Modern Client Management for BigFix 10
管理者ガイド

特記事項

本書および本書で紹介する製品をご使用になる前に、特記事項 (##### 79)に記載されている情報をお読みください。

本書に関する注意事項

本書は、BigFix バージョン 10、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. 概説

このガイドは、HCL BigFix マスター・オペレーター (MO) と BigFix デプロイメントの管理者を対象としています。最新のクライアント管理 (MCM) の使用方法については、ユーザーズ・ガイド *(#####　　)*を参照してください。

MCM オファリングにより、ベンダーのモバイル・デバイス・マネージャー (MDM) API を通じてオペレーティング・システムを実行しているエンドポイントを管理できます。この機能により、BigFix は MDM を通じてデバイスおよびエンドポイントとやり取りできます。BigFix では、コンソールまたは WebUI を通じて、プロファイル、カスタム・コンテンツ、パッチ、ソフトウェア、BigFix エージェントをデプロイできます。BigFix ではデバイスが紛失または盗難にあった場合に、リモートでデバイスをワイプまたはロックすることもできます。MDM サーバーは、MDM API を介して BigFix コンソールまたは WebUI から呼び出すすべてのアクションを管理します。

本リリースの新機能

BigFix 10 用 MCM の現在のリリースで行われた機能強化の概要。

MCM v1.1 の更新

- **Apple 自動デバイス登録**

  MCM v1.1 では、新しい macOS デバイスまたは工場出荷時リセットの macOS デバイスを自動的にセットアップおよび事前設定するための機能が導入されています。完全な情報とセットアップの説明については、「Apple 自動デバイス登録 *(##### 42)*」を参照してください。
- **Windows 10 デバイスの Autopilot 登録**

  このリリースでは、新しい Windows 10 デバイスまたは工場出荷時リセットの Windows 10 デバイスを自動的にセットアップおよび事前設定するための Autopilot 機能が導入されています。完全な情報とセットアップの説明については、「Autopilot 登録 - Windows 10 *(#####　　)*」を参照してください。
- **Windows 10 デバイスの一括登録**

MCM v1.1 の一括登録機能を使用すると、多数の BigFix 管理対象 Windows 10 デバイスを数分で MDM サーバーに登録できるようになります。詳しくは、『一括登録 - Windows *(##### 34)*』を参照してください。

- **証明書管理**

  MCM v1.1 では、macOS と Windows の両方の MDM エンドポイントに証明書ポリシーをデプロイする機能が導入されており、証明書の管理が非常に簡単になります。手順については、「証明書ポリシー *(#####)*」を参照してください。

- **WebUI を使用して BigFix MCM を構成および管理する**

  このリリースには、WebUI を介して BigFix MCM を構成および管理する機能が含まれています。WebUI を使用すると、MCM コンポーネントのインストール、アップグレード、およびアンインストールを簡単に行うことができます。詳細な手順については、『MCM ユーザー・ガイド *(#####)*』を参照してください。

- **MDM エンドポイントへのソフトウェアのデプロイ**

  このリリースでは、WebUI を介して MDM API を使用して、MDM エンドポイントにソフトウェア・アプリケーションを迅速にデプロイできます。手順については、「アプリケーションの事前ステージング *(#####)*」を参照してください。

- **制限プロファイル**

  MCM v1.1 では、Windows と macOS の両方に制限プロファイルを作成できます。MDM エンドポイントでプライバシーやユーザー・エクスペリエンスなどの多くの設定を構成するのはシンプルで簡単です。

- **LDAPS ユーティリティー**

  MCM v1.1 では、LDAPS の問題を迅速にトラブルシューティングできるコマンド・ライン・ユーティリティーが導入されています。

- **登録解除**

  このリリース以降、MCM からデバイスの登録を解除する場合は、WebUI を使用してデバイスを登録解除できます。その手順については、『デバイスの登録解除 *(#####)*』を参照してください。

- **MCM コンポーネントをアップグレードするための Fixlet**

  MCM v1.1 リリースでは、Apple デバイス用の MDM 登録プロファイルを更新できます。関連する Fixlet の BESUEM サイトをご覧ください。

- **パフォーマンスの向上**

  このリリースには、安定性とパフォーマンスの向上とフィックスが多数含まれています。キャパシティー・プランニングと構成に関する推奨事項については、BigFix パフォーマンスとキャパシティー・プランニングのリソース (#####　　)で BigFix キャパシティー・プランニングのドキュメントを参照してください。
- **対処されたセキュリティーの脆弱性**

  MCM v1.0.1 の製品セキュリティーの脆弱性の問題は、このリリースで解決されています。

以前のリリースで追加された機能

BigFix 10 用 MCM の以前のリリースで行われた機能強化の概要。

MCM v1.0.1 の更新

- **BigFix Work from Home Solution のサポート**

  MCM v1.0.1 は、BigFix Work from Home Solution をサポートしています。BigFix Work from Home Solution の詳細については、『BigFix Work from Home Solution ガイド (#####　　)』を参照してください。
- **パフォーマンスの向上**

  このリリースには、安定性とパフォーマンスの向上とフィックスが多数含まれています。キャパシティー・プランニングと構成に関する推奨事項については、BigFix パフォーマンスとキャパシティー・プランニングのリソース (#####　　)で BigFix キャパシティー・プランニングのドキュメントを参照してください。
- **オペレーティング・システムのサポートの拡張**
  - MCM ソリューションは、Docker CE+ をインストールするための回避策により MDM サーバーおよびプラグイン・ポータル・サーバーでの RHEL 8 をサポートします。詳しくは、『RHEL8 の Docker CE+ Docker 構成のインストール (##### 50)』を参照してください。
  - MCM ソリューションは、MCM エンドポイントで実行されている Windows 10 (Pro、Enterprise、および Home) をサポートします。

注: 特定の Windows エディションのみが、MDM を介して構成されているすべての使用可能なオペレーティング・システムの機能をサポートします。詳細については、Windows 構成サービス・プロバイダー (CSP) リファレンス (### ##) のドキュメントを参照してください。各 CSP では、どの Windows エディションがサポートされているかが強調表示されます。

- **MCM コンポーネントをアップグレードするための Fixlet**

  MCM v1.0.1 リリースでは、BigFix コンソールから入手できる Fixlet を使用して MCM コンポーネントをアップグレードできます。関連する Fixlet の BESUEM サイトをご覧ください。

- **MCM の保守性のための WebUI 正常性チェック・ダッシュボード**

  WebUI 正常性チェック・ダッシュボードは、BigFix MCM デプロイメントの正常性を監視するために使用できます。詳細については、「正常性チェック (#####)」を参照してください。

- **対処されたセキュリティーの脆弱性**

  MCM v1.0.0 の製品セキュリティーの脆弱性の問題は、このリリースで解決されています。

第 2 章. 前提条件および要件

最新のクライアント管理 (MCM) をインストールする前に Red Hat® Enterprise Linux® システムに次のパッケージがプリインストールされている必要があります。

MDM サーバー

ターゲット・コンピューターには、次の要素がインストールされている必要があります。

- コンピューターは RHEL 7+ または RHEL 8+ で実行されている必要があります
- Docker (CE v19.x または RHEL バージョン 1.13 以降) および Docker Compose 1.25.x
- BigFix クライアント・バージョン 10.0.2 以降
- OpenSSL
- unzip

注: RHEL8 はデフォルトでは Docker CE+ をサポートしていません。RHEL8 に互換性のある Docker CE+ バージョンをインストールするための回避策については、次を参照してください。 RHEL8 の Docker CE+ Docker 構成のインストール *(##### 50)*

プラグイン・ポータル

ターゲット・コンピューターには、次の要素がインストールされている必要があります。

1. BigFix クライアント・バージョン 10.0.2 以降
2. プラグイン・ポータルのバージョン 10.0.2 以降
3. Mongo DB 4.2.3 以降

注:

- BESAgent 10.0.1 では、有効期限の証明書検査は機能しません。したがって、証明書インスペクターが MDM 証明書の有効期限を確認するには、BigFix クライアント・バージョン 10.0.2 が必要です。
- プラグイン・ポータル 10.0.2 は、MCM v1.1 へのアップグレードの際に、いくつかの重要なプラグインからプラグイン・ポータル API への変更に互換性を持たせるために必要です。
- プラグイン・ポータルをプラットフォーム 10.0.2 にアップグレードする場合は、API の変更に対応するために MCM を 1.1 バージョンにアップグレードする必要があります。

要件

サポートされるシステム環境

このセクションでは、BigFix 10 用 MCM でサポートされるシステム環境について説明します。

コンポーネント	サポート対象の環境
プラグイン・ポータルとプラグイン	RHEL7.4 以降、RHEL8 以降、または Windows 2012 R2 以降
MDM サーバー・ホストと Docker	RHEL 7 から RHEL 8
デバイスのオペレーティング・システム	Windows 10 (Pro、Enterprise、および Home[1])、macOS 10.14 以降

1. 特定の Windows エディションのみが、MDM を介して構成されているすべての使用可能なオペレーティング・システムの機能をサポートします。詳細については、Windows 構成サービス・プロバイダー・リファレンス *(#####)* のドキュメントを参照して

コンポーネント	サポート対象の環境
Docker エンジン	CE v19.x または RHEL バージョン 1.13 以降
Docker-compose	1.25.x
MongoDB	RHEL7.4 以降、RHEL8 以降、および Windows 10/Server 2016 以降

最小ハードウェア所要量

ハードウェアの最小要件については、BigFix キャパシティー・プランニング (#####)のドキュメントを参照してください。

BigFix のデプロイメントと管理に関する詳細および最新情報については、「BigFix のパフォーマンスとキャパシティー・プランニングのリソース (#####)」を参照してください。

ポート要件

BigFix が MDM プラグインを介して管理するデバイスと適切に通信するには、ファイアウォールで次のポートが開かれていることを確認してください。

ポート番号	タイプ	目的	方向
443	HTTPS	すべてのデバイス登録と管理要求がこのポートに送信されます。エンドポイントが登録サーバーに到達するには、インターネットに接続するポートである必要があります。	MDM 管理対象エンドポイントが存在するネットワークから MDM サーバーへのインバウンド

ください。各 CSP では、どの Windows エディションがサポートされているかが強調表示されます

ポート番号	タイプ	目的	方向
5671	AMQP	MDM プラグインは、MDM サーバーがこのポートを介して登録済みデバイスから取得する非同期通知を受信します。セッションを確立し、デバイス通知を受信するには、この MDM サーバーへのインバウンド・ポートをプラグイン・ポータル・サーバー用に開く必要があります。	プラグイン・ポータル・サーバーから MDM サーバーへのアウトバウンド
8443	HTTPS	MDM サーバー REST API に HTTPS 要求を送信する場合。	プラグイン・ポータル・サーバーから MDM サーバーへのアウトバウンド
636	LDAPS	Active Directory で登録時にエンド・ユーザーを安全に認証する場合。	MDM サーバーからカスタマー LDAP への送信
389	LDAP	Active Directory で登録時にエンド・ユーザーのセキュリティーで保護されていない認証を行う場合。 **注:** Active Directory のセキュア・ポートが有効になっていない場合、デフォルトの安全でないポートは 389 です。最良の結果を得るには、Active Directory で LDAPS (セキュアな通信) を使用します。	MDM サーバーからカスタマー LDAP へのアウトバウンド
2195*	TCP	MDM サーバーから APN にメッセージを送信する場合。	MDM サーバーから APN サーバー (インターネット) へのアウトバウンド。
2196*	TCP	MDM サーバーがフィードバックのために APN に接続するために使用します。	MDM サーバーから APN サーバー (インターネット) へのアウトバウンド。

ポート番号	タイプ	目的	方向
5223	TCP	ネットワーク内のコンピューターから APNS にメッセージを送信する場合。	Mac デバイス (どちらのネットワーク上にある場合でも) から APN サーバー (インターネット) へのアウトバウンド。

*信頼性の高いサーバー通信を確保するには、TCP ポート 2195 および 2196 を介して、MDM サーバーから Apple 17.0.0.0/8 ブロックへのアウトバウンド接続を許可します。

第 3 章. BigFix のインストール

BigFix プラットフォームをインストールするには、ライセンスを取得し、インストール・ウィザードを実行し、ガイドに従って BigFix ルート・サーバー、コンソール、クライアント、WebUI をインストールします。

License Key Center アカウントを使用して BigFix ライセンス認証ファイル (`*.BESLicenseAuthorization`) のライセンスを購入し取得します。概念実証を評価する場合は、HCL の技術営業担当員にお問い合わせください。

BigFix とそのコンポーネントのインストールの詳細については、「BigFix のインストール *(#####　　)*」をご覧ください。

第 4 章. LDAPS 認証の設定

BigFix MDM では、さまざまなデバイス登録オプションを使用できます。オプションの 1 つは、セキュア・ライトウェイト・ディレクトリー・アクセス・プロトコル (LDAPS) 認証を、Over-the-Air (OTA) 登録用に構成することです。これにより、MDM サーバーへの登録が承認済みユーザーのみに制限されます。BigFix 10 の MCM を使用すると、管理者は、LDAPS 認証を使用してデバイスのユーザーを認証して、 Windows™ および Apple® デバイスを管理できます。

その他のデバイス登録オプションについては、次を参照してください。 デバイス登録 *(### ## 28)*

LDAPS のセットアップ

BigFix 管理者は、デバイスを BigFix MDM サーバーに登録する前に、LDAPS 認証を使用してユーザーの資格情報を確認します。
デバイスが Microsoft Active Directory サーバー (MSAD) または LDAP サーバーに接続するための次の前提条件を満たす必要があります。

- LDAPS URL
- 基本識別名 (ベース DN)
- バインド用識別名 (バインド DN)
- バインドのパスワード

これらのパラメーターは Fixlet で定義されています。Fixlet を使用して MDM サーバーをセットアップおよび構成する方法の詳細については、「MDM サーバーのインストール *(##### 18)*」をご覧ください。LDAPS 設定の詳細については、「LDAPS パラメーター *(#####)*」をご覧ください。

関連情報

LDAPS 接続のトラブルシューティング *(##### 52)*

第 5 章. 証明書の構成

MDM サーバーと Apple デバイス間で証明書を構成し、認証された接続を確立する方法について説明します。

Apple® プッシュ通知

Apple プッシュ通知 (APN) は、MDM サーバーにチェック・インするよう Apple デバイスに通知するために使用されます。Apple デバイスに通知をプッシュするには、モバイル・デバイスを管理するために必要なAPN 証明書 (### ##)が必要です。

注: APN 証明書を作成するには、有効な Apple ID (できれば会社の Apple ID) が必要です。

MDM サーバーと Apple プッシュ通知サーバー間の認証済み接続を確立するには、証明書署名要求 (CSR) を作成し、署名のために HCL に CSR ファイルを送信する必要があります。署名後、Apple 開発者アカウントに CSR ファイルをアップロードして、Apple からプロバイダー証明書を取得する必要があります。

Apple からプロバイダー証明書を取得するには、次の手順を実行します。

1. コマンド行インターフェースで、以下のコマンドを実行して CSR を作成します。

```
openssl req -newkey rsa:2048 -nodes -keyout PUSHCERTNAME_te
mp.key -out PUSHCERTNAME.csr -subj "/C=US/CN=HOSTNAME/email
Address=EMAILADDRESS"
```

注:

- `PUSHCERTNAME` は、任意の名前に置き換えることができます。
- `EMAILADDRESS` は、組織に固有である必要があります。HCL または BigFix が保存または直接使用することはありません。
- `HOSTNAME` は、MDM サーバーが実行されるサーバーの FQDN である必要があります。

2. 以下のコマンドを実行します。

```
openssl rsa -des3 -in PUSHCERTNAME_temp.key -out PUSHCERTNAME.key
```

プロンプトが表示されたら、選択した PEM パス・フレーズを入力します。その後、確認を求められます。

重要: 生成された `PUSHCERTNAME.csr` および `PUSHCERTNAME.key` を安全な場所に保存します。これらのファイルは、1 年後の Apple での証明書の更新時に使用できます。また、証明書を更新するために安全な場所に PEM パス・フレーズを保管してください。

3. `CSR` ファイルを BFAppleCSR@hcl.com *(#####)* に送信します。

重要: メールの本文に HCL カスタマー ID または BigFix サーバーのシリアル番号を含めます。

4. HCL 署名付きバージョンの `CSR` ファイルに加えて、BFAppleCSR@hcl.com *(#####)* からの追加の指示が、1 営業日以内に送信者の電子メール・アドレスに返されます。その電子メールの指示に従って、Apple Developer アカウントから必要なファイルを入手します。

MDM SSL 証明書

MDM クライアント認証証明書

MDM サーバーに対してプラグインを認証するには、SSL 証明書が必要です。安全な通信を行うには、BigFix ルート・サーバーで `BESAdmin` コマンドを実行するときに、新しいオプションを使用して証明書を生成する必要があります。コマンドを実行して SSL 証明書を生成する前に、ディレクトリーを作成します。コマンドの実行後に生成されたすべての SSL 証明書は、作成したディレクトリーに保存されます。

注:

- BES 管理ツールでコマンドを実行して証明書を生成するには、到達可能な DNS ホスト名が必要です。

Windows BigFix ルート・サーバーで SSL 証明書を生成するには、次のコマンドを実行します。

```
BESAdmin.exe /generateplugincertificates /certificatespath:<path-to-store-certs> [/commonname:<CN-for-server-and-client-cert>]
```

Linux BigFix ルート・サーバーで SSL 証明書を生成するには、次のコマンドを実行します。

```
BESAdmin -generateplugincertificates
 -certificatespath=<path-to-store-certs> [-commonname:<CN-for-server-and-client-cert>
```

注:

- *commonname* には、MDM サーバーの FQDN 名を使用します。
- これらのコマンドは、*`path-to-store-certs`* ディレクトリーが存在する場合にのみ機能します。

作成したフォルダーに次の SSL 証明書が生成されます。

- `ca.cert.pem`
- `client.cert.pem`
- `client.key`
- `server.cert`
- `server.key`

注: MDM プラグインと MDM サーバーのインストール時に、上記の SSL 証明書とキーを使用します。

MDM サーバー証明書

実稼働環境の MDM サーバー用に、CA 署名付きドメイン SSL 証明書を取得する必要があります。エンドポイントで MDM サーバーに登録して通信するには、信頼できる CA SSL 証明書が必要です。SSL 証明書は、サービスを開始する前に `/var/opt/BESUEM/certs` ディレクトリーで使用できるようにする必要があります。すべての証明書は、MDM サーバー・インストール Fixlet を通じてデプロイされます。

Windows MDM のサポートのみにステージング環境とラボ環境を使用している場合は、次のように自己署名証明書を生成する必要があります。

- OpenSSL コマンドライン・インターフェースの任意の RHEL サーバーで次のコマンドを実行して、指定したディレクトリーに `mdmserver.key` および `mdmserver.crt` ファイルを生成します。MDM サーバーをデプロイする準備ができたら、この SSL 証明書とキーが必要になります。

```
DNSNAME=<MDM_FQDN_HOSTNAME>; (cat /etc/pki/tls/openssl.cnf;
 printf "\n[SAN]\nsubjectAltName=DNS:$DNSNAME\n") | openssl
 req -new -newkey rsa:2048 -days 365 -nodes -x509 -sha256 -
keyout mdmserver.key -out mdmserver.crt -subj "/CN=$DNSNAME
" -config /dev/stdin
```

注: macOS 10.15 以降を使用している場合、コマンドライン・インターフェースを使用して作成された自己署名証明書は macOS MDM では機能しません。この場合、信頼された CA 証明書を使用する必要があります。

第 6 章. 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 で提供される MCM テクノロジーのサーバー・インフラストラクチャーを提供します。

最新のクライアント管理 プラグイン・ポータルと 1 つ以上の MDM プラグインをプラグイン・ポータルにインストールする必要があります。

プラグイン・ポータルをインストールするための前提条件

プラグイン・ポータルをインストールするコンピューターに、次のアプリケーションをインストールします。

- BigFix クライアント、バージョン 10.0 以降
- MongoDB バージョン 4.2.3 以降

プラグイン・ポータルのインストール

プラグイン・ポータルを BigFix クライアントのサービスとしてインストールするには、BES サポート・サイトで利用可能な最新バージョンの **「BigFix プラグイン・ポータルをインストール」** Fixlet を実行します。このタスクでは、選択したターゲットに BigFix プラグイン・ポータルをインストールします。

プラグイン・ポータルのインストールと基本構成の詳細については、 プラットフォームの資料 *(#####　　)*をご覧ください。

プラグイン・ポータルは通常、次のディレクトリーにインストールされます。

- Windows:
  - C:\Program Files (x86)\BigFix Enterprise\BES Plugin Portal
- Linux:
  - /var/opt/BESPluginPortal
  - /opt/BESPluginPortal

注:

- 環境内に複数のプラグイン・ポータルがある場合がありますが、特定のターゲット・コンピューターにインストールするプラグイン・ポータルは 1 つのみにする必要があります。
- MDM デプロイメントでは、1 つの Windows MDM プラグイン *(##### 24)*と 1 つの Apple または macOS MDM プラグイン *(##### 25)*のみを使用できます。したがって、例えば、2 つのプラグイン・ポータルを使用している場合、各プラグイン・ポータルに 1 つの MDM プラグイン (Windows または macOS) のみを含めることができます。

MCM で動作するには、プラグイン・ポータルに MDM プラグインが必要です。MDM プラグイン・インストール・タスクは、システムに有効なプラグイン・ポータルが存在する場合のみ関連状態になります。ローカル BES クライアントは、タスクを定期的に評価して、タスクが関連しているかどうかを確認します。

第 7 章. MDM サーバーのインストール

MDM サーバーは、WebUI を介して、または BESUEM コンテンツ・サイトから適切なタスクを実行して設定できます。WebUI を使用して MDM サーバーを設定する手順については、「MDM コンポーネントのインストール *(#####　　)*」を参照してください。BESUEM タスクを使用した設定手順については、このセクションを参照してください。

- Docker Engine、Docker Compose、OpenSSL をインストールします。
- 次のいずれかのユーザー・ロールがあることを確認します。
  - MDM サーバー・ターゲット・マシンの可視性と BESUEM サイトの可視性を持つマスター・オペレーター (MO)
  - インストールを実行する権限を持つ管理者。
- BESClient 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、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。

BESUEM コンテンツ・サイトでは、一部のタスクで、macOS® MDM サーバーまたは Windows™ 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。インストール後、他のタスクを使用して MDM サーバー機能をさらに追加できます。これらのタスクを使用して、macOS と Windows の両方の MDM サーバーを構成することもできます。
Install BigFix Windows MDM Server タスクまたは Install BigFix macOS MDM Server タスクは、次のアクティビティを完了します。

1. ディレクトリーを作成します。
2. 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。
3. サーバーが実行される プラグイン証明書 *(##### 13)*と TLS 証明書を含むサービスと証明書、および macOS MDM サーバーをインストールする場合は Apple プッシュ証明書をインストールします。
4. 必要なすべての構成を適用します。

Windows エンドポイント用の BigFix MDM サーバーのインストール

Windows エンドポイント用の BigFix MDM サーバーをインストールする方法について説明します。

WebUI を使用して Windows エンドポイント用の BigFix MDM サーバーをインストールする方法については、「Windows エンドポイント用の BigFix MDM サーバーのインストール *(#####)*」を参照してください。

このセクションでは、BESUEM タスク `Install BigFix Windows MDM Server` を使用して Windows エンドポイント用 BigFix MDM サーバーをインストールする方法について説明します。

始める前に: Windows 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。「MDM SSL 証明書 *(##### 13)*」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 エージェントが必要です。

`Install BigFix Windows MDM Server` タスクでは、次の情報を指定します。

1. 組織名を入力します。デバイスを登録すると、組織名がユーザーに表示され、残りのプロファイル情報も表示されます。
2. ユーザー向けのホスト名を入力します。例えば、「`mdmserver.deploy.bigfix.com`」と入力します。
3. LDAP パラメーターを入力します。これは、無線で MDM にユーザーを登録するための承認に使用されます。これにより、MDM サーバーへの登録が承認済みユーザーのみに制限されます。すべての LDAP パラメーターを省略すると、MDM に登録するために LDAP 認証を行う必要がなくなります。

   注: LDAP 認証はデフォルトでオンになっています。
4. 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. 文字列を入力して TLS キー・パスワードを設定します。
   b. 「MDM サーバーの TLS 証明書」コンテンツ・セクションで、生成された TLS `.crt` ファイルのテキスト・コンテンツ全体を入力します。

c. 「MDM サーバーの TLS キー」コンテンツ・セクションで、生成された TLS `.key` ファイルのテキスト・コンテンツ全体を入力します。

ヒント: 自己署名証明書を使用したい場合、`.crt` と `.key` ファイルを生成する方法については、「MDM SSL 証明書 *(##### 13)*」をご覧ください。

5. MDM サーバー認証証明書とキー・コンテンツの詳細を入力します。
   a. 「MDM サーバーの認証局」コンテンツ・セクションで、生成された `ca.cert.pem` ファイルのテキスト・コンテンツ全体を入力します。
   b. 「MDM サーバーの証明書」コンテンツ・セクションで、生成された `server.cert.pem` ファイルのテキスト・コンテンツ全体を入力します。
   c. 「MDM サーバーのキー」コンテンツ・セクションで、`server.key` ファイルのコンテンツを入力します。

   ヒント: `.pem` と `.key` ファイルの生成方法の詳細については、「MDM SSL 証明書 *(##### 13)*」をご覧ください。
6. ターゲット・システムにタスクをデプロイします。

Apple エンドポイント用の BigFix MDM サーバーのインストール

タスク `Install BigFix Apple MDM Server` を使用して、Apple エンドポイント用の BigFix MDM サーバーをインストールできます。

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。「MDM SSL 証明書 *(##### 13)*」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 エージェントが必要です。

注: 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 プッシュ証明書 PEM ファイルが必要です。

`Install BigFix Apple MDM Server` タスクでは、次の情報を指定します。

1. 組織名を入力します。デバイスを登録すると、組織名がユーザーに表示され、残りのプロファイル情報も表示されます。
2. ユーザー向けのホスト名を入力します。これは、登録するデバイスで指定する必要があるサーバーのホスト名です。値は有効な URL である必要があります。例えば、`mdmserver.deploy.bigfix.com` です。
3. 使用する MDM API パスワードを入力します (任意のパスワードを使用できます。これは構成後は外部からは見えません)。
4. LDAP パラメーターを入力します。これは、無線で MDM にユーザーを登録するための承認に使用されます。 これにより、MDM サーバーへの登録が承認済みユーザーのみに制限されます。すべての LDAP パラメーターを省略すると、MDM に登録するために LDAP 認証を行う必要がなくなります。

   注: LDAP 認証はデフォルトでオンになっています。
5. Apple プッシュ証明書とキー・コンテンツを入力します。
   a. Apple プッシュ・キー・パスワードを入力します。
   b. Apple プッシュ証明書 PEM コンテンツ・セクションに `Push PEM` ファイルのテキスト・コンテンツ全体を入力します。
   c. Apple プッシュ・キー・コンテンツ・セクションに `Push key` ファイルのテキスト・コンテンツ全体を入力します。
6. 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. 文字列を入力して TLS キー・パスワードを設定します。
   b. 「MDM サーバーの TLS 証明書」コンテンツ・セクションで、生成された TLS `.crt` ファイルのテキスト・コンテンツ全体を入力します。
   c. 「MDM サーバーの TLS キー」コンテンツ・セクションで、生成された TLS `.key` ファイルのテキスト・コンテンツ全体を入力します。

      ヒント: 自己署名証明書を使用したい場合、`.crt` と `.key` ファイルを生成する方法については、「MDM SSL 証明書 *(##### 13)*」をご覧ください。
7. MDM サーバー認証証明書とキー・コンテンツの詳細を入力します。
   a. 「MDM サーバーの認証局」コンテンツ・セクションで、生成された `ca.cert.pem` ファイルのテキスト・コンテンツ全体を入力します。
   b. 「MDM サーバーの証明書」コンテンツ・セクションで、生成された `server.cert.pem` ファイルのテキスト・コンテンツ全体を入力します。

c. 「MDM サーバーのキー」コンテンツ・セクションで、`server.key` ファイルのコンテンツを入力します。

ヒント: `.pem` と `.key` ファイルの生成方法の詳細については、「MDM SSL 証明書 *(##### 13)*」をご覧ください。

8. エンド・ユーザー契約のメッセージ・テキストを入力します。これは任意指定フィールドです。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。
9. ターゲット・システムにタスクをデプロイします。

BigFix Apple MDM 登録プロファイルを更新

BigFix Apple MDM サーバーのインストール中に最初にセットアップされた Apple デバイスの MDM 登録プロファイルを更新できます。

Apple MDM Server をインストールした後、任意の時点で Apple デバイスの登録プロファイルを更新する場合は、`Modify BigFix Apple MDM Server Enrollment Profile Parameters` タスクで、次のパラメーターの更新情報を指定し、対象のシステムにタスクをデプロイします。

1. 組織名。
2. ユーザー向けホスト名。
3. アクセス権。これは、登録済みデバイス上の MDM サーバーの機能を決定します。値は 4 桁の 10 進数でなければなりません。数値の計算方法の詳細については、次を参照してください。 https://developer.apple.com/documentation/devicemanagement/mdm *(#####)*
4. ユーザー契約のテキスト。

第 8 章. 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。 BESUEM タスクを使用した MDM プラグインの設定手順については、このセクションを参照してください。WebUI を使用してセットアップする方法については、『WebUI ユーザーズ・ガイド (#####)』を参照してください。

サーバー・ホストでプラグイン・ポータルが実行され、BigFix エージェント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。

注:

- MDM プラグインの 2 つのバージョンが利用可能です。macOS と Windows。
- タスクでは、(特に cacert からの) 資格証明書、クライアント証明書、BESAdmin から生成されたクライアント・キーが必要です。詳しくは、MDM SSL 証明書 (#####13)を参照してください。

次のステップでは、Install BigFix Plugin for MDM on macOS タスクまたは Install BigFix Plugin for MDM on Windows タスクを実行して、ターゲット・コンピューターに適切なプラグインをインストールします。

MDM プラグイン・インターフェースの理解

MDM プラグイン・インターフェースは MDM サーバーと通信します。ここから要求を MDM サーバーに転送し、MDM インフラストラクチャーから結果を取得します。MDM プラグインは、プラグイン・ポータルと MDM サーバー間のインターフェースとして機能します。

MDM プラグイン・インターフェースには、次のコンポーネントが含まれています。

MDM サーバーへの要求

これらの要求は、MDM サーバーへのアウトバウンド・インターフェースです。プラグインが登録済みデバイスからの情報を必要とする場合、またはデバイスまたは MDM サーバーからのアクションを要求する必要がある場合、プラグインはこのインターフェースを使用します。ほとんどの要求は、インバウンド・インターフェースから受信した非同期応答になります。これは、MDM プラグインと MDM サーバー間のセキュアな接続であり、クライアントとサーバーの証明書によって保護されています。

MDM サーバーからの応答

MDM プラグインは、MDM サーバーからのメッセージのサブスクライバーとして登録します。MDM プラグインは、登録されたデバイスからいつでもこのインターフェースから情報を受信できます。これは、MDM プラグインと MDM サーバー間のセキュアな接続であり、クライアントとサーバーの証明書によって保護されています。

Windows での MDM プラグインのインストール

サポートされている MDM プラグインを Windows プラグイン・ポータルにデプロイするには、以下の手順を実行します。

前提条件

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。

手順

1. **「MDM サーバー・アドレス」**フィールドに、MDM サーバーのホスト名または IP アドレスを入力します。
2. 次のパラメータを入力します。
    a. `ca.cert.pem` ファイルのテキスト・コンテンツ全体をコピーして**「認証局コンテンツ」**フィールドに貼り付けます。
    b. `client.cert.pem` ファイルのテキスト・コンテンツ全体をコピーして**「クライアント認証コンテンツ」**フィールドに貼り付けます。

c. `client.key` ファイルのテキスト・コンテンツ全体をコピーして**「クライアント・キー・コンテンツ」**フィールドに貼り付けます。

ヒント: `.pem` と `.key` ファイルの生成方法の詳細については、「MDM SSL 証明書 *(##### 13)*」をご覧ください。

3. ターゲット・システムにタスクをデプロイします。

- MDM プラグインは次の場所にあります。
  - Windows - `C:\Program File (x86)\BigFix Enterprise\BES Plugin Portal\Plugins`
  - Linux
    - バイナリー - `/opt/BESPluginPortal/Plugins`
    - データ・ファイル - `/var/opt/BESPluginPortal`

macOS での MDM プラグインのインストール

サポートされている MDM プラグインを macOS プラグイン・ポータルにデプロイするには、以下の手順を実行します。

前提条件

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。

手順

1. **「MDM サーバー・アドレス」**フィールドに、MDM サーバーのホスト名または IP アドレスを入力します。
2. 次のパラメータを入力します。
   a. `ca.cert.pem` ファイルのテキスト・コンテンツ全体をコピーして**「認証局コンテンツ」**フィールドに貼り付けます。
   b. `client.cert.pem` ファイルのテキスト・コンテンツ全体をコピーして**「クライアント認証コンテンツ」**フィールドに貼り付けます。

c. `client.key` ファイルのテキスト・コンテンツ全体をコピーして**「クライアント・キー・コンテンツ」**フィールドに貼り付けます。

ヒント: `.pem` と `.key` ファイルの生成方法の詳細については、「MDM SSL 証明書 *(##### 13)*」をご覧ください。

3. ターゲット・システムにタスクをデプロイします。

- MDM プラグインは次のパスにあります。
  - Windows - `C:\Program Files (x86)\BigFix Enterprise\BES Plugin Portal\Plugins`
  - Linux
    - バイナリー - `/opt/BESPluginPortal/Plugins`
    - データ・ファイル - `/var/opt/BESPluginPortal`

第 9 章. Apple 開発者アカウントの登録

プッシュ証明書を取得するには、BigFix 管理者として、企業に関連付けられた Apple ID が必要です。Apple Developer アカウントに登録して入手することもできます。開発者アカウントの登録方法の詳細については、 「Mac 開発者アカウントの登録 (#####　　)」をご覧ください。

第 10 章. デバイス登録

BigFix MDM で管理するには、デバイスを登録する必要があります。BigFix MDM サーバーは API 経由で、デバイスに適用されている MDM ポリシーに基づき、登録されたデバイスと通信します。

BigFix MDM 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 MDM では、デバイス・ユーザーがデバイスを自己登録したり、管理者ユーザーがデバイスを自動的に大量に登録するように設定を構成したりするためのオプションがあります。次の表は、登録方法とオペレーティング・システムの異なる組み合わせとシナリオを示しています。

登録方法	オペレーティング・システム	シナリオ
登録 URL を使用した登録 • Windows *(##### 29)* • macOS *(##### 40)*	Windows 10、macOS	• デバイスは既に従業員と一緒にある。 • 登録するデバイスの数は比較的少ない。
一括登録 *(#####)*	Windows 10	• MDM サーバーに登録する多数の Windows 10 デバイス。 • 登録をユーザーの介入なしに自動化する必要がある。 • デバイスには BigFix エージェントが既にインストールされている。
Autopilot 登録 - Windows *(##### 35)*	Windows 10	• MDM サーバーに登録するために初期 OS セットアップが必要な、多数の

登録方法	オペレーティング・システム	シナリオ
		会社所有の Windows 10 デバイス。 • 登録をユーザーの介入なしに自動化する必要がある。
Apple 自動デバイス登録 *(##### 42)*	macOS	• MDM サーバーに登録するために初期 OS セットアップが必要な、多数の会社所有の macOS デバイス。 • 登録をユーザーの介入なしに自動化する必要がある。

Windows デバイスの登録

さまざまな方法で、Windows 10 デバイスを BigFix MDM に登録することができます。

- 登録 URL を使用した登録 - Windows *(##### 29)*: ユーザーは、自分の Windows 10 デスクトップを自己登録できます。
- 一括登録 *(#####)*: MCM 管理者は、Windows プロビジョニング・ツールを使用してポリシーを構成し、BigFix WebUI を介して登録をトリガーできます。この方法では、同じ構成の多数の Windows 10 デバイスを一度に登録できます。
- Autopilot 登録 - Windows *(##### 35)*Windows Autopilot (更新予定)

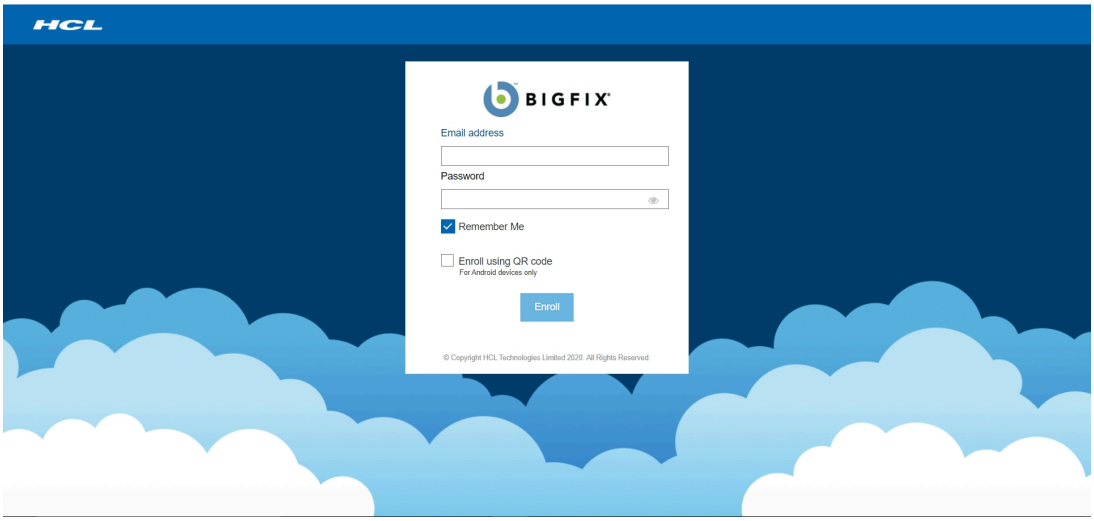
登録 URL を使用した登録 - Windows

管理者が登録 URL を共有する場合に、ユーザーが Windows 10 デバイスを MDM に登録する方法については、このセクションをお読みください。

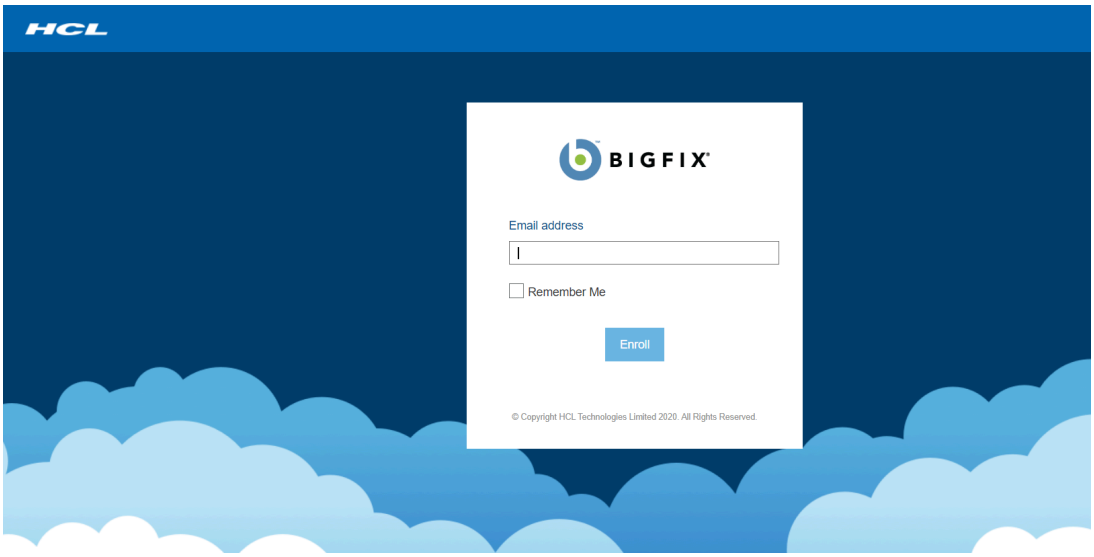
- BigFix管理者が電子メールまたはチャットを通じて共有する、MDM サーバー登録 URL を知っている必要があります。MDM サーバー登録 URL は、MDM サーバーの完全修飾ドメイン名である必要があります (https://enroll-mdm.bigfix.com など)。
- 登録 URL にログインするには、有効な Active Directory (AD) 資格情報に関連付けられた電子メール ID とパスワードが必要です。
- デバイスを正常に登録するには、Windows 10 デバイスで登録を行うユーザーが Windows 10 デバイスの管理者である必要があります。

MDM に Windows 10 デバイスを登録するには、次の手順を実行します。

1. 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 サーバー上で作成され、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。

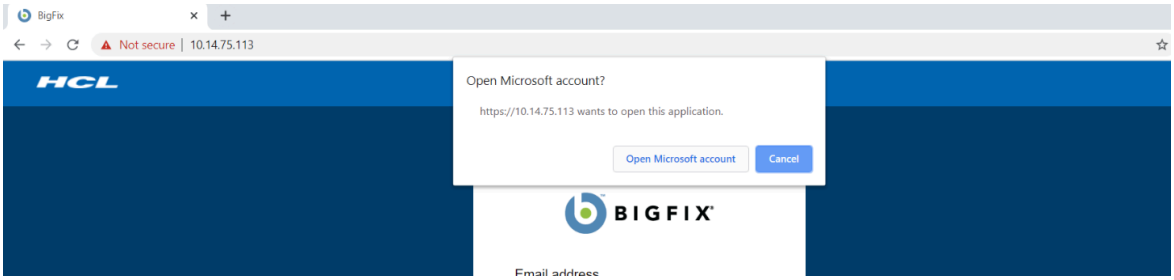


   資格情報の有効な AD セットに関連付けられた電子メール・アドレスとパスワードを入力し、**「登録」**をクリックします。ppkg ファイルがダウンロードされ、登録プロセスが開始されます。
   - 一括登録オプションが FALSE に設定されている場合は、次の画面が表示されます。

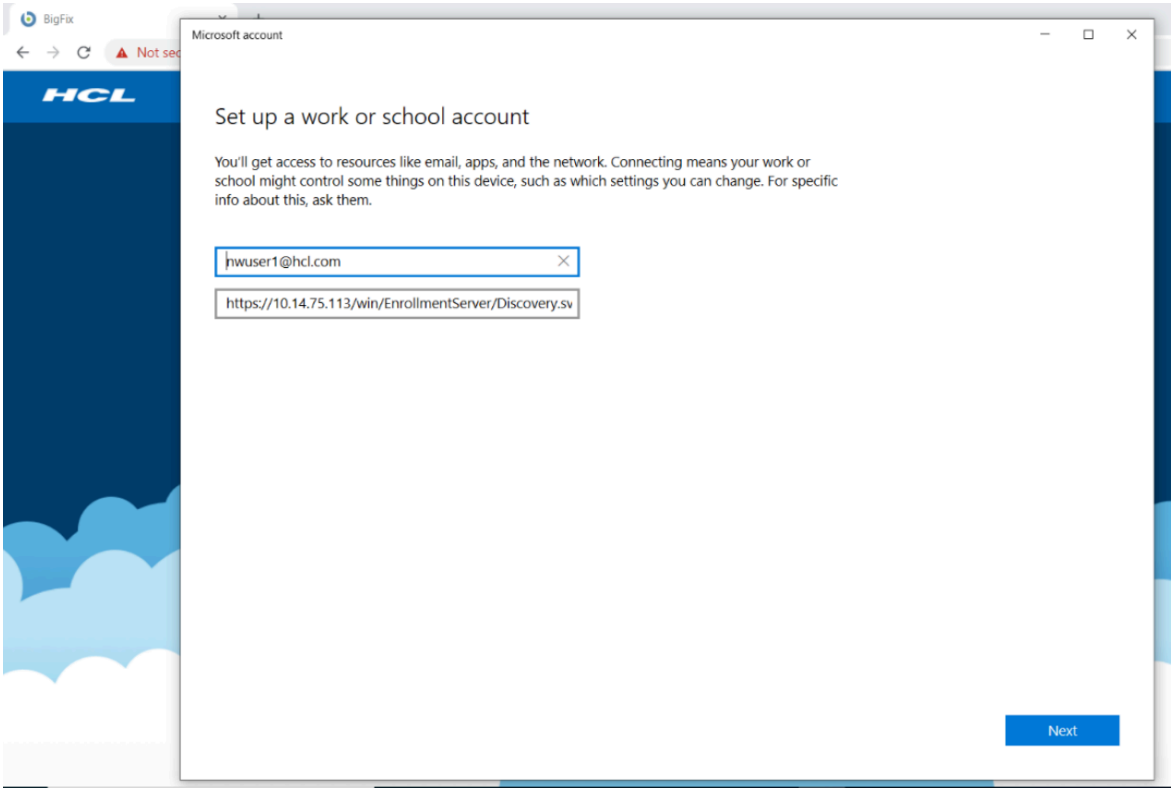


資格情報の有効な AD セットに関連付けられた電子メール・アドレスを入力し、**「登録」**をクリックします。登録プロセスが開始されます。

2. ポップアップ・ウィンドウが開き、Microsoft アカウントを開くよう要求されたら**「Microsoft アカウントを開く」**をクリックします。

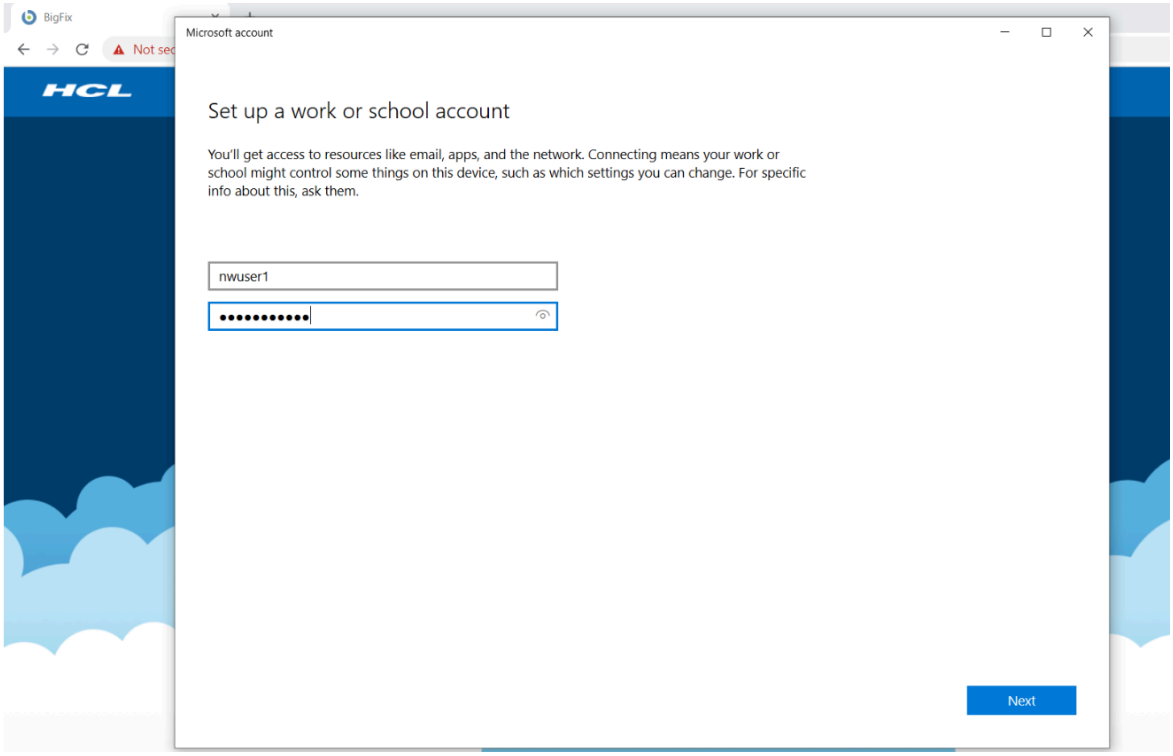


3. 次の画面で、資格情報の有効な AD 資格情報セットに関連付けられている電子メール・アドレスを入力します。MDM 登録サーバーの URL は既に事前に構成されている必要があり、変更する必要はありません。



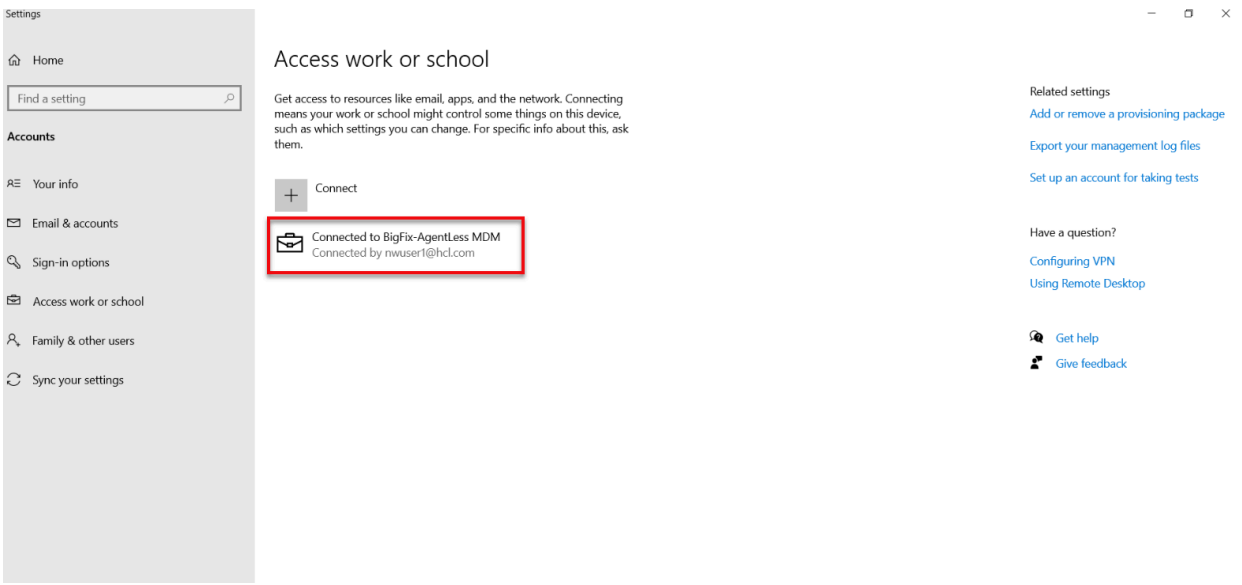
4. **「次へ」** をクリックします。
5. 次の画面で、以下の情報を入力します。
    - ユーザー名または電子メール ID – このフィールドはオプションで、空にすることができます。
    - パスワード – このフィールドは必須です。

    注: MDM 環境で LDAP がオフになっている場合は、デバイスを登録する任意の値を入力します。



6. **「次へ」** をクリックします。

認証が成功すると、デバイスは登録されます。MDM 登録ステータスを確認するには、**「設定」**>**「職場または学校にアクセス」**に移動します。デバイスが MDM に接続されていることを確認できます。



ppkg ファイルを使用して登録した場合は、「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」に移動して、登録されたデバイスの ppkg ファイルの名前を表示できます。ここで構成したプロビジョニング・パッケージを確認できます。

今後このデバイスを再び一括登録する必要がある場合は、このプロビジョニング・パッケージも削除し、「設定」>「アカウント」>「職場または学校にアクセス」の MDM プロファイルを接続解除する必要があります。その後、Windows 10 登録アクションを WebUI から開始することができます。

一括登録 - Windows

一括登録は、膨大な数の Windows 10 デバイスを BigFix MDM サーバーにセットアップして登録するための効率的な方法です。

Windows 10 デバイスの一括登録の詳細については、「一括登録 (#####　　)」を参照してください。

一括登録の主な利点は次のとおりです。

- 大規模登録 – この登録方法を使用すると、膨大な数の Windows 10 デバイスを効率的に登録できます。
- ワンタイム構成 – 管理者は、Windows プロビジョニング・パッケージ (.ppkg) を 1 回だけ構成するだけで済みます。その後、多数のデバイスに同じ設定を簡単に適用できます。

  注: プロビジョニング・パッケージ (.ppkg) は、構成設定のコレクションのコンテナーです。詳細については、「Windows 10 のプロビジョニング・パッケージ (#####)」を参照してください。

  また、ユーザーが BigFix を自動的にインストールし、カスタム MSI をインストールし、デフォルトの Windows 制限ポリシーを構成できるようにするデフォルトの Windows プロファイルを構成することもできます。

Windows 10 デバイスを一括登録する方法については、「一括登録 - Windows 10 (#####)」を参照してください。

Autopilot 登録 - Windows

BigFix 10 の MCM は、Windows Autopilot 登録をサポートしています。

Windows Autopilot とは

Windows Autopilot は、新しいまたは工場出荷時の Windows 10 デバイスを設定して事前に構成するのに役立つテクノロジーのコレクションです。このソリューションは、管理するインフラストラクチャーがほとんどないデバイスを、簡単かつシンプルなプロセスで、登録および管理するのに役立ちます。エンド・ユーザーが必要とする操作は、ネットワークに接続して資格情報を確認する操作だけです。それ以上のすべてが自動化されています。また、Windows Autopilot を使用して、デバイスのリセット、再利用、および回復を行うこともできます。

Windows Autopilot 登録の詳細については、Windows Autopilot (#####) の Windows 公式ドキュメントを参照してください。

動作説明

管理者は、Azure Active Directory (Azure AD) で Autopilot の設定を構成します。Windows Autopilot に登録するように構成されたデバイスは、最初の起動時に BigFix MDM に自動的に登録されます。デバイスは、適用するデフォルトの Windows プロファイルを自動的に持つ構成が可能です。デフォルトの Windows プロファイルは、BigFix と会社が選択したその他のアプリケーション、カスタム MSI を自動的にインストールし、デフォルトの Windows 制限ポリシーを設定するように構成できます。

構成ワークフロー

管理者は、アクティブな Azure AD Premium ライセンス (#####)を使用して Azure ポータル (#####)にサインインし、BigFix MDM サーバー、Autopilot グループ、デプロイメント・プロファイル、デバイスを構成し、Windows Autopilot を使用してユーザーをデバイスの登録に割り当てる必要があります。Azure AD を使用して Windows Autopilot 設定を構成する方法の詳細については、『自動操縦構成ガイド (#####)』を参照してください。

Autopilot 登録を簡単に構成するには、次の手順を実行します。

1. Azure AD で BigFix MDM アプリケーションを構成します。
2. Autopilot ユーザーとデバイス・グループを作成します。これにより、作成したグループにデバイスを割り当て、グループごとにデバイスを管理できます。
3. デフォルトのデプロイメント・プロファイルを構成します。デフォルトのデプロイメント・プロファイルは、Microsoft Azure AD (#####) または WebUI を使用して (#####)構成できます。Autopilot 登録によってデバイスが登録されると、構成済みのプロファイルがデフォルトで適用されます。
4. デバイス ID を `.csv` ファイルに収め、Autopilot デバイスの構成をアップロードしてユーザーを割り当てます。
5. Windows 10 Autopilot サービス利用条件の構成 (#####)。これにより、会社のロゴと利用規約を追加して、エンド・ユーザー契約画面をカスタマイズできます。

構成が完了すると、ユーザーがマシンをオンにし、インターネットに接続し、割り当てられたユーザーのパスワードを入力すると、登録プロセスが開始されます。

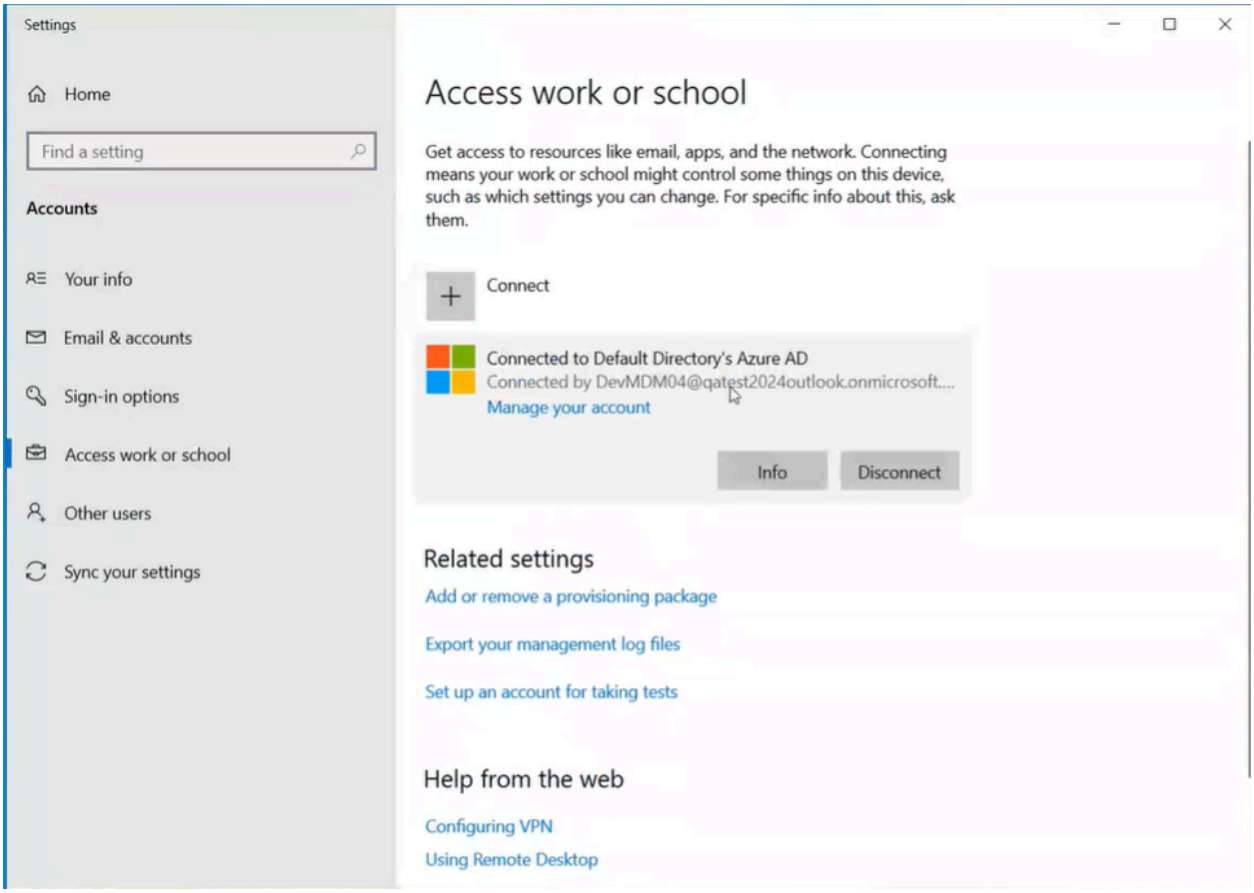
登録プロセス

Autopilot 登録プロセスは、デバイスの最初の電源投入時、または工場出荷時設定へのリセット後の電源投入時に開始されます。

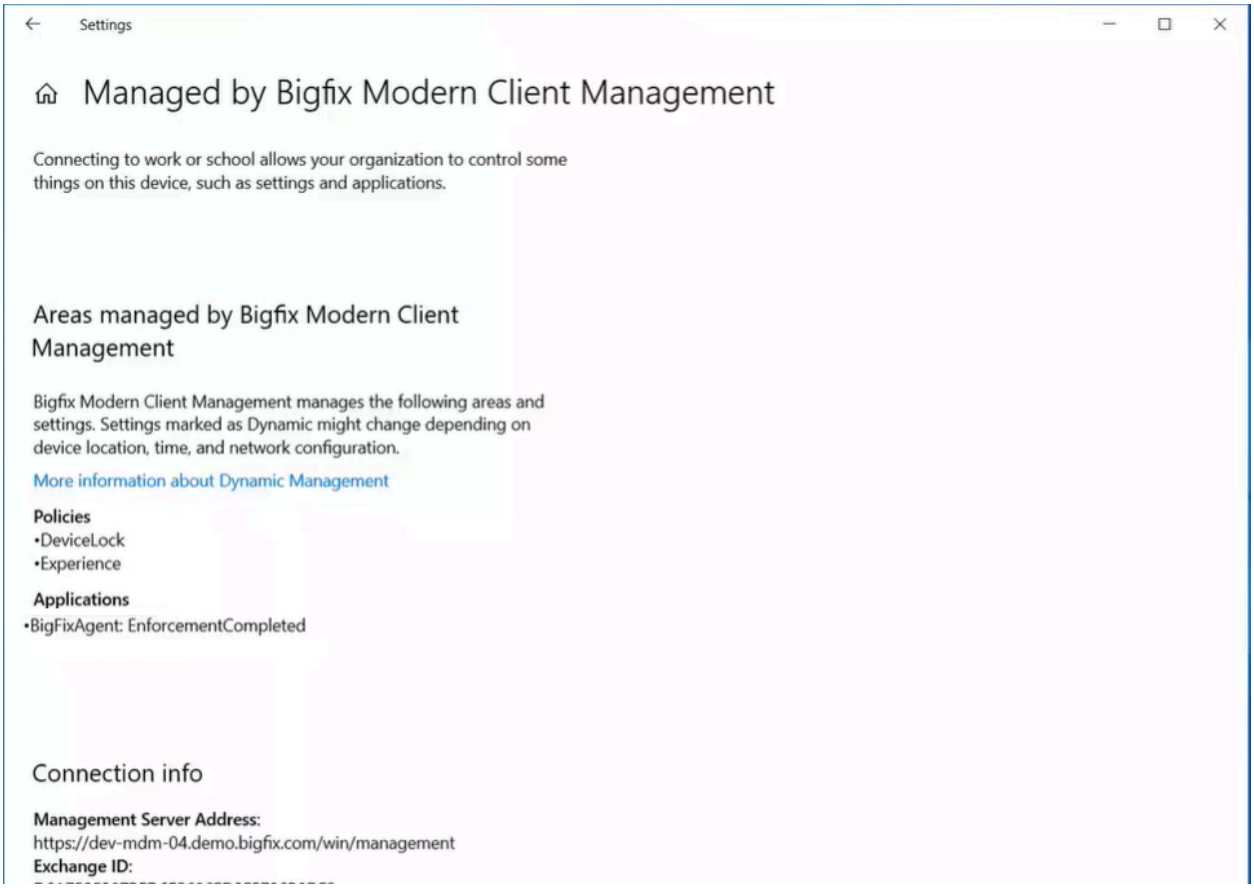
登録プロセスを開始するには、次の手順を実行します。

1. MDM サーバーに関連付けられている Windows 10 デバイスを開きます。インターネットに接続します。Azure AD で設定されているパスワードを入力します。パスワードを更新します。
2. 「エンド・ユーザーのご使用条件」ページが表示されます。確認後にご使用条件のチェック・ボックスをオンにし、**「同意する」**をクリックします。Autopilot 登録プロセスが開始されます。

登録が完了したら、**「設定」 > 「職場または学校にアクセス」**に移動して MDM サーバーの詳細を確認します。

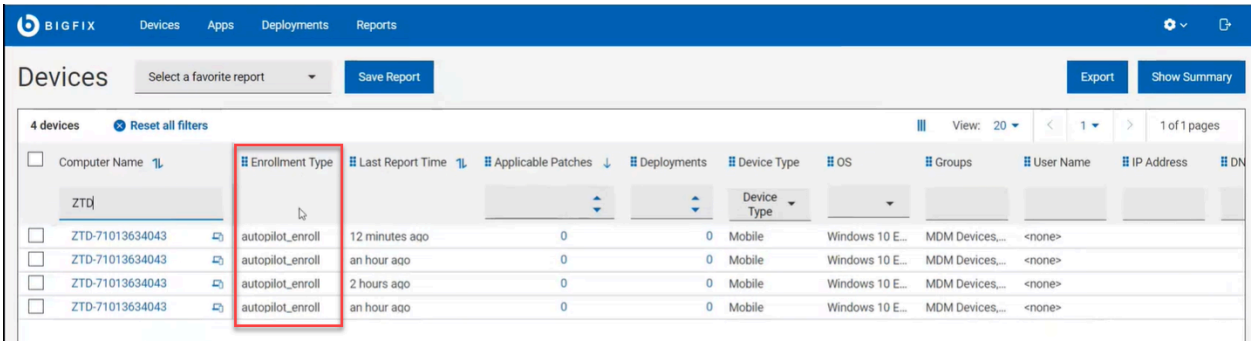


「情報」をクリックして、ポリシーとアプリケーションの詳細を確認します。

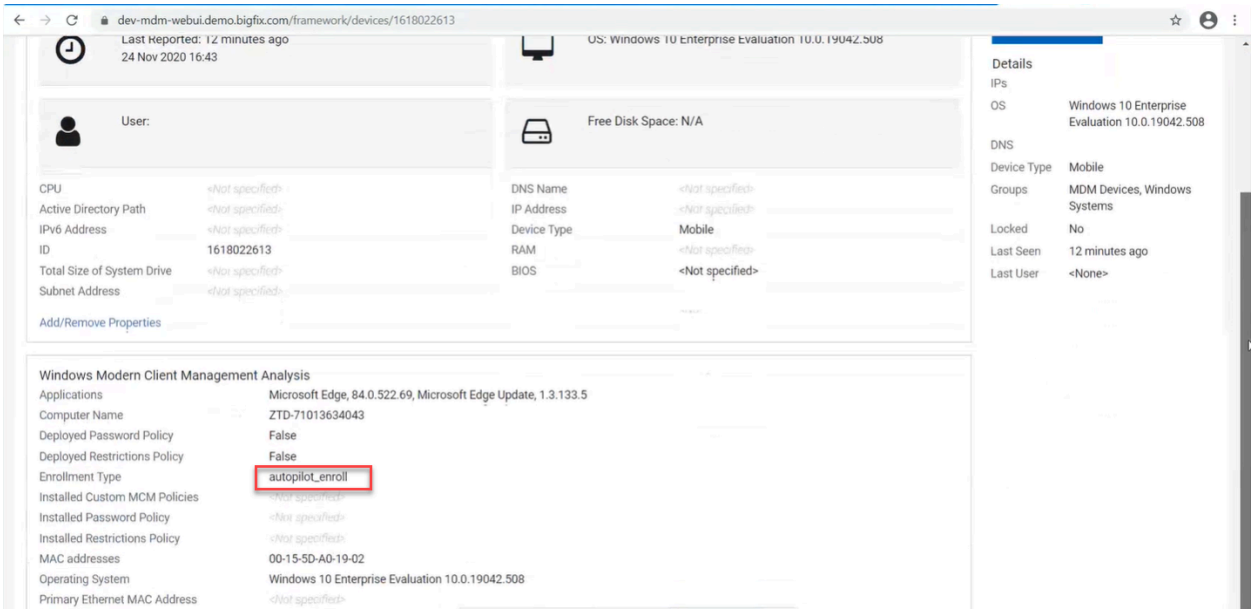


WebUI を使用した管理

登録されたデバイスは WebUI を通じて管理できます。WebUI デバイスの一覧では、登録の種類が autopilot_enroll として表示されます。



デバイスのドキュメントでは、登録の種類が autopilot_enroll として表示されます。



BigFix MDM をさらに管理する方法については、次を参照してください。 MDM デバイスの管理 *(#####)*

⚠ **警告:** Autopilot 登録済み Windows 10 デバイスを登録を解除 *(#####)*すると、職場または学校のアカウントが削除され、デバイスから AD ユーザーが切断されます。デバイスの登録を解除した後、管理者は、既存のローカル・オペレーター・アカウントがない限り、デバイスに再ログインできません。カスタム・ローカル・オペレーター・アカウントを作成する方法については、「https://docs.microsoft.com/en-us/windows/client-management/mdm/accounts-csp *(#####)*」を参照してください。

Apple デバイスの登録

次の方法で、Apple デバイスを BigFix MDM に登録することができます。

- 登録 URL を使用した登録 - macOS *(##### 40)*: ユーザーは、登録 URL を使用して Apple デバイスを登録できます。
- Apple 自動デバイス登録 *(#####)*: 管理者は、組織が Apple または認定再販業者を通じて購入して従業員に提供する、すぐに使用できる Apple デバイスの登録を構成および自動化できます。

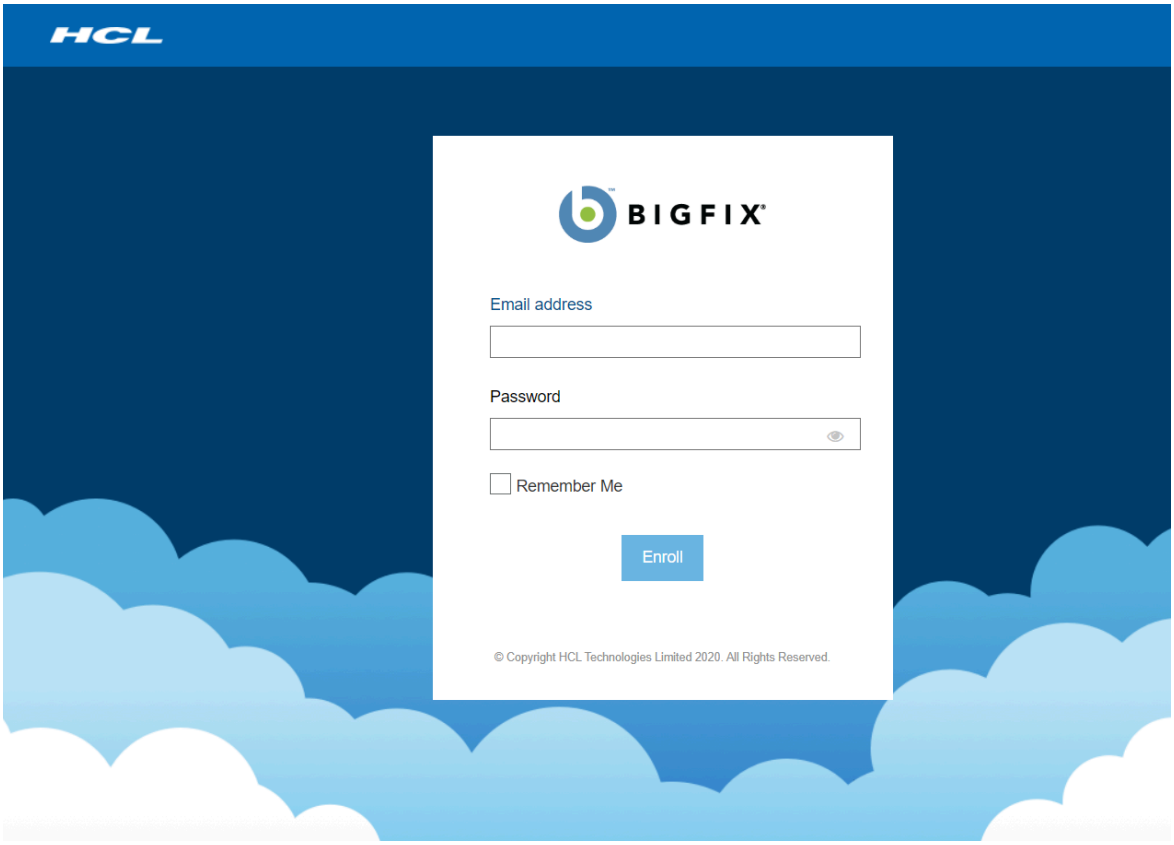
登録 URL を使用した登録 - macOS

管理者が登録 URL を共有する場合に、ユーザーが macOS デバイスを MDM に登録する方法については、このセクションをお読みください。

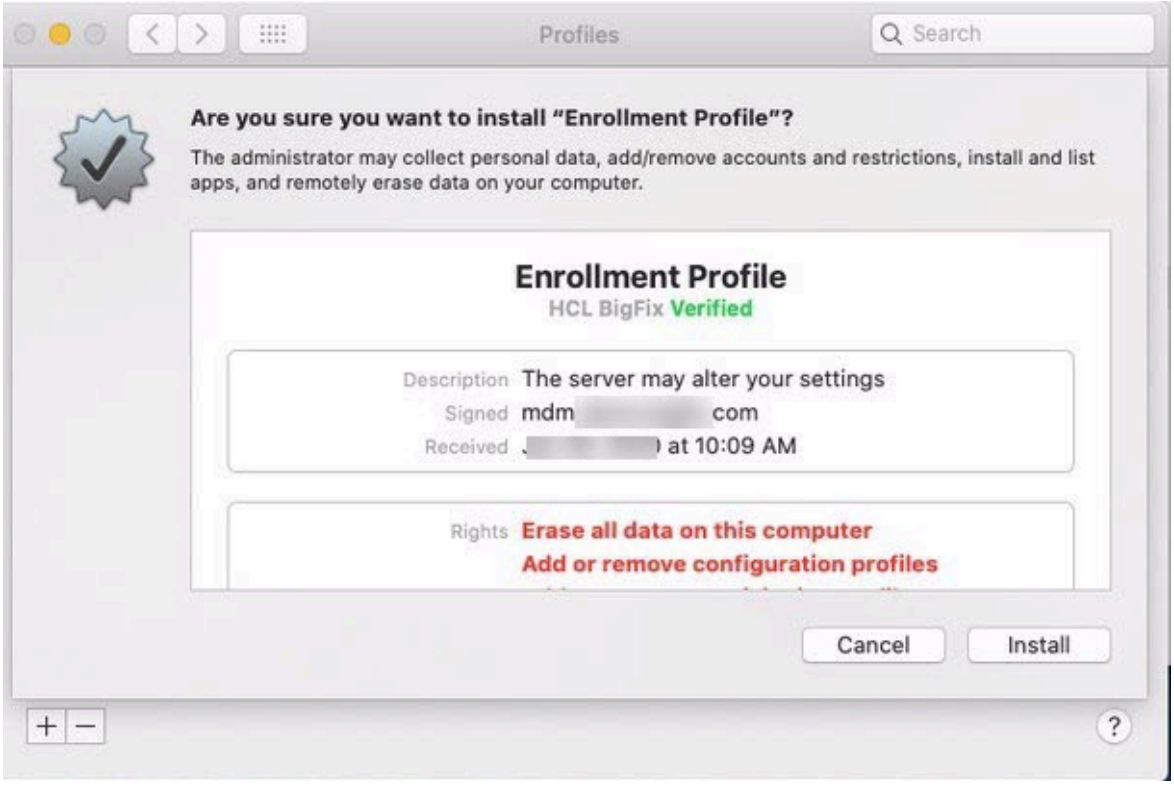
ユーザーは、BigFix 管理者が共有する登録 URL にアクセスする必要があります (メールまたはチャットを使用)。この登録 URL は、MDM サーバーの FQDN です (例えば、https://enroll-mdm.bigfix.com)。この登録ポータルで認証後、ユーザーは管理者としてデバイスに登録プロファイルをインストールする必要があります。

macOS デバイスを MDM に登録するには、以下の手順に従います。

1. macOS デバイスで、Web ブラウザーを起動し、MDM サーバー URL に移動します。



2. MDM サーバーのセットアップ時に構成された Active Directory デプロイメントに関連付けられた有効な電子メール・アドレスとパスワードを入力します。
3. **「登録」**をクリックして、Mac 登録プロファイルをダウンロードします。
4. OSX はこの登録プロファイルを開き、登録しようとしている MDM デプロイメントに関する情報をユーザーに表示します。問題がないように見える場合は、**「インストール」**をクリックして MDM にデバイスを登録します。



Apple 自動デバイス登録

BigFix 10 用 MCM 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 BigFix MCM に自動的に登録できるようにすることができます。

プログラムの資格を得る方法や Apple Business Manager と Apple School Manager 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 BigFix MCM サーバーの構成方法については、『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 macOS 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。Mac 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 *(#####)*できます。

第 11 章. 既知の問題

ユーザーが登録 URL を使用して Windows クライアントを MDM サーバーに登録しようとすると、デフォルトのアプリケーションをインストールするコマンドは成功応答 (200) を返しますが、アプリケーションはインストールされません。

WebUI で一括登録 `.ppkg` パッケージを再度作成する必要がある場合は、WebUI から一括登録パッケージの作成アクションを開始する前に、次のクリーンアップ手順を実行します。

- Windows 10 エンドポイントの `MCMPPKG` ディレクトリーをクリアします。
- BES サーバー上の uploadManager タスクに関連するすべてのディレクトリーをクリアします (コンピュータ ID に依存)。
- `wwwrootbes` の MCM ディレクトリーをクリアします。
- MDM サーバーの `/var/opt/BESUEM/packages/bigfix-mcm-enroll.ppkg` をクリアします。

第 12 章. トラブルシューティング

この章は、BigFix MCM の使用中に発生する問題をユーザーが解決する際に役立ちます。

ログ

MCM コンポーネントがログ・ファイルを生成し、問題をトラブルシューティングする場合に追加情報を入手できます。

ログ・ファイルの場所

次の表は、Windows および Linux システムに格納されているさまざまな MCM ログの場所を示しています。

Component	Windows	Linux
Plugin Portal log (Configurable through _BESPluginPortal_HTTPServer_LogFilePath)	`C:\Program Files (x86)\BigFix Enterprise\BES Plugin Portal\BESPluginPortal.log`	`/var/log/BESPluginPortal.log`
Windows MDM Plugin	`C:\Program Files (x86)\BigFix Enterprise\BES Plugin Portal\Plugins\WindowsMDMPlugin\Logs`	`/var/opt/BESPluginPortal/Plugins/WindowsMDMPlugin/Logs`
macOS MDM Plugin	`C:\Program Files (x86)\BigFix Enterprise\BES Plugin`	`/var/opt/BESPluginPortal/Plugins/MacMDMPlugin/Logs`

Component	Windows	Linux
	`Portal\Plugins\MacMDMPlugin\Logs`	
Windows MDM Server	N/A	`/var/opt/BESUEM/windows/logs/windowsmdm.log`
macOS MDM Server	N/A	`/var/opt/BESUEM/mac/logs/micromdm.log`
macOS MDM Gateway	N/A	`/var/opt/BESUEM/mac/logs/mdmgateway.log`
macOS MDM Webhook	N/A	`/var/opt/BESUEM/mac/logs/mdmwebhook.log`
WebUI log (Configurable through the server setting _WebUI_Logging_LogPath)	`c:\Program Files (x86)\BigFix Enterprise\BESWebUI\WebUI\logs\`	`/var/opt/BESWebUI/WebUI/logs/`

クライアント設定 - プラグインまたはプラグイン・ポータルの詳細ログ

パラメーター	説明
`_BESPluginPortal_Log_Verbose`	値が 0 の場合はプラグイン・ポータルの詳細を Off に設定します (クリティカル・メッセージのみが記録されます)。値が 1 の場合は、この値を On に設定します (ログ記録を有効にします)。デフォルト値は 0 です。
`_BESPluginPortal_Log_EnabledLogs`	プラグイン・ポータルの詳細が有効になっている場合、プラグイン・ポータル・メッセージ・タイプの構成を設定します。使用可能な値は、以下のとおりで

パラメーター	説明

	す。すべて、クリティカル、デバッグ、タイミング、イベント。セミコロンで区切られた値を追加できます。
	例:
	`_BESPluginPortal_Log_Verbose = 1`
	`_BESPluginPortal_Log_EnabledLogs = events;timing`
	デフォルトのメッセージ・タイプは「すべて」です。
	注: これは、プラグイン・ポータルのパフォーマンスに悪影響を及ぼす可能性があります。

`_WindowsMDMPlugin_LogVerbose`	値が 1 の場合は Windows MDM プラグインの詳細を On に設定し、値が 0 の場合は Off に設定します。デフォルト値は 0 です。
`_AppleMDMPlugin_LogVerbose`	値が 1 の場合は Apple プラグインの詳細を On に設定し、値が 0 の場合は Off に設定します。デフォルト値は 0 です。

Logrotate

Logrotate は、ログ・ファイルの自動ローテーションと圧縮を処理して、使用可能なディスク・スペースを管理します。1 時間ごとに 0 分にログ・ファイルがローテーションされ、次のコンテナで cron ジョブを実行して、古いログ・ファイルが圧縮され、バックアップとして保持されます。

- windowsmdm
- applemdm

- rabbitmq
- openresty

バックアップ・ファイル名の形式は 、<Filename.log>_<YYYY-MM-DD>_<HH-mm-ss>.gz です。たとえば、 `mdmgateway.log_2020-06-03_07-13-00.gz`

ログは次の条件でローテーションされ、次のログの場所にバックアップされます。

Container	Log location	Max File size	Rotate Count	Scheduled cron JOB running
For all containers	Container's internal path	10 MB	10	every hour 0th minute
For macmdm log	/var/opt/BESUEM/mac/logs	50 MB	10	every hour 0th minute
For windowsmdm log	/var/opt/BESUEM/windows/logs	50 MB	10	every hour 0th minute
For openresty log	/var/opt/BESUEM/openresty/logs	50 MB	10	every hour 0th minute

注: ログ・ファイルのサイズが 50 MB 未満の場合、logrotate cron ジョブを実行しても、新しいログ・ファイルは作成されません。

MCM デバッグ・ロギング

デバッグ・ログは、ログのロギング・レベルが拡張されているため、問題のトラブルシューティングに役立ちます。BESUEM サイトで、TROUBLESHOOTING としてマークされている Fixlet を探して、異なる MCM コンポーネントのログを有効にします。コンポーネントが使用可能な場合は、これらのコンポーネントが関連します。

エラー・コード

以下に、一般的に発生するエラー・メッセージと関連情報を示します。

Windows エンドポイント登録エラー・コード

エラー・コード	説明	原因
0x80190191	無許可のユーザー	ユーザーは許可されていません。
0x80190190	サーバーは転送要求を処理できませんでした。	リモート・ファイル名の構文が無効です。
0x801901F4	アプリが開かないようにしたり、開いた後すぐに閉じるように強制します。	Windows レジストリーでシステム設定が正しく構成されていないか、または不規則なエントリーです。
0x8600023	既にこのパッケージをインポート済みです	この PPKG のインポートは以前に試行されており、アクションは失敗しました
0x80180026	デバイスは外部管理されています	これは、デバイスがプロビジョニング・モードでロックされている場合に発生します。
0x80192ee7	ネットワーク名が解決されていません	DNS が使用できないか、またはコンピューターにインターネット・アクセスがありません。
0x8004002	ファイルが見つかりません	プロビジョニング・パッケージ・ファイルを読み取ることができません。
0x8004005	アクセスが拒否されました	これは、UAC が無効になっている場合、または MDM 登録プロンプトでだれかが 「いいえ」をクリックした場合に発生します。

エラー・コードの包括的な一覧については、「https://docs.microsoft.com/en-us/windows/win32/mdmreg/mdm-registration-constants (#####　　)」を参照してください。

RHEL8 の Docker CE+ Docker 構成のインストール

RHEL8 はデフォルトでは Docker CE+ をサポートしていません。次の情報は、RHEL8 に互換性のある Docker CE+ をインストールするための回避策を提供します。

RHEL 8 に Docker CE+Docker 構成をインストールする

RHEL 8 に Docker CE+Docker 構成をインストールするには

1. 次のコマンドを実行して、外部リポジトリーを追加します。

```
sudo dnf config-manager
 --add-repo=https://download.docker.com/linux/centos/docker-ce.repo
```

   a. リポジトリーが有効になっているかどうかを確認します。これを行うには、有効なすべてのリポジトリーに関する詳細情報を返す次のコマンドを実行します。

```
sudo dnf repolist -v
```

2. --nobest オプションを指定して docker-ce をインストールします。このオプションを使用すると、満たすことができる依存関係を持つ最初のバージョンの `docker-ce` が「フォールバック」バージョンとして選択されます。

```
sudo dnf install --nobest docker-ce
```

3. 利用可能な最新の containerd.io パッケージを手動でインストールする

```
sudo dnf install
 https://download.docker.com/linux/centos/7/x86_64/stable/Packages/con
tainerd.io-1.2.6-3.3.el7.x86_64.rpm
```

4. 最新バージョンの docker-ce をインストールします。

```
sudo dnf install docker-ce
```

5. docker デーモンを起動して有効にします

```
sudo systemctl enable --now docker
```

   a. 次のコマンドを実行して、デーモンがアクティブかどうかを確認します。

```
systemctl is-active docker
```

6. docker-compose をグローバルでインストールします。
   a. プロジェクトの GitHub ページからバイナリー・ファイルをダウンロードします。

```
curl -L
 "https://github.com/docker/compose/releases/download/1.23.2/dock
er-compose-$(uname -s)-$(uname -m)" -o docker-compose
```

   b. バイナリー・ファイルをダウンロードした後、それを `/usr/local/bin` フォルダーに移動し、実行可能にします。

```
sudo mv docker-compose /usr/local/bin && sudo chmod
 +x /usr/local/bin/docker-compose
sudo ln -s /usr/local/bin/docker-compose /usr/bin/docker-compose
```

詳しくは、「https://linuxconfig.org/how-to-install-docker-in-rhel-8 (#####　　)」を参照してください。

このインストール後、Docker CE コンテナー接続の問題が発生する可能性があります。この問題を解決するには、以下の手順を実行します。

Docker CE コンテナー接続の問題を解決します。

Docker CE コンテナー接続の問題を解決するには、次の手順を実行します。

1. どのインターフェース Docker が使用されているかを確認します。例えば、「docker0」です。

```
ip link show
```

2. 使用可能なファイアウォール・ゾーンを確認します。例えば、「パブリック」です。

```
sudo firewall-cmd --get-active-zones
```

3. Docker インターフェースがバインドされているゾーンを確認します。通常、Docker インターフェースはまだゾーンにバインドされていません。

```
sudo firewall-cmd --get-zone-of-interface=docker0
```

4. 「パブリック」ゾーンに「docker0」インターフェースを追加します。変更は、ファイアウォールが再ロードされた後にのみ表示されます。

```
sudo nmcli connection modify docker0 connection.zone public
```

5. マスカレードにより、Docker の入力と出力が可能になります。

```
sudo firewall-cmd --zone=public --add-masquerade --permanent
```

6. ファイアウォールを再ロードします

```
sudo firewall-cmd --reload
```

7. dockerd を再起動します

```
sudo systemctl restart docker
```

LDAPS 接続のトラブルシューティング

条件

LDAP 接続失敗。

原因

MDM サーバーを構成するには、LDAP 資格情報を入力する必要があります。間違った値または誤った形式で値を入力した場合、値は検証されません。ただし、Fixlet アクションは正常に完了し、接続の問題が発生します。

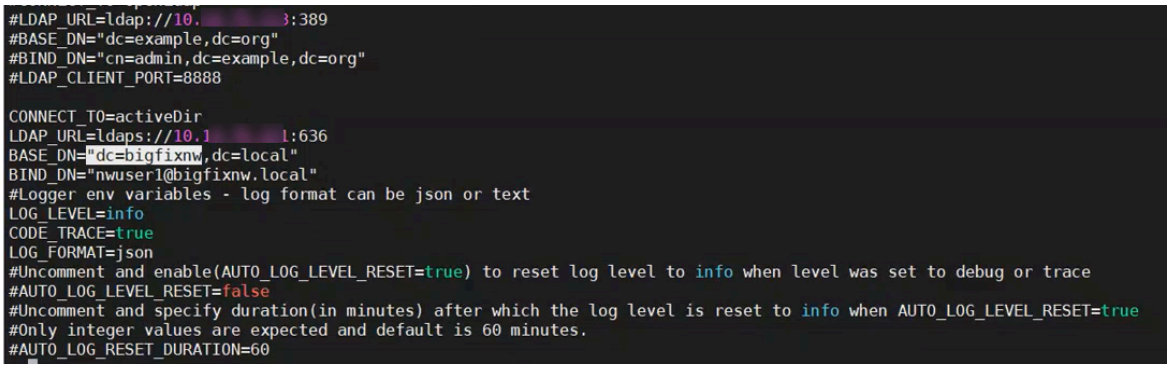
解決策

コマンド・ライン・ユーティリティー BESmdmldaputil を使用すると、LDAP パラメーター、電子メール、およびユーザ認証を検証して、LDAP 接続の問題をトラブルシューティングできます。

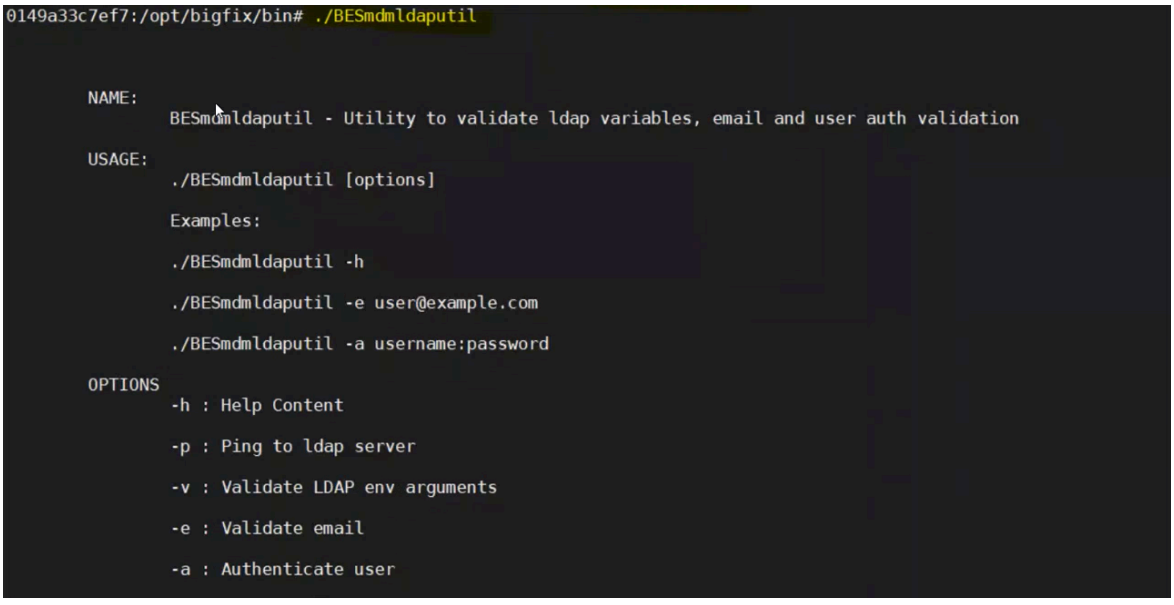
注: `.env` ファイル内の LDAP パラメーターを変更した場合、変更を有効にするには、openresty サービスを再起動する必要があります。

このユーティリティーは Linux MDM サーバー上の `/opt/bigfix/bin#` にあります。このユーティリティーを実行するには、`/opt/bigfix/bin#` に移動して ./BESmdmldaputil を実行します。

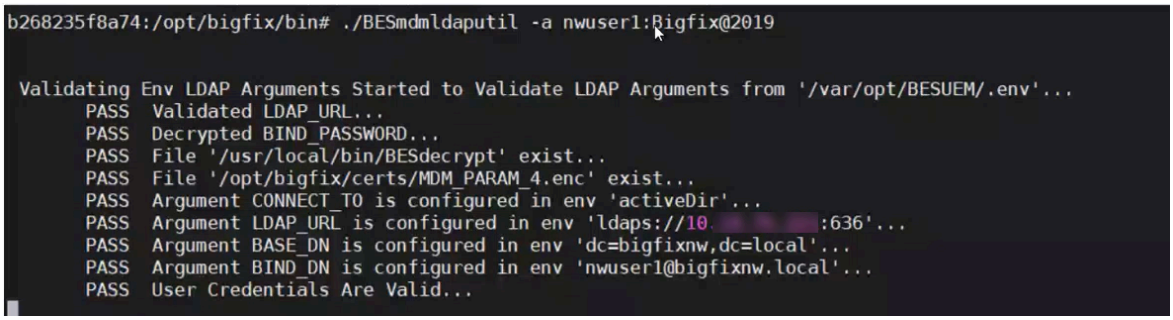
- このユーティリティーは、MDM サーバーのインストールまたはメンテナンス Fixlet を通じて提供され、次の図に示すように `/var/opt/BESUEM/.env` ディレクトリーに格納されている LDAP パラメーターを検証します:



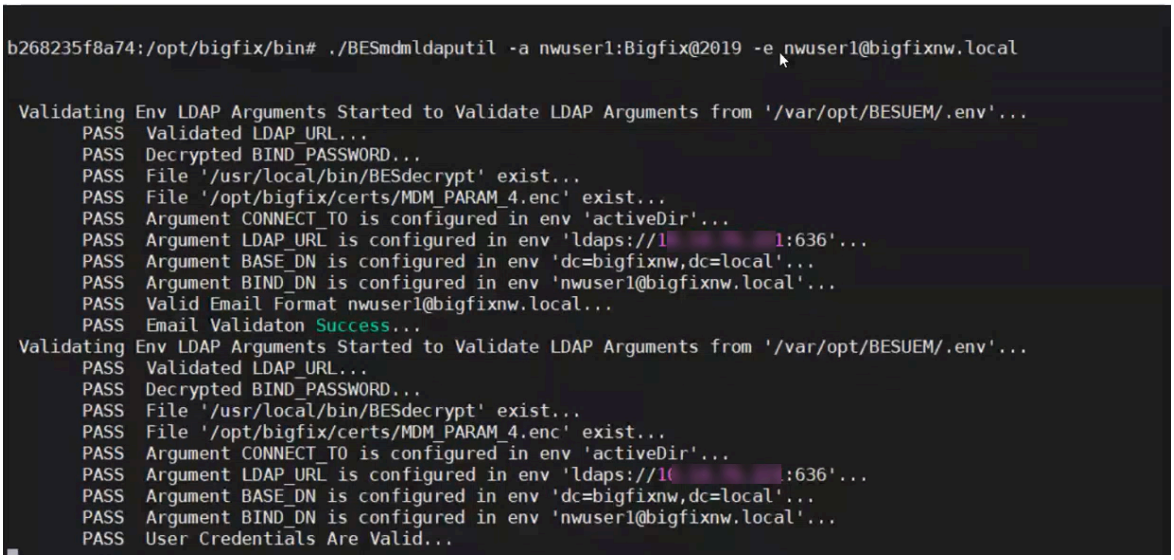
- 次の図は、このユーティリティーで使用できるオプションと、それらのオプションの使用方法の例を示しています。



- 次の図は、オプション -a を使用して特定のユーザーを認証する場合の検証メッセージを示しています。



- また、複数のオプションを組み合わせて目的の結果を得ることもできます。次の図は、指定された値のオプション -a および -e の結果を示しています。



これにより、構成済みの接続が機能しているかどうか、また動作していない場合は、具体的に何を探す必要があるのかを理解できます。

DEP のトラブルシューティング

このセクションでは、DEP 登録のトラブルシューティング情報を示します。

デバイスからプロファイルへの割り当て

MicroMDM は、すべての DEP デバイス情報を `/opt/bigfix/config/dep-devices.json` ファイルに書き込みます。このファイルは約 30 分ごとに更新されます。プロファイルの状態と UUID を他のデバイス情報と共に確認できます。現在のデバイスから登録されているすべてのデバイスのプロファイルへの割り当てを、このファイルから見つけることができます。

`dep-devices.json` ファイルのサンプル・コンテンツ


```
[
   {
      "serial_number":"************",
      "model":"iPad",
      "description":"IPAD WI-FI 32GB SPACE GRAY-USA",
      "color":"SPACE GRAY",
      "asset_tag":"",
      "profile_status":"assigned",
      "profile_uuid":"180E3526801006EB204EDC9C3A4C3141",
      "DEPProfileAssignedDate":"2020-10-06T21:07:54Z"
   },
   {
      "serial_number":"************",
      "model":"MacBook Pro 15\"",
      "description":"MBP 15.4/16GB",
      "color":"SILVER",
      "asset_tag":"",
      "profile_status":"pushed",
      "profile_uuid":"180E3526801006EB204EDC9C3A4C3141",
      "DEPProfileAssignedDate":"2020-10-06T21:07:54Z"
   },
   {
      "serial_number":"************",
      "model":"iPhone XR",
```

```
      "description":"IPHONE XR BLACK 64GB VZW-USA",
      "color":"BLACK",
      "asset_tag":"",
      "profile_status":"assigned",
      "profile_uuid":"180E3526801006EB204EDC9C3A4C3141",
      "DEPProfileAssignedDate":"2020-10-06T21:07:54Z"
   }
]
```


MacOS MCM コンポーネントのログとメトリックを監視する

DEP ログは `/var/log/apple-mdm.log` ファイルで使用できます。

`apple-mdm.log` ファイルのサンプル・コンテンツ


```
{

  "cursor":
 "MDowOjE2MTA2NzY3NTA3NzM6MTYxMDY4MTUxOTA5NDp0cnVlOjE2MTA2NzY3NTA3NzM",
  "file":
 "/opt/bigfix/src/github.com/micromdm/micromdm/platform/dep/sync/depsync.go
:313",
  "func": "github.com/micromdm/micromdm/platform/dep/sync.(*Watcher).Run",
  "level": "info",
  "module": "default",
  "msg": "Sync DEP devices",
  "time": "2021-01-15T04:01:58Z"
}
{
  "devices": 0,
  "fetched": "2021-01-15T02:12:30Z",
  "file":
 "/opt/bigfix/src/github.com/micromdm/micromdm/platform/dep/sync/depsync.go
:347",
```

```
  "func": "github.com/micromdm/micromdm/platform/dep/sync.(*Watcher).Run",
  "level": "info",
  "module": "default",
  "more": false,
  "msg": "DEP sync success",
  "phase": "sync",
  "time": "2021-01-15T04:01:59Z"
}
{
  "device_count": 0,
  "file":
 "/opt/bigfix/src/github.com/micromdm/micromdm/platform/device/worker.go:12
4",
  "func":
 "github.com/micromdm/micromdm/platform/device.(*Worker).updateFromDEPSync"
,
  "level": "info",
  "module": "default",
  "msg": "Updating devices from DEP",
  "time": "2021-01-15T04:02:00Z"
}
{
  "FilterUDID": null,
  "count of udids in query": 0,
  "file":
 "/opt/bigfix/src/github.com/micromdm/micromdm/platform/device/builtin/db.g
o:65",
  "func":
 "github.com/micromdm/micromdm/platform/device/builtin.(*DB).List",
  "level": "info",
  "module": "restapi",
  "msg": "List device db operation called",
```

```
  "time": "2021-01-15T04:02:00Z"
}

{
  "file":
 "/opt/bigfix/src/github.com/micromdm/micromdm/platform/dep/define_profile.
go:46",
  "func":
 "github.com/micromdm/micromdm/platform/dep.MakeDefineProfileEndpoint.func1
",
  "level": "info",
  "module": "restapi",
  "msg": "Apply dep profile request",
  "profile_name": "DEPTestProfile",
  "time": "2021-01-15T04:12:33Z"
}
{
  "file":
 "/opt/bigfix/src/github.com/micromdm/micromdm/platform/dep/define_profile.
go:51",
  "func":
 "github.com/micromdm/micromdm/platform/dep.MakeDefineProfileEndpoint.func1
",
  "level": "info",
  "module": "restapi",
  "msg": "Apply dep profile success",
  "profile_name": "DEPTestProfile",
  "profile_uuid": "EB7A65BC96583B0C77DE990633C2EAD3",
  "time": "2021-01-15T04:12:33Z"
}
{
```

```
  "file":
 "/opt/bigfix/src/github.com/micromdm/micromdm/platform/dep/sync/apply_auto
assigner.go:32",
  "func":
 "github.com/micromdm/micromdm/platform/dep/sync.MakeApplyAutoAssignerEndpo
int.func1",
  "level": "info",
  "module": "restapi",
  "msg": "Apply dep autoassigner request",
  "profile_uuid": "EB7A65BC96583B0C77DE990633C2EAD3",
  "time": "2021-01-15T04:12:33Z"
}
{
  "file":
 "/opt/bigfix/src/github.com/micromdm/micromdm/platform/dep/sync/apply_auto
assigner.go:37",
  "func":
 "github.com/micromdm/micromdm/platform/dep/sync.MakeApplyAutoAssignerEndpo
int.func1",
  "level": "info",
  "module": "restapi",
  "msg": "Apply dep autoassigner success",
  "profile_uuid": "EB7A65BC96583B0C77DE990633C2EAD3",
  "time": "2021-01-15T04:12:33Z"
}
{
  "file":
 "/opt/bigfix/src/github.com/micromdm/micromdm/platform/dep/sync/syncnow.go
:21",
  "func":
 "github.com/micromdm/micromdm/platform/dep/sync.MakeSyncNowEndpoint.func1"
,
```

```
  "level": "info",
  "module": "restapi",
  "msg": "Dep syncnow request",
  "time": "2021-01-15T04:13:01Z"
}
{
  "file":
 "/opt/bigfix/src/github.com/micromdm/micromdm/platform/dep/sync/depsync.go
:380",
  "func": "github.com/micromdm/micromdm/platform/dep/sync.(*Watcher).Run",
  "level": "info",
  "module": "default",
  "msg": "Explicit DEP sync requested",
  "time": "2021-01-15T04:13:01Z"
}
{
  "cursor":
 "MDowOjE2MTA2NzY3NTA3NzM6MTYxMDY4MzMxOTA5Mjp0cnVlOjE2MTA2NzY3NTA3NzM",
  "file":
 "/opt/bigfix/src/github.com/micromdm/micromdm/platform/dep/sync/depsync.go
:313",
  "func": "github.com/micromdm/micromdm/platform/dep/sync.(*Watcher).Run",
  "level": "info",
  "module": "default",
  "msg": "Sync DEP devices",
  "time": "2021-01-15T04:13:01Z"
}
{
  "devices": 0,
  "fetched": "2021-01-15T02:12:30Z",
```

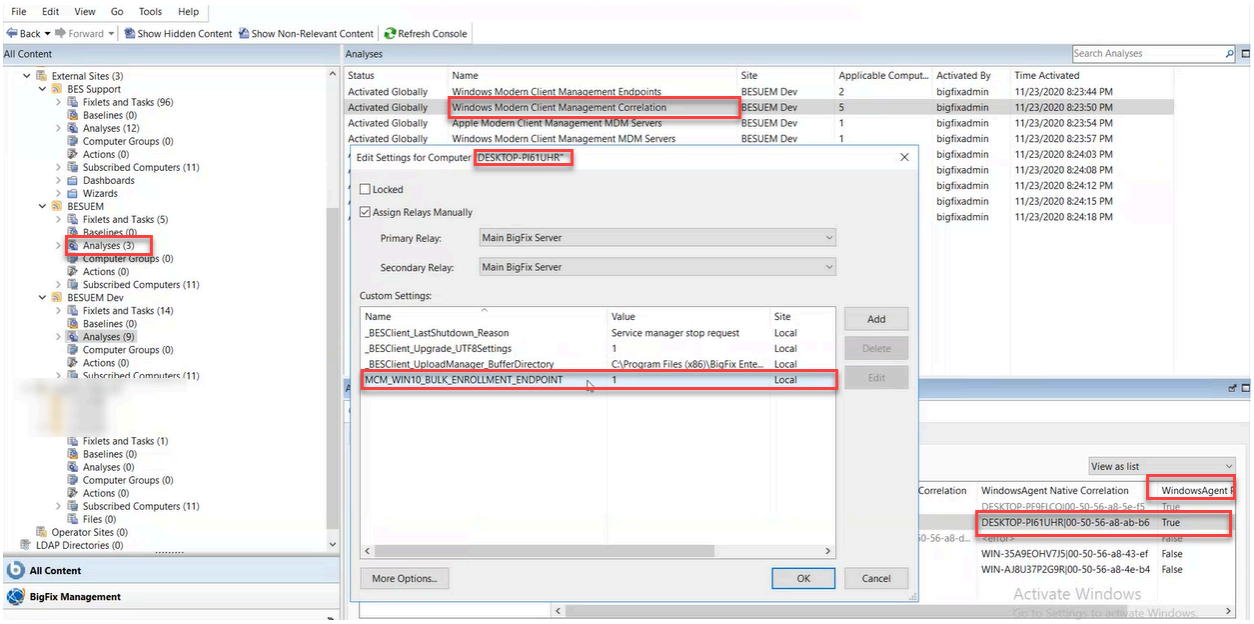
```
  "file":
 "/opt/bigfix/src/github.com/micromdm/micromdm/platform/dep/sync/depsync.go
:347",
  "func": "github.com/micromdm/micromdm/platform/dep/sync.(*Watcher).Run",
  "level": "info",
  "module": "default",
  "more": false,
  "msg": "DEP sync success",
  "phase": "sync",
  "time": "2021-01-15T04:13:01Z"
}
```


PPKG 生成ポイントが一括登録用に設定されているかどうかを確認します。

一括登録の問題をトラブルシューティングするには、対象のデバイスがプロビジョニング・パッケージ生成ポイントとして指定されているかどうかを確認します。

これを行うには、BigFix コンソールで、**「BESUEM」 > 「分析」 > 「Windows モダン・クライアント管理の相関関係」**に移動します。確認するデバイスについて、次のパラメーターの値を確認します。

- **WindowsAgent PPKG Designation** パラメーターの値が True になります。
- 指定されたデバイスを右クリックし、「コンピューター設定の編集」を選択します。クライアント設定 **MCM_BULK_ENROLL_ENDPOINT** は 1 に設定されます。


File Edit View Go Tools Help
Back Forward Show Hidden Content Show Non-Relevant Content Refresh Console
All Content
Analyses
Search Analyses
Status Name Site Applicable Comput... Activated By Time Activated
Activated Globally Windows Modern Client Management Endpoints BESUEM Dev 2 bigfixadmin 11/23/2020 8:23:44 PM
Activated Globally Windows Modern Client Management Correlation BESUEM Dev 5 bigfixadmin 11/23/2020 8:23:50 PM
Activated Globally Apple Modern Client Management MDM Servers BESUEM Dev 1 bigfixadmin 11/23/2020 8:23:54 PM
Activated Globally Windows Modern Client Management MDM Servers BESUEM Dev 1 bigfixadmin 11/23/2020 8:23:57 PM
bigfixadmin 11/23/2020 8:24:03 PM
bigfixadmin 11/23/2020 8:24:08 PM
bigfixadmin 11/23/2020 8:24:12 PM
bigfixadmin 11/23/2020 8:24:15 PM
bigfixadmin 11/23/2020 8:24:18 PM
External Sites (3)
BES Support
Fixlets and Tasks (96)
Baselines (0)
Analyses (12)
Computer Groups (0)
Actions (0)
Subscribed Computers (11)
Dashboards
Wizards
BESUEM
Fixlets and Tasks (5)
Baselines (0)
Analyses (3)
Computer Groups (0)
Actions (0)
Subscribed Computers (11)
BESUEM Dev
Fixlets and Tasks (14)
Baselines (0)
Analyses (9)
Computer Groups (0)
Actions (0)
Fixlets and Tasks (1)
Baselines (0)
Analyses (0)
Computer Groups (0)
Actions (0)
Subscribed Computers (11)
Files (0)
Operator Sites (0)
LDAP Directories (0)
All Content
BigFix Management
Edit Settings for Computer DESKTOP-PI61UHR"
Locked
Assign Relays Manually
Primary Relay: Main BigFix Server
Secondary Relay: Main BigFix Server
Custom Settings:
Name Value Site
_BESClient_LastShutdown_Reason Service manager stop request Local
_BESClient_Upgrade_UTF8Settings 1 Local
_BESClient_UploadManager_BufferDirectory C:\Program Files (x86)\BigFix Ente... Local
MCM_WIN10_BULK_ENROLLMENT_ENDPOINT 1 Local
Add
Delete
Edit
More Options...
OK
Cancel
View as list
Correlation WindowsAgent Native Correlation WindowsAgent
DESKTOP-PI61UHR|00-50-56-a8-ab-b6 True
WIN-35A9EOHV7J5|00-50-56-a8-43-ef False
WIN-AJ8U37P2G9R|00-50-56-a8-4e-b4 False
Activate Windows

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 チャンネル (#####　　)
- BigFix フォーラム (#####　　)

付録 B. 用語集

この用語集は、BigFix の最新のクライアント管理ソフトウェアおよび製品の用語と定義を記載しています。

この用語集では次の相互参照が使用されています。

- 「*###*」は、非優先用語の場合は優先用語を、省略語の場合は省略していない形式を示すものです。
- 「*###*」は、関連する用語または対比される用語を示します。

A *(##### 64)* B *(##### 65)* C *(##### 66)* D *(##### 68)* E *(##### 70)* F *(##### 70)* G *(##### 70)* L *(##### 71)* 月 *(##### 71)* N *(##### 72)* O *(##### 73)* P *(##### 73)* R *(##### 73)* 日 *(##### 74)* T *(##### 76)* U *(##### 77)* V *(##### 77)* W *(##### 78)*

A

action

1. 「Fixlet *(##### 70)*」を参照。
2. 操作タスクや管理用タスク (パッチのインストール、デバイスのリブートなど) を実行するアクション・スクリプト・コマンドのセット。

アクション・スクリプト (Action Script)

エンドポイントでアクションを実行するために使用する言語。

エージェント (agent)

「BigFix エージェント (BigFix agent) *(##### 65)*」を参照。

あいまいなソフトウェア (ambiguous software)

別の実行可能ファイルとよく似た実行可能ファイルがあるソフトウェア、またはカタログ内の複数の場所に存在するソフトウェア (スタンドアロン製品と

しての Microsoft Word と Microsoft Office にバンドルされた Microsoft Word が存在する場合など)。

監査パッチ (audit patch)

修正不能であり管理者の確認を要する状態を検出するために使用されるパッチ。監査パッチにはアクションが含まれず、監査パッチをデプロイすることはできない。

自動コンピューター・グループ (automatic computer group)

指定されたデバイスのプロパティーをグループ・メンバーシップに設定された基準と比較することにより、実行時にメンバーシップが決まるコンピューター・グループ。自動グループ内のデバイスのセットは動的である。これは、そのグループが変化する可能性があること、また実際に変化することを意味する。「コンピューター・グループ *(##### 66)*」も参照。

B

ベースライン (baseline)

一緒にデプロイされるアクションの集合。ベースラインは、通常、デプロイメントを単純化するため、またはアクションのセットが適用される順序を制御するために使用される。「デプロイメント・グループ (deployment group) *(##### 68)*」も参照。

BigFix エージェント (BigFix agent)

BigFix による管理とモニタリングを可能にするエンドポイント上の BigFix コード。

BigFix クライアント (BigFix client)

「BigFix エージェント (BigFix agent) *(##### 65)*」を参照。

BigFix コンソール (BigFix console)

プライマリー BigFix 管理インターフェース。このコンソールは、完全な機能セットを BigFix 管理者に提供する。

C

クライアント (client)

サーバーからのサービスを要求するソフトウェア・プログラムまたはコンピューター。サーバー (server) *(##### 75)* も参照。

クライアント時間 (client time)

BigFix クライアントのデバイス上のローカル時間。

クラウド

コンテナーまたは仮想マシンで実行されるコンピューターおよびストレージ・インスタンスまたはサービスのセット。

Common Vulnerabilities and Exposures 識別番号 (CVE ID) (Common Vulnerabilities and Exposures Identification Number (CVE ID))

National Vulnerability Database の特定のエントリーを識別する番号。ベンダーのパッチ文書には、通常、CVE ID が含まれる (CVE ID が使用可能な場合)。「National Vulnerability Database *(##### 72)*」も参照。

Common Vulnerabilities and Exposures (CVE) システム (Common Vulnerabilities and Exposures system (CVE))

米国連邦情報・技術局 (NIST) が保守する National Vulnerabilities Database (NVD) の一部である公式に知られたネットワーク脆弱性の参照。

コンポーネント

複数のアクションを含むデプロイメント内の個々のアクション。「デプロイメント・グループ (deployment group) *(##### 68)*」も参照。

コンピューター・グループ (computer group)

関連するコンピューターのグループ。管理者はコンピューター・グループを作成して、システムを意味のあるカテゴリーに編成し、複数のコンピューターへのコンテンツのデプロイメントを容易にできる。「自動コンピューター・グループ *(##### 65)*」、「手動コンピューター・グループ *(##### 71)*」も参照。

コンソール

「BigFix コンソール (##### 65)」を参照。

コンテンツ (content)

データ、ルール、クエリー、基準、その他の指示を含むデジタル署名されたファイル。ネットワーク全体でのデプロイメント用にパッケージ化されている。BigFix エージェントはコンテンツ内の検出基準 (Relevance ステートメント) およびアクション指示 (アクション・スクリプト・ステートメント) を使用して、脆弱性を検出したりネットワーク・ポリシーを施行したりする。

コンテンツの関連度 (content relevance)

パッチまたはソフトウェアが 1 つ以上のデバイスへのデプロイメントに適しているかどうかの判定。「デバイスの関連度 (##### 69)」も参照。

協定世界時 (UTC) (Coordinated Universal Time (UTC))

世界中で原子時計によって保持される国際標準時。

問題のあるパッチ (corrupt patch)

前のパッチで行われた修正が変更または危殆化された場合にオペレーターに警告するパッチ。この状況は、前のサービス・パックまたはアプリケーションがより新しいファイルを上書きし、パッチが適用されたファイルが現行ファイルではなくなった場合に発生する可能性がある。問題のあるパッチによって、この状態にフラグが立てられる。これを使用して、より新しいパッチを再適用することができる。

カスタム・コンテンツ (custom content)

ユーザーが独自のネットワークで使用するために作成した BigFix コード (カスタム・パッチやカスタム・ベースラインなど)。

CVE

「Common Vulnerabilities and Exposures システム (##### 66)」を参照。

CVE ID

「Common Vulnerabilities and Exposures 識別番号 (##### 66)」を参照。

D

データ・ストリーム (data stream)

パッケージ・データのソースとして機能する情報のストリング。

デフォルト・アクション (default action)

Fixlet のデプロイ時に実行されるように指定されたアクション。デフォルト・アクションが定義されていない場合、オペレーターには、いくつかのアクションから選択するか、単一アクション関する情報に基づく意思決定を行うように求めるプロンプトが出されます。

確定パッケージ (definitive package)

コンピューター上のソフトウェアの存在を識別するための主な方法となるデータのストリング。

デプロイ (deploy)

ソフトウェアのインストールやパッチの更新などの目的で、実行により操作やタスクを完了するために 1 つ以上のエンドポイントにコンテンツをディスパッチすること。

デプロイメント (deployment)

1 つ以上のエンドポイントにディスパッチされたコンテンツに関する情報 (ディスパッチされたコンテンツの特定のインスタンス)。

デプロイメント・グループ (deployment group)

オペレーターがデプロイメント用に複数のアクションを選択した場合、またはベースラインがデプロイされた場合に作成されたアクションの集合。「ベースライン *(##### 65)*」、「コンポーネント *(##### 66)*」、「デプロイメント・ウィンドウ *(##### 69)*」、「複数のアクション・グループ *(##### 72)*」も参照。

デプロイメント状態 (deployment state)

エンドポイント上で実行するデプロイメントの適格性。状態には、オペレーターによって設定されたパラメーター (「Start at 1AM, end at 3AM」など) が含まれる。

デプロイメント状況 (deployment status)

すべての対象デバイスの累積の結果。デプロイメントの成功のパーセンテージとして表示される。

デプロイメント・タイプ (deployment type)

デプロイメントに含まれるアクションが 1 つか複数かを示すもの。

デプロイメント期間 (deployment window)

デプロイメントのアクションが実行に適格である期間。例えば、Fixlet に 3 日間のデプロイメント期間があり、オフラインの適格デバイスがこの 3 日の期間内に BigFix に通信した場合、そのデバイスは Fixlet を取得します。この 3 日間の期限が切れた後にデバイスがオンラインに戻った場合、そのデバイスは Fixlet を取得しません。「デプロイメント・グループ (deployment group) *(##### 68)*」も参照。

デバイス (device)

BigFix が管理しているラップトップ、デスクトップ、サーバー、仮想マシンなどのエンドポイント。BigFix エージェントを実行しているエンドポイント。

デバイスの所有者 (device holder)

BigFix 管理対象コンピューターを使用する個人。

デバイス・プロパティー (device property)

BigFix によって収集されたデバイスに関する情報 (デバイスのハードウェア、オペレーティング・システム、ネットワーク状況、設定、BigFix クライアントに関する詳細を含む)。カスタム・プロパティーをデバイスに割り当てることもできる。

デバイスの関連度 (device relevance)

BigFix コンテンツの一部をデバイスに適用する必要があるか (パッチを適用する、ソフトウェアをインストールする、ベースラインを実行するなど) の判定。「コンテンツの関連度 *(##### 67)*」も参照。

デバイスの結果 (device result)

特定のエンドポイントのデプロイメントの状態 (結果を含む)。

災害対策サーバー・アーキテクチャー (DSA)

障害が発生した場合に備えて完全な冗長性を実現するために複数のサーバーをリンクするアーキテクチャー。

DSA

「災害対策サーバー・アーキテクチャー (DSA) *(##### 70)*」を参照。

動的に対象指定 (dynamically targeted)

コンピューター・グループを使用してデプロイメントを対象にすることに関連する。

E

エンドポイント (endpoint)

BigFix エージェントを実行するネットワーク・デバイス。

F

フィルター (filter)

項目のリストを、特定の属性を持つものに絞ること。

Fixlet

操作またはタスクを実行するために一緒にバンドルされた Relevance ステートメントおよびアクション・スクリプト・ステートメントを含む BigFix コンテンツの一部。Fixlet は BigFix コンテンツの基本的なビルディング・ブロックである。Fixlet は、ネットワーク管理アクションやレポート・アクションを実行するために BigFix エージェントに指示を提供する。

G

グループ・デプロイメント (group deployment)

複数のアクションが 1 つ以上のデバイスにデプロイされたデプロイメントのタイプ。

H

ハイブリッド・クラウド

クラウド・サービスの異なるセット (通常はパブリック・クラウドとプライベート・クラウド) を最適に組み合わせて使用すること。

L

ロック (locked)

デバイスのロックが解除されるまで BigFix のアクションの大部分が実行できないエンドポイントの状態。

月

MAG

「複数アクション・グループ (##### 72)」を参照。

管理権限 (management rights)

指定されたコンピューターのグループへのコンソール・オペレーターの制限。サイト管理者またはマスター・オペレーターのみが管理権限を割り当てることができる。

マニュアル・コンピューター・グループ (manual computer group)

オペレーターによる選択によってメンバーシップが決まるコンピューター・グループ。マニュアル・グループ内のデバイスの組み合わせは静的であり、変化しない。「コンピューター・グループ (##### 66)」も参照。

マスター・オペレーター (master operator)

管理権限を持つコンソール・オペレーター。マスター・オペレーターは、サイト管理者とほぼ同等のことを実行できるが、オペレーターを作成することはできない。

マストヘッド (masthead)

BigFix プロセス (Fixlet コンテンツへの URL など) のパラメーターを含むファイルの集合。BigFix エージェントは、サブスクライブされているマストヘッドに基づいてコンテンツを企業内に取り込む。

ミラー・サーバー (mirror server)

企業で直接の Web アクセスは許可していないが、代わりにパスワード・レベルの認証を必要とするプロキシー・サーバーを使用する場合に必要な BigFix サーバー。

マルチクラウド (Multicloud)

別個のクラウド・サービス・セットを使用すること。通常、複数ベンダーから提供され、特定のアプリケーション群は単一のクラウド・インスタンスに限定される。

複数アクション・グループ (MAG) (multiple action group (MAG))

ベースラインなどで複数のアクションが一緒にデプロイされたときに作成される BigFix オブジェクト。1 つの MAG には複数の Fixlet またはタスクが含まれる。「デプロイメント・グループ (deployment group) *(##### 68)*」も参照。

N

National Vulnerability Database (NVD)

米国連邦情報・技術局 (NIST) が保持する公式に知られた情報セキュリティーの脆弱性およびエクスポージャーのカタログ。「Common Vulnerabilities and Exposures 識別番号 *(##### 66)*」も参照。

NVD

「National Vulnerability Database *(##### 72)*」を参照。

O

オファー (offer)

デバイスの所有者が、BigFix アクションに同意するか同意しないこと、および実行時に何らかの制御を行うことを可能にするデプロイメントのオプション。例えば、デバイス所有者が、ソフトウェア・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、インストールを夜間に実行するか昼間に実行するかを決定できる。

無期限のデプロイメント (open-ended deployment)

終了日も有効期限もないデプロイメント。継続的に実行され、ネットワーク上のコンピューターが準拠しているかを検査するものなど。

オペレーター (operator)

BigFix WebUI または BigFix コンソールの一部を使用する個人。

P

パッチ (patch)

問題を修正するために、2 つのリリースの間にユーザーに提供される当面のソリューションとしてベンダー・ソフトウェアに追加されるコードの断片。

パッチ・カテゴリー (patch category)

バグ修正やサービス・パックなど、パッチのタイプおよび操作の一般領域の説明。

パッチの重大度 (patch severity)

ネットワークの脅威または脆弱性によってもたらされるリスクのレベル、およびそれに関連してそのパッチを適用する重要度。

R

リレー (relay)

特殊なサーバー・ソフトウェアを実行しているクライアント。リレーは、サーバーとクライアントの間の直接ダウンロードを最小限に抑え、アップストリーム・データを圧縮することにより、サーバーとネットワークの負荷を軽減する。

関連度

指定のエンドポイントへのコンテンツの適用可能性を判別するために使用される BigFix クエリー言語。関連度では「はい」または「いいえ」の質問が行われ、その結果が評価される。関連度のクエリーの結果により、アクションを適用できるか、またはアクションを適用する必要があるかが決定される。関連度は Fixlet のアクション・スクリプトと対になっている。

日

SCAP

「Security Content Automation Protocol *(##### 75)*」を参照。

SCAP チェック (SCAP check)

Security Content Automation Protocol (SCAP) チェックリスト内の特定の構成チェック。チェック項目は XCCDF で記述されており、SCAP テンプレートに従って SCAP 列挙と SCAP マッピングを組み込む必要がある。

SCAP チェックリスト (SCAP checklist)

機械可読言語 (XCCDF) で記述された構成チェックリスト。Security Content Automation Protocol (SCAP) チェックリストは、NIST National Checklist Program に提出され、承認されている。これらは、SCAP 製品およびサービスとの互換性を確保するため、SCAP テンプレートにも準拠している。

SCAP コンテンツ (SCAP Content)

自動化 XML 形式で表されたセキュリティー・チェックリスト・データ、脆弱性および製品名関連の列挙、および列挙間のマッピングで構成されたリポジトリー。

SCAP 列挙 (SCAP enumeration)

すべて既知のセキュリティー関連ソフトウェア欠陥 (CVE)、既知のソフトウェア構成問題 (CCE)、および標準ベンダー名および製品名 (CPE) のリスト。

SCAP マッピング (SCAP mapping)

ソフトウェア欠陥および構成問題に対して標準ベースの影響の測定を提供する列挙の相互関係。

Security Content Automation Protocol (SCAP)

米国連邦情報・技術局 (NIST) による脆弱性およびコンプライアンスの自動化、測定、管理に使用される標準のセット。

サーバー (server)

他のソフトウェア・プログラムまたはコンピューターにサービスを提供するソフトウェア・プログラムまたはコンピューター。「クライアント (##### 66)」も参照。

署名パスワード (signing password)

デプロイメント用のアクションに署名するためにコンソール・オペレーターが使用するパスワード。

単一デプロイメント (single deployment)

単一のアクションが 1 つ以上のデバイスにデプロイされたデプロイメントのタイプ。

site

BigFix コンテンツの集合。サイトは、同様のコンテンツを一緒にまとめる。

サイト管理者 (site administrator)

BigFix のインストール、新規コンソール・オペレーターの承認と作成に関する責任者。

ソフトウェア・パッケージ (software package)

デバイスにソフトウェア製品をインストールする Fixlet の集合。ソフトウェア・パッケージは、配布のためにオペレーターによって BigFix にアップロードされる。BigFix ソフトウェア・パッケージには、インストール・ファイ

ル、ファイルをインストールするための Fixlet、およびパッケージに関する情報 (メタデータ) が含まれる。

SQL Server

Microsoft が提供する完全なデータベース・エンジン。取得して BigFix システムにインストールすると、基本的なレポート作成とデータ・ストレージを超えるニーズを実現できる。

標準デプロイメント (standard deployment)

単一の管理ドメインを持つワークグループおよび企業に適用される BigFix のデプロイメント。すべてのクライアント・コンピューターが単一の社内サーバーに直接アクセスできる設定を目的としている。

静的に対象指定 (statistically targeted)

デバイスまたはコンテンツの一部に対してデプロイメントを対象指定するために使用する方式に関連する。静的に対象指定されたデバイスは、オペレーターによって手動で選択されている。

置き換えられたパッチ (superseded patch)

以前のバージョンのパッチがより新しいバージョンによって置き換えられている場合にオペレーターに通知するパッチのタイプ。これは、新しいパッチが以前のパッチと同じファイルを更新した場合に発生する。置き換えられたパッチは、より新しいパッチで修正可能な脆弱性にフラグを立てる。置き換えられたパッチはデプロイできない。

システムの電源状態 (system power state)

システムの全体的な電力使用量の定義。BigFix 電源管理がトラッキングする主な電源状態は、「アクティブ」、「アイドル」、「スタンバイ」または「休止状態」、「電源オフ」の 4 つです。

T

対象 (target)

デプロイメント用のコンテンツを選択するか、コンテンツを受け取るデバイスを選択することにより、コンテンツをデプロイメント内のデバイスとマッチングすること。

対象指定 (targeting)

デプロイメント内のエンドポイントを指定するために使用する方式。

タスク (task)

継続中の保守タスクを実行するためなど、再使用のために設計された Fixlet のタイプ。

U

UTC

「協定世界時 (Coordinated Universal Time) *(##### 67)*」を参照。

V

仮想プライベート・ネットワーク (VPN) (virtual private network (VPN))

パブリック・ネットワークまたはプライベート・ネットワークの既存フレームワーク上で企業のイントラネットを拡張したもの。VPN を使用すると、接続の 2 つのエンドポイント間で送信されるデータを保護できる。

VPN

「仮想プライベート・ネットワーク (virtual private network) *(##### 77)*」を参照。

脆弱性 (vulnerability)

オペレーティング・システム、システム・ソフトウェア、またはアプリケーション・ソフトウェア・コンポーネントでの機密漏れ。

W

Wake-from-Standby

アプリケーションが、Wake on LAN を必要とせずに、事前定義された時間にコンピューターを待機モードから起動できるようにするモード。

Wake on LAN

時間外の保守のためにユーザーがシステムをリモートで起動できるテクノロジー。Intel と IBM の Advanced Manageability Alliance の成果であり、Wired for Management Baseline Specification の一部である。このテクノロジーのユーザーは、リモートでサーバーを起動したりネットワーク経由でサーバーを制御したりできるため、ソフトウェアのインストール、アップグレード、ディスク・バックアップ、およびウィルス・スキャンを自動化して時間を節約できる。

WAN

「広域ネットワーク (wide area network) *(##### 78)*」を参照。

広域ネットワーク (WAN) (wide area network (WAN))

ローカル・エリア・ネットワーク (LAN) や大都市圏ネットワーク (MAN) で提供されるよりも大きい地理上の領域で、デバイス間の通信サービスを提供するネットワーク。

特記事項

本書は米国で提供される製品およびサービスについて作成したものです。

本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 HCL の営業担当員にお尋ねください。本書で HCL 製品、プログラム、またはサービスに言及していても、その HCL 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、HCL の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用できます。ただし、HCL 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

HCL は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

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

2 バイト文字セット (DBCS) 情報についてのライセンスに関するお問い合わせは、お住まいの国の HCL Intellectual Property Department に連絡するか、書面にて下記宛先にお送りください。

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

HCL TECHNOLOGIES LTD. 本書を特定物として現存するままの状態で提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。HCL は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において HCL 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この HCL 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

HCL は、お客様が提供するいかなる情報も、お客様に対して何ら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

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

本プログラムに関する上記の情報は、適切な使用条件の下で使用できますが、有償の場合もあります。

本書で説明されているライセンスプログラムまたはその他のライセンス資料は、HCL 所定のプログラム契約の契約条項、HCL プログラムのご使用条件、またはそれと同等の条項に基づいて、HCL より提供されます。

本書に含まれるパフォーマンスデータは、特定の動作および環境条件下で得られたものです。実際の結果は、異なる可能性があります。

HCL 以外の製品に関する情報は、その製品の供給者、出版物、もしくはその他の公に利用可能なソースから入手したものです。HCL は、それらの製品のテストは行っておりません。したがって、他社製品に関する実行性、互換性、またはその他の要求については確証できません。HCL 以外の製品の性能に関する質問は、それらの製品の供給者にお願いします。

HCL の将来の方向または意向に関する記述については、予告なしに変更または撤回される場合があり、単に目標を示しているものです。

本書には、日常の業務処理で用いられるデータや報告書の例が含まれています。より具体性を与えるために、それらの例には、個人、企業、ブランド、あるいは製品などの名前が含まれている場合があります。これらの名称はすべて架空のものであり、類似する個人や企業が実在しているとしても、それは偶然にすぎません。

著作権使用許諾:

本書には、さまざまなオペレーティング・プラットフォームでのプログラミング手法を例示するサンプル・アプリケーションプログラムがソース言語で掲載されています。お客様は、サンプルプログラムが書かれているオペレーティングプラットフォームのアプリケー

ションプログラミングインターフェースに準拠したアプリケーションプログラムの開発、使用、販売、配布を目的として、いかなる形式においても、HCL に対価を支払うことなくこれを複製し、改変し、配布できます。このサンプルプログラムは、あらゆる条件下における完全なテストを経ていません。したがって HCL は、これらのサンプルプログラムについて信頼性、利便性もしくは機能性があることをほのめかしたり、保証したりすることはできません。これらのサンプルプログラムは特定物として現存するままの状態で提供されるものであり、いかなる保証も提供されません。HCL は、お客様の当該サンプルプログラムの使用から生ずるいかなる損害に対しても一切の責任を負いません。

それぞれの複製物、サンプルプログラムのいかなる部分、またはすべての派生的創作物にも、次のように、著作権表示を入れていただく必要があります。© (お客様の会社名) (西暦年). このコードの一部は、HCL Ltd. のサンプルプログラムから取られています。

商標

HCL Technologies Ltd.、HCL Technologies Ltd. ロゴ、および hcl.com は、世界の多くの国で登録された HCL Technologies Ltd. の商標または登録商標です。

Adobe、Adobe ロゴ、PostScript、PostScript ロゴは、Adobe Systems Incorporated の米国およびその他の国における登録商標または商標です。

Java およびすべての Java 関連の商標およびロゴは、Oracle やその関連会社の商標または登録商標です。

Microsoft、Windows、Windows NT および Windows ロゴは、Microsoft Corporation の米国およびその他の国における商標です。

Linux は、Linus Torvalds の米国およびその他の国における登録商標です。

UNIX は The Open Group の米国およびその他の国における登録商標です。

他の製品名およびサービス名等は、それぞれ HCL または各社の商標である場合があります。

製品資料に関するご使用条件

これらの資料は、以下のご使用条件に同意していただける場合に限りご使用いただけます。

適用条件

HCL Web サイトの「ご利用条件」に加えて、以下のご使用条件が適用されます。

個人使用

これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、非商業的な個人による使用目的に限り複製できます。ただし、HCL の明示的な承諾を得ずに、これらの資料またはその一部について、二次的著作物を作成したり、配布 (頒布、送信を含む) または表示 (上映を含む) したりすることはできません。

商業的使用

これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、お客様の企業内に限り、複製、配布、および表示できます。ただし、HCL の明示的な承諾を得ずに、これらの資料の二次的著作物を作成したり、お客様の企業外で資料またはその一部を複製、配布、または表示したりすることはできません。

権利

ここで明示的に許可されているもの以外に、資料や資料内に含まれる情報、データ、ソフトウェア、 またはその他の知的所有権に対するいかなる許可、ライセンス、または権利を明示的にも黙示的 にも付与するものではありません。

資料の使用が HCL の利益を損なうと判断された場合や、上記の条件が適切に守られていないと判断された場合、HCL はいつでも自らの判断により、ここで与えた許可を撤回できるものとさせていただきます。

お客様がこの情報をダウンロード、輸出、または再輸出する際には、米国のすべての輸出入 関連法規を含む、すべての関連法規を遵守するものとします。

HCL は、これらの資料の内容についていかなる保証もしません。これらの資料は、特定物として現存するままの状態で提供され、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任なしで提供されます。