テクニカルホワイトペーパー

HP Manageability Integration Kit

HP Client Management Solutions

2018 年 7 月

925167-004

目次

画像一覧

テーブル一覧

1 概要

HP のコンピューターは管理性を持たせるように設計されています。 それは 2 つの理念を中心にしています。

- IT 管理者に対して、コンピュータに付属の HP BIOS、ハードウェア、およびプレインストールされたソフトウェアの管理に役立つ方法を提供します。
- 管理者が選択したクライアント管理コンソールと連携するソリューションを提供します。

HP Manageability Integration Kit（MIK）はこれら 2 つの原則に対処するために開発されたソリューションです。

HP MIK は、管理面を HP のハードウェア、BIOS、およびソフトウェアの機能に拡張する、クライアント管理コンソールにとらわれないソリューションです。

HP MIK の目的は、既存のツールやワークフローに統合することによって、日常的なエンタープライズプロセスとタスクを簡素化するユーザーエクスペリエンスを実現することです。

HP MIK を展開するとこれらの主要な利点を得る事ができます。

- 管理の基本をスピードアップ - イメージ、BIOS、およびシステムセキュリティの作成、展開、および管理に必要なステップ数を減らして、ビジネスに集中できるようにします。
- データの保護 - BIOS 設定の保護、認証と認証情報の要件の設定、Device Guard の有効化、および Trusted Platform Module（TPM）ファームウェアアップデートの管理を行います。
- ソフトウェアの管理 - IT 管理者は HP Client Security や HP Sure Click など、ソフトウェアでサポートされている機能をリモートで管理できます。

HP MIK は、Microsoft ® System Center Configuration Manager(SCCM)と連携するように最適化されていますが、スクリプトを介して他のクライアント管理コンソールと連携します。このドキュメントには、Configuration Manager 内の HP Manageability Integration Kit プラグインの例とスクリーンショットのみが含まれています。完全なユーザーガイドについては、HP Manageability の以下の Web サイトを参照してください。
http://www.hp.com/go/clientmanagement.

2 システム要件

HP Manageability Integration Kit は、サポートされているバージョンの Microsoft System Center Configuration Manager を実行しているサーバー、およびサポートされている Windows ® オペレーティングシステムを実行しているクライアントにインストールできます。

2.1 Microsoft System Center Configuration Manager のサポートバージョン

HP Manageability Integration Kit は、次のバージョンの Microsoft System Center Configuration Manager を実行しているサーバーにインストールできます。サーバーオペレーティングシステムの要件を判断するには、Microsoft System Center Configuration Manager のドキュメントを参照してください。

- Microsoft System Center 2012 R2 Configuration Manager service pack 1 (SP1)
- Microsoft System Center 2012 R2 Configuration Manager service pack 1 (SP1) cumulative update 1 (CU1) 以上
- Microsoft System Center 2012 R2 Configuration Manager
- Microsoft System Center 2012 Configuration Manager SP2
- Microsoft System Center 2012 Configuration Manager SP2 CU1 以上
- Microsoft System Center 2012 Configuration Manager SP1
- Microsoft System Center Configuration Manager 1511 以上

2.2 クライアント OS のサポートバージョン

HP Manageability Integration Kit クライアントコンポーネントは、以下のクライアントオペレーティングシステムでサポートされています。（クライアントコンピュータにインストールする必要があります）

注記
いくつかの HP Manageability Kit の機能では追加の要件があります。

- **Windows 10**
- **Windows 8.1**
- **Windows 7**

3 HP Manageability Integration Kit のダウンロード

HP Manageability Integration Kit のダウンロード方法:

1. 次の URL にアクセスします。http://www.hp.com/go/clientmanagement.
2. Resources の下から、[HP Download Library]を選択します。
3. HP Manageability Integration Kit (MIK) for Microsoft System Center Configuration Manager をダウンロードします。
4. MIK Client requirements の下から、MIK の機能に関連する管理に必要な SoftPaq をダウンロードします。

4 HP Manageability Integration Kit の Configuration Manager へのインストール

1. Configuration Manager コンソールのすべてのインスタンスが閉じていることを確認します。
2. システムに HP Client Integration Kit（CIK）がインストールされている場合は、それをアンインストールします。
3. ダウンロードした HP Manageability Integration Kit (MIK) for Microsoft System Center Configuration Manager の SoftPaq を実行し、画面の指示に従ってインストールを完了します。
4. Configuration Manager コンソールを開き資産とコンプライアンスの下に HP Manageability Integration Kit が表示される事を確認します。

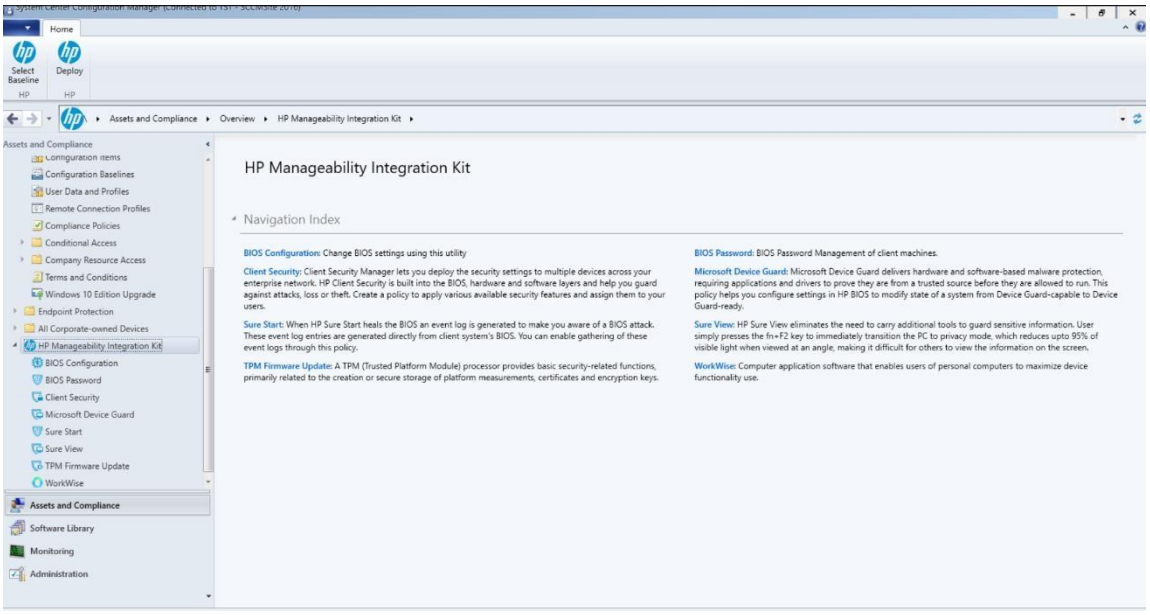


Figure 1 HP Manageability Integration Kit – Navigation Index

4.1 HP Client Support Packages の配布

インストールが完了したら、HP Client Support Packages をローカルの配布ポイントに配布する必要があります。

1. **Configuration Manager で、[ソフトウェアライブラリ]→[概要]→[アプリケーション管理]→[パッケージ]→[HP Client Support Packages]の順に選択します。**

注記

依存するタスクシーケンスの失敗を防ぐために、このフォルダ内のパッケージを削除または名前を変更しないでください。

パッケージを削除した場合は、HP Manageability Integration Kit を再インストールし、インストールウィザードで[修復]を選択してください。次に、パッケージを使用してタスクシーケンスを更新します。詳細については、「タスクシーケンスの更新」を参照してください。

---

2. 初めてのインストールの場合は、[HP Client BIOS Configuration Utility]を右クリックし、[コンテンツの配布]を選択して画面の指示に従ってウィザードを完了します。

   – または –

   アップグレードの場合は、[HP Client BIOS Configuration Utility]を右クリックし、[配布ポイントの更新]を選択して画面の指示に従ってウィザードを完了します。

3. 初めてのインストールの場合は、[HP Client Support Tools]を右クリックし、[コンテンツの配布]を選択して画面の指示に従ってウィザードを完了します。

   – または –

   アップグレードの場合は、[HP Client Support Tools]を右クリックし、[配布ポイントの更新]を選択して画面の指示に従ってウィザードを完了します。

Configuration Manager のソフトウェアライブラリでは、HP Manageability Integration Kit を介してドライバパックまたはブートイメージを作成した後に、次のメニュー項目（破線で表示）、フォルダ（一点鎖線で表示）、およびパッケージ（実線で表示）が作成されます。

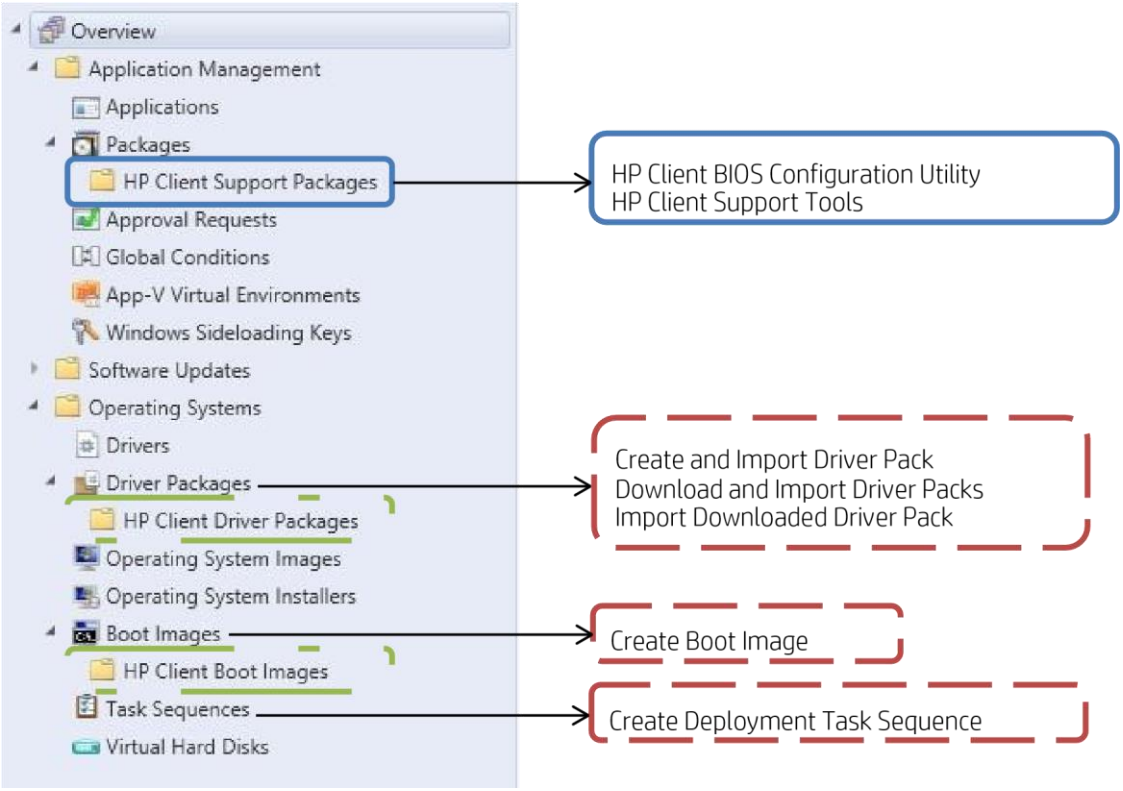


Figure 2 Software Library of Configuration Manager

メニュー項目を開くには、リボンメニューで選択するか、右クリックのコンテキストメニューを使用します。

5 HP MIK プラグイン

インストーラーは[HP Manageability Integration Kit]ノードの下にさまざまなプラグインを追加することによって、Configuration Manager の機能を拡張します。

HP MIK を使用してこれらのプラグインを管理する方法の詳細については、このドキュメント内のプラグインのそれぞれのセクションを参照してください。

現在のプラグイン:

- **HP BIOS Configuration**
- **HP BIOS Password Manager**
- **HP Client Security with Intel Authenticate**
- **Device Guard**
- **HP Sure Start**
- **HP Sure Run**
- **HP Sure Recover**
- **HP SureView**
- **TPM Firmware Update**
- **HP WorkWise**
- **HP Collaboration Keyboard**
- **HP Sure Click**
- **HP PhoneWise**

HP MIK には、オペレーティングシステムとソフトウェアの展開に役立つ機能も含まれています。これらの機能については、このドキュメントの以下のセクションで詳しく説明します。

- **HP Client Driver Packs**
- **HP Client Boot Images**
- **HP Client Task Sequences**

5.1 コンプライアンス設定

HP MIK プラグインを使用して作成または編集されたポリシーは、Configuration Manager のコンプライアンス設定として保存されます。

ポリシーの場所:

1. Configuration Manager で、[資産とコンプライアンス]を選択します。
2. [概要]→[コンプライアンス設定]→[構成項目]の順に選択します。

このページでは、[プロパティ]ダイアログボックスを開いたり、サポートされているオペレーティングシステムとハードウェアを設定したりするなど、Configuration Manager の機能を実行できます。

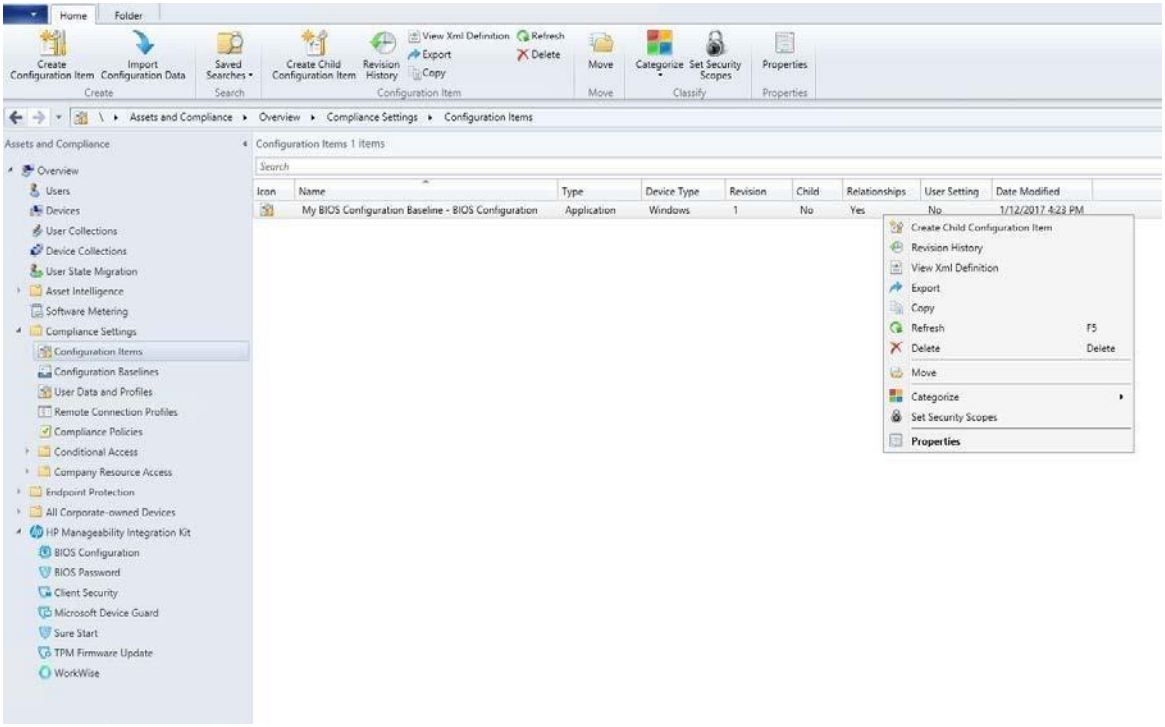


Figure 3 Configuration Items

プラグインを使用して構成アイテムを作成した場合、デフォルト名はベースライン名とプラグイン名の両方で構成されます。たとえば、My BIOS Configuration Baseline という名前のベースラインと HP BIOS Configuration プラグインを使用して作成された設定項目は、デフォルトでは My BIOS Configuration Baseline - BIOS Configuration という名前になります。

5.2 構成基準

IT 管理者は 1 つの設定基準に対して複数の設定項目を選択できます。構成基準は、さまざまなコレクションに対して展開できます。

構成基準を右クリックして、次のいずれかのオプションを選択します。

- コピー—構成基準を複製します。
- 削除—構成基準を削除します。
- 展開—異なるコレクションに展開します。
- プロパティ—展開されたコレクションの表示、評価条件の編集、カテゴリやユーザーのフィルタをします。

6 HP BIOS Password Manager

HP BIOS Password Manager インタフェースを使用すると、IT 管理者はクライアントシステムの BIOS パスワード入力を管理できます。

6.1 サポートされるクライアントプラットフォーム

・ 2015 年以降の HP コマーシャルコンピュータ

6.2 サポートされるクライアント OS

- **Windows 10**
- **Windows 8.1**
- **Windows 7**

6.3 前提条件

- **Microsoft .NET Framework 4.0** 以上
- **HP Manageability Integration Kit**

6.4 ユーザーインターフェース

BIOS パスワードインターフェースは、現在の BIOS パスワードと変更パスワード（パスワードの変更/設定または削除）の 2 つのセクションからなり非常に単純です。

BIOS パスワードを変更または削除するには、現在のパスワードを入力する必要があります。

6.5 ポリシーの作成

1. Configuration Manager で、[資産とコンプライアンス]→[概要]の順に選択します。
2. [HP Manageability Integration Kit]を選択し、[BIOSPassword]を右クリックして、[Create Policy]を選択します。

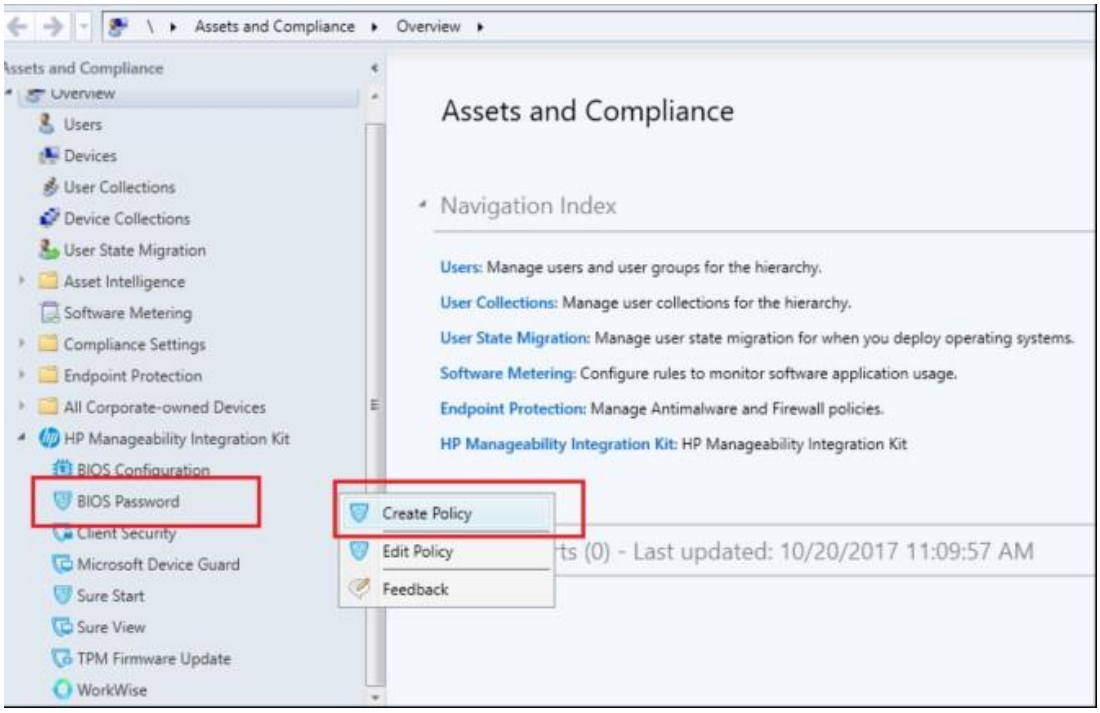


Figure 4 Create Policy

3. ベースラインの作成で、ベースライン名を入力します。

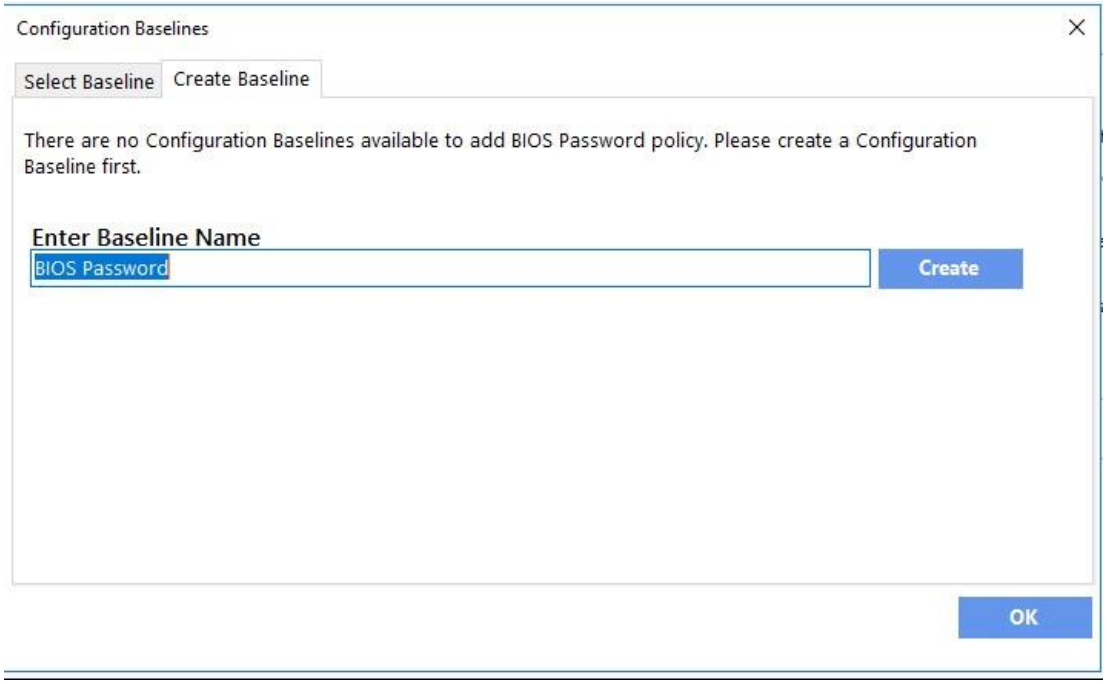
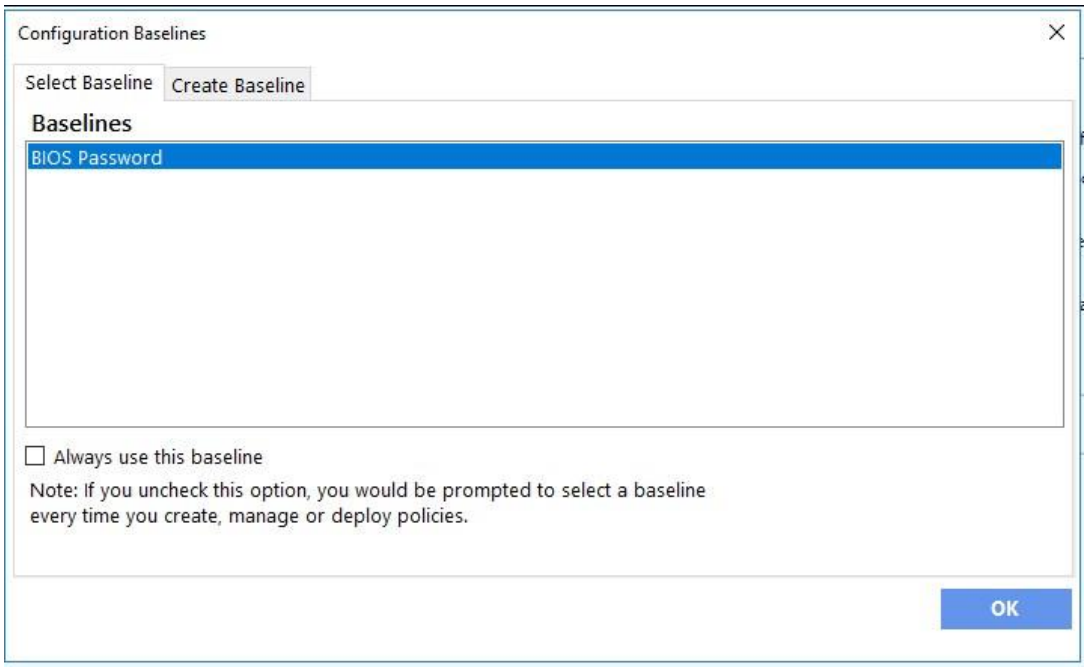


Figure 5 Creating a baseline name

4. [作成]をクリックします。



5. 新規に作成したベースラインを選択し、[OK]をクリックします。

Figure 6 Completing the Create Baseline task

6. BIOS Password Manager インターフェースで、必要に応じて適切なパスワードを入力します。

6.6 BIOS パスワードの変更

このタスクは、クライアントシステムに設定されている現在のパスワードを新しいパスワードに変更します。コレクションに BIOS パスワードが設定されているデバイスと設定されていないデバイスが混在する場合、このポリシーはすべてのデバイスに新しいパスワードを適用します。

1. [現在の BIOS パスワード]にパスワードを入力します。
2. [パスワードオプション]のチェックボックスにチェックを付けます。
3. [BIOS パスワードの変更]のラジオボタンを選択します。
4. [新しいパスワード]と[新しいパスワードの確認]の両方に新しいパスワードを入力します。
5. [Create Policy]をクリックします。
6. [ポリシーの保存]をクリックします。

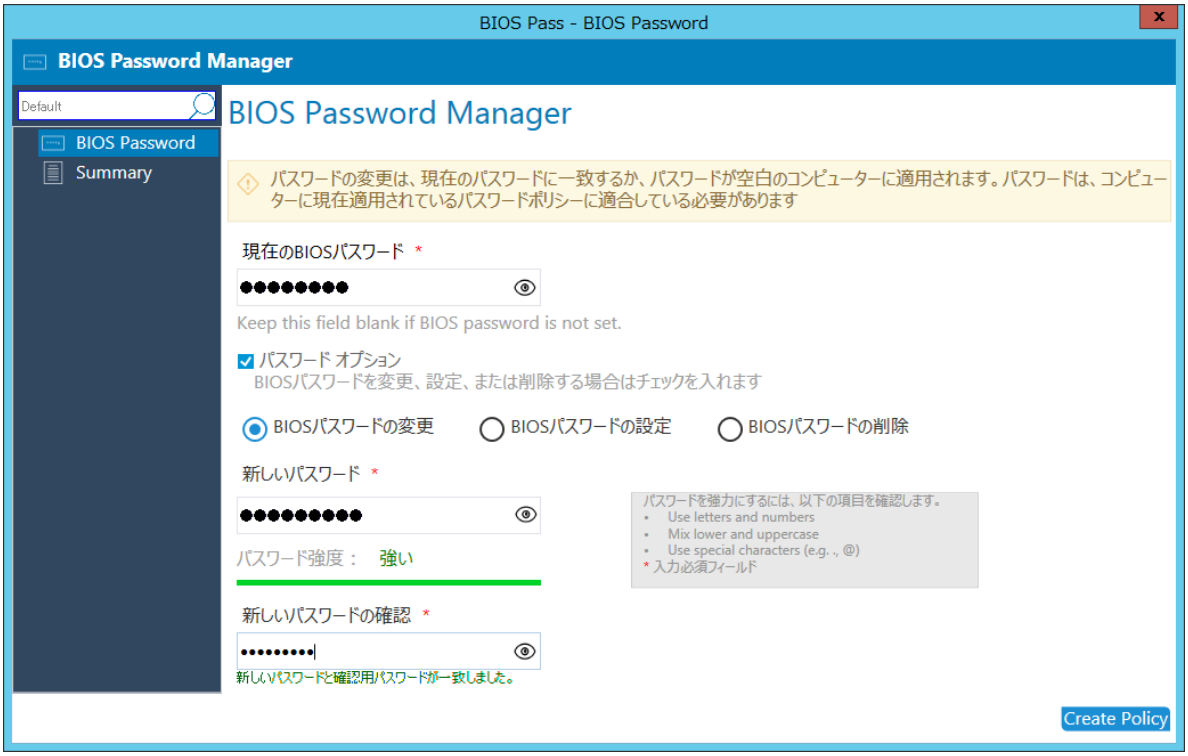


Figure 7 Changing the BIOS password

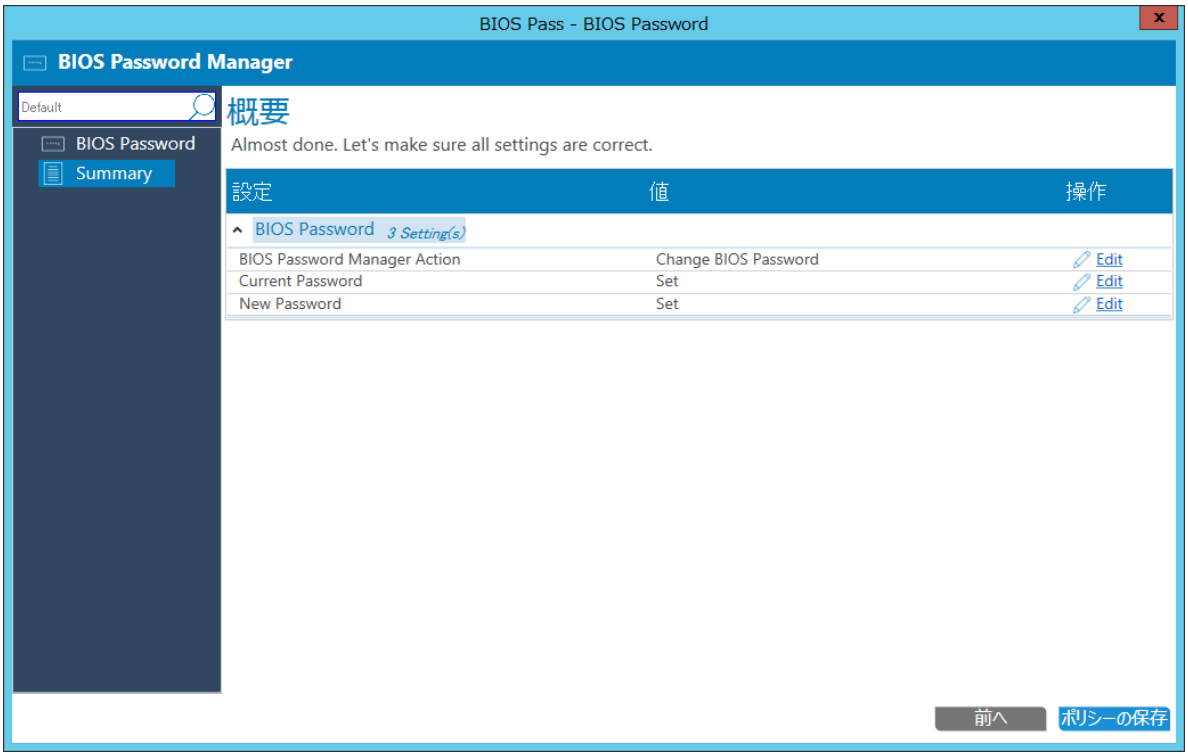


Figure 8 BIOS Password change summary

6. [ポリシーの展開]ボタンをクリックします。

7. [ポリシーの展開]の代わりに[閉じる]をクリックした場合、MIK は後で使用できるように、このベースラインとその設定を[資産とコンプライアンス]→ [概要]→ [コンプライアンス設定]→ [設定基準]に保存します。

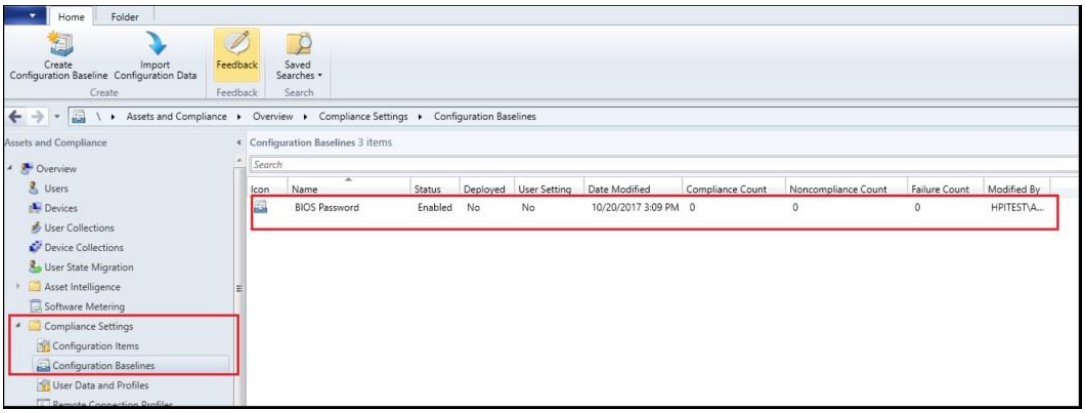


Figure 9 Compliance settings

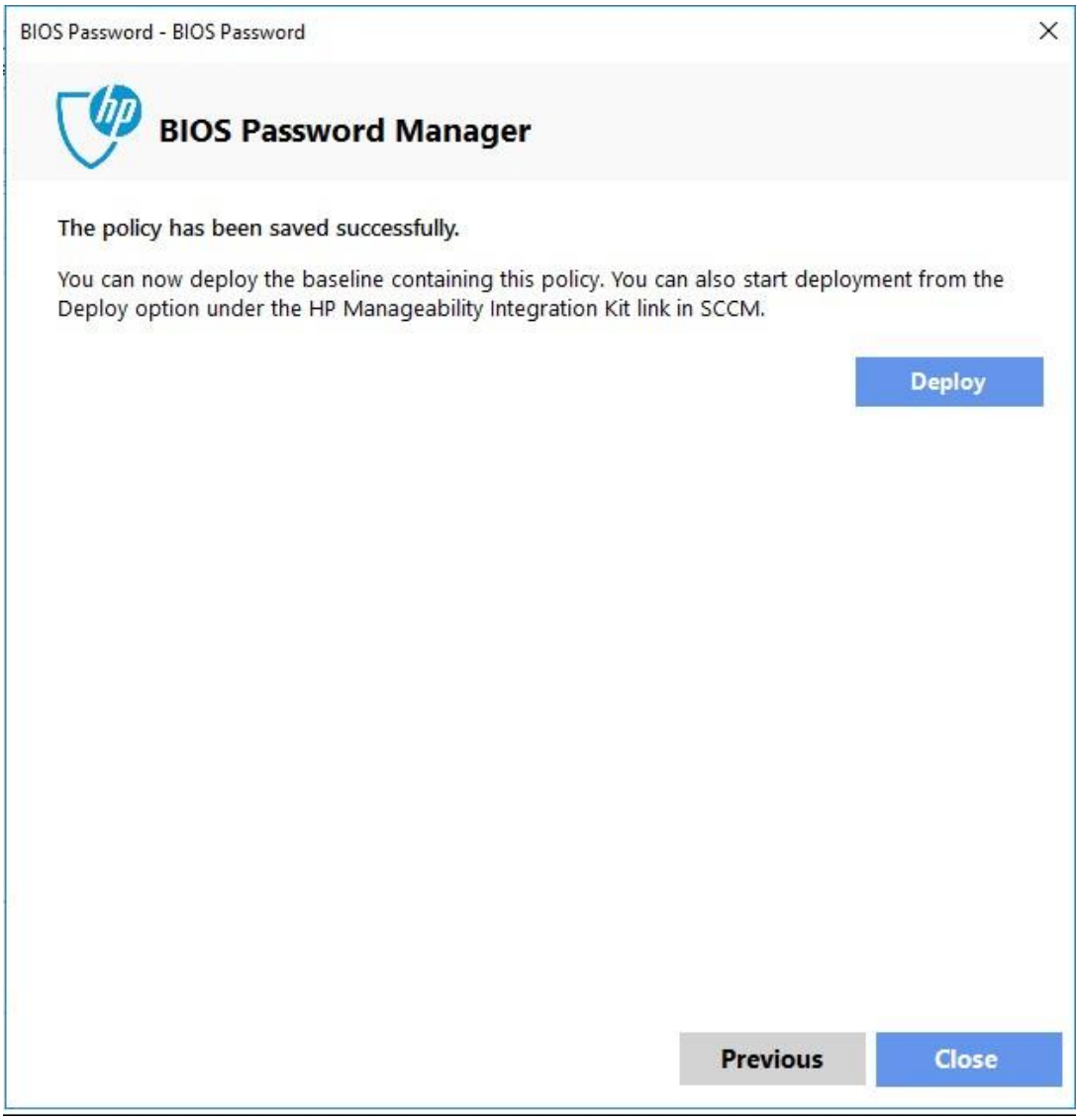
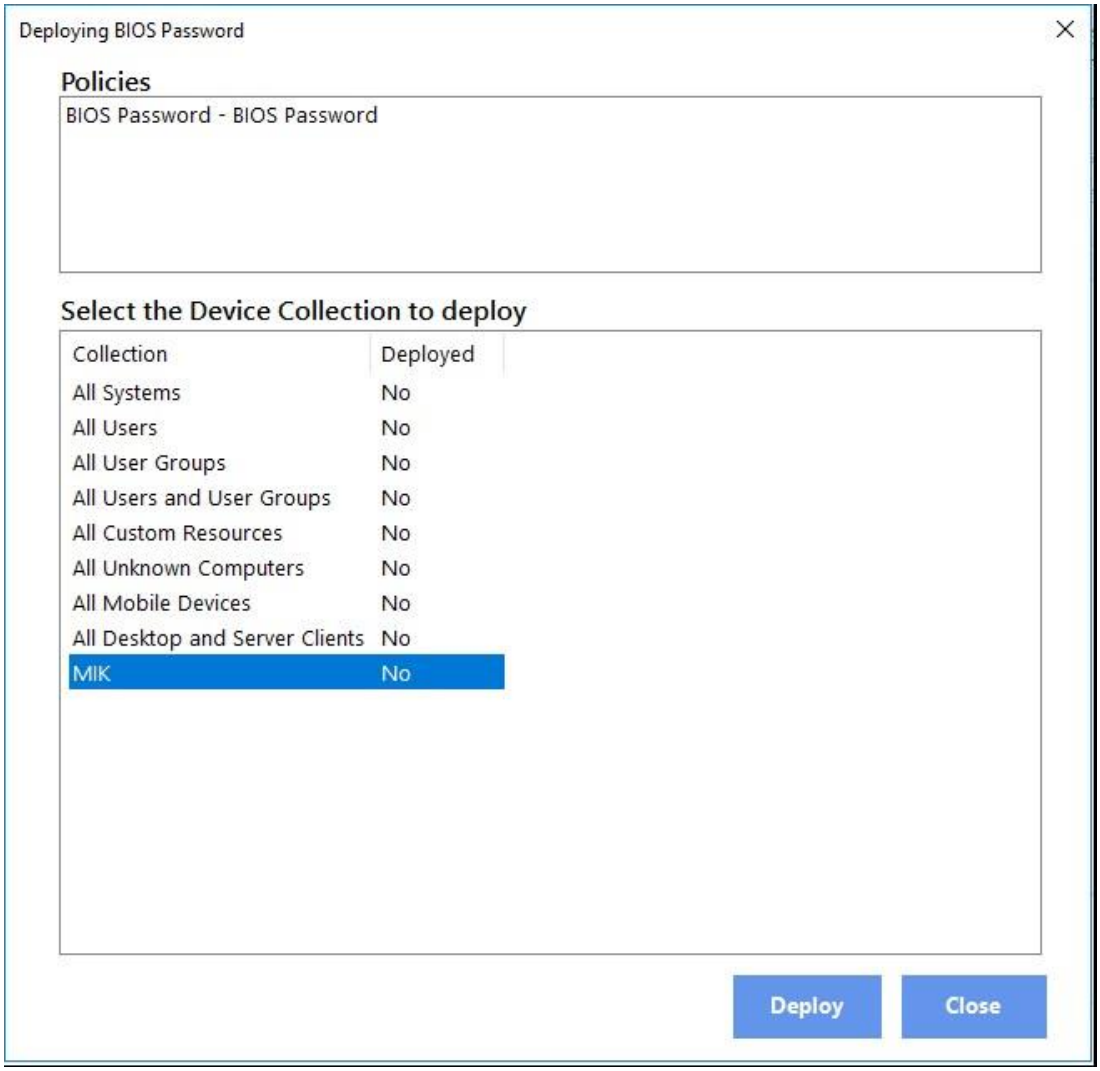


Figure 10 Deploy compliance settings



8. ポリシーを適用するための適切なコレクションを選択して、[Deploy]をクリックします。

Figure 11 Select Device Collection

6.7 BIOS パスワードの削除

このタスクは、クライアントシステムに設定されている現在の BIOS パスワードを削除します。コレクションに BIOS パスワードが設定されているデバイスと設定されていないデバイスが混在している場合、ポリシーはすべてに適用され、準拠として返されます。

クライアントシステムに、削除しようとしているものと異なる BIOS パスワードが設定されていると、ポリシーは失敗し、エラーが返されます。

1. [現在の BIOS パスワード]にパスワードを入力します。
2. [パスワードオプション]のチェックボックスにチェックを付けます。

3. [BIOS パスワードの削除]のラジオボタンを選択します。

Figure 12 Removing the BIOS password

4. [Create Policy]をクリックします。

5. [ポリシーの保存]をクリックします。

6. BIOS パスワードの削除を選択したことを確認するダイアログが表示されます。 [OK]をクリックして続行します。

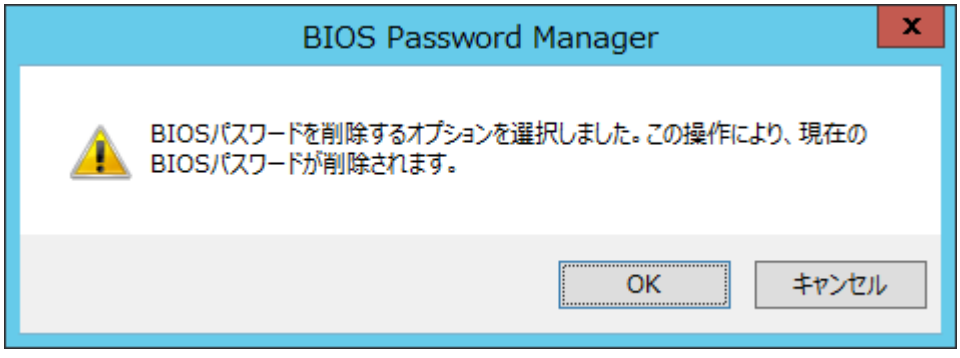


Figure 13 Confirming BIOS password removal

7. [ポリシーの展開]ボタンをクリックして次の画面に進みます。

8. ポリシーを適用するための適切なコレクションを選択して、[Deploy]をクリックします。

6.8 BIOS パスワードの設定

このタスクは、現在の BIOS パスワードが設定されていないクライアントシステムに新しい BIOS パスワードを設定します。

1. [パスワードオプション]のチェックボックスにチェックを付けます。
2. [BIOS パスワードの設定]ラジオボタンを選択します。
3. [新しいパスワード]と[新しいパスワードの確認]の両方に新しいパスワードを入力します。

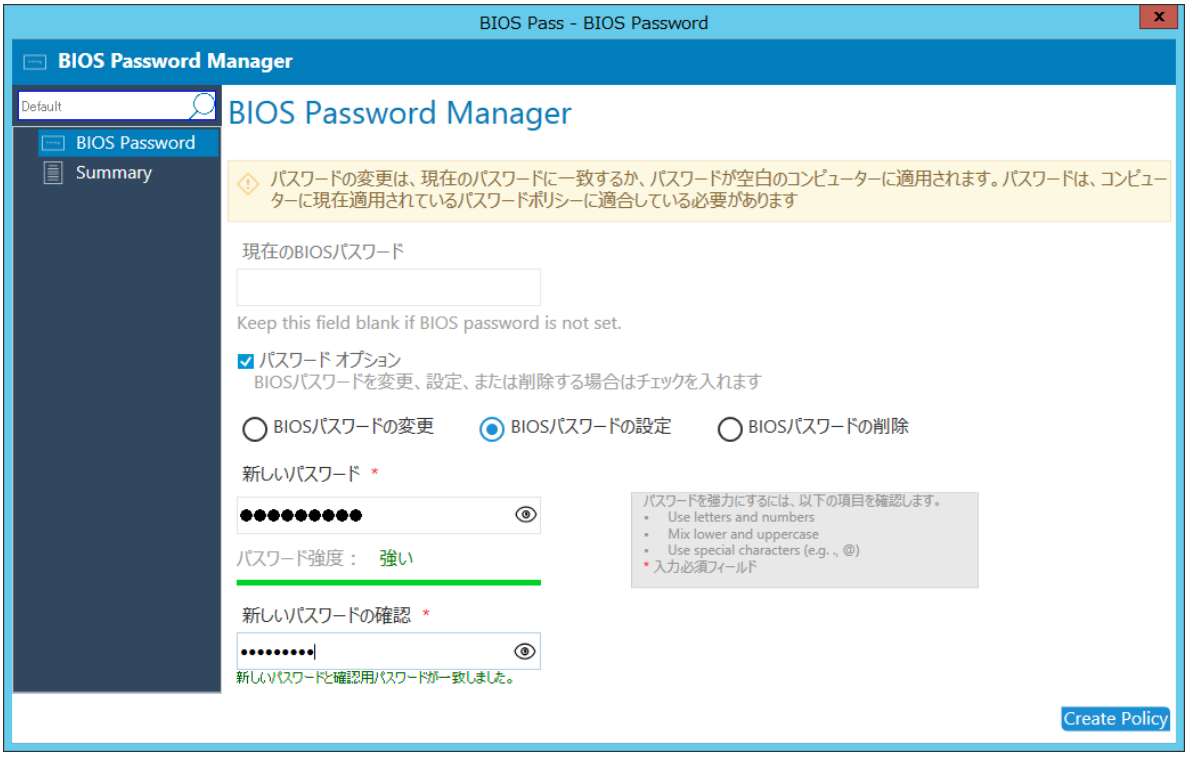


Figure 14 Set new BIOS password

4. [Create Policy]をクリックします。
5. [ポリシーの保存]をクリックします。
6. クライアントシステムに BIOS パスワードが設定されていないことを確認するダイアログが表示される場合は、 [OK]をクリックして続けます。

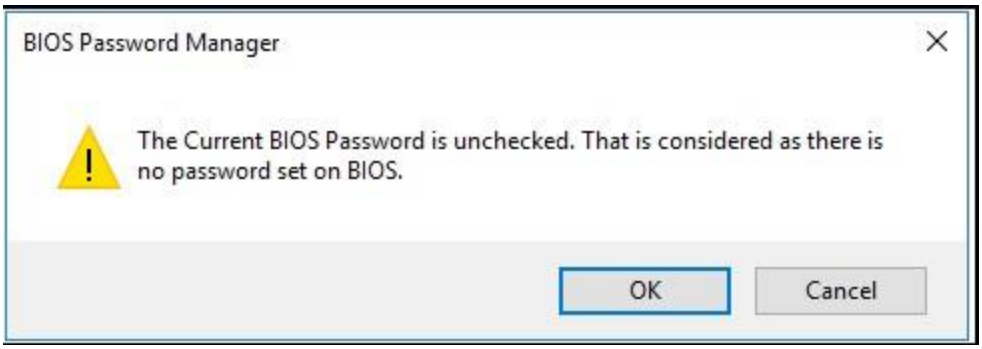


Figure 15 Confirming new BIOS password

7. [ポリシーの展開]ボタンをクリックして次の画面に進みます。
8. ポリシーを適用するための適切なコレクションを選択して、[Deploy]をクリックします。

7 HP BIOS Configuration

BIOS Configuration インターフェースを使用して、IT 管理者は BIOS 設定ポリシーを定義してクライアントコンピュータに展開できます。

7.1 サポートされるクライアントプラットフォーム

- 2015 年以降の HP コマーシャルコンピュータ

7.2 サポートされるクライアント OS

- **Windows 10**
- **Windows 8.1**
- **Windows 7**

7.3 前提条件

- **Microsoft .NET Framework 4.0** 以上
- **HP Manageability Integration Kit**

7.4 ユーザーインターフェース

HP BIOS Configuration ウィンドウには 3 つの列があります。

[選択]列は、設定がポリシーによって適用されるかどうかを指定するために使用されます。設定が選択されている場合は、指定された値に設定されます。設定がクリアされても、変更されません。

設定欄には設定名が表示されます。

[値]列を使用して、設定に応じて値を入力するか、ドロップダウンメニューから値を選択することができます。入力値に特定の構文が必要な場合は、構文が正しい場合はボックスの背景が緑色になり、構文を修正する必要がある場合は赤色になります。

注記:
カテゴリ表示では、3 つの列すべてを表示するようにカテゴリを展開する必要があります。

一部の設定の横にあるアイコンは、次の動作を示しています。

- 設定は次の再起動時に一度だけ有効になり、その後は初期値に戻ります。

- 設定は次の再起動時にユーザーの確認が要求されます。確認のためのキー入力が実施されるまでは再起動が完了しません。

7.5 カテゴリ表示ボタン

このボタンを選択すると、BIOS 設定がグループ化されたカテゴリとして表示されます。

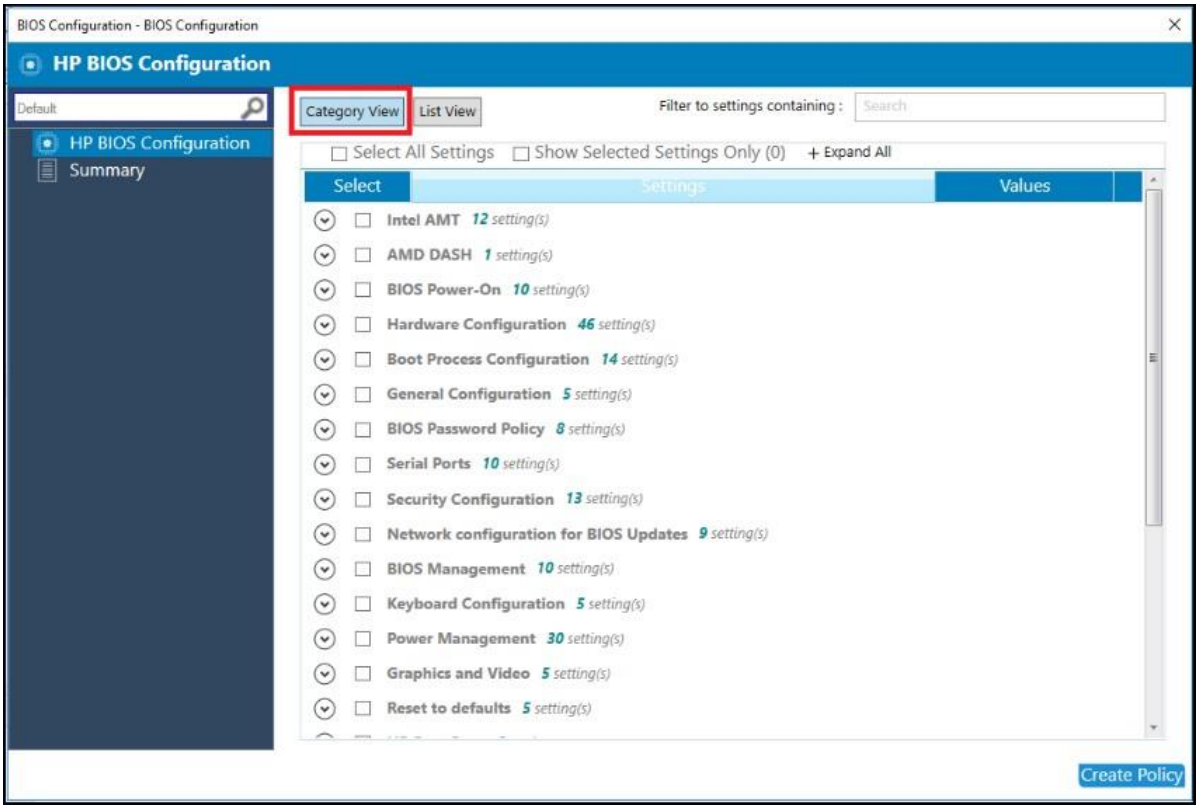


Figure 16 HP BIOS Configuration (Category view)

7.6 リスト表示ボタン

このボタンを選択すると、BIOS 設定がリストとして表示されます。

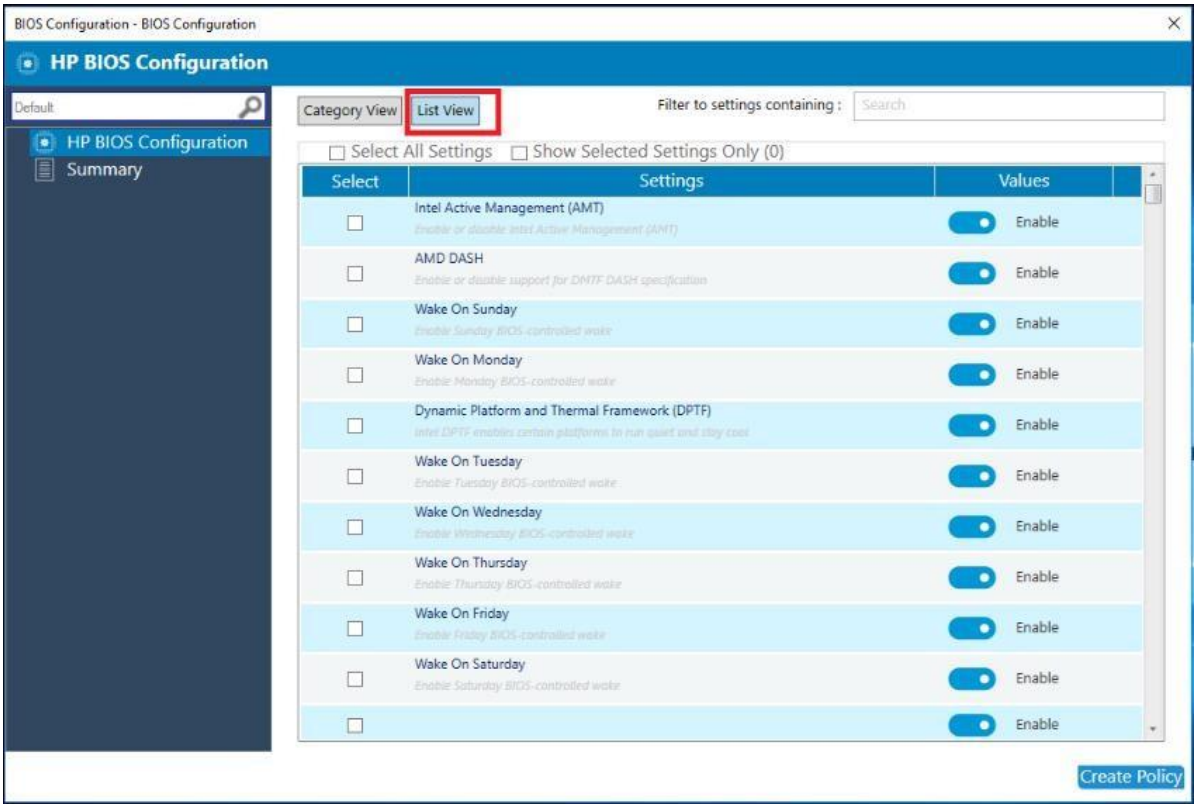


Figure 16 HP BIOS Configuration (List view)

7.7 すべての設定を選択

カテゴリビューまたはリストビューですべての設定を選択するには、このチェックボックスオプションを選択します。

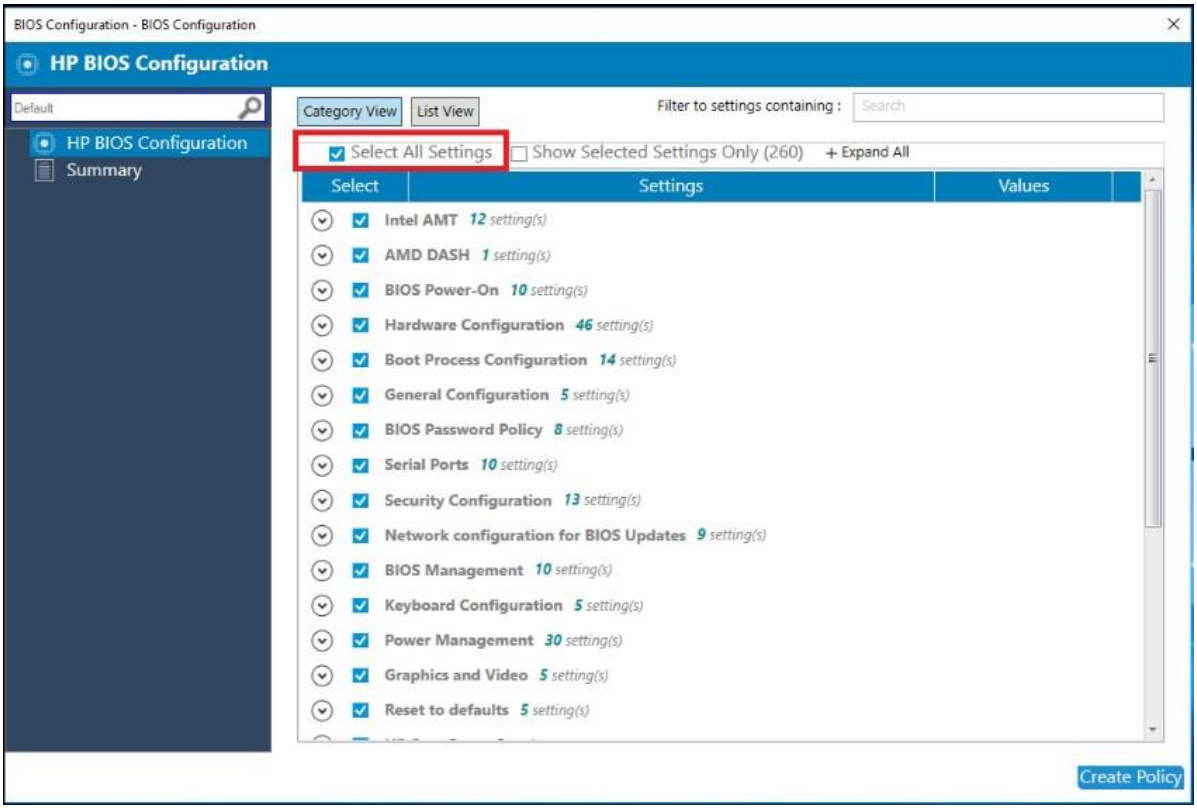


Figure 17 HP BIOS Configuration (Select All Settings)

7.8 選択した設定のみ表示

選択されている設定のみを表示するには、このチェックボックスオプションを選択します。

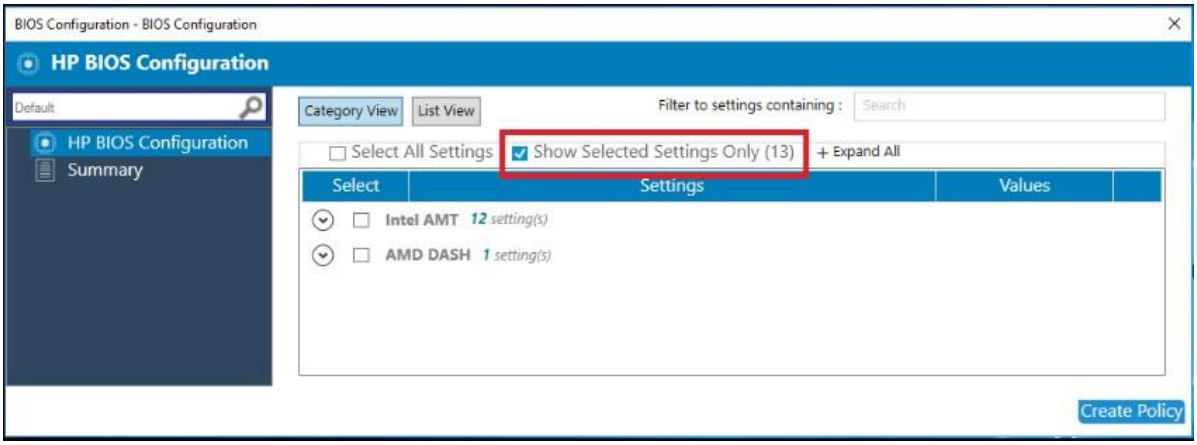


Figure 18 HP BIOS Configuration (Show Selected Settings Only)

7.9 すべて展開 / すべて折りたたむ

このボタンを選択して、各設定の詳細を拡大または縮小します。

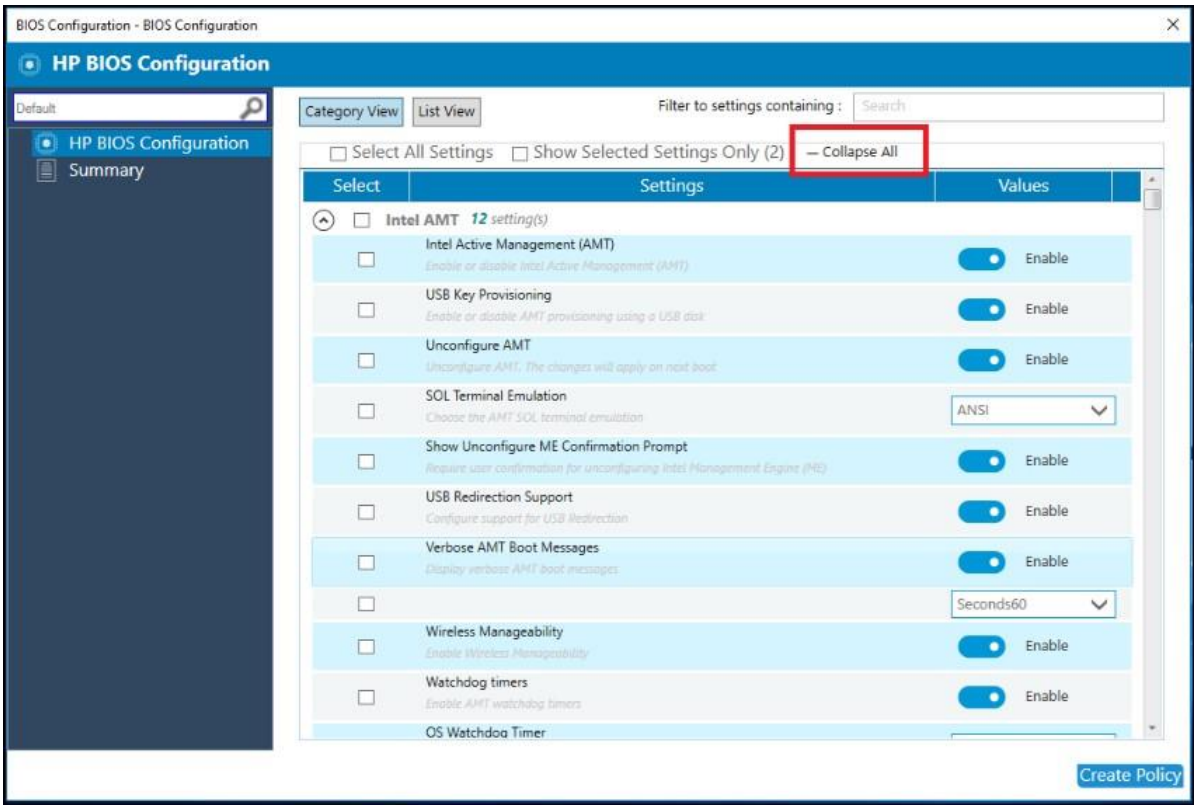


Figure 19 Expand/Collapse All

7.10 設定の検索

部分的な文字列の一致に基づいて、設定の一覧で設定をすばやく見つけるための文字列を入力します。

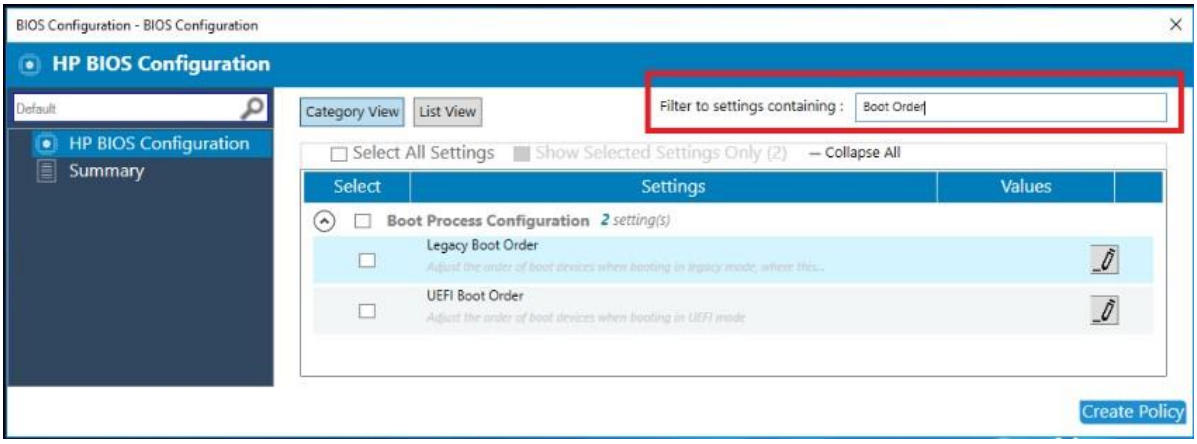
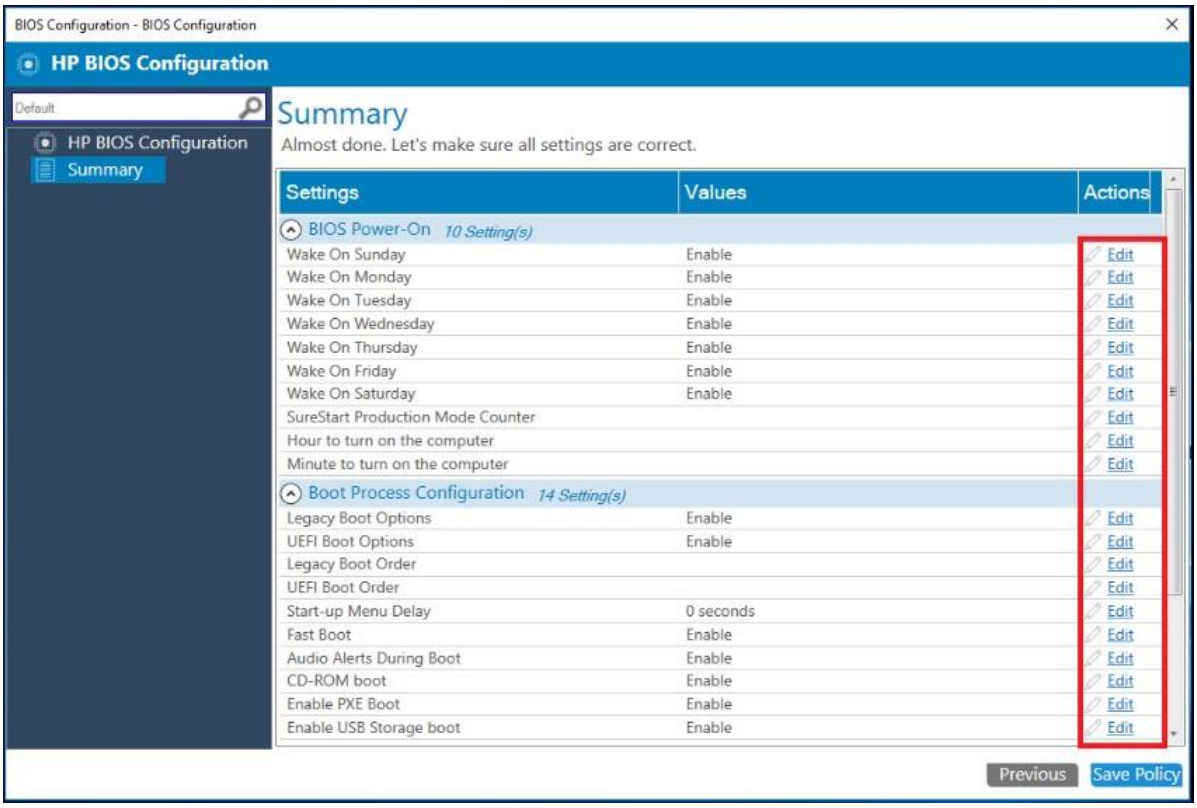


Figure 20 HP BIOS Configuration (Filter to settings containing)

7.11 ポリシーの作成

1. Configuration Manager で、[資産とコンプライアンス]→[概要]の順に選択します。
2. [HP Manageability Integration Kit]を展開し、[BIOSConfiguration]を右クリックして、[Create Policy]を選択します。
3. ベースライン名を入力して、ポリシー作成ウィザードを起動します。
4. BIOS 設定を選択してから新しい値を選択して、設定を変更します。
5. [Create Policy]を選択します。
6. 概要ページで設定を確認します。変更が必要な場合は[前へ]ボタンをクリックします。問題ない場合は[ポリシーの保存]ボタンをクリックします。



7. ポリシーが正常に保存されたら、[ポリシーの展開]を選択してから、ポリシーを適用するターゲットコレクションを選択します。

8. クライアントコンピュータを再起動して、BIOS 設定が有効になるようにします。

7.12 ポリシーの編集

1. Configuration Manager で、[資産とコンプライアンス]→[概要]の順に選択します。

2. HP Manageability Integration Kit を展開し、 [BIOS Configuration]を右クリックして、[Edit Policy]を選択します。

3. 編集する既存のベースラインポリシーを選択し、[OK]をクリックしてウィザードを続行します。

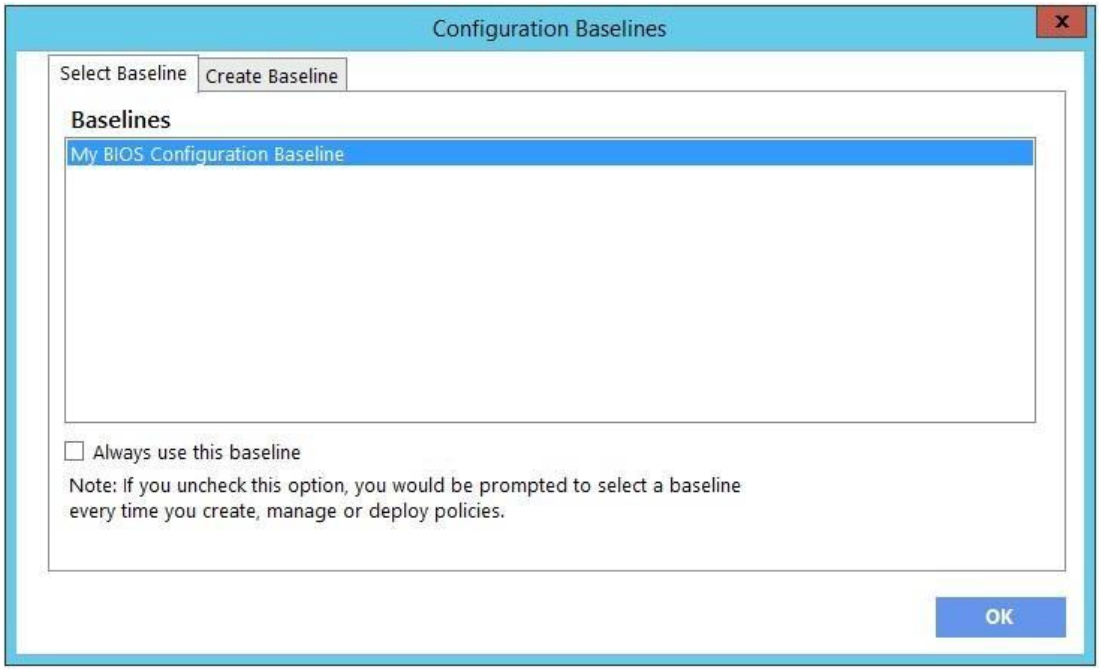


Figure 21 Configuration baseline list

4. ポリシーの作成のステップ 4 から 8 に従います。

注記:
クライアントコンピュータでは、 HP MIK BIOS Configuration ログは %PROGRAMDATA%\HP\HP MIK\Logs フォルダに保存されます。

8 Intel Authenticate をサポートする HP Client Security

Intel ® Authenticate™をサポートする HP Client Security では、Configuration Manager を介して HP Client Security ソフトウェアを管理できます。HP Client Security は、BIOS、ハードウェア、およびソフトウェアの各レイヤーに組み込まれた機能を使用して、攻撃、紛失、または盗難から保護します。また、インテル ® Authenticate™ 機能を利用してセキュリティーをさらに強化することもできます。

8.1 サポートされるクライアントプラットフォーム

- KBL プロセッサを搭載する 2015 年以降の HP コマーシャルコンピュータ
- Intel Authenticate の要件として、ME firmware 11.8.50.3399
- 3 要素認証の要件として、 vPro の有効化
- モダンスタンバイの無効化 – 現時点では、Intel Authenticate は Modern Standby を完全にはサポートしていません。 Intel 認証を使用する場合は、OS でこの機能を無効にしてください。

8.2 サポートされるクライアント OS

- **Windows 10 (Intel® Authenticate™ は Windows 10 のみをサポート)**
- **Windows 8.1**
- **Windows 7**

8.3 その他のクライアントシステムの前提条件

- **Microsoft .NET Framework 4.6.1** 以上
- **HP Client Security Manager 9.3.10.2571** 以上
- **The HP Device Access Manager 8.4.12.0** 以上
- **Intel Authenticate Engine 3.0.0.78 (**任意**)**

注記: Intel ® Authenticate™エンジンは、Intel ® Authenticate™の強化されたセキュリティ機能を利用するために必要であり、以下の追加ドライバが必要です。

– Intel Management Engine Driver 11.6.0.1019 以上

– Intel Bluetooth ® Driver 19.00.1626.3453 以上

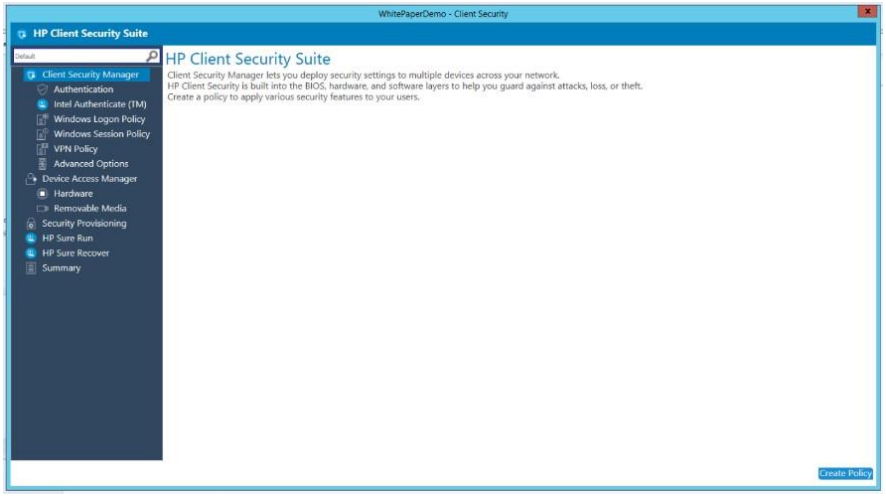
– Intel Graphics Driver 21.20.16.4481 以上 - Intel Authenticate は Intel グラフィックカードの使用を必要とします。PC に複数のグラフィックスソリューションがある場合は、Intel Authenticate PTD PIN 認証に Intel グラフィックスを使用する必要があります。

– Synaptics Touch Fingerprint Driver 5.5.6.1099 以上 (スワイプセンサーはサポートされません)

8.4 ユーザーインターフェース

HP Client Security には Client Security Manager、 Device Access Manager、 Sure Run、Sure Recover が含まれます。

HP Client Security を開くと、プラグインの概要説明が表示されます。ポリシーの作成を選択します。新しいポリシーベースラインに名前を付け、新しいベースラインを選択し、必要な BIOS パスワードを入力するように求められます（HP BIOS Password Manager を参照）。



8.5 Client Security Manager

8.5.1 Authentication

このページでは、HP Client Security Manager の認証オプションを設定できます。

Figure 22 Configure high-level features of HP Client Security Manager

以下の認証オプションを設定できます。

- Windows のログオン—Windows ログオン時に認証を要求します。（OS の起動後）
- Power On Authentication—コンピュータの起動時、OS の起動前に認証を要求します。
- ワンステップログオン—最初のログオンプロンプトで 1 回のみ認証を要求します。Power-On Authentication を有効にする必要があります。
  （Intel ® Authenticate™を使用する場合、セキュリティレベルを高めるためにワンステップログオンはサポートされません。）
- HP Password Manager—パスワードを忘れた場合、または認証デバイスを紛失した場合にセキュリティの質問を使用して安全なログオンを許可します。

8.5.2 Intel Authenticate

クライアントコンピュータに Intel Authenticate Engine がインストールされている場合、このページで Intel Authenticate を設定できます。

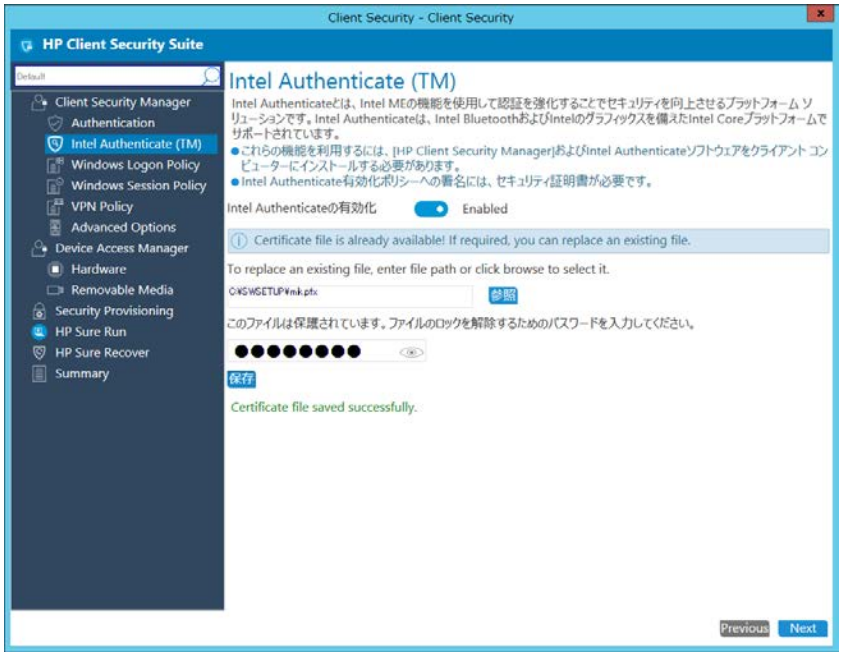


Figure 23 Configure Intel Authenticate

以下のオプションを設定できます。

- Intel Authenticate の有効化—Intel Authenticate サポートを有効にします。Intel Authenticate では、ポリシーを適用するコレクション内のすべてのコンピュータで特定のハードウェアおよびソフトウェアの前提条件が満たされている必要があります。また、AMD プロセッサでは使用する事ができませんので、Intel Authenticate の最小条件を満たすデバイスコレクションを別途作成する必要があります。Authenticate_Check.exe を使用して、コンピュータが最小要件を満たしているかどうかを判断できます。Authenticate_Check.exe の最小要件と使用方法に関する情報は、HP Manageability ウェブサイトの Intel Authenticate Engine に付属の “Intel(R) Authenticate OEM Bring Up Guide” から入手できます。このオプションが有効になっている場合は、クライアントコンピュータの Intel Authenticate Engine とのプロビジョニングや通信に使用する証明書を選択できます。
- Type the location of the security certificate—参照ボタンをクリックして Personal Information Exchange (PFX) フォーマットの X.509 証明書ファイルを選択します。（ファイルは別途用意する必要があります）
- ファイルのロックを解除するためのパスワードを入力してください。—証明書がパスワードで保護されている場合はこのオプションを選択してパスワードを入力します。

8.5.3 Windows Logon Policy

このページでは、Windows ログオン認証を設定できます。

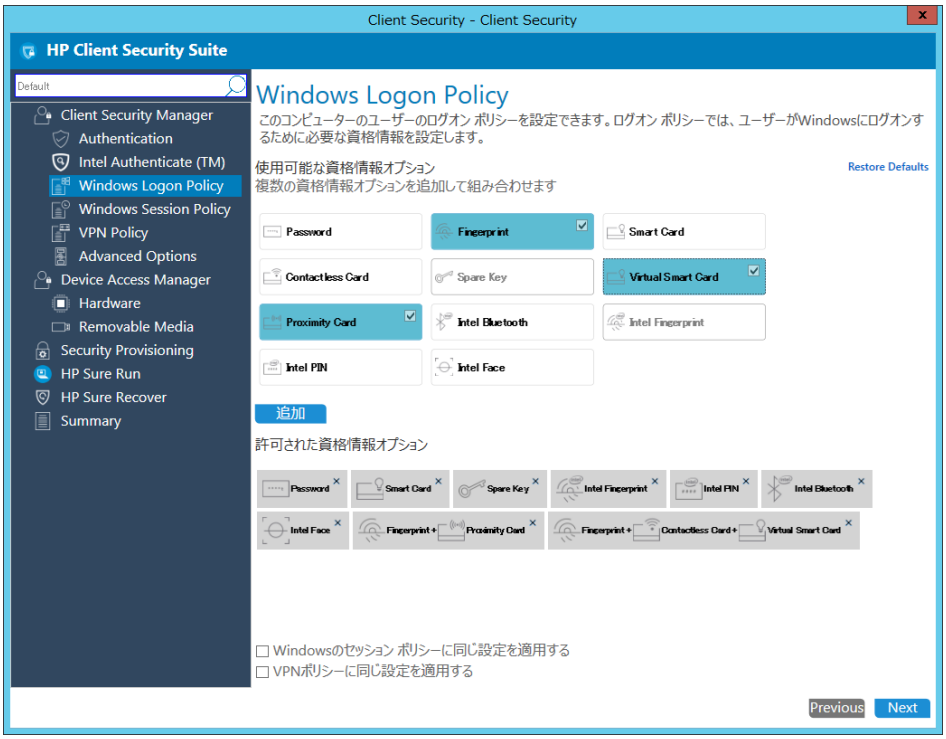
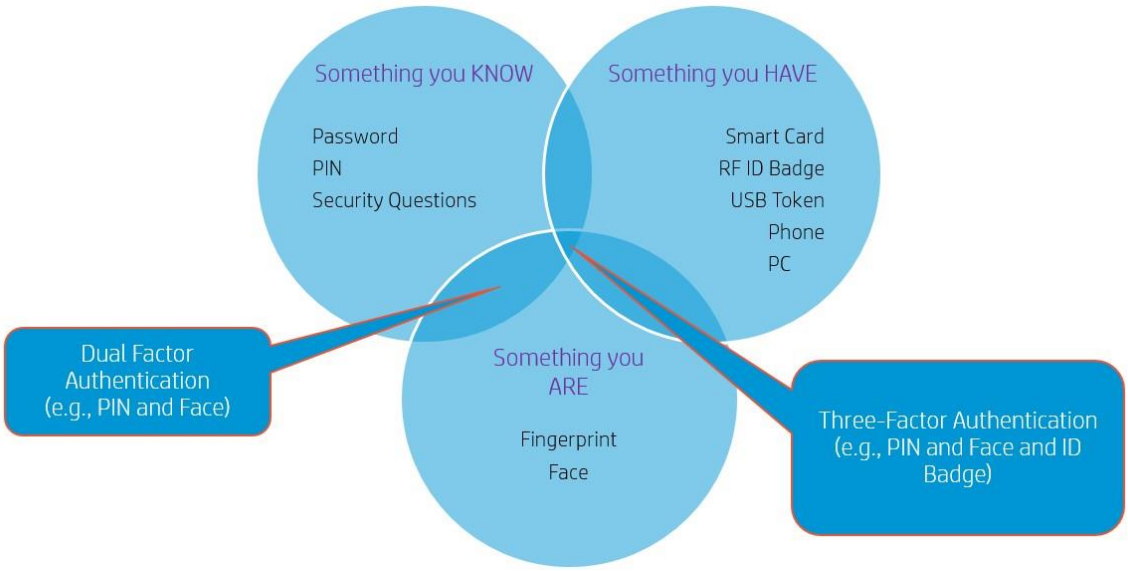


Figure 24 Configure Windows Logon authentication

- 使用可能な資格情報オプション— Windows ログオンに必要な資格情報、または 2 つまたは 3 つの資格情報の組み合わせ（3 要素認証ではクライアントコンピュータで vPro を有効にする必要があります）を選択します。設定した認証情報を削除するには、認証情報の右上隅にある[X]アイコンを選択します。各資格情報は 1 つの組み合わせでのみ使用できます。

- 注記: Intel Authenticate フィンガープリントと従来の Fingerprint の両方を許可する場合は、両方のポリシーを一致させる必要があります。たとえば、Intel Fingerprint とパスワードを組み合わせる場合は、従来の Fingerprint もパスワードと組み合わせる必要があります。
- Intel Authenticate Bluetooth を許可する場合は、次の点に注意してください。Intel Authenticate アプリケーションは、Android または iOS 用の適切なストアからダウンロードする必要があります。 BLE を介して電話機を強制的にペアリングするには、電話機をコンピュータにペアリングしている間にアプリケーションを開く必要があります。 (Intel Authenticate Bluetooth Pairing Steps の文書を参照してください) また、このガイドの執筆時点では、認証しようとしたときに IPhone が error31 または error35 を受け取るという問題がいくつか報告されています。この問題があなたの環境で修正されるかテストされるまでは、Intel Authenticate Bluetooth による認証を許可する場合、Bluetooth が失敗した場合には別の認証情報も許可されることが推奨されます。
- 認証に Intel Authenticate Fingerprint の使用を許可している場合、インターネット接続が利用できない場合、一部のセンサーがタイムアウトして認証されないことが報告されています。これを解決するには、タッチエリア指紋センサーリーダーに最新のドライバがあることを確認してください。前提条件のセクションをご覧ください。
- この記事の執筆時点では、Intel Authenticate はデバイスごとに 1 人のユーザーしかサポートしていません。これは 2018 年末の将来のリリースで強化される予定です。複数のユーザーがコンピュータにログインしようとしている場合は、Intel 認証を有効にしないことをお勧めします。

- Restore Default—デフォルト設定を復元し、既知の状態から設定を開始する方法を提供します。
- Windows のセッション ポリシーに同じ設定を適用する – このページの設定を Windows Session ページに自動的に適用します。
- VPN ポリシーに同じ設定を適用する – このページの設定を VPN ポリシーページに自動的に適用します。
- ポリシー作成の提案: ポリシーを作成するときは、3 種類の認証方法を覚えておいてください。これらの要素には、あなたが知っているもの（パスワード/PIN）、あなた自身（指紋/顔）、そしてあなたが持っているもの（電話/非接触カード）が含まれます。これらの項目を認証に使用することを許可する場合は、最高のセキュリティを確保するために各種類の要素から 1 つを組み合わせることをお勧めします。Bluetooth 電話など、自分の持っているものでポリシーを作成するときは、認証項目にアクセスできない場合に備えて別の認証方法を許可しておくことをお勧めします。



8.5.4 Windows Session Policy と VPN Policy

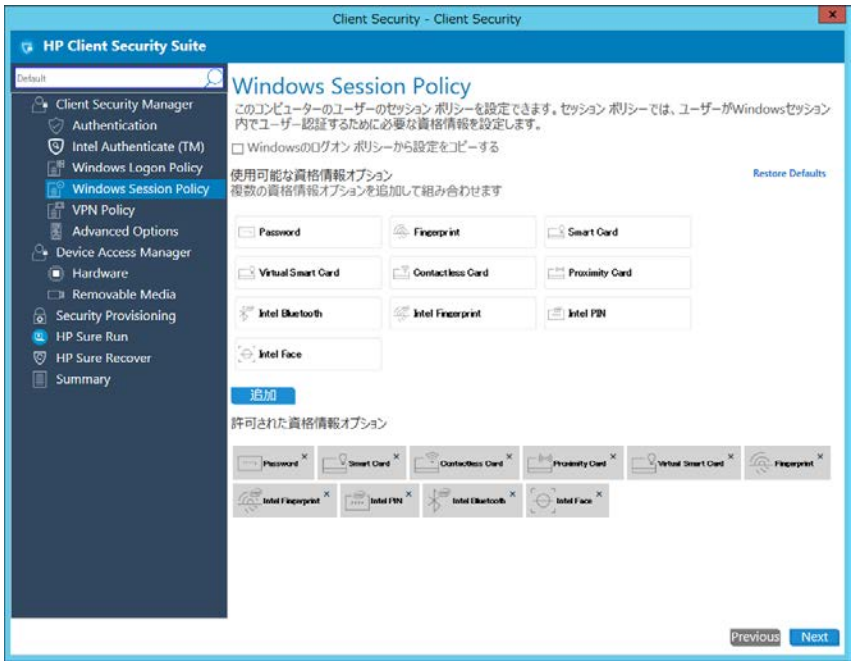


Figure 25 Configure policy and credentials for Windows sessions and VPN policies

このページでは、Windows セッションに使用されるポリシーと認証情報を設定できます。これは、Password Manager や Device Access Manager などのアプリケーションで認証するためのものです。 次のページでは、VPN 認証に使用されるポリシーを設定できます。 Intel Authenticate で認証するように VPN 環境を設定する方法については、VPN_Setup_Instructions という文書を参照してください。

- Windows のログオンポリシーから設定をコピーする—ログオンポリシーから設定を自動的にコピーします。
- 使用可能な資格情報オプション— 使用を許可する 1 つの資格情報、または 2 つまたは 3 つの資格情報の組み合わせ（3 要素認証ではクライアントコンピュータで vPro を有効にする必要があります）を選択します。

8.5.5 Advanced Options

このページでは、HP Client Security によって管理されるさまざまな認証情報の詳細を構成できます。

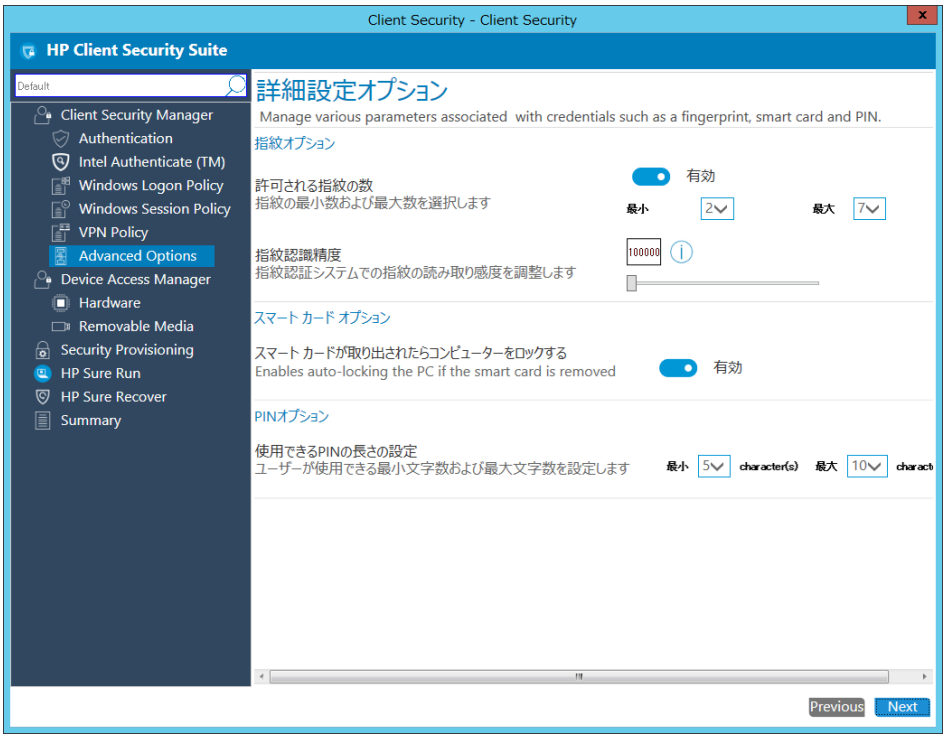


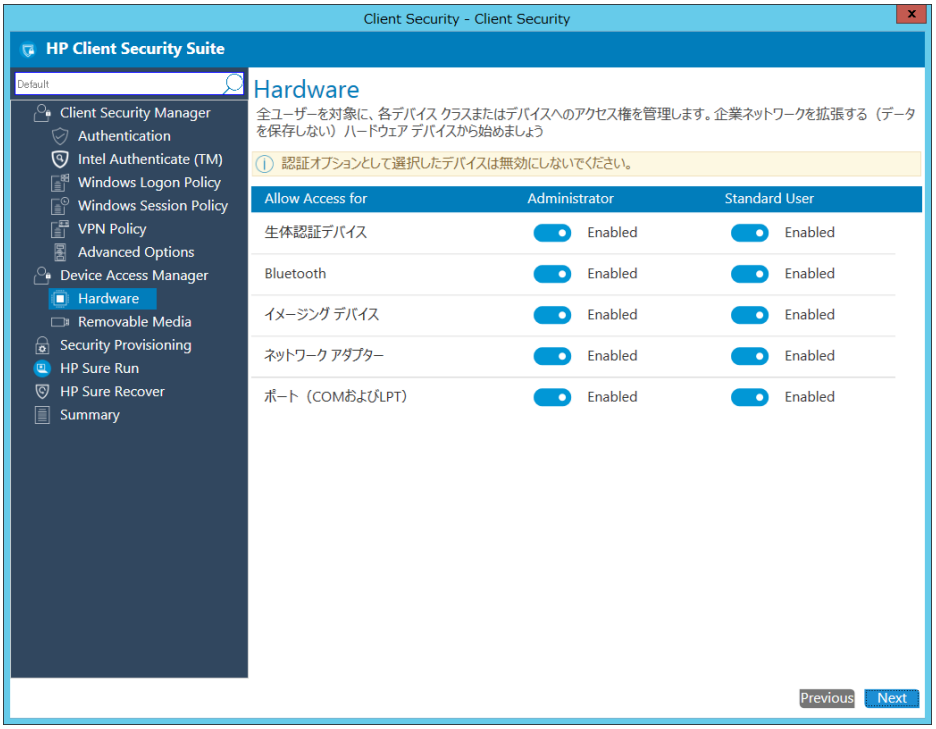
Figure 26 Configure Advanced Options

- 指紋オプション
  - 指紋の最小数および最大数を選択します—登録可能な指紋の最小値と最大値を指定します。登録する指紋の数を強制する必要があります。
  - 指紋認識精度—指紋リーダーの精度を調整します。（Intel Authenticate Fingerprint ではサポートされません）

- ・スマートカードオプション
  - – スマートカードが取り出されたらコンピュータをロックする—資格情報として使用されているスマートカードが取り出されると、コンピュータを自動的にロックします。
- ・PIN オプション
  - – 使用できる PIN の長さの設定—ユーザーが PIN に使用できる文字の最小値と最大値を設定します。（Intel Authenticate PIN ではサポートされません）

8.6 Device Access Manager

8.6.1 Hardware

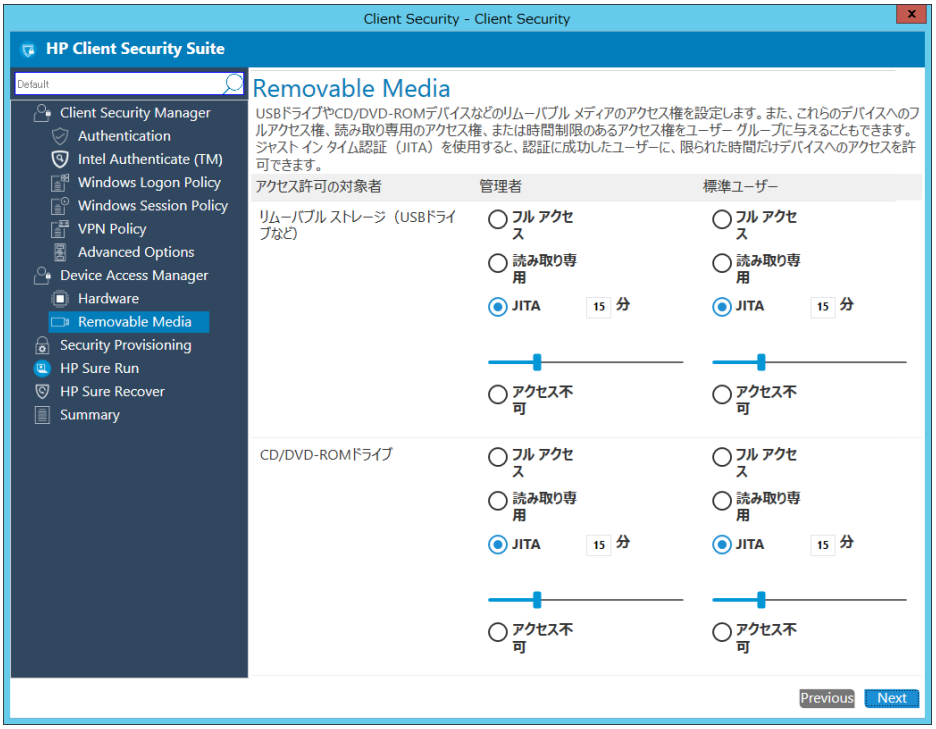


このページでは、さまざまなデバイスクラスまたはデバイスに対するアクセス許可を展開できます。アクセス許可は管理者と標準ユーザーの両方に設定できます。以下のデバイスクラスとデバイスがリストされています。

: 生体認証デバイス、Bluetooth、イメージング デバイス、ネットワーク アダプター、ポート（COM および LPT）

- Allow Access for Administrators—管理者がデバイスクラスやデバイスにアクセスできるようにします。
- Allow Access for Standard User—標準ユーザーがデバイスクラスやデバイスにアクセスできるようにします。

8.6.2 Removable Media



このページでは、IT 管理者が USB ドライブや CD / DVD-ROM ドライブなどのリムーバブルストレージに対するアクセス許可を設定できます。リムーバブルメディアオプションを設定します。

オプションは、管理者と標準ユーザーの両方に対して、それぞれ次のいずれかの権限で構成できます。

- フル アクセス—選択したリムーバブルメディアからファイルを追加、編集、削除、および読み取りすることをユーザーに許可します。
- 読み取り専用—選択したリムーバブルメディアから読み取りのみをユーザーに許可します。
- JITA (Just In Time Authentication)—ユーザーが自分の資格情報を入力した後、ドロップダウンボックスで指定した時間の間、追加、編集、削除、および読み取りすることをユーザーに許可します。
- アクセス不可—選択したリムーバブルメディアで利用可能なファイルへのユーザーアクセスを無効にします。

8.7 ポリシーの作成

1. Configuration Manager で、[資産とコンプライアンス]→[概要]の順に選択します。
2. [HP Manageability Integration Kit]を選択し、[Client Security Manager]を右クリックして、[Create Policy]を選択します。
3. ベースライン名を入力してポリシー作成ウィザードを起動します。
4. 設定を編集し、[Next]をクリックします。

5. Summary ページで設定を確認します。変更が必要な場合は[Previous]ボタンで前の画面に戻ります。問題ない場合は[ポリシーの保存]をクリックします。

Figure 27 Review Summary

6. ポリシーが正常に保存されたら、[ポリシーの展開]を選択してから、ポリシーを適用するターゲットコレクションを選択します。

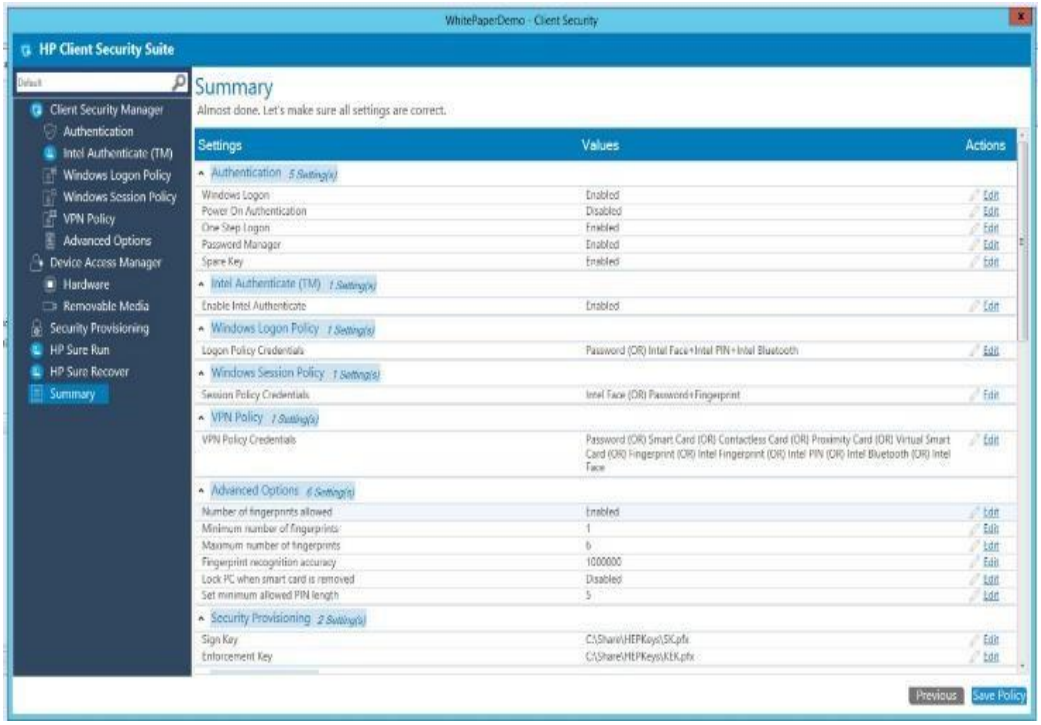
8.8 ポリシーの編集

1. Configuration Manager で、[資産とコンプライアンス]→[概要]の順に選択します。
2. [HP Manageability Integration Kit]を選択し、[Client Security Manager]を右クリックして、[Edit Policy]を選択します。
3. 編集する既存のベースラインポリシーを選択し、[OK]をクリックしてウィザードを続行します。
4. 画面の指示に従ってウィザードを完了します。

8.9 補足情報

HP Client Security で作成されたポリシーは、Client Security Manager と Device Access Manager の両方の構成項目を作成します。

Intel Authenticate を使用する場合は、ポリシーを作成する前に必ず Intel Authenticate を設定してください。お使いのコンピュータがサポートされているかどうか、および Intel Authenticate の設定方法について詳しくは、Intel Authenticate のマニュアルを参照してください。



8.10 Security Provisioning

HP Sure Run と HP Sure Recover を有効化するためにリモート管理システムを構成する必要があります。

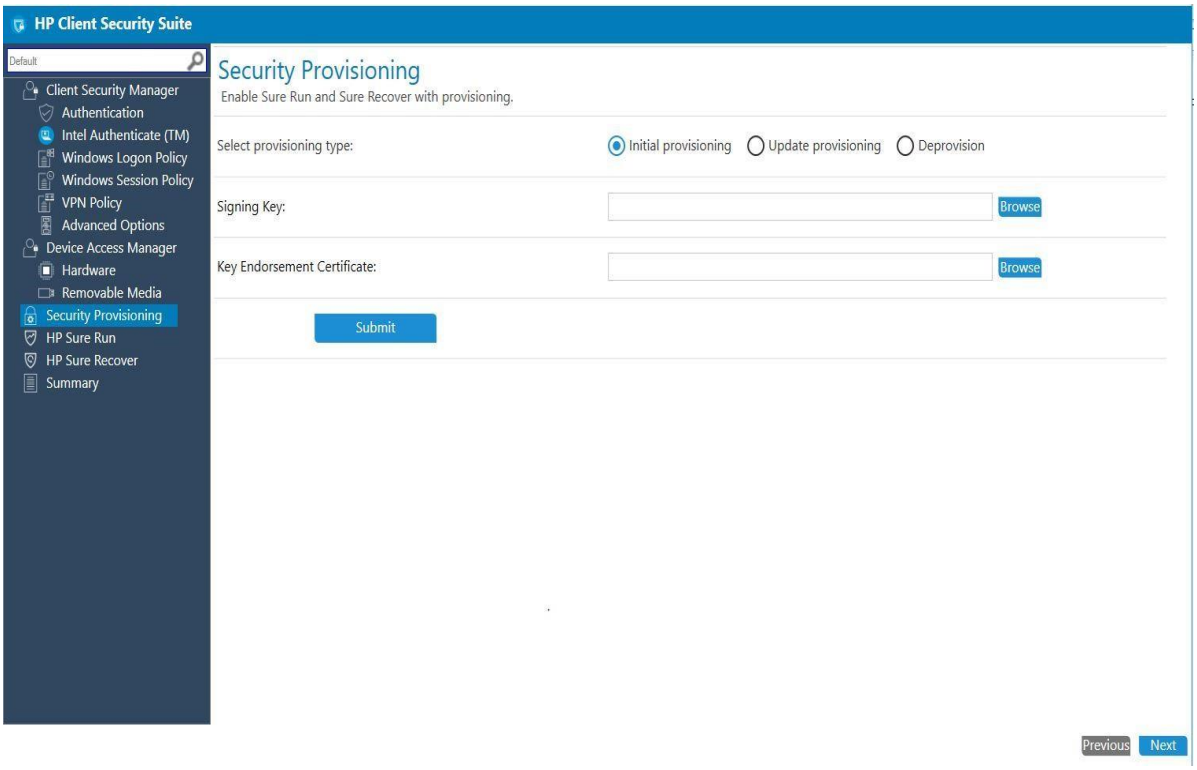
HP Sure Run と HP Sure Recover は公開鍵と秘密鍵のペアを使用する暗号検証済みコマンドを使用して管理されます。以下の手順では、2 つの別々の鍵ペアを設定します。

- 送信する設定に署名するために使用される秘密鍵を含む鍵ペアである「署名鍵」
- 秘密鍵が「署名鍵」の更新に署名するためにのみ使用される「鍵承認証明書」内に埋め込まれている鍵ペア。クライアントシステムは、プロビジョニング後の最初の起動時に、この証明書に指定されている組織文字列も表示します。

このプロビジョニングは通常一度だけ行われ、公開鍵は将来の HP Sure Run および HP Sure Recover コマンドの署名検証に使用する鍵としてクライアントシステムに送信されます。

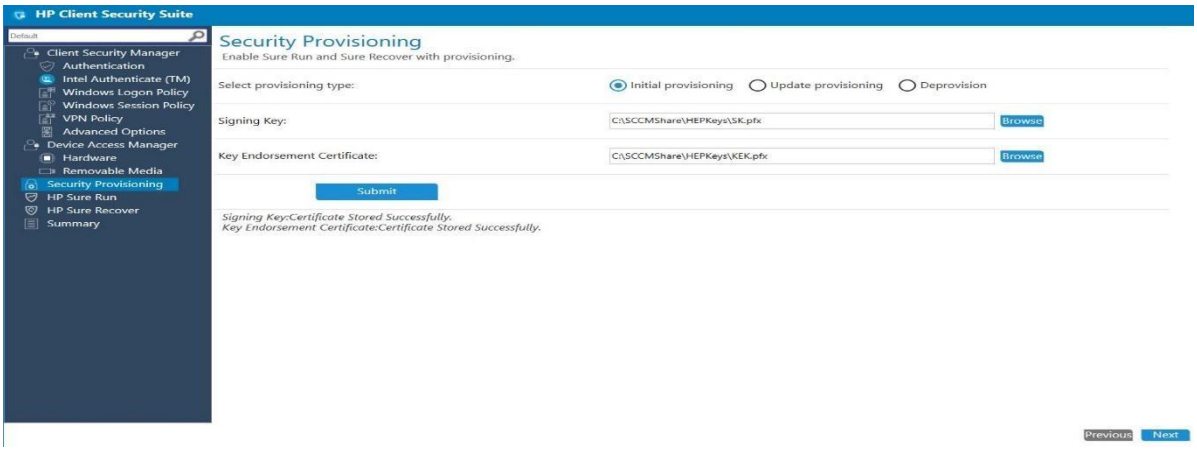
8.10.1 初期プロビジョニングまたはプロビジョニングの更新

8.10.1.1 初期プロビジョニング – 初回のセットアップのためのシステム設定



エンドユーザーは、初期プロビジョニングのために署名鍵と鍵承認証明書の両方を用意する必要があります。テキストフィールドの横にある[参照]オプションをクリックして、ローカルディスクに保存されているキー/証明書を選択します。

選択したら[送信]を選択し、[次へ]をクリックします。 - サポートされているキーフォーマットは Personal Information Exchange（PFX）です。



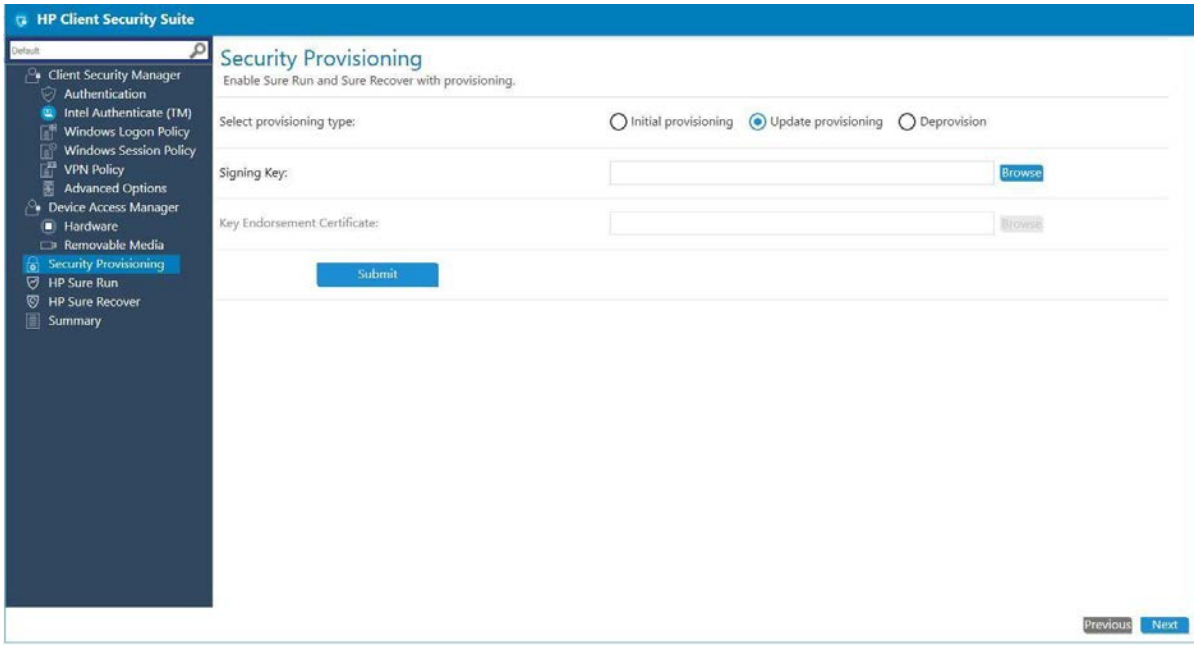
8.10.1.2 プロビジョニングの更新

上記ですでにプロビジョニングされているシステムを修正するために、IT 管理者は更新された署名キーを使用して再プロビジョニングすることができます。

Security Provisioing に移動して、[プロビジョニングの更新]オプションを選択します。

管理者は更新プロビジョニング用の署名キーを提供する必要があります。テキストフィールドの横にある[参照]オプションをクリックして、ローカルディスクに保存されているキーを選択します。

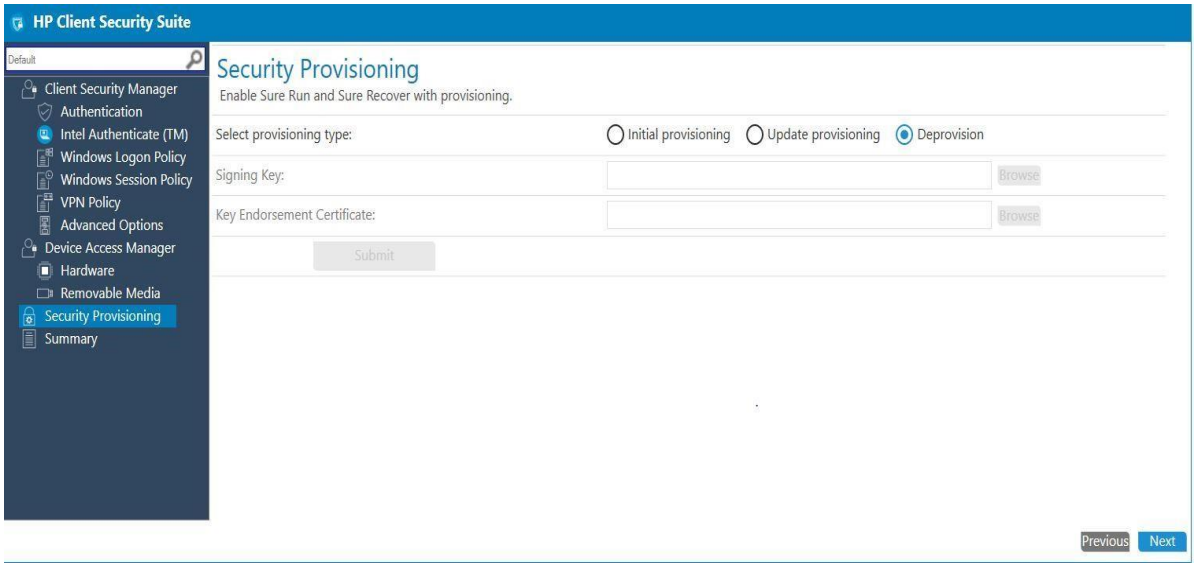
選択したら[送信]を選択し、[次へ]をクリックします。



8.10.2 プロビジョニング解除

すでにプロビジョニングされているシステムを修正するために、IT 管理者はシステムのプロビジョニングを解除することができます。

Security Provisioing に移動して、[プロビジョニング解除]オプションを選択します。[次へ]をクリックしてプロビジョニングを解除します。



以前にプロビジョニングされたシステムのプロビジョニングを解除している間、HP Sure Run および HP Sure Recover の機能は、ポリシーのプッシュの一環として自動的に無効になります。

8.10.3 補足情報

8.10.3.1 クライアントシステムを正常にプロビジョニングするには

1. ポリシー展開後にクライアントシステムを 1 回再起動する必要があります。

2. 再起動後、エンドユーザーは起動時に画面に表示される 4 桁のセキュリティコードを入力するよう求められます。

3. IT 管理者は、プロビジョニングに必要な鍵が安全な場所に保存されていることを確認する必要があります。署名鍵は HP Sure Run または HP Sure Recover の設定を変更するたびに使用されます。鍵保証証明書は、署名鍵の更新が必要な場合にのみ使用されます。

8.10.3.2 すでにプロビジョニングされているシステムのプロビジョニングの更新

署名鍵と Key Endorsement 証明書の両方を更新するには、管理者は最初にプロビジョニングを解除して初期プロビジョニングを再度実行する必要があります。

署名鍵の秘密鍵が危険にさらされた場合は、[プロビジョニングの更新]オプションを選択して新しい署名鍵を選択してから[次へ]をクリックすることで置き換える事ができます。

注記: 鍵承認証明書の秘密鍵が危険にさらされた場合、それを置き換えるために使用される方法はクライアントシステム上の署名鍵の秘密の半分の状態に依存します。

- クライアントシステムで署名鍵が置き換えられていない場合は、プロビジョニング解除を実行し、新しい署名鍵ペアと新しい鍵承認証明書を使用して最初のプロビジョニングを再度実行します。すべてのシステムが正常に更新されたことを確認することが重要です。
- クライアントシステムで署名キーが置き換えられた場合は、BIOS F10 セットアップの[Secure Platform Management]メニューの[Unprovision SPM]オプションを使用する必要があります（このオプションはリモートでは使用できません）。

8.10.3.3 クライアントシステムを正常にプロビジョニング解除するには

1. プロビジョニング解除を成功させるためには、SCCM 内で複数回の[評価]試行が必要な場合があります。

2. 最初に HP Sure Run や HP Sure Recover を無効にするポリシーを送信してから、続いてプロビジョニング解除のポリシーを送信する事をお勧めします。

8.10.3.4 プロビジョニング解除に失敗するシステム

HP Sure Run / HP Sure Recover は、先着順で、ローカル（HP Client Security Manager）またはリモート（MIK）の方法でのみ管理できます。これらの方法のいずれかを使用して有効にして設定すると、もう一方は、その設定が解除されて無効になるまで使用できなくなります。無効化は、BIOS F10 セットアップの[Secure Platform Management]メニューの[Unprovision SPM]オプションを使用して実行できます（このオプションはリモートでは使用できません）。

8.10.3.5 署名鍵または鍵承認証明書を紛失した場合の対処方法

BIOS F10 セットアップの[Secure Platform Management]メニューの[Unprovision SPM]オプションを使用して、HP Sure Run と HP Sure Recover を手動でプロビジョニング解除することができます（このオプションはリモートでは使用できません）。

8.10.3.6 BIOS 管理者パスワード

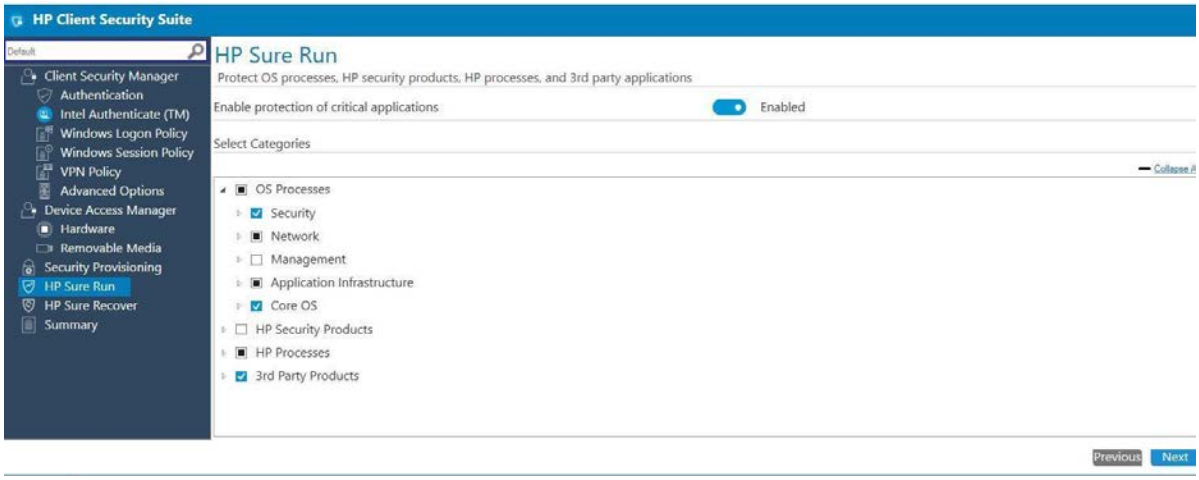
BIOS 管理者パスワードは、HP Sure Run または HP Sure Recover の使用に必須ではありませんが、物理的にアクセスできる攻撃者が HP コンピューター（BIOS）セットアップページで HP Sure Run を無効にできないようにするために BIOS 管理者パスワードを使用することをお勧めします。

8.11 HP Sure Run

8.11.1 概要

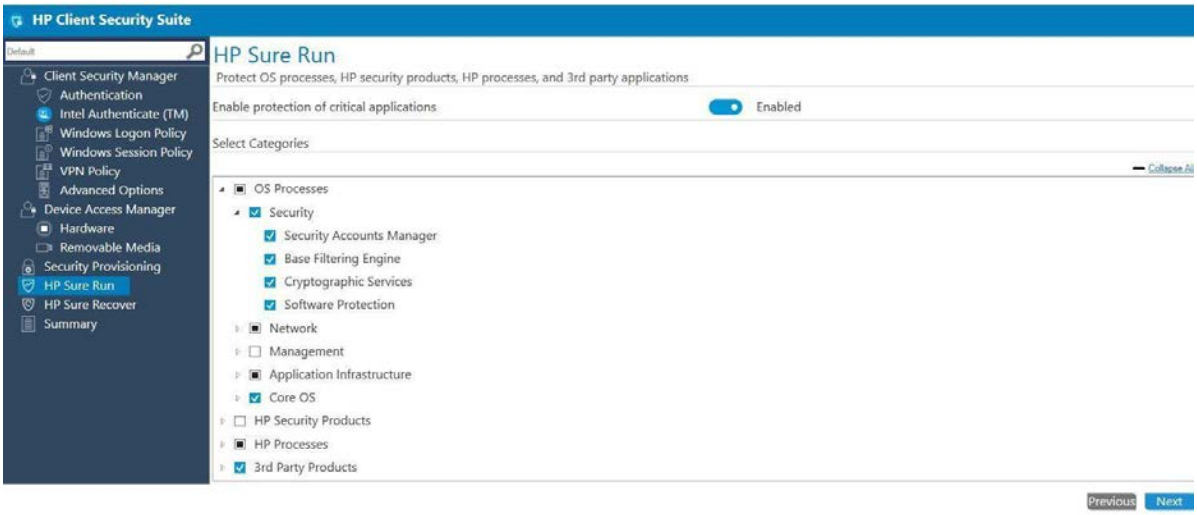
HP Sure Run は、外部からの脅威に備えて重要なアプリケーションを監視し、ユーザーに警告するのに役立ちます。

HP Sure Run では、監視対象とする個々のアプリケーションまたはアプリケーションカテゴリを選択できます。

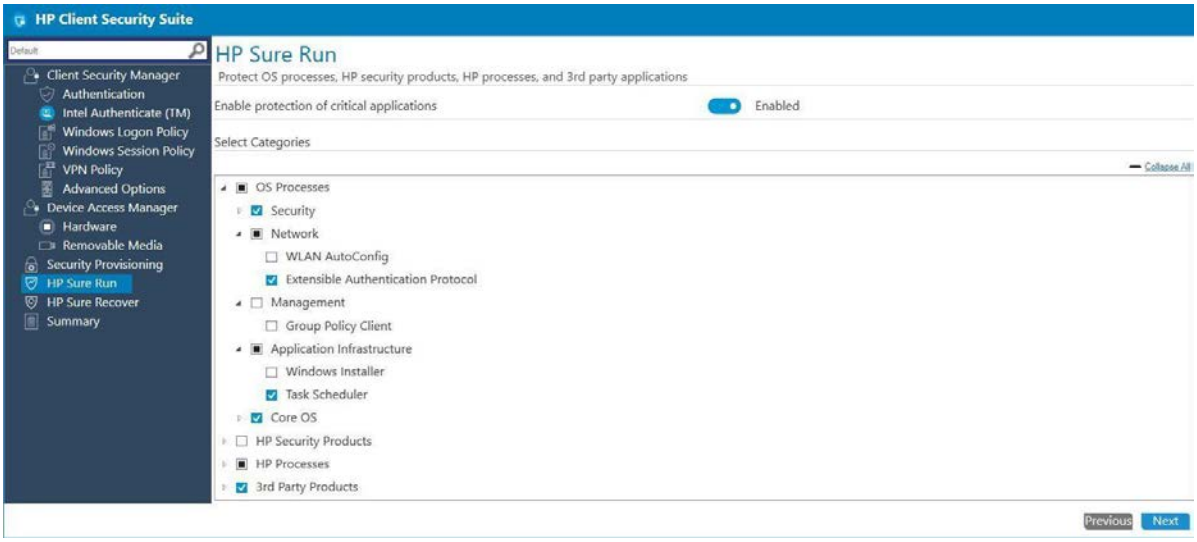


IT 管理者は、HP が推奨する事前選択されたポリシーを必要に応じて変更する事ができます。以下に、監視対象として選択できるカテゴリとサブカテゴリを示します。

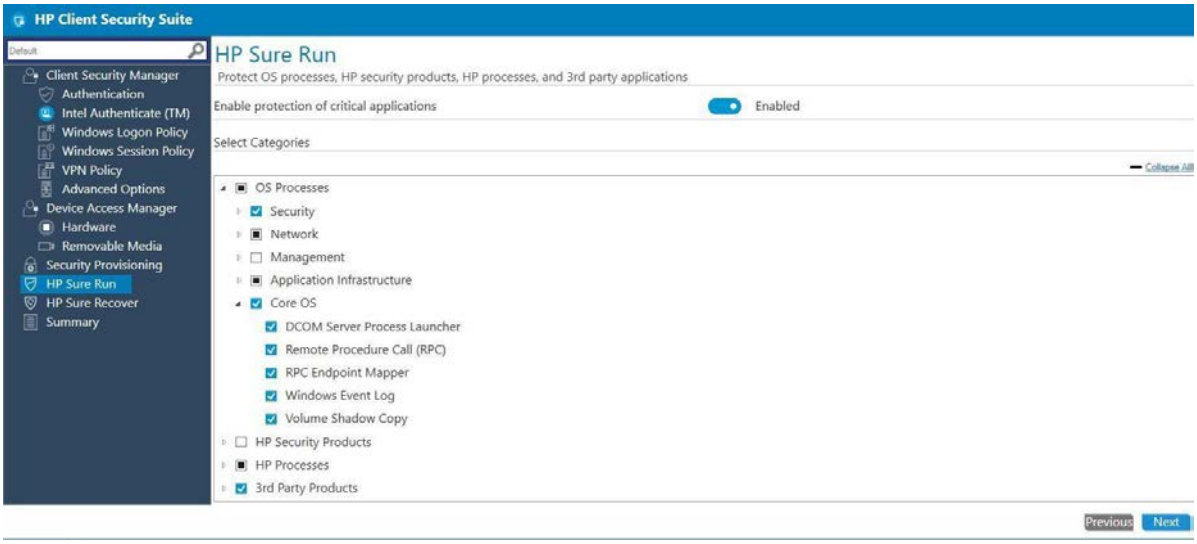
OS Processes – サブカテゴリ “Security”



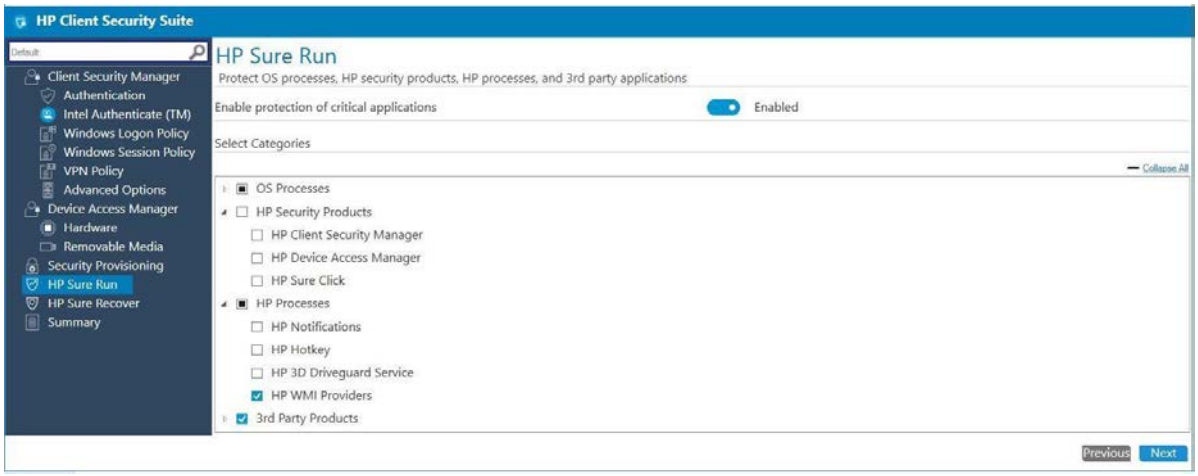
OS Processes – サブカテゴリ “Network” / “Management” / “Application Infrastructure”



OS Processes – サブカテゴリ “Core OS”

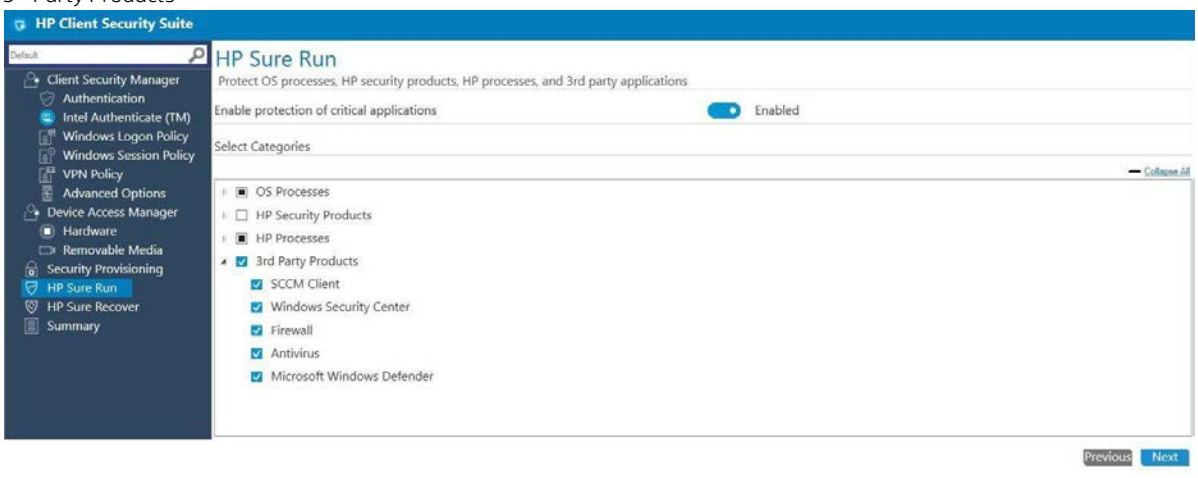


HP Products / HP Processes



HP Client Security with Intel Authenticate Support

3rd Party Products



8.11.3 サポートされるクライアントプラットフォーム

- HP コマーシャル PC – Intel (KBL-R 搭載、800 シリーズ以上) 、 AMD (Ryzen 搭載 、700 シリーズ)

8.11.4 サポートされるクライアント OS

- Windows 10 RS3 以上

8.11.5 その他のクライアントシステムの要件

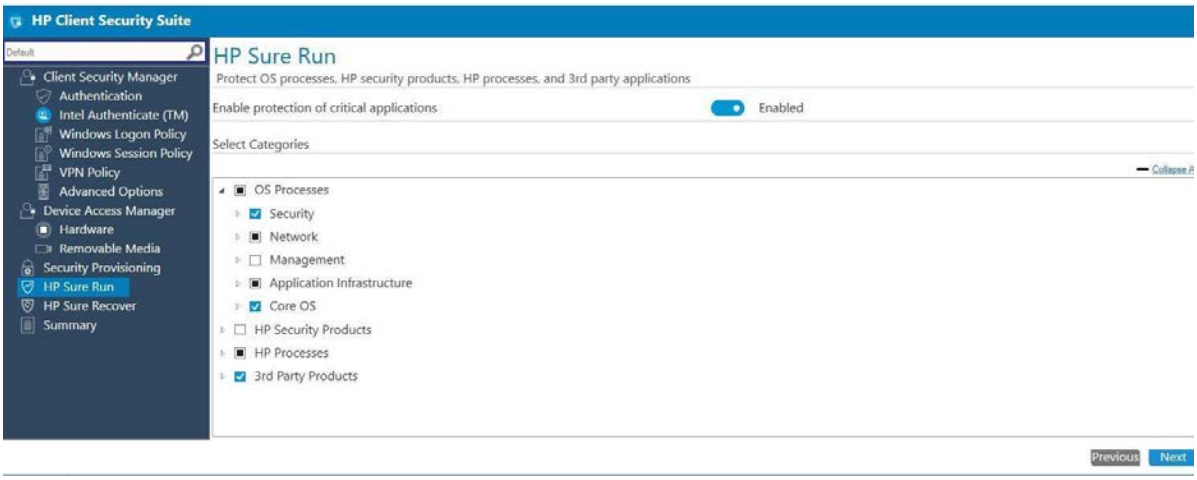
- **Microsoft .NET Framework 4.6.1** 以上
- **HP Client Security Manager 9.3.11.XXXX** 以上
- **HP MIK Client v2.0.18.1** 以上

8.11.6 前提条件

すべてのクライアントシステムは HP Sure Run ポリシーが適用されるようにプロビジョニングされていること。詳細については Security Provisioning のセクションをご参照ください。

8.11.7 ポリシーの作成

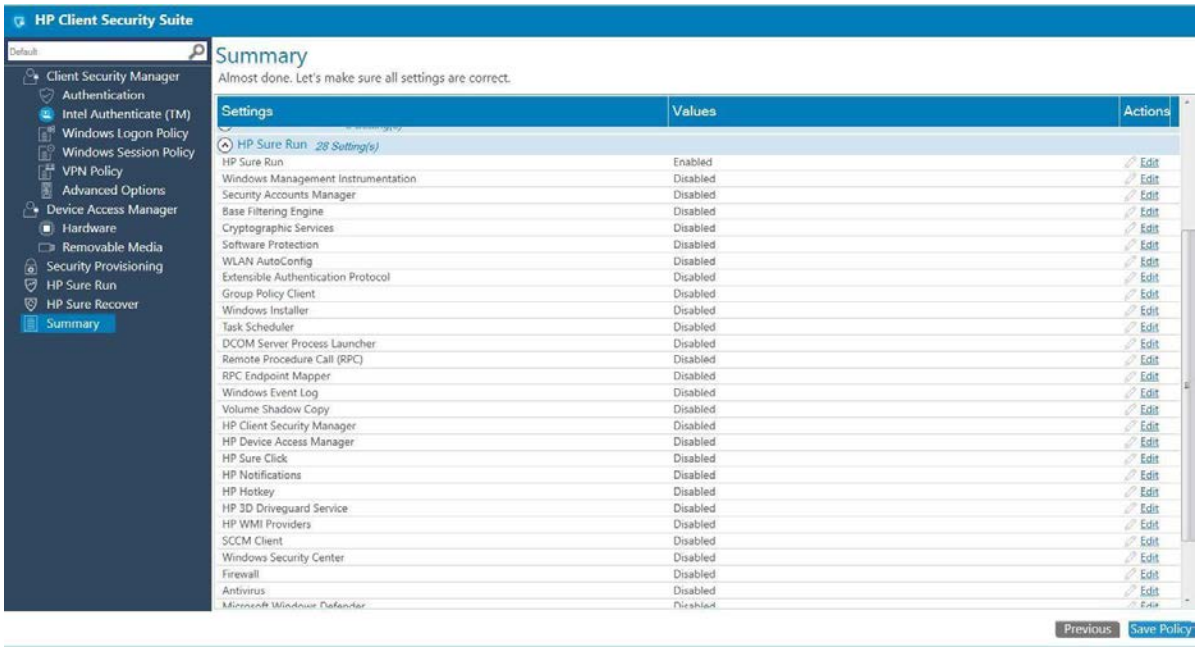
1. Configuration Manager で、[資産とコンプライアンス]→[概要]の順に選択します。
2. [HP Manageability Integration Kit]を選択し、[Client Security Manager]を右クリックして、[Create Policy]を選択します。
3. ベースライン名を入力してポリシー作成ウィザードを起動します。
4. [HP Sure Run]ページに移動します。初期値を確認し、必要があれば変更してから[Next]をクリックします。



5. 概要ページの HP Sure Run セクションで、選択したサブカテゴリの最終確認と変更ができます。いずれかのサブカテゴリの[編集]をクリックすると、ポリシー更新のために HP Sure Run ページが再度開きます。

6. [ポリシーの保存]をクリックします。

7. ポリシーが正常に保存されたら、[ポリシーの展開]を選択してから、ポリシーを適用するターゲットコレクションを選択します。



8.11.8 補足情報

1. ポリシーを正しく適用するために、クライアントシステムを再起動する必要があります。ポリシーの展開に失敗した場合は、追加の再起動が必要になることがあります。

2. IT 管理者は、選択したアプリケーションがクライアントシステムにインストールされていることを確認する必要があります。それ以外の場合、エンドユーザーにはインストールされていないアプリケーションに対する継続的なトースター通知が表示されます。

3. クライアントシステムで悪意のある活動が発生した場合以下が起こります

    o エンドユーザーにトースターポップアップが表示されます。

    o 同じ HP Sure Run メッセージが Windows イベントビューアに

    記録される 。

8.11.8.1 保護されているアプリケーションのアンインストール

保護されたアプリケーションが不要になった場合、アンインストールする前に HP Sure Run の設定を変更して、そのアプリケーションを監視リストから削除する必要があります。

8.11.8.2 HP Sure Run と HP Sure Recovery の相互関係

HP Sure Recover を使用して OS のリカバリを実行した場合は、リカバリ処理後に HP Sure Run が自動的に無効になるため、再度有効にする必要があります。

8.11.8.3 TPM をリセットまたはクリアすると HP Sure Run が停止します

HP Sure Run は、署名および復号化操作を実行するために TPM 2.0 を使用する必要があります。TPM がリセットまたはクリアされると、HP Sure Run によって作成されたキーは無効になり使用できなくなります。これを解決する唯一の方法は、HP Sure Run を無効にしてから再度有効にすることです。

8.12 HP Sure Recover

8.12.1 概要

HP Sure Recover は、最小限のユーザー操作でネットワークを介して OS / DVD イメージを復元するのに役立ちます。

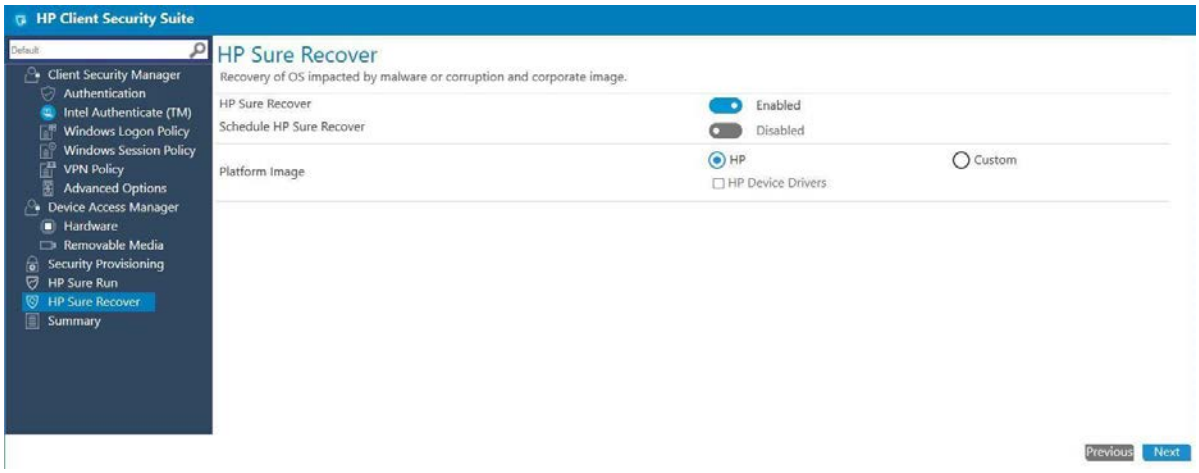
8.12.2 構成

HP Sure Recover ページに移動します。 HP Sure Recover を有効にするには、[有効]を選択します。

IT 管理者は OS イメージをダウンロードする場所として HP の FTP かまたは企業のカスタムの場所を設定できます。

8.12.2.1 HP イメージのリカバリ

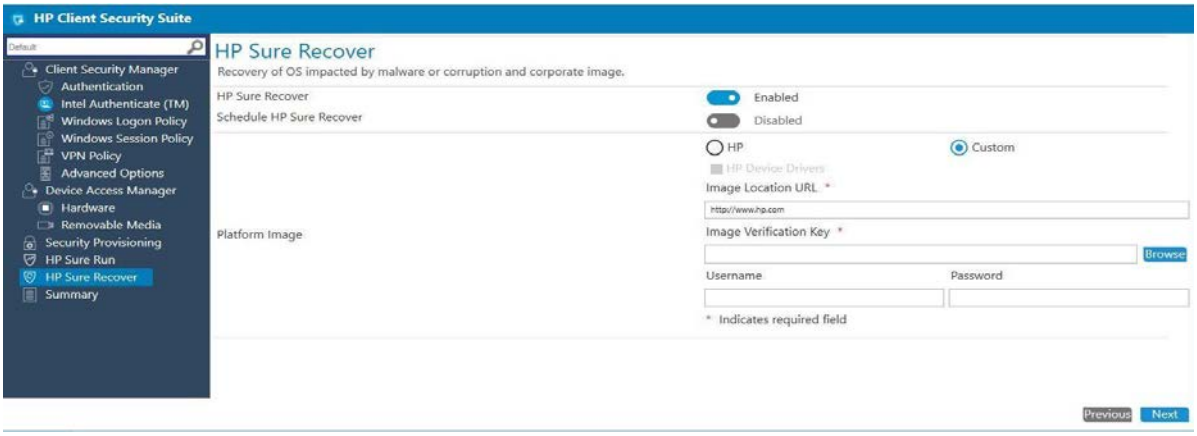
IT 管理者は HP が推奨する事前選択されたポリシーを必要に応じて変更することができます。



HP 推奨の OS（ドライバ付き）イメージのダウンロードからリカバリするには、[HP から入手したイメージ]を選択し、[プラットフォームのドライバー]チェックボックスを選択してください。

8.12.2.2 カスタムのリカバリ

カスタマイズした OS イメージを使用してリカバリするには[Corporation]オプションを選択します。IT 管理者は、イメージのダウンロード元の URL とイメージ検証キーを提供する必要があります。

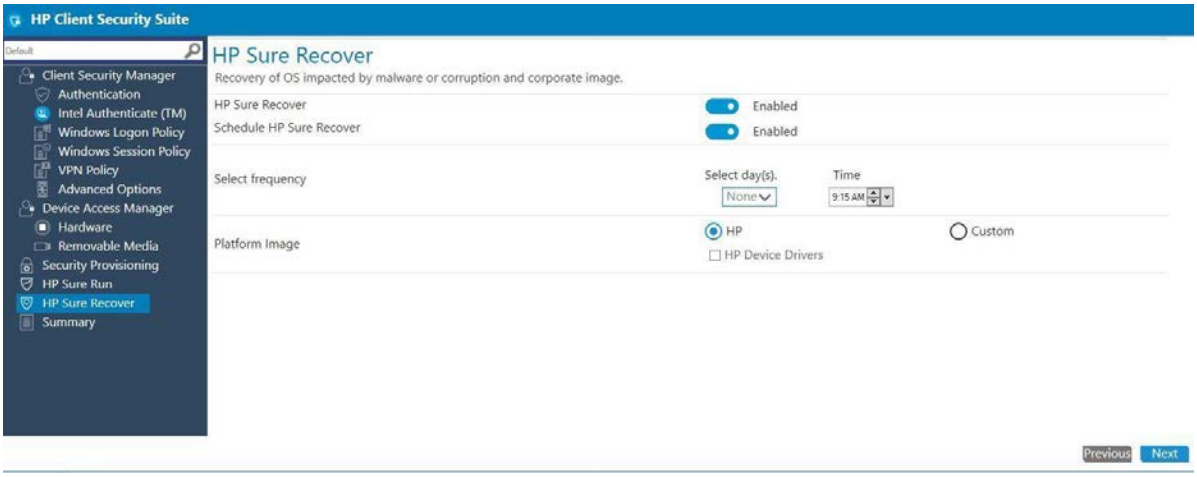


注記

1. FTP と HTTP がサポートされています。
2. FTP/HTTP のアカウント設定によってはユーザー名とパスワードが必要になります。
3. イメージ検証キーのフォーマットとして .pem と .pfx がサポートされています。
4. URL は次の形式にする必要があります。 - 例 ftp://abc.ftp.com/<folder>/<name>.mft
   詳細は#8.12.8 マニュフェストファイル作成方法のための補足情報のセクションをご参照ください。

8.12.2.3 クライアントシステムのリカバリのスケジュール

IT 管理者は[HP Sure Recover のスケジュール]を有効にすることで、管理対象デバイスの OS のリカバリをスケジュールできます。回復は、特定の時間に 1 日または週に複数日にスケジュールすることができます。



8.12.3 サポートされるクライアントプラットフォーム

- HP コマーシャル PC – Intel (KBL-R 搭載、800 シリーズ以上) 、 AMD (Ryzen 搭載 、700 シリーズ)

8.12.4 サポートされるクライアント OS

- Windows 10 RS3 以上

8.12.5 その他のクライアントシステムの要件

- Microsoft .NET Framework 4.6.1 以上
- HP Client Security Manager 9.3.11.XXXX 以上
- HP MIK Client v2.0.18.1 以上

8.12.6 前提条件

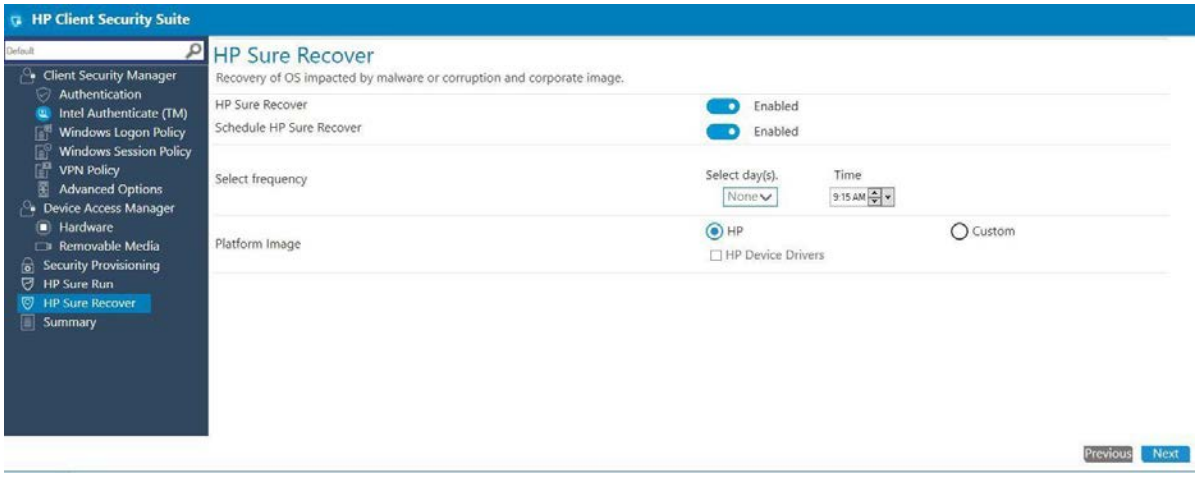
すべてのクライアントシステムは HP Sure Run ポリシーが適用されるようにプロビジョニングされていること。詳細については Security Provisioning のセクションをご参照ください。

8.12.7 ポリシーの作成

1. Configuration Manager で、[HP Manageability Integration Kit]を選択し、[Client Security Manager]を右クリックして、[Create Policy]を選択します。

2. ベースライン名を入力してポリシー作成ウィザードを起動します。

3. HP Sure Recover ページに移動します。初期値を確認し、必要があれば変更してから[Next]をクリックします。



4. 概要ページの HP Sure Run セクションで、最終確認と変更ができます。表示されている項目のいずれかの[編集]をクリックすると、ポリシー更新のために HP Sure Recover ページが再度開きます。

5. [ポリシーの保存]をクリックします。

6. ポリシーが正常に保存されたら、[ポリシーの展開]を選択してから、ポリシーを適用するターゲットコレクションを選択します。

8.12.8 補足情報

1. ポリシーを正しく適用するために、クライアントシステムを再起動する必要があります。ポリシーの展開に失敗した場合は、追加の再起動が必要になることがあります。

2. マニュフェストファイルの作成手順

   a. 前提条件として、sha256sum ツールと Openssl ツールが必要です。

   b. イメージマニュフェストファイルの作成

      カスタムイメージのマニフェストは SHA256SUM.EXE コマンドを使用して作成します。

      例:

      >sha256sum os-drivers.wim > image.mft

      >type image.mft
      8f161eac8d9197088ad8892e5d529b0287b5a9b8604c546e5a66d8737531c1ab *os-drivers.wim

      注記:

      i. sha256sum ツールはフリーソフトをダウンロードできます。

      ii. os-driver.wim の部分は実際の OS イメージ(.wim)ファイル名を指定します。

      iii. 実際に出力されるハッシュ値蒸は上記とは異なります。

   c. マニュフェストファイルへの署名

      RSA 2048 bit 鍵ペアを作成します。

      C:\OpenSSL\bin>openssl.exe dgst -sha256 -sign recovery_private.pem -out image.sig image.mft

      注記:

      i. 使用する署名鍵はプロビジョニング時に使用したものと一致する必要があります。そうしないと、回復プロセスの実行時に認証エラーが発生します。

      ii. openssl ツールはフリーソフトをダウンロードできます。

8.12.8.1 HP Sure Run と HP Sure Recover の相互関係

HP Sure Recover を使用して OS のリカバリを実行した場合は、リカバリ処理後に HP Sure Run が自動的に無効になるため、再度有効にする必要があります。

9 Device Guard (Windows 10 のみ)

Device Guard は Windows 10 に含まれており、アプリケーションとドライバが実行を許可される前に信頼できるソースからのものであることを確認することによって、ハードウェアおよびソフトウェアベースのマルウェア保護を提供します。 HP MIK の Device Guard ポリシーは IT 管理者が Device Guard を有効にするための簡単なオプションを提供します。

9.1 サポートされるクライアントプラットフォーム

・ ・ 2015 年以降の HP コマーシャルコンピュータ

9.2 サポートされるクライアント OS

・ ・ Windows 10 （Enterprise Edition または Education Editiion）

9.3 その他のクライアントシステム要件

- Microsoft .NET Framework 4.0 以上
- HP MIK

9.4 ポリシーの作成

1. Configuration Manager で、[資産とコンプライアンス]→[概要]の順に選択します。
2. [HP Manageability Integration Kit]を選択し、[Device Guard]を右クリックして、[Create Policy]を選択します。
3. ベースライン名を入力してポリシー作成ウィザードを起動します。
4. 次のオプションのいずれかを選択します。

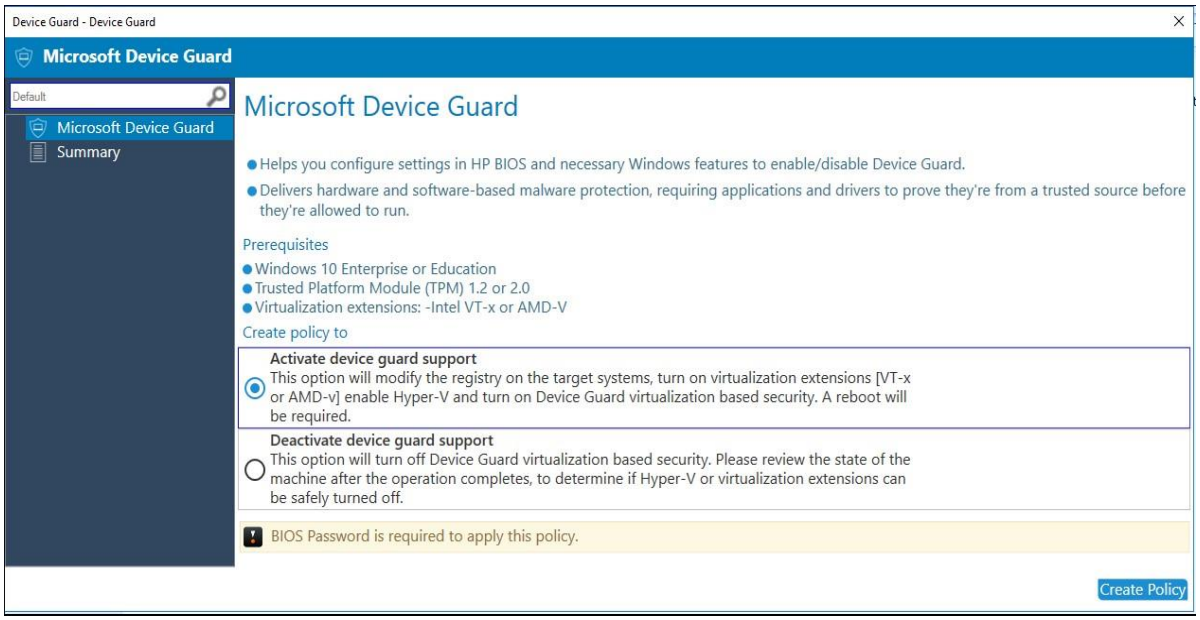


Figure 28 Microsoft Device Guard

a. [Device Guard]のサポートの有効化—ターゲットシステムのレジストリを変更し、仮想化拡張機能を有効にし、Hyper-V を有効にし、Device Guard の仮想化ベースのセキュリティを有効にします。

以下のレジストリ設定が変更されます:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceGuard]
    "EnableVirtualizationBasedSecurity"=dword:00000001
    "HypervisorEnforcedCodeIntegrity"=dword:00000001
    "RequirePlatformSecurityFeatures"=dword:00000002
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa]
    "LsaCfgFlags"=dword:00000001
```

以下の Windows の機能が変更されます:

Microsoft Hyper-V と分離ユーザーモードが有効になります。

以下の BIOS 設定が変更されます。（クライアントコンピュータで利用可能な場合）

SVM CPU Virtualization が有効になります。(AMD)

Virtualization Technology (VTx)が有効化になります。(Intel)

Virtualization Technology for Directed I/O (VTd)が有効になります。 (Intel)

TPM デバイスが利用可能になります。

TPM 状態が利用可能になります。

CD-ROM ブートが無効に なります。

PXE ブートが無効になります。

USB ストレージブートが無効になります。

レガシーブートが無効になります。

UEFI ブートが有効になります。

レガシーサポートおよびセキュアブートの構成の設定がレガシーサポ

ートの無効化およびセキュアブートの有効化になります。

b. [Device Guard]のサポートの無効化—Device Guard の仮想化ベースのセキュリティを無効にします。

Device Guard を無効にすると、レジストリ設定がデフォルト設定に戻ります。

Hyper-V が無効になります。

BIOS の Virtualization Technology が無効になります。

5. 概要ページを確認します。変更が必要な場合は、[前へ]ボタンをクリックしてください。それ以外の場合は、[ポリシーの保存]を選択します。

6. ポリシーが正常に保存されたら、[Deploy]を選択してから、ポリシーを適用するターゲットコレクションを選択します。

9.5 ポリシーの編集

1. Configuration Manager で、[資産とコンプライアンス]→[概要]の順に選択します。

2. [HP Manageability Integration Kit]を選択し、[Device Guard]を右クリックして、[Edit Policy]を選択します。

3. 編集する既存のベースラインポリシーを選択してから、[OK]を選択します。

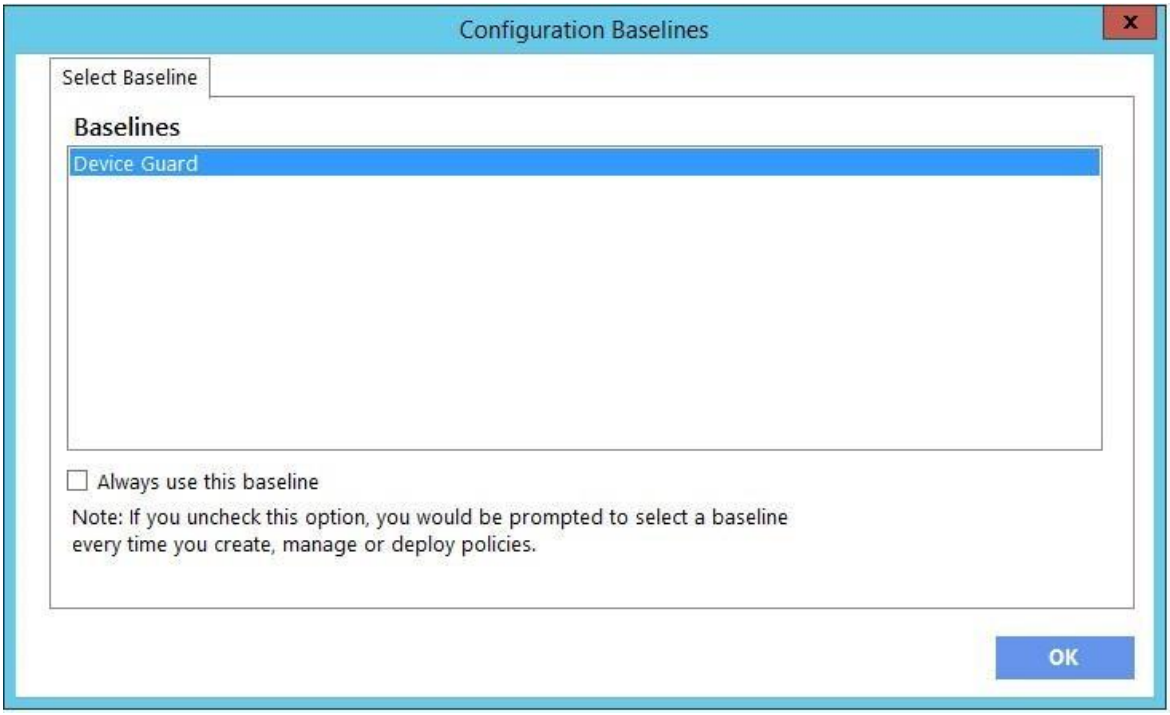


Figure 29 Edit baseline policies

4. ポリシーの作成のステップ 4 から 6 の手順を実行します。

9.6 補足情報

クライアントコンピュータでは、 HP MIK の Device Guard ポリシーのログは以下の場所に作成されます。

%PROGRAMDATA%\HP\HP MIK\Logs

以下のエラーコードがあります。

Table 1 Device Guard error code table

Error code	説明
0	OK
1	不明なエラーです。インストールエラーが発生する可能性があります。
2	オペレーティングシステムはサポートされていません。オペレーティングシステムの要件を参照してください。
3	CPU /チップセットはサポートされていません。プラットフォームの要件を参照してください。
4	古いグラフィックドライバです。操作を再試行する前にグラフィックドライバを更新してください。
5	BIOS の CPU Virtualization の有効化に失敗しました。
6	BIOS の TPM Device の利用可能化に失敗しました。
7	BIOS の USB デバイスブートの無効化に失敗しました。

8	BIOS の PXE ブートの無効化に失敗しました。
9	BIOS のフロッピーブートの無効化に失敗しました。
10	BIOS の CD-ROM ブートの無効化に失敗しました。
11	BIOS のブートモードの UEFI ネイティブ(Without CSM) への変更に失敗しました。
12	BIOS のセキュアブートの有効化に失敗しました。
13	Hyper-V の設定に失敗しました。
14	分離ユーザーモードの設定に失敗しました。
15	レジストリ値の設定でエラーが発生しました。
16	Windows の機能の変更に失敗しました。

10 HP Sure Start

HP Sure Start は、デフォルトでコンピュータの起動時または再起動時に BIOS の整合性を検証することで、マルウェアやウイルスの脅威から HP BIOS を保護します。追加のポリシーでは、BIOS が検証される頻度を増やすことができ、BIOS イベントログポリシーは任意のイベントをキャプチャすることができます。

HP MIK の HP Sure Start ポリシー管理を使用すると、リモートでポリシーを管理でき、BIOS での悪意のある攻撃やセキュリティ侵害とその後の修復について、適切なログ記録と通知を確実に実行できます。

Figure 30 HP Sure Start

10.1 サポートされるクライアントプラットフォーム

- 2014 年以降の HP 700 シリーズ以上のコマーシャルコンピュータ
- 2018 年以降の HP 600 シリーズのコマーシャルコンピュータ

10.2 サポートされるクライアント OS

- Windows 10
- Windows 8.1
- Windows 7

10.3 その他のクライアントシステム要件

- Microsoft .NET Framework 4.0 以上
- HP MIK

10.4 ユーザーインターフェース

10.4.1 BIOS Security Settings タブ

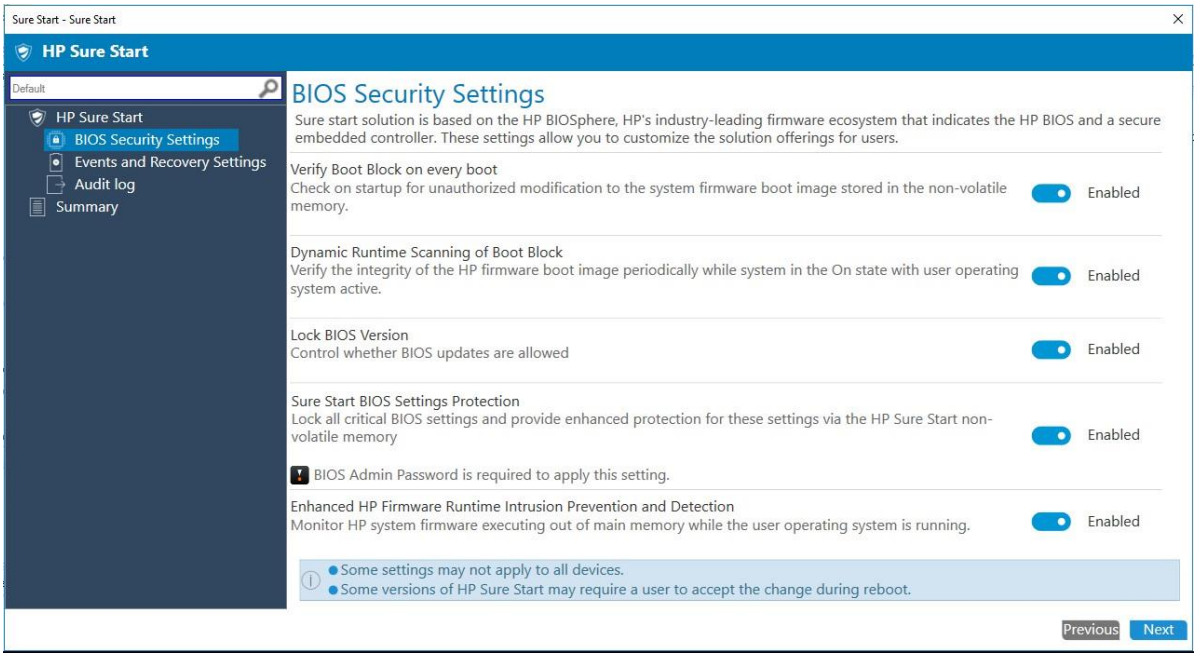


Figure 31 BIOS security settings

- 毎起動時の起動ブロックの確認—不揮発性メモリに保存されているシステムファームウェアブートイメージに対する不正な変更がないか起動時に確認します。

  有効にすると、HP Sure Start は、コンピューターの起動時または再起動時、あるいは休止状態またはスリープモードからの復帰時に、HP ファームウェアの起動イメージの整合性を検証します。この設定によりセキュリティが強化されますが、開始時間が長くなる可能性があります。

  無効になっている場合、HP Sure Start は、コンピューターが休止状態またはスリープモードを開始または終了するときに、HP ファームウェアブートイメージの整合性を確認します。

- ブートブロックの動的ランタイムスキャン—コンピュータの電源が入っていてオペレーティングシステムが動作している間に、HP ブートイメージの整合性を定期的に確認します。

  有効にすると、HP Sure Start は 15 分ごとに HP ブートイメージの整合性を検証します。

- BIOS のバージョンのロック—BIOS の更新を無効にします。
- Sure Start による BIOS 設定の保護—重要なすべての BIOS 設定への変更を無効にし、HP Sure Start 不揮発性メモリを介してこれらの設定に対する保護を強化します。この設定を有効にするには、BIOS 管理者パスワードが必要です。
- HP ファームウェアのランタイム侵入防止および検知機能の強化—オペレーティングシステムの実行中に、メインメモリから実行されている HP システムファームウェアを監視します。

10.4.2 Events and Recovery Settings タブ

これらの設定は、BIOS の攻撃や破損などの重大なセキュリティイベントが識別された後の HP Sure Start の動作を制御します。

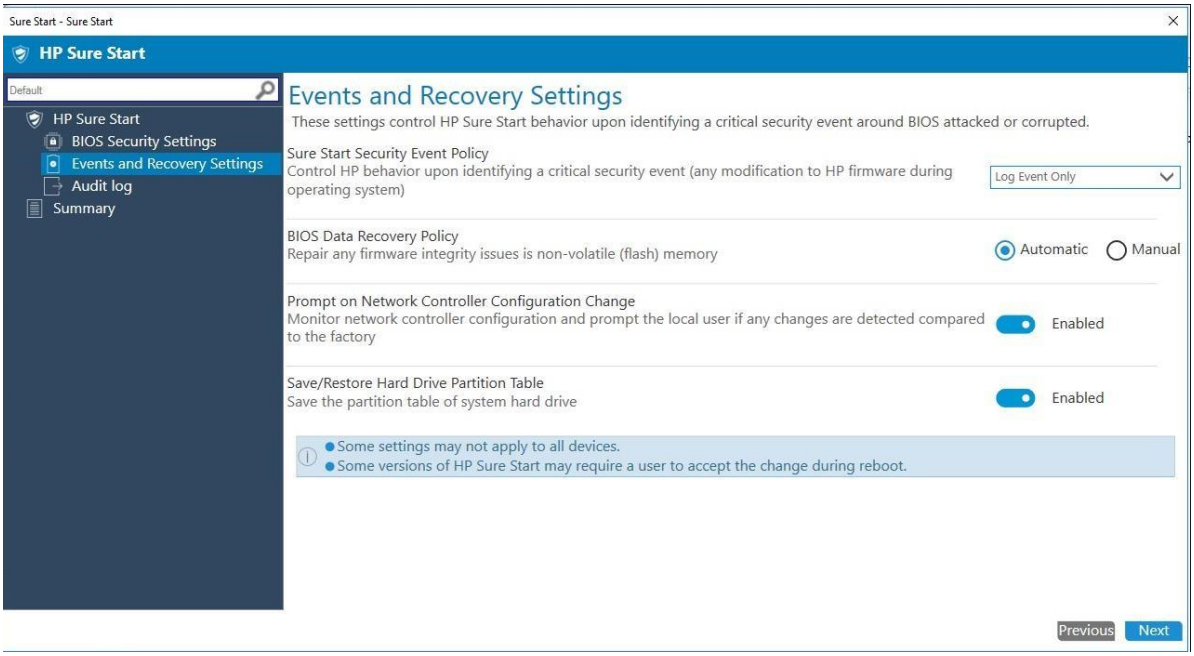


Figure 32 Events and Recovery Settings

- Sure Start のセキュリティイベントポリシー—HP Sure Start の不揮発性メモリ内のすべての重要なセキュリティイベントを HP Sure Start の監査ログに記録するには、[Log Event Only]を選択します。 HP Sure Start セキュリティイベントを検出してログに記録した後にシステムの電源を切るには、[Log Event and Power Off System]を選択します。データが失われる可能性があるため、システムのセキュリティの整合性がデータ損失の危険性よりも優先される状況でのみ、この設定を使用することをおすすめします。
- BIOS データのリカバリポリシー—不揮発性（フラッシュ）メモリ内のファームウェアの整合性の問題を自動的に修復するには、[Automatic]を選択します。Esc + Windows + ↑ + ↓ キーを押したときにファームウェアの整合性の問題を修復するには、[Manual]を選択します。この設定は IT 管理者のみにお勧めします。
- ネットワークコントローラー設定の変更時に通知を表示する—ネットワークコントローラー設定を監視し、工場出荷時と比較して変更が検出された場合にローカルユーザーに通知を表示します。
- ハードドライブパーティションテーブルの保存/復元—システムのハードドライブの Master Boot Record (MBR) または GUID Partition Table (GPT)を保存して変更があった場合に復元できるようにします。

10.4.3 Audit Log タブ

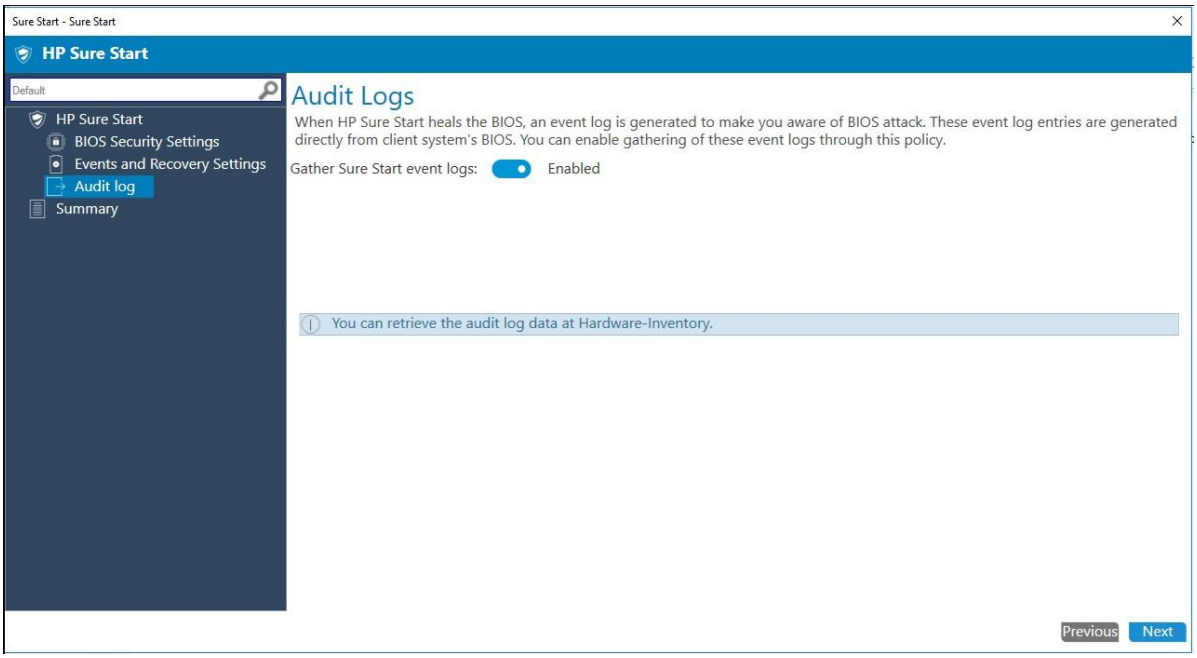


Figure 33 HP Sure Start Audit Log

[Gather Sure Start event logs]を有効にすると、HP MIK はクライアントコンピュータから HP Sure Start イベントログを収集し、それらを Configuration Manager ハードウェアインベントリに保存します。

10.5 ポリシーの作成

1. Configuration Manager で、[資産とコンプライアンス]→[概要]の順に選択します。
2. [HP Manageability Integration Kit]を選択し、[Sure Start]を右クリックして、[Create Policy]を選択します。
3. ベースライン名を入力し、[OK]をクリックします。

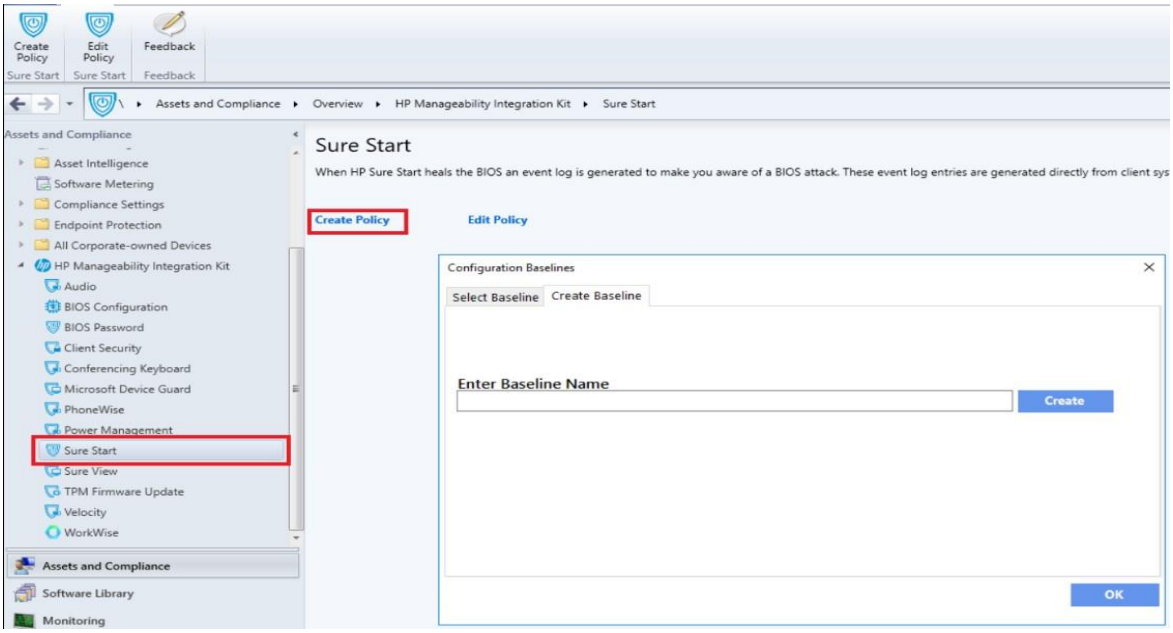


Figure 34 HP Sure Start Policy Configuration

4. 設定を変更し、[Nest]をクリックします。
5. 概要ページを確認します。変更が必要な場合は、[前へ]ボタンをクリックしてください。それ以外の場合は、[ポリシーの保存]を選択します。
6. ポリシーが正常に保存されたら、[Deploy]を選択してから、ポリシーを適用するターゲットコレクションを選択します。

10.6 ポリシーの編集

1. Configuration Manager で、[資産とコンプライアンス]→[概要]の順に選択します。
2. [HP Manageability Integration Kit]を選択し、[Sure Start]を右クリックして、[Edit Policy]を選択します。
3. 編集する既存のベースラインポリシーを選択し、[OK]をクリックしてウィザードを続行します。

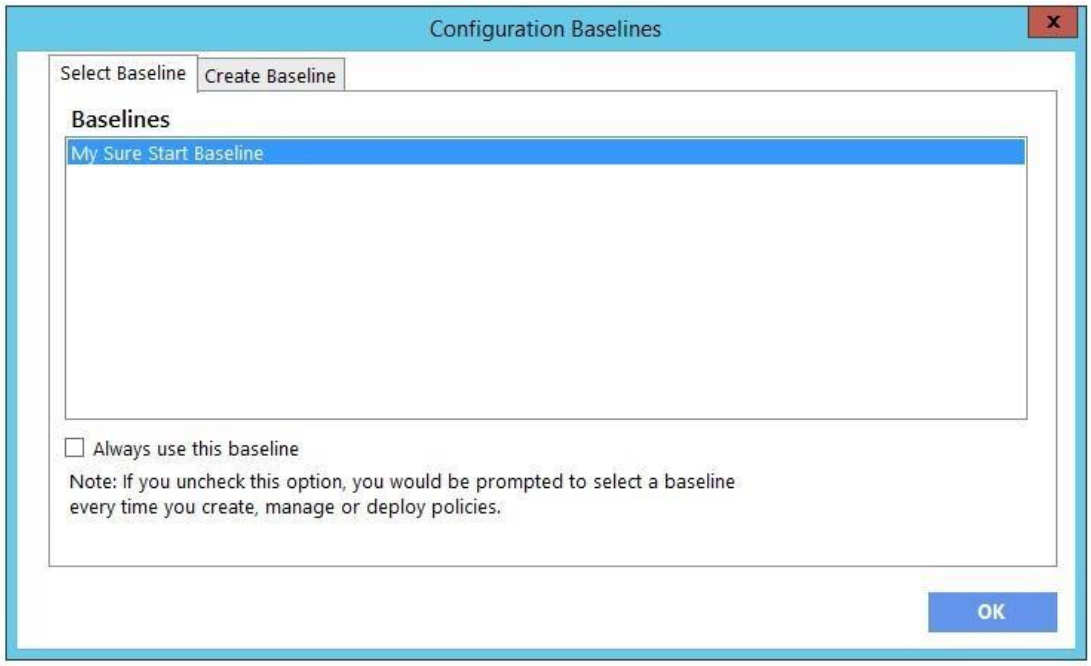


Figure 35 Configure Sure Start Baselines

4. ポリシーの作成のステップ 4 から 6 の手順を実行します。

10.7 補足情報

システムによってはサポートされていない機能もあります。

特定のシステムでは、設定変更後に手動で再起動する必要があります。

10.7.1 監査ログ

クライアントコンピュータでは、HP MIK の Sure Start ポリシーのログは以下の場所に作成されます。

```
%PROGRAMDATA%\HP\HP MIK\Logs.
```

監査ログが有効になっている場合、HP MIK は Configuration Manager ハードウェアインベントリの一部として HP Sure Start ログを取得します。

監査ログの表示方法:

1. Configuration Manager で、[資産とコンプライアンス]→[概要]→[デバイス]の順に選択します。
2. デバイスを右クリックし、[開始]→[リソースエクスプローラ]の順に選択します。
3. [ハードウェア]→[HP Sure Start Audit Logs]の順に選択します。

Figure 36 HP Sure Start Audit Logs

11 HP Sure View

11.1 概要

HP Sure View を使用すると機密情報を覗き見から防止するためのプライバシーフィルターを持ち歩く必要がなくなります。ユーザーは単に F2 キーを押すだけで、PC を直ちにプライバシーモードに切り替えることができます。これにより、斜めから見たときに最大 95%の可視光が減少し、他の人が画面の情報を見ることが難しくなります。

11.2 サポートされるクライアントプラットフォーム

- HP EliteBook 830/840 G5
- HP EliteBook x360 1020/1030 G2
- HP EliteBook x360 1030 G3
- HP EliteBook x360 1040 G5

11.3 サポートされるクライアント OS

- Windows 10

11.4 ポリシーの作成

1. Configuration Manager で、[資産とコンプライアンス]→[概要]の順に選択します。

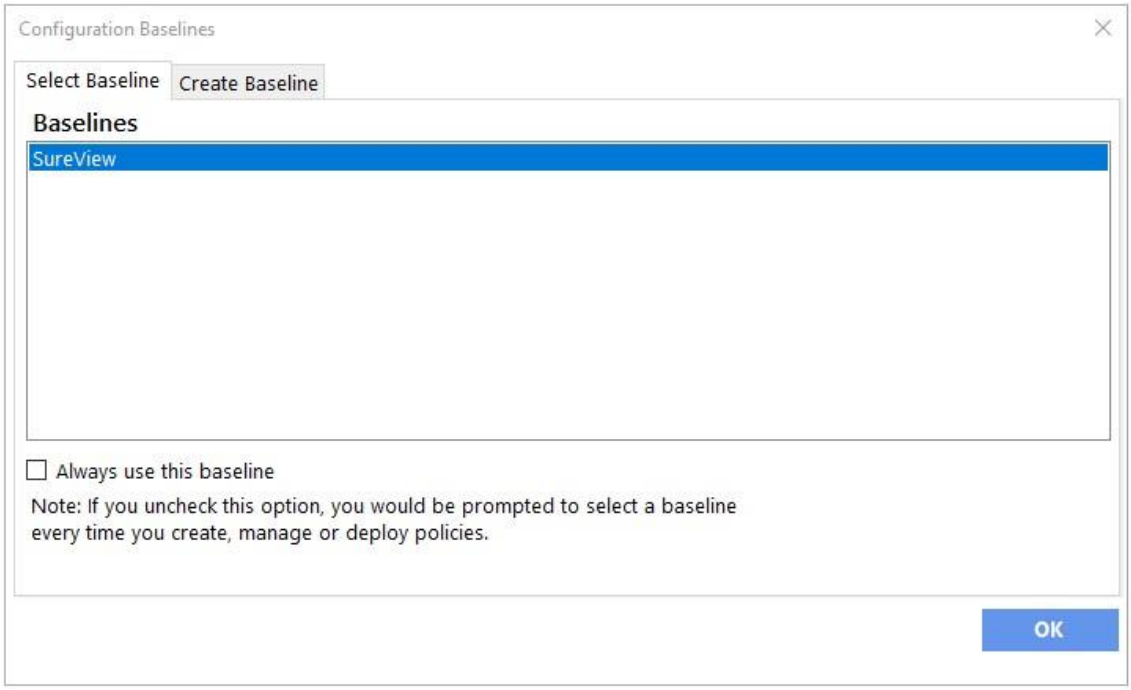


Figure 37 HP SureView Baseline configuration

2. [HP Manageability Integration Kit]を選択し、[SureView]を右クリックして[Create Baseline]を選択します。
3. ベースライン名を入力し、[OK]をクリックしてその名前でベースラインを保存します。
4. HP Sure View は初期状態で有効になっています。

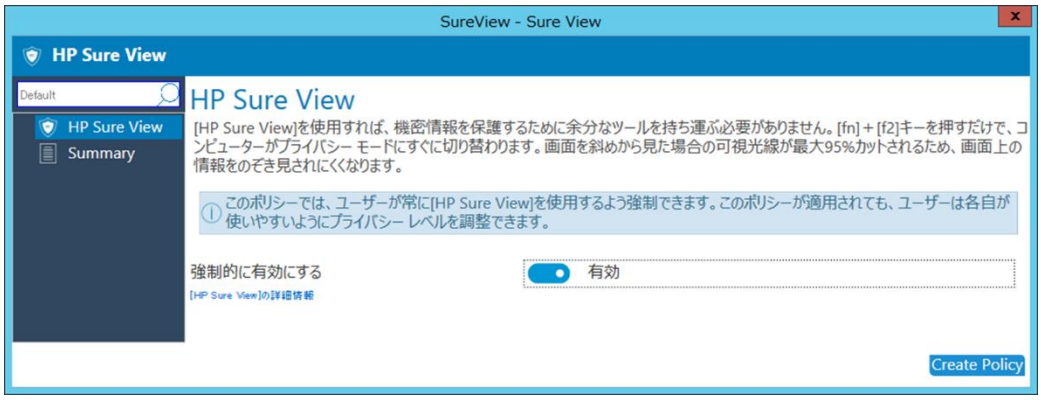


Figure 38 HP Sure View

5. [Create Policy]をクリックしてポリシーを保存します。次に、ポリシーを適用する必要があるコレクションを選択します。

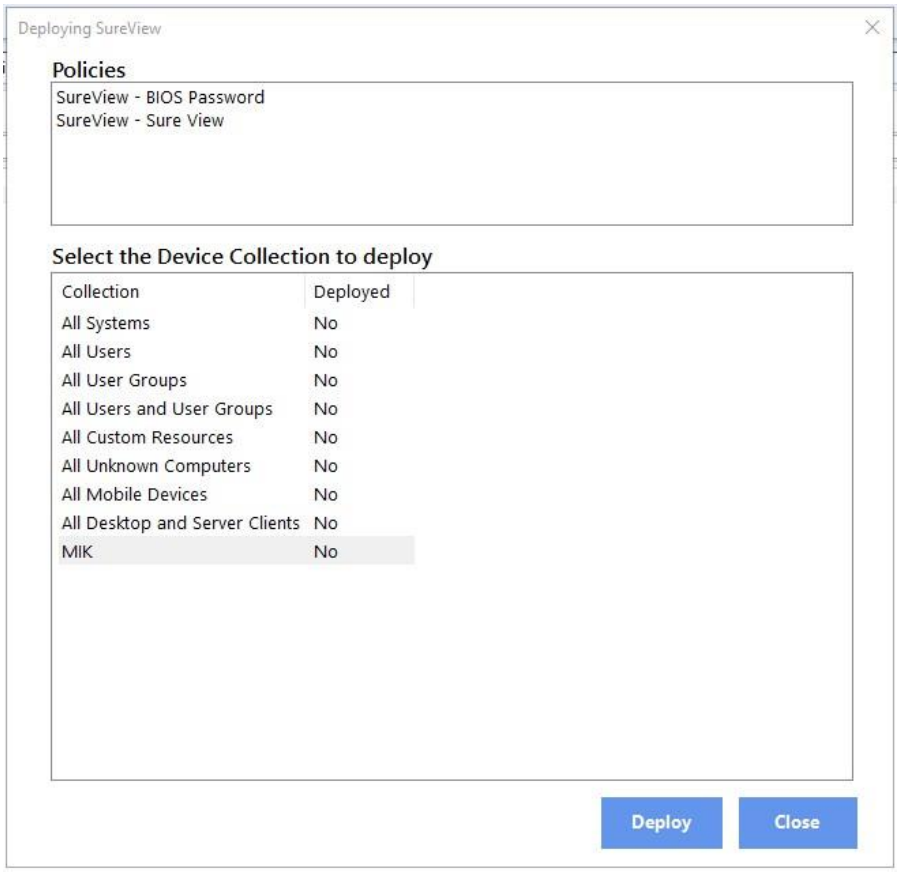


Figure 39 Deploy a Device Collection

6. [Deploy]をクリックして、コレクション内のクライアントシステムにポリシーを適用します。

11.5 ポリシーの編集

1. Configuration Manager で、[資産とコンプライアンス]→[概要]の順に選択します。
2. [HP Manageability Integration Kit]を選択し、[SureView]を右クリックして、[Edit Policy]を選択します。
3. 編集する既存のポリシーベースラインを選択し、[OK]をクリックしてウィザードを続行します。

Figure 40 HP SureView baselines

4. ポリシーの作成のステップ 4 から 6 の手順を実行します。

12 TPM Firmware Update

TPM firmware update ポリシーは、次の操作を実行するのに役立ちます。

- 古い TPM 1.2 ファームウェアを新しい TPM 1.2 ファームウェアにアップグレードする
- 古い TPM 2.0 ファームウェアを新しい TPM 2.0 ファームウェアにアップグレードする
- TPM 1.2 から TPM 2.0 に変換する
- TPM 2.0 から TPM 1.2 に変換する

12.1 サポートされるクライアントプラットフォーム

12.1.1 デスクトップコンピュータ

- HP EliteDesk 705 G2 Desktop Mini PC
- HP EliteDesk 800 35W G2 Desktop Mini PC
- HP EliteDesk 800 65W G2 Desktop Mini PC
- HP EliteDesk 800 G2 Small Form Factor PC
- HP EliteDesk 800 G2 Tower PC
- HP EliteOne 800 G2 23-inch Non-Touch All-in-One PC
- HP EliteOne 800 G2 23-inch Touch All-in-One PC
- HP ProDesk 400 G2 Desktop Mini PC
- HP ProDesk 400 G3 Microtower PC
- HP ProDesk 400 G3 Small Form Factor PC
- HP ProDesk 480 G3 Microtower PC
- HP ProDesk 490 G3 Microtower PC
- HP ProDesk 498 G3 Microtower PC
- HP ProDesk 600 G2 Desktop Mini PC
- HP ProDesk 600 G2 Microtower PC
- HP ProDesk 600 G2 Small Form Factor PC
- HP ProOne 400 G2 20-inch Non-Touch All-in-One PC
- HP ProOne 400 G2 20-inch Touch All-in-One PC
- HP ProOne 600 G1 All-in-One PC
- HP ProOne 600 G2 21.5-inch Non-Touch All-in-One PC
- HP RP9 G1 Retail System Model 9015
- HP RP9 G1 Retail System Model 9018

12.1.2 ノートブックコンピュータ

- HP EliteBook 1030 G1 Notebook PC
- HP EliteBook 1040 G3 Notebook PC
- HP EliteBook 725 G3 Notebook PC
- HP EliteBook 745 G3 Notebook PC
- HP EliteBook 755 G3 Notebook PC
- HP EliteBook 820 G3 Notebook PC
- HP EliteBook 840 G3 Notebook PC
- HP EliteBook 850 G3 Notebook PC
- HP EliteBook Folio G1 Notebook PC
- HP Elite x2 1012 G1
- HP ProBook 430 G3 Notebook PC
- HP ProBook 440 G3 Notebook PC
- HP ProBook 450 G3 Notebook PC
- HP ProBook 455 G3 Notebook PC
- HP ProBook 470 G3 Notebook PC
- HP ProBook 640 G2 Notebook PC
- HP ProBook 645 G2 Notebook PC
- HP ProBook 650 G2 Notebook PC
- HP ProBook 655 G2 Notebook PC
- HP ZBook 15 G3 Mobile Workstation
- HP ZBook 17 G3 Mobile Workstation
- HP ZBook Studio G3 Mobile Workstation

12.2 サポートされるクライアント OS

- Windows 10
- Windows 8.1
- Windows 7 (TPM 1.2 のみ)

12.3 その他のクライアントシステム要件

- Infineon SLB9670 TPM チップ
- 最新のコマーシャル BIOS
- Microsoft .NET Framework 4.0 以上
- HP MIK

12.4 ポリシーの作成

1. IConfiguration Manager で、[資産とコンプライアンス]→[概要]の順に選択します。
2. [HP Manageability Integration Kit]を選択し、[TPM Firmware Update]を右クリックして、[Create Policy]を選択します。
3. ベースライン名を入力し、[OK]をクリックしてその名前でベースラインを保存します。
4. ターゲット TPM のバージョンを選択し、[Create Policy]を選択します。警告および制限事項については追加情報を参照してください。

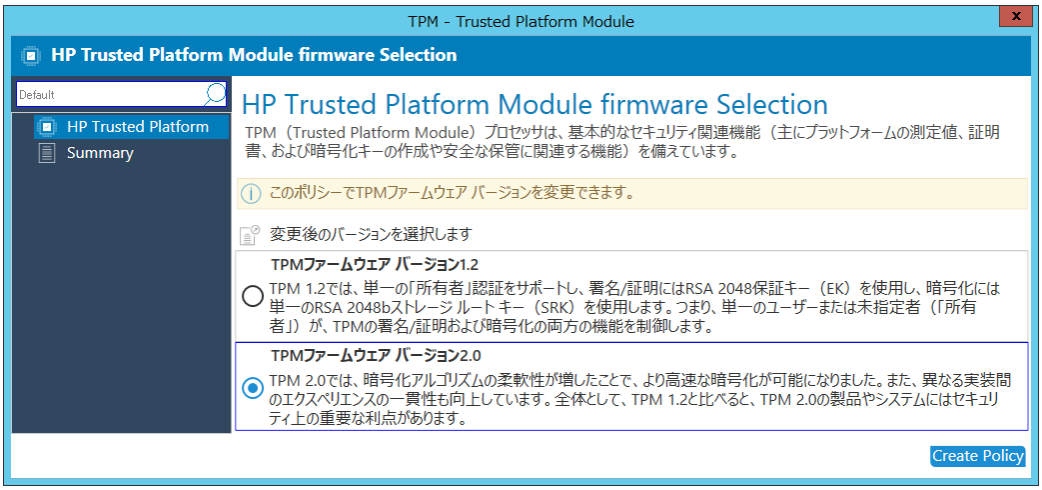


Figure 41 HP Trusted Platform Module Firmware Update

5. 概要ページを確認します。変更が必要な場合は、[前へ]ボタンをクリックしてください。それ以外の場合は、[ポリシーの保存]を選択します。
6. ポリシーが正常に保存されたら、[Deploy]を選択してから、ポリシーを適用するターゲットコレクションを選択します。

12.5 ポリシーの編集

1. Configuration Manager で、[資産とコンプライアンス]→[概要]の順に選択します。
2. [HP Manageability Integration Kit]を選択し、[TPM Firmware Update]を右クリックして、[Edit Policy]を選択します。
3. 編集する既存のベースラインポリシーを選択し、[OK]をクリックしてウィザードを続行します。

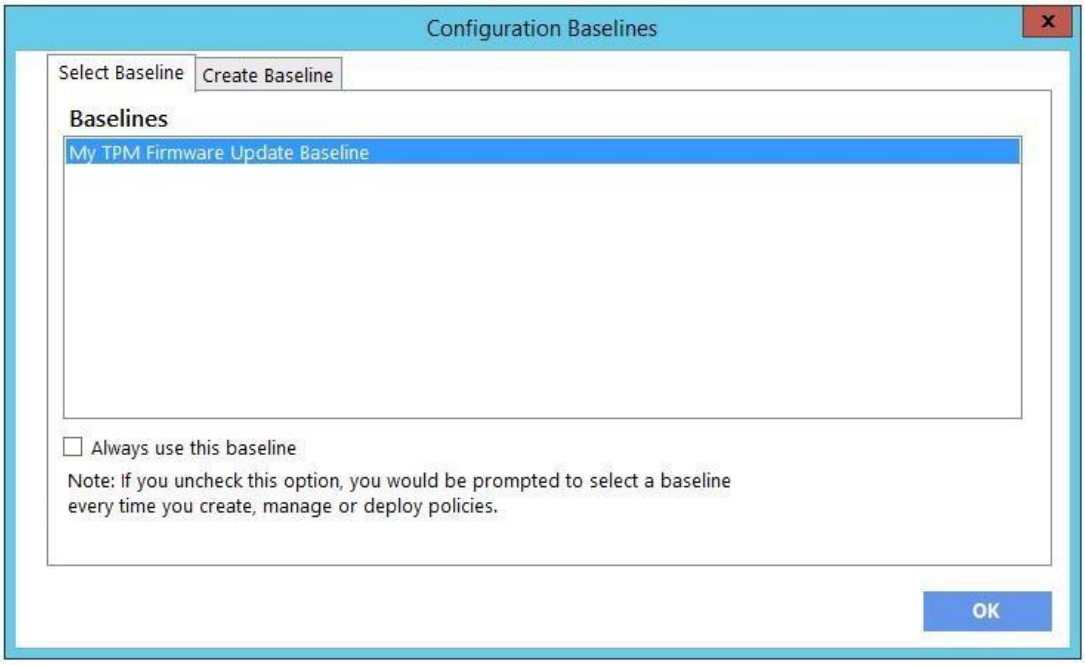


Figure 42 HP TPM Firmware Update Baseline

4. ポリシーの作成ステップの 4 から 6 の手順を実行します。

12.6 補足情報

警告!
プライマリドライブを暗号化している場合はこの、データの完全な損失を回避するためにポリシーを適用する前に復号化状態にする必要があります。このポリシーには、BitLocker および WinMagic のディスク暗号化ソリューションのみに対する組み込みチェックがあります。BitLocker または WinMagic ドライブの暗号化が使用されている場合、ポリシーはログに記録された適切なエラーコードで終了します。このポリシーは他のディスク暗号化ソリューションを検出しません。

TPM は TPM 1.2 と TPM 2.0 の間で最大 64 回まで変換できます。

TPM の変換には、新しい TPM ファームウェアへのアップグレードが含まれる場合があります。以下の規則がこの操作を左右します。

- システムに TPM 1.2 があり、ターゲットが TMP 2.0 の場合、TPM 2.0 が有効になり、最新のファームウェアバージョンにアップグレードされます。
- システムに TPM 2.0 があり、ターゲットが TPM 1.2 の場合、TPM 1.2 が有効になり、最新のファームウェアバージョンにアップグレードされます。
- システムに TPM 1.2 があり、ターゲットが TPM 1.2 の場合、TPM 1.2 は最新のファームウェアバージョンにアップグレードされます。

- システムに TPM 2.0 があり、ターゲットが TPM 2.0 の場合、TPM 2.0 は最新のファームウェアバージョンにアップグレードされます。
- この手順では、再起動を完了するために手動の操作が必要です。

13 HP WorkWise (Windows 10 のみ)

HP WorkWise は、スマートフォンとコンピュータを統合した HP アプリで、PC エクスペリエンスを保護、監視、および簡素化するのに役立ちます。

ユーザーは Microsoft の App Store からアプリをダウンロードできますが、IT 管理者はクライアントコンピュータで利用できる機能を指定できます。

※2019 年 1 月より、[HP WorkWise]のサポートは提供されなくなります。[HP WorkWise]は 2019 年 1 月以降もお使いのコンピューターで引き続きご利用いただけますが、OS の今後のバージョンには対応しない可能性があります。

13.1 サポートされるクライアントプラットフォーム

・・2016 年以降の HP コマーシャル コンピュータ

13.2 クライアントシステム要件

- Windows 10 1703 以上
- Microsoft .NET Framework 4.0 以上

HP WorkWise ソフトウェアをクライアントコンピュータにインストールする必要があります。アプリ固有の要件については、HP WorkWise のドキュメントを参照してください。

13.3 ユーザーインターフェース

このアプリのユーザーインターフェイスでは、HP WorkWise の機能を有効または無効にすることができます。

Figure 43 HP WorkWise Feature Selection

- HP WorkWise の機能をすべて有効にする—すべての機能を有効にするために選択します.
- セキュリティ—コンピュータのロック/ロック解除と不正アクセス検出を有効にするために選択します。
- パフォーマンス—パフォーマンスモニター機能のダッシュボードと、過熱状態の PC の検出を有効にするために選択します。
- プリンター—プリンタードライバーのインストールを有効にするために選択します。

- 健康—フォーカスモードを有効にするために選択します。

13.4 ポリシーの作成

1. Configuration Manager で、[資産とコンプライアンス]→[概要]の順に選択します。
2. [HP Manageability Integration Kit]を選択し、[HP WorkWise]を右クリックして、[Edit Policy]を選択します。
3. ベースライン名を入力し、[OK]をクリックしてその名前でベースラインを保存します。
4. 設定を変更します。
5. 概要ページを確認します。変更が必要な場合は、[前へ]ボタンをクリックしてください。それ以外の場合は、[ポリシーの保存]を選択します。
6. ポリシーが正常に保存されたら、[Deploy]を選択してから、ポリシーを適用するターゲットコレクションを選択します。

13.5 ポリシーの編集

1. Configuration Manager で、[資産とコンプライアンス]→[概要]の順に選択します。
2. [HP Manageability Integration Kit]を選択し、[HP WorkWise]を右クリックして、[Edit Policy]を選択します。
3. 編集する既存のベースラインポリシーを選択し、[OK]をクリックしてウィザードを続行します。

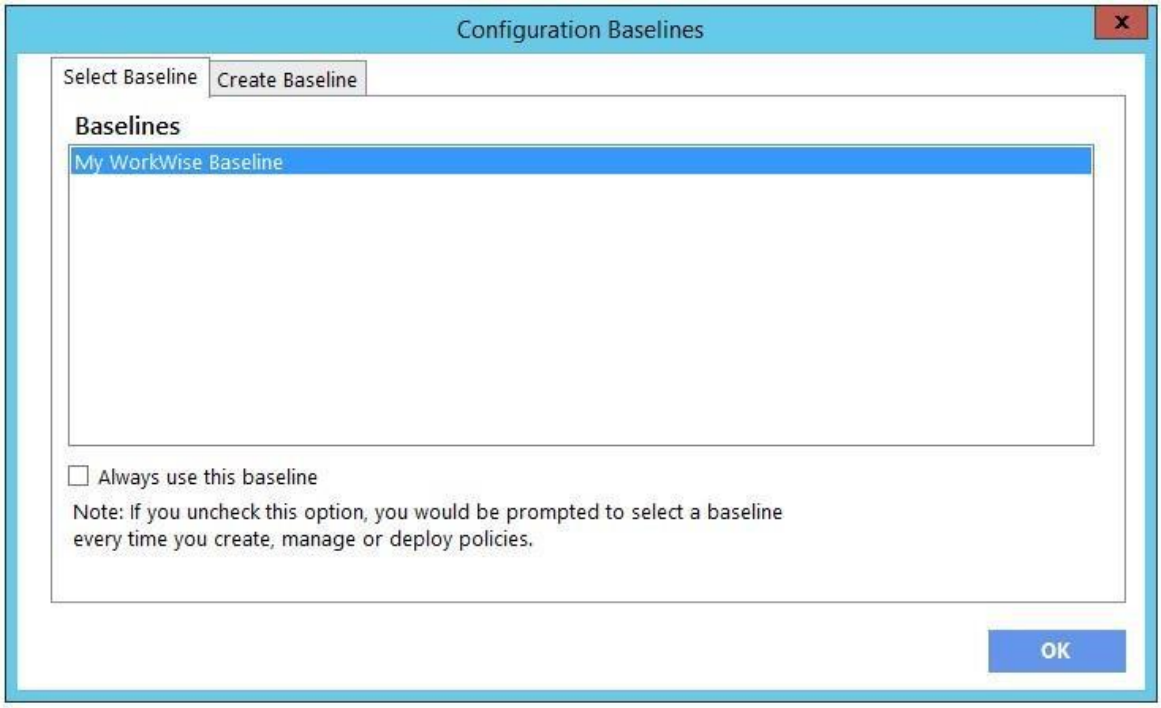


Figure 44 HP WorkWise Baseline configuration

4. ポリシーの作成のステップ 4 から 6 の手順を実行します。

14 HP Client Driver Packs

14.1 HP クライアントドライバーパックの作成とインポート

HP クライアントドライバーパックの作成とインポート]オプションは、サポートされている HP 製品のドライバを表示します。これは、HP CIK で以前に利用可能だったオプションと同様の機能です。

1. Configuration Manager で、[ソフトウェアライブラリ]→[概要]→[オペレーティングシステム]→[ドライバパッケージ]の順に選択します。

2. コンソールのリボンから[Create and Import HP Client Driver Pack]をクリックします。Create and Import HP Client Driver Pack ウィザードが起動します。

3. Operating system を選択します。

4. ドライバパックの作成をサポートしている製品のみが Available products 列に表示されます。必要に応じて、[HP 製品名]ボックスにキーワードを入力し、[Enter]を押して使用可能な製品のリストを絞り込みます。

5. 使用可能な製品を選択し、>ボタンをクリックして Selected products 列に製品を追加します。

6. 必要に応じて、手順 5 を繰り返して別の製品を選択します。最適な関連ドライバを含むドライバパックを作成するために、同じファミリモデルの製品を選択することをおすすめします。また、ドライバパックあたり 5 つ以下の製品を選択することをお勧めします。

   例えば、HP ProBook 640 G1 Notebook PC と HP ProBook 650 G1 Notebook PC を選択して HP ProBook 600 series G1 Notebook PC 用のドライバーパックを作成します。

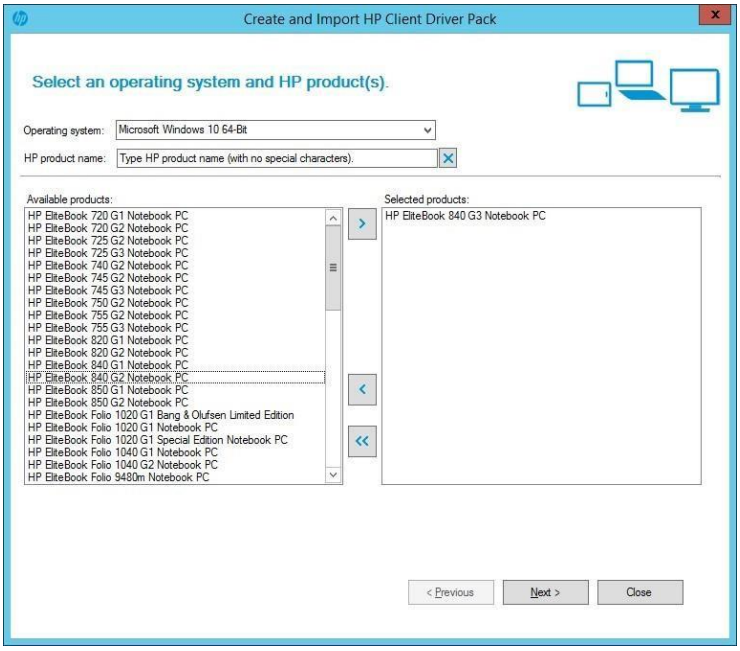


Figure 45 HP Client Driver Pack selection

7. [Next]をクリックします。

8. デフォルトでは、Import option に Create driver package with the selected drivers below が選択されています。このオプションで選択したドライバーを含むドライバーパッケージを作成します。

   a. ドライバーパッケージの名前と、必要に応じてバージョンとコメントを入力します。

   b. Drivers の下に、ドライバパッケージに含めるドライバが選択されていることを確認し、他のすべてのドライバがクリアされていることを確認します。

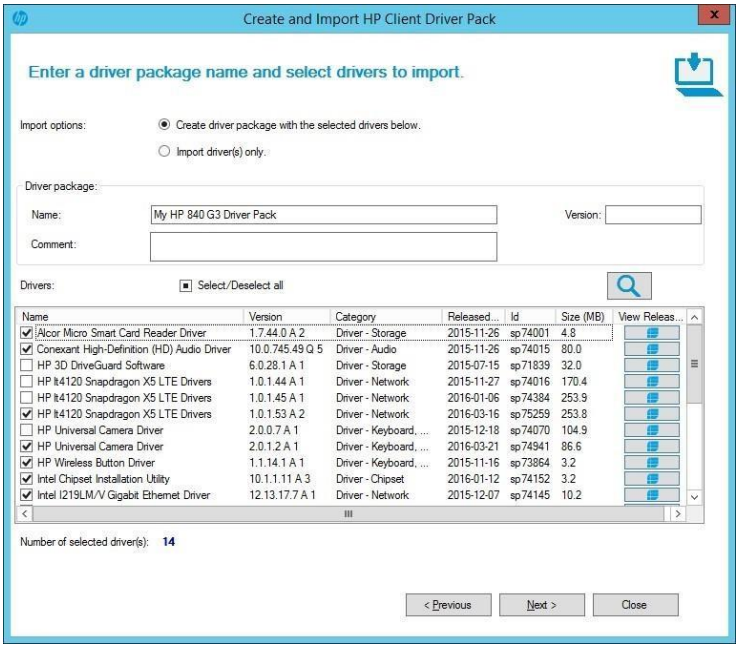


Figure 46 HP Client Driver Pack Create and Import

– または –

後でドライバパックを作成するためにドライバをインポートするには、Import driver(s) only オプションを選択します。デフォルトでは、インポートされたドライバのドライバカテゴリは HP Client Driver です。必要に応じて別のドライバカテゴリを選択してください。

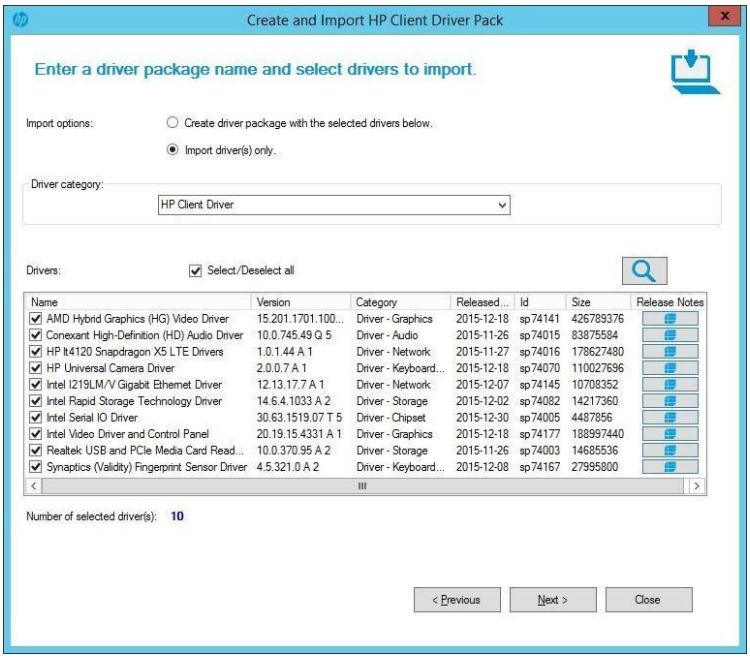


Figure 47 HP Client Driver Pack Driver Selection

9. [Next]をクリックします。

10. ドライバーパッケージを作成している場合は、以下の手順で配布ポイントとネットワーク共有を設定します。

    a. 配布ポイントを選択します。クラウド配布ポイントはサポートされていません。

    b. Configuration Manager がドライバーとドライバーパックを保存するためのネットワーク共有フォルダを選択します。 指定された場所に、必要なすべてのユーザーアカウントがアクセスできる十分な権限があることを確認してください。

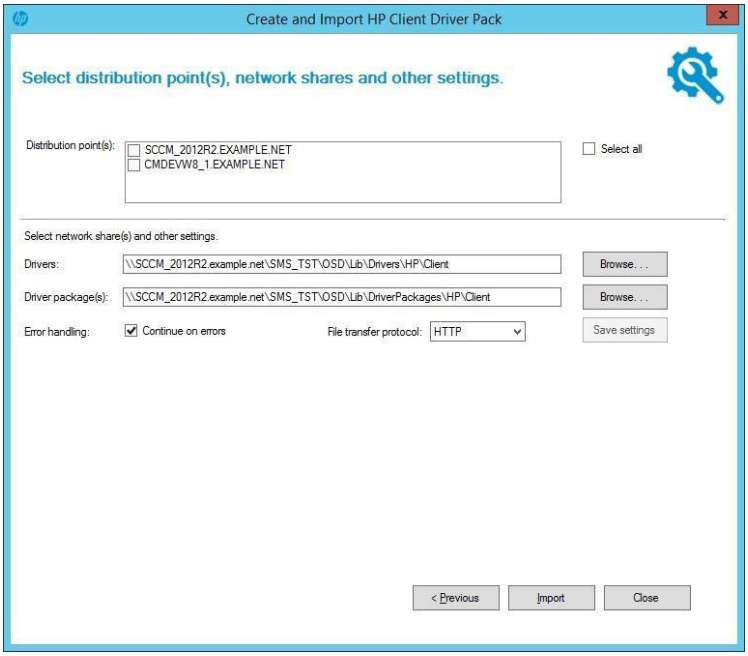


Figure 48 HP Client Driver Pack Distribution Point, Network Shares, and other settings

11. ドライバーをインポートするだけの場合は、Configuration Manager がドライバーを保存するためのネットワーク共有フォルダを選択します。指定された場所に、必要なすべてのユーザーアカウントがアクセスできる十分な権限があることを確認してください。

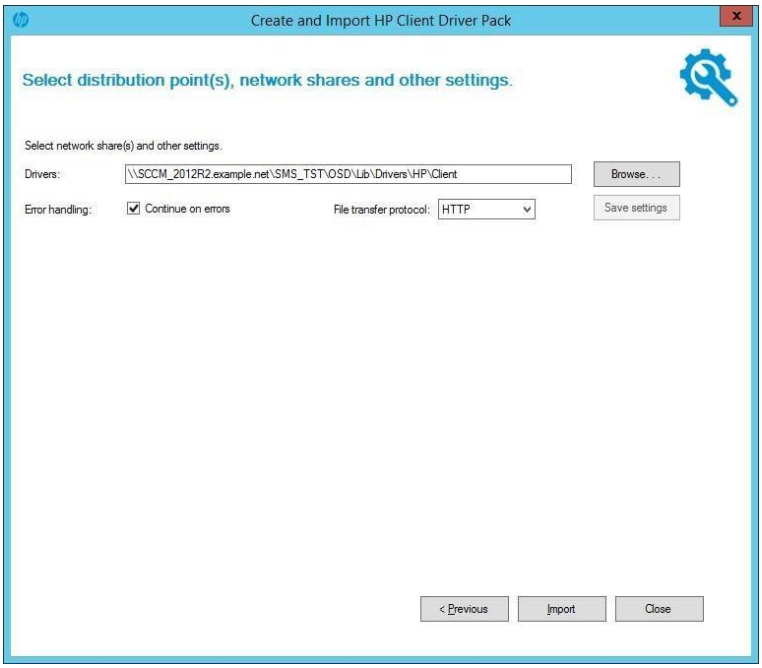


Figure 49 HP Client Driver Pack Distribution Points, Network Shares, and other settings

12. エラーが発生したときにインポートを停止する必要がある場合は、［Continue on errors］オプションをオフにします。デフォルトでは、このボックスは選択されています。複数のドライバが選択されてい

る場合、現在のドライバのインポートに失敗した場合は、次に選択されているドライバがインポートされます。

13. デフォルトでは、HP MIK は HTTP を使用して選択したドライバーをダウンロードします。必要に応じて FTP を選択してください。

14. Select network share(s) and other settings の設定を変更すると、Save settings ボタンが有効になります。後続のドライバおよびドライバパッケージの作成またはインポートのために設定を保存するには、このボタンを選択します。

15. [Import]をクリックするとドライバーパックの作成とインポートのプロセスが開始します。

14.2 HP ドライバーパックのダウンロードとインポート

{Download and Import Driver Packs]オプションを選択すると、HP 製品とドライバパックの一覧が表示されます。これは、HP CIK で以前に利用可能だったオプションと同様に機能します。.

1. Configuration Manager で、[ソフトウェアライブラリ]→[概要]→[オペレーティングシステム]→[ドライバパッケージ]の順に選択します。

2. コンソールのリボンから[Download and Import Driver Packs]をクリックします。

3. Operating system を選択します。

4. Available products 列に、ドライバパックをサポートしている製品が表示されます。オプションで、[HP product name]ボックスにキーワードを入力して[Enter]キーを押すと、利用可能なドライバパックのリストを絞り込むことができます。

5. ターゲットオペレーティングシステムの展開に含めるドライバパックを選択し、>ボタンを選択して製品を Selected products 列に追加します。選択した製品の関連ドライバパックが Available driver packs リストに表示されます。

6. 必要に応じて、配布ポイントを選択してインポートしたドライバパックを特定の配布先に割り当てます。ただし、クラウド配布ポイントはサポートされていません。

7. 必要に応じて、ドライバとドライバパッケージを保存するように Configuration Manager のデフォルトの場所を変更します。指定した場所に、必要なすべてのユーザーアカウントがアクセスできる十分な権限があることを確認してください。

8. Select network share(s) and other settings の設定を変更すると、Save settings ボタンが有効になります。後続のドライバパッケージのダウンロードおよびインポートのために設定を保存するには、このボタンを選択します。

9. エラーが発生したときにインポートを停止する必要がある場合は、［Continue on errors］オプションをオフにします。デフォルトでは、このボックスは選択されています。複数のドライバーパックが選択されている場合、現在のドライバーパックのインポートに失敗した場合は、次に選択されているドライバーパックがインポートされます。

10. デフォルトでは、HP MIK は HTTP を使用して選択したドライバーをダウンロードします。必要に応じて FTP を選択してください。

11. [Download and Import]をクリックするとドライバーパックのダウンロードとインポートのプロセスが開始します。

注記:

[Reset Form]ボタンをクリックするとすべての選択が解除されます。

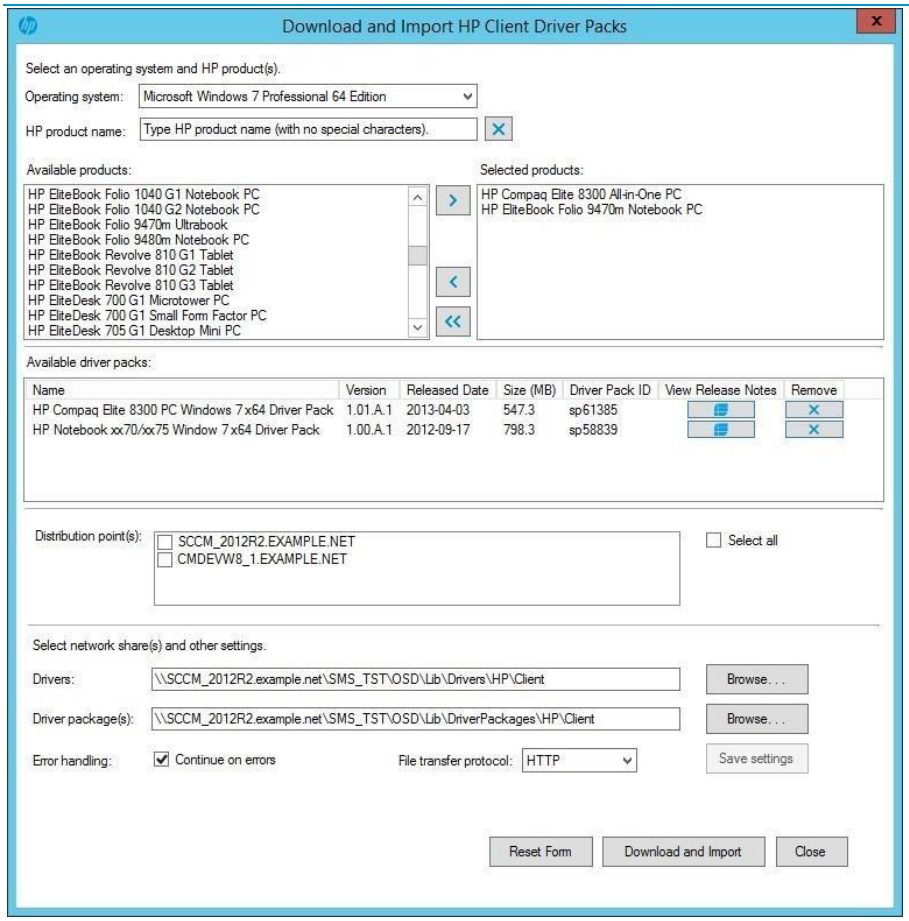


Figure 50 HP Client Driver Packs – Download and Import

ダウンロードおよびインポートプロセス中に、ダイアログボックスに現在の操作と進行状況が表示されます。プロセスは選択されたドライバパックをダウンロードし、それらを Configuration Manager にインポートします。1 つ以上の選択されたドライバパックが Configuration Manager に既に存在する場合、プロセスは既存のドライバパックをスキップまたは上書きするようにユーザーに促します。

プロセスが完了すると、各ドライバパックのインポートステータスの概要が表示されます。

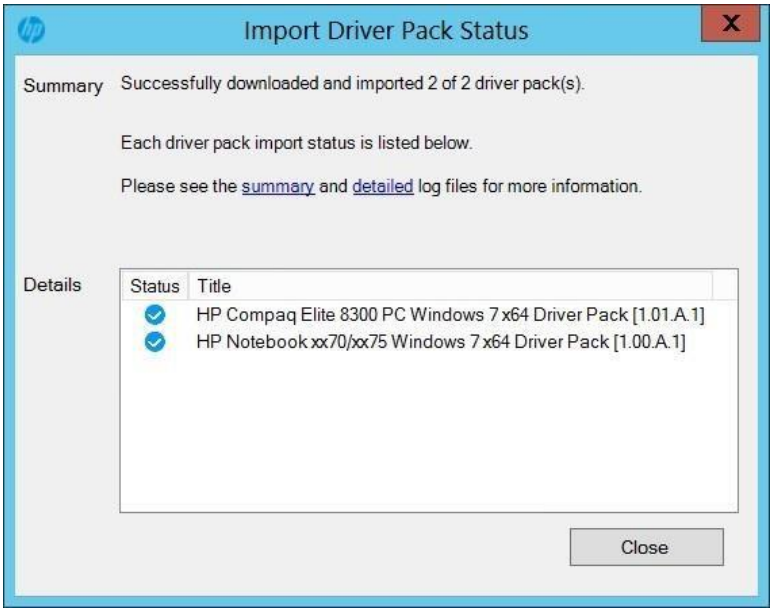


Figure 51 HP Import Driver Pack Status Window

インポートされたドライバパックは、[ドライバパッケージ]→ [HP Client Driver Packages]に作成されます。

インポートしたドライバパックをタスクシーケンスで使用する前に、それらを配布ポイントにプッシュする必要があります。ダウンロードとインポートのダイアログボックスで配布ポイントが選択されていない場合、または追加の配布ポイントが必要な場合は、インポートした各ドライバパックを選択し、コンテンツの配布を選択します。

注記:
このプロセスでは、Configuration Manager から ftp.hp.com へのインターネット接続が必要となります。Configuration Manager コンソールがインストールされているデバイスの ftp.hp.com からドライバーパック情報を取得できない場合は、ブラウザーセッションを開いて接続を確認してから、もう一度このプロセスを実行してください。

Configuration Manager がインストールされているデバイスから ftp.hp.com へのインターネット接続ができない場合は、以下のいずれかの方法で HP ドライバーパックを入手し、代わりに Import Downloaded Driver Pack を使用してください。

14.3 HP ドライバーパックの入手方法

ドライバーパックを入手する方法はいくつかあります。

注記:
ダウンロード可能なすべてのドライバパックが HP MIK で使用できるわけではありません。[システム - ソフトウェア管理]などのカテゴリに一覧表示されているドライバパックは、HP MIK ではインポートできません。

- HP Client Management Solutions ウェブサイト

- HP SoftPaq Download Manager (SDM)

HP Client Management Solutions Web サイトからのドライバーパック入手方法

1. Web ブラウザで http://www.hp.com/go/clientmanagement. にアクセスします。
2. Resources の下の[HP Driver Packs]を選択します。
3. 対象の OS に応じて、32-bit または 64-bit を選択します。
4. 対象のクライアントコンピュータとオペレーティングシステム用の適切なドライバパックをダウンロードします。

注記:
ダウンロードページにリストされている WinPE ドライバパックは、HP クライアントのブートイメージを作成するためにのみ使用します。

HP SDM を使用したドライバーパックの入手方法:

1. Web ブラウザで http://www.hp.com/go/clientmanagement にアクセスします。
2. Resources の下の[HP Download Library]を選択します。
3. SoftPaq Download Manager をダウンロードします。
4. スタートメニューから[HP]→[HP SoftPaq Download Manager]を選択して HP SDM を起動します。
5. [すべての製品を表示]を選択します。
6. [ツール]→[構成オプション]を選択します。
7. [Filter]→[OS]に SDM に表示する OS の種類を選択します。
8. [Filter]→[Language]に[English – International]を選択します。
9. 構成オプションで[OK]をクリックします。
10. 製品カタログで、対象の製品名と OS を選択し、[利用可能な Softpaq の検索]をクリックします。
11. Category Manageability – Driver Pack にあるドライバーパックをダウンロードします。

14.4 HP SDM を使用したドライバーパックの作成方法

HP SDM (バージョン 3.5.2.0 以上)を使用してドライバーパックを作成します。

1. スタートメニューから[HP]→[HP SoftPaq Download Manager]を選択して HP SDM を起動します。
2. [ツール]→[構成オプション]を選択します。
    a. [Filter]→[OS]で SDM に表示する OS の種類を選択します。

b. [Filter]→[Language]に[English – International]を選択します。

c. [OK]をクリックします。

3. 製品カタログで、対象の製品名と OS を選択し、[利用可能な SoftPaq の検索]をクリックします。

4. すべての利用可能な SoftPaq で、ドライバーパックに含める SoftPaq を選択します。

5. ダウンロードされた SoftPaq ウィンドウで、ダウンロードボタンの横のドロップダウンメニューから以下のいずれかのオプションを選択します。

   - CAB ファイルのビルド— Microsoft Deployment Toolkit または HP MIK を Configuration Manager と組み合わせて使用してドライバーパックを展開するには、このオプションを選択します。
   - ZIP ファイルのビルド—このオプションを選択すると、HP MIK を Configuration Manager と共に使用したり、別のアプリケーションを介してドライバーパックを手動で展開したりできます。

6. [ダウンロード]をクリックします。

7. 使用許諾契約書画面が表示されたら、[使用許諾契約書に同意します。]を選択して,[続行]をクリックします。

8. Driver Pack Builder 画面で、OS-Bitness に OS の種類とビット数を選択します。

9. ドタイバーパックの名前や出力先のフォルダを設定して、[Build]をクリックします。

10. [ドライバーパックの圧縮が完了しました]のメッセージが表示されたら[OK]をクリックします。

ドライバーパックと関連のログファイルが出力先フォルダに作成されます。

14.5 HP ドライバーパックのインポート

1. Configuration Manager で、[ソフトウェアライブラリ]→[概要]→[オペレーティングシステム]→[ドライバーパッケージ]の順に選択します。

2. コンソールのリボンから[Import Driver Pack]をクリックします。

3. **Driver package** の下の[**Browse**]をクリックしてインポートする HP ドライバーパックを選択します。

4. 必要に応じて、配布ポイントを選択してインポートしたドライバパックを特定の配布先に割り当てます。ただし、クラウド配布ポイントはサポートされていません。

5. 必要に応じて、Configuration Manager がドライバーやドライバーパックを保存するデフォルトの場所を変更します。指定された場所に、必要なすべてのユーザーアカウントがアクセスできる十分な権限があることを確認してください。ユーザーごとの場所は、正常にインポートされた後に自動的に保存されます。

   このパスまたはその他の設定を変更すると、[Save settings]ボタンが有効になります。後続のドライバパッケージのダウンロードおよびインポート手順の設定を保存するには、このボタンを選択します。

6. [Import]をクリックします。

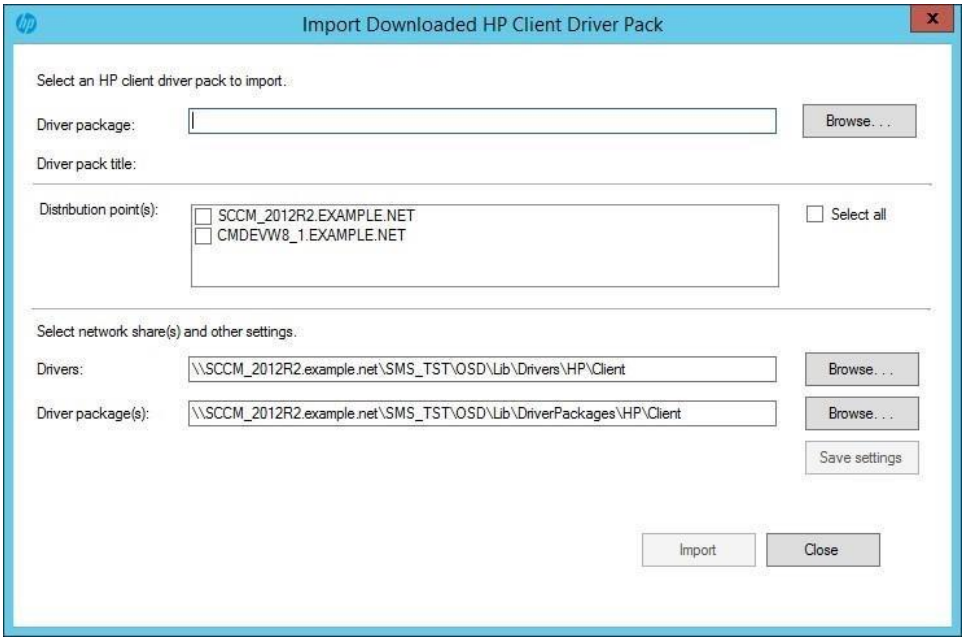


Figure 52 HP Client Driver Pack Import Download

インポート処理中、ダイアログボックスに現在の操作と進行状況が表示されます。

インポートプロセスが完了すると、インポートされたドライバパックはソフトウェアライブラリの[HP Client Driver Packages]の下に表示されます。インポートしたドライバパックをタスクシーケンスで使用する前に、配布ポイントにプッシュする必要があります。インポート処理中に配布ポイントが選択されていない場合、または追加の配布ポイントが必要な場合は、ドライバパックを選択してから[コンテンツの配布]を選択します。

15 HP Client Boot Images

15.1 WinPE 用ドライバーパックの入手方法

1. Web ブラウザで http://www.hp.com/go/clientmanagement にアクセスします。
2. Resources の下の[HP Download Library]を選択します。
3. [HP WinPE Driver Pack 32-bit]または[HP WinPE Driver Pack 64-bit]をダウンロードします。

WinPE 4.0 には、オペレーティングシステムの展開をサポートするために必要なハードウェアドライバが多数含まれているため、すべてのプラットフォームまたは構成に WinPE 4.0 ドライバパックが必要なわけではありません。追加されたドライバは、それらを必要としないシステムや構成に影響を与えないため、WinPE 4.0 ドライバパックを作成して使用することをおすすめします。

WinPE 5.0 は、2011 年から 2013 年に出荷された HP のコマーシャルデスクトップ、ノートブック、およびワークステーションをネイティブでサポートします。 WinPE 5.0 ドライバパックは WinPE 4.0 では使用できません。また、WinPE 4.0 ドライバパックは WinPE 5.0 でも使用できません。

Configuration Manager の各バージョンは、特定のバージョンの WinPE へのドライバおよびコンポーネントのカスタマイズまたは追加のみをサポートしているため、HP MIK ブートイメージの作成は限定的なサポートを提供します。 WinPE のカスタマイズに関する特定の要件の詳細については、 http://technet.microsoft.com/en-us/library/dn387582.aspx を参照してください。

ブートイメージを配布ポイントで利用できるようにする前に、Configuration Manager は Windows アセスメント & デプロイメントキット（ADK）、特に DISM.exe を使用してブートイメージにドライバを挿入することがあります。 DISM には ADK のバージョンとオペレーティングシステムに依存する特定の要件があるため、DISM はブートイメージに追加された一部の起動に不可欠なドライバの署名を適切に認識できない可能性があります。詳細については、 http://technet.microsoft.com/enus/library/hh825070.aspx を参照してください。

HP MIK のブートイメージ作成機能は、ブートイメージに対する Configuration Manager と ADK のカスタマイズサポートを利用します。そのため、HP MIK の制限は、Configuration Manager のバージョン、ADK のバージョン、およびサイトサーバーのオペレーティングシステムのバージョンによって異なります。

15.2 WinPE ドライバーパックのインポートとブートイメージの作成

1. Configuration Manager で、[ソフトウェアライブラリ]→[概要]→[オペレーティングシステム]、[ブートイメージ]の順に選択します。
2. リボンメニューの[HP Client PC]セクションで、[Create Boot Image]を選択します。
3. [Create HP Client Boot Image(s)]で、[Browse]を選択してインポートする HP WinPE ドライバパックを選択します。 HP MIK は、選択された WinPE ドライバパックに適し、Configuration Manager によるカスタマイズがサポートされているブートイメージのみを表示します。
4. 使用する Base Boot Image を選択します。[Create]を選択して、選択した HP WinPE ドライバパックのドライバを使用してブートイメージを作成します。

5. 必要に応じて、配布ポイントを選択してブートイメージを特定の保存先に割り当てます。ただし、クラウド配布ポイントはサポートされていません。

6. 必要に応じて、Configuration Manager のデフォルトの場所を変更して、ドライバ、ドライバパッケージ、およびブートイメージを保存します。指定された場所に、必要なすべてのユーザーアカウントがアクセスできる十分な権限があることを確認してください。

保存先やその他の設定を変更すると、[Save Settings]ボタンが有効になります。このボタンを選択して、以降の起動イメージ作成およびドライバまたはドライバパックのインポート手順のために設定を保存します。

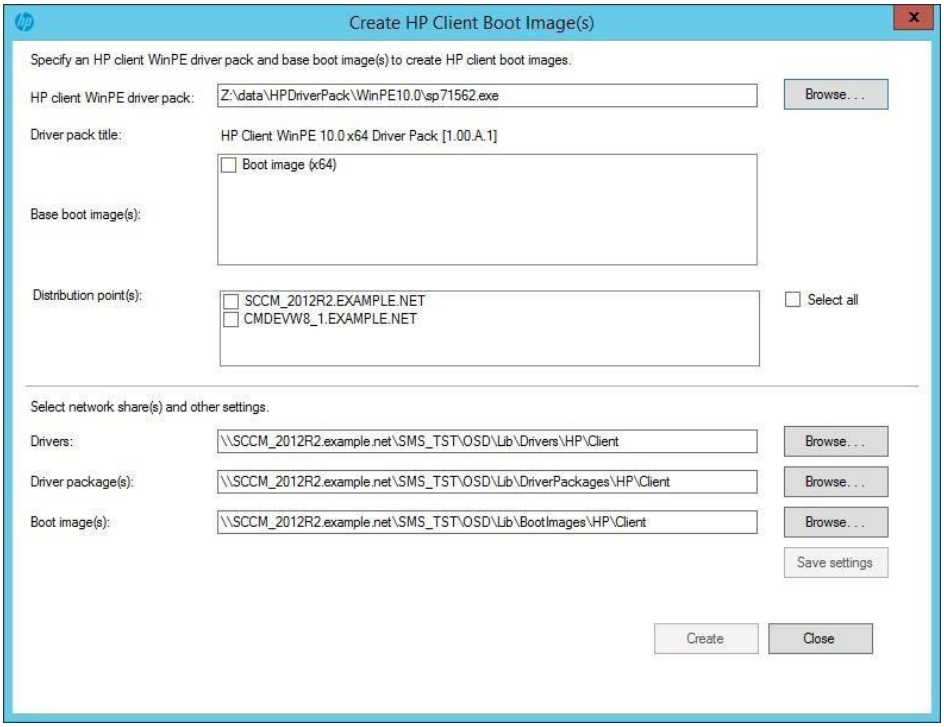


Figure 53 Create HP Client Boot Image(s)

ベースイメージのアーキテクチャと Windows プレインストールでサポートされているアーキテクチャによって異なります。

WinPE ブートイメージ、x86 または x64、あるいはその両方のイメージが作成されます。 Windows 10 用の HP Windows PE ドライバパックには、64 ビットブートイメージ用のドライバが含まれています。以前のバージョンの Windows 用の Windows PE ドライバパックには、32 ビットと 64 ビットの両方のブートイメージ用のドライバが含まれています。

プロセスが完了すると、新しブートイメージが[ブートイメージ]→[HP Client Boot Images]に作成されます。

WinPE の起動時にデバッグ目的でコマンドプロンプトを使用するには以下の設定を行います。

1. ブートイメージを右クリックして[プロパティ]→[カスタマイズ]を選択します。
2. [コマンドサポートを有効にする（テストのみ）]を有効にします。

これらのブートイメージをタスクシーケンスで使用する前に、ブートイメージを配布ポイントにプッシュする必要があります。インポートプロセスで配布ポイントが選択されていない場合、追加の配布ポイントが必要な場合、またはブートイメージのプロパティに変更がある場合は、ブートイメージを選択してから[コンテンツの配布]を選択します。

16 HP Client Task Sequences

16.1 展開タスクシーケンスの作成

1. Configuration Manager で、[ソフトウェアライブラリ]→[概要]→[オペレーティングシステム]→[タスクシーケンス]の順に選択します。

2. リボンメニューの[Create Deployment Task Sequence]を選択します。

3. Task Sequence Template のドロップダウンメニューからテンプレートを選択します。

   以下の例は、展開プロセスを支援するために HP のツールを参照する方法を示します。

4. 画面の指示に従って情報を入力します。

5. BitLocker ドライブ暗号化（BDE）を使用しない場合は、[Include BitLocker Drive Encryption steps]オプションをオフにします。 Configuration Manager BDE 手順の詳細については、https://technet.microsoft.com/enus/library/hh846237.aspx を参照してください。

6. [Create]を選択して、HP クライアントシステム用の基本的なベアメタル展開タスクシーケンスを作成します。タスクシーケンスが正常に作成されたことを示すメッセージボックスが表示されます。

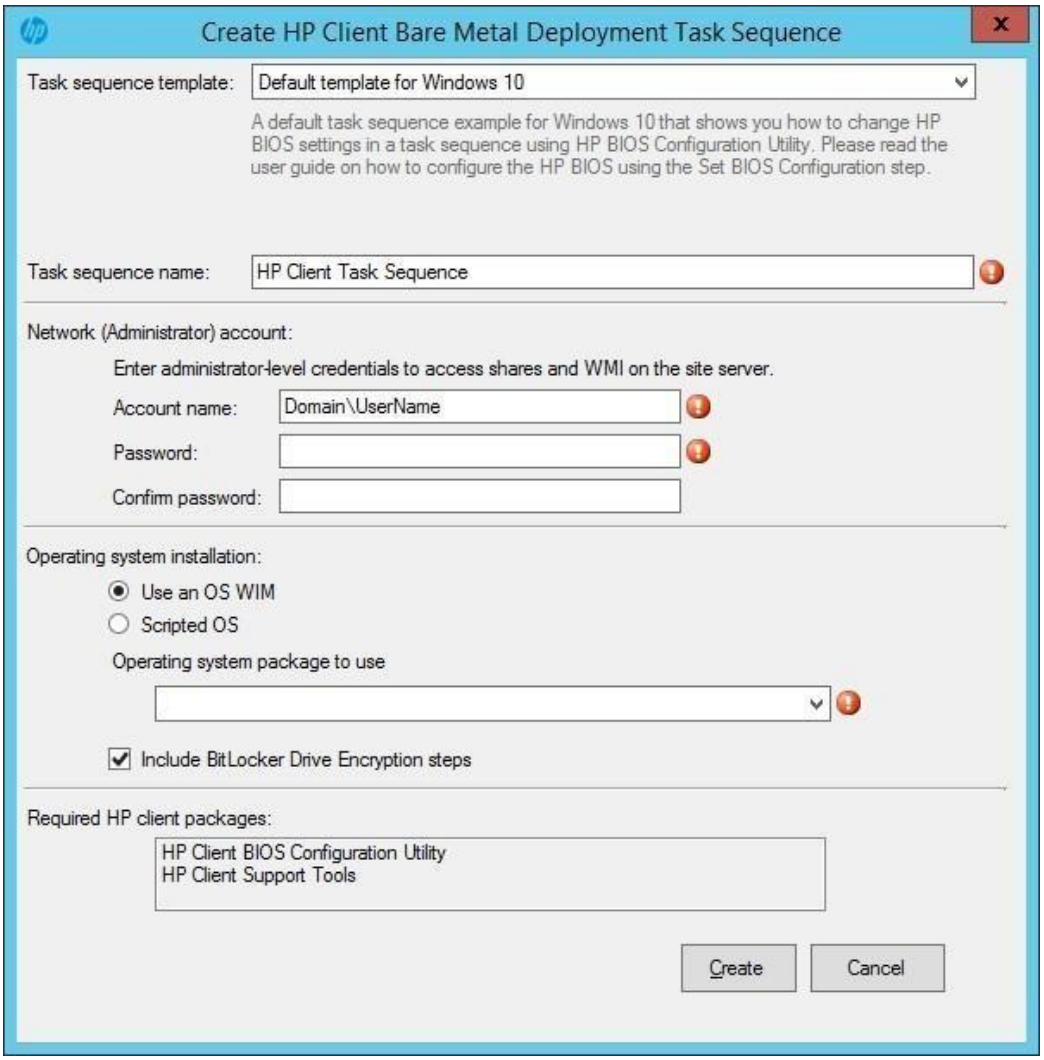


Figure 54 HP Client Bare Metal Deployment Task Sequence

重要!

選択したテンプレートに応じて、作成したタスクシーケンスの一部の手順は以下のようにシステムを初期化します。

- ディスクパーティションの削除 (diskpart clean)
- フォーマットとディスクパーティションの作成
- Intel RSTCli ユーティリティの実行 – すべてのメタデータの削除
- Intel RSTCli ユーティリティの実行 – RAID ボリュームの構成

作成したタスクシーケンスはテスト環境で十分に検証してから本番環境で実行するようにしてください。HP ではこれらのタスクシーケンスの実行によるいかなるデータ消失に対しても責任を負いかねます。

16.2 タスクシーケンスの設定

作成したタスクシーケンスを表示するためにタスクシーケンスのリストを更新します。タスクシーケンスを使用する前に、タスクシーケンスが正常に実行されるように追加の設定を実施する必要があります。

Configure RAID Example テンプレート特有の手順は Configure RAID Example テンプレートの使用で説明します。

1. 対象のクライアントコンピュータのドライバーパックがインポートされている事を確認します。詳細は HP ドライバーパックのインポートを参照してください。

2. タスクシーケンスを右クリックして[編集]を選択します。

   次の図は、Windows 7 または Windows 8 用の既定のテンプレートによって作成されたタスクシーケンスです。このタスクシーケンスは、Windows 7 または Windows 8 のどちらでも使用できます。

   Windows 10 用のデフォルトのテンプレートもあります。テンプレート内のデフォルトのディスクパーティション設定は異なります。 Windows 10 の場合、推奨される Windows 回復ツールパーティションはドライブの最後にあります。 Windows の以前のバージョンでは、それは始めにありました。デフォルトのパーティションはディスク容量の 1%を占めます。この値を Windows のリカバリイメージのサイズ、通常少なくとも 500 メガバイト（MB）に変更します。

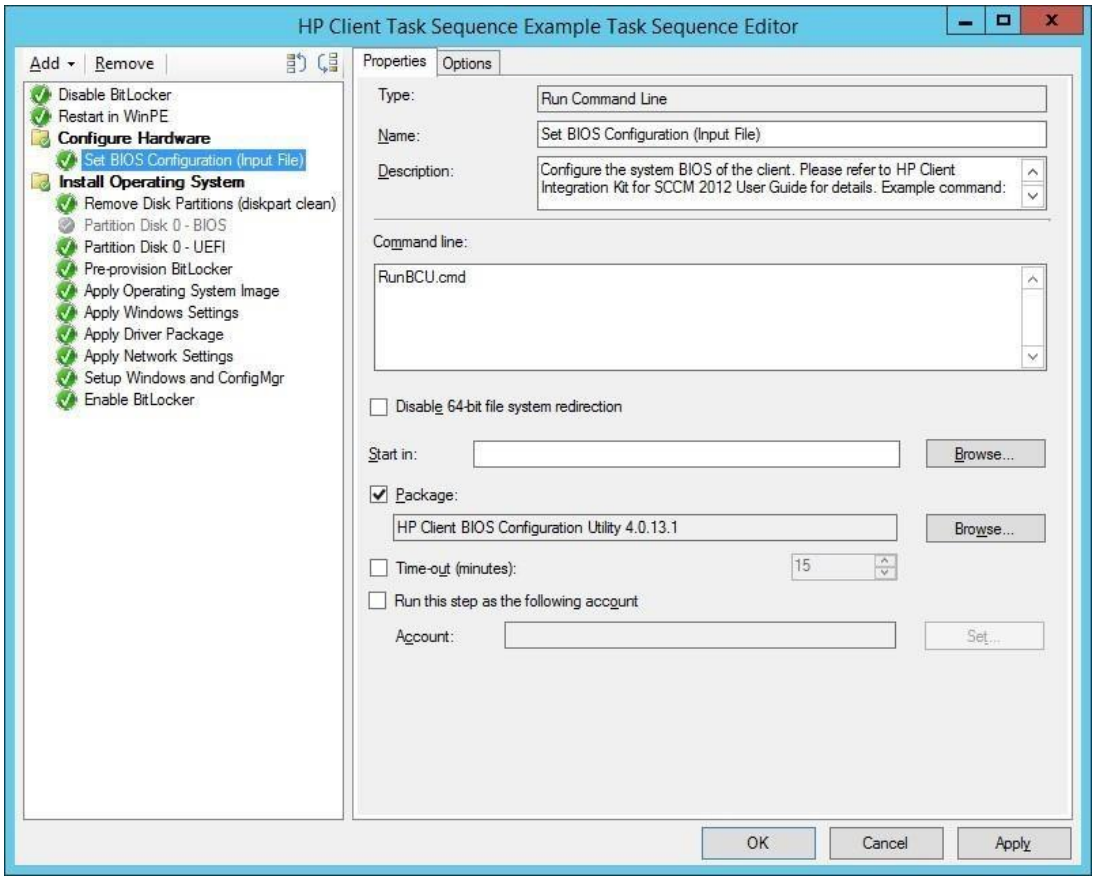


Figure 55 HP Client Task Sequence Example Task Sequence Editor

3. 展開対象の OS に応じて、次の手順の一部または全部を設定する必要があります。

   - Set BIOS Configuration (Input File)—BIOS Configuration Utility を使用して BIOS 設定を変更できるようにします。TPM は使用する前に有効にして初期化されている必要があります。詳細については、Set BIOS Configuration タスクステップの設定 を参照してください。
   - Remove Disk Partitions (diskpart clean)—このステップの設定へ不要です。ただし、すべてのディスクシナリオでタスクシーケンスを正しく実行するには、展開、およびその中のすべてのパッケージとコンテンツを、ネットワークから直接アクセスできるように構成する必要があります。詳細は、 展開コンテンツへのアクセス許可 を参照してください。
   - Format & Partition Disk—必要に応じてディスクのフォーマットとパーティションの作成のための手順を有効にします。例えば、UEFI または UEFI ハイブリッド（CSM あり）に設定されているシステムに展開する場合は、EFI フォーマットステップを有効にして BIOS フォーマットステップが無効になっていることを確認してください。
   - Apply Driver Package—展開する OS イメージに追加するための HP ドライバーパックを選択します。
   - Apply Network Settings—展開におけるワークグループまたはドメインのオプションを指定します。Active Directory ドメインに参加する場合は適切なアカウント情報を入力します。必要に応じて、追加のタスクシーケンス手順を確認し、必要なパラメータを設定します。

4. すべてのタスクシーケンスステップを設定したら、[OK]または[適用]をクリックして変更を保存します。実行したい操作のために、必要に応じてタスクシーケンスを設定変更したり、ステップを追加することができます。

16.2.1 ブートイメージの割当て

1. タスクシーケンスを右クリックして[プロパティ]を選択します。
2. [詳細設定]タブを選択し、[ブートイメージを使用する]をクリックして有効にします。
3. [参照]をクリックして HP Client Boot Images フォルダーから適切なブートイメージを選択します。

注記:
ブートイメージは展開する OS イメージと同じアーキテクチャのものを選択します。例えば、x86/32-bit OS の場合は x86 イメージを、x64/64-bit OS の場合は x64 イメージを選択します。

16.2.2 展開コンテンツへのアクセス許可

HP MIK タスクシーケンスを正しく実行するためには、Remove Disk Partitions (diskpart clean)ステップをネットワークから直接実行する必要があります。これを行うには、タスクシーケンスのパッケージとコンテンツ（ブートイメージを含む）のすべてを次のように構成する必要があります。

1. コンテンツ/パッケージを右クリックして[プロパティ]を選択します。
2. [データアクセス]タブを選択し、[このパッケージの配布ポイントのパッケージ共有にコピーする]をクリックして有効にします。
3. [OK]をクリックします。

4. 必要に応じて、ウィザードの配布ポイントステップで、[配布ポイントから直接コンテンツにアクセスする]オプションを選択します。

   この手順が不要な場合、またはダウンロードコンテンツ設定を使用する場合は、このタスクシーケンス手順を無効にします。コンテンツをローカルにダウンロードするオプションが選択されている場合でも、このステップを実行できるようにする必要がある場合は、 Remove Disk Partitions (diskpart clean) ステップが必要だがコンテンツに直接アクセスするオプションが使用できない場合 を回避策として参照してください。

5. タスクシーケンスが必要に応じて変更および修正されたら、ターゲットコレクションに展開し、タスクシーケンスを使用するために必要に応じてコンテンツを配布します。画面上の指示に従ってこのプロセスを完了します。

16.3 Set BIOS Configuration タスクステップの設定

Set BIOS Configuration (Input File) タスクステップでは HP の管理されたプラットフォームの BIOS 設定を変更することができます。このコマンドラインの実行タスクは BCU（BIOS Configuration Utility）を使用します。

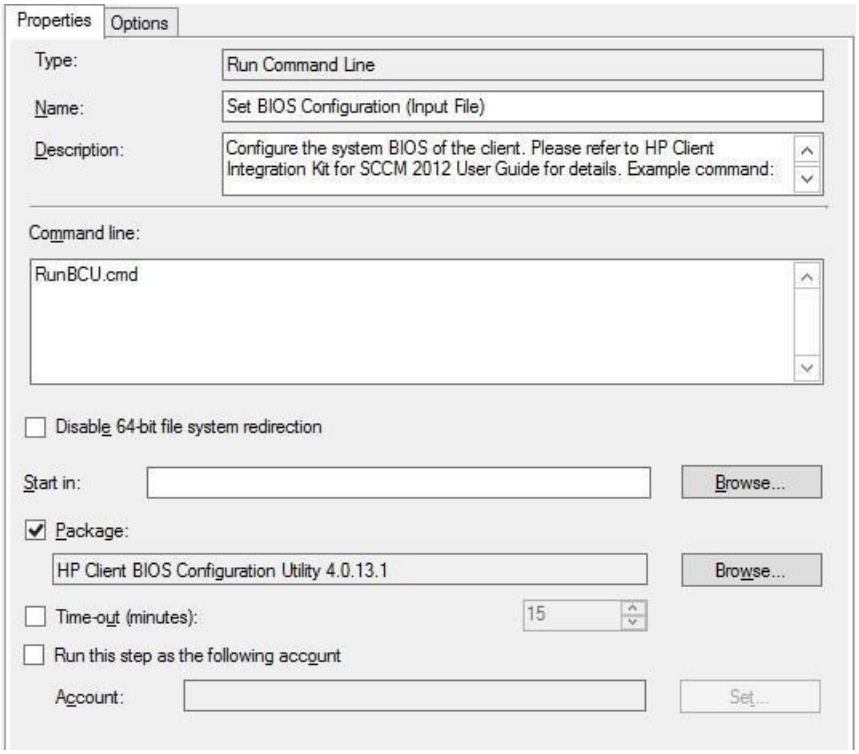


Figure 56 Configuring the Set BIOS Configuration task step

このタスクシーケンスステップでは以下のコマンドラインを実行します。

RunBCU.cmd <BCU に渡すパラメータ>

パラメータやオプションの一覧は *HP BIOS Configuration Utility User Guide* を参照してください。

この操作は、選択された REPSET ファイルで指定された BIOS 設定を適用したり、指定されたコマンドラインオプションを実行したりします。バッチファイルは、現在のオペレーティングシステムのアーキテクチャに応じて適切なバージョンの BCU を呼び出します。

REPSET ファイルの例がパッケージに含まれています。 パッケージのソースフォルダの Config フォルダにあり、BCUSettingExampleOnly.REPSET という名前です。この REPSET ファイルをこのタスクステップで使用する場合、コマンドラインは次のようになります。

RunBCU.cmd /setconfig:"Config\BCUSettingExampleOnly.REPSET"

REPSET ファイルは、コマンドラインで簡単に参照できるように、パッケージのソースフォルダまたはサブフォルダに保存することをおすすめします。

16.3.1 設定ファイルの追加と編集

注記:
タスクシーケンスステップを使用する際は以下に注意してください。

- 変更を加えたり、パッケージフォルダに設定（REPSET）ファイルを追加した後は、必ず HP Client BIOS Configuration Utility パッケージを配布ポイントを更新して、新しい設定ファイルがタスクシーケンスで使用できるようにしてください。
- 一部の BIOS 設定の変更は、ターゲットクライアントの再起動後まで有効にならない可能性があります。すべての設定を確実に適用するために、再起動が必要になる場合があります。
- 特定の BIOS 設定を変更すると、タスクシーケンスが完了しない可能性があります。タスクシーケンスを広く展開する前に、必ず目的の BIOS 設定ファイルをテストしてください。
- BIOS パスワードで使用される特定の文字は、正しく機能するために特別なエスケープを必要とするかもしれません。詳細については、HP BIOS Configuration Utility User Guide を参照してください。

1. ターゲットプラットフォームから設定ファイルを取得し、新しい値を設定し、このコンフィギュレーションを通じて適用する必要のない設定と値を設定（REPSET）ファイルから削除して、ファイルを編集します。
2. BCU のパッケージソースフォルダの場所に移動します。デフォルトでは、パッケージは Configuration Manager のソフトウェアライブラリの[HP Client Support Packages]セクションにあります。
3. ソースフォルダの場所を選択して、設定（REPSET）ファイルをそのフォルダにコピーします。
4. 設定（REPSET）ファイルがタスクシーケンスで利用できるように配布ポイントを更新します。

16.4 タスクシーケンスリファレンスの更新

次のいずれかが当てはまる場合は、タスクシーケンスリファレンスを更新する必要があります。

- HP MIK をアンインストールしてから再インストールした。

- インストーラの修復オプションを使用して、HP Client Support Packages の一部または全部を削除し、再インストールした。

タスクシーケンスリファレンスを更新するには次のようにします。

1. タスクシーケンスを右クリックして[編集]を選択します。
2. 以下のテーブルの Action 列の内容に従います。

Table 2 Refreshing task sequence references

Task sequence step	Action
Set BIOS Configuration (Input File)	HP Client Support Packages フォルダの HP Client BIOS Configuration Utility パッケージを選択します。
Remove Disk Partitions (diskpart clean)	HP Client Support Packages フォルダの HP Client Support Tools パッケージを選択します。

16.5 RAID の設定例のテンプレートの使用

16.5.1 タスクシーケンスで使用するブートイメージの準備

1. WinPE ドライバパックのインポートとブートイメージの作成に示すように、ブートイメージに必要なドライバが含まれていることを確認します。
2. 次の手順で追加するドライバとの競合を避けるために、既存の Intel Rapid Storage Technology（Intel RST）RAID ドライバをすべて削除します。
3. ターゲットクライアントシステムをサポートする Intel Rapid Storage Technology RAID ドライバのバージョンをブートイメージに追加します。

16.5.2 タスクシーケンスで使用するパッケージの準備

1. HP ドライバパックのインポートの説明に従って、ターゲットプラットフォームのドライバパックがインポートされていることを確認します。

2. https://downloadcenter.intel.com にアクセスしてから、Smart Response Technology Command Line Interface Deployment Tool を検索します。ドライバのバージョンと一致するツールのバージョンを探し、画面の指示に従ってダウンロードします。

> **注記:**
> ドライバとコマンドラインツールのメジャーバージョンとマイナーバージョンの値は一致している必要があります。たとえば、コマンドラインツールのバージョン 12.8.x はドライバのバージョン 12.8.x と連動します。

3. ダウンロードしたファイルを展開します。展開したフォルダの中にある x64 と x86 の zip ファイルも展開する必要があります。

4. コマンドラインツールの展開したファイルとフォルダを、このツールのソフトウェアパッケージのソースとなる場所にコピーします。

5. ソースの場所を参照するソフトウェアパッケージを作成します。

16.5.3 タスクシーケンスステップの設定

1. **設定を開始するには、タスクシーケンスを右クリックして[編集]を選択します。**

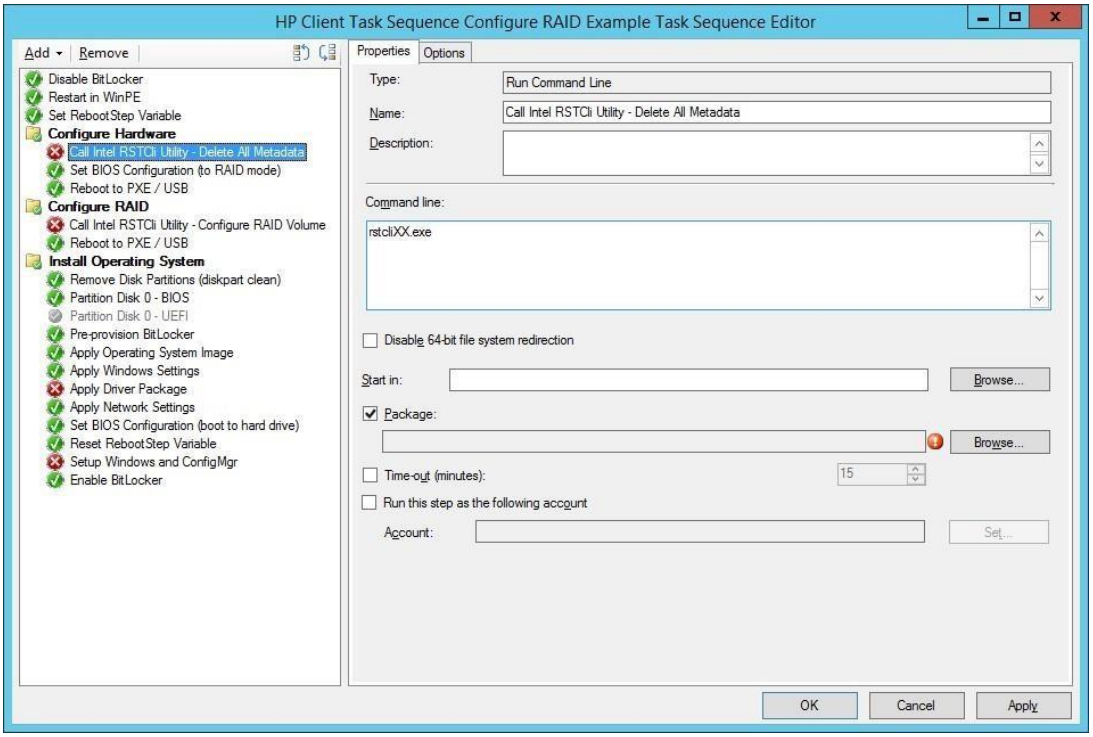


Figure 57 HP Client Task Sequence Configure RAID Example Task Sequence Editor

2. 以下のステップを設定する必要があります。

   a. Call Intel RSTCli Command Line Utility – Delete All Metadata—既存の構成済みディスクメタデータをすべて削除します。

i. コマンドの変更：このステップ内のコマンドライン rstcliXX.exe は単なる入力例です。ユーティリティのドキュメントを参照して、実際の環境に合わせて書き換えてください。前の準備ステップで設定したコマンドラインユーティリティを使用する必要があります。次はコマンドラインの例です。

IntelRSTCli\12.8\x64\rstcli64.exe --manage --delete – all-metadata

このコマンドライン例の、 IntelRSTCli\12.8\x64 はパッケージのソースフォルダからの相対パスです。

ii. 前のステップで準備した Intel コマンドラインツールを選択します。

b. Set BIOS Configuration (to RAID mode)—BCU を使用して BIOS 設定を変更します。詳細は Set BIOS Configuration タスクステップの設定を参照してください。

c. Call Intel RSTCli Command Line Utility – Configure RAID Volume—ターゲットクライアントの RAID ボリュームを設定します。

i. コマンドの変更: Delete all metadata のステップと同様に、このステップ内のコマンド rstcliXX.exe は単なる入力例です。ユーティリティのドキュメントを参照して、実際の環境に合わせて書き換えてください。前の準備ステップで設定したコマンドラインユーティリティを使用する必要があります。 次はハードドライブを RAID1（ミラー）に設定するコマンドラインの例です。

IntelRSTCli\12.8\x64\rstcli64.exe --create --level 1 – n Volume
0-0-0-0 0-10-0

IntelRSTCli\12.8\x64 はパッケージのソールフォルダからの相対パスです。

ii. 前のステップで準備した Intel コマンドラインツールを選択します。

d. Remove Disk Partitions (diskpart clean)—このステップの設定変更は不要です。ただし、タスクシーケンスですべてのディスクシナリオを正しく実行するには、展開、およびその中のすべてのパッケージとコンテンツをネットワークから直接コンテンツにアクセスできるように構成しておく必要があります。詳細は、 展開コンテンツへのアクセス許可を参照してください。

e. Format & Partition Disk—デフォルトでは、タスクシーケンスは BIOS（レガシー/ MBR）フォーマットステップが有効になっており、EFI（GPT）ステップが無効になっています。 UEFI または UEFI Hybrid（CSM あり）に設定されているシステムにデプロイする場合は、EFI フォーマットステップを有効にし、BIOS フォーマットステップを無効にします。

f. Apply Driver Pack—ターゲットプラットフォームおよびオペレーティングシステム用にインポートされた HP ドライバパックを指定します。

g. Require Reboot to PXE/USB—このタスクシーケンスでは、ディスクがまだ定義されていないときに WinPE で 1 回以上の即時再起動が必要であるため、RebootStep 変数を使用してタスクシーケンスの流れを制御します。

3. 各タスクシーケンス手順を確認し、残りのタスク手順に必要なパラメータを設定します。これらの手順が機能しない場合は、タスクシーケンス作成ダイアログで正しいネットワーク認証情報が入力されていることを確認してください。

4. すべてのタスクシーケンス手順を設定したら、[OK]または[適用]を選択して変更を保存します。タスクシーケンスを変更や、必要に応じてタスクシーケンスステップを追加して、必要な操作を実行できます。

16.5.4 ブートイメージの割り当て

1. タスクシーケンスを右クリックして[プロパティ]を選択します。
2. [詳細設定]タブを選択し、[ブートイメージを使用する]をクリックして有効にします。
3. [参照]をクリックして、HP Client Boot Images フォルダから Intel RST RAID ドライバーを追加したブートイメージを選択します。

注記:
ブートイメージはデプロイメント対象の OS と同じアーキテクチャのものを選択します。例えば、x86/32-bit OS の場合は x86 イメージを、x64/64-bit OS の場合は x64 イメージを選択します。

16.5.5 展開コンテンツへのアクセス許可設定

正しく実行するには、HP MIK RAID の構成例タスクシーケンスの[ディスクパーティションの削除（diskpart clean）]ステップをネットワークから直接実行する必要があります。これを行うには、タスクシーケンス内のすべてのパッケージとコンテンツ（ブートイメージを含む）を次のように構成する必要があります。

1. コンテンツ/パッケージを右クリックして[プロパティ]を選択します。
2. [データアクセス]タブを選択し、[このパッケージのコンテンツを配布ポイントのパッケージ共有にコピーする]をクリックして有効にします。
3. [OK]をクリックします。
4. 展開するときに、ウィザードの[配布ポイント]ステップで[配布ポイントから直接コンテンツにアクセスする]オプションを選択できます。
5. タスクシーケンスが必要に応じて変更および修正されたら、ターゲットコレクションに展開し、タスクシーケンスを使用するために必要に応じてコンテンツを配布します。画面上の指示に従ってこのプロセスを完了します。

16.5.6 タスクシーケンスの実行フローの理解

タスクシーケンスは次の 3 つのグループに分類されます。—Configure Hardware（ハードウェアの設定）、Configure RAID（RAID の設定）、Install Operating System（OS のインストール）。

3 つのグループの条件とコンピューター変数を使用して、PXE / USB を介した複数回の再起動を伴うタスクシーケンスの処理を制御します。Set RebootStep Variable タスクは、実行されるたびに RebootStep 変数を 1 つずつ増やします。変数が存在しない場合は、変数が作成され、0 に設定されます。

タスクシーケンスの最初の実行中に、[Configure Hardware]グループのタスクが実行されます。再起動後、タスクシーケンスを再実行すると、Set RebootStep Variable タスクは RebootStep の値を 2 に増やします。

Configure Hardware グループには RebootStep 変数の値が 1 の場合にのみ実行されるという条件があるため、このグループは再起動後にスキップされます。次のグループである Configure RAID Volume の設定では、RebootStep の値が 2 であることを確認してから実行されます。最後のグループである Install Operating System は、RebootStep 値が 3 であることを探します。この条件が満たされると、ステップの 3 番目のグループが実行されます。

タスクシーケンスの終了に向かい、Reset RebootStep Variable タスクは RebootStep をゼロ（0）にリセットします。

タスクシーケンスの展開に関する次の点に注意してください。

- PXE / USB から再起動してタスクシーケンスを展開する場合は、[配布ポイント]画面で、実行中のタスクシーケンスで必要に応じて展開オプションを[配布ポイントからコンテンツに直接アクセスする]に設定します。このオプションをタスクシーケンスで参照される各パッケージで使用できるようにするには、[プロパティ]ダイアログボックスの[データアクセス]タブを選択し、[このパッケージの内容を配布ポイントのパッケージ共有にコピーする]を選択します。
- タスクシーケンスが[必須]ではなく、[利用可能]として展開されている場合は、再起動時にタスクシーケンスを選択して展開を続行する必要があります。
- この手順を正しく機能させるには、ターゲットのクライアントシステムで適切な起動順序が再起動用に設定されている必要があります。（つまり、PXE 経由で起動する場合、PXE NIC は起動順序で他のどの起動デバイスよりも前にある必要があります。）ターゲットのクライアントシステムで必要なタスクシーケンスを再実行するには、PXE advertisement を消去します。

    a. Configuration Manager で[資産とコンプライアンス]を選択します。

    b. [デバイス]を選択します。

    c. ターゲットのクライアントシステムを選択します

    d. リボンから[要求された PXE 展開を削除する]を選択します。

- タスクシーケンスの実行に失敗してしまう場合は、以下のようにして RebootStep 変数の値をクリアまたはリセットする必要がある場合があります。

    a. ターゲットのクライアントシステムを右クリックして[プロパティ]を選択します。

    b. [変数]タブを選択します。

    c. RebootStep 変数を選択し、削除ボタン（X）を選択します。

17 HP BIOS Configuration Utility (BCU)

BCU は、以下のことを可能にする無料のツールです。

- サポートされているデスクトップ、ワークステーション、またはノートブックコンピュータから利用可能な BIOS 設定とその値を読み取る。
- サポートされているデスクトップ、ワークステーション、またはノートブックコンピュータでセットアップパスワードを設定またはリセットする。
- 複数のクライアントコンピュータ間で BIOS 設定を複製する。

詳細は HP BIOS Configuration Utility ユーザーガイドを参照してください。

注記:
HP MIK に含まれているバージョンの BCU には、現在のオペレーティングシステムを自動的に検出して正しいバージョンの BCU（32 ビットまたは 64 ビット）を実行するバッチファイル（RunBCU.cmd）が含まれています。

18 HP Sure Click

HP Sure Click は、インターネットを閲覧する際にコンピュータを保護します。Sure Click をインストールすると、Web サイトをマイクロ VM の中で開くようになり、Web サイトによって実行される悪意のあるコードがマイクロ VM の中に制限されるため マルウェアがコンピュータに感染することを防ぐコンテナとして機能します。

以下の HP Sure Click の機能が MIK で管理できます。

- Sure Click のアクティブ化（初期設定）
- Sure Click の有効化の強制
- Sure Click の無効化の防止
- アプリケーション内の信頼済みサイトの更新

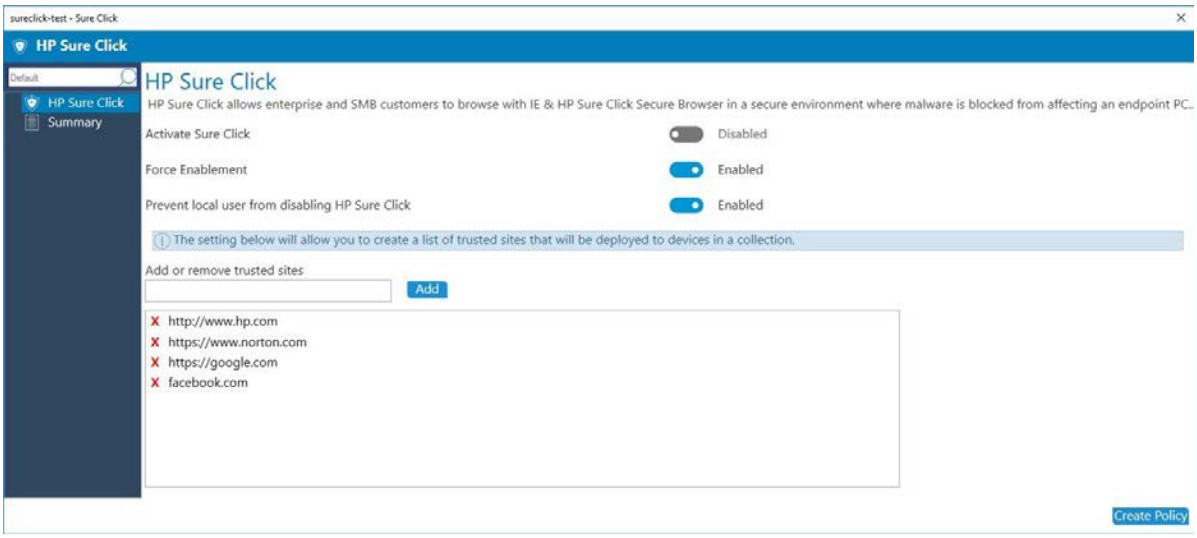


Figure 58: HP Sure Click Options Screen

19 HP Password Utility

HP Password Utility は、BCU パスワードファイルパラメータで使用できる暗号化パスワードファイルを作成するためのツールです。このツールは BCU に含まれています。詳細は、 HP BIOS Configuration Utility ユーザーガイドを参照してください。

20 HP Collaboration Keyboard

HP Collaboration Keyboard ソフトウェアは、特定の HP キーボードの組み込みコントロールを使用して電話会議を管理するために使用されます。

HP MIK を使用して、ソフトウェアの次の機能を管理できます。

- デフォルトの会議アプリの指定

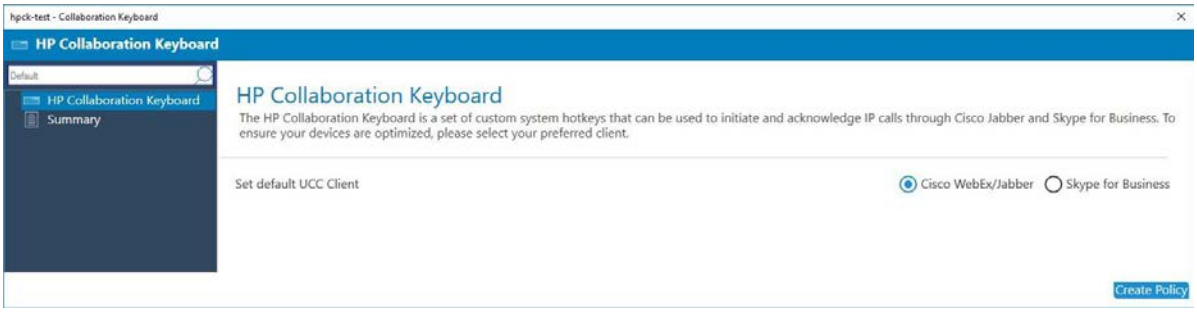


Figure 59: HP Collaboration Keyboard options

21 HP MIK のアンインストール

1. コントロールパネルで[プログラムと機能]を選択します。
2. [HP Manageability Integration Kit]を選択し、[アンインストール]を選択します。

インポートされたドライバパッケージとブートイメージ、および HP MIK によって作成されたタスクシーケンスは、サーバー上に残ります。サポートしているクライアントパッケージとソースファイルは削除されます。ただし、BIOS 設定ファイルを保存するために、BCU のソースフォルダは削除されません。

22 付録 A—デバイスコレクションクエリの例

IT 管理者は Configuration Manager のクエリルールで定義されているデバイスコレクションを作成できます。デバイスコレクションとクエリルールの作成方法の詳細については、https://technet.microsoft.com/en-us/library/gg712295.aspx を参照してください。

注記:
テスト環境でデバイスコレクションクエリを検証して、サポートされているシステムへのソフトウェアおよびポリシーの正確な展開を確認してから、クエリを実稼働環境で実施することをおすすめします。

以下は、HP システムおよび HP MIK 機能を使用する際の出発点として使用できる基本的な HP コレクションクエリです。

22.1 すべての HP システム

注記:
古いモデルでは、製造元として Hewlett-Packard という名前が付けられている場合があります。これらのシステムを含めるためには、照会に条件が必要な場合があります。各 HP MIK 機能のサポートプラットフォームリストを確認して、機能を管理するための適切なシステムコレクションを作成してください。

```
select SMS_R_SYSTEM.ResourceID,

SMS_R_SYSTEM.ResourceType,

SMS_R_SYSTEM.Name,

SMS_R_SYSTEM.SMSUniqueIdentifier,

SMS_R_SYSTEM.ResourceDomainORWorkgroup,

SMS_R_SYSTEM.Client from SMS_R_System inner

join SMS_G_System_COMPUTER_SYSTEM on

SMS_G_System_COMPUTER_SYSTEM.ResourceId = SMS_R_System.ResourceId and
SMS_G_System_COMPUTER_SYSTEM.Manufacturer like 'HP%'
```

22.2 古いモデルを含むすべての HP システム

```
select SMS_R_SYSTEM.ResourceID,

SMS_R_SYSTEM.ResourceType,

SMS_R_SYSTEM.Name,

SMS_R_SYSTEM.SMSUniqueIdentifier,

SMS_R_SYSTEM.ResourceDomainORWorkgroup, SMS_R_SYSTEM.Client from SMS_R_System
inner join SMS_G_System_COMPUTER_SYSTEM on SMS_G_System_COMPUTER_SYSTEM.ResourceId
= SMS_R_System.ResourceId where

(SMS_G_System_COMPUTER_SYSTEM.Manufacturer like 'Hewlett-Packard%' and
SMS_G_System_COMPUTER_SYSTEM.Model not  like '%Proliant%') or
SMS_G_System_COMPUTER_SYSTEM.Manufacturer like 'HP%
```

22.3 特定のモデル名の HP システム

```
select SMS_R_SYSTEM.ResourceID,

SMS_R_SYSTEM.ResourceType,

SMS_R_SYSTEM.Name,

SMS_R_SYSTEM.SMSUniqueIdentifier,

SMS_R_SYSTEM.ResourceDomainORWorkgroup,

SMS_R_SYSTEM.Client from SMS_R_System

inner join SMS_G_System_COMPUTER_SYSTEM on SMS_G_System_COMPUTER_SYSTEM.ResourceId
= SMS_R_System.ResourceId and

SMS_G_System_COMPUTER_SYSTEM.Model = 'HP EliteBook 850 G4'
```

22.4 Windows 10 Enterprise システム

```
select SMS_R_SYSTEM.ResourceID,

    SMS_R_SYSTEM.ResourceType,

    SMS_R_SYSTEM.Name,

    SMS_R_SYSTEM.SMSUniqueIdentifier,

    SMS_R_SYSTEM.ResourceDomainORWorkgroup,

    SMS_R_SYSTEM.Client from SMS_R_System inner join

SMS_G_System_COMPUTER_SYSTEM on
```

```
SMS_G_System_COMPUTER_SYSTEM.ResourceId = SMS_R_System.ResourceId and
SMS_G_System_COMPUTER_SYSTEM.Manufacturer like 'HP%'

inner join SMS_G_System_Operating_System on SMS_R_System.ResourceID =

SMS_G_System_Operating_system.ResourceID and

SMS_G_System_Operating_System.Caption  like '%Windows%10%Enterprise%'
```

22.5 デバイスガードを有効にできるかどうかの判断

どのシステムで Device Guard を有効にできるかを判断するには、https://blogs.technet.microsoft.com/enterprisemobility/2015/10/30/managing-windows-10-device-guardwithconfiguration-manager/ にアクセスし、Determine applicable systems section の手順に従ってください。

23 HP Sure Start をサポートするシステム

HP Manageability Integration Kit を搭載したすべての HP クライアントコンピュータでは、HP Sure Start サポート情報は、Configuration Manager ハードウェアインベントリ拡張機能を通じて取得できます。

HP_SureStartPolicy BIOS Sure Start 設定と Sure Start のバージョン情報を Configuration Manager のデフォルトのクライアント設定に追加するには、次の手順を実行します。

1. Configuration Manager で、[管理]→[クライアント設定]の順に選択します。
2. [デフォルトクライアント設定]を右クリックして、[プロパティ]を選択します。
3. デフォルト設定ウィンドウで、[ハードウェアインベントリ]を選択し、[クラスの設定]を選択します。
4. ハードウェアインベントリクラスウィンドウで、[追加]を選択します。
5. ハードウェアインベントリクラスの追加ウィンドウで、[接続]を選択します。
6. HP MIK クライアントがインストールされている HP システムに Configuration Manager がインストールされている場合、デフォルトのコンピュータ名（コンソールがあるシステム）をそのまま使用します。それ以外の場合、HP MIK クライアントがインストールされているシステムの名前を指定してください。
7. WMI 名前空間に root\HP\InstrumentedServices\v1 を入力します。
8. [再帰]を選択し、指定したシステムの WMI に接続するためのユーザー名とパスワードを入力します。
9. HP_SureStartPolicy クラスを追加します。クラスをハードウェアインベントリに追加するには、[OK]を選択します。

クライアントコンピュータが更新されたコンピュータポリシーをダウンロードしてハードウェアインベントリサイクルを実行した後、拡張データは Configuration Manager に報告されます。データはその後、コレクションを作成するために利用可能です。

以下は、HP Sure Start をサポートするすべての HP システムを選択するためのクエリです。

```
select SMS_R_SYSTEM.ResourceID, SMS_R_SYSTEM.ResourceType,
```

```
SMS_R_SYSTEM.Name,

SMS_R_SYSTEM.SMSUniqueIdentifier,

SMS_R_SYSTEM.ResourceDomainORWorkgroup,

SMS_R_SYSTEM.Client from SMS_R_System inner join

SMS_G_System_COMPUTER_SYSTEM on

SMS_G_System_COMPUTER_SYSTEM.ResourceId = SMS_R_System.ResourceId and
SMS_G_System_COMPUTER_SYSTEM.Manufacturer like 'HP%'

inner join SMS_G_System_HP_SureStartPolicy on SMS_R_System.ResourceId =

SMS_G_System_HP_SureStartPolicy.ResourceId and

SMS_G_System_HP_SureStartPolicy.SureStartVersion like 'SS%'
```

23.1 TPM クエリ

これらの TPM クエリの例では、クライアントからの ROOT \ cimv2 \ Security \ MicrosoftTpm 名前空間の Win32_TPM クラスの TPM データを使用しています。この TPM クラスがハードウェアインベントリに追加されていることを確認してください。クライアントコンピューターが最新のコンピューターポリシーを適用し、そのハードウェアインベントリデータが Configuration Manager に報告されたことを報告するときは、クライアントを適切な TPM コレクションに含める必要があります。

23.1.1 TPM バージョン 1.2 のシステム

```
select SMS_R_SYSTEM.ResourceID,

SMS_R_SYSTEM.ResourceType,

SMS_R_SYSTEM.Name,

SMS_R_SYSTEM.SMSUniqueIdentifier,

SMS_R_SYSTEM.ResourceDomainORWorkgroup, SMS_R_SYSTEM.Client from

SMS_R_System inner join SMS_G_System_COMPUTER_SYSTEM on

SMS_G_System_COMPUTER_SYSTEM.ResourceId = SMS_R_System.ResourceId and
SMS_G_System_COMPUTER_SYSTEM.Manufacturer like 'HP%' inner join
SMS_G_System_TPM on SMS_R_System.ResourceId = SMS_G_System_TPM.ResourceId
and MS_G_System_TPM.SpecVersion like '1.2%'
```

23.1.2 TPM バージョン 2.0 のシステム

```
select SMS_R_SYSTEM.ResourceID,

SMS_R_SYSTEM.ResourceType,

SMS_R_SYSTEM.Name,

SMS_R_SYSTEM.SMSUniqueIdentifier,
```

```
SMS_R_SYSTEM.ResourceDomainORWorkgroup, SMS_R_SYSTEM.Client from

SMS_R_System inner join SMS_G_System_COMPUTER_SYSTEM on

SMS_G_System_COMPUTER_SYSTEM.ResourceId = SMS_R_System.ResourceId and
SMS_G_System_COMPUTER_SYSTEM.Manufacturer like 'HP%' inner join
SMS_G_System_TPM on SMS_R_System.ResourceId = SMS_G_System_TPM.ResourceId
and SMS_G_System_TPM.SpecVersion like '2.0%'
```

23.2 特定のアプリケーションがインストールされているシステム

```
select SMS_R_SYSTEM.ResourceID,

SMS_R_SYSTEM.ResourceType,

SMS_R_SYSTEM.Name,

SMS_R_SYSTEM.SMSUniqueIdentifier,

SMS_R_SYSTEM.ResourceDomainORWorkgroup, SMS_R_SYSTEM.Client from
SMS_R_System

inner join SMS_G_System_COMPUTER_SYSTEM on
SMS_G_System_COMPUTER_SYSTEM.ResourceId = SMS_R_System.ResourceId  and
SMS_G_System_COMPUTER_SYSTEM.Manufacturer like 'HP%' and
(SMS_R_System.ResourceId in (select ResourceId from

SMS_G_System_ADD_REMOVE_PROGRAMS_64 where ProdID = '<Application product
ID>' and Version

>= '<Miminum supported application version>')

or (SMS_R_System.ResourceId in (select ResourceId from
SMS_G_System_ADD_REMOVE_PROGRAMS where ProdID = '<Application product ID>'
and Version >= '<Miminum supported application version>')))
```

例えば、次のクエリは、HP WorkWise バージョン 1.3.1.1 以降がインストールされているシステムを返します。

```
select SMS_R_SYSTEM.ResourceID,

SMS_R_SYSTEM.ResourceType,

SMS_R_SYSTEM.Name,

SMS_R_SYSTEM.SMSUniqueIdentifier,

SMS_R_SYSTEM.ResourceDomainORWorkgroup, SMS_R_SYSTEM.Client from
SMS_R_System

inner join SMS_G_System_COMPUTER_SYSTEM on
SMS_G_System_COMPUTER_SYSTEM.ResourceId =  SMS_R_System.ResourceId  and
SMS_G_System_COMPUTER_SYSTEM.Manufacturer like 'HP%' and
(SMS_R_System.ResourceId in (select ResourceId from

SMS_G_System_ADD_REMOVE_PROGRAMS_64 where ProdID = '{56051A5A-7A04-
4CD4A5CD-
```

```
781F1AC10112}' and Version >= '1.3.1.1')

or (SMS_R_System.ResourceId in (select ResourceId from
SMS_G_System_ADD_REMOVE_PROGRAMS where ProdID = '{56051A5A-7A04-4CD4-A5CD-
781F1AC10112}' and Version >= '1.3.1.1') ))
```

23.3 HP Client Security のために Intel Authenticate または有効な Intel Authenticate ポリシーが適用されているシステム

HP Client Security（HP MIK サポート付き）がインストールされているすべての HP システムでは、CM_IntelAuthenticatePolicies のプロパティ State と IsValidPolicyInstalled の WMI クラスは Configuration Manager ハードウェアインベントリ拡張機能を介して取得できます。

CM_IntelAuthenticatePolicies を Configuration Manager の既定のクライアント設定に追加するには、次の手順を実行します。

1. Configuration Manager で、[管理]→[クライアント設定]の順に選択します。
2. [デフォルトクライアント設定]を右クリックし、[プロパティ]を選択します。
3. デフォルト設定ウィンドウで、[ハードウェアインベントリ]を選択し、[クラスの設定]を選択します。
4. ハードウェアインベントリクラスウィンドウで、[追加]を選択します。
5. ハードウェアインベントリクラスの追加ウィンドウで[接続]を選択します。
6. HP MIK クライアントがインストールされている HP システムに Configuration Manager がインストールされている場合、デフォルトのコンピュータ名（コンソールがあるシステム）をそのまま使用します。それ以外の場合、HP MIK クライアントがインストールされているシステムの名前を指定してください。
7. WMI 名前空間に root\HP\InstrumentedServices\v1 を入力します。
8. [再帰]を選択し、指定したシステムの WMI に接続するためのユーザー名とパスワードを入力します。
9. [CM_IntelAuthenticatePolicies]クラスを追加します。[OK]をクリックしてハードウェアインベントリに追加します。
10. [OK]をクリックします。再度[OK]をクリックしてすべてのウィンドウを閉じます。

クライアントコンピュータが更新されたコンピュータポリシーをダウンロードしてハードウェアインベントリサイクルを実行した後、拡張データは Configuration Manager に報告されます。データはその後、コレクションを作成するために利用可能です。

次の図は、クライアントコンピューターの CM_IntelAuthenticatePolicies WMI クラスを示しています。

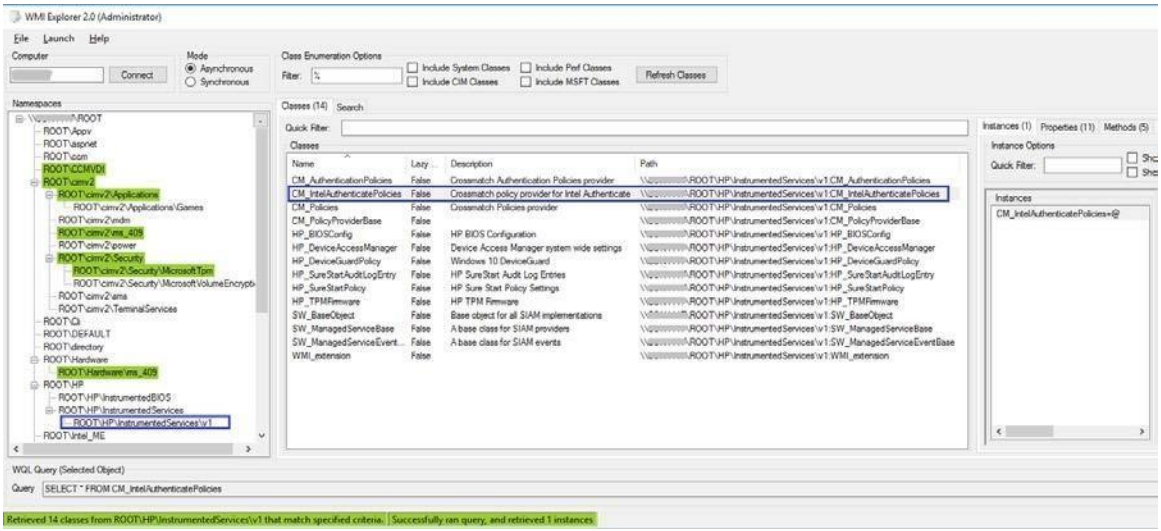


Figure 58 CM_IntelAuthenticatePolicies WMI Class

次のクエリは、HP Client Security のための Intel Authenticate ポリシーを受け取る準備ができているすべての HP システムを選択します。

```
select SMS_R_SYSTEM.ResourceID,
    SMS_R_SYSTEM.ResourceType,
    SMS_R_SYSTEM.Name,
    SMS_R_SYSTEM.SMSUniqueIdentifier,
    SMS_R_SYSTEM.ResourceDomainORWorkgroup,
SMS_R_SYSTEM.Client
```

```
from SMS_R_System inner join SMS_G_System_COMPUTER_SYSTEM on
SMS_G_System_COMPUTER_SYSTEM.ResourceId = SMS_R_System.ResourceId and
SMS_G_System_COMPUTER_SYSTEM.Manufacturer like 'HP%'

inner join SMS_G_System_CM_IntelAuthenticatePolicies on
SMS_R_System.ResourceId =
SMS_G_System_CM_IntelAuthenticatePolicies.ResourceId  and
SMS_G_System_CM_IntelAuthenticatePolicies.State = 'Active'
```

システムに Intel Authenticate がインストールされていない場合、State は NotInstalled を返します。これは、Intel Authenticate がインストールされていないか、インストールに失敗したことを意味します。 Intel Authenticate をインストールしてクライアントコンピュータを再起動し、HP Client Security がステータスの変化を検出できるようにします。

同様に、HP Client Security のための有効な Intel Authenticate ポリシーが有効になっているすべての HP システムを選択するためのクエリは次のとおりです。

```
select SMS_R_SYSTEM.ResourceID,

    SMS_R_SYSTEM.ResourceType,

    SMS_R_SYSTEM.Name,

    SMS_R_SYSTEM.SMSUniqueIdentifier,

    SMS_R_SYSTEM.ResourceDomainORWorkgroup,

SMS_R_SYSTEM.Client   from SMS_R_System inner join

SMS_G_System_COMPUTER_SYSTEM on

SMS_G_System_COMPUTER_SYSTEM.ResourceId = SMS_R_System.ResourceId and
SMS_G_System_COMPUTER_SYSTEM.Manufacturer like 'HP%'

inner join SMS_G_System_CM_IntelAuthenticatePolicies on
SMS_R_System.ResourceId =
SMS_G_System_CM_IntelAuthenticatePolicies.ResourceId

and SMS_G_System_CM_IntelAuthenticatePolicies.IsValidPolicyInstalled ='True'
```

システムに HP Client Security 用の有効な Intel 認証ポリシーがない場合、IsValidPolicyInstalled プロパティは False を返します。

24 付録 B—トラブルシューティング

24.1 HP MIK インストールの問題

サポートパッケージ（HP Client BIOS Configuration Utility または HP Client Support Tools）のインストール中にエラーが発生した場合、インストーラを実行しているユーザーアカウントに、Configuration Manager サーバーへのアクセスおよびデータの変更権限があることを確認するか、それらの権限を持つユーザーとしてログオンして再度インストールします。

HP MIK が完全にアンインストールされない
インポートされたドライバパック、作成されたブートイメージ、および HP MIK を介して作成されたタスクシーケンスは、製品をアンインストールしても削除されません。不要になった場合は、Configuration Manager から削除できます。

HP MIK を再インストールまたは修復した後、タスクシーケンスが実行されない
HP MIK を再インストールおよび/または修復するときに、HP MIK によってインストールされたパッケージを使用した既存のタスクシーケンスは自動的には更新されません。正しく機能するには、タスクシーケンスの参照を更新する必要があります（詳細については、タスクシーケンスの参照の更新を参照してください）。

24.2 ドライバーパックの問題

Configuration Manager が SoftPaq が有効なドライバーパックでないことを報告する
HP MIK では、[管理性 - ツール]カテゴリのドライバパックのみをインポートできます。他のカテゴリ（ソフトウェア - システム管理など）にリストされている他のドライバパックは、HP MIK では使用できません。

HP MIK がドライバーINF の処理中にドライバーパックのインポートプロセスを完了できない
これは、既存のドライバが検出されてもドライバのソースが見つからない場合に発生する可能性があります。既存のドライバのソースが存在することを確認してください。そうでない場合は、ドライバを削除してドライバパックを再インポートするか、足りないドライバソースを復元します。This might happen if an existing driver

24.3 WinPE イメージ作成の問題

いくつかの利用可能なブートイメージがベースブートイメージとして選択できない
Configuration Manager の各バージョンは、カスタマイズ、または特定のバージョンの WinPE へのドライバーおよびコンポーネントの追加のみをサポートしているため、HP MIK ブートイメージ作成機能では限定的なサポートしか提供できません。 WinPE のカスタマイズに関する特定の要件の詳細については、
http://technet.microsoft.com/en-us/library/dn387582.aspx を参照してください。

ブートイメージの作成中に ADK とサイトサーバーのオペレーティングシステムが一部のドライバーの署名を適切に確認できない場合は、この HP MIK エラーが発生する可能性があります。

```
Object version mismatch error; a ConfigMgr object has been modified or
updated before changes could have been saved. Please try the operation
again.
```

再試行に失敗した場合は、手動でドライバをカスタマイズするか、起動イメージに追加してください。

24.4 タスクシーケンスをトラブルシューティングする前に

- タスクシーケンス設定を確認します。タスクシーケンスの失敗の主な原因は、タスクシーケンスの手順で指定した設定に関連しています。次のタスクシーケンス手順を確認してください。
  - 有効な環境変数またはタスクシーケンス変数の参照。
  - 有効なパッケージの参照 - タスクシーケンスで参照されているすべてのパッケージが配布ポイントから利用可能であり、最新のものであることを確認する必要があります。
- タスクシーケンスが、現在インストールされているキットで作成されたのか、または更新される以前にインストールされたバージョンで作成されたのかを確認します。キットをアンインストールしてから再インストールした場合、または HP Client Support Package を削除したがセットアップによって再インストールした場合は、それらを使用するタスクシーケンス手順で HP パッケージを再度選択する必要があります。新しいパッケージ参照を使用してタスクシーケンスを更新する方法の詳細については、このドキュメントを参照してください。
- 一時ダウンロードしたドライバパックが HP MIK によって正しく削除されたことを確認します。
  - HP MIK によってダウンロードされたドライバパックは、%TEMP%\ hpdriverpack に格納されます。ここで、%TEMP%は、現在ログオンしているユーザーのデフォルトのアプリケーションの一時的な場所を定義する環境変数です。 HP MIK は、インポートが成功した後、ダウンロードしたドライバーパックを削除しようとします。
- ログファイルの確認
  - Configuration Manager コンソールのログファイルは AdminUILog フォルダーにあります。このフォルダは、Configuration Manager コンソールのインストールディレクトリにあります。
  - HP MIK によって生成されたログファイルは、%TEMP%\ hpclient に保存されます。ここで、%TEMP%は、現在ログオンしているユーザーのデフォルトのアプリケーションの一時的な場所を定義する環境変数です。

    レジストリにデバッグフラグを追加することで、拡張ログ情報をキットログファイルに追加できます。レジストリで、DebugLogging という名前の DWORD 値を追加し、該当するレジストリキーの値を 1 に設定します。

    HKLM\Software\Wow6432Node\HP\Client\ConfigMgr Integration Kit
  - 追加の適用可能なログファイルが Configuration Manager ログフォルダ（通常は次の場所にあります）にあります。

    %ProgramFiles%\Microsoft Configuration Manager\Logs).

24.5 タスクシーケンス共通の問題

以下は、発生する可能性があるいくつかの一般的な問題です。問題がここにリストされていない場合は、後続のトラブルシューティングのセクションで回答を得ることができます。

一部のドライバーがブートイメージに挿入されない

これは、DISM およびオペレーティングシステムがサポートしているものよりも新しいドライバ署名方法でドライバが署名されている場合に発生する可能性があります。その場合、ドライバは署名なしドライバとして扱われ、ブートイメージに挿入されません。たとえば、Windows Server 2008 R2 上で SCCM 2012 SP1 を実行している場合、一部の Windows 8 / 8.1 ドライバを Windows プレインストール環境のブートイメージに挿入することはで

きません。問題のドライバが環境に必要ない場合は、ブートイメージドライバリストからドライバを削除してから、残りのドライバを手動で再挿入します。詳細については、https://technet.microsoft.com/en-us/library/hh825070.aspx にアクセスしてください。

ターゲットプラットフォームが Windows プレインストール環境で起動した後にタスクシーケンスが開始されない

次のように、いくつかの原因が考えられます。

- ネットワークアダプタがサポートされていないため、ネットワーク接続ができない。
- ブートイメージに必要なネットワークドライバが含まれていないため、ネットワーク接続ができない。
- Configuration Manager は、ターゲットの HP クライアントプラットフォームを認識できない。
- タスクシーケンスで参照されている 1 つ以上のパッケージが利用できない。

これらの問題を解決するには次のようにします。

1. サポートされているネットワークアダプタを取り付け、それを PXE NIC として設定します。
2. 適切な HP WinPE ドライバパックを含む HP Client WinPE イメージを使用します。
3. ターゲットの HP クライアントプラットフォームが正しい識別情報で Configuration Manager にインポートされたことを確認します。
4. タスクシーケンスを開き、存在する可能性があるエラーを修正します。

タスクシーケンスの実行中に、更新された、または新しい BIOS 設定入力ファイルが使用されていないか使用できない

HP Client BIOS 設定ユーティリティパッケージが適切な配布ポイントにプッシュされたことを確認します。

タスクシーケンスは開始するが、続行できない

次のように、いくつかの原因が考えられます。

- BIOS 設定を変更すると、システムが正常に起動しなくなります。
- ターゲットプラットフォーム用に誤ったドライバパッケージが選択された。

この問題を解決するには次のようにします。

1. 特定のターゲットプラットフォームに正しいドライバパッケージが選択されていることを確認します。
2. タスクシーケンスのすべての依存関係が、対象のクライアントまたはコレクションがアクセスできる配布ポイントまたはグループに配布されていることを確認します。

タスクシーケンスを編集用に開くことができない、または特定のタスクシーケンスステップを表示しているときにエラーメッセージが表示される

次のように、いくつかの原因が考えられます。

- プラグインがアンインストールされた。（「タスクシーケンスオブジェクトに含まれるステップが多すぎる可能性があります」などのエラーメッセージが表示されることがあります。）
- プラグインが壊れています。

- HP MIK がプライマリサイトサーバーにインストールされていない。

この問題を解決するには次のようにします。

1. プラグインを再インストールして、必要なファイルがすべて存在し登録されていることを確認します。
2. プライマリサイトサーバーに HP MIK をインストールします。
3. プラグインのインストールを修復します。これは、セットアップを再度実行して[修復]を選択するか、[コントロールパネル]の[プログラムと機能]で[修復]オプションを選択することによって実行できます。
4. 新しいタスクシーケンスにタスクシーケンスを再作成します。
5. いくつかのタスクシーケンス手順についてパッケージを再選択します（タスクシーケンス参照の更新を参照）。

24.6 タスクシーケンスの作成と管理の問題

HP MIK によって作成されたタスクシーケンスを編集しようとすると“タスクシーケンスオブジェクトに含まれるステップ数が多すぎます”のエラーが表示される

このエラーは通常、HP MIK がサーバーからアンインストールされたときに表示されます。タスクシーケンスを表示または編集する前に、HP MIK をサーバーに再インストールする必要があります。

ディスクパーティションの削除（diskpart clean）手順が必要ですが、[直接コンテンツにアクセス]オプションを使用できません

以下の回避策があります。

- ネットワークフォルダに接続]タスクシーケンスステップを使用してパッケージファイルを含むネットワーク共有に接続し、[コマンドラインの実行]タスクを使用してネットワーク共有からステップを実行します。
- パッケージファイルをブートイメージに追加し、コマンドラインの実行タスクを使用してブートイメージのファイルを参照してステップを実行します。

これらのアクションを実行する方法について詳しくは、Configuration Manager の資料を参照してください。

24.7 タスクシーケンス実行の問題

システムが PXE ブートに失敗する

クライアントコンピュータが HP ElitePad 900 などの EFI x86（IA-32）の場合、PXE ブートを正常に機能させるには、Configuration Manager 2012 SP1 用の累積的な更新プログラム 1（KB2817245）をインストールする必要があります。Configuration Manager 2012 R2 ではこの更新プログラムは不要です。

PXE は、ブロードキャストタイプの通信を使用する DHCP の拡張です。ブロードキャスト通信は標準のタイムアウト値を使用しますが、これはすぐには変更できません。その結果、コンピュータは、タイムアウトして障害状態が発生する前に、デフォルトの時間枠で DHCP または PXE 応答を受信するのを待ちます。コンピュータを再起動するたびに、スイッチとの接続を再交渉する必要があります。一部のネットワークスイッチは、接続の遅延を引き起こす可能性があるデフォルト設定で設定されて到着します。スイッチの設定は、時間内に接続をネゴシエートできないため、DHCP または PXE のタイムアウトを引き起こす可能性があります。

以下の機能は、ネゴシエーションタイムアウトによって影響を受ける可能性があります。

1. Spanning Tree Protocol (STP)— STP はループを防ぎ、ネットワーク内で冗長性を提供するプロトコルです。このアルゴリズムを使用するネットワーキングデバイスは、他のネットワークデバイスに関する情報を収集するため、ある程度の待ち時間が発生する可能性があります。この情報収集期間中、サーバーは PXE から起動し、Windows 展開サービスからの応答を待っている間にタイムアウトすることがあります。これらの問題を回避するには、STP を無効にするか、ターゲットサーバーのエンドノードポートで PortFast を有効にします。詳細については、製造元のマニュアルを参照してください。
2. EtherChannel or Port Aggregation Protocol (PAgP)— EtherChannel を使用すると、デバイス間の複数のリンクが 1 つの高速リンクとして機能し、リンク間で負荷を共有できます。自動モードで EtherChannel プロトコルを実行すると、最大 15 秒の接続遅延が発生する可能性があります。この遅延を解消するには、手動モードに切り替えるか、この機能をオフにしてください。
3. Speed and duplex negotiation—スイッチのオートネゴシエーションがオフに設定されていて、サーバがその速度とデュプレックス設定に設定されていない場合、スイッチはそのサーバとネゴシエーションしません。

PXE もサーバー上で正しく実行されていることを確認してください。他の起動可能デバイスがシステムに存在する前に、システムを PXE から起動するように設定する必要があります。

システムは PXE を起動するが、PXE サーバーの応答を待ってタイムアウトする

WinPE ブートイメージが適切な配布ポイントにプッシュされていることを確認してください。さらに、使用される配布ポイントでは PXE が有効になっている必要があります。

以下の手順で確認します。

1. [管理]→[サイトの構成]→[サーバーおよびサイトシステムの役割]の順に選択します。
2. 適切な配布ポイントを選択します。
3. 配布ポイントの役割を右クリックし、[プロパティ]→[PXE]の順に選択します。

WinPE がタスクシーケンスを開始しない

次の場所にある SMSTS.LOG ファイルを確認します。 X:\windows\temp\smstslog\smsts.log. パッケージがダウンロードされない、またはアクセスできない場合は、適切なネットワークドライバがインストールされていない可能性があります。ターゲットプラットフォーム用の新しい WinPE ドライバで WinPE イメージを更新する必要がある可能性があります。タスクシーケンスで参照されているすべてのパッケージが配布ポイントから入手できることを確認します。WinPE はすべてのパッケージを検証して、タスクシーケンスを処理する前にそれらが利用可能であることを確認します。

コンテンツシーケンスのステータスが“配布済み”であっても、タスクシーケンスが“タスクシーケンスの依存関係の解決に失敗しました”と報告します。

Configuration Manager には、パッケージのハッシュが生成されないことがあるという問題があります。これにより、ハッシュがこれらの目的で使用されているため、デバイスがコンテンツを見つけることができないという結果になります。able to locate the content since the hashes are used for those purposes.

この問題を解決するには次のようにします。

1. [ドライバーパック]を選択します。
2. 右クリックして、[配布ポイントの更新]を選択します。
3. 表示されるダイアログボックスで[はい]を選択します。

このプロセスが完了すると、タスクシーケンスによってドライバーパックを見つけて解決できます。

ターゲットシステムが、更新された BCU ファイルの実行または使用に失敗する

構成ファイルを変更、追加、または削除するときには、BCU パッケージを含む配布ポイントを更新する必要があります。

有効なドライブが存在する場合、デフォルトの起動順序では PXE は起動されません

アクティブパーティションがハードドライブ上に作成されると、有効なオペレーティングシステムがインストールされていれば自動的に起動可能なデバイスになります。PXE NIC が起動順序のハードドライブより後にある場合、ハードドライブは PXE よりも前に Windows で起動するか、Windows がインストールされていない場合は「無効なシステムパーティション」エラーを引き起こします。

この問題を解決するには次のようにします。

1. 起動順序で PXE がハードドライブの前に配置されていることを確認します。
2. 必要に応じて、タスクステップで HP Client BIOS 設定ユーティリティを使用して起動順序を設定します。

   – または –

   ターゲットプラットフォームの BIOS で起動順序を設定します。これを行う方法についての具体的な指示については、プラットフォームの資料を参照してください。

BCU を使用して起動順序を設定する方法の詳細については、Set BIOS Configuration タスクステップの設定 を参照してください。

PXE が起動順序の先頭にある場合、Configuration Manager を実行するために必須のタスクシーケンスがない限り、コンピューターは実際には PXE から起動しません。

タスクシーケンスが“ポリシーのダウンロードに失敗しました”のエラーで失敗する

このエラーコード（0x80093102 または 0x80004005）は、証明書検証の問題を示しています。 SMSTS.LOG ファイルには、次のテキストのいずれかのエントリが表示されます。

```
CryptDecryptMessage ( &DecryptParams, pbEncrypted, nEncryptedSize,0,
&nPlainSize,0 ), HRESULT=80093102 no
cert available for policy decoding
```

考えられる原因は次のとおりです。

- DNS がサイトサーバーを指していない、またはサイトサーバーが有効な FQDN を指定していない（DNS リストで参照されている）など、ドメインまたはサイトサーバーの設定が誤っていると、このエラーが発生することがあります。サイトサーバーが FQDN を指定せず、NETBIOS 名のみを指定していて、DNS サーバーが FQDN を参照しようとしている場合、誤った参照によってこのエラーが発生する可能性があります。
- PXE とブートメディアに使用されている証明書がブロックされているか、存在しません。サイトの設定ノードの下にある証明書のいずれかがブロックされているか存在しないかを確認します。証明書を開き、それらが実際に証明書ストアにインストールされていることを確認します。インストールされていない場合は、それらをインストールします。

それでもタスクシーケンスが失敗する場合は、配布ポイントまたはグループ、あるいはその両方からパッケージを削除して、再度追加します。これにより、パッケージハッシュが再生成されます。

PXE 提供情報を消去してもタスクシーケンスが再実行されない

以前にタスクシーケンスを実行したかどうかにかかわらず、提供情報がコンピューターに適用されるように、展開が再実行を許可するように設定されていることを確認する必要があります。

この問題を解決するには次のようにします。

1. 展開のページのプロパティで、[スケジューリング]を選択します。
2. [再実行の動作]を選択します。

タスクシーケンスが Apply Operating System ステップで“ボリューム X:\bootable の作成に失敗しました”のエラーメッセージが表示されて失敗する

この問題は、次のメッセージのようなログの内容で示されます。

```
MakeVolumeBootable( pszVolume ), HRESULT=80004005
(e:\nts_sms_fre\sms\client\osdeployment\applyos\installcommon.cpp,759)
Failed to make volume E:\ bootable. Please ensure that you have set an
active partition on the boot disk before installing the operating system.
Unspecified error (Error: 80004005; Source: Windows)
ConfigureBootVolume(targetVolume), HRESULT=80004005
(e:\nts_sms_fre\sms\client\osdeployment\applyos\applyos.cpp,326)
Process completed with exit code 2147500037
```

タスクシーケンスで Format & Partition アクションを使用して MBR システム用にハードドライブをパーティション分割する場合にこの問題を解決するには、次の手順を実行します。

- [これをブートパーティションにする]オプションを選択します。このオプションを選択せず、コンピュータにハードドライブが 1 つしか存在しない場合、タスクシーケンスエンジンは自動的にいずれかのパーティションをブートパーティションにします。複数のドライブがある場合は、どのブートパーティションを起動可能にする必要があるかを自動的に判断することはできません。

システム環境変数は、タスクシーケンスの次のアクションに引き継がれません

タスクシーケンスが実行されると、コマンドはコマンドシェルで実行されます。そのタスクが終了すると、そのコマンドシェル環境も終了し、そのタスク内で定義されているシステム変数がすべて失われます。タスク間を通過する変数がタスクシーケンス変数、コレクション変数、またはマシン変数として設定されていることを確認します。

タスクシーケンスの実行中にエラーが報告される

タスクシーケンスが完全に実行されないのにはさまざまな理由がありますが、タスクシーケンスの実行の問題を解決するために解決する必要がある可能性のある一般的な理由がいくつかあります。

- DNS サーバーと WINS サーバーが正しく機能し、安定していることを確認してください。
- タスクシーケンス手順で指定された資格情報が、タスクシーケンス変数と PXE フラグを消去および設定するために SCCM サーバーへの必要なアクセス権を持っていることを確認してください。
- WinPE で BCU を介して BIOS 設定を適用しようとしている場合は、パッケージをシステムにダウンロードできるようにディスクをパーティションに分割してフォーマットしておく必要があります。

次のドライバーパックまたはタスクシーケンスエラーの診断 の手順 5 に示すように、ログファイルを調べることも失敗の理由の調査に役立ちます。

24.8 ドライバーパックまたはタスクシーケンスエラーの診断

1. タスクシーケンスを右クリックして[エクスポート]を選択して、タスクシーケンスをエクスポートします。

2. 問題が発生した場合は、関連部分の画面キャプチャーを収集してください。

3. 問題が製品のインストールに関連しているか、インストール後すぐに発生する場合は次のようにします。

   a. 一時ファイルディレクトリにある MSI インストールログをコピーします（%TEMP%環境変数を使用して見つけます）。このファイルは通常“1”ディレクトリにあり、ランダムな名前で次のようにフォーマットされています。

      MSI<RandomCharacters>.LOG.

   b. 一時ファイルディレクトリにあるサポートパッケージのインストールログをコピーします（環境変数%TEMP%を使用して見つけます）。ファイル名は HPClientSCCM2012Kit-setup.log です。

4. コンソールの使用中に問題が発生した場合は、%TEMP%\ hpclient にある HP MIK ログファイルをコピーしてください。さらに、Configuration Manager コンソールの AdminUILog フォルダーにある Configuration Manager コンソールのログファイルもコピーする必要があります。

5. タスクシーケンスの実行中に問題が発生した場合は、次のファイルを WinPE 環境からコピーする必要があります。これらのファイルは、タスクシーケンスの実行中に[F8]キーを押してコマンドプロンプトを開くことでアクセスできます。WinPE でコマンドプロンプトを使用するには、ブートイメージに対して[コマンドサポートを有効にする]オプションを選択します。このオプションは、ブートイメージを右クリックして[プロパティ]を選択し、次に[Windows PE]を選択すると表示されます。

   a. WinPE が保管されている場所から SMSTS.LOG ファイルをコピーします。

      - PXE ブートの場合、X:\Windows\Temp\Smstslog
      - ローカルドライブ（C:や D:）の \Smstslog
      - SMSTSLOG<Time-Based-Name>.LOG

   b. 構成 INI ファイルや XML ファイルなど、入力として使用されているファイルを構成タスクにコピーします。

   c. PXE ブートの場合、X:\Windows\inf に格納されている WinPE から SetupAPI.APP.LOG と SetupAPI.DEV.LOG をコピーします。

6. エラーがベースラインとポリシーに関連している場合は、以下のログファイルを採取します。

   a. 次のフォルダ内の HP MIK コンソールログファイル。 %PROGRAMDATA%\HP\HP MIK\Logs

   b. 次のフォルダ内のすべての HP MIK Client のログファイル。%PROGRAMDATA%\HP\HP MIK\Logs および

      %\SYSTEMROOT%\System32\config\systemprofile\AppData\Roaming\hpqLog\com.hp.si am.log

7. これらのログファイルを調べても問題が解決せず、HP に連絡する必要がある場合は、次のような問題の詳細な説明を用意してください。

a. 正確な失敗のポイント（例えば、プロセスが失敗したときに実行されているアクション、エラーメッセージとエラーコードの説明または画面キャプチャー）

b. 構成されているコンピューターの詳細な説明（モデル、ハードウェア構成、および NIC の詳細）- 以下のような他の状況の説明。

   i. このタスクシーケンスまたはアクションはこれまでに機能していたか？いつから機能しなくなったか？

   ii. 以前に機能していた場合、今回は何が違うのか？

   iii. タスクシーケンスはさまざまな機種のコンピュータに適用していますか？別々の構成ファイルまたはタスクシーケンス変数を使用していますか？

25 付録 C – MIK 用の Sure Run および Sure Recover 鍵の生成

HP Sure Run および HP Sure Recover で使用される鍵承認証明書には、他のすべての操作を承認するために使用される最上位レベルのキーが含まれています。そのため、その目的は、対応する秘密鍵を強く管理することです。さらに、将来的にはファームウェアが証明書が EV 証明書であるという要件を強制することが期待されています。 その間、ファームウェアは、HP Sure Run と HP Sure Recover をテストするための自己署名証明書の使用をサポートします。

以下は、オープンソースの openssl コマンドを使用してキーエンドースメント証明書と署名キー証明書を生成するためのサンプルステップです。これらの手順の最後の、key_endorsement_cert.pfx ファイルに鍵承認証明書があり、signing_key_cert.pfx ファイルに署名鍵証明書があります。

> 警告: これらの手順は、プラットフォーム上で Sure Run / Sure Recover を安全に構成するために使用される秘密鍵を作成しています。ここで生成されるファイルと一時ファイルが作成するファイルを保護するために適切な注意を払う必要があります。

鍵承認証明書の作成

1. 前の操作からの一時ファイルが存在しないように削除します。（ファイルが無ければ削除不要です）

```
del key.pem
del cert.pem
```

2. 鍵承認証明書に使用する証明書を生成します。（以下のコマンドは単一行として入力してください）

```
openssl req -x509 -nodes -newkey rsa:2048   -
keyout key.pem -out cert.pem -days 3650
  -subj
"/C=US/ST=State/L=City/O=Company/OU=Org/CN=www.example.com"
```

> 注記: 最初のコマンドの-subj コマンドラインパラメータは、組織に固有の情報を反映するように変更する必要があります。このパラメータを含めないと、openssl は情報の入力を促します。この情報は、将来のバージョンのファームウェアでユーザーおよび管理者に報告される可能性があるため、正しく入力してください。

3. 自己署名付き公開証明書を PKCS#12 形式に変換します。（以下のコマンドは 1 行に入力してください）

```
openssl pkcs12  -inkey key.pem -in cert.pem -export
  -keypbe PBE-SHA1-3DES -certpbe PBE-SHA1-3DES
  -out key_endorsement_cert.pfx
  -name "Sure Run / Sure Recover Key Endorsement Certificate"
```

このステップでは、「パスワードのエクスポート」の入力を求められますが、そのまま Enter キーを押すだけです。（つまり、パスワードは入力しません）

注記: ファイル key.pem と cert.pem は安全に破棄されるべき一時ファイルです。

NOTE: ここで使用されている秘密鍵は、すべてのファイルで保護されていません。

鍵署名証明書の作成

1. 前の操作からの一時ファイルが存在しないように削除します。（ファイルが無ければ削除不要です ）

```
del key.pem
del cert.pem
```

2. 署名鍵に使用する RSA 秘密鍵を生成します。

```
openssl.exe genrsa -out signing_key.pem 2048
```

3. 鍵署名証明書に使用する証明書を生成します。（以下のコマンドは単一行として入力してください）

```
openssl req -x509 -nodes -new -key signing_key.pem
  -keyout key.pem -out cert.pem -days 3650
  -subj
"/C=US/ST=State/L=City/O=Company/OU=Org/CN=www.example.com"
```

注記: 最初のコマンドの-subj コマンドラインパラメータは、組織に固有の情報を反映するように変更する必要があります。このパラメータを含めないと、openssl は情報の入力を促します。

4. 自己署名付き公開証明書を PKCS#12 形式に変換します。（以下のコマンドは 1 行に入力してください）

```
openssl pkcs12 -inkey key.pem -in cert.pem -export
  -keypbe PBE-SHA1-3DES -certpbe PBE-SHA1-3DES
```

```
-out signing_key_cert.pfx
-name "Sure Run / Sure Recover Signing Key Certificate"
```

このステップでは、「パスワードのエクスポート」の入力を求められますが、そのまま Enter キーを押します。（つまり、パスワードは入力しません）

注記: ファイル key.pem と cert.pem は安全に破棄されるべき一時ファイルです。

注記: ここで使用されている秘密鍵は、すべてのファイルで保護されていません。

補足情報:

- ユーザーが[証明書の送信]ボタンを押すと、ファイルが読み込まれ、サイトコントロール内の埋め込みプロパティとして保存されます。この時点でファイルは不要になります。
- MIK が提供された証明書またはキーに問題がある場合は、「署名キー証明書の保存に失敗しました」または「キー承認証明書の保存に失敗しました」などの一般的なメッセージが表示されます。
- 鍵は 2048 ビット長で、0x10001 の指数を使用する必要があります。

26 関連情報

クライアントの管理性に関するすべてのニーズについては、HP Client Management Solutions Web サイトにアクセスしてください。 http://www.hp.com/go/clientmanagement すべての HP クライアントツールおよびドライバパックについては、HP Client Management Solutions ホームページの[HP Download Library]を選択してください。