカスタマイズします。

```
{
 "safeBootDisabled": true,
 "screenCaptureDisabled": true,
 "factoryResetDisabled": true,
 "cameraDisabled": true,
  "systemUpdate": {
  "type": "WINDOWED",
  "startMinutes": 120,
```

```
 "endMinutes": 240
},
"kioskCustomLauncherEnabled": true,
"keyguardDisabled": true,
"applications": [
{
        "packageName":"com.olacabs.oladriver",
        "installType":"FORCE_INSTALLED",
        "defaultPermissionPolicy":"GRANT"
     },
     {
        "packageName":"com.screencast",
        "installType":"FORCE_INSTALLED"
     },
     {
        "packageName":"com.android.chrome",
        "installType":"FORCE_INSTALLED",
        "defaultPermissionPolicy":"GRANT"
     },
     {
        "packageName":"org.mozilla.firefox",
        "installType":"FORCE_INSTALLED",
        "defaultPermissionPolicy":"GRANT"
     },
     {
        "packageName":"com.ubercab",
        "installType":"FORCE_INSTALLED",
        "defaultPermissionPolicy":"GRANT"
     },
     {
        "packageName":"com.jio.media.jiobeats",
        "installType":"FORCE_INSTALLED",
```

```
         "defaultPermissionPolicy":"GRANT"
      },
      {
         "packageName":"com.microsoft.office.outlook",
         "installType":"FORCE_INSTALLED",
         "managedConfiguration":{

 "com.microsoft.outlook.EmailProfile.EmailAddress":"johndoe@hcl.com",
            "com.microsoft.outlook.EmailProfile.EmailAccountName":"John
 Doe",

 "com.microsoft.outlook.EmailProfile.ServerHostName":"outlook.office365.com
",
   "com.microsoft.outlook.EmailProfile.EmailUPN": "prod\\John Doe"
        }
      }
 ]
}
```

アプリケーション適用サンプル・テンプレートの確認

このカスタム・テンプレートは、Android デバイスのアプリケーション適用ポリシーを作成するためのものです。

アプリ適用の検証機能により、Google Play プロテクトは Android デバイスにインストールされているすべてのアプリをスキャンして、インストールの前後に有害なソフトウェアがないかを確認し、悪意のあるアプリが企業データを侵害できないようにします。この設定はオプションです。

カスタム・テンプレートを変更してパーソナライズするには、以下の手順を実行します。

1. MCM アプリケーションで**「ポリシーの作成」**をクリックし、**「テンプレートからカスタム」**を選択します。
2. **「一般設定」**ページで**「ポリシー名」**と**「説明」**を入力します。
3. **オペレーティング・システム**として Android を選択します。

4. **「サイトへのポリシーの割り当て」**ドロップダウンから、ポリシーを割り当てるサイトを選択します。
5. **「テンプレートからポリシーを選択する」**ドロップダウンから、「アプリケーション適用サンプル・テンプレートの確認」を選択します。
6. *packageName* と *installType* を編集して、このポリシーによってインストールする必要があるアプリケーションをカスタマイズします。

```
{
  "advancedSecurityOverrides": {
    "developerSettings": "DEVELOPER_SETTINGS_ALLOWED",
    "untrustedAppsPolicy": "DISALLOW_INSTALL",
    "googlePlayProtectVerifyApps": "VERIFY_APPS_ENFORCED"
  },
  "applications": [
    {
      "packageName": "com.android.chrome",
      "installType": "AVAILABLE"
    }
   ]
}
```

7. **「保存」**をクリックします。

ユーザー選択サンプル・テンプレートを使用したアプリケーションの確認

このカスタム・テンプレートは、Android デバイスのユーザーが選択したアプリケーション適用ポリシーを作成するためのものです。

アプリ適用の検証機能により、Google Play プロテクトは Android デバイスにインストールされているすべてのアプリをスキャンして、インストールの前後に有害なソフトウェアがないかを確認し、悪意のあるアプリが企業データを侵害できないようにします。このカスタム・ポリシーを使用して IT 管理者は、デバイス・ユーザーに `Scan apps with Play Protect` の設定をオンまたはオフにするオプションを提供できます。これにより、ユー

ザーがアプリの検証を有効にするかどうかを選択できるようにします。この設定はオプションです。

カスタム・テンプレートを変更してパーソナライズするには、以下の手順を実行します。

1. MCM アプリケーションで**「ポリシーの作成」**をクリックし、**「テンプレートからカスタム」**を選択します。
2. **「一般設定」**ページで**「ポリシー名」**と**「説明」**を入力します。
3. **オペレーティング・システム**として Android を選択します。
4. **「サイトへのポリシーの割り当て」**ドロップダウンから、ポリシーを割り当てるサイトを選択します。
5. **「テンプレートからポリシーを選択する」**ドロップダウンから、「ユーザー選択サンプル・テンプレートを使用したアプリケーションの確認」を選択します。
6. *packageName* と *installType* を編集して、このポリシーによってインストールする必要があるアプリケーションをカスタマイズします。

```
{
  "advancedSecurityOverrides": {
    "developerSettings": "DEVELOPER_SETTINGS_ALLOWED",
    "untrustedAppsPolicy": "DISALLOW_INSTALL",
    "googlePlayProtectVerifyApps": "VERIFY_APPS_USER_CHOICE"
  },
  "applications": [
    {
      "packageName": "com.android.chrome",
      "installType": "AVAILABLE"
    },
    {
      "packageName": "com.spotify.music",
      "installType": "AVAILABLE"
    }
   ]
}
```

7. **「保存」**をクリックします。

Android WiFi サンプル・テンプレート

Android デバイスでは、ポリシーを使用して WiFi 設定を管理 (（ページ　　)できます。このセクションでは、WebUI のテンプレートを使用してカスタム Android WiFi ポリシーを作成する方法について説明します。

Android WiFi テンプレートからカスタム Android WiFi ポリシーを作成するには、次の手順を実行します。

1. WebUI から、**「アプリ」 > 「MCM」**を選択します。
2. WebUI の MCM ダッシュボードが表示されます。**「ポリシーの作成」**をクリックします。
3. 使用可能なポリシー・オプションのリストから、**「テンプレートからカスタム」**を選択します。
4. 「一般設定」ページで、次の手順を実行します。
   a. **「ポリシー名」**と**「説明」**を入力します。
   b. **「オペレーティング・システム」**で「Android」を選択します。
   c. **「サイトへのポリシーの割り当て」**ドロップダウンから、ポリシーを割り当てるサイトを選択します。
   d. **「テンプレート・ポリシー」**セクションの**「テンプレートからポリシーを選択する」**ドロップダウンで**「Android WiFi サンプル・テンプレート」**を選択し、必要なパラメーターを編集します。

```
{
   "deviceRadioState": {
   "wifiState": "WIFI_ENABLED"
   },
   "deviceConnectivityManagement": {
     "configureWifi": "ALLOW_CONFIGURING_WIFI",
     "wifiDirectSettings": "ALLOW_WIFI_DIRECT"
   },
   "openNetworkConfiguration": {
     "NetworkConfigurations": [
       {
```

```
        "GUID": "cc0b4c66-aa58-4c49-8bae-af927643cec0",
        "Name": "Simple Network",
        "Type": "WiFi",
        "WiFi": {
          "SSID": "{{SSID_NAME}}",
          "Security": "WPA-PSK",
          "Passphrase": "{{PASSWORD}}",
          "AutoConnect": true
        }
      }]
  },
  "networkEscapeHatchEnabled": true,
  "wifiConfigsLockdownEnabled": true,
  "wifiConfigDisabled": true
}
```

- テンプレートの **`{{SSID_NAME}}`** をお使いの WiFi の SSID に置き換えます。
- テンプレートの **`{{PASSWORD}}`** をお使いの WiFi のパスワードに置き換えます。

Android でサポートされているオープン・ネットワーク構成の詳細については、https://developers.google.com/android/management/configure-networks#multiple_wifi_networks を参照してください。

e. **「保存」**をクリックしてカスタム WiFi ポリシーを保存します。

5. 保存したポリシーを Android のポリシー・グループに追加し、MDM サーバーにデプロイします。

ポリシーが MCM 管理対象 Android デバイスにデプロイされると、そのデバイスは、ユーザーの介入なしに、WiFi ポリシーで定義されている Wi-Fi ネットワークに自動的に接続されます。

iOS/iPadOS カスタム・ポリシー

このセクションでは、iOS/iPadOS カスタム・ポリシーで使用できるカスタム・テンプレートについて説明します。

Apple SCEP テンプレート

このカスタム・テンプレートは、Android デバイスにデプロイする SCEP ポリシーを作成するためのものです。

Apple SCEP テンプレートを使用してカスタム・ポリシーを作成するには、次の手順を実行します。

1. MCM アプリケーションで**「ポリシーの作成」**をクリックし、**「テンプレートからカスタム」**を選択します。
2. **「一般設定」**ページで**「ポリシー名」**と**「説明」**を入力します。
3. **「オペレーティング・システム」**として macOS を選択します。
4. **「サイトへのポリシーの割り当て」**ドロップダウンから、ポリシーを割り当てるサイトを選択します。
5. **「テンプレートからポリシーを選択する」**ドロップダウンから、Apple SCEP テンプレートを選択します。
6. **「保存」**をクリックして、カスタム Apple SCEP デバイス ID ポリシーを保存します。ポリシーのデプロイ時に、必要なパラメーターが SCEP (Simple Certificate Enrollment Protocol) の構成 (（ページ　　）) に従って置き換えられます。

ポリシーを適切なポリシー・グループに追加して、Apple デバイスにデプロイします。

Apple 電子メールのサンプル・テンプレート

Apple デバイスでは、ポリシーを使用して 電子メール構成を管理 (（ページ　　）)できます。専用の電子メール・クライアント・アプリ (Outlook など) または Web ベースのソリューション (Google Workspace など) を使用するように登録済みデバイスを設定できます。このセクションでは、WebUI のテンプレートを使用してカスタム Apple 電子メール・ポリシーを作成する方法について説明します。

Apple 電子メール・テンプレートからカスタム・ポリシーを作成するには、次の手順を実行します。

1. WebUI から、**「アプリ」 > 「MCM」**を選択します。
2. WebUI の MCM ダッシュボードが表示されます。**「ポリシーの作成」**をクリックします。
3. 使用可能なポリシー・オプションのリストから、**「テンプレートからカスタム」**を選択します。
4. 「一般設定」ページで、次の手順を実行します。
    a. **「ポリシー名」**と**「説明」**を入力します。
    b. **「オペレーティング・システム」**には、**macOS** または **iOS/iPadOS** を選択します。
    c. **「サイトへのポリシーの割り当て」**ドロップダウンから、ポリシーを割り当てるサイトを選択します。
    d. **「テンプレート・ポリシー」**セクションの**「テンプレートからポリシーを選択する」**ドロップダウンで**「Apple 電子メール・サンプル・テンプレート」**を選択し、必要なパラメーターを編集します。

        注: すべてのプレースホルダー情報に、特定の値を入力するか、リストから値を選択します。
        - テンプレートの **%%** は、入力の必要があるデータのプレースホルダーを示します
        - **| (垂直バー)** は、選択可能なパラメーターの選択肢を示します。

        必要な設定については、「Apple デバイスのメール MDM ペイロード設定」を参照してください。

        。
    e. **「保存」**をクリックして、カスタム電子メール・ポリシーを保存します。

macOS または iOS/iPadOS のポリシー・グループ (（ページ） *386)*に、保存したポリシーを追加してデプロイします。MDM 登録 Apple デバイスにこのポリシーをデプロイすると、システムは登録時に入力されたプライマリー・ユーザーの名前と E メール・アドレスを取得して、電子メール・アプリにログインします。

Apple VPN サンプル・テンプレート

Apple デバイスでは、ポリシーを使用して VPN 構成を管理 (（ページ　　)できます。このセクションでは、WebUI のテンプレートを使用してカスタム Apple VPN ポリシーを作成する方法について説明します。

Apple VPN テンプレートからカスタム・ポリシーを作成するには、次の手順を実行します。

1. WebUI から、**「アプリ」 > 「MCM」**を選択します。
2. WebUI の MCM ダッシュボードが表示されます。**「ポリシーの作成」**をクリックします。
3. 使用可能なポリシー・オプションのリストから、**「テンプレートからカスタム」**を選択します。
4. 「一般設定」ページで、次の手順を実行します。
   a. **「ポリシー名」**と**「説明」**を入力します。
   b. **「オペレーティング・システム」**には、**macOS** または **iOS/iPadOS** を選択します。
   c. **「サイトへのポリシーの割り当て」**ドロップダウンから、ポリシーを割り当てるサイトを選択します。
   d. **「テンプレート・ポリシー」**セクションの**「テンプレートからポリシーを選択する」**ドロップダウンで**「Apple VPN サンプル・テンプレート」**を選択し、必要なパラメーターを編集します。

      注: すべてのプレースホルダー情報に、特定の値を入力するか、リストから値を選択します。
      - テンプレートの **%%** は、入力の必要があるデータのプレースホルダーを示します
      - **| (垂直バー)** は、選択可能なパラメーターの選択肢を示します。

      必要な設定については、「Apple デバイスの VPN 設定の概要」を参照してください。
   e. **「保存」**をクリックして、カスタム VPN ポリシーを保存します。

macOS または iOS/iPadOS のポリシー・グループ (（ページ） *386)*に、保存したポリシーを追加してデプロイします。MDM 登録 Apple デバイスにこのポリシーをデプロイすると、MCM サーバーはデバイスに VPN プロファイルを作成します。ユーザーが VPN に接続すると、インストールおよび設定時に設定された VPN 資格情報が取得され、VPN 接続が確立されます。

Apple WiFi サンプル・テンプレート

Apple デバイスでは、ポリシーを使用して WiFi 構成を管理 (（ページ）)できます。このセクションでは、WebUI のテンプレートを使用してカスタム Apple WiFi ポリシーを作成する方法について説明します。

Apple WiFi テンプレートからカスタム WiFi ポリシーを作成するには、次の手順を実行します。

1. WebUI から、**「アプリ」 > 「MCM」**を選択します。
2. WebUI の MCM ダッシュボードが表示されます。**「ポリシーの作成」**をクリックします。
3. 使用可能なポリシー・オプションのリストから、**「テンプレートからカスタム」**を選択します。
4. 「一般設定」ページで、次の手順を実行します。
    a. **「ポリシー名」**と**「説明」**を入力します。
    b. **「オペレーティング・システム」**には、必要に応じて **macOS** または **iOS/iPadOS** を選択します。
    c. **「サイトへのポリシーの割り当て」**ドロップダウンから、ポリシーを割り当てるサイトを選択します。
    d. **「テンプレート・ポリシー」**セクションの**「テンプレートからポリシーを選択する」**ドロップダウンで**「Apple WiFi サンプル・テンプレート」**を選択し、必要なパラメーターを編集します。

    注: すべてのプレースホルダー情報に、特定の値を入力するか、リストから値を選択します。

- テンプレートの **%%** は、入力の必要があるデータのプレースホルダーを示します
- **| (垂直バー)** は、選択可能なパラメーターの選択肢を示します。

必要な設定については、「Apple デバイスの WiFi MDM 設定」を参照してください。

e. **「保存」**をクリックして、Apple カスタム WiFi ポリシーを保存します。

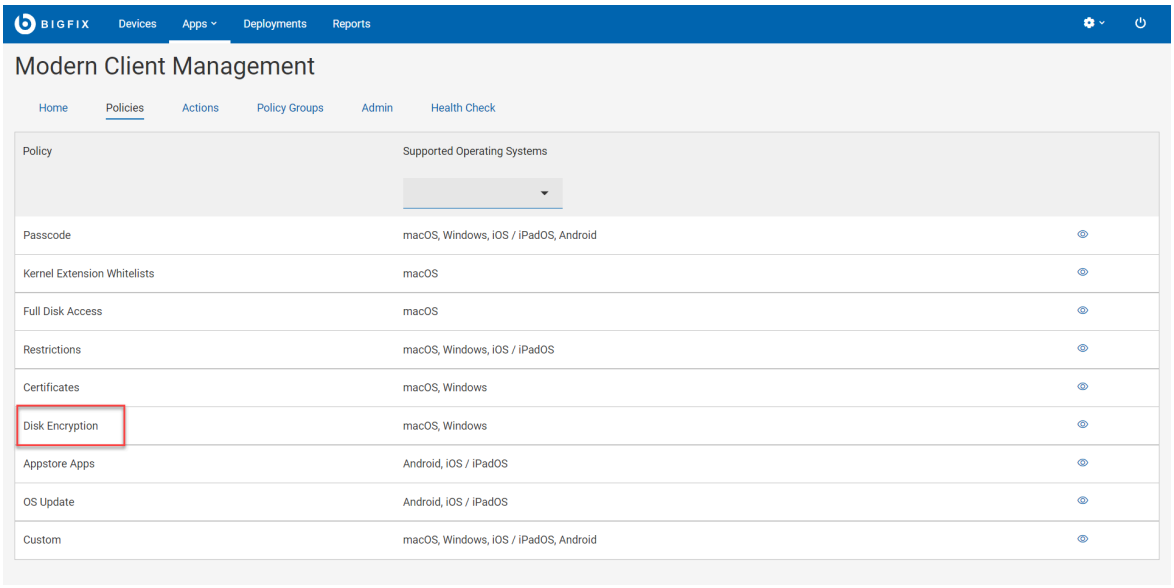
macOS または **iOS/iPadOS** 用の ポリシー・グループ (（ページ） *386)* に、保存された WiFi ポリシーを追加し、必要に応じてデプロイします。この WiFi ポリシーが MDM 登録 Apple デバイスにデプロイされると、Wi-Fi 設定はポリシーに従ってデバイス上で自動的に構成されます。

ディスク暗号化ポリシー

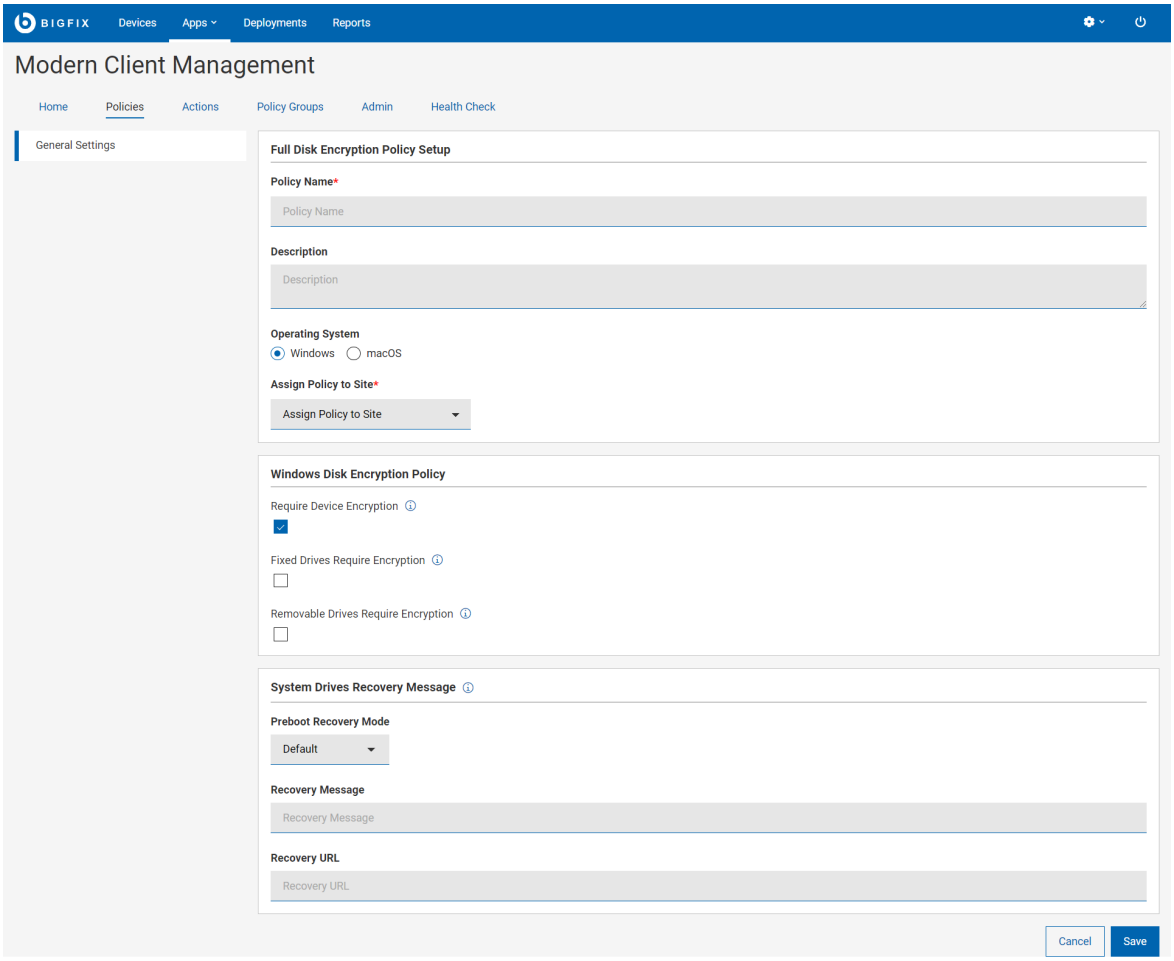
ユーザーは、他の MDM ポリシーと同様に、フル・ディスク暗号化 (FDE) ポリシーを作成してデプロイできます。

詳しくは、フル・ディスク暗号化 (（ページ）)を参照してください。FDE ポリシーを作成するには、以下のステップを実行します。

1. WebUI のメイン画面で、**「アプリケーション」 > 「MCM」**をクリックし、右上にある**「ポリシーの作成」**をクリックします。
2. ポリシー・タイプのリストから、**「ディスク暗号化」**を選択します。

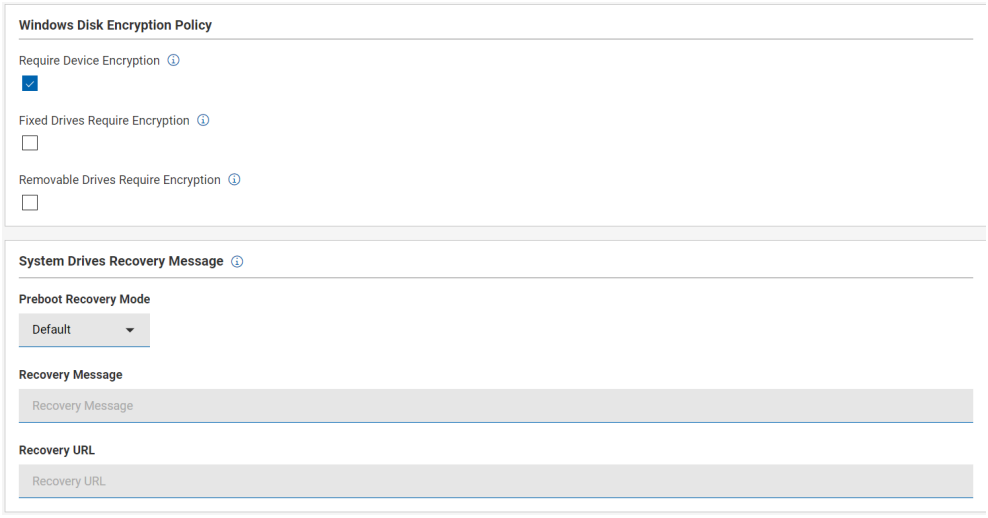


3. 「ディスク暗号化ポリシー」ページで、必要な情報を入力します。



Windows

オペレーティング・システムに Windows を選択した場合は、以下の情報を指定します。クライアント UI オファーが (利用可能で) 必要か、またはすぐに再開する必要があるか、構成する必要があります。



- Windows ディスク暗号化ポリシー
  - **デバイスの暗号化が必要**: ディスク暗号化を適用する場合に選択します。これは、デフォルトで選択されています。
  - **修正されたドライブには暗号化が必要** : この設定は、固定データ・ドライブをコンピューター上で書き込み可能にするために、BitLocker による保護が必要かどうかを判別します。暗号化されていない場合、固定ドライブは読み取り専用のままになります。
  - **リムーバブル・ドライブには暗号化が必要** : この設定は、コンピューターがリムーバブル・データ・ドライブにデータを書き込むことができるようにするために、BitLocker による保護が必要かどうかを設定します。暗号化されていない場合、リムーバブル・ドライブは読み取り専用のままになります。
- システム・ドライブのリカバリー・メッセージ: この設定では、OS ドライブがロックされたときにプリブート・キー・リカ

バリー画面に表示されるリカバリー・メッセージ全体を設定したり、既存の URL を置き換えたりすることができます。

- プリブート・リカバリー・モード
  - 無効
  - デフォルト
  - カスタム・メッセージ
  - カスタム URL
- リカバリー・メッセージ: リカバリー・メッセージが BitLocker リカバリー・ページに表示されます。
- リカバリー・URL

macOS

オペレーティング・システムに macOS を選択した場合は、以下の情報を指定します。

- macOS ディスク暗号化ポリシー
  - **リカバリー・キーの出力パス** 。リカバリー・キー情報が保管されるパスを指定できるオプション・フィールド。
  - **リカバリー・キー・エスクローの場所**: リカバリー・キーがエスクローされる場所の説明。このテキストは、FileVault を有効にするときにユーザーに表示されるメッセージに挿入されます。必須フィールド。リカバリー・キーを取得する場所についてユーザーに表示できるメッセージを入力します。例えば、 ヘルプ・デスクのサポート。

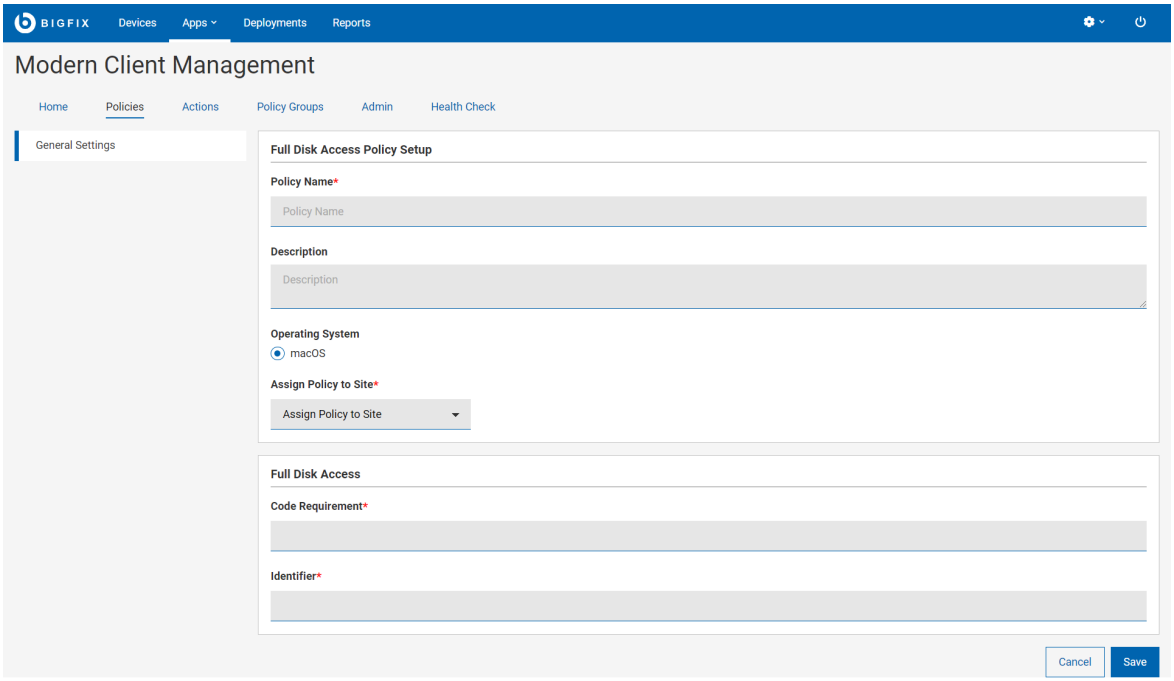
注: macOS デバイスでフル・ディスク暗号化を有効にすると、自動ログインが無効になります。詳しくは、https://support.apple.com/en-us/HT201476 および https://support.apple.com/en-us/HT204837 の Apple 公式ドキュメントを参照してください。

4. **「保存」**をクリックします。

フル・ディスク・アクセス

このセクションを使って、フル・ディスク・アクセス・ポリシーを作成できます。フル・ディスク・ポリシーを作成すると、BigFix エージェント (およびその他のアプリケーション) は OSX デバイス上でスムーズに機能します。フル・ディスク・ポリシーを使用して構成されたアプリケーションには、OSX 上で完全なディスク・アクセスが許可されます。

1. ポリシー・タイプのリストから**「フル・ディスク・アクセス」**を選択します。



2. **「一般設定」**で、ポリシー名と説明を入力します。
3. ドロップダウンからサイトを選択し、ポリシーをサイトに割り当てます。

> **注:** マスター以外のオペレーターの場合は、アクセスできるサイトのみドロップダウンに表示されます。

4. **「フル・ディスク・アクセス」**で、「コード要件」と「識別子」を入力します。
5. **「保存」**をクリックします。
6. デプロイするポリシー・グループにポリシーを追加します。

カーネル拡張ホワイトリスト

カーネル拡張機能は、開発者が macOS カーネルに動的にコードを読み込む機能を提供します。これにより、内部カーネル・インターフェースにアクセスできるため、複雑なアプリケーションが正常に機能します。

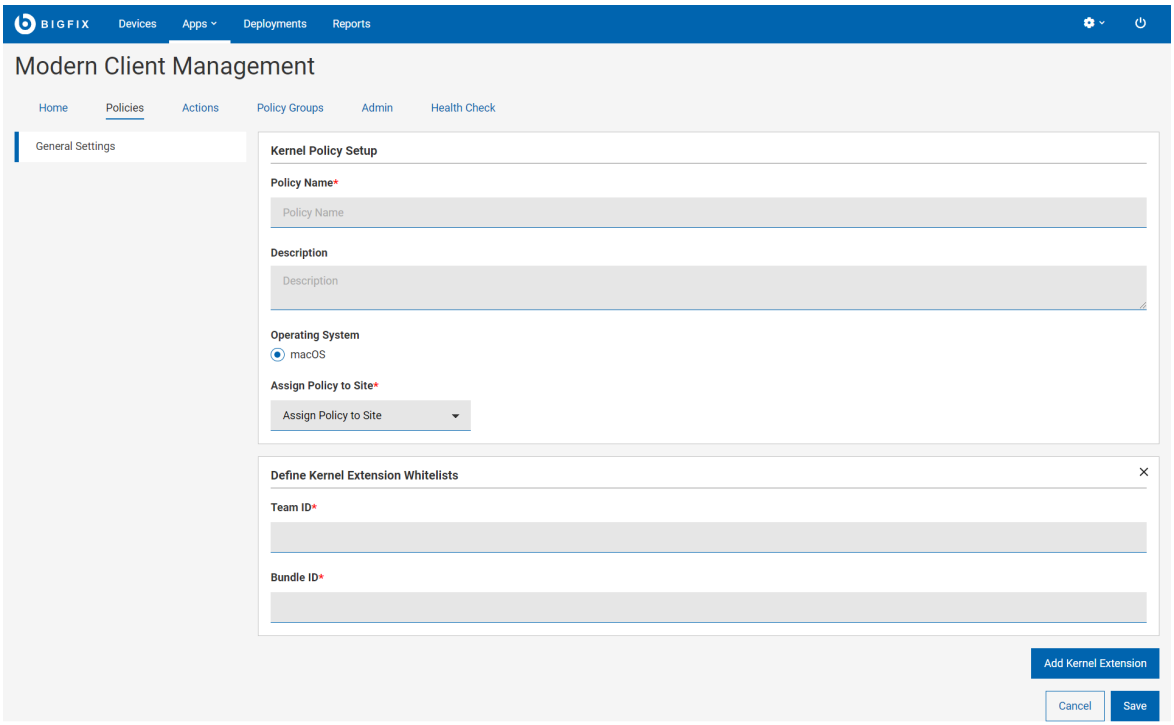
カーネル拡張について詳細は、「カーネル拡張の概要」を参照してください。

特定のアプリケーションに関連付けられているカーネル拡張機能が macOS MDM を介してホワイトリストに登録されている場合、これらのアプリケーションはユーザーの介入や承認なしにシームレスにインストールできます。

特定のアプリケーションのカーネル拡張ホワイトリスト用の macOS MDM ポリシーを作成できます。カーネル拡張を使用して特定のアプリケーションをインストールする前に、作成したカーネル拡張ホワイトリスト・ポリシーを適用する必要があります。

カーネル拡張ホワイトリスト・ポリシーを作成するには、次の手順に従います。

1. MDM アプリケーションを開きます。
2. **「ポリシーの作成」**をクリックします。
3. ポリシー・タイプのリストから**「カーネル拡張ホワイトリスト 」**を選択します。以下のページが表示されます。



4. **「一般設定」**に以下の詳細を入力します。
   - **ポリシー名**: カーネル拡張ホワイトリスト・ポリシーの名前を入力します。
   - **説明**: ポリシーの説明を入力します。
   - **オペレーティング・システム**: これは macOS にのみ適用されるので、変更できません。
   - **サイトへのポリシーの割り当て**: ドロップダウン・メニューからサイトを選択し、ポリシーを選択したサイトに割り当てます。マスター以外のオペレーターの場合は、アクセスできるサイトのみドロップダウン・メニューに表示されます。
5. **「カーネル拡張ホワイトリストを定義」**の「チーム ID」と「バンドル ID」を入力します。
   - **チーム ID**: チーム ID は、特定の開発チームに固有です。これは、KEXT 証明書識別子に署名するための開発者またはベンダーの開発者 ID である英数字の文字列です。
   - **バンドル ID**: バンドル ID は、特定のベンダーのアプリケーションを一意に識別する英数字の文字列です。特定のチーム ID に対して、複数のバンドル ID をコンマで区切って指定できます。

sqlite3 を使用してチーム ID とバンドル ID を識別するには、次の手順を実行します。

a. サポートされている macOS バージョンを実行しているマシンにターゲット製品をインストールします。
b. フラグが設定されている拡張機能のインストールをユーザーが手動で承認できるようにします。
c. チーム ID とバンドル ID を取得するには、次のコマンドを使用して SQLite データベースを確認します。

```
sqlite3 /var/db/SystemPolicyConfiguration/KextPolicy
SELECT * FROM kext_policy;
```

このコマンドは、すべての製品にわたってマシン上で有効なすべてのカーネル拡張を表示します。ホワイトリストへの登録に関係するものを見つけ、ホワイトリストに登録するすべてのものを対象とするポリシーを作成する必要があります。

出力は次のようになります: `EQHXZ8M8AV|com.google.dfsfuse.filesystems.dfsfuse|1|Google, Inc.|8"`

ここで、`EQHXZ8M8AV` はチーム ID で `com.google.dfsfuse.filesystems.dfsfuse` はバンドル ID です。

注:

- 特定のベンダーのアプリケーションのカーネル拡張をホワイトリストに登録するには、チーム ID とバンドル ID の両方を指定する必要があります。
- リストの最後のエントリーのみが実際に使用されるので、同じチーム ID を持つ複数のエントリーを追加しないでください。同じチーム ID を使用してホワイトリストに登録する複数のアプリケーションがある場合は、すべてのバンドル ID をコンマで区切って 1 つのエントリーに追加します。例:

```
Bundle IDs: BundleID1,BundleID2,BundleID3
```

6. **カーネル拡張の追加**: 1 つのポリシー内で異なるベンダーの複数の製品をホワイトリストに登録する場合は、「拡張の追加」をクリックして、チーム ID とバンドル ID を同じポリシーに追加します。
7. **「保存」**をクリックします。カーネル拡張ホワイトリストの作成が完了しました。

キオスク・ポリシー

Android、iOS、および iPad デバイス用のキオスク・ポリシーを作成する方法について説明します。ここでは、キオスク・モードでデバイスをロックダウンし、デバイス・ユーザーが構成済みのアプリとデバイス設定のみにアクセスできるように制限するアプリと設定を構成できます。

Android または iOS/iPadOS デバイス用に、シングルアプリまたはマルチアプリ・キオスク・ポリシーを作成できます。キオスク管理について詳しくは、「キオスク管理」を参照してください。キオスク・ポリシーを作成するには、以下の手順を実行します。

1. WebUI のメイン・ページで、**「アプリケーション」 > 「MCM」**をクリックし、右上にある**「ポリシーの作成」**をクリックします。
2. ポリシー・タイプのリストから、**「キオスク」**を選択します。
3. 「キオスク・ポリシー・セットアップ」ページで、以下の情報を入力します。
    - ポリシー名: 一意で意味のあるポリシー名を入力します。
    - 説明: ポリシーの説明を入力します。
    - オペレーティング・システム: ターゲット・デバイスのオペレーティング・システムを選択します。
    - サイトへのポリシーの割り当て: ポリシーを割り当てることができるサイトを選択します。
    - キオスク・モード:
        - シングル・アプリ - シングル・アプリを使用してキオスク・モードでデバイスをロックする場合は、このオプションを選択します。デバイス・ユーザーは、構成されているシングル・アプリ以外のアプリにはアクセスできません。
        - マルチアプリ - デバイス・ユーザーがキオスク・モードで複数のアプリにアクセスできるようにするには、このオプションを選択します。マルチアプリ・キオスク・モードでは、承認された一連のアプリケーションへ

のユーザー・アクセスを制限し、ユーザーが選択したアプリのみを使用できる制御された環境を作成できます。このモードは、キオスク環境内で複数のアプリへのアクセスを許可しながら、限定された機能を提供したい場合に便利です。

4. アプリの選択: 使用可能なアプリは、 (（ページ）)にリストされています。必要に応じて 1 つ以上のアプリを選択します。
    - **Android**

        シングル・アプリ: 「シングル・アプリ」オプションを選択した場合、利用可能なアプリから複数のアプリを選択できますが、シングル・アプリの**「プライマリー」**ラジオ・ボタンを選択する必要があります。プライマリー・アプリはデバイスのホーム画面に位置が固定されています。選択した他のアプリはサポート・アプリとしてインストールされますが、ユーザーは位置固定されたプライマリー・アプリから移動したり終了したりすることはできません。

        複数のアプリ: マルチアプリ・オプションを選択した場合、複数のアプリを選択でき、ユーザーはキオスク・モードのデバイス内の選択したすべてのアプリにアクセスできます。

    - **iOS/iPadOS**

        シングル・アプリ: 「シングル・アプリ」オプションを選択した場合、使用可能なアプリから 1 つのアプリのみ選択できます。デバイス・ユーザーはそのアプリにのみアクセスできます。

        複数のアプリ: マルチアプリ・オプションを選択した場合、複数のアプリを選択でき、ユーザーはキオスク・モードのデバイス内の選択したすべてのアプリにアクセスできます。
5. オプションのカスタマイズ設定を構成します。

    Android シングル・アプリ・キオスク・モード

    シングル・アプリ・キオスク・モードで画面キャプチャーを有効または無効にすることができます。

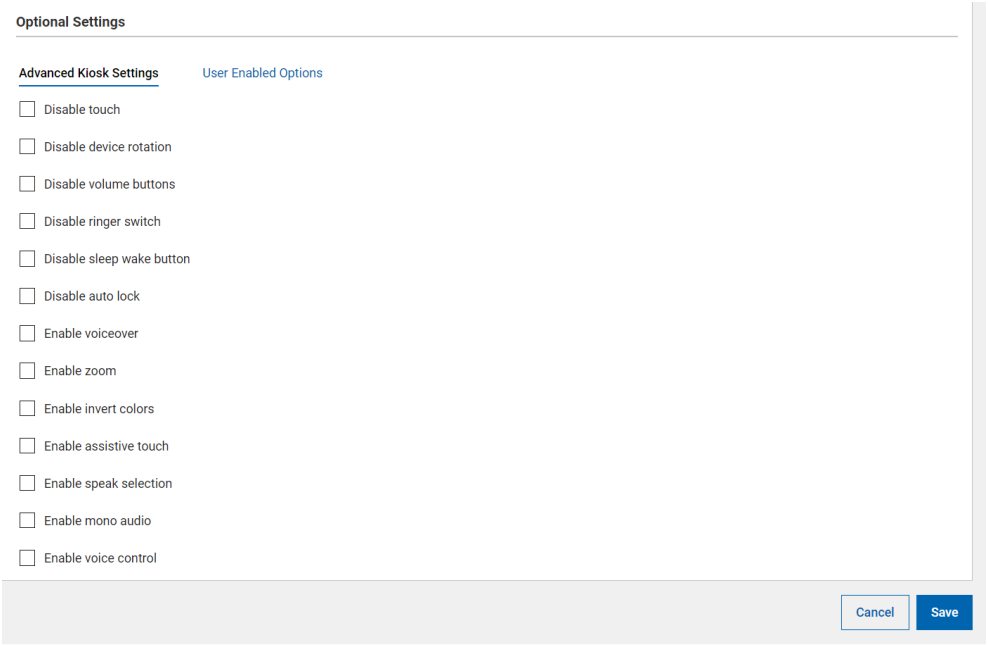
    Android マルチアプリ・キオスク・モード

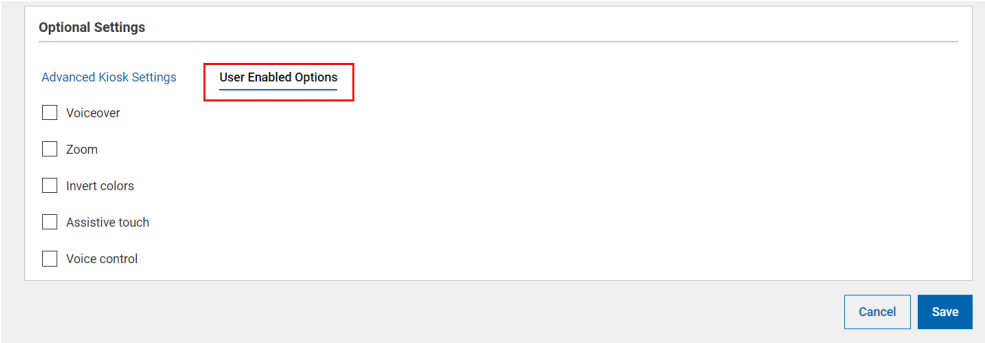
マルチアプリ・キオスク・モードでは、以下のデバイス設定を構成できます。

- 画面キャプチャーの無効化
- 音量調整無効
- 電源ボタンの操作
- システム・エラーの警告
- システム・ナビゲーター
- ステータス・バー
- デバイスの設定

iOS/iPadOS シングル・アプリ・キオスク・モード

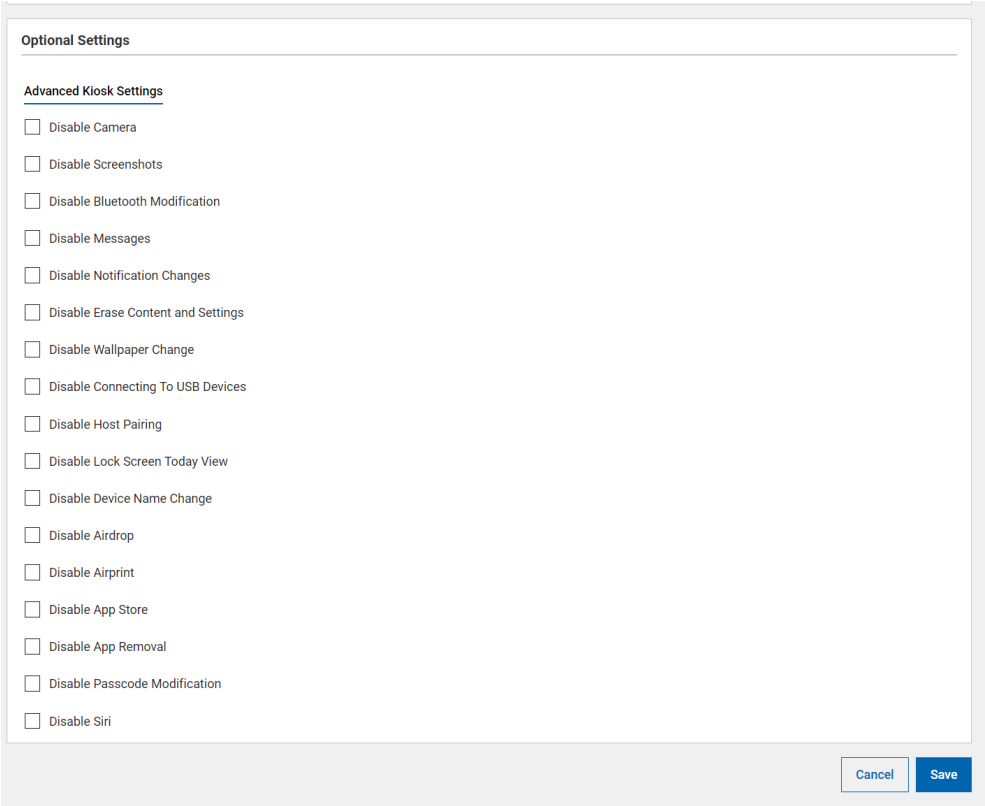
このページから、シングル・アプリ・キオスク・モードの以下のオプション設定を構成できます。





iOS/iPadOS マルチアプリ・キオスク・モード

このページから、マルチアプリ・キオスク・モードの以下のオプション設定を構成できます。



6. **「保存」**をクリックします。ポリシーが保存され、WebUI には保存されたキオスク・ポリシーのすべての情報が表示されます。

キオスク・ポリシーは、専用 Android デバイスおよび監視対象 iOS/iPadOS デバイスにのみ適用されます。専用デバイスまたは監視対象デバイスのみを対象とするポリシー・グループにキオスク・ポリシーを確実に追加します。

重要: キオスク・モード・デバイスを設定するには、ポリシー・グループを使用する必要があります。

iOS キオスク・ポリシーをマルチアプリからシングルアプリ (またはその逆) に変更する

Android キオスク・ポリシーとは異なり、iOS/iPadOS キオスク・ポリシーを編集してマルチアプリからシングルアプリ (またはその逆) に変更することはできません。

キオスク・モードを変更する場合は、必要な設定をした別個のキオスク・ポリシーを作成してポリシー・グループに追加し、デバイスにデプロイする必要があります。

OS の更新ポリシー

OS の更新ポリシーを使用して、Android、macOS、iOS/iPadOS デバイスのシステム更新を管理できます。OS の更新は、自動的にインストールするように、またはメンテナンス期間中にインストールするように設定できます。これにより、ユーザーが操作しなくてもシステム更新をインストールできます。

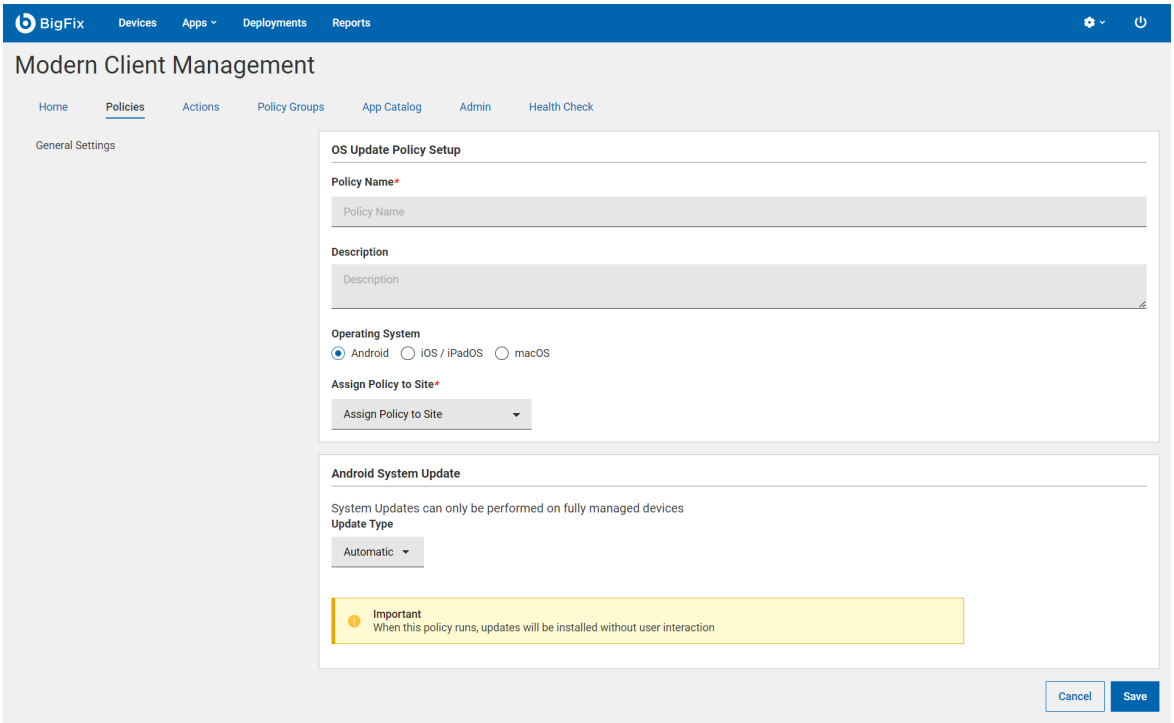
iOS/iPadOS デバイスが OS 更新をサポートするための前提条件:

- iOS 10.3 以降では、サポートされているソフトウェア更新コマンドは監視が必要ですが、DEP 登録は必要ありません。つまり、デバイスは OTA 登録または DEP 登録のいずれかになります。デバイスにパスコードがある場合、ユーザーはパスコードを入力してソフトウェア更新を開始する必要があります。☒
- iOS 10.3 以前のバージョンでは、監視対象デバイスはパスコードがなく、DEP 登録されている必要があります。
- 電源に接続されている場合を除き、バッテリーレベルが 50% を下回ると、更新プログラムはインストールされません。

OS の更新ポリシーの作成

OS の更新ポリシーを作成するには、以下のステップを実行します。

1. BigFix WebUI にログインします。
2. **「アプリケーション」 > 「MCM」**に移動します。
3. 右上隅にある**「ポリシーの作成」**をクリックします。
4. ポリシー・タイプのリストから**「OS の更新ポリシー」**を選択します。**「OS 更新ポリシー」**ページが表示されます。



5. **「一般設定」**セクションで、OS の更新ポリシーの名前と説明を入力します。
6. **オペレーティング・システム**を選択します。
7. **「サイトへのポリシーの割り当て」**ドロップダウンからサイトを選択します。
8. OS に固有の設定を構成します。

Android システムの更新

このセクションは、オペレーティング・システムとして「Android」を選択した場合に表示されます。この機能は、完全管理対象デバイスまたは専用デバイスで Android バージョン 10 以降を実行している場合に使用できます。必要な**「更新タイプ」**を選択します。

- **自動**: 使用可能になったシステム更新は (ユーザーが操作しなくても) インストールされます。このポリシー・タイプを設定すると、延期済みまたはメンテナンス・ウィンドウで待機中だった保留中の更新が直ちにインストールされます。
- **ウィンドウ表示**: 日次メンテナンス・ウィンドウで (ユーザーが操作しなくても) システム更新がインストールされます。ウィンドウ表示されたポリシーを作成するには、日次メンテナンス・ウィンドウの開始時刻と終了時刻を設定します。
- **延期済み**: システム更新のインストールを 30 日間延期します。30 日が経過すると、システムはデバイス・ユーザーに更新のインストールを求めるプロンプトを表示します。

iOS/iPadOS システムの更新

このセクションは、オペレーティング・システムとして「iOS/iPadOS」を選択した場合に表示されます。iOS/iPadOS の場合、システム更新は監視対象のデバイスでのみ実行できます。このポリシーをデプロイすると、選択した更新タイプを定期的に実行する未処理アクションが作成されます。

- **バージョン**: ここでは、環境内で検出された、使用可能な特定のバージョンが一覧表示されます。また、「最新」を選択すると、バージョンに関係なく最新版に更新できます。
- **更新タイプ**:
  - **ダウンロードとインストール**: デバイスの状態に応じて、システム更新をダウンロードまたはインストールします。更新をインストールするには、ポリシー・アクションの 2 つのアプリケーションが必要です。
  - **ダウンロードのみ**: ソフトウェアの更新がダウンロードされますが、インストールはされません。
  - **インストールのみ:** : ダウンロード済みの更新をインストールします。

    注: : デバイスでパスコードが設定されていない場合、デバイスはインストールの実行時にエンド・

ユーザーにプロンプトを出さずに再起動されます。パスコードが設定されている場合、デバイス・ユーザーに更新のインストールを求めるプロンプトが表示されます。ユーザーは拒否することもできます。

- **頻度の適用 (日)**: ドロップダウンからオプションを選択して、システム更新を実行する頻度を設定します。

macOS

これらのセクションは、オペレーティング・システムとして macOS を選択した場合に表示されます。

- **全般的な macOS システムの更新設定**: macOS ソフトウェアの更新設定を構成し、Mac が新しい更新を自動的に確認してダウンロードするかどうかを指定します。
- **macOS 更新の遅延設定**: 必要に応じて、監視対象デバイスでの新しいシステム・ソフトウェア更新の表示を最大 90 日間遅延させるように設定します。この機能を使用すると、新しい更新を含む重要なアプリケーションやインフラストラクチャーをテストしてからデプロイできます。

9. **「保存」**をクリックします。

OS 更新ポリシーが作成され、ポリシー・グループに追加し、必要に応じて Android、iOS/iPadOS、macOS デバイスにデプロイできるようになります。

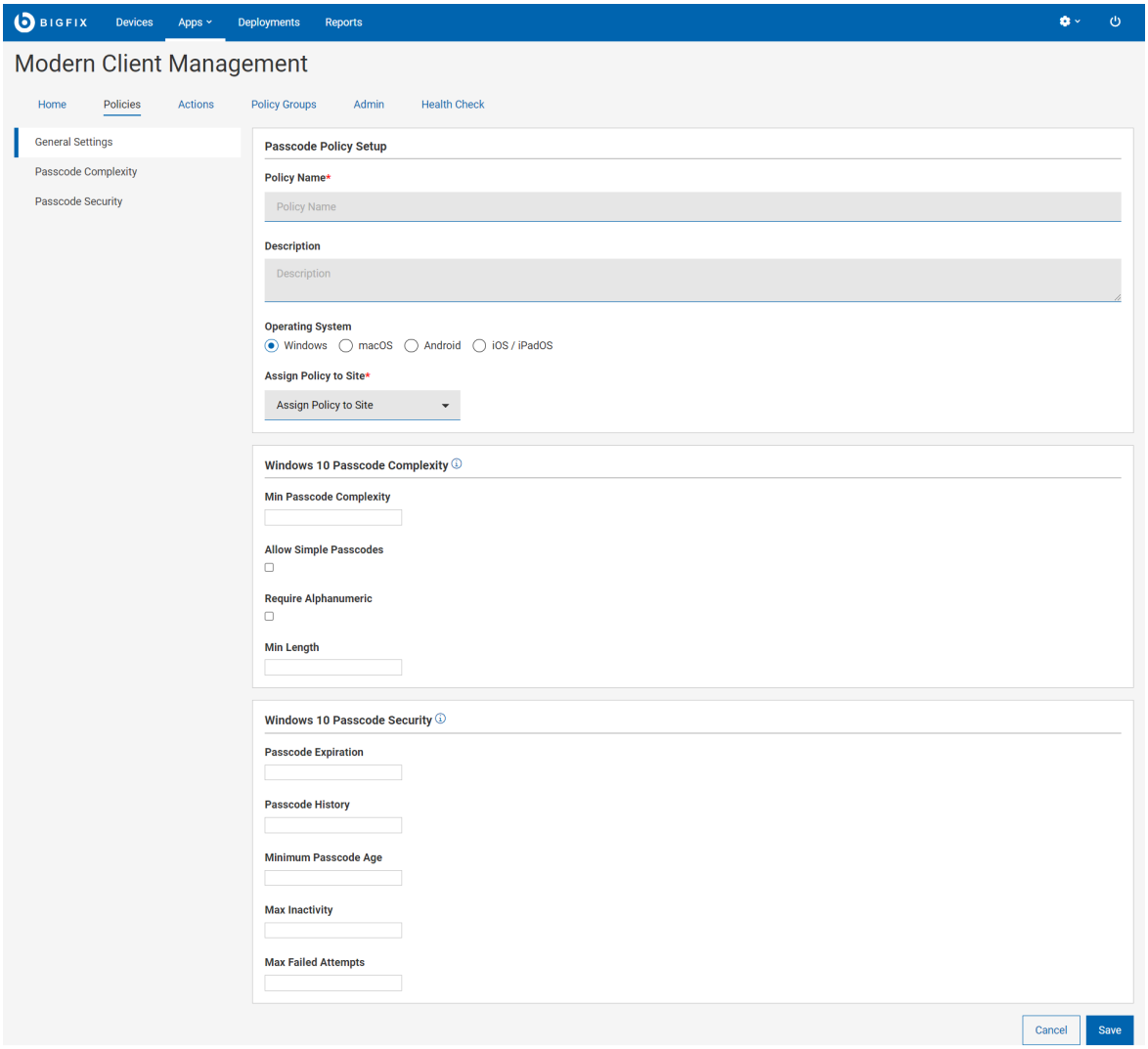
パスコード・ポリシー

パスコード・ポリシーによって、BigFix 管理者は
Windows、macOS、iOS、iPadOS、Android MDM デバイスにおいて、さまざまなパスワード/非アクティブ設定をロックダウンできます。

次の手順でパスコード・ポリシーを作成します。

1. WebUI にログインします。
2. WebUI のメイン・ページから、**「アプリ」 > 「MCM」**をクリックします。
3. **「ポリシーの作成」**をクリックします。

4. **「パスコード」**を選択し、パスコード・ポリシーを作成します。
5. 左側のナビゲーション・バーで**「一般設定」**をクリックします。



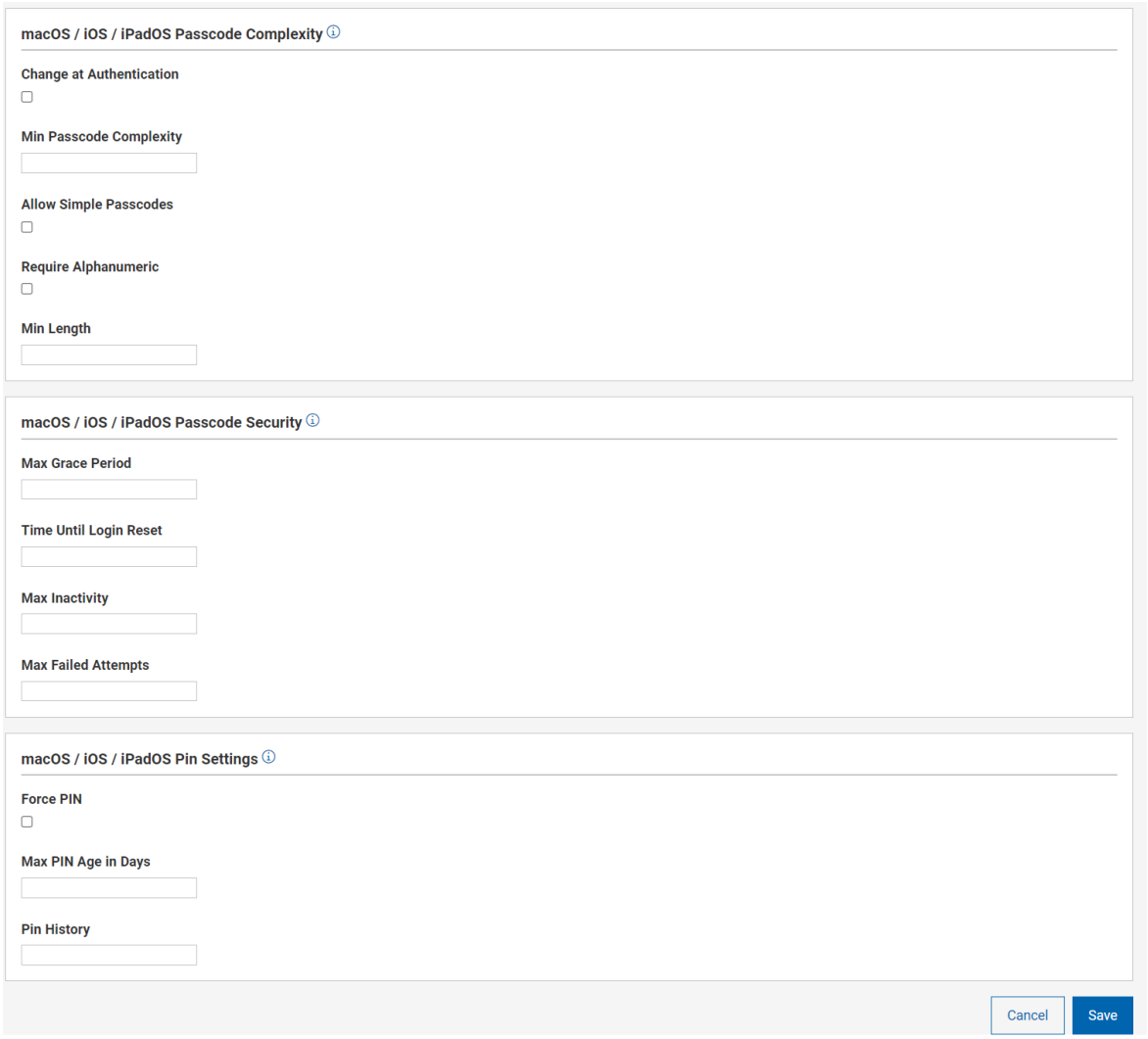
6. **「一般設定」**に詳細を入力します。
   a. **「ポリシー名」**を入力します。
   b. ポリシーの**「説明」**を入力します。

c. オペレーティング・システムを選択します。オペレーティング・システムを選択すると、そのオペレーティング・システムに固有の追加フィールドが表示されます。
d. **「サイトへのポリシーの割り当て」**ドロップダウンからサイトを選択し、サイトにポリシーを割り当てます。マスター以外のオペレーターの場合は、自分がアクセスできるサイトのみドロップダウンに表示されます。

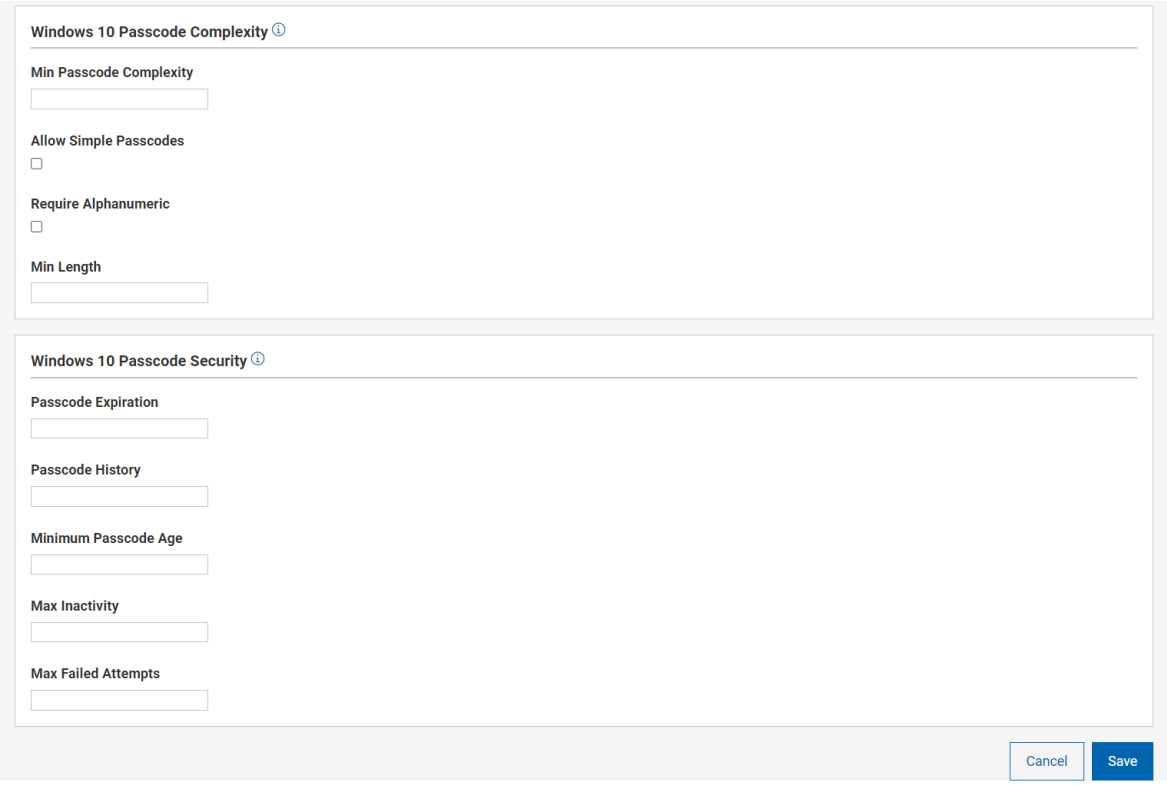
7. 選択した OS (Windows、macOS、Android、iOS/iPadOS) に固有の設定を構成します。各設定については、情報アイコンの上にマウスを置きます。
8. **「保存」**をクリックします。パスコード・ポリシーが作成され、デプロイの準備ができました。

オプション設定

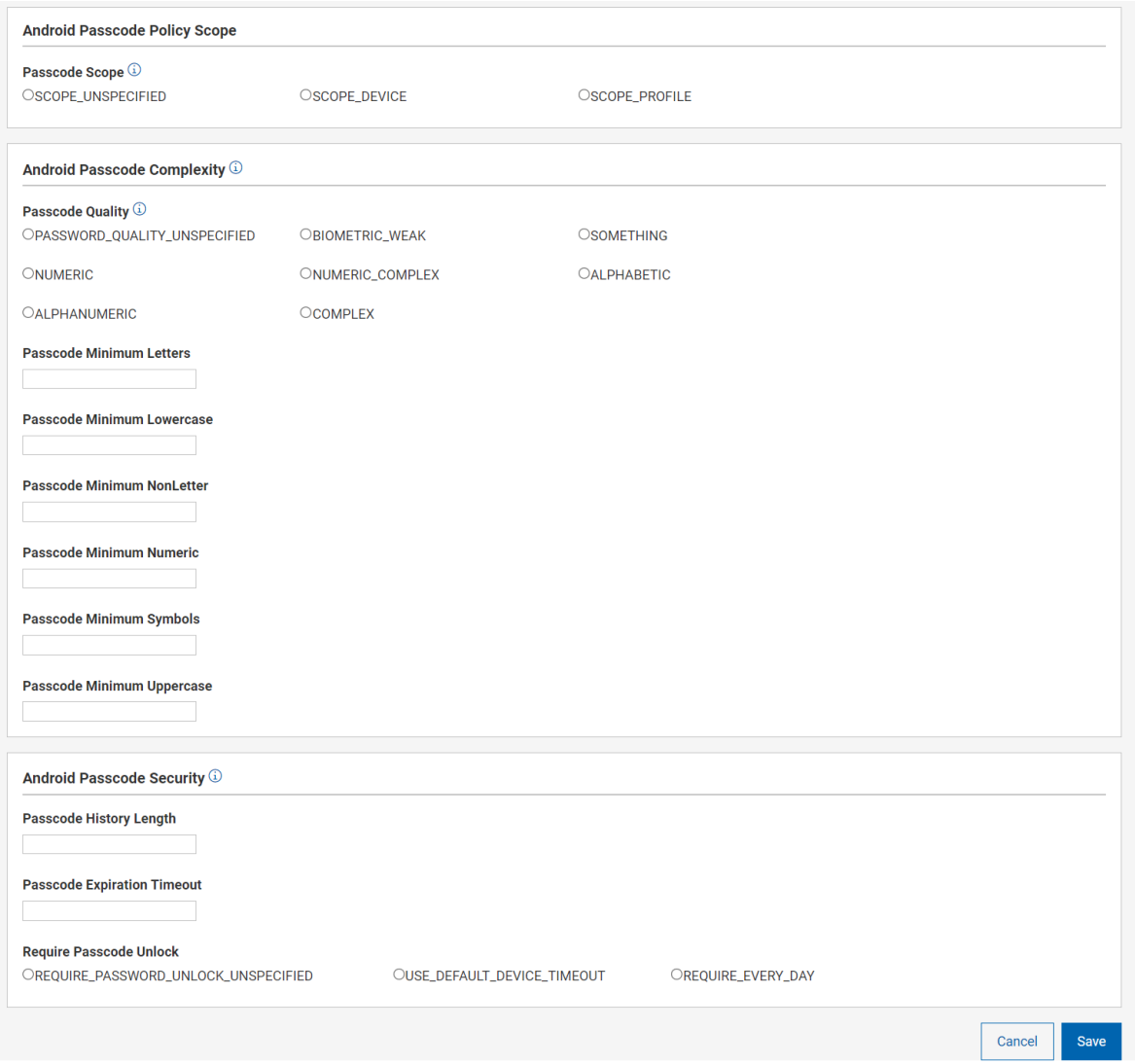
- macOS および iOS/iPadOS 固有の設定:



- Windows 固有の設定:



- Android 固有の設定

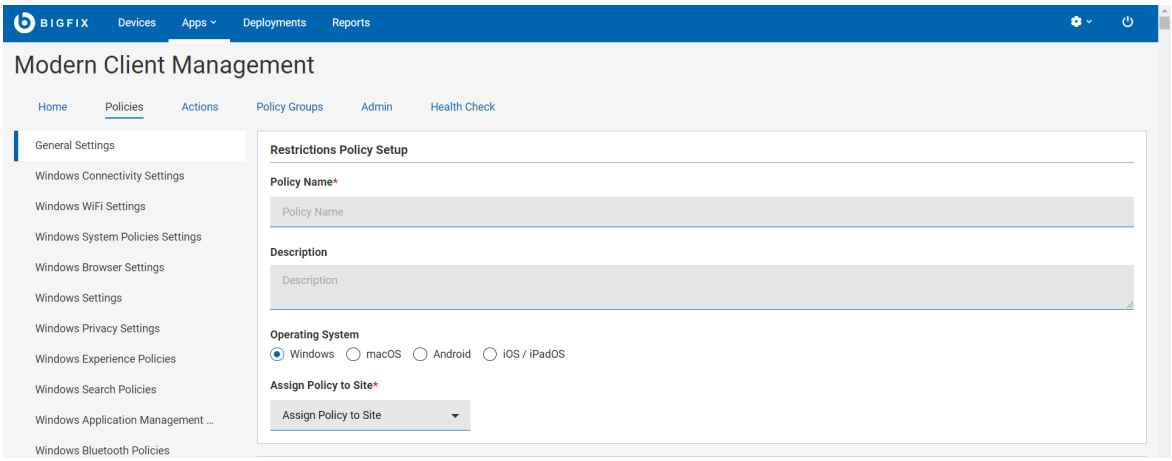


制限ポリシー

制限プロファイルを使用すると、会社のデバイスの機能を制御 (有効化または無効化) し、潜在的なセキュリティーの脅威を防ぐことができます。これにより、エンド・ユーザーはカメラの使用など、特定のデバイス機能を使用できなくなります。これは MacOS、iOS、iPadOS、Android、Windows でサポートされています。

制限ポリシーを作成するには、次のステップを実行します。

1. WebUI のメイン・ページから、**「アプリケーション」** > **「MCM」**を選択します。
2. 「Modern Client Management」ページの右隅にある**「ポリシーの作成」**ボタンをクリックします。
3. ポリシー・タイプのリストから**「制限」**を選択します。以下のページが表示されます。



4. **「一般設定」**セクションで、次の操作を行います。
   a. ポリシーの名前と説明を入力します。
   b. オペレーティング・システムを選択します。
   c. すべてのオペレーティング・システムには、固有の制限ポリシー・セットがあります。左側のナビゲーション・パネルで、選択した各オペレーティング・システム固有の設定に移動します。そのオペレーティング・システム固有の制限ポリシーの設定を設定できます。
   d. **「サイトへのポリシーの割り当て」**ドロップダウンで、「マスター・アクション・サイト」を選択します。
5. **「保存」**をクリックします。制限ポリシーが作成されます。

   ポリシーを確認し、**「ポリシーのデプロイ」**をクリックして、選択したデバイスにデプロイできます。

構成した設定で、選択したオペレーティング・システムの制限ポリシーが作成されました。

作成した制限ポリシーをポリシー・グループ (（ページ） *386)* に追加して、適格なデバイスにデプロイします。

Android の制限設定

管理者は、制限ポリシー設定を適用することで、ユーザーによる Android デバイスへのアクセスおよび操作を制御できます。

一部の設定は、会社所有のデバイスでのみ使用できます。詳しくは、『Add company owned devices to the inventory』を参照してください。

設定カテゴリーと設定をクリックします。詳しくは以下のセクションで、制限設定について参照してください。

https://support.google.com/a/answer/6328708?hl=en#top&zippy=%2Cavailable-apps%2Cusb-file-transfer%2Cphysical-media

---

関連情報

Android ハードウェア・セキュリティー (（ページ）　　)

iOSと iPadOS の制限の設定

モバイル・デバイス管理 (MDM) ソリューションに登録されている iPhone および iPad デバイスに対して、デバイスとその機能の変更などの制限を設定できます。

iPhone および iPad デバイスの MDM の制限について詳しくは、以下を参照してください。 https://support.apple.com/en-in/guide/deployment/dep0f7dd3d8/web

一部の制限は、監視対象でモバイル・デバイス管理 (MDM) ソリューションに登録されている Apple デバイスでのみ使用できます。詳しくは、次を参照してください。 https://support.apple.com/en-in/guide/deployment/dep6b5ae23e9/1/web/1.0

macOS 制限設定

MDM 登録済み macOS デバイスに対して、デバイスとその機能を変更するための制限を設定できます。

これらの設定について詳しくは、以下を参照してください。 https://developer.apple.com/documentation/devicemanagement/restrictions

Windows の制限の設定

Windows オペレーティング・システムにはさまざまな制限設定が用意されており、特定のコンピューターでのユーザー・アクセスと動作が制御されます。IT 管理者は、ポリシーを使用して Windows の制限の設定を構成し、システム・セキュリティを確保して、機密情報への不正アクセスやその変更を防止できます。

: MCM では、Windows デバイスで使用可能な制限設定のサブセットがサポートされます。MCM でサポートされている制限設定の完全なリストを表示するには、WebUI 制限ポリシー (（ページ） *451)* ページで Windows をオペレーティング・システムとして選択します。制限設定は、該当する Windows エディションおよびサービス・パック・レベルのエンドポイントでのみ機能します。特定の制限設定の範囲、エディション、該当する OS の詳細については、Microsoft のマニュアル、

https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-configuration-service-provider を参照してください。

関連情報

Windows 上の Microsoft Edge のホーム・ページの設定 (（ページ）)

システム拡張ホワイトリスト

システム拡張により、ネットワーク拡張機能やエンドポイント・セキュリティー・ソリューションなどのソフトウェアは、カーネル・レベルのアクセスを必要とせずに macOS の機能を拡張できます。

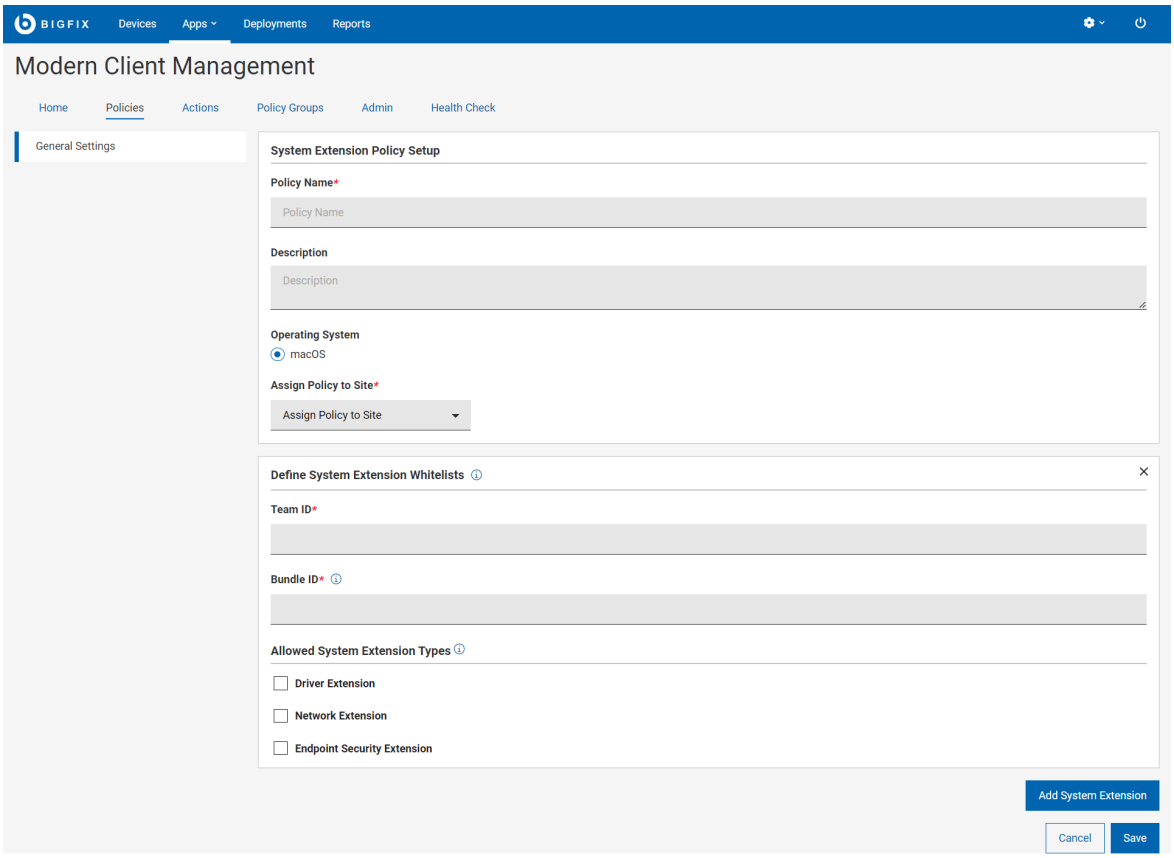
インストールが完了すると、ホワイトリストに登録された拡張機能を macOS システム上のすべてのユーザーが使用できるようになり、以前にカーネル拡張用に予約されていたタスクを実行できます。システム拡張について詳しくは、こちらを参照してください。

注:

- 1 つのポリシー自体に、複数のシステム拡張ホワイトリストを指定できます。
- 複数のシステム拡張ホワイトリスト・ポリシーを「ポリシー・グループ」(（ページ） 386)に追加してデプロイできます。

システム拡張ホワイトリスト・ポリシーを作成するには、次の手順に従います。

1. MDM アプリケーションを開きます。
2. **「ポリシーの作成」**をクリックします。
3. ポリシー・タイプのリストから**「システム拡張ホワイトリスト」**を選択します。以下のページが表示されます。



4. 次の詳細を入力します。

- **ポリシー名**: ポリシーの名前を入力します。
- **説明**: ポリシーの説明を入力します。
- **オペレーティング・システム**: これは macOS にのみ適用されるので、変更できません。
- **サイトへのポリシーの割り当て**: ドロップダウン・メニューからサイトを選択し、ポリシーを選択したサイトに割り当てます。マスター以外のオペレーターの場合は、アクセスできるサイトのみドロップダウン・メニューに表示されます。

5. **「システム拡張ホワイトリストを定義」**に、チーム ID とバンドル ID を入力します。
   - **チーム ID**: チーム ID は、特定の開発チームに固有です。これは 10 桁の英数字ストリングで、Apple が生成し、開発者またはベンダーの「開発者 ID」に関連付けます。
   - **バンドル ID**: バンドル ID は、システム拡張ポリシーを一意に識別する英数字のストリングです。特定のチーム ID に対して、複数のバンドル ID をコンマで区切って指定できます。

   チーム ID とバンドル ID を特定するには、以下のコマンドを使用して、ターミナル経由でマシンに存在するシステム拡張のリストを取得します。

   ```
   systemextensionsctl list
   ```

   このコマンドは、すべての製品にわたってマシン上で有効なすべてシステム拡張を表示します。ホワイトリストへの登録に関係するものを見つけ、ホワイトリストに登録するすべてのものを対象とするポリシーを作成する必要があります。

   出力は以下のようになります。

   ```
   bigfixmdm@LP2-US-xxxxxxxx mdm % systemextensionsctl list

   1 extension(s)

   --- com.apple.system_extension.network_extension

   enabledactiveteamIDbundleID (version)name[state]
   ```

```
**PXPZ95SK77com.paloaltonetworks.GlobalProtect.client.extension
 (5.2.6-87/1)GlobalProtectExtension[activated enabled]
```

ここで、`PXPZ95SK77` はチーム ID で `com.paloaltonetworks.GlobalProtect.client.extension` はバンドル ID です。

注:

- 特定のベンダーのアプリケーションのシステム拡張をホワイトリストに登録するには、チーム ID とバンドル ID の両方を指定する必要があります。
- リストの最後のエントリーのみが実際に使用されるので、同じチーム ID を持つ複数のエントリーを追加しないでください。同じチーム ID を使用してホワイトリストに登録する複数のシステム拡張がある場合は、すべてのバンドル ID をコンマで区切って 1 つのエントリーに追加します。例:

  ```
  Bundle IDs: BundleID1,BundleID2,BundleID3
  ```

- 拡張タイプを指定しない場合、ポリシーはチーム ID に関連付けられたすべてのシステム拡張が許可されていると想定します。

6. **許可されたシステム拡張タイプ:**
   - **ドライバー拡張**: DriverKit フレームワークを使用し、ユーザーが macOS にインストールできる USB、シリアル、NIC、HID デバイス用のドライバーを作成する場合に選択します。DriverKit について詳しくは、こちらを参照してください。
   - **ネットワーク拡張**: ネットワーク拡張アプリ (コンテンツ・フィルター、DNS プロキシー、VPN クライアントなど) を macOS のシステム拡張として配布する場合に選択します。ネットワーク拡張について詳しくは、こちらを参照してください。
   - **エンドポイント・セキュリティー拡張**: エンドポイント検出および応答ソフトウェア、アンチウィルス・ソフトウェアを含むエンドポイント・セキュリティー・クライアントは、新しいエンドポイント・セキュリティー API を使用

して、システム・イベントのモニターとブロックを行い、セキュリティー・ポリシーにさらに準拠し、潜在的な悪意のある行為から保護します。エンドポイント・セキュリティーについて詳しくは、こちらを参照してください。

7. **システム拡張の追加**: 1 つのポリシー内で異なるベンダーの複数の製品をホワイトリストに登録する場合は、「拡張の追加」をクリックして、チーム ID とバンドル ID を同じポリシーに追加します。
8. **「保存」**をクリックします。システム拡張ホワイトリストが作成されます。

システム拡張ホワイトリスト・ポリシーが作成され、デプロイの準備ができました。

作成したポリシーを「ポリシー・グループ」 (（ページ） *386)*に追加し、MDM サーバーまたは適格なデバイスにデプロイします。

カスタム・ポリシーのアップロード

カスタム・ポリシー・ファイルは、`.xml`、`.mobileconfig`、または `syncML` 形式でアップロードできます。

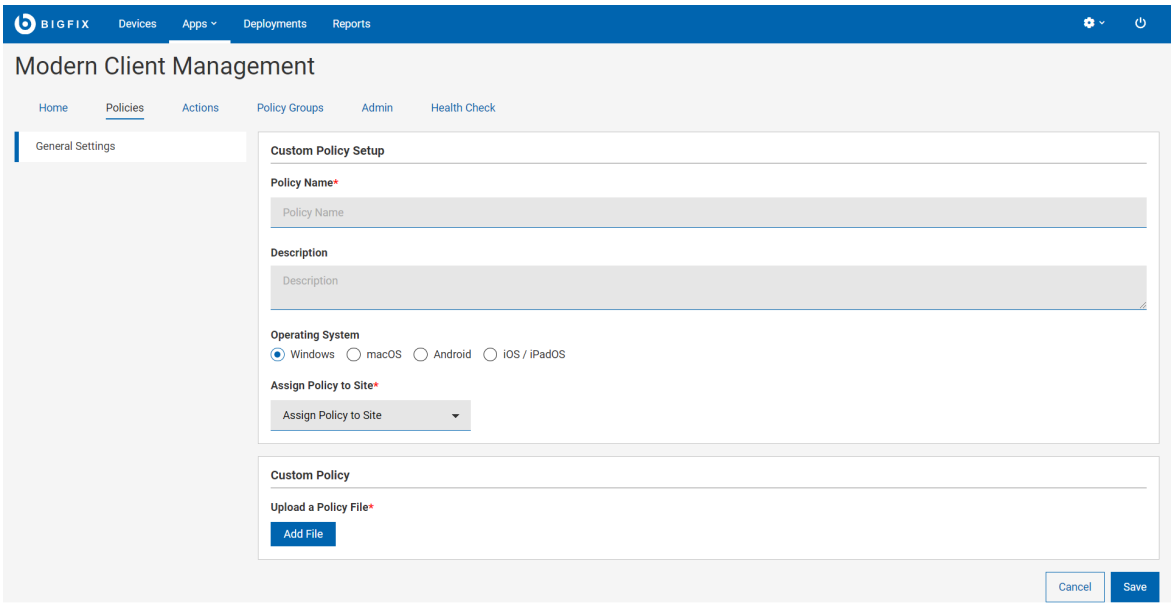
このウィザードを使って、カスタム・ポリシーを作成できます。

注:

- macOS/iOS/iPadOS では、プロファイル・クリエーターを使って、カスタム・ポリシーを作成し、`.mobileConfig` ファイルをカスタム・ポリシー・ウィザードにアップロードできます。
- Windows の場合、Windows のカスタム・ポリシーで使用できるすべての CSPS については、https://docs.microsoft.com/en-us/windows/client-management/mdm/configuration-service-provider-reference を参照してください。

- Android の場合、カスタム・ポリシーの構成に使用できる使用可能な設定の詳細については、 https://developers.google.com/android/management/reference/rest/v1/enterprises.policies を参照してください。
- Microsoft docs を使って、適切な .syncml または .xml ファイルをリファレンスとして作成後、ユーザーはそのファイルをカスタム・ポリシー・ウィザードにアップロードできます。

1. WebUI のメイン・ページから、**「アプリケーション」** > **「MCM」**を選択します。
2. 「Modern Client Management」ページの右隅にある**「ポリシーの作成」**ボタンをクリックします。
3. 表示されるポリシー・タイプのリストから**「カスタム」**を選択します。以下のページが表示されます。



。

4. **「一般設定」**で、ポリシーの名前と説明を入力します。
5. オペレーティング・システムを選択します。
6. ポリシーをサイトに割り当てるには、「サイトへのポリシーの割り当て」ドロップダウンからサイトを選択します。マスター以外のオペレーターの場合は、アクセスできるサイトのみドロップダウンに表示されます。

7. **注:**
   - 一度に 1 つのオペレーティング・システムのチェックボックスのみ選択できます。
   - 書き込み権限を持つサイトでのみ、ポリシーの作成とポリシーの割り当てができます。
8. 「カスタム・ポリシー」で**「ファイルの追加」**をクリックし、`.xml`、`.mobileconfig`、または `.syncml` のポリシー・ファイルをアップロードします。

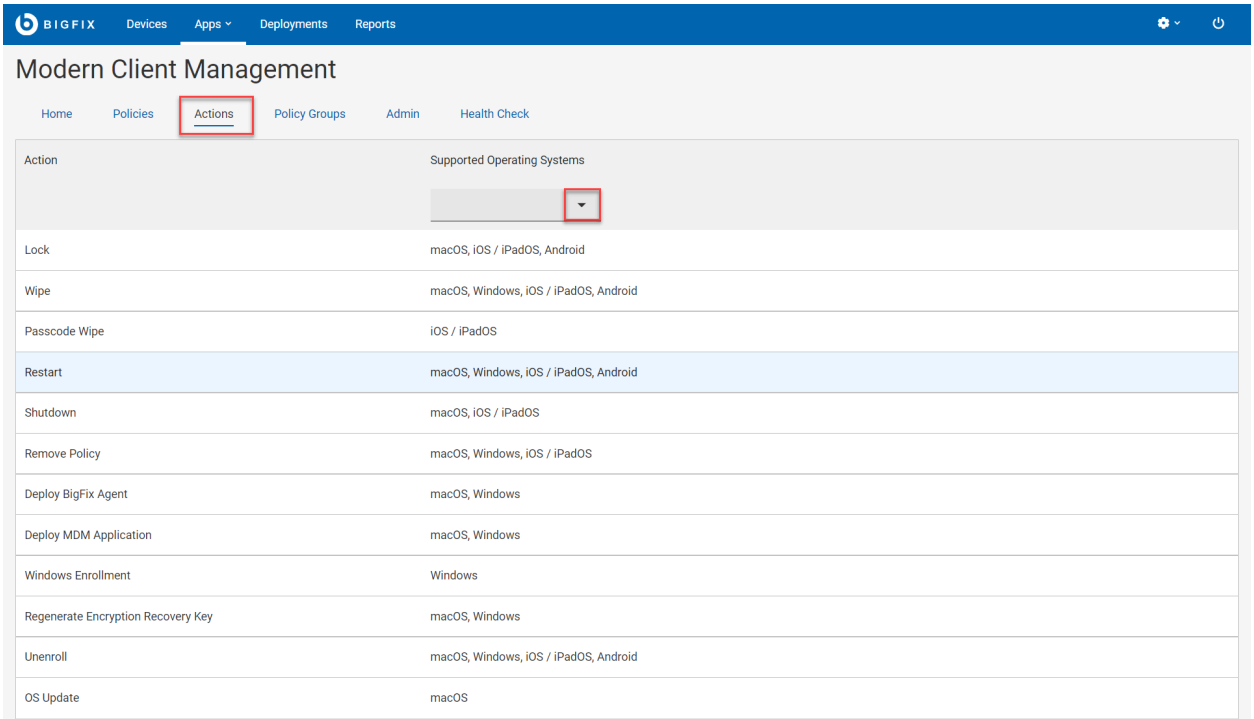
   注: ポリシー・ファイルがサポートされている形式ではない場合、またはバイナリー文字が含まれている場合、WebUI では「ファイルから UUID を解析できません」というエラー・メッセージが表示されます。詳しくは、「ファイルから UUID を解析できない (（ページ）　　)」を参照してください。
9. **「保存」**をクリックします。
10. 保存されたカスタム・ポリシーをポリシー・グループに追加して、MDM サーバーまたは適用可能なデバイスにデプロイします。

MCM アクションのデプロイ

MCM and BigFix Mobile では、MDM 固有の以下のアクションを実行できます。

- ロック
- ワイプ
- パスコード・ワイプ
- 再始動
- シャットダウン
- ポリシーの削除
- BigFix エージェントのデプロイ
- MDM アプリケーションのデプロイ
- Windows の登録
- 暗号化リカバリー・キーの再生成
- 登録解除

- OS の更新
- ユーザー割り当て



注:

- MDM アクションは、MCM および BigFix Mobile が管理しているデバイスへのみデプロイできます。
- また、MDM アクションは、MCM および BigFix Mobile 表記のある相関デバイスにもデプロイできます。
- 一部のアクションはオペレーティング・システム固有であり、各アクションには、適用されるオペレーティング・システムを示すオペレーティング・システムのロゴが表示されます。1 つのアクションに複数のロゴが表示される場合は、示される各オペレーティング・システムでそのアクションを適用できます。

- 「BigFix エージェントのデプロイ」アクションのデプロイを正常に動作させるためには、事前にステージングするインストーラー・パッケージが必要です。macOS の場合は、『macOS BigFix インストーラーの事前ステージ (（ページ） 355)』を参照してください 。Windows の場合は、「Windows BigFix インストーラーの事前ステージ (（ページ） 357)」を参照してください。

他の MDM アクションを実行するには、次の手順を実行します。

1. WebUI にログインします。
2. **「アプリケーション」**をクリックし、**「MCM」**を選択します。
3. 「Modern Client Management」ページで、**「アクション」**をクリックします。
4. 「MDM アクション」ページには、考えられるすべてのアクションと、各アクションでサポートされているオペレーティング・システムが表示されます。「サポートされているオペレーティング・システム」フィルターを使用して、適用可能なアクションをフィルターすることもできます。MDM エンドポイントにデプロイする特定の MDM アクションをクリックします。

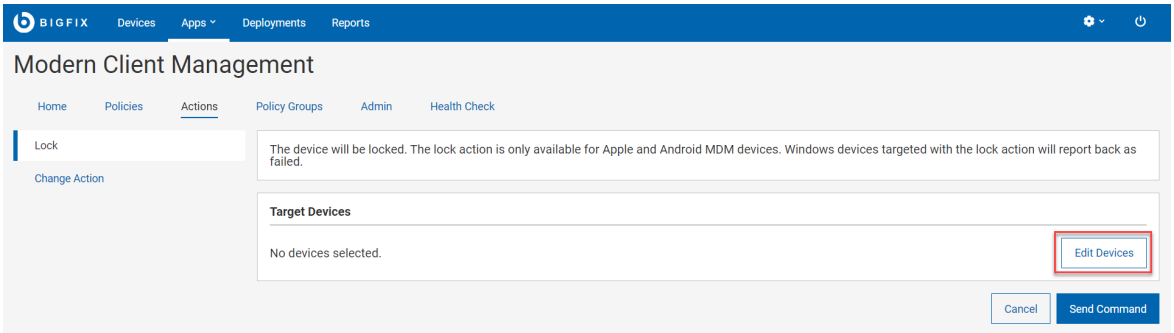
デバイスのロック

このアクションは、紛失または盗難にあったデバイスをリモートでロックするために使用します。ロックすることで、紛失または盗難があった場合にデバイスに保存されているデータを保護します。ロック・アクションを実行後にデバイスが戻ってきた場合、WebUI から起動したアクションに初期設定されたリカバリー・ピンを使用することで、デバイスをアンロックできます。

注:

- ロック・アクションは、macOS、iOS、iPadOS、Android デバイスに適用できます。
- ロック・アクションは Windows デバイスには適用できません。Windows MDM デバイスにロック・アクションをデプロイしても、Windows デバイスはロックされず、このアクションは失敗として報告されます。

1. 使用可能なアクションのリストから、**「ロック」**を選択します。
2. 以下の画面で**「デバイスの編集」**をクリックして、デバイスを追加または削除します。



3. **「コマンドの送信」**をクリックして、アクションを対象デバイスにデプロイします。
結果: 対象デバイスはロックされます。

注: オペレーティング・システムに応じて、ロック操作中にユーザーに表示されるオプションは異なります。Android デバイスの場合、ユーザーは Android コマンドの所要時間 (秒) を入力できます。指定された時間内に実行されなかった場合、コマンドは失効します。

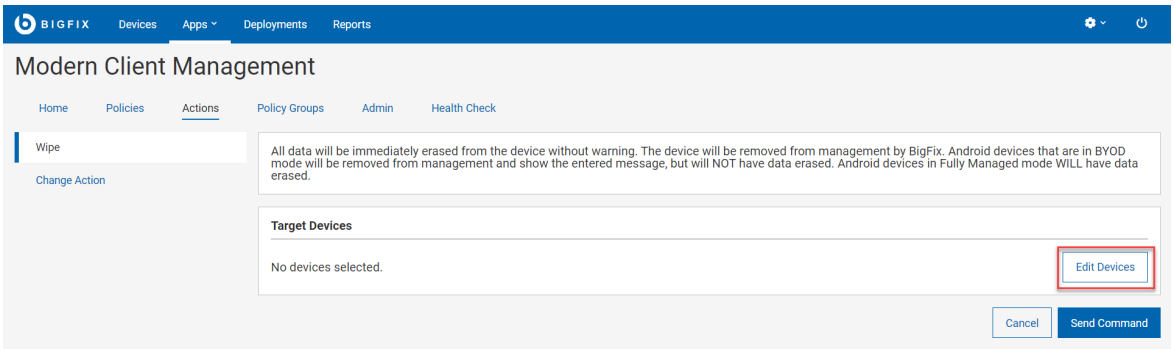
ワイプ

このアクションは、リモート・デバイスのデータ消去に使います。デバイスがロックされている場合でも使用できます。「ワイプ」アクションによって、BigFix 管理から対象デバイスのデータを完全に消去できます。エンド・ユーザーに警告は出ません。

注:

- リカバリー・コードは macOS デバイスにのみ適用されます。Windows デバイスの場合はリカバリー PIN を無視して、「ワイプ」アクションを実行します。
- ユーザーは一度に 1 つのデバイスのみをワイプでき、デバイス・グループでワイプを実行することはできません。
- Android デバイスを対象とする場合、以下のオプションを使用して Android デバイスでのワイプのレベルを指定できます。
  - データのワイプ未指定: この値は無視されます。
  - リセット保護データの保持: デバイス出荷時のリセット保護データを保持します。
  - 外部ストレージのワイプ: 追加でデバイスの外部ストレージをワイプします。

1. 使用可能なアクションのリストから、**「ワイプ」**を選択します。
2. 次の画面で、**「デバイスの編集」**をクリックしてワイプするターゲット・デバイスを選択します。



3.
   - **macOS**: ワイプに macOS デバイスを選択した場合は、6 桁のリカバリー PINを設定します。この PIN は、デバイスにオペレーティング・システムを再インストールする際に必要になります。必ず記録して、デバイスの所有者と共有してください。
   - **Windows**: ワイプ・アクションを実行する Windows デバイスを選択すると、次のオプションが表示されます。

- **完全ワイプ:** デバイスをリモートから完全にワイプし、すべてのユーザー・データ、アプリケーション、および設定を削除します。これにより、デバイスが工場出荷時の状態に完全に復元され、実質的に個人情報や機密情報の痕跡がすべて消去されます。デバイスの紛失、盗難、廃棄準備など、データ・セキュリティーが重要なシナリオでよく使用される徹底的な対策です。この設定は、**「この PC をリセット」を選択し、設定アプリから「すべて削除する」を選択し、「データを消去する」を「いいえ」に設定し、「ファイルを削除する」を「はい」に設定する**手順と同じです。
- **ユーザー・データの保持:** デバイスをリモートでリセットし、ユーザー・アカウントとデータを保持します。機密情報のワイプとユーザー固有の構成の保持のバランスをとることで、ユーザーの中断を最小限に抑えながらデータ・セキュリティーを強化します。この設定は、**「この PC をリセット」を選択し、設定アプリから手動でリセットを開始するときに「個人用ファイルを保持する」**を選択する手順と同じです。

  注: ワイプ・アクションが完了したら、デバイスを再登録する必要があります。

- **プロビジョニングされたデータの保持:** デバイスをリモートで完全にワイプします。
- **保護されたワイプ**: リモート・ワイプを実行し、デバイス上の保護されたデータとパーティションを消去して、安全な領域に保存されている機密情報を完全に消去します。ワイプ・プロセスが正常に完了するまで継続的にリセットを容易に実行でき、特にデバイスの紛失や盗難が発生した場合に、操作のセキュリティーや信頼性が強化されます。

  注: 一部のデバイス構成では、このコマンドによってデバイスが起動できなくなることがあります。この問題を解決するには、IT 管理者にお問い合わせください。

注: デバイス上のワイプ・アクションのデプロイメント状況が「レポートされていません」と表示されている場合、ユーザーはターゲット・デバイスを手動で同期して、そのデバイスでワイプ・アクションを完了する必要があります。

4. **「コマンドの送信」**をクリックして、アクションを対象デバイスにデプロイします。

結果: デプロイメントが完了すると、対象デバイスは MDM からワイプされます。

パスコードのワイプ

このアクションは、対象の iOS および iPadOS デバイスからパスコードを削除するために使用します。

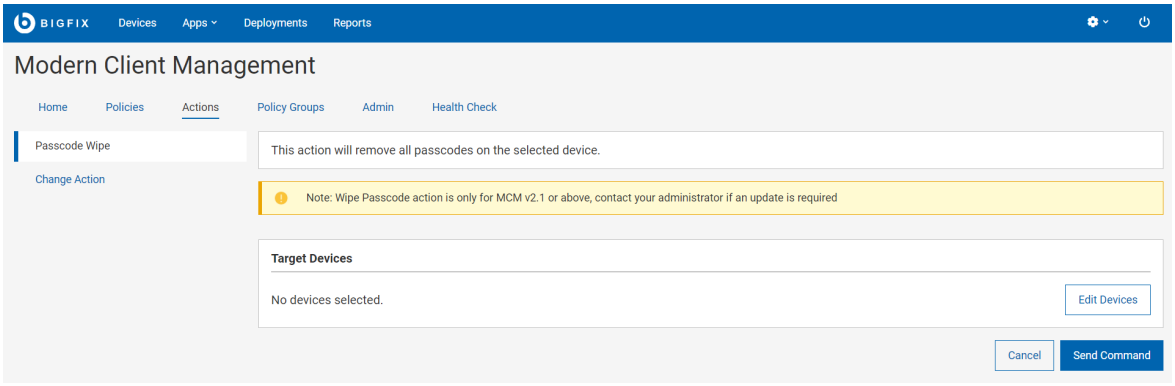
注:

- このアクションを成功させるには、対象の iOS または iPadOS デバイスが監視対象のデバイスである必要があります。
- iOS 15 以降はすべて監視対象となります。

iOS または iPadOS デバイスのユーザーがパスコードを忘れた場合、IT 管理者がリモートでデバイスからパスコードを削除することにより、ユーザーはデバイスへのアクセス権を取り戻すことができます。

選択したデバイスでパスコードをワイプするには、次の手順を実行します。

1. 使用可能なアクションのリストから、**「パスコードのワイプ」**を選択します。
2. 以下の画面で**「デバイスの編集」**をクリックして、デバイスを追加または削除しま



す。

3. **「コマンドの送信」**をクリックして、アクションを対象デバイスにデプロイします。

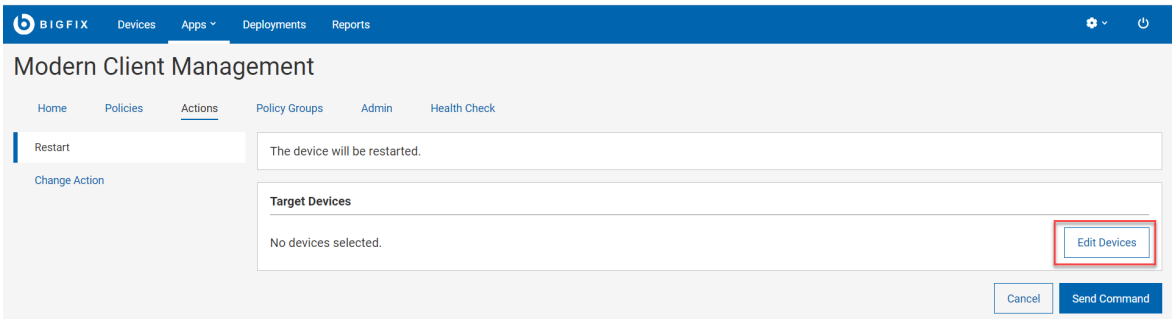
アクションが完了すると、対象の iOS や iPadOS デバイスからパスコード、PIN、パターンが削除されます。

再始動

このアクションは、対象デバイスの再始動に使用します。

注: Mac、iOS、iPadOS: このアクションは、監視対象デバイス (施設所有) として登録されたデバイスに対してのみ機能します。

1. 使用可能なアクションのリストから、**「再始動」**を選択します。
2. 以下の画面で**「デバイスの編集」**をクリックして、デバイスを追加または削除しま



す。

3. **「コマンドの送信」**をクリックして、アクションを対象デバイスにデプロイします。

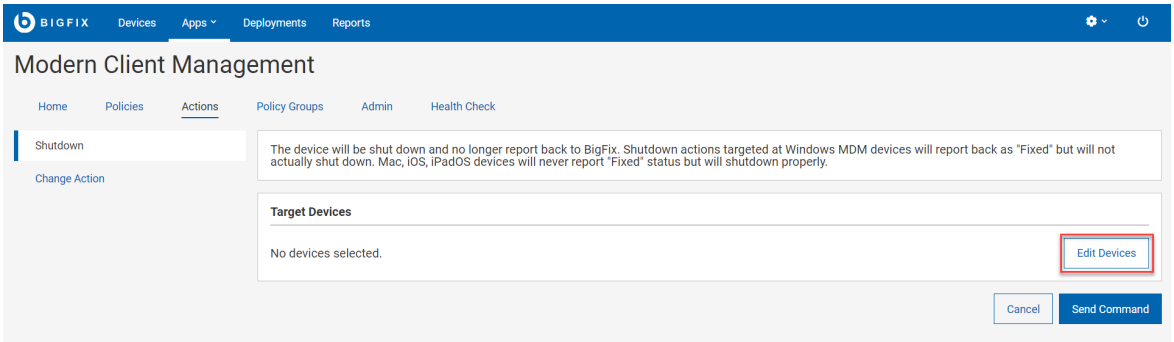
シャットダウン

このアクションは、対象デバイスのシャットダウンに使用します。

注:

- デバイスがシャットダウンされ、BigFix にレポートされなくなります。
- 「シャットダウン」アクションは macOS/iOS/iPadOS でのみ使用でき、Windows では使用できません。
- Windows: Windows MDM デバイスを対象としたシャットダウン・アクションは、「修正済み」としてレポートされますが、実際にはシャットダウンされません。
- Mac、iOS、iPadOS: このアクションは、監視対象デバイス (施設所有) として登録されたデバイスに対してのみ機能します。デバイスは「修正済み」状況をレポートしませんが、正しくシャットダウンされています。

1. 使用可能なアクションのリストから、**「シャットダウン」**を選択します。
2. 以下の画面で**「デバイスの編集」**をクリックして、デバイスを追加または削除します。



3. **「コマンドの送信」**をクリックして、アクションを対象デバイスにデプロイします。

注: 再始動アクションは、Apple DEP デバイスでのみ使用できます。再始動アクションの対象となる監視対象外の Apple デバイスは、再始動のコマンドを無視します。

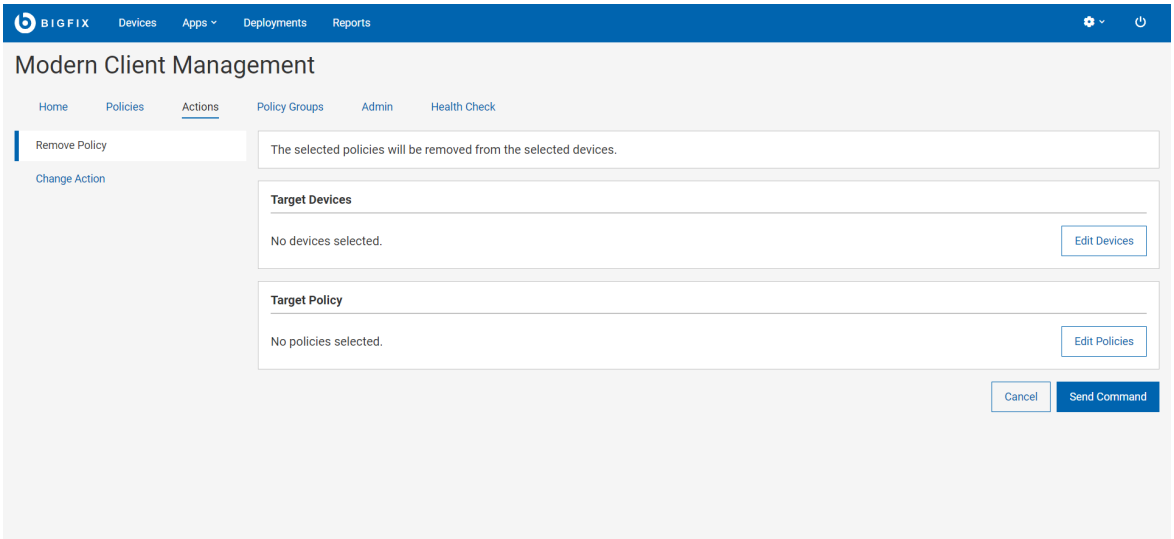
ポリシーの削除

このアクションを使って、選択したデバイスからポリシーを削除できます。MCM および BigFix Mobile に登録されているデバイスのポリシーのみを削除できます。

注:

- 選択したポリシーを持たない macOS デバイスにポリシーの削除アクションを送信すると、アクションは失敗します。
- Android ポリシーは削除できません。ポリシー・グループ (（ページ） 386) から別のポリシーをデプロイすることによってのみ、Android ポリシーを上書きできます。

1. 使用可能なアクションのリストから、**「ポリシーの削除」**を選択します。
2. 以下の画面で**「デバイスの編集」**をクリックして、デバイスを追加または削除します。



3. **「ポリシーの編集」**をクリックし、対象デバイスから削除する必要があるポリシーを選択します。
4. **「コマンドの送信」**をクリックして、アクションを対象デバイスにデプロイします。

BigFix エージェントのデプロイ

「BigFix エージェントのデプロイ (（ページ） 379)」を参照してください。

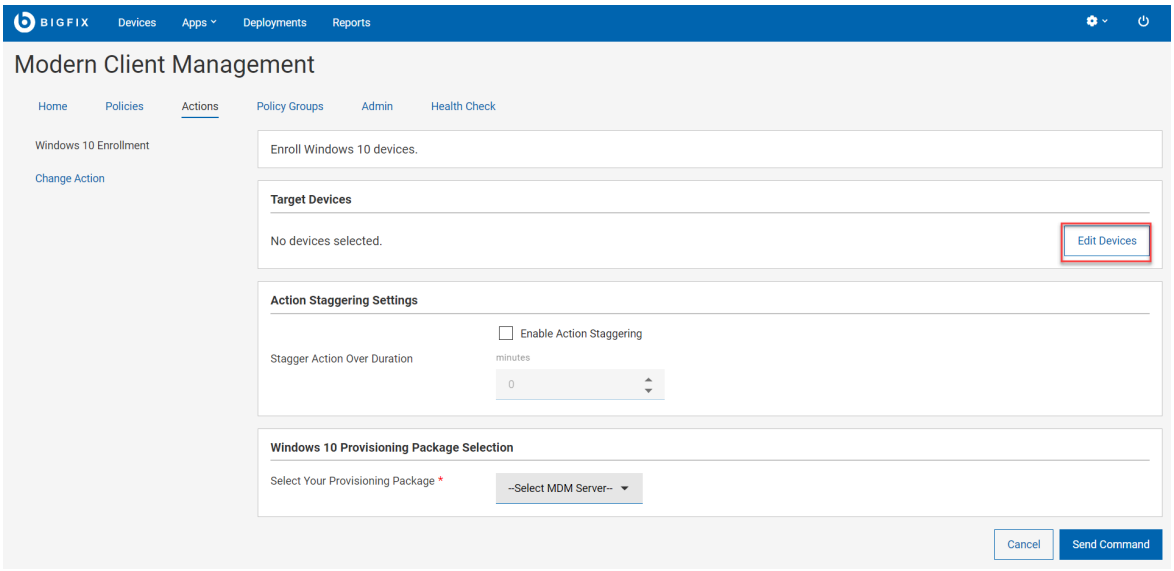
MDM アプリケーションのデプロイ

「BigFix エージェントのデプロイ (（ページ） 379)」を参照してください。

Windows の登録

ppkg ファイルが MDM サーバーに存在する場合は、このページから「Windows の一括登録」（（ページ） 335)を開始することもできます。このためには、以下の手順に従います。

1. 使用可能なアクションのリストから、**「Windows の登録」**を選択します。
2. 以下の画面で、**「デバイスの編集」**をクリックして、BigFix agent がインストールされている環境内のデバイスを選択します。



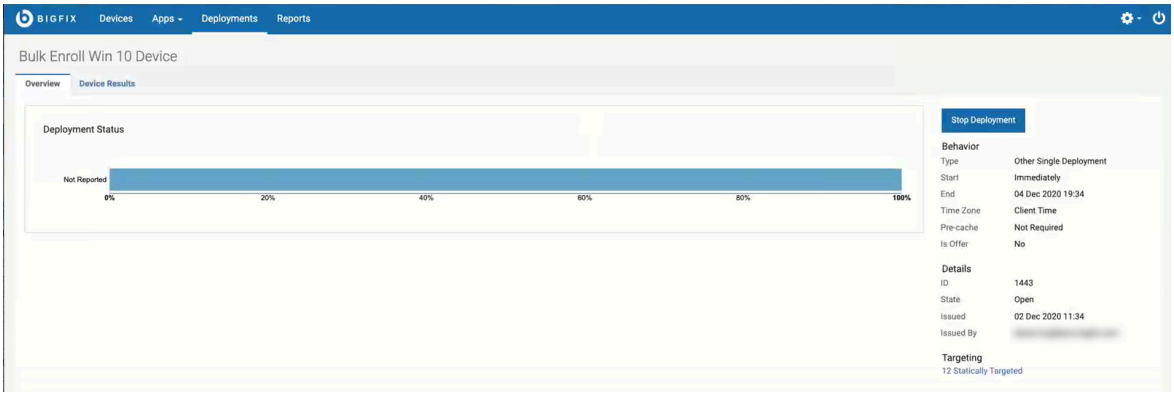
3. アクションの分散設定: **「アクション分散の有効化」**を選択し、**「期間 (分) にわたってアクションを分散」**に入力します。この設定を使用すると、MDM サーバーとネットワークにかかる負荷を分散し、対象となるすべてのエンドポイントが同時に登録を試みるのを防ぐことができます。登録エンドポイントを分散することで、期間がより管理しやすくなり、新しく登録されるデバイスによって発生するトラフィックの量が

正規化されます。この設定を行うと、各エンドポイントは、指定された時間間隔内で時間をランダムに選択して、登録を行います。

4. **「プロビジョニング・パッケージの選択」**で、選択したデバイスを登録する MDM サーバーを選択します。

   注: このドロップダウンには、(（ページ）　　) に従って PPKG がデプロイされている MDM サーバーがリストされます。

5. **「コマンドの送信」**をクリックします。
   - 選択したデバイスで MDM 登録を開始する BigFix 適用環境が生成されます。
   - 対象デバイスとデバイス結果に関する情報を含むデプロイメント文書 (（ページ） *214)*が表示されます。
   - 対象デバイスが登録プロセスを開始します。
   - 任意の時点でデプロイメントを停止するには、**「デプロイメントの停止」**をクリックします。



暗号化リカバリー・キーの再生成

「暗号化リカバリー・キーの再生成 (（ページ） 375)」を参照してください。

登録解除

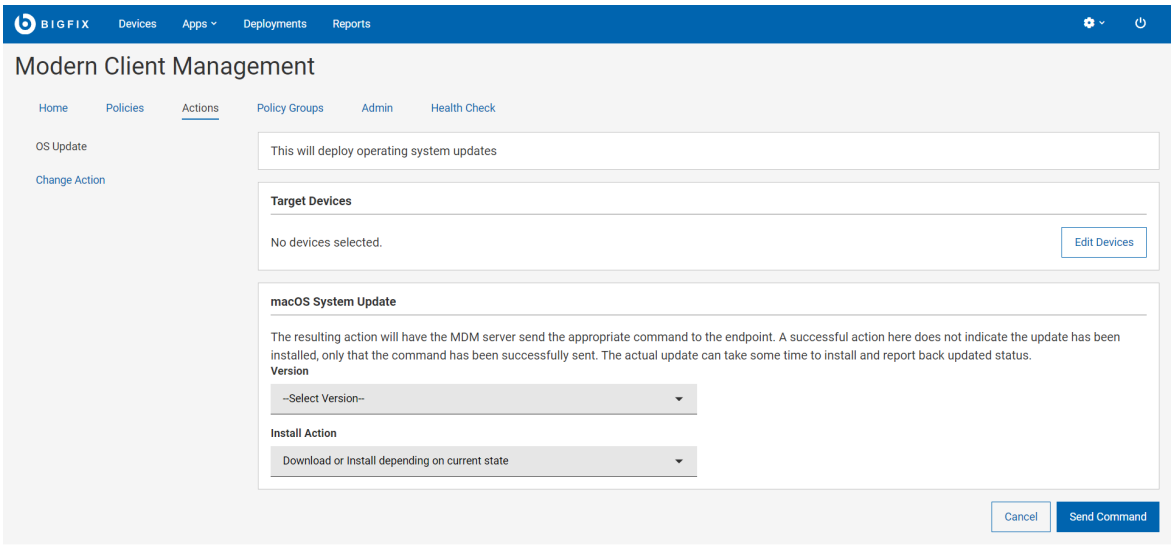
参照 デバイスの登録解除 (（ページ） 475)

OS の更新

このアクションは、macOS デバイスのシステム・ソフトウェアの更新に使用します。OS の更新ポリシー (（ページ） 443) を使用してソフトウェア・アップデート設定を構成することもできます。

macOS デバイスでシステム・ソフトウェアを更新するには、次の手順を実行します。

1. macOS で使用可能なアクションのリストから、**「OS の更新」**を選択します。
2. 「OS の更新」ページの**「対象デバイス」**で、**「デバイスの編集」**をクリックし、適用可能な対象デバイスまたはグループを選択します。



3. 「macOS システムの更新」で、更新する macOS の**「バージョン」** を選択します。このドロップダウンには、環境内の macOS デバイスに適用可能なセキュリティー・パッチ、マイナー・バージョンとメジャー・バージョン、その他すべてのソフトウェアの更新が動的にリストされます。

重要:

- **サポート対象**: macOS の更新では、Big Sur および Monterey のみがサポートされます。
- **サポート対象外**: Catalina OS アップグレード (10.15.X) はサポートされていません。

4. **「インストール・アクション」**を選択します。選択したアクションに応じて、WebUI は検討すべき適切なメッセージを表示します。
5. **「コマンドの送信」**をクリックします。

注:

- このアクションは、指定された更新が使用可能としてリストされているエンドポイントにのみ関連し、実行されます。
- アクションが正常に完了すると、MDM サーバーにのみ更新が送信され、オペレーティング・システムのルールに従って更新をスケジュールするようにオペレーティング・システムに通知することが示されます。これは、OS の実際のシステム更新を示すものではありません。
- 以前は更新が適用可能であったが、OS 更新コマンドの送信が正常に完了した後に適用できなくなった場合は、更新が OS にインストールされたことを示しています。これは、最新表示をした後にのみ分析に反映されます。

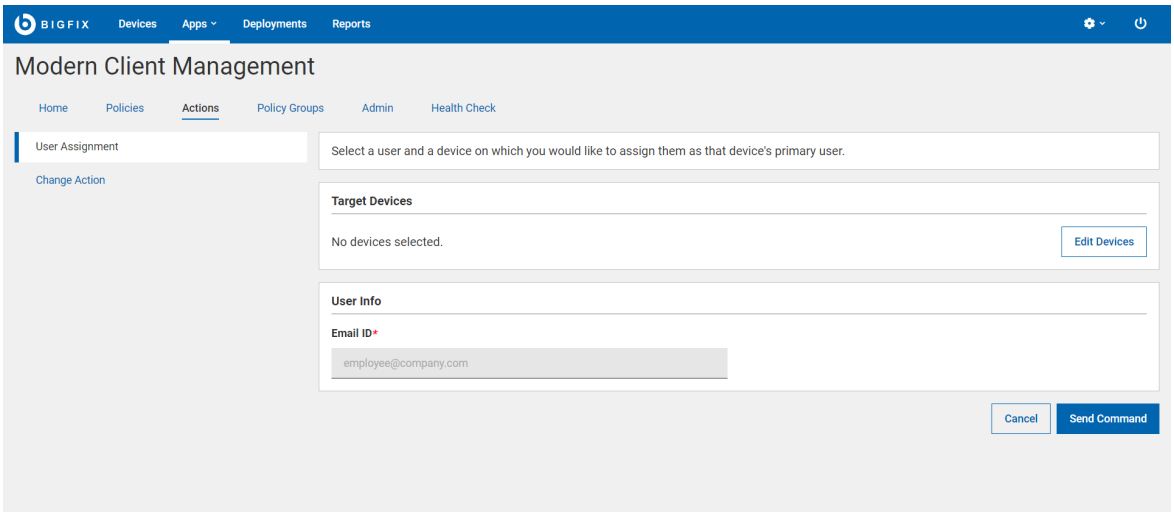
ユーザー割り当て

このアクションは、MCM 登録済みデバイスにユーザーを割り当てるために使用します。登録時にデバイスに割り当てられたプライマリー・ユーザーを設定または変更できます。ユーザーが既にデバイスに割り当てられている場合、このアクションにより指定されたユーザーはオーバーライドされ、プライマリー・デバイス・ユーザーとして割り当てられます。ユーザーが以前に割り当てられていない場合、このアクションによりプライマリー・デバイス・ユーザーが新たに割り当てられます。

注: MCM v3.0 では、このアクションを使用して一度に 1 台のデバイスにプライマリー・ユーザーを割り当てることができます。多数のデバイスにプライマリー・ユーザーを割り当てる場合は、`BigFixServices@hcl.in` の HCL サポートに連絡してください。

ユーザーをデバイスに割り当てるには、次の手順を実行します。

1. 使用可能なアクションのリストから、**「ユーザー割り当て」**を選択します。
2. 「ユーザー割り当て」ページの**「対象デバイス」**で、**「デバイスの編集」**をクリックし、デバイスを選択します。



3. 「ユーザー情報」で、対象デバイスを割り当てるユーザーの**「電子メール ID」**を入力します。
4. **「コマンドの送信」**をクリックします。

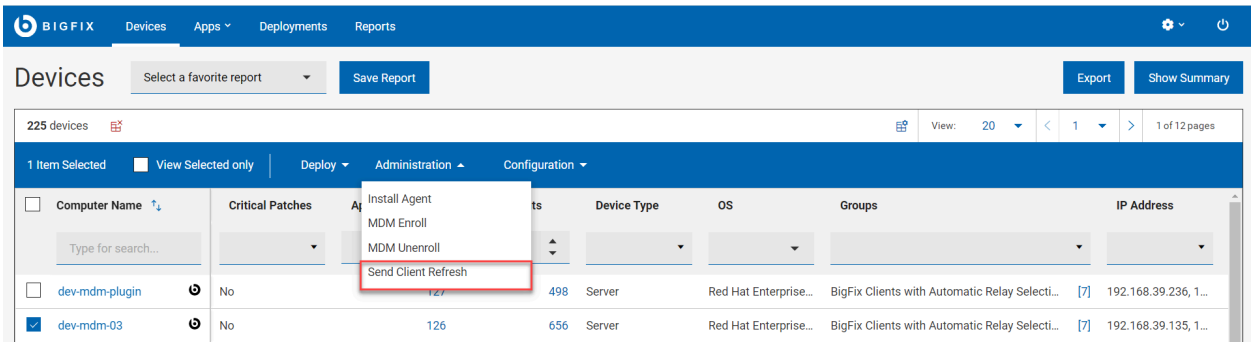
注: アクションが正常に完了すると、WebUI は入力された電子メール ID をプライマリー・ユーザーとして登録します。

クライアント更新の送信

このアクションは、デバイスにクライアントの更新を送信するために使用します。

このアクションは、MDM、BigFix ネイティブ・エージェント、またはクラウド・プラグインによってデバイスが管理されているかどうかに関係なく、BigFix が管理するすべてのデバイスで使用できます。

「デバイス・リスト」（（ページ） *22)*から1 つ以上のデバイスを選択すると、「管理」メニューで「クライアントの更新を送信」アクションが使用可能になります。



「クライアントの更新を送信」アクションをデプロイすることで、デバイスに完全なクライアントの更新リクエストを送信できます。これは、BigFix コンソールで「更新の送信」を実行するのと同じです。

BigFix 9.5 では、「クライアントの更新を送信」により、対象デバイスに対して ActionScript がクライアントに ForceRefresh を通知するアクションが作成されます。

MCM および BigFix Mobile では、WebUI がダイレクト API の呼び出しを送信して、クライアントに完全な更新を実行するよう強制します。

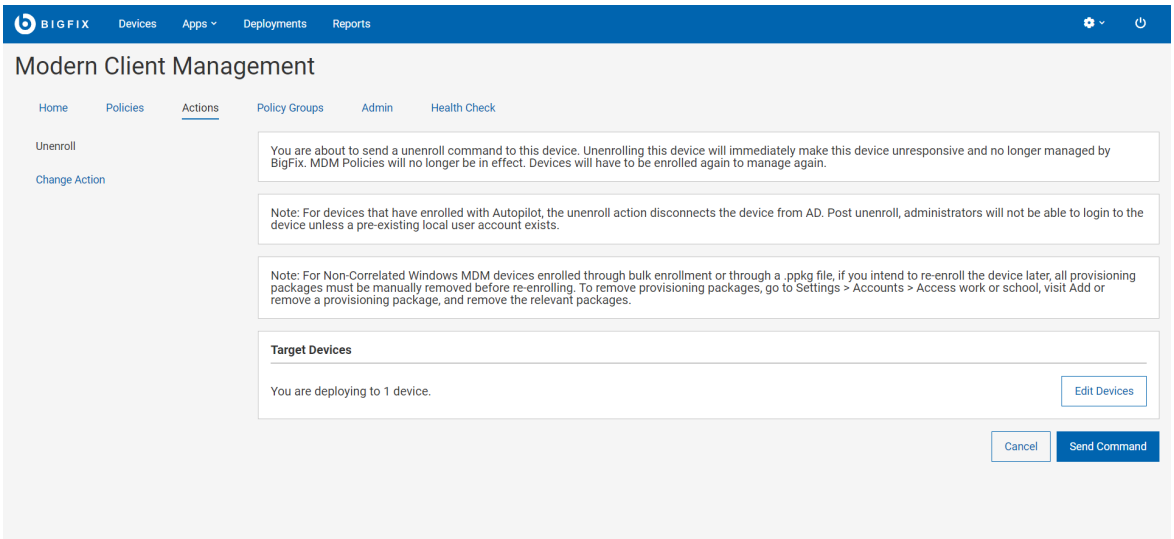
デバイスの登録解除

MDM から登録を解除すると、BigFix MCM でデバイスを管理できなくなります。MDM ポリシーは、登録解除されたデバイスでは無効になります。

WebUI を使用した登録解除

WebUI を使用してデバイスの登録を解除するには、次の手順を実行します。

1. WebUI メイン・ページで、**「デバイス」**をクリックします。
2. リストされたデバイスから、登録解除するデバイスを選択します。
3. 青で表示されるアクション・バーから、**「管理」 > 「MDM 登録解除」**を選択します。次のページが表示されます。



4. ターゲットを変更する場合は、**「デバイスの編集」**をクリックします。情報を確認して、**「コマンドの送信」**をクリックします。デバイスが登録解除されます。

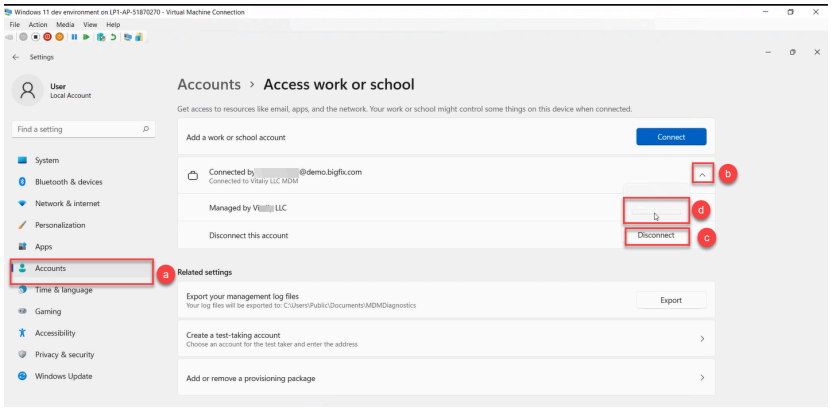
注:

- BigFix Platform バージョン 10.0.8 より前のバージョンをインストールした場合、MDM デバイスを登録解除して後で再登録すると、WebUI とコンソールに一意のコンピューター ID を持つ複数のデバイスが表示されます。これを回避するには、BigFix Platform バージョンを 10.0.8 以降にアップグレードすると、登録解除されたデバイスがルート・サーバー、コンソール、および WebUI から削除されます。
- ODJ ポリシーで登録されているエンドポイントが、登録解除されても Active Directory から切断されません。この問題を修正するには、「登録解除後に AD から切断されたエンドポイント (（ページ）　　)」を参照してください。

デバイス・ユーザーによる登録解除

Windows

- デフォルトでは、MCM は登録されているすべての Windows デバイスでユーザーによる登録解除を許可します。
    - デバイス・ユーザーとして、Windows デバイスの登録を解除するには、以下のステップを実行します。
        - a. 左側のナビゲーション・ペインから **「アカウント」**を選択します。
        - b. **「接続者」**の横にあるキャレット記号をクリックします。
        - c. **「切断」**、**「職場または学校にアクセスする」**をクリックし、**「切断」**をクリックします。デバイスは MDM サービスから登録解除されます。
        - d. さらに、Windows 11 デバイスで登録を解除するには、**「切断」**をクリックした後に表示されるポップアップボタン(空白行として表示されます)をクリックします。



- 組織が、ユーザーによる会社所有のデバイスの登録解除を禁止する場合は、カスタム・ポリシーを使用して実行できます。カスタム・ポリシーをポリシー・グループに追加し、MDM・サーバーにデプロイします。コードについては、デバイス・ユーザーによる完全管理対象 (会社所有) デバイスの登録解除を制限するカスタム・ポリシー ((ページ) 349)を参照してください。

Apple

DEP: ユーザーが自分自身を登録解除する機能は、デバイスに適用された DEP プロファイルで構成されます。「自動デバイス登録ポリシーの構成」ページで構成中に、`Is MDM Removable` オプションが選択されている場合、Apple デバイス・ユーザーは登録を解除できます。それ以外の場合、このオプションは無効になり、ユーザーは登録を解除できません。ユーザーが登録解除を開始すると、「アプリケーション」と「制限」セクションの下の項目は空になります。
iPhone または iPad デバイスを登録解除するには:

1. デバイスの**「設定」**を開きます。
2. **「一般」 > 「デバイス管理」**に移動します。
3. MDM プロファイルを選択します。
4. **「管理の除去」**を選択します。

macOS デバイスを登録解除するには:

1. **「システム環境設定」**を開きます。
2. **「プロファイル」** セクションに移動します。
3. メインの MDM プロファイルを選択します。
4. 「-」ボタンをクリックし、プロンプトに従って登録解除を確認します。

BYOD: Apple User Enrollment を介して加入した Apple BYOD デバイスは、WebUI を介してリモートで登録解除できません。Apple BYOD デバイスを登録解除するには、デバイスの「設定」の下にある管理対象アカウントからサインアウトして、手作業で登録解除する必要があります。

Android

ユーザーは、会社所有のデバイス (新規または出荷時にリセットされたデバイス) の登録を解除できません。

ユーザーは、仕事用プロファイルを削除することにより、BYOD Android デバイスの登録を解除できます。仕事用プロファイルを削除するには、以下のようにします。

1. **「設定」** > **「アカウント」** > **「Remove work profile」**に移動します。
2. **「削除」**をタップして、仕事用プロファイル内のすべてのアプリケーションとデータの削除を確認します。
3. ポリシー・アプリケーション (「デバイス・ポリシー」) がアンインストールされ、デバイス上に存在しないことを確認します。

仕事用プロファイルが削除されると、そのプロファイル内のデバイス上のすべてのローカル・データが削除されます。

デバイスを工場出荷時設定にリセットして、すべてのアプリケーションとデータ (個人と仕事用の両方) を削除することもできます。

第 15 章. BigFix 管理機能の拡張

BigFix 11 は、デバイスが物理デバイスか仮想デバイスかに関係なく、ネットワーク上のデバイスの可視性と管理を強化するいくつかの重要な新機能を備えています。

最新の IT インフラストラクチャーの管理で直面する課題

インフラストラクチャーの管理は、IT 組織にとってますます困難で複雑になっています。複数の種類のサーバー、さまざまなオペレーティング・システム、ソフトウェア、クラウド・コンピューティングとサービス、刻々と変化するテクノロジーの出現により、IT 環境の追跡、制御、管理が難しくなります。

- クラウド・コンピューティングやモビリティなどのテクノロジーは、IT ランドスケープを急速に変化させ、最新の状態を維持することが困難になります。
- 従来のコンプライアンスを遵守しながら、新しいコンプライアンスと規制の要件に対応するために、コスト効率の高いソリューションの必要性が高まっています。
- IT 組織が最新のテクノロジーを中心に運用を拡大し続けると、セキュリティーが大きな関心事になります。
- 高度なコンピューティングとデータ分析をサポートする高度な IT インフラストラクチャーには、効率的で費用対効果の高いデータ抽出とデータ・ストレージ技術が必要です。

BigFix 11 の機能

異機種 IT 環境全体の透明性を実現するには、BigFix 11 のようなより自動化された包括的で堅牢なソリューションが必要です。このまったく新しいバージョンの BigFix は、ネットワーク内のリソースの正確なビュー、主要な分析、詳細な分析情報を提供するため、意思決定者は、IT 管理に関する情報に基づいたより迅速な意思決定を行うことができます。

関連情報

クラウド・リソースの管理 (（ページ）　　)

クラウド・プラグインの管理

BigFix プラットフォームでは、Amazon Web Services (AWS)、Microsoft Azure、VMware、Google Cloud Platform (GCP) などの各クラウド・プロバイダーのプラグインがサポートされています。各クラウド・プロバイダーには独自の機能や外部プログラムとの接続方法があり、データへのアクセスや機能をさまざまな方法で処理しています。

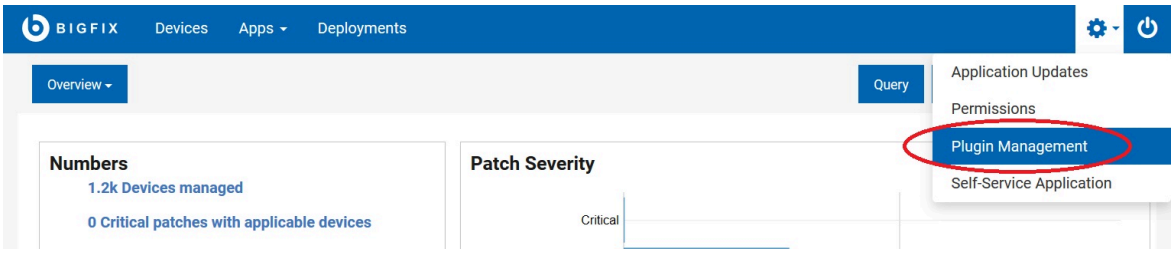
プラグイン・ポータルおよびクラウド・プラグインをインストールできるようにするには、マスター・オペレーター (MO) 権限が必要です。

プラグイン・ポータルのインストール

プラグイン・ポータルは、BigFix 10 に導入された新しいコンポーネントであり、クラウド・デバイスや、BigFix に登録されている Windows 10 や MacOS のエンドポイントなどの最新デバイスを管理するのに役立ちます。最新のクライアント管理の詳細については、「最新のクライアント管理と BigFix Mobile」を参照してください。

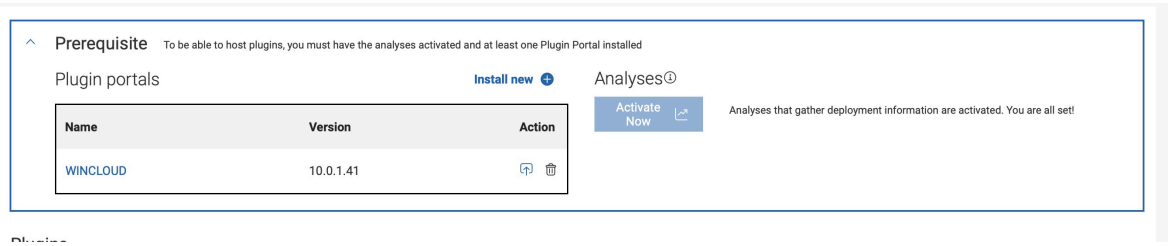
プラグイン・ポータルは、クラウド・インスタンスとモダン・クライアントの管理をサポートするために BigFix 11 に導入されたスケーラブルなコンポーネントです。

1. 右上隅にある歯車アイコンをクリックします。
2. **「プラグイン管理」**をクリックします。



「プラグイン管理」ページが開きます。

3. 「前提条件」セクションでは、プラグインのインストールを続行するために適切なコンポーネントが使用可能な状態にあり、開始されていることを確認できます。



a. インストールしていない場合は、プラグイン・ポータルをインストールします。
   - プラグイン・ポータルセクションで「インストール」をクリックします。「BigFix プラグイン・ポータルのインストール」が開きます。
   - **「コンテンツのデプロイ」**をクリックします。

b. 分析がアクティブ化されているかどうかを確認します。アクティブ化されていない場合は、ボタンを押して、検出されたデータが BigFix データベースに正しく報告されるようにします。

クラウド・プラグインのインストール

クラウド・プラグインをインストール、管理します。

クラウド・プラグインをインストールするには、以下の手順を実行します。

1. 「プラグイン」セクションで**「新規インストール」**をクリックします。ドロップダウン・メニューでプロバイダーを選択します。
2. クラウド・プラグインのインストール・ページが開きます。2 つ以上のセクションがあり、各セクションに構成パラメーターが含まれています。
3. **「一般」**セクションが表示されます。
4. ホスト・ポータルを指定します。
5. ディスカバリーの頻度の値を分単位で指定します。
6. **「プロバイダー固有の設定」**セクションが表示されます。このセクションは AWS 専用であり、ここでデフォルトのリージョンを指定する必要があります。
7. **「認証」**セクションが表示されます。
8. プラグインをインストールするときは、資格証明セットを 1 つ指定する必要があります。後から必要な数だけ資格証明セットを追加できます。「クラウド・プラグインで

の作業 (（ページ） *488)*」セクションを参照してください。管理しやすくするために、各資格情報にはラベルがあります。資格情報の検索や管理の簡素化のために使用できる名前を入力します。このフィールドの名前は **「アカウント・ラベル」**です。使用するクラウド・プロバイダー (AWS、Azure、VMware または GCP) によって、以下の必須パラメーターのリストは異なります。

- 「クラウド・プロバイダー」に Microsoft Azure を指定した場合は、以下の情報を入力する必要があります: テナント ID、サブスクリプション ID、クライアント ID (アプリケーション ID)、パスワード (クライアント・シークレット)。
- 「クラウド・プロバイダー」に vSphere を指定した場合は、以下の情報を入力する必要があります: vCenter サーバー、ユーザー名、パスワード。
- GCP を指定した場合は、GCP クラウド管理者から受け取った .json ファイルをアップロードして、サービス・アカウント・キーを入力する必要があります。
- AWS を指定した場合、認証パラメーターは以下のとおりです: AWS ユーザー・リージョン、アクセス・キー ID、シークレット・アクセス・キー。資格情報の保守を簡素化するために、BigFix ではオプションで、ディスカバリーなどの API を介してクラウドでアクションを実行するために、この資格情報が使用できる役割を追加できます。役割を使用することで、AWS プラグインで使用および構成される資格情報のリストを簡素化および短縮できます。これは、AWS でこの設定が実施されている場合にのみ可能です。また、各役割に外部 ID も指定できます。役割と外部 ID の使用法に関する詳細については、AWS の資料を参照してください。役割と外部 ID を追加するには、**「新規追加」**ボタンを押します。テーブルが表示されるので、その行に値を入力できます。役割は完全修飾名 (例: arn:aws:iam::123456789012:root) で指定する必要があります。必要な数だけ追加できます。

9. **「詳細設定」**セクションが表示されます。
10. Microsoft Azure と AWS には、以下を指定できる詳細設定セクションがあります。
    - Microsoft Azure の場合は、「ログのパス」と「ログの詳細」。
    - AWS の場合は、ロギング情報に加えて「プロキシー URL」、「プロキシー・ユーザー名」、「プロキシー・パスワード」などのプロキシー設定も指定できます。
11. **「インストール」**をクリックします。
12. **「インストール」**をクリックします。

IAM ロールのサポート

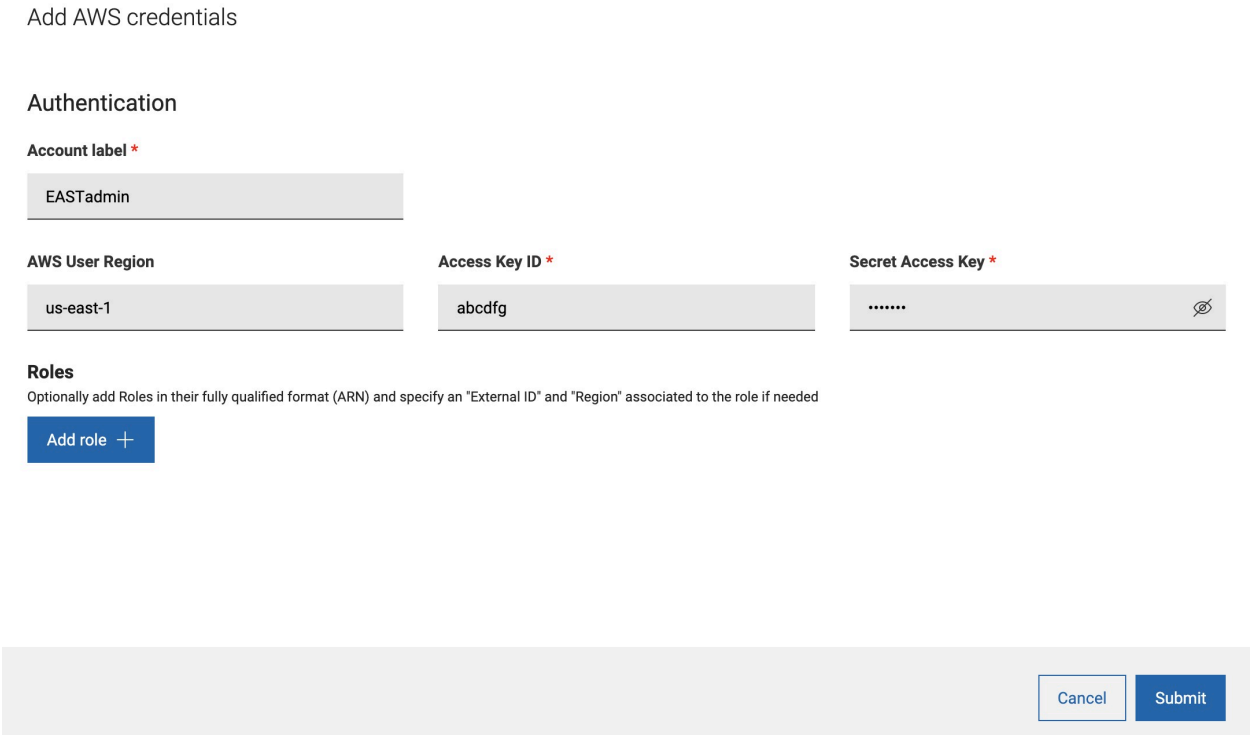
BigFix バージョン 10.0.4 では、AWS 資格情報の管理を簡素化するために、IAM ロールのサポートが導入されました。

BigFix は、表示または管理の使用権を持つプロバイダー固有の資格情報に基づいて、クラウド・インスタンスを検出できます。これは、プラグイン設定で非常に多くの資格情報を指定する必要がある可能性を意味し、関連する資格情報を最新に保つという負担が伴います。ロールを使用することで、この数は大幅に減少する可能性があります。BigFix がロールを偽装してディスカバリーを開始することで、ロールに基づくディスカバリーが行われるため、複数の資格情報を管理する必要がなくなるからです。

もちろんこの場合、一部のユーザーに複数のロールを与えて、クラウド環境全体を検出できるように AWS クラウドを構成する必要があります。ロールは、ARN (Amazon リソース名) と呼ばれる完全修飾名で BigFix に提供される必要があります。これらの情報は通常、クラウド管理者と BigFix MO の間で交換されます。

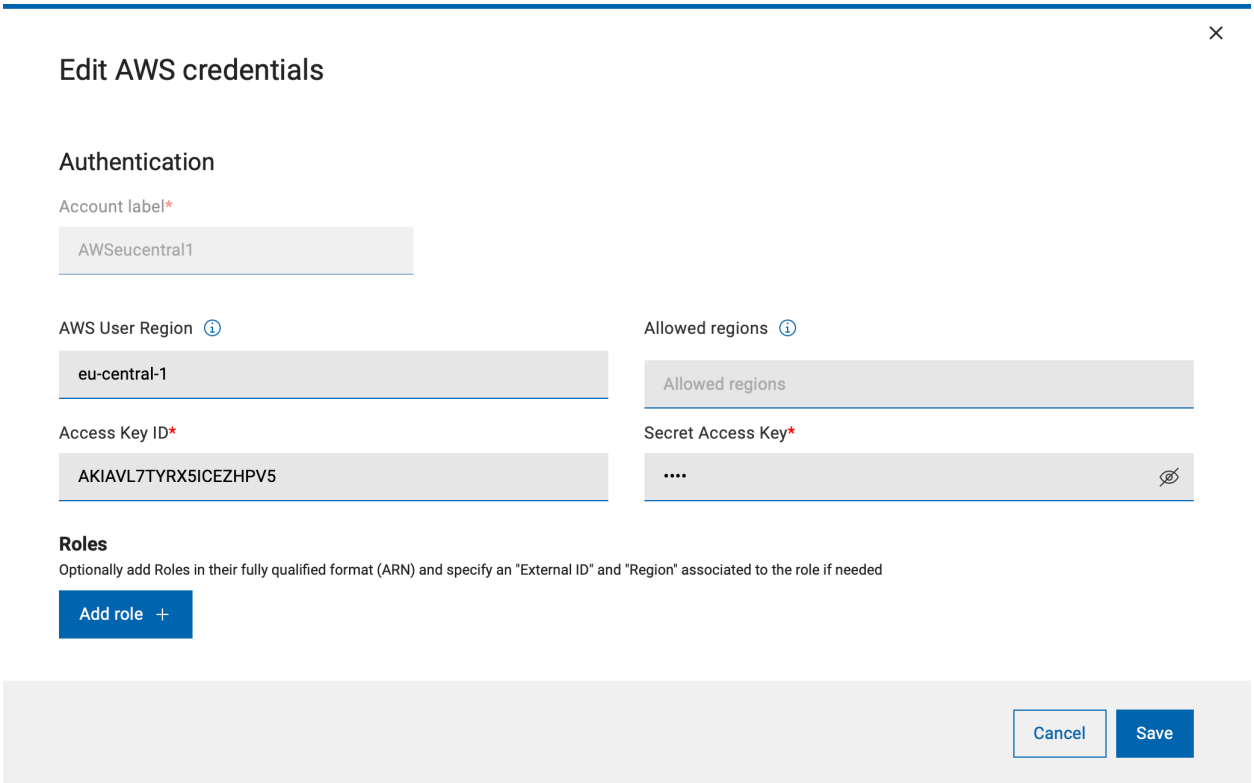
注: AWS ロールが挿入されると、AWS プラグインは、取得元の資格情報ではなく、検出時に AWS ロールを使用します。クラウド環境で検出するすべての AWS デバイスがこれらの役割に含まれるようにする必要があります。そうしないと、一部のマシンは検出されない場合があります。

AWS で、プラグインのインストール時または資格情報の追加/編集時に、ユーザーがロールを指定する方法を以下に示します。



「ロールの追加」を押すと、ロールの完全修飾 ARN、クラウド管理者から提供された場合は外部 ID、AWS API でディスカバリーを開始するために必要なデフォルトの地域が含まれるテーブルが表示されます。これらのフィールドはすべてオプションですが、外部 ID または地域が指定されている場合は ARN が必要です。

BigFix Platform バージョン 10.0.5 では、ユーザーは資格情報レベルでスキャンを制限することもできます。



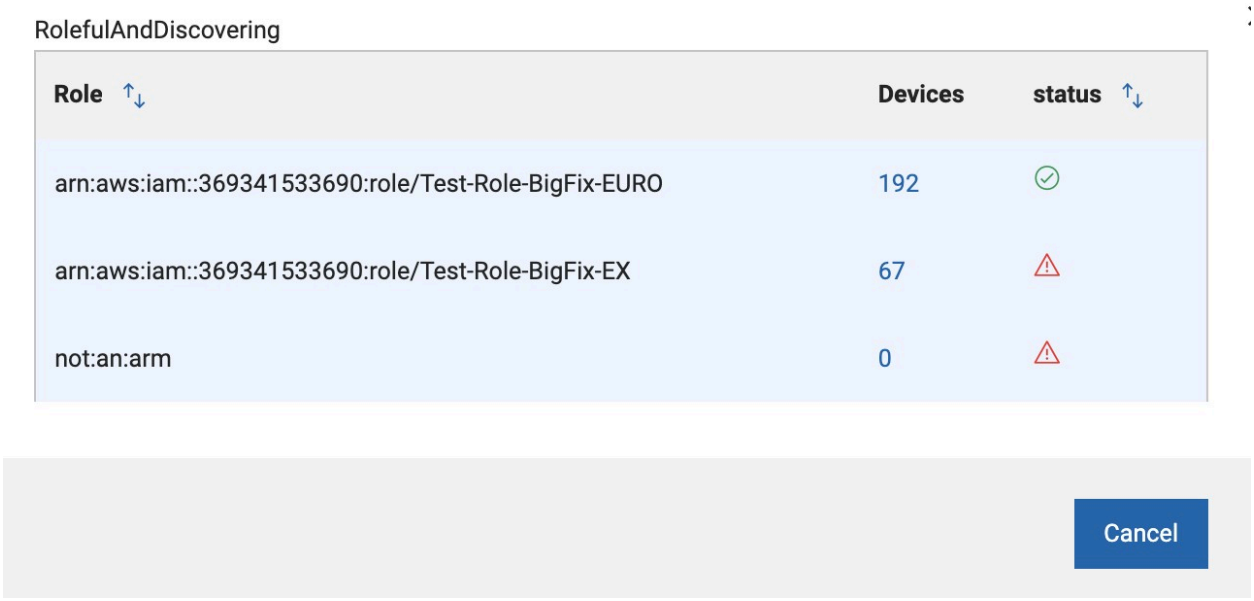
プラグインがインストールされると、メインの**「プラグイン管理」**ページでプラグインの動作を制御できるようになります。

各プロバイダーには専用の水平タブがあり、タブに移動すると、左側のサイドバーにプラグインごとに 1 つのエントリーが表示されます。ご使用の環境に複数のポータルがある場合は、複数のプラグインになります。実際には、各ポータルにインストールできる特定のプロバイダーのプラグインは 1 つのみです。

プラグイン名の横にあるアイコンは、プラグインが正常に機能しているかどうかを簡単に確認できるインジケーターです。黄色または赤のアイコンがある場合は、**「認証」**テーブルに移動して、問題の原因となっている資格情報セットを見つけます。

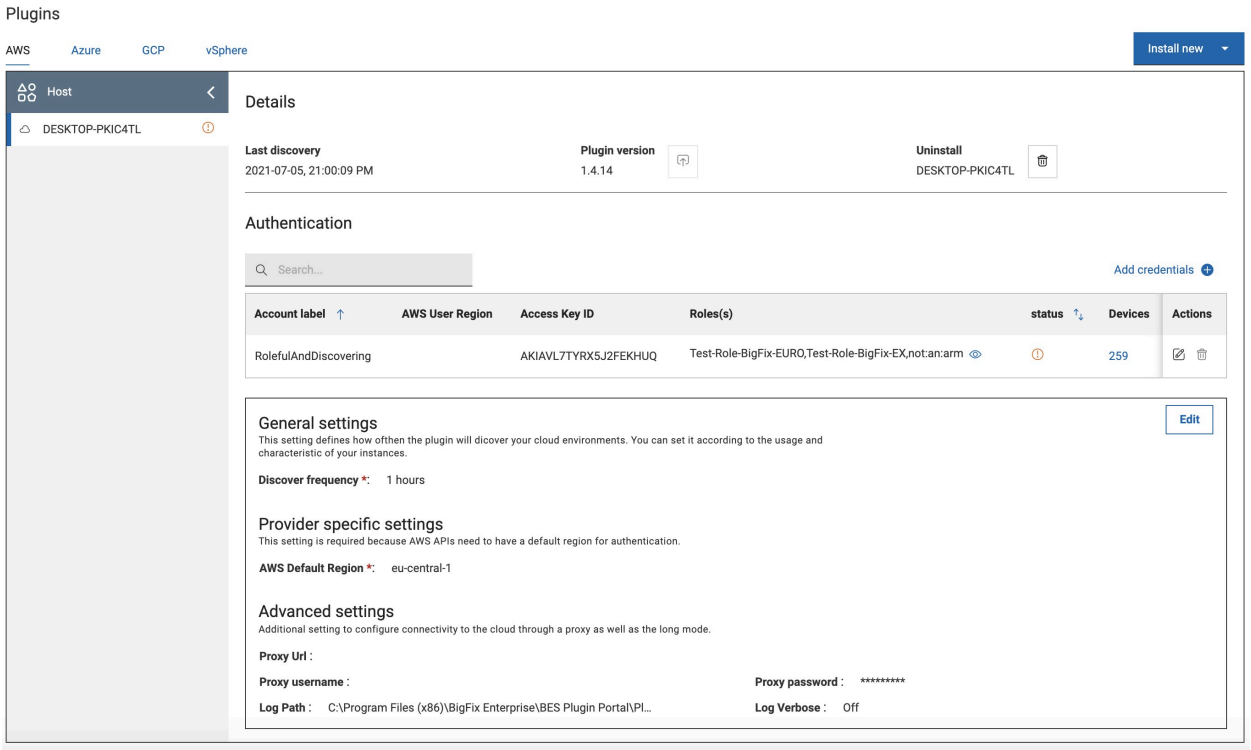
このテーブルには、資格情報、ロール (指定されている場合)、状況、資格情報を使用して検出されたデバイスの数、編集および削除の可能性が含まれます。

「目」のアイコンは、ロールの詳細を示すモーダル・ウィンドウを開きます。



このページには、以下の情報が含まれています。

- 最後にディスカバリーを実行した日時。
- プラグインのバージョンと、新しいバージョンが使用可能な場合にアップグレードする可能性。
- プラグインをアンインストールする可能性。



初回のインストール後に、さらに資格情報を追加することや、既存の資格情報を編集または削除することができます。**「一般設定」**セクションでは、ディスカバリーの頻度、ロギング、プロキシーなどの、プロバイダー固有の情報を設定できます。

クラウド・プラグインでの作業

クラウド・プラグインを有効にしていて、お使いの環境でクラウド・インスタンスが見つかった場合は、「デバイス」ページからそれらのクラウド・デバイスにアクセスして使用できます。

「デバイス」ページには、お使いの環境内のすべてのデバイスが列挙され、それらが物理デバイスか、仮想デバイスか、カテゴリー内にいくつあるか、BigFix エージェントがインストールされているかどうかが示されます。

データ・グリッド・ビューは簡単にカスタマイズでき、列の追加/削除/再編成が可能です。

デバイス相関の目的は、リソースの重複を防いでデバイス管理を効率化することです。BigFix がクラウド上 (プライベートまたはパブリック) でデバイスを発見すると、それらがシステムで既知のものかトラッキングされているものかどうかを確認します。アセット相関の利点は、1 つのエンドポイントの複数の表現がある場合に、それらすべてを集約

して 1 つのエンドポイントとして**「デバイス」**ページに表示できる点です。オペレーターは任意のグループ (表現など) を選択してアクションをターゲット設定したあと、グループ内の表現を各特定のアクションの対象として選択できます。オペレーターのアクセスをデバイスの特定の表現管理のみに制限することもできます。

クラウド・プラグインをインストールしてクラウド・リソースを見つけたら、「クラウド・ダッシュボード」の「WebUI の概要」にクラウド・デバイスの要約が表示されます。クラウド・ダッシュボードを表示するには、ナビゲーション・バーの下の**「概要」**ボタンをクリックし、**「クラウド・ダッシュボード」**を選択します。ダッシュボードには、環境内のクラウド・リソース量を監視するタイルがあり、エージェントのインストールの有無にかかわらず、タイプと地域ごとの分布が表示されます。任意の棒グラフをクリックすると「デバイス」ページが開き、BigFix エージェント状況でフィルタリングされ、「管理対象」が事前選択されたリソースのリストが表示されます。

BigFix オペレーターは、デバイス文書を表示できます。デバイス文書には、さまざまなソースから収集された情報が記載されています。

クラウド・インスタンスの場合は、このページにもクラウドに関連するデータが表示されます。検索をクラウド・デバイスに絞り込むには、「BigFix エージェント状況」(インストールまたは未インストール) または「管理元」(クラウドとクラウド・プロバイダー) などのフィルターを使用できます。

プラグイン設定

以下の設定は、「プラグイン・ポータル」の共通ヘッダーからエクスポートされた `SetPluginSettingsIntoStore` 関数を使用して設定できます。これらの設定は、コンソールのダッシュボードと WebUI のダッシュボードの入力に使用されるすべてのプラグインの保存設定を取得します。

表 17. SetPluginSettingsIntoStore 設定

プラグイン名	説明
`Credentials_LoginSuccess`<useralias>	ロックアウト・ポリシーが設定されている場合に資格情報のロックを回避します。

表 17. SetPluginSettingsIntoStore 設定 (続く)

プラグイン名	説明
	値: ログインが成功すると「1」に設定されます。クラウド・プロバイダーが資格情報を拒否すると「0」に設定されます。 例えば、HTTP エラー 401 ではこの設定が「0」になり、パスワードが有効ではなくなったことを示します。HTTP 401 以外の理由でログインに失敗した場合 (ネットワーク・エラーや他の HTTP エラー・コードなど) は、何も設定されません。
`Discovery_LastScan`	最後のディスカバリーの試行のタイムスタンプ (unix 時間) が含まれます。
`Discovery_LastScanNoErrors`	最後にディスカバリーがエラーなく完了したときのタイムスタンプ (unix 時間) が含まれます。これは、マルチクレデンシャルをサポートするためのものです。例えば、10 個の資格情報セットがある場合、ディスカバリーはそれぞれに対して試行されます。1 つの資格情報セットが有効期限切れで失敗した場合、既に 1 回のディスカバリーが行われているため `LastScan` が設定されますが、`LastScanNoErrors` は設定されません。エラーが 1 つも発生しなかった場合、`LastScanNoErrors` と `LastScan` は同じ値に設定されます。
`Discovery_LastError`	すべてのディスカバリーの実行中に見つかった最後のエラー・メッセージが含まれます。これは、すべてのディス

表 17. SetPluginSettingsIntoStore 設定 (続く)

プラグイン名	説明
	カバリーがエラーなく終了した場合にリセットされます。つまり、これは `LastScanNoErrors` != `LastScan` の場合に設定され、`LastScanNoErrors` == `LastScan.` の場合は “” に設定されます。

AWS リージョンの制限によるデバイス検出範囲の設定

AWS では、データ・センターと仮想インスタンスがリージョンによって整理されています。クラウド・インスタンスのこのプロパティーは、`Amazon Web Services Resources` の分析によって AWS リージョンで報告されます。

AWS リージョン

AWS リージョンとは、ある地域に存在する AWS リソースの集合です。1 つのリージョンで作成したリソースは、AWS サービスが提供する複製機能を使用しない限り、他のリージョンには存在しません。リージョンを有効化すると、AWS はそのリージョンでアカウントを準備するためのアクションを実行します。詳しくは、 で AWS 公式資料を参照してください。 https://docs.aws.amazon.com/general/latest/gr/rande-manage.html

スキャンするリージョンの制限

検出を高速化するには、スキャン範囲を使用する AWS リージョンのみに制限することを推奨します。これを指定しない場合、各種リージョンに対してプラグインによって追加で定義された資格情報の権限にかかわらず、クラウド環境にログインした後、ログイン・フェーズで取得されたすべての AWS 管理対象リージョンに対して検出が実行されます。

例えば、プラグインのインストール時に指定された IAM ユーザー資格情報に `us-west1` リージョンへのアクセス権限のみが付与されている場合、プラグインのログイン時にすべての AWS アカウント管理リージョンの取得が試行され、検出が開始されます。この時点で、AWS プラグインは IAM ユーザー資格情報を使用してすべての AWS 管理リージョンにログインしようとします。このログインは、この資格情報に `us-west1` 以外のリージョンにアクセスする権限が与えられていないため失敗します。

BigFix プラットフォーム 10.0.5 では、Allowed regions のパラメーターを使用して検出対象とするリージョンを制限できるようになりました。これを指定すると検出範囲が制限され、ネットワーク・トラフィックの最適化によりエラーが最小限に抑えられます。

AWS 設定を変更するか、新しい AWS の資格情報を追加することにより、許可するリージョンの設定をカスタマイズできます。

以下の表は、パラメーターの使用方法と、指定しない場合の動作を示しています。

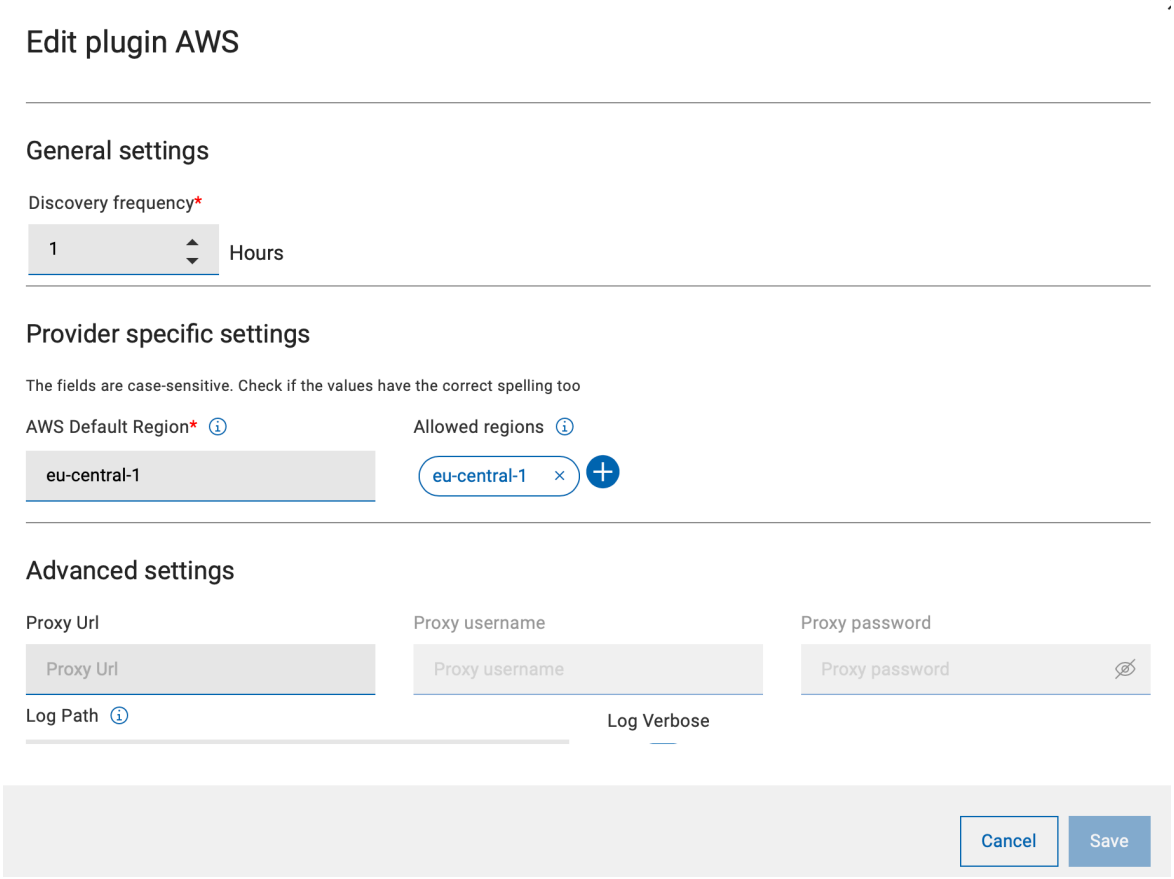
適用条件	パラメーター名	用途	使用しない場合
プラグイン	**AWS デフォルト・リージョン***	ログイン (API を使用してセッションを開く)	インストール時に必須
	許可リージョン (1)	プラグイン検出の有効範囲の設定 ユーザーが使用できる全リージョンのうち検出対象とするリージョンを列挙する	すべての管理リージョンが検出の対象となる
アカウント・ラベル	**AWS ユーザー・リージョン** (アカウント・ラベルのリージョン)	ログイン後、指定された **AWS デフォルト・リージョン**を上書き	**AWSDefaultregion** が使用される
	許可リージョン (アカウント・ラベル用)	プラグインの**許可リージョン** (1) を上書き (存在する場合) ユーザーが使用できる全リージョンのうち検出対象とするリージョンをリストアップしてアカウント検出範囲を絞り込む	プラグインの**許可リージョン** (1) が使用される

	リージョン (役割リージョン)	ログインに使用され、カスケードで**AWS ユーザー・リージョン**と**AWS デフォルト・リージョン**を上書きする	**AWS ユーザー・リージョン**またはカスケードで **AWS のデフォルト・リージョン**が使用される

プラグイン・レベルでの AWS リージョンの制限

AWS リージョンをプラグイン・レベルで設定するには、以下のステップを実行します。

1. **「AWS」**タブをクリックします。
2. **「プラグインの管理」** ページで、プラグインの**「一般設定」**を編集します



-

- 1 つ以上のリージョンを追加して、検出を制限します。追加されたリージョンは、丸のマーク付きでリストに表示されます。

  重要: BigFix ではリージョン名が正確に入力されたかどうかを検証する機能がないため、リージョン名は正しいスペルで入力してください。「AWS リージョンの名前およびコード」を参照してください。

- リージョンは簡単に削除できます。

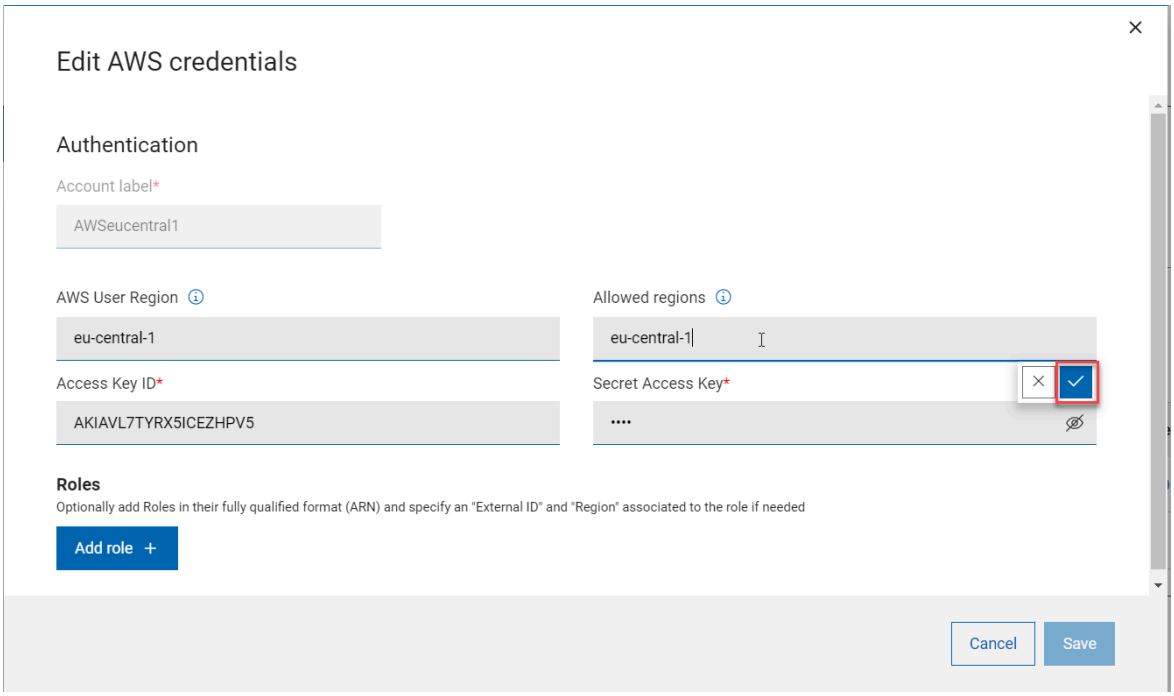
必要なリージョンをすべて追加した後、**「保存」**をクリックします。これで Fixlet がデプロイされ、構成の変更が適用されます。

資格情報レベルでの AWS リージョンの制限

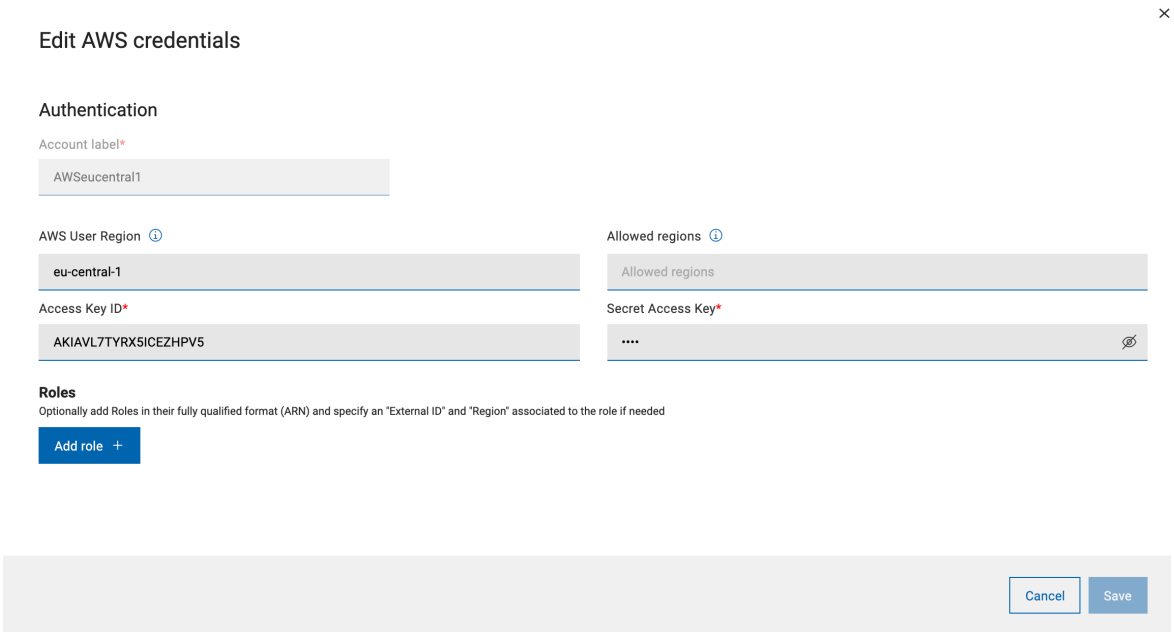
AWS リージョンを資格情報レベルで制限するには、以下の手順を実行します。

1. 認証テーブルで、対象の資格情報の **「資格証明の編集」** をクリックします。

2. **「AWS 資格情報の編集」**ページで AWS リージョンを入力し、チェック・マークをクリックして追加します。必要なリージョンを追加します。

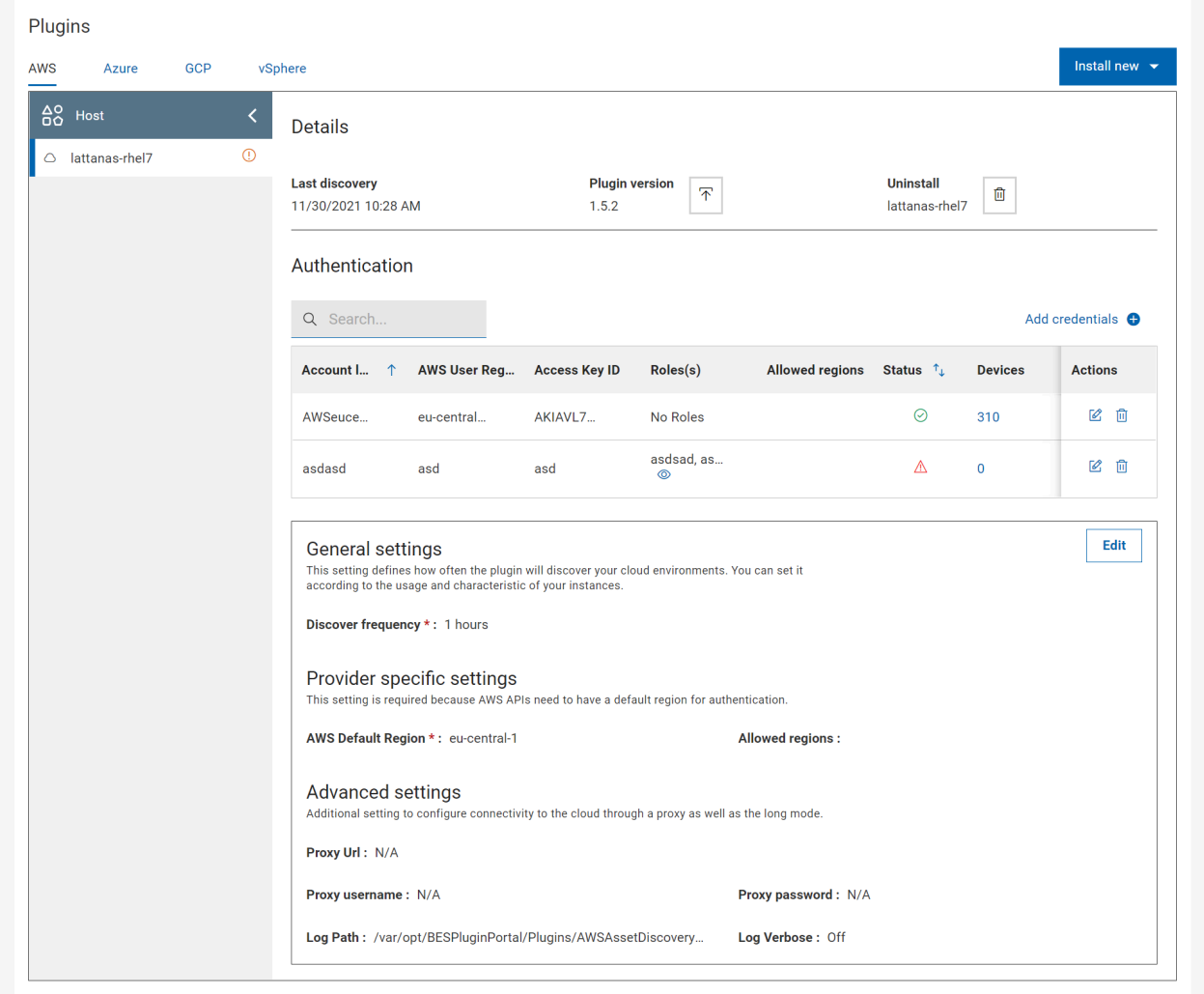


- **重要:** リージョン名が正確に入力されたかどうかは検証されないため、リージョン名は正しいスペルで入力してください。
- 「x」マークをクリックすると、リージョンを削除することもできます。



3. 必要なリージョンをすべて追加したら、**「送信」**をクリックします。これで Fixlet がデプロイされ、構成の変更が適用されます。

変更が適用されると、AWS プラグイン・タブの関連セクション (「認証テーブル」列の「許可リージョン」または「一般設定」セクション) に表示されます。



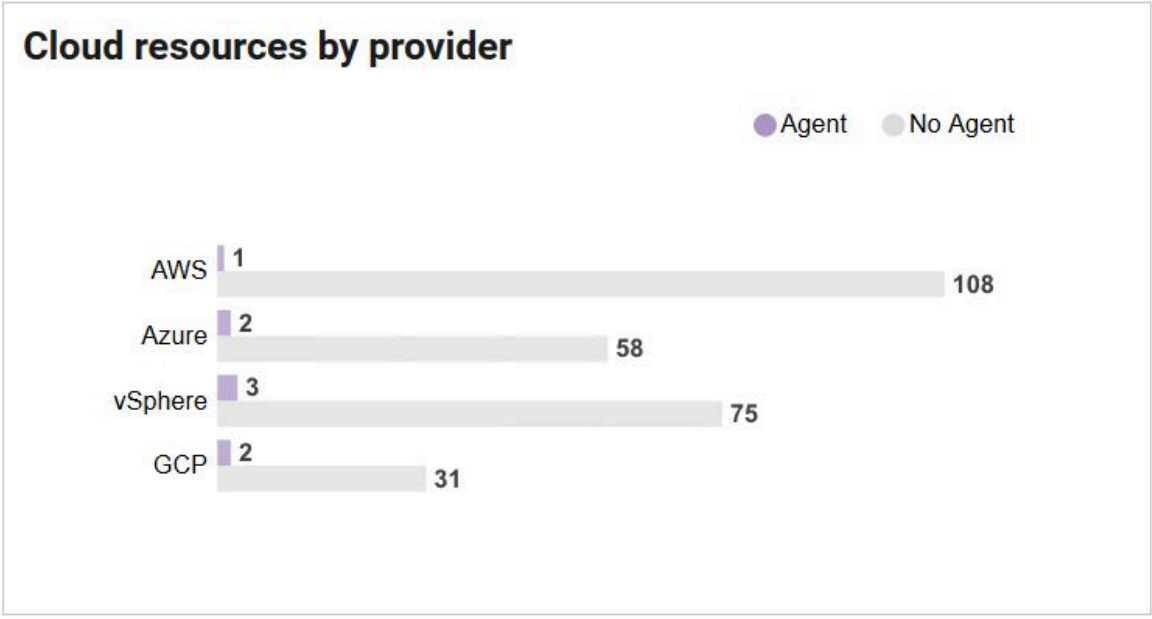
クラウドで検出されたデバイスへの BigFix エージェントのインストール

BigFix Web UI から、クラウド・プラグインで検出されたデバイスに BigFix エージェント・コードをインストールできます。

- クラウドで検出されたデバイスに Windows または Linux x 86 64bit オペレーティング・システムがある場合のみ、BigFix エージェントをインストールできます。
- CDT インフラストラクチャを設定する必要があります。CDT 文書とログ・ファイルはトラブルシューティングにも活用できます。詳しくは、https://help.hcl-software.com/bigfix/10.0/platform/Platform/Installation/c_using_the_cdt.htmlを参照してください。

WebUI では、すでに BigFix で採用されているクライアント・デプロイメント・ツール (CDT) テクノロジーを使用します。CDT ウィザードと比べて、WebUI はシンプルで効率化されたプロセスになっています。BigFix エージェントを WebUI 経由でデプロイするには、以下の手順を実行します。

1. WebUI のランディング・ページから、**「概要」**をクリックし、ドロップダウン・メニューで**「クラウド・ダッシュボード」**を選択します。
2. **「プロバイダーごとのクラウド・リソース」**ダッシュボードには、BigFix エージェントの有無にかかわらず検出されたすべてのデバイスの概要がまとめられています。目的のクラウド・プロバイダーに属するデバイスで、BigFix エージェントがインストールされていないものを表すバーをクリックします。



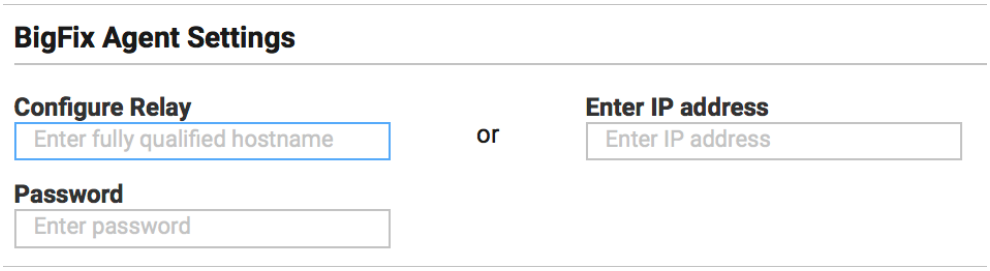
これで、**「デバイス」**（（ページ） *22)*ページが以下のプロパティーにフィルタリングされた内容が表示されます。

- **管理元**: <選択したクラウド・プロバイダー>
- **BigFix エージェントの状態**: `Not installed`

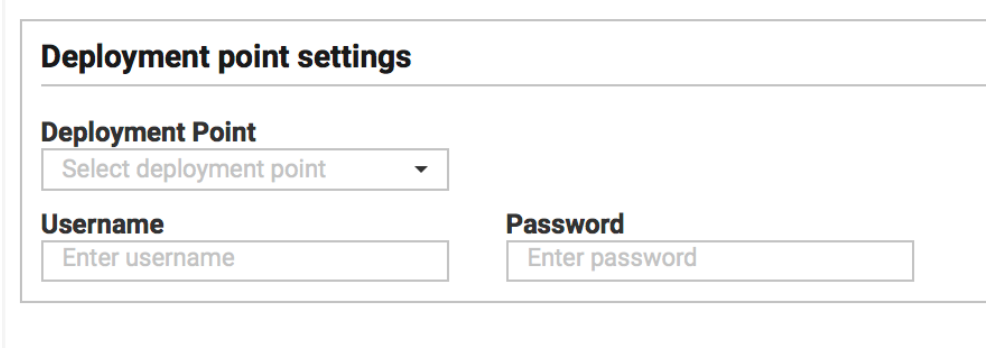
3. フィルターされたリストから、BigFix エージェントをインストールするデバイスを 1 つ以上選択します。
4. **「デプロイ」**ドロップダウン・ボタンをクリックし、**「BigFix エージェントのデプロイ」**を選択します。ここで、既存の CDT インフラストラクチャを通じて BigFix エージェントのインストールに必要なパラメーターをカスタマイズできます。設定を指定する前に、ページ右上の**「デバイスの編集」**ボタンをクリックして、対象デバイスのリストを見直し、変更できます。

   デプロイメント設定

   BigFix エージェント設定: この設定は任意であり、リレー接続に関連しています。指定しない場合は、BigFix エージェントの開始時にデプロイメント設定に基づいてトップ・レベル・リレーのルート・サーバーに接続します。ホスト名または IP でリレーを指定する際、選択したリレーに認証が設定されている場合はパスワードが必要になることがあります。



デプロイメント・ポイント設定: この設定では、ターゲットにエージェント・コードを配信する CDT デプロイメント・ポイント (利用可能な Windows デプロイメント・ポイントから) を選択できます。

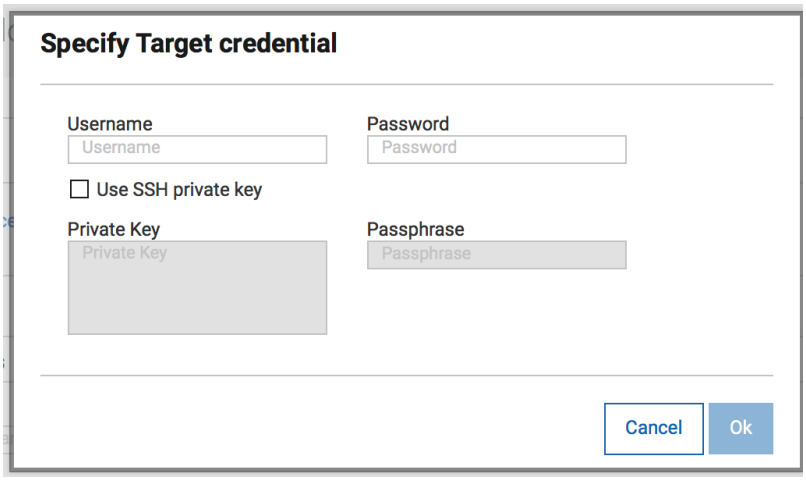


注: すべての配信に対して、使用できるのは 1 つのデプロイメント・ポイントのみです。ターゲットの異なるバケットに複数のデプロイメント・ポイントを割り当てることはできません。コンピューターのユーザー名とパスワードも必要です。

デプロイメント・ポイントを選択するとき、対象デバイスとデプロイメント・ポイントがお互いを ping する (接続する) ようにする必要があります。BigFix コンソールの CDT ウィザードとは異なり、通信を保証するためのプロキシを設定できないためです。

BigFix エージェントの事前定義済みバージョンがインストールされます。新しいバージョンが利用可能な場合は、BigFix サポート・サイトにあるアップグレード fixlet 経由でエージェントをアップグレードできます。

対象の資格情報の指定: この設定では、BigFix エージェント・コードのインストールを許可するためにターゲット・マシンに資格情報を設定できるようにします。同時に複数のデバイスを選択して同じ資格情報を割り当てる (必要な場合)、または 1 つずつ異なる資格情報を割り当てることができます。デバイスは IP で識別されます (コンピューターを名前で選択しても CDT がこれらのデバイスに IP 経由で接続するのはこのためです)。コンピューターに複数の IP がある場合、CDT は 1 回目の応答が得られるまですべての IP への接続を試行します。



検索フィールドでは、必要に応じてこのリスト内の特定のマシンを検索できます。

選択できたら、**「資格情報を設定」**をクリックしてユーザー名とパスワードの組み合わせか、SSH プライベート・キーをポップアップに入力します。

5. すべての必要な設定を終えたら、**「デプロイ」**ボタンをクリックしてデプロイメントを開始します。
これで、**「デプロイメント」**ページに CDT プロセスを開始するためのアクションの状態が示されるようになります。

注: このアクションの成功は、CDT がプロセスを正常に開始したことのみを示し、エージェントが対象デバイスにインストールされたことを示すものではありません。

BigFix エージェントがデバイスに正常にインストールされたら、以下が起こります。

- デバイスが BigFix エージェントを介して BigFix サーバーに接続します。
- デバイスのエントリーが、クラウド・ディスカバリーに関連する既存のエントリーと関連付けられます。
- 「デバイス」ページのデバイスの視覚化が、クラウド・アイコンから BigFix ロゴとクラウド・アイコンに変わります。例えば、 

から のようになります。 

BigFix エージェントは、「デバイス」ページから**「管理元」**と**「BigFix エージェントの状態」**フィルターを適切に選択してクラウド・デバイスにインストールすることもできます。

注: システムから適切なエラー・メッセージが返されます。

- BigFix エージェントのデプロイにクラウドで検出されたデバイスと MDM デバイスの組み合わせを選択した場合
- すでに BigFix エージェントがインストールされているデバイスを選択し、「デプロイ」ドロップダウン・アクションから BigFix エージェントのデプロイを試行した場合

クラウド・ネイティブのデバイスへの BigFix エージェントのインストール

BigFix WebUI から、AWS および Azure 環境に BigFix エージェントをインストールし、クラウド・プロバイダー・サービスを使用できます。

このタスクは、BigFix プラットフォームのバージョン 10 パッチ 2 から利用可能です。このパッチをインストールしてから、このタスクを開始する必要があります。

WebUI はネイティブのクラウド API サービスを使用します。

WebUI を介して BigFix エージェントをデプロイするには、次の手順を実行します。

1. WebUI のランディング・ページで、右上隅にある歯車アイコンをクリックし、ドロップダウン・メニューから**「エージェントのインストール」**を選択します。
2. **「BigFix エージェントのインストール」**ページに、使用可能なインストール方法のいずれかを使用して、BigFix で既に検出され登録されているデバイスにエージェントをインストールできる画面が表示されます。

   AWS ネイティブ API

   このメソッドは、Amazon Web Services のネイティブ・クラウド API サービスを使用してエージェントをデプロイし、実行権限を持つ AWS アクセスを必要とします。

   Azure ネイティブ API

   このメソッドは、Microsoft Azure ネイティブ・クラウド API サービスを使用してエージェントをデプロイし、実行特権を持つ Azure アクセスを必要とします。

   注: これらの選択肢は、括弧内に表示され、次の条件を満たすデバイスにリンクされます。
   - インストール Fixlet に関連するデバイス。
   - インストールに必要な前提条件を満たすデバイス。

   クラウド・プラットフォームでもっと多くのデバイスが検出される場合がありますが、ネイティブ API サービスを利用するために必要な前提条件を満たしていなければ、デバイスは表示されません。

注: ネイティブ・エージェントのインストール・エラー (終了コード) および推奨アクションの詳細については、「BigFix クラウド・リソースへのエージェントのインストール (（ページ）　　)」を参照してください。

「デバイス」ページからのエージェントのインストール

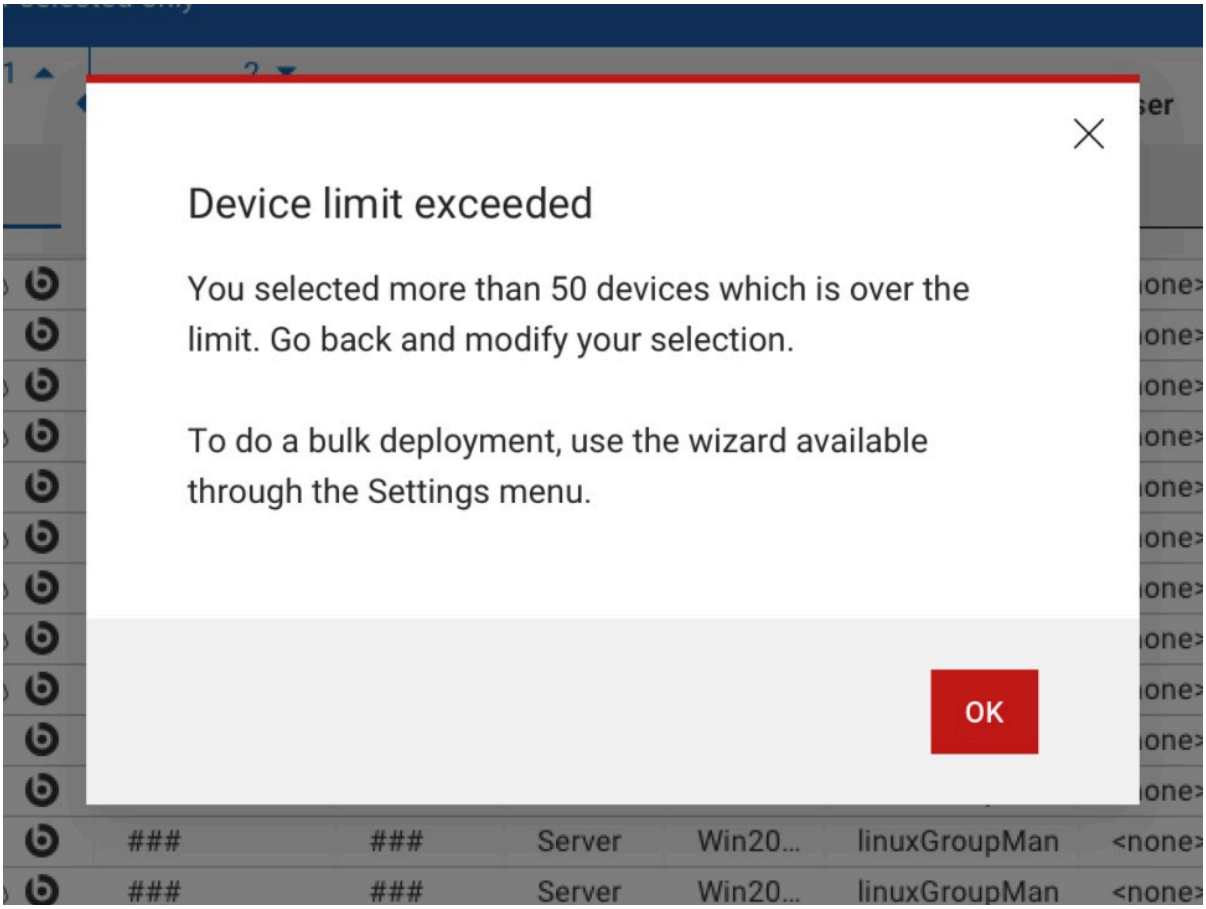
デバイスを選択した後、「デバイス」ページの**「管理」**メニューからエージェントをインストールできます。

「管理」で、**「エージェントのインストール」**を選択します。

選択したデバイスの組み合わせによって、アクションの完了を警告するメッセージや禁止するメッセージが表示されます。

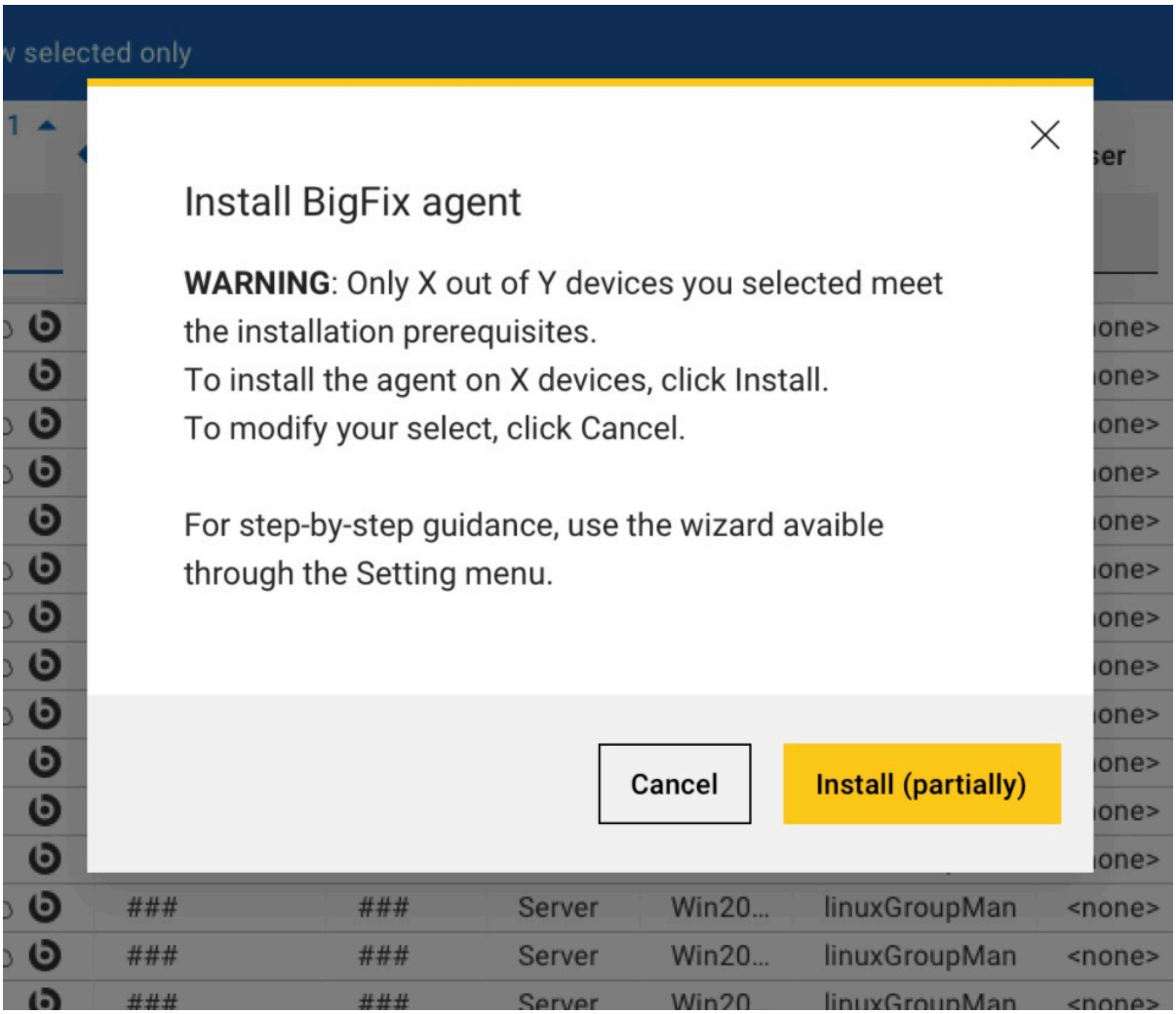
シナリオ 1

50 台を超えるデバイスを選択しました。最適なパフォーマンスを得るには、代わりにウィザードを使用して、アクションは送信されません。



シナリオ 2

選択したデバイスのサブセットのみが、ネイティブ・インストールの前提条件を満たしています。したがって、アクションを実行すると、そのアクションはデバイスのサブセットに対してのみ送信されます。



シナリオ 3

選択したデバイスが混在しています。例えば、MDM とクラウドで管理するデバイスを選択したとします。この場合、WebUI は、エージェントがまだインストールされていない混在デバイスのインストールをブロックします。

付録 A. サポート

この製品について詳しくは、以下のリソースを参照してください。

- BigFix サポート・ポータル
- BigFix Developer
- YouTube の BigFix プレイリスト
- YouTube の BigFix Tech Advisors チャネル
- BigFix フォーラム

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.