

HP Manageability Integration Kit ホワイトペーパー

株式会社 日本HP

サービス・ソリューション事業本部 技術本部

2017年4月



目次

	ページ	
概要	4	
システム要件	5	
HP Manageability Integration Kitの入手方法	6	
Configuration ManagerへのHP MIKのインストール	7	
HP Client Support Packagesの配布	8	
HP MIK プラグイン	HP MIK プラグイン	10
	コンプライアンス設定	11
	HP BIOS Configuration	12
	HP BIOS Password	19
	HP Client Security	20
	Device Guard (Windows 10のみ)	31
	HP Sure Start	34
	TPM Firmware Update	40
	HP WorkWise (Windows 10のみ)	43

目次

		ページ
ソフトウェアライブラリ	ソフトウェアライブラリ	48
	HP Client Driver Pack	49
	HP Client Boot Image	64
	HP Client Task Sequence	68
本書の取り扱いについて		91

概要

HPのコンピュータは以下の2つの主旨に基づき、容易に管理できるように設計されています。

- IT管理者がコンピュータに付属のHP BIOS、ハードウェア、およびプリインストールされたソフトウェアを管理するのに役立つ手段を提供します。
- 管理者が選択したクライアント管理コンソールで動作するソリューションを提供します。

これらの2つの原則に対処するために作成されたソリューションがHP Manageability Integration Kit (MIK) 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まで拡張する、クライアント管理コンソールに依存しないソリューションです。

HP MIKの目的は、既存のツールとワークフローに統合することで、日常の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を導入して、次のような主なメリットを享受してください。

- 管理の基本をスピードアップ - イメージ、BIOS、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、ビジネスに集中できます。
- データ保護 - BIOS設定を保護し、認証と資格情報の要件を設定し、Device Guardを有効にし、TPM (Trusted Platform Module) ファームウェアの更新を管理します。
- ソフトウェアの管理 - IT管理者は、HP Client Security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で動作するように最適化されていますが、スクリプトを使用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の管理機能のWebサイト

(<http://www.hp.com/go/clientmanagement>) を参照してください。

システム要件

HP Manageability Integration KitサポートされているバージョンのMicrosoft System Center Configuration Manager (SCCM) 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

サポートされているMicrosoft System Center Configuration Managerのバージョン

- Microsoft System Center 2012 R2 Configuration Manager service pack 1 (SP1) with or without cumulative update 1 (CU1) or later
- Microsoft System Center 2012 R2 Configuration Manager
- Microsoft System Center 2012 Configuration Manager SP2 with or without CU1 or later and
- Microsoft System Center 2012 Configuration Manager SP1 and
- Microsoft System Center Configuration Manager 1511, 1602, or 1606

サポートされているクライアントOS

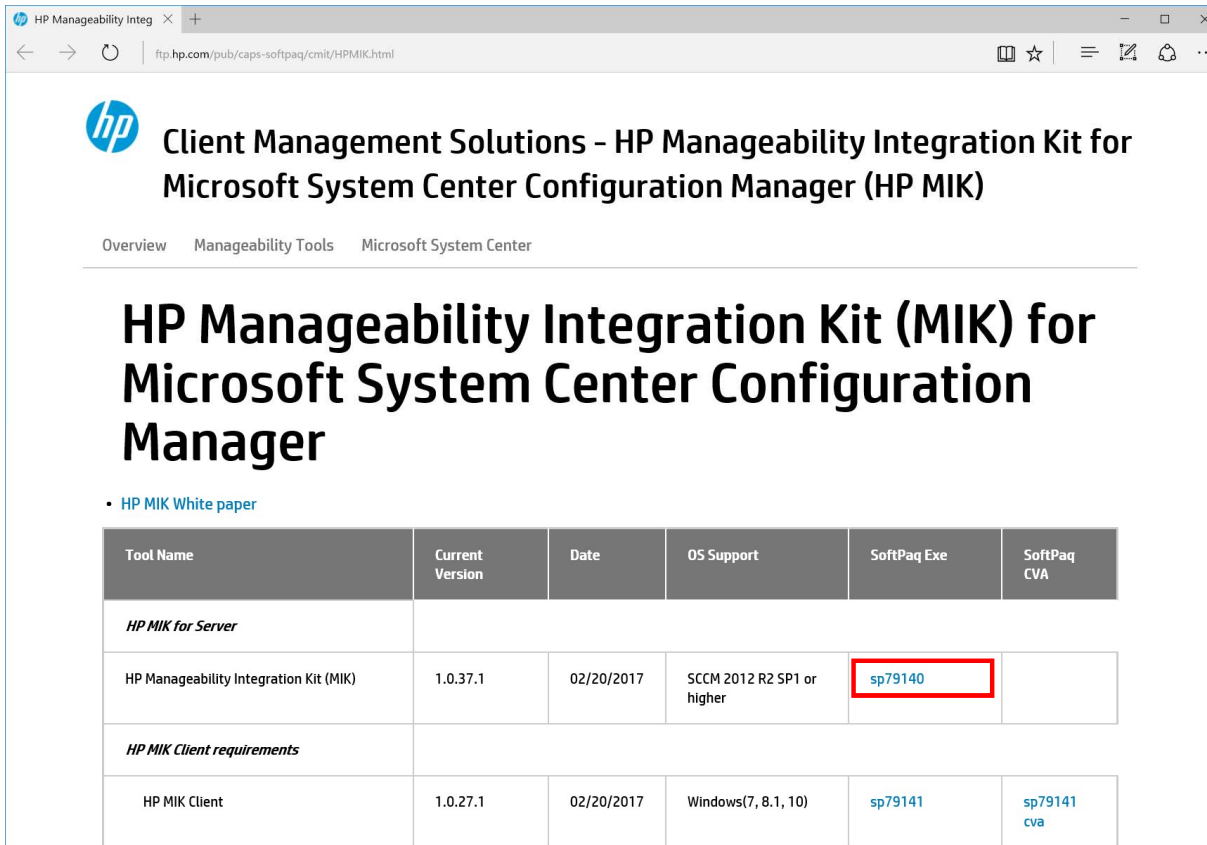
※いくつかのHP Manageability Integration Kitの機能には追加の要件があります

- Windows 10
- Windows 8.1
- Windows 7

HP Manageability Integration Kitの入手方法

HP Manageability Integration Kitは以下のURLより無償でダウンロード可能です。

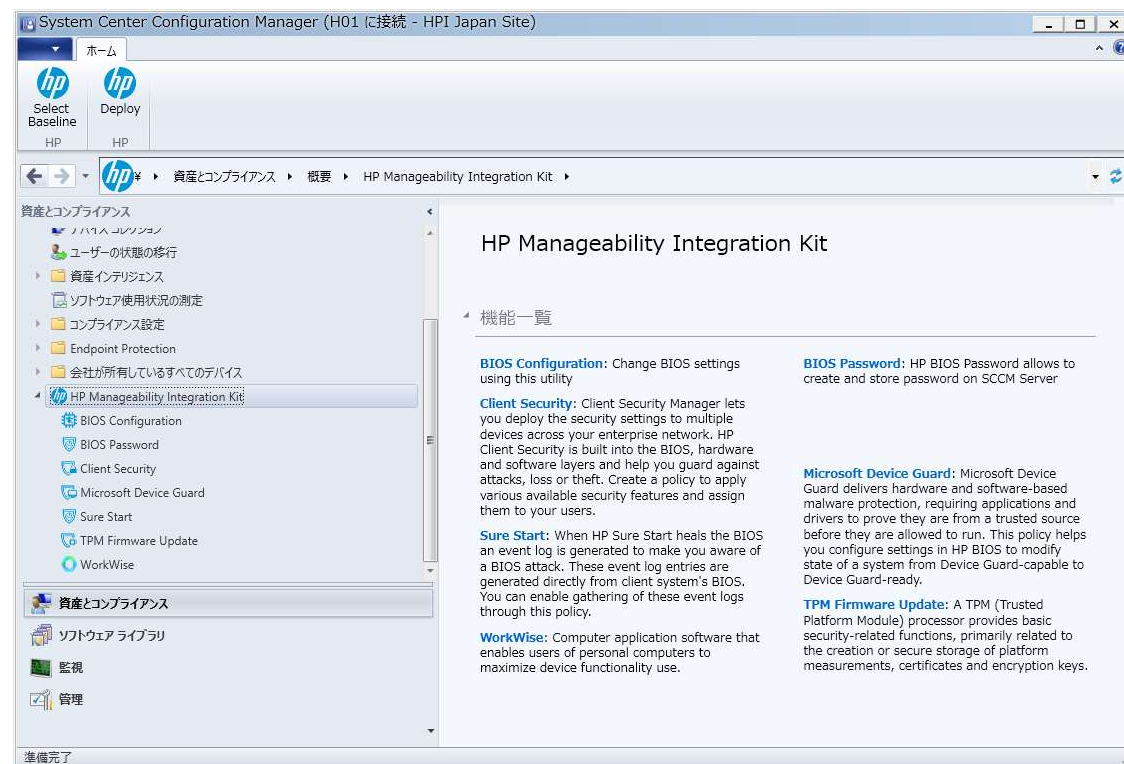
<http://ftp.hp.com/pub/caps-softpaq/cmit/HPMIK.html>



Tool Name	Current Version	Date	OS Support	SoftPaq Exe	SoftPaq CVA
<i>HP MIK for Server</i>					
HP Manageability Integration Kit (MIK)	1.0.37.1	02/20/2017	SCCM 2012 R2 SP1 or higher	sp79140	
<i>HP MIK Client requirements</i>					
HP MIK Client	1.0.27.1	02/20/2017	Windows(7, 8.1, 10)	sp79141	sp79141 cva

Configuration ManagerへのHP MIKのインストール

1. Configuration Managerコンソールのインスタンスがすべて閉じていることを確認します。
2. HP Client Integration Kit (CIK) がシステムにインストールされている場合は、アンインストールします。
3. Microsoft System Center Configuration Manager SoftPaq用にダウンロードしたHP管理容易性統合キット (MIK) 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、[Assets and Compliance]にHP Manageability Integration Kitが表示されていることを確認します。



HP Client Support Packagesの配布

インストールが完了した後、HP Client Support Packages内のコンテンツを配布ポイントに配布します。

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を選択します。

注記

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

パッケージが削除されている場合は、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ます。次に、パッケージを使用してタスクシーケンスをリフレッシュします。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。

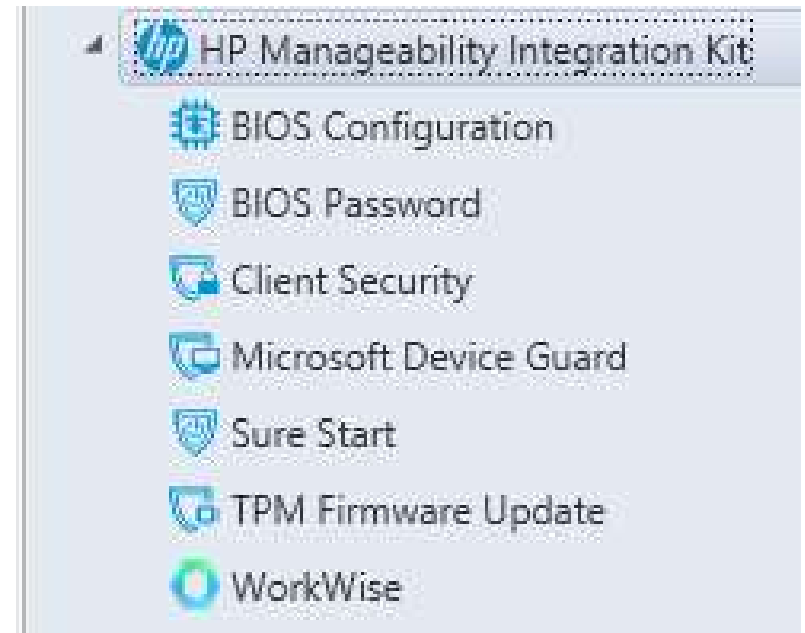
2. 初めてのインストールの場合は、[HP Client BIOS Configuration Utility]を右クリックし、[コンテンツの配布]を選択し、画面の指示に従ってウィザードを完了します。アップグレードの場合は、HP Client BIOS Configuration Utilityを右クリックし、配布ポイントの更新を選択し、画面の指示に従ってウィザードを完了します。
3. [HP Client Support Tools]に対しても2と同様の内容を実行します。

HP MIKプラグイン

HP MIKプラグイン

HP Manageability Integration Kitをインストールすると管理とコンプライアンスにHP Manageability Integration Kitが追加されます。HP Manageability Integration Kitノードの下には7つのプラグインがあります。

- HP BIOS Configuration : BIOS設定のポリシーを作成します
- HP BIOS Password : BIOSパスワードを作成しSCCMに保存します
- Client Security : HP Client Security設定のポリシーを作成します
- Microsoft Device Guard : システムのBIOS設定をDevice Guard-CapableからDevice Guard-Readyに変更します
- Sure Start : Sure Start関連のBIOS設定の変更とSure Startのイベントログ収集の有効・無効を設定します
- TPM Firmware Update : TPMファームウェアのアップデートを行います
- WorkWise : WorkWiseアプリケーションソフトウェアの有効・無効を設定します



コンプライアンス設定

HP MIKプラグインを使用して作成したポリシーはConfiguration Managerのコンプライアンス設定として保存されます。場所は、資産とコンプライアンス→コンプライアンス設定→構成項目になります。

構成項目はHP MIKのプラグインごとに作成され、デフォルトでは名前にプラグイン名が含まれます。

1つの構成基準には1つまたは複数の構成項目が含まれています。構成基準はコレクションごとに展開することができます。

アイコン	名前	種類	デバイスの種類	リビジョン	子	関係	ユーザー設定
	MIK Test - Device Guard	ソフトウェア	Windows	1	いいえ	はい	いいえ
	MIK Test - Trusted Platform Module	ソフトウェア	Windows	1	いいえ	はい	いいえ

HP BIOS Configuration

BIOS Configuration プラグインを使用してBIOS設定のポリシーを作成してクライアントコンピュータに展開する事ができます。

サポート対象のクライアントコンピュータ

- 2015年モデル以降のHPコマーシャルコンピュータ

サポート対象のOS

- Windows 10
- Windows 8.1
- Windows 7

前提条件

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

HP BIOS Configuration

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。

Select列ではポリシーで強制するBIOS設定を選択します。

Settings列にはBIOS設定の名前が表示されます。

Values列には値を入力するかドロップダウンメニューから値を選択します。BIOS設定によっては入力した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変わります。

注記

Category Viewの場合、3つの列全てを表示するにはカテゴリを展開する必要があります。

いくつかの設定の隣にあるアイコンはそれぞれ以下を示します。



—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。



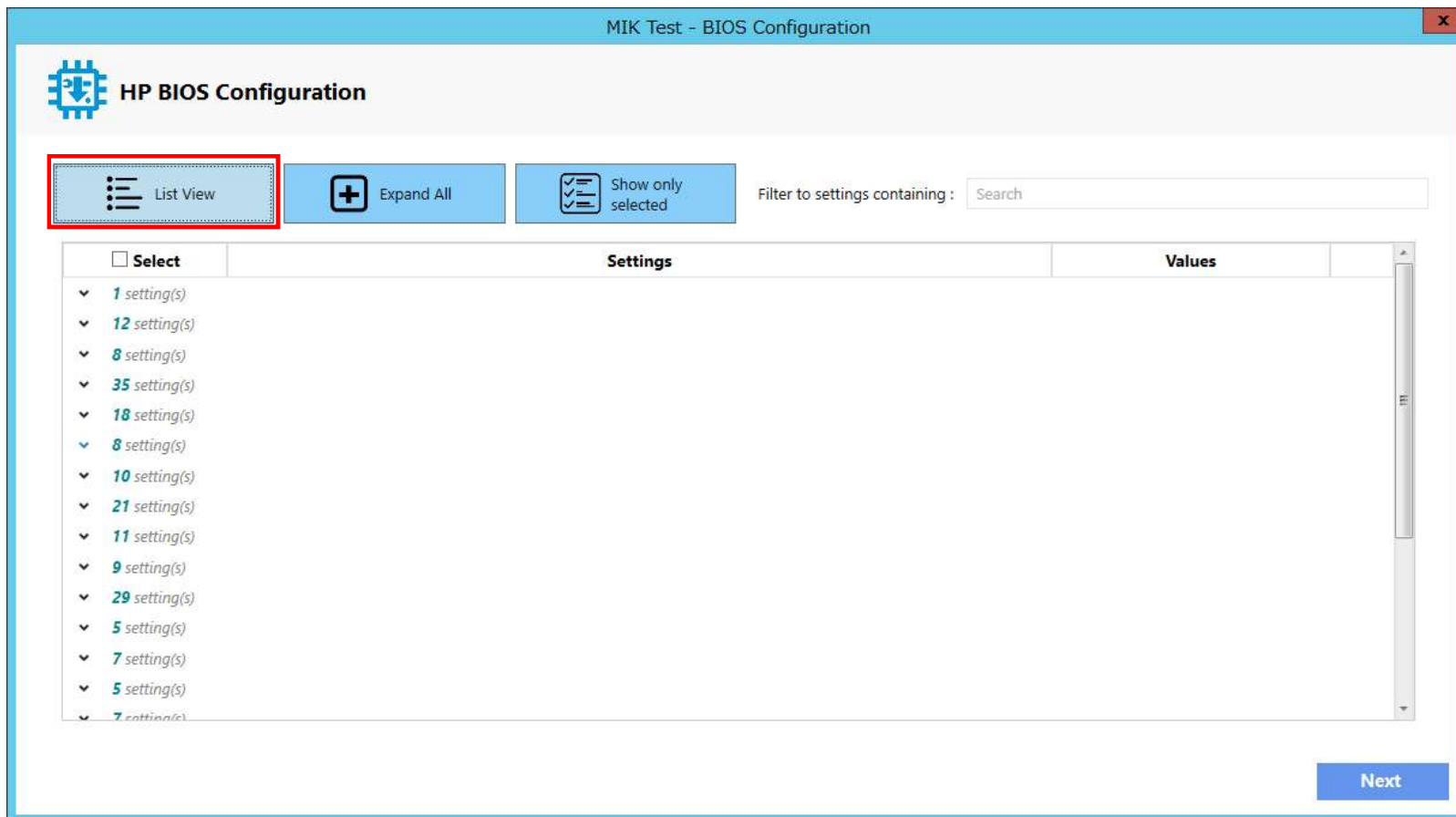
—設定は次の再起動時にユーザーの確認が要求されます。

確認のためのキー入力の実施されるまでは再起動が完了しません。

HP BIOS Configuration

List View/Category Viewボタン

BIOS設定の表示を一覧表示（List View）またはカテゴリ表示（Category View）に切り替えます。

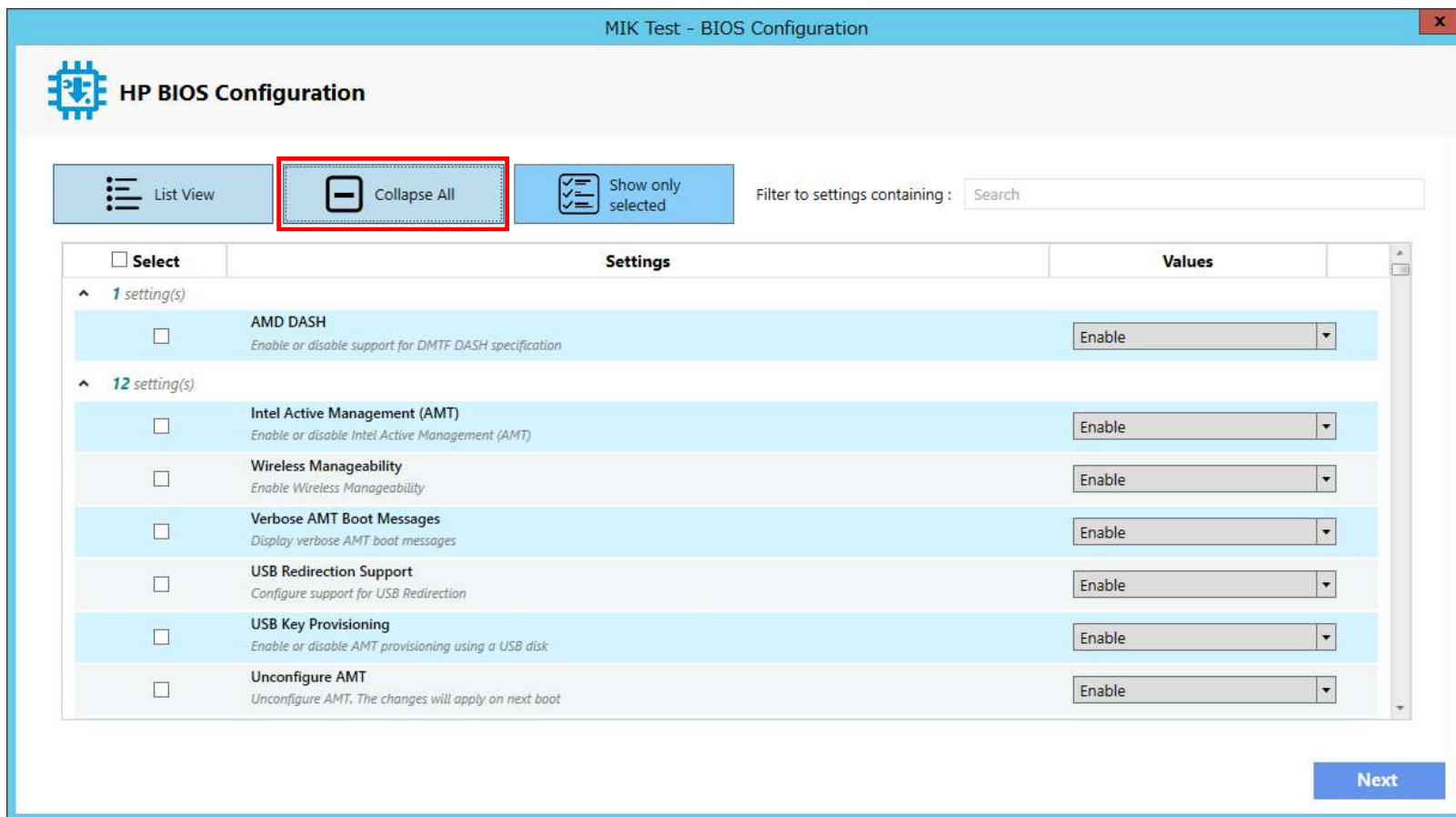


The screenshot shows the HP BIOS Configuration window titled "MIK Test - BIOS Configuration". The interface includes a header with the HP logo and "HP BIOS Configuration". Below the header, there are three buttons: "List View" (highlighted with a red box), "Expand All", and "Show only selected". To the right of these buttons is a search filter labeled "Filter to settings containing:" with a text input field. The main area is a table with columns for "Select", "Settings", and "Values". The "Select" column contains a list of expandable items, each with a dropdown arrow and a count of settings (e.g., "1 setting(s)", "12 setting(s)", "8 setting(s)", "35 setting(s)", "18 setting(s)", "8 setting(s)", "10 setting(s)", "21 setting(s)", "11 setting(s)", "9 setting(s)", "29 setting(s)", "5 setting(s)", "7 setting(s)", "5 setting(s)", "7 setting(s)"). A "Next" button is located at the bottom right of the window.

HP BIOS Configuration

Expand All/Collapse Allボタン

カテゴリ表示の際に全ての設定を表示または非表示にします。



The screenshot shows the HP BIOS Configuration interface. At the top, the title bar reads "MIK Test - BIOS Configuration". Below the title bar, the HP logo and "HP BIOS Configuration" are displayed. A navigation bar contains three buttons: "List View", "Collapse All" (highlighted with a red box), and "Show only selected". To the right of these buttons is a search filter: "Filter to settings containing: Search". Below the navigation bar is a table with columns for "Select", "Settings", and "Values". The table lists several settings, including "AMD DASH" and "Intel Active Management (AMT)", each with a checkbox and a dropdown menu set to "Enable". A "Next" button is located at the bottom right of the window.

Select	Settings	Values
<input type="checkbox"/>	AMD DASH <i>Enable or disable support for DMTF DASH specification</i>	Enable
<input type="checkbox"/>	Intel Active Management (AMT) <i>Enable or disable Intel Active Management (AMT)</i>	Enable
<input type="checkbox"/>	Wireless Manageability <i>Enable Wireless Manageability</i>	Enable
<input type="checkbox"/>	Verbose AMT Boot Messages <i>Display verbose AMT boot messages</i>	Enable
<input type="checkbox"/>	USB Redirection Support <i>Configure support for USB Redirection</i>	Enable
<input type="checkbox"/>	USB Key Provisioning <i>Enable or disable AMT provisioning using a USB disk</i>	Enable
<input type="checkbox"/>	Unconfigure AMT <i>Unconfigure AMT. The changes will apply on next boot</i>	Enable

HP BIOS Configuration

Show only selected/Show Allボタン

選択した設定のみを表示するかまたは全ての設定を表示するか切り替えます。

The screenshot shows the HP BIOS Configuration interface. At the top, there is a title bar 'MIK Test - BIOS Configuration'. Below it, the HP logo and 'HP BIOS Configuration' are displayed. A navigation bar contains three buttons: 'List View', 'Collapse All', and 'Show only selected'. The 'Show only selected' button is highlighted with a red box. To the right of these buttons is a search filter: 'Filter to settings containing: Search'. Below the navigation bar is a table of settings. The table has three columns: 'Select', 'Settings', and 'Values'. The 'Select' column contains checkboxes. The 'Settings' column contains the setting name and a description. The 'Values' column contains dropdown menus. The settings listed are: 'Allow spaces in passwords' (No), 'Require a lowercase character in BIOS passwords' (No), 'Serial Port A' (Enable), 'Serial Port B' (Enable), 'I/O Address A' (Default Address), 'I/O Address B' (Default Address), 'I/O Address C' (Default Address), and 'I/O Address D' (Default Address). A 'Next' button is located at the bottom right of the window.

Select	Settings	Values
<input type="checkbox"/>	Allow spaces in passwords <i>If enabled, the Administrator and User passwords may contain spaces</i>	No
<input type="checkbox"/>	Require a lowercase character in BIOS passwords <i>If enabled, the Administrator and User passwords must contain at least one lowercase letter</i>	No
^ 10 setting(s)		
<input type="checkbox"/>	Serial Port A <i>Enable or disable serial port A, where available</i>	Enable
<input type="checkbox"/>	Serial Port B <i>Enable or disable serial port B, where available</i>	Enable
<input type="checkbox"/>	I/O Address A <i>Port I/O Address A</i>	Default Address
<input type="checkbox"/>	I/O Address B <i>Port I/O Address B</i>	Default Address
<input type="checkbox"/>	I/O Address C <i>Port I/O Address C</i>	Default Address
<input type="checkbox"/>	I/O Address D <i>Port I/O Address D</i>	Default Address

HP BIOS Configuration

ポリシーの作成

1. Configuration Managerで、[資産とコンプライアンス]を選択し、[概要]を選択します。
2. HP Manageability Integration Kitを展開し、[BIOS Configuration]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、ポリシー作成ウィザードを開始します。
4. 設定を選択し、新しい値を選択して設定を変更します。
5. BIOS設定を選択して変更したら、[次へ]を選択します。
6. Summaryページで設定内容を確認して[Save Policy]をクリックします。
7. ポリシーの保存が完了したら、[Deploy]をクリックします。
8. ポリシーを適用するターゲットのコレクションを選択し、[Deploy]をクリックします。
9. クライアントコンピュータにポリシーが適用された後、クライアントコンピュータを再起動して設定が変更されている事を確認します。

HP BIOS Configuration

ポリシーの編集

1. Configuration Managerで、[資産とコンプライアンス]を選択し、[概要]を選択します。
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. ベースライン名を選択し、[OK]をクリックしてます。
4. ポリシー作成ウィザードのSummary画面が表示されますので[Previous]をクリックします。
5. ポリシーの作成の4~9と同じ手順を実行します。

注記

クライアントコンピュータにBIOSパスワードが設定されている場合は、次のHP BIOS Passwordの手順を先に実行しておく必要があります。

クライアントコンピュータでHP MIK BIOS Configurationのログは%PROGRAMDATA%\HP\HP MIK\Logsに保存されます。

HP BIOS Password

クライアントコンピュータにBIOSパスワードが設定されている場合はこの機能を使用してHP Manageability Integration KitがHP BIOS Configuration等の機能でBIOS設定を変更する際に使用するためのBIOSパスワードを登録します。

この機能からはクライアントコンピュータのBIOSパスワードを変更する事は出来ません。BIOSパスワードの設定・変更はHP BIOS Configurationプラグインから行います。



The image shows a screenshot of a Windows-style dialog box titled "MIK BIOS Password Management". The dialog box has a blue header bar with the HP logo and the text "BIOS Password". Below the header, there are two text input fields: "Password" and "Confirm Password". At the bottom of the dialog box, there are two buttons: "Cancel" and "Apply".

HP Client Security

HP Client Security プラグインを使用して Configuration Manager から HP Client Security を管理できます。また Intel® Authenticate™ の設定を行うことができます。

サポート対象のクライアントコンピュータ

- 2015年モデル以降のHPコマーシャルコンピュータ

サポート対象のOS

- Windows 10
- Windows 8.1
- Windows 7

前提条件

- Microsoft .NET Framework 4.6.1 以上
- HP Client Security Manager 9.3.0.2368 以上
- HP Device Access Manager 8.4.6.0 以上
- Intel Authenticate Engine (オプション)

注記

Intel Authenticate Engine には次のドライバー要件があります。

- Intel Management Engine Driver 11.6.0.1019 以上
- Intel Bluetooth® Driver 19.00.00.1626.3453 以上
- Intel Graphics Driver 21.20.16.4481 以上
- Synaptics Touch Fingerprint Driver 5.2.5002.26 以上

Intel Authenticate Engine では Intel Authenticate support へのアクセスが要求されます。

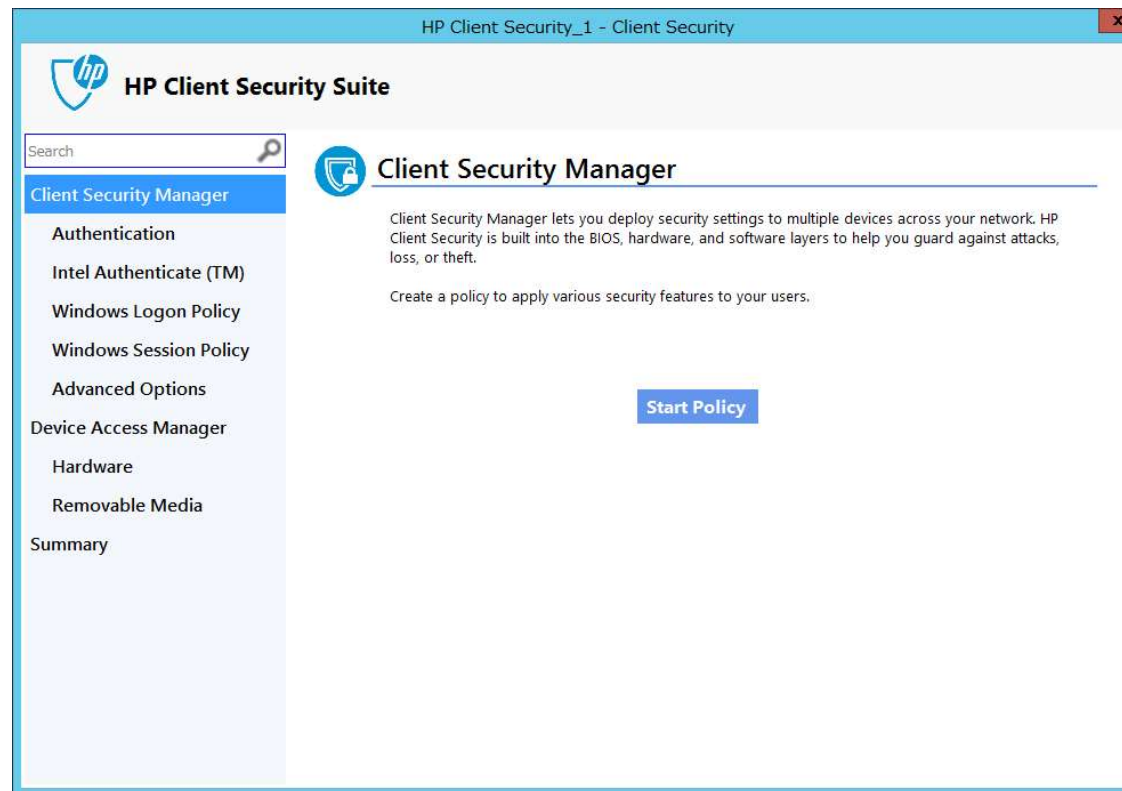


HP Client Security

ユーザーインターフェース

HP Client SecurityはClient Security ManagerとDevice Access Managerの2つに分かれています。

HP Client Securityプラグインを開くとClient Security Managerの概要紹介画面が表示されます。[Start Policy]をクリックします。



HP Client Security

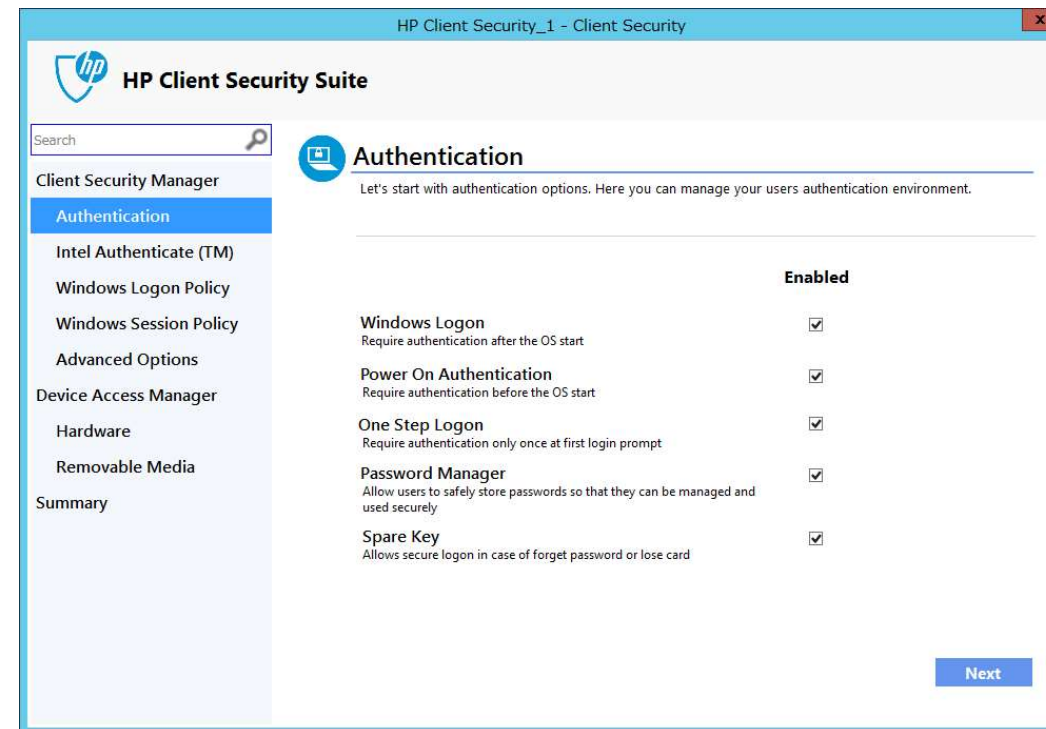
Client Security Manager

Authenticationタブ

このタブではHP Client Security Managerのセキュリティ機能を設定します。

以下の設定の有効化・無効化が可能です。

- Windows Logon—強力な認証を使用してWindowsアカウントを保護します。
- Power On Authentication—電源投入時認証を有効にしてWindows起動前のシステムを保護します。
- One Step Logon—電源投入時認証が有効な場合に電源投入時に入力した資格情報をWindowsログオンに使用できます。
- Password Manager—Windowsログオン後にWebサイトやアプリケーションに入力したパスワードをHP Password Managerに安全に保存し、そのパスワードを入力する代わりにHP Client Securityの認証で自動的に使用できます。



HP Client Security

Intel Authenticate タブ

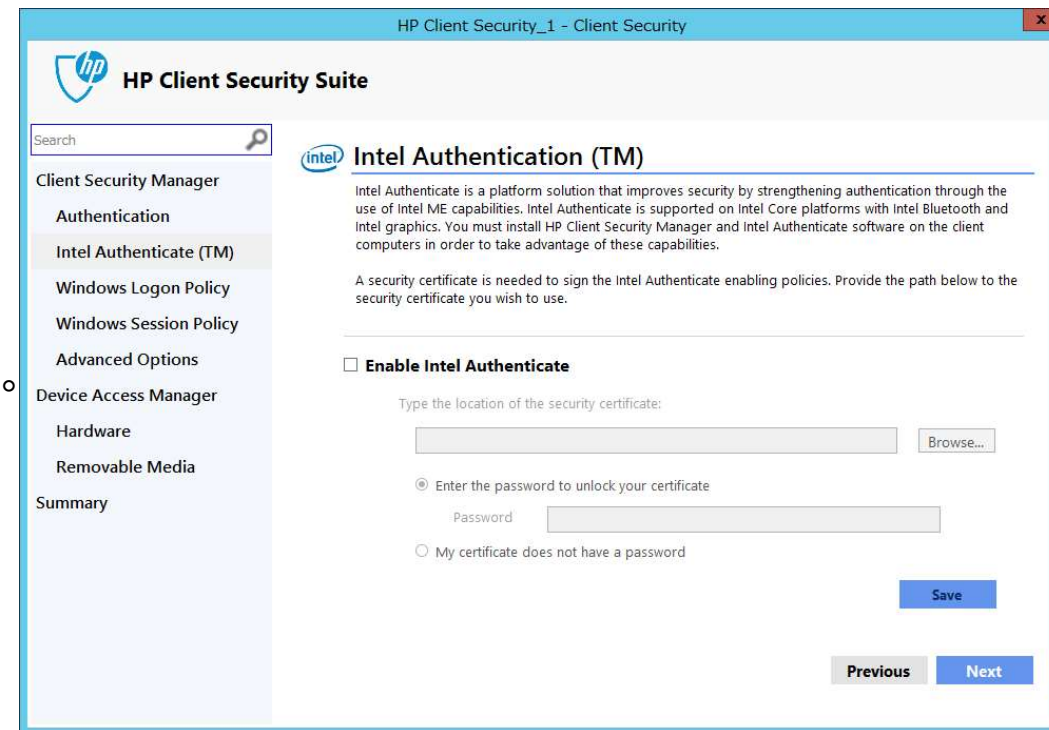
このタブではIntel Authenticateを設定します。クライアントコンピュータにIntel Authenticate Engineがインストールされている必要があります。

以下の設定ができます。

- Enable Intel Authenticate—Intel Authenticateサポートを有効にします。

この設定が有効の場合、クライアントコンピュータのIntel Authenticate Engineが使用する証明書を選択できます。

- Type the location of the security certificate—Personal Information Exchange(PFX)形式のX.509証明書ファイルを選択します。
- Enter the password to unlock your certificate—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。
- My Certificate does not have a password—証明書がパスワードで保護されていない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。



HP Client Security

Windows Logon Policy タブ

このタブではWindows ログオン認証で使用する資格情報のポリシーを設定します。

以下の設定ができます。

- Add Credential—Windows ログオンで使用する追加の認証方式を追加します。追加した認証方式を削除するには認証のアイコンの右上のXアイコンをクリックします。
- Restore Default—設定を初期状態に戻します。



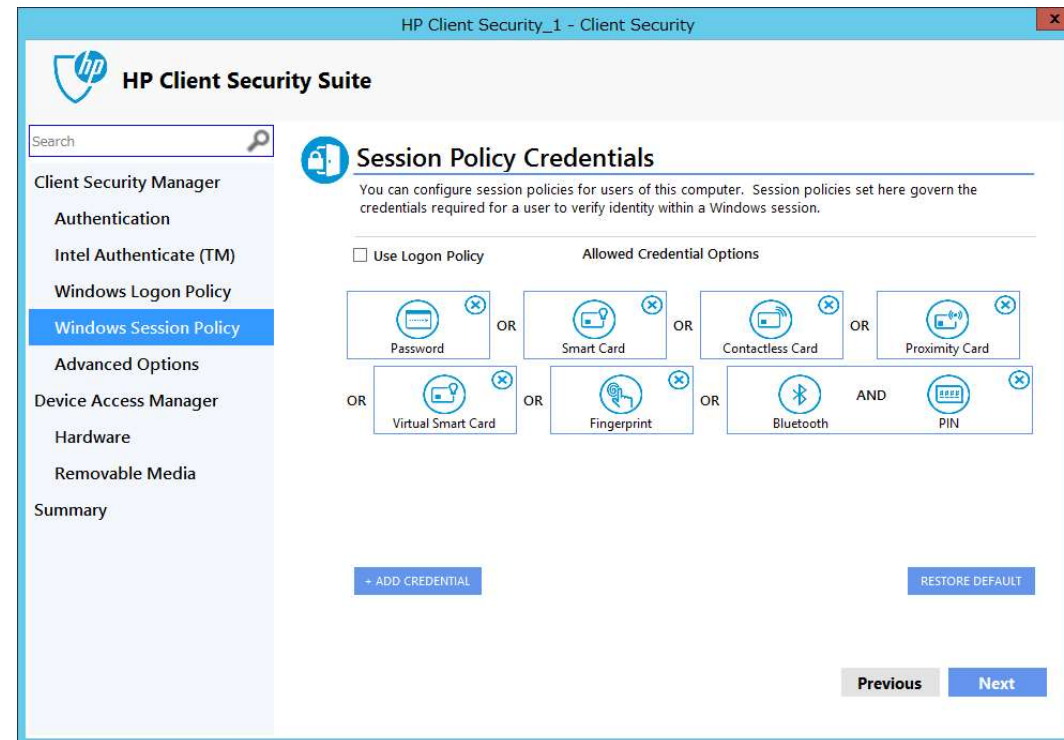
HP Client Security

Windows Session Policyタブ

このタブではWindowsセッションで使用する資格情報のポリシーを設定します。

以下の設定ができます。

- Use Logon Policy—設定済みのログオンポリシーを使用します。
- Add Credential—Windowsログオンで使用する追加の認証方式を追加します。追加した認証方式を削除するには認証のアイコンの右上のXアイコンをクリックします。
- Restore Default—設定を初期状態に戻します。



HP Client Security

Advanced Options タブ

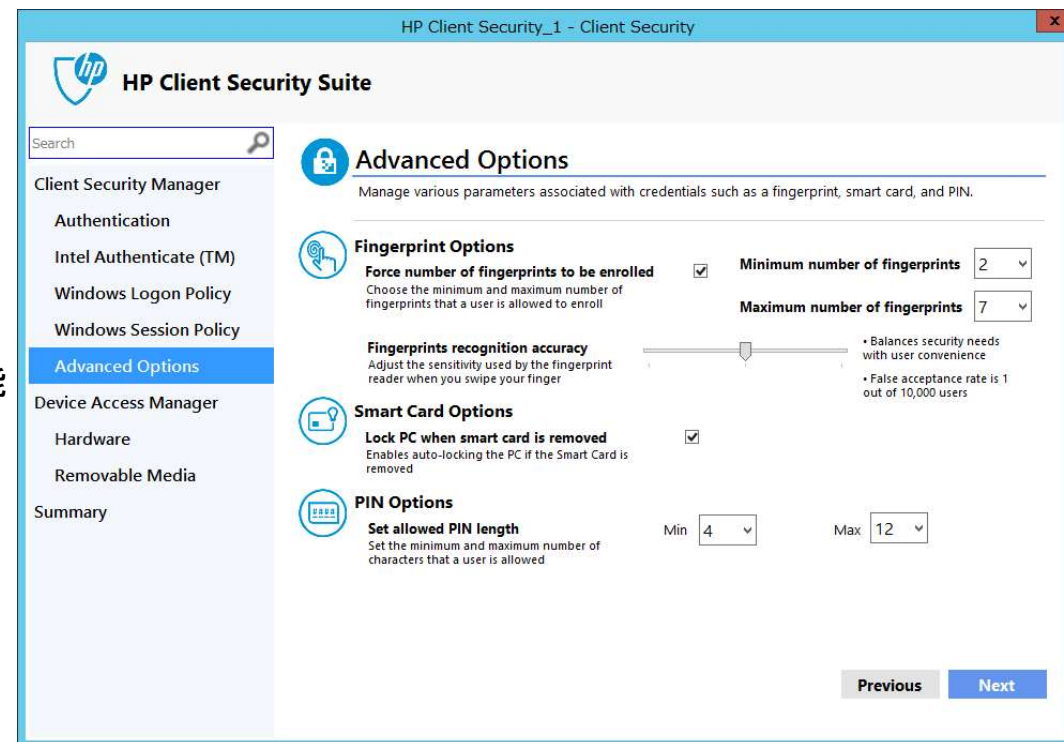
このタブではHP Client Securityで使用する資格情報の詳細設定をします。

以下の設定ができます。

- Fingerprint Options
 - Minimum number of fingerprints—1人のユーザーが登録可能な指紋の数の最小値
 - Maximum number of fingerprints—1人のユーザーが登録可能な指紋の数の最大値

Force number of fingerprints to enrollが有効な時にのみ設定可能

- Fingerprint recognition accuracy—指紋リーダーの性格率を設定します。
- Smart Card Options
 - Lock PC When smart card is removed—スマートカードが取り外された際にPCを自動的にロックします。
- PIN Options
 - Set allowed PIN length—PINの最小文字数を設定します。



HP Client Security

Device Access Manager

Hardwareタブ

このタブでは様々なデバイスやデバイスクラスのアクセス権を設定します。アクセス権は管理者（Allow Access for Administrator）と一般ユーザー（Allow Access for Standard User）ごとに設定できます。

以下のデバイスやデバイスクラスについて設定ができます。

- Biometric Devices（生体認証デバイス）
- Bluetooth（ブルートゥース）
- Imaging Devices（イメージングデバイス）
- Network adapters（ネットワークアダプタ）
- Ports(COM & LPT)（ポート（COM & LPT））

HP Client Security Suite

Search

Client Security Manager

- Authentication
- Intel Authenticate (TM)
- Windows Logon Policy
- Windows Session Policy
- Advanced Options
- Device Access Manager
- Hardware**
- Removable Media
- Summary

Device Access Manager - Hardware

Manage access permission to each device class or devices across your users.
Let's start with hardware devices that do not store data but extend your corporate network.

	Allow Access for Administrator	Allow Access for Standard User
Biometric Devices	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Bluetooth	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Imaging Devices	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Network adapters	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Ports (COM & LPT)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Note: You should not disable devices if you have selected them for authentication options.

Previous Next

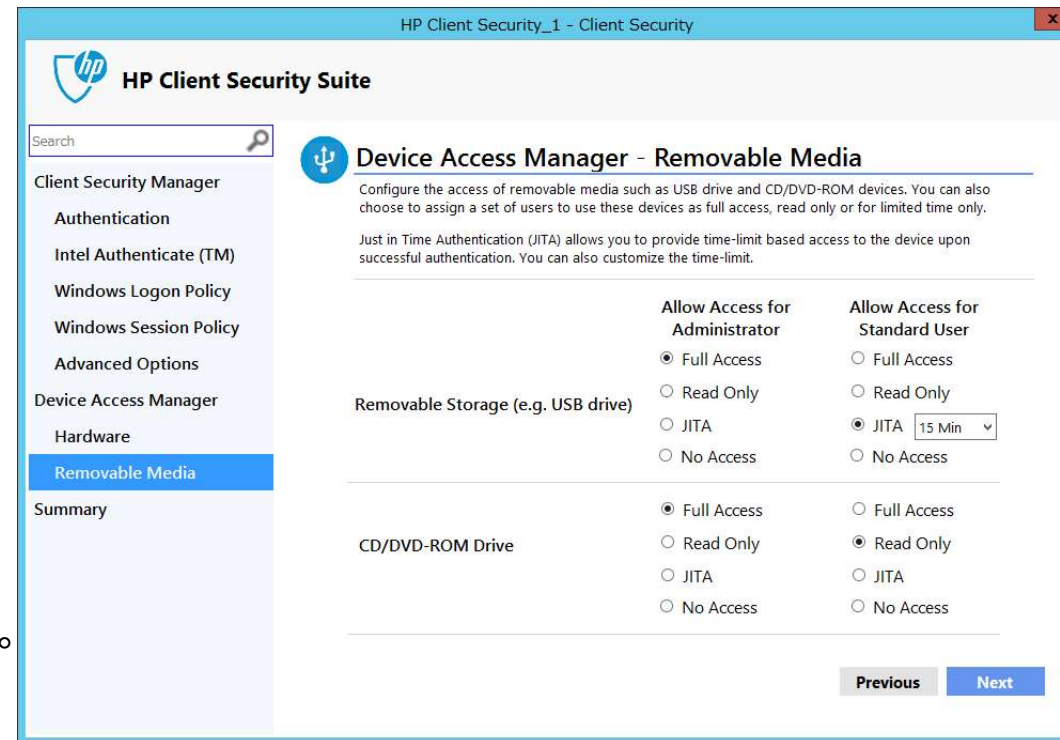
HP Client Security

Removable Mediaタブ

このタブではUSBドライブなどのリムーバブルストレージやCD/DVDドライブへのアクセス権を設定します。アクセス権は管理者（Allow Access for Administrator）と一般ユーザー（Allow Access for Standard User）ごとに設定できます。

選択したリムーバブルメディアに対して以下のアクセス権を設定できます。

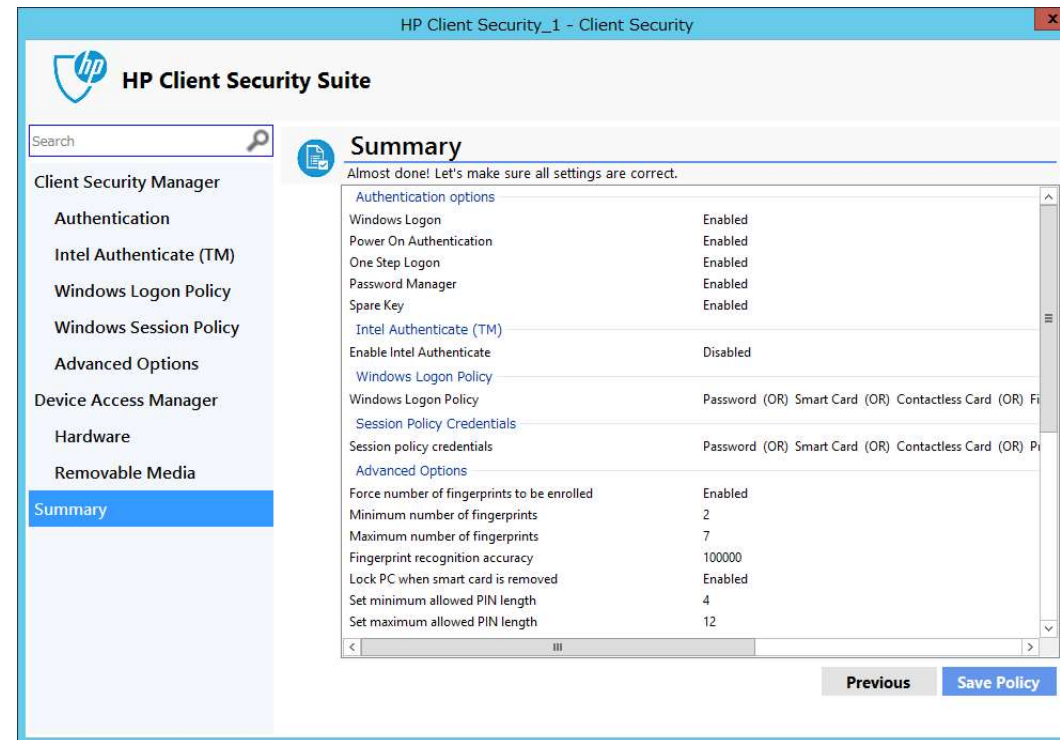
- Full Access—ファイルの追加、読み取り、編集、削除を許可します。
- Read Only—ファイルの読み取りのみを許可します。
- JITA(Just In Time Authentication)—ユーザーが資格情報を入力した後、一定時間（ドロップダウンボックスで指定して時間）ファイルへのフルアクセスを許可します。
- No Access—ファイルへのアクセスを禁止します。



HP Client Security

ポリシーの作成

1. Configuration Managerで、[資産とコンプライアンス]を選択し、[概要]を選択します。
2. HP Manageability Integration Kitを展開し、[Client Security]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、ポリシー作成ウィザードを開始します。
4. Client Securityの設定を変更したら、[次へ]を選択します。
5. Summaryページで設定内容を確認して[Save Policy]をクリックします。
6. ポリシーの保存が完了したら、[Deploy]をクリックします。
7. ポリシーを適用するターゲットのコレクションを選択し、[Deploy]をクリックします。



HP Client Security

ポリシーの編集

1. Configuration Managerで、[資産とコンプライアンス]を選択し、[概要]を選択します。
2. HP Manageability Integration Kitを展開し、[Client Security]を右クリックして、[Edit Policy]を選択します。
3. ベースライン名を選択し、[OK]をクリックしてます。
4. ポリシー作成ウィザードのSummary画面が表示されますので[Previous]をクリックします。
5. ポリシーの作成と同じ手順を実行します。

追加情報

HP Client SecurityのポリシーにはClient Security ManagerとDevice Access Managerの両方の設定が含まれます。

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、およびインテルの認証を設定する方法の詳細については、「インテルの認証」マニュアルを参照してください。

Device Guard(Windows 10のみ)

Device GuardはWindows 10 Enterprise Editionの機能で、ハードウェアおよびソフトウェアベースのマルウェア対策機能です。アプリケーションやドライバーを実行する前にそれらが信頼された提供元からのものであるかを確認し、信頼されない場合は実行されません。HP MIKのDevice Guardポリシーを使用してDevice Guardを有効化するための設定を簡単に行うことができます。

サポート対象のクライアントコンピュータ

- 2015年モデル以降のHPコマーシャルコンピュータ

サポート対象のOS

- Windows 10

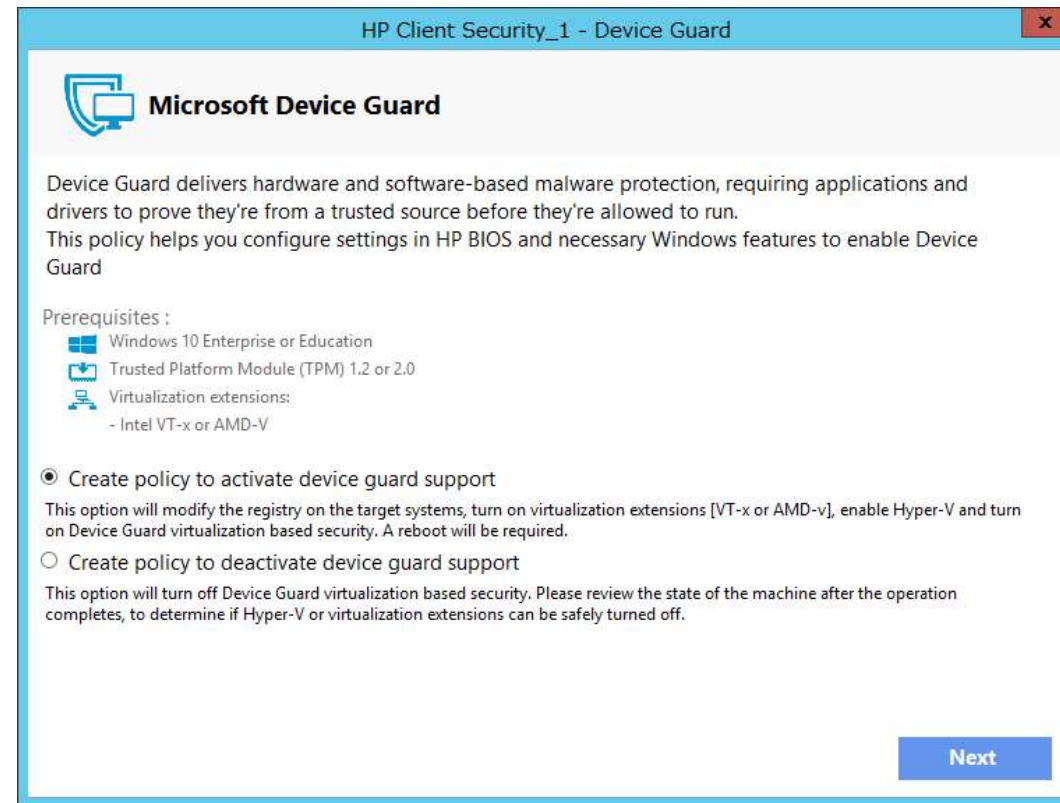
前提条件

- Microsoft .NET Framework 4.0以上
- HP MIK

Device Guard

ポリシーの作成

1. Configuration Managerで、[資産とコンプライアンス]を選択し、[概要]を選択します。
2. HP Manageability Integration Kitを展開し、[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、ポリシー作成ウィザードを開始します。
4. 以下のオプションのどちらかを選択します。
 - A) Create a policy to activate device guard support—Device Guardを有効にするために対象デバイスのレジストリ設定を変更し、仮想化技術を有効にします。
 - B) Create a policy to deactivate device guard support—Device Guardを無効にするために対象デバイスのレジストリ設定を変更し、仮想化技術技術を無効にします。
5. Summaryページで設定内容を確認して[Save Policy]をクリックします。
6. ポリシーの保存が完了したら、[Deploy]をクリックします。
7. ポリシーを適用するターゲットのコレクションを選択し、[Deploy]をクリックします。



Device Guard

Device GuardポリシーでDevice Guard supportを有効にした際に変更される設定

レジストリ設定

```
[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
```

Windowsの機能

Microsoft Hyper-V と Isolated User Mode を有効にします

BIOS設定

- SVM CPU Virtualization を有効にします (AMD プラットフォーム)
- Virtualization Technology (VTx) を有効にします (Intel プラットフォーム)
- Virtualization Technology for Directed I/O (VTd) を有効にします (Intel プラットフォーム)
- TPM Device を利用可能にします
- TPM State を利用可能にします
- CD-ROM Boot を無効にします
- PXE Boot を無効にします
- USB Storage Boot を無効にします
- Legacy Boot を無効にします
- UEFI Boot を有効にします
- Configure Legacy Boot Support を Legacy Support Disable and Secure Boot Enable にします

Device Guard

ポリシーの編集

1. Configuration Managerで、[資産とコンプライアンス]を選択し、[概要]を選択します。
2. HP Manageability Integration Kitを展開し、[Device Guard]を右クリックして、[Edit Policy]を選択します。
3. ベースライン名を選択し、[OK]をクリックします。
4. ポリシーの作成と同じ手順を実行します。

追加情報

クライアントコンピュータでHP MIK Device Guardのログは%PROGRAMDATA%\HP\HP MIK\Logsに保存されます。

次のエラーコードが発生する可能性があります

エラーコード	説明
0	正常終了
1	不明なエラー。インストールエラーの可能性
2	OSがサポートされていません
3	CPU/チップセットがサポートされていません
4	古いグラフィックスドライバです
5	BIOSのCPU仮想化の有効化に失敗
6	BIOSのTPMデバイスの利用可能に失敗
7	BIOSのUSBブートの無効化に失敗
8	BIOSのPXEブートの無効化に失敗
9	BIOSのフロッピーブートの無効化に失敗
10	BIOSのCD-ROMブートの無効化に失敗
11	BIOS Boot ModeのUEFI Nativeへの変更に失敗
12	BIOSセキュアブートの有効化に失敗
13	Hyper-Vの設定に失敗
14	分離ユーザーモードの設定に失敗
15	レジストリ設定の変更に失敗
16	Windows機能の変更に失敗

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の整合性を確認することにより、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を検証する頻度の増加や、HP Sure Startのイベントログを収集する事ができます。

HP MIKのHP Sure Startポリシー管理では、ポリシーをリモートで管理し、BIOSの悪意のある攻撃やセキュリティ侵害の適切なログと通知、およびその後の修復を保証します。

サポート対象のクライアントコンピュータ

- 2014年モデルのHP 700シリーズ以上の
コマーシャルノートPC
- 2015年モデル以降のHP 700シリーズ以上の
コマーシャルコンピュータ

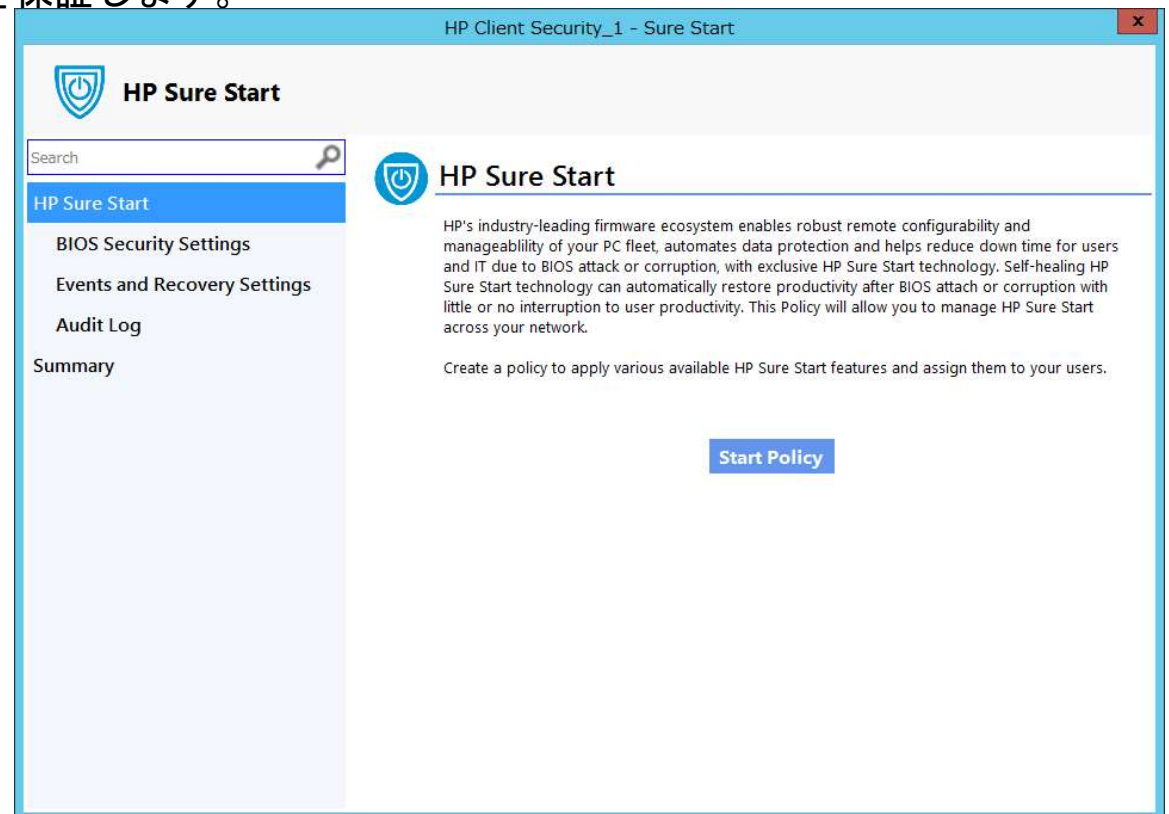
サポート対象のOS

- Windows 10
- Windows 8.1
- Windows 7

前提条件

Microsoft .NET Framework 4.0以上

HP MIK

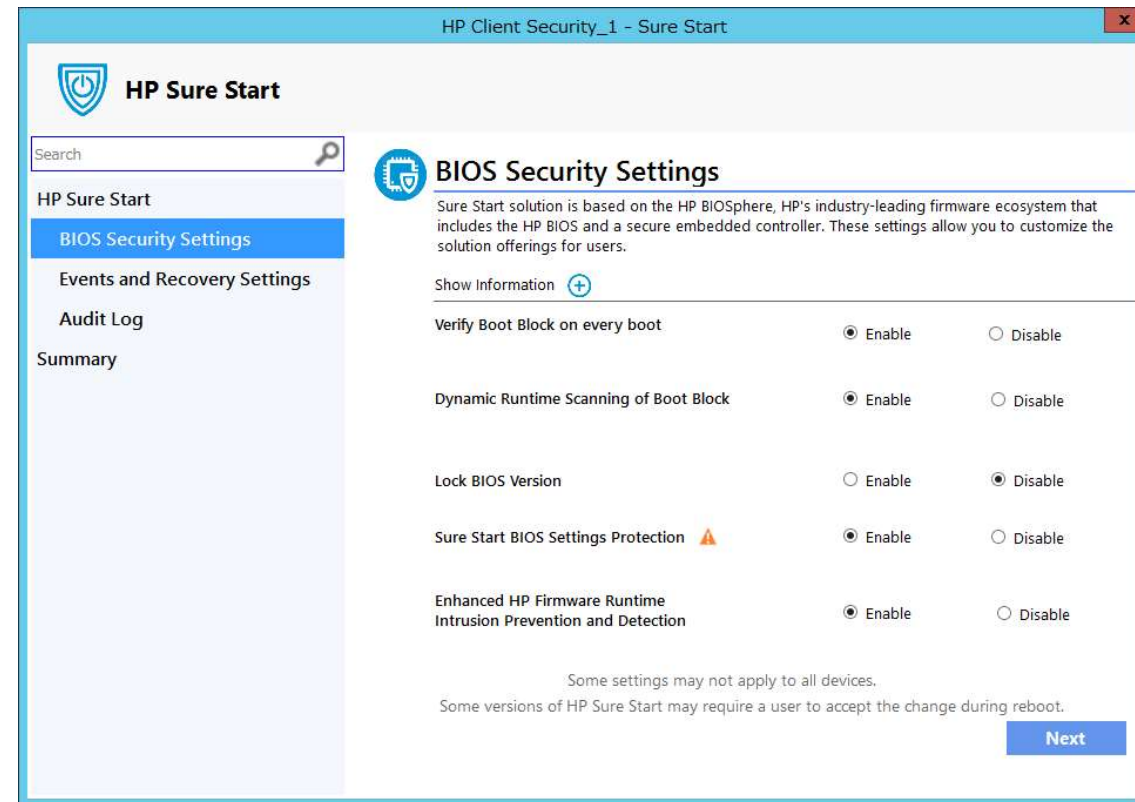


HP Sure Start

ユーザーインターフェース

BIOS Security Settingsタブ

- Verify Boot Block on every boot—システムブートイメージへの許可された変更が不揮発性メモリに格納されていることを確認します。
- Dynamic Runtime Scanning of Boot Block—コンピュータが起動していてOSが動作している時にHPブートイメージの完全性を定期的に確認します。
- Lock BIOS Version—BIOSのアップデートを禁止します。
- Sure Start BIOS Setting Protection—全てのBIOS設定の変更を無効にしてHP Sure Startの不揮発性メモリからこれらのBIOS設定の保護を強化します。この設定を有効にするにはBIOS管理者パスワードの設定が必要です。
- Enhanced HP Firmware Runtime Intrusion Protection and Detection—OSが動作している時にメインメモリで実行されているHPシステムファームウェアを監視します。

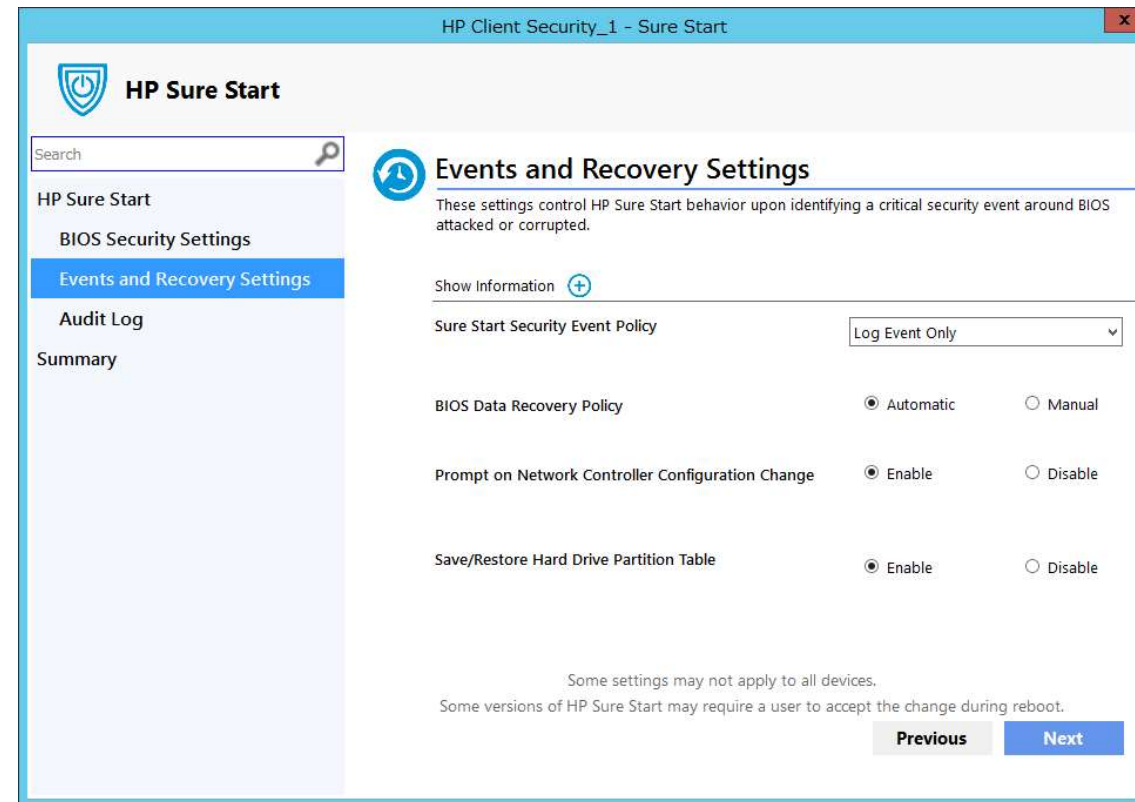


HP Sure Start

Events and Recovery Settings タブ

これらの設定ではBIOSが攻撃を受けたり破損するなどの危機的なセキュリティイベントが確認された際のHP Sure Startの動作を制御します。

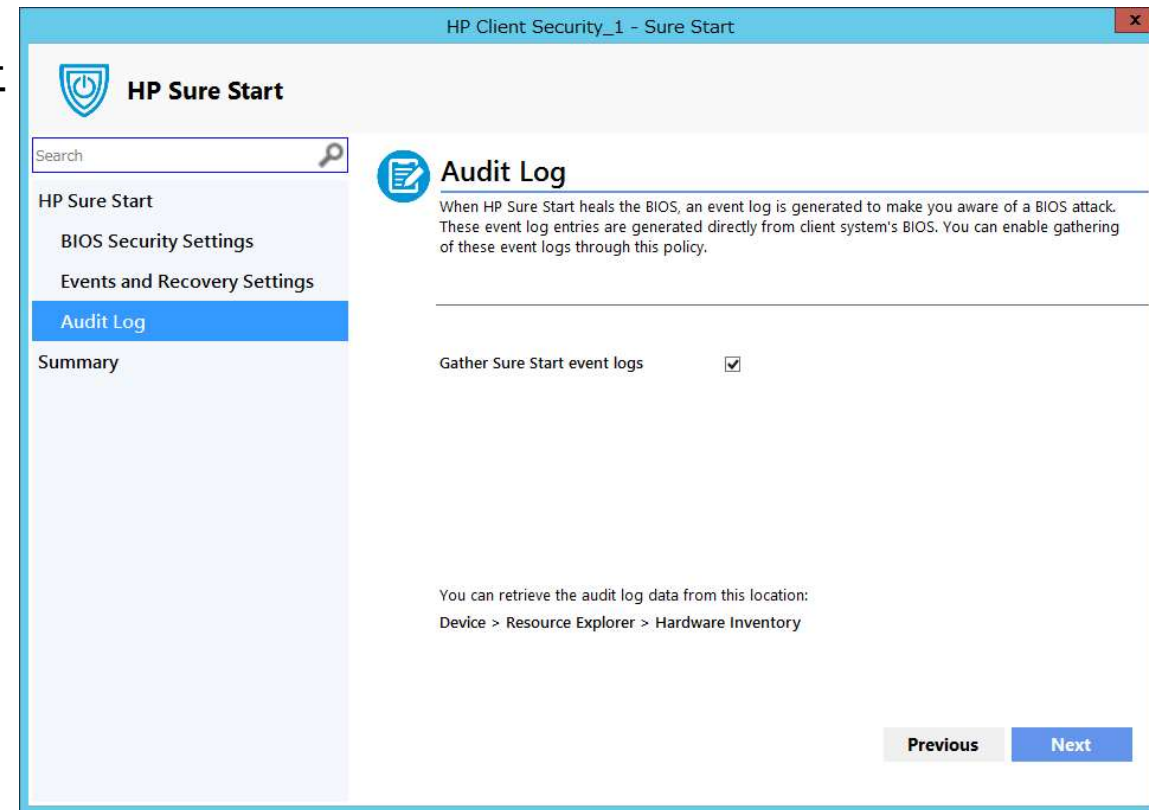
- Sure Start Security Event Policy—ログレベルを選択します。
 - Log Event Only—HP Sure Start不揮発メモリ内の監査ログの全てのクリティカルセキュリティイベントをWindowsイベントログに収集します
 - Log Event and Power Off System—セキュリティイベントを検出してログ収集した後システムの電源を強制的に切ります。
- BIOS Data Recovery Policy—Manualを選択した場合BIOSデータの復旧にEsc+Windows+ ↑ + ↓ キーの入力が必要になります。
- Prompt on Network Controller Configuration Change—ネットワークコントローラの構成を監視して工場出荷状態からの変更を検出した際にユーザーに通知します。
- Save/Restore Hard Drive Partition Table—システムドライブのMBRまたはGPTを保存します。



HP Sure Start

Audit Logタブ

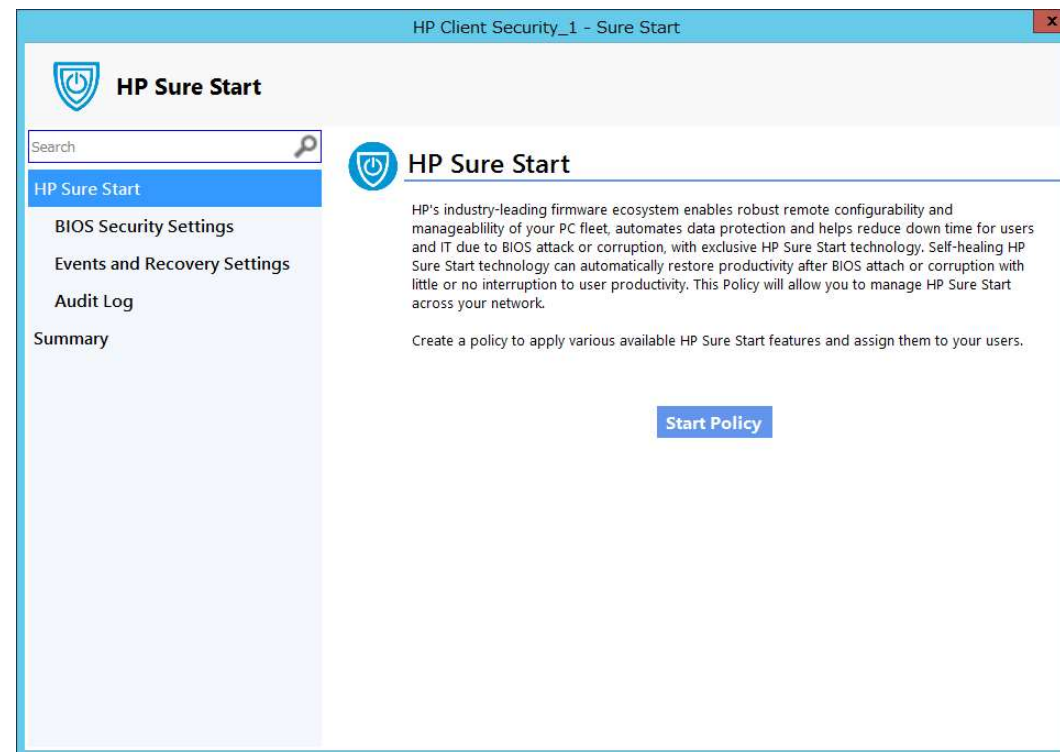
[Gather Sure Start event logs]を選択するとクライアントコンピュータからHP Sure StartイベントログをConfiguration Managerのハードウェアインベントリに収集します。



HP Sure Start

ポリシーの作成

1. Configuration Managerで、[資産とコンプライアンス]を選択し、[概要]を選択します。
2. HP Manageability Integration Kitを展開し、[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、[Start Policy]をクリックします。
4. 設定を変更し、[Next]をクリックします。
5. Summaryページで設定内容を確認して[Save Policy]をクリックします。
6. ポリシーの保存が完了したら、[Deploy]をクリックします。
7. ポリシーを適用するターゲットのコレクションを選択し、[Deploy]をクリックします。



HP Sure Start

ポリシーの編集

1. Configuration Managerで、[資産とコンプライアンス]を選択し、[概要]を選択します。
2. HP Manageability Integration Kitを展開し、[Sure Start]を右クリックして、[Edit Policy]を選択します。
3. ベースライン名を選択し、[OK]をクリックします。
4. ポリシー作成ウィザードのSummary画面が表示されますので[Previous]をクリックします。
5. ポリシーの作成と同じ手順を実行します。

追加情報

システムによっては一部の機能がサポートされていない場合があります。特定のシステムでは、構成の変更後に手動で再起動する必要がある場合があります。

監査ログ

クライアントコンピュータでHP MIK Sure Startのログは%PROGRAMDATA%\HP\HP MIK\Logに保存されます。

設定が有効の場合、HP MIKはHP Sure StartログをConfiguration Managerのハードウェアインベントリとして収集します。

以下の手順で監査ログを表示します。

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

TPM Firmware Update

TPM Firmware Updateポリシーでは以下の事ができます。ノートPC

- 古いTPM1.2から新しいTPM1.2へのアップグレード
- 古いTPM2.0から新しいTPM2.0へのアップグレード
- TPM1.2からTPM2.0への変換
- TPM2.0からTPM1.2への変換

サポート対象のクライアントコンピュータ

デスクトップPC

- HP EliteDesk 800 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 ProDesk 400 G2 Desktop Mini PC
- HP ProDesk 400 G3 Small Form Factor PC
- HP ProDesk 600 G2 Desktop Mini PC
- HP ProDesk 600 G2 Microtower PC
- HP ProDesk 600 G2 Small Form Factor PC
- HP ProOne 600 G1 All-in-One PC
- HP RP9 G1 Retail System Model 9015 / 9018

- HP EliteBook 1030 G1 Notebook PC
- HP EliteBook 725 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 450 G3 Notebook PC
- HP ProBook 455 G3 Notebook PC
- HP ProBook 470 G3 Notebook PC
- HP ZBook 15 G3 Mobile Workstation 26
- HP ZBook 17 G3 Mobile Workstation
- HP ZBook Studio G3 Mobile Workstation

サポートOS

- Windows 10
- Windows 8.1
- Windows 7

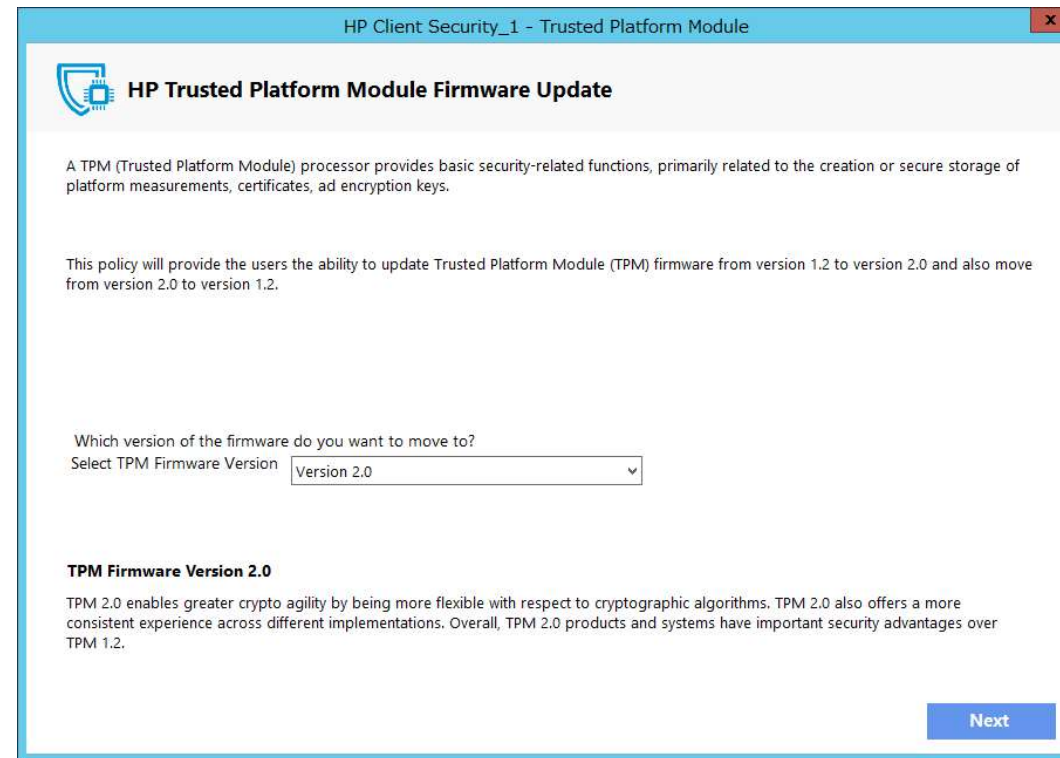
前提条件

- Infineon SLB9670 TPMチップ
- 最新バージョンのBIOS
- Microsoft .NET Framework 4.0以上
- HP MIK

TPM Firmware Update

ポリシーの作成

1. Configuration Managerで、[資産とコンプライアンス]を選択し、[概要]を選択します。
2. HP Manageability Integration Kitを展開し、[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、[Start Policy]をクリックします。
4. 変更後のTPMのバージョンを選択し、[Next]をクリックします。警告と制限については追加情報をご参照ください。
5. Summaryページで設定内容を確認して[Save Policy]をクリックします。
6. ポリシーの保存が完了したら、[Deploy]をクリックします。
7. ポリシーを適用するターゲットのコレクションを選択し、[Deploy]をクリックします。



TPM Firmware Update

ポリシーの編集

1. Configuration Managerで、[資産とコンプライアンス]を選択し、[概要]を選択します。
2. HP Manageability Integration Kitを展開し、[TPM Firmware Update]を右クリックして、[Edit Policy]を選択します。
3. ベースライン名を選択し、[OK]をクリックします。
4. ポリシー作成ウィザードのSummary画面が表示されますので[Previous]をクリックします。
5. ポリシーの作成と同じ手順を実行します。

追加情報

警告

データの消失を防ぐためにプライマリドライブの暗号化を解除してからこのポリシーを展開してください。このポリシーではBitLockerとWinMagicドライブ暗号化のみをチェックします。BitLockerやWinMagicドライブ暗号化を使用している場合、このポリシーはエラーコードを出して終了します。このポリシーではその他のドライブ暗号化ソリューションを検出しません。

TPM1.2とTPM2.0の間の変換は最大64回可能です。

TPMを変換すると新しいバージョンのTPMファームウェアにアップグレードされます。

- TPM1.2からTPM2.0に変換するとTPM2.0が有効になり、TPM2.0の新しいバージョンにアップグレードされます。
- TPM2.0からTPM1.2に変換するとTPM1.2が有効になり、TPM1.2の新しいバージョンにアップグレードされます。
- TPM1.2からTPM1.2に変換するとTPM1.2の新しいバージョンにアップグレードされます。
- TPM2.0からTPM2.0に変換するとTPM2.0の新しいバージョンにアップグレードされます。

HP WorkWise(Windows 10のみ)

HP WorkWiseはスマートフォンを利用するアプリケーションで、PCのセキュリティ向上、監視、操作の簡略化などの機能があります。ユーザーは各自のスマートフォンにHP WorkWiseアプリをストアからダウンロードしてインストールできますが、IT管理者はクライアントコンピュータでどの機能の利用を許可するかを指定する事ができます。

サポート対象のクライアントコンピュータ

- 2017年モデル以降のHPコマーシャルコンピュータ

サポート対象のOS

- Windows 10 Anniversary Update

前提条件

- Microsoft .NET Framework 4.0以上
- HP WorkWiseソフトウェア

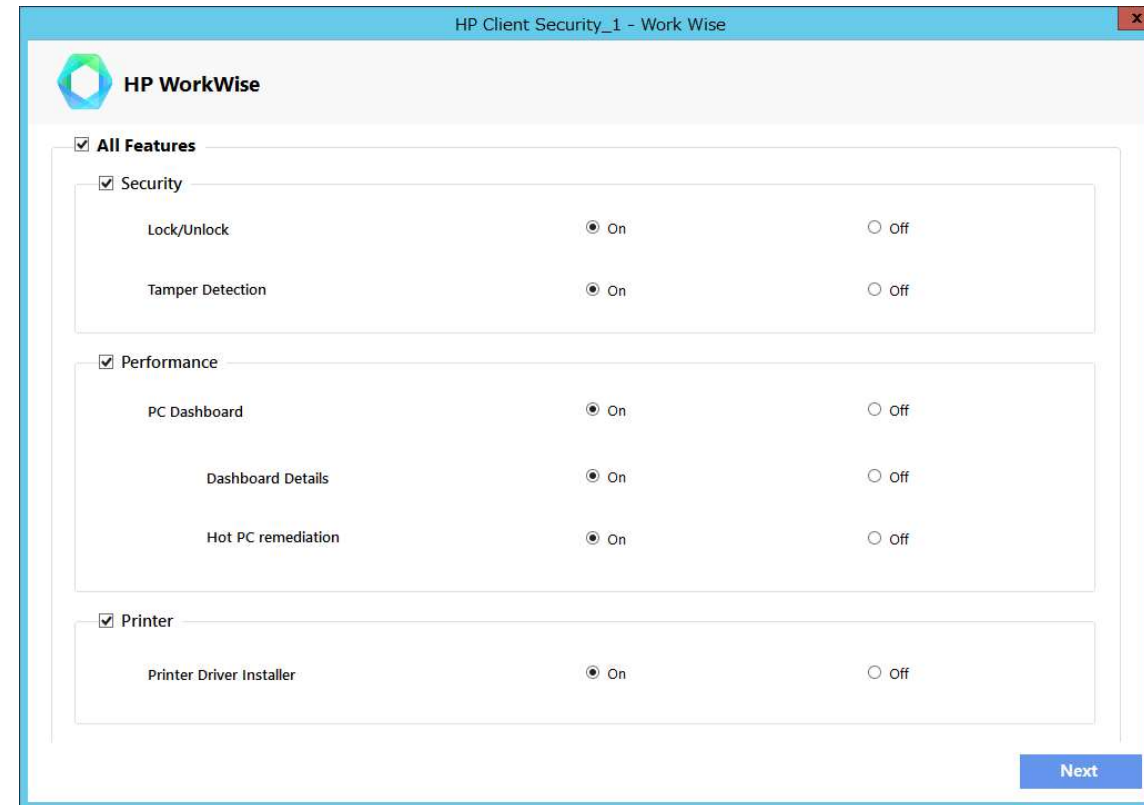
HP WorkWiseの各機能に固有の要件についてはHP WorkWiseのドキュメントをご参照ください。

HP WorkWise

ユーザーインターフェース

HP WorkWiseの機能の有効/無効を設定できます。

- All Features—全ての機能を有効にします。
- Security—Lock/UnLockとTamper Detectionの機能を有効/無効にします。
- Performance—PC DashboardとHot PC remediation機能を有効/無効にします。
- Printer—Printer Driver Installerの機能を有効/無効にします。



HP WorkWise

ポリシーの作成

1. Configuration Managerで、[資産とコンプライアンス]を選択し、[概要]を選択します。
2. HP Manageability Integration Kitを展開し、[HP WorkWise]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、[Start Policy]をクリックします。
4. 変更後のTPMのバージョンを選択し、[Next]をクリックします。警告と制限については追加情報をご参照ください。
5. Summaryページで設定内容を確認して[Save Policy]をクリックします。
6. ポリシーの保存が完了したら、[Deploy]をクリックします。
7. ポリシーを適用するターゲットのコレクションを選択し、[Deploy]をクリックします。

ソフトウェアライブラリ

ソフトウェアライブラリ

HP Manageability Integration Kitをインストールするとソフトウェアライブラリに以下の項目が追加（青色実線）または作成可能（緑色破線）になります。

ソフトウェアライブラリ

- 概要
 - アプリケーション管理
 - アプリケーション
 - ストア アプリのライセンス情報
 - パッケージ
 - HP Client Support Packages** (青色実線)
 - HP Client BIOS Configuration Utility
 - HP Client Support Tools
 - 承認要求
 - グローバル条件
 - App-V 仮想環境
 - Windows サイドローディング キー
 - アプリケーション管理ポリシー
 - アプリ構成ポリシー
- ソフトウェア更新プログラム
- オペレーティング システム
 - ドライバー
 - ドライバー パッケージ
 - HP Client Driver Packages (緑色破線)
 - オペレーティング システム イメージ
 - オペレーティング システム アップグレード パッケージ
 - ブート イメージ
 - HP Client Boot Images (緑色破線)
 - タスク シーケンス
 - タスク シーケンス (緑色破線)

HP Client Driver Pack

ドライバーパッケージとは

ドライバパッケージは1つまたは複数のデバイスドライバの内容を含むConfiguration Managerのパッケージです。ドライバーパッケージはタスクシーケンスの中でOSイメージに追加します。OSイメージに新しいPCの機種のためのドライバーパッケージを追加する事でそのOSイメージを新しいPCの機種で利用できるようになります。

HP MIKの機能

HP MIKをインストールするとドライバーパッケージを作成するための以下の3つの機能が追加されます。

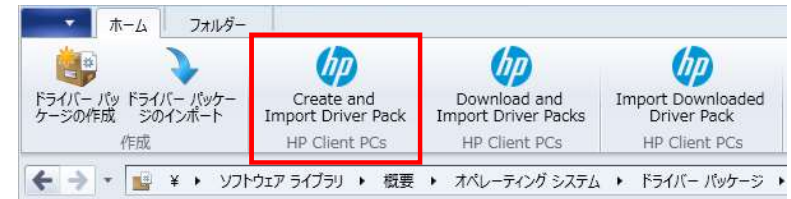
- Create and Import Driver Pack
 - 複数の機種用のドライバーをHPからダウンロードして複数の機種に対応するドライバーパッケージを作成することができます。
 - HPドライバーパックの作成をサポートする機種でのみ利用可能です。
- Download and Import Driver Pack
 - 1つのHPドライバーパックをHPからダウンロードして1つのドライバーパッケージを作成することができます。
 - HPドライバーパックが提供されている機種（600シリーズ以上のビジネスPC製品）でのみ利用可能です。
- Import Downloaded Driver Pack
 - 自分で作成したドライバーパックをインポートして1つのドライバーパッケージを作成することができます。
 - HPドライバーパックが提供されていない機種（400シリーズ以下のビジネスPC製品）ではこの方法を使用します。

HP Client Driver Pack

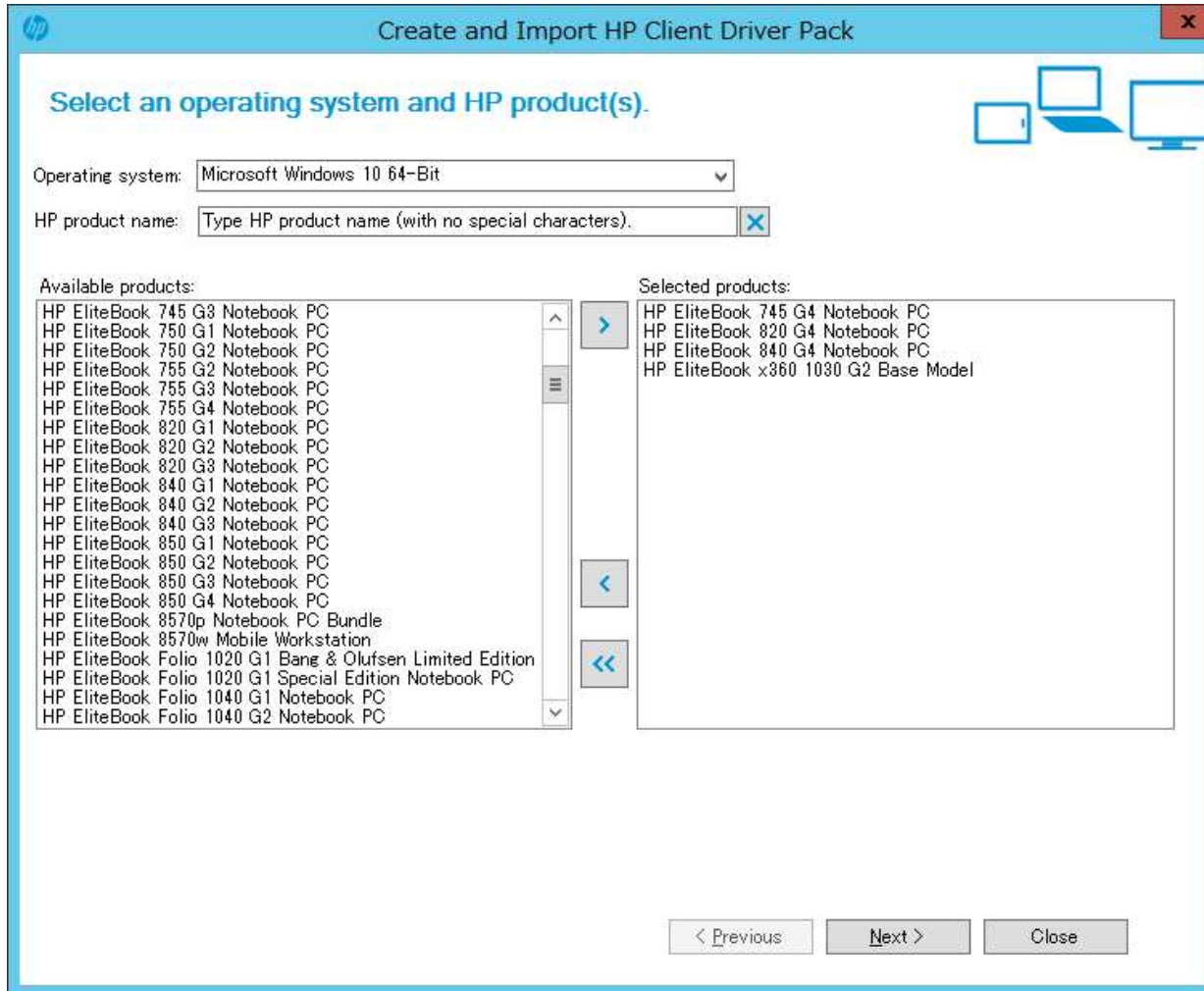
HPドライバーパックの作成とインポート

Create and Import Driver PackオプションではサポートされるHP製品のドライバーが表示されます。

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]→[ドライバーパッケージ]を選択します。
2. リボンメニューのHP Client PCsセクションの[Create and Import Driver Pack]を選択します。Create and Import Driver Packウィザードが表示されます。
3. [Operating System]を選択します。
4. ドライバーパックの作成をサポートする製品のみが、Available Products列に表示されます。必要に応じてキーワードをHP製品名ボックスに入力し、Enterキーを押して使用可能な製品の一覧をフィルタします。
5. 使用可能な製品を選択し、右矢印ボタンを選択してSelected製品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。同じファミリモデルの製品を選択することをお勧めします。最適なドライバを使用してドライバパックを作成します。また、ドライバーパックごとに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ノートブックPCとHP ProBook 650 G1ノートブックPCを選択して、HP ProBook 600シリーズG1ノートブックPCドライバパックを作成することができます。



HP Client Driver Pack

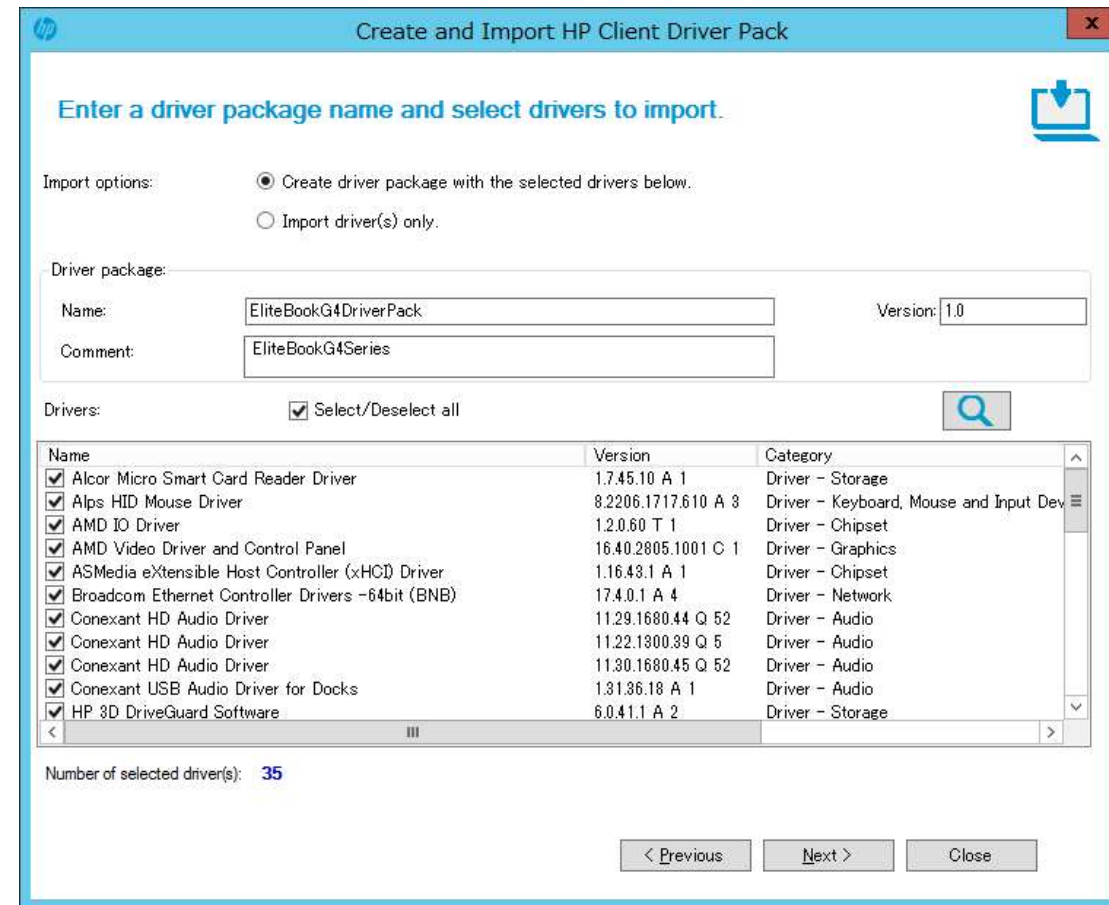


HP Client Driver Pack

8. [Next]をクリックします。
9. 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。このオプションでは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に付ける名前を入力します。必要に応じてバージョンとコメントを入力します。
 - B. Driversの下で、ドライバーパッケージに含めるドライバーが選択されている事と、その他のドライバーのチェックが外れている事を確認します。

または、自動適用するドライバをインポートして後でドライバパックを作成するには、[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ます。

10. [Next]をクリックします。



HP Client Driver Pack

8. 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DriversとDriver Package(s)を保存するためのネットワーク共有を選択します。
11. ドライバーをインポートするだけの場合は、Configuration ManagerがDriversを保存するためのネットワーク共有を選択します。
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、このボックスが選択されています。複数のドライバが選択されている場合、現在のドライバがインポートに失敗した場合は、次に選択されたドライバがインポートされます。

Create and Import HP Client Driver Pack

Select distribution point(s), network shares and other settings.

Distribution point(s): HPI-SCCM.HPILOCAL Select all

Select network share(s) and other settings.

Drivers: \\HPI-SCCM\hpi.local\SMS_H01\OSD\Lib\Drivers\HP\Client Browse...

Driver package(s): \\HPI-SCCM\hpi.local\SMS_H01\OSD\Lib\DriverPackages\HP\Client Browse...

Error handling: Continue on errors File transfer protocol: HTTP Save settings

< Previous Import Close

HP Client Driver Pack

12. デフォルトではFile transfer protocolがHTTPになっており、HP MIKは選択したドライバーのダウンロードにHTTPを使用します。必要に応じて[FTP]を選択してください。
13. ネットワーク共有の選択やその他の設定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手順の設定を保存するには、このボタンを選択します。

注記

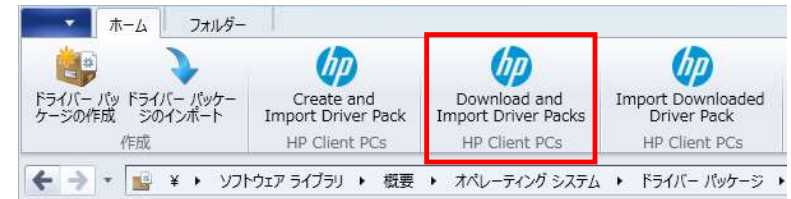
このプロセスではConfiguration Managerから<ftp.hp.com>へのインターネット接続が必要となります。インターネット接続できない場合は次の手順の方法でドライバーパックを入手した後、[Import Downloaded Driver Pack]メニューを使用してインポートします。

HP Client Driver Pack

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 PackオプションではサポートされるHP製品とドライバーパックが表示されます。

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]→[ドライバーパッケージ]を選択します。
2. リボンメニューのHP Client PCsセクションの[Download and Import Driver Pack]を選択します。
3. [Operating System]を選択します。
4. ドライバーパックの作成をサポートする製品のみが、Available Products列に表示されます。必要に応じてキーワードをHP製品名ボックスに入力し、Enterキーを押して使用可能な製品の一覧をフィルタします。
5. 対象となる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、右矢印ボタンを選択して、Selected products列に製品を追加します。選択した製品の関連するドライバーパックがAvailable driver packsの一覧に表示されます。
6. 配布ポイントを選択して、インポートされたドライバパックを特定の宛先に割り当てます。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Configuration Managerがドライバーやドライバーパッケージを保存するデフォルトの場所を変更します。保存先の選択やその他の設定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。



HP Client Driver Pack

- 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、このボックスが選択されています。複数のドライバが選択されている場合、現在のドライバがインポートに失敗した場合は、次に選択されたドライバがインポートされます。
- デフォルトではFile transfer protocolがHTTPになっており、HP MIKは選択したドライバーパックのダウンロードにHTTPを使用します。必要に応じて[FTP]を選択してください。
- [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。

ダウンロードとインポートのプロセスの最中には処理内容と進捗状況のダイアログボックスが表示されます。このプロセスでは選択したドライバーパックをダウンロードして、Configuration Managerにインポートします。選択したドライバーパックがConfiguration Managerの中に既に存在している場合は既存のドライバーパックを上書きするか、またはスキップするかを選択するためのプロンプトが表示されます。プロセスが完了すると各ドライバーパックごとのインポート状態のサマリが表示されます。

インポートしたドライバーパックは[ドライバーパッケージ]→[HP Driver Packages]の下に作成されます。

インポートしたドライバーパックをタスクシーケンスで使用するには配布ポイントに展開されている必要があります。Download and Import Driver Packsウィザードで配布ポイントを選択していなかったり、追加の配布ポイントを使用したい場合はドライバーパックを選択して[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。インターネット接続できない場合は次の手順の方法でドライバーパックを入手した後、[Import Downloaded Driver Pack]メニューを使用してインポートします。

HP Client Driver Pack

HPドライバーパックのダウンロードとインポート

Select an operating system and HP product(s).

Operating system:

HP product name:

Available products:

- HP EliteDesk 800 35W G2 Desktop Mini PC
- HP EliteDesk 800 35W G8 Desktop Mini PC (ENERGY STAR)
- HP EliteDesk 800 65W G2 Desktop Mini PC
- HP EliteDesk 800 65W G8 Desktop Mini PC
- HP EliteDesk 800 G2 Small Form Factor PC
- HP EliteDesk 800 G2 Tower PC
- HP EliteDesk 880 G2 Tower PC
- HP EliteOne 705 G2 23-inch Touch All-in-One PC
- HP EliteOne 800 G2 23-inch Non-Touch All-in-One PC
- HP EliteOne 800 G2 23-inch Touch All-in-One PC

Selected products:

- HP EliteDesk 800 G3 Small Form Factor PC

Available driver packs:

Name	Version	Released Date	Size (MB)	Driver Pack ID	View Release Notes	Remove
HP ElitePro 600/800 G3 PC Win10 x64 Driver Pack	5.00.A.1	2017-02-23	722.3	sp79189	<input type="button" value="View"/>	<input type="button" value="X"/>

Distribution point(s): Select all

Select network share(s) and other settings.

Drivers:

Driver package(s):

Error handling: Continue on errors File transfer protocol:

HP Client Driver Pack

HPドライバーパックの入手方法

HPドライバーパックにはいくつかの入手方法があります。

注記

一部のドライバーはHP MIKで利用できないものもあります。例えばシステム—ソフトウェア管理の下のカテゴリのドライバーはHP MIKからインポートできません。

- HP Client Management Solutionウェブサイト
- HP Softpaq Download Manager(SDM)

HP Client Management Solutionウェブサイトからのドライバーパックの入手方法

1. <http://www.hp.com/go/clientmanagement> にアクセスします。
2. Resourcesの下の[HP Driver Packs]をクリックします。
3. 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OSに対応したドライバーパックをダウンロードします。

HP Client Driver Pack

HP SDMを使用したドライバーパックの入手方法

1. <http://www.hp.com/go/clientmanagement>にアクセスします。
2. Resourcesの下の[HP Download Library]をクリックします。
3. [SoftPaq Download Manager]をダウンロードします。
4. ダウンロードしたSDMをインストールします。
5. SDMを起動します。[すべてのプログラム]→[HP]→[HP Softpaq Download Manager]。
6. [すべての製品を表示]を選択します。
7. [ツール]→[構成オプション]を選択します。
8. Filter→OSにSDMで表示するOSの種類を選択します。
9. Filter→Languageに[English – International]を選択します。
10. 構成オプションで[OK]をクリックします。
11. 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。
12. CategoryがManageability – Driver Packにあるドライバーパックをダウンロードします。

HP Client Driver Pack

HP SDMを使用したドライバーパックの作成方法

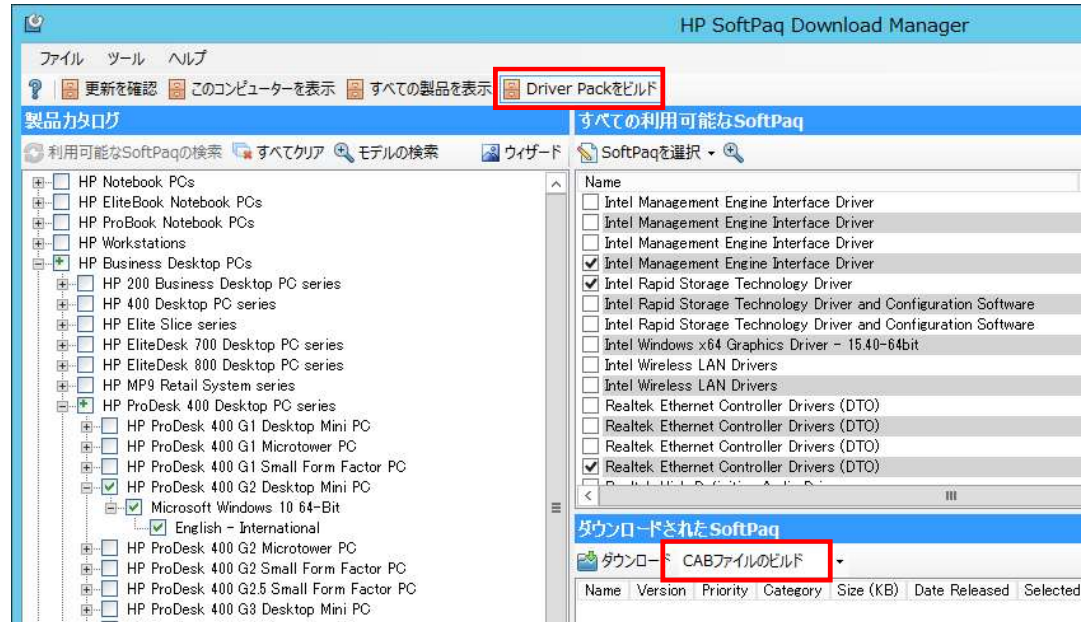
HP SDM(バージョン3.5.2.0以上) を使用してドライバーパックする事ができます。ドライバーパックが提供されていないコンピュータではこの方法を使用して自作します。

1. SDMを起動します。[すべてのプログラム]→[HP]→[HP Softpaq Download Manager]。
2. [Driver Packをビルド]を選択します。
3. [ツール]→[構成オプション]を選択します。
4. Filter→OSでSDMで表示するOSの種類にチェックを付けます。
5. Filter→Languageに[English – International]を選択します。
6. 構成オプションで[OK]をクリックします。
7. 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。
8. 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。
9. ダウンロードされたSoftPaqで、ダウンロードボタンの隣のドロップダウンメニューから[CABファイルのビルド]を選択します。
10. [ダウンロード]をクリックします。

HP Client Driver Pack

11. 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。
12. Driver Pack BuilderウィンドウでOS-BitnessにOSとビット数を選択します。
13. ドラ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。
14. ドライバーパックの圧縮が完了しましたのダイアログが表示されたら[OK]をクリックします。

ドライバーパックと関連のログが出力先フォルダに作成されます。



HP Client Driver Pack

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]を選択します。
2. リボンメニューのHP Client PCsセクションの[Import Downloaded Driver Pack]を選択します。
3. [Browse]をクリックしてインポートするドライバーパックを選択します。
4. 配布ポイントを選択して、インポートされたドライバパックを特定の宛先に割り当てます。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ケージを保存するデフォルトの場所を変更します。
6. 保存先の選択やその他の設定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。
7. [Import]をクリックします。

ダウンロードとインポートのプロセスの最中には処理内容と進捗状況のダイアログボックスが表示されます。インポートしたドライバーパックは[ドライバーパッケージ]→[HP Driver Packages]の下に作成されます。

インポートしたドライバーパックをタスクシーケンスで使用するには配布ポイントに展開されている必要があります。Download and Import Driver Packsウィザードで配布ポイントを選択していなかったり、追加の配布ポイントを使用したい場合はドライバーパックを選択して[コンテンツの配布]を選択します。



HP Client Driver Pack

HP ドライバーパックのインポート

Import Downloaded HP Client Driver Pack

Select an HP client driver pack to import.

Driver package: C:\HPSDM\ProDesk400G2DMDriverPack\ProDesk400G2DM_DriverPack_wt64_2017-03- Browse...

Driver pack title: ProDesk400G2DM DriverPack

Distribution point(s): HPI-SCCM.HPILOCAL Select all

Select network share(s) and other settings.

Drivers: \\HPI-SCCM.hpi.local\SMS_H01\OSD\Lib\Drivers\HP\Client Browse...

Driver package(s): \\HPI-SCCM.hpi.local\SMS_H01\OSD\Lib\DriverPackages\HP\Client Browse...

Save settings

Import Close

HP Client Boot Image

WinPEドライバーパックの入手

1. <http://www.hp.com/go/clientmanagement> にアクセスします。
2. Resourcesの下の[HP Download Library]をクリックします。
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。

注記

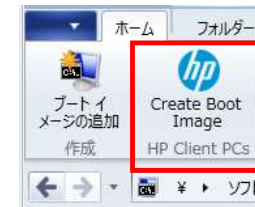
Configuration Managerの各バージョンは、特定のバージョンのWinPEのみにドライバやコンポーネントをカスタマイズまたは追加することをサポートしているため、HP MIK Create Boot Imageは限定的なサポートを提供します。WinPEのカスタマイズの要件の詳細については、

[http : //technet.microsoft.com/en-us/library/dn387582.aspx](http://technet.microsoft.com/en-us/library/dn387582.aspx)

を参照してください。

HP MIK ブートイメージの作成機能は、ブートイメージ用のConfiguration ManagerとADKカスタマイズサポートを活用しているため、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依存します。

HP Client Boot Image



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

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]を選択します。
2. リボンメニューのHP Client PCsセクションの[Create Boot Image]を選択します。
3. [Browse]をクリックしてインポートするWinPEドライバパックを選択します。HP MIKには、選択したWinPEドライバパックに適したブートイメージのみが表示され、Configuration Managerによるカスタマイズがサポートされています。
4. 対象のブートイメージ（Base boot image）を選択します。[Create]をクリックして選択したHP WinPEドライバパックを含んだブートイメージを作成します。
5. 配布ポイントを選択して、インポートされたドライバパックを特定の宛先に割り当てます。しかし、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がドライバやドライバパッケージを保存するデフォルトの場所を変更します。
7. 保存先の選択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。後続のドライバおよび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。

HP Client Boot Image

Specify an HP client WinPE driver pack and base boot image(s) to create HP client boot images.

HP client WinPE driver pack: C:\Users\Administrator\Downloads\sp78464.exe Browse...

Driver pack title: HP Client WinPE 10.0 x64 Driver Pack [1.30.A.1]

Base boot image(s): Boot image (x64)

Distribution point(s): HPI-SCCMHPILOCAL Select all

Select network share(s) and other settings.

Drivers: %%HPI-SCCMhpi.local\SMS_H01\OSD\Lib\Drivers\HP\Client Browse...

Driver package(s): %%HPI-SCCMhpi.local\SMS_H01\OSD\Lib\DriverPackages\HP\Client Browse...

Boot image(s): %%HPI-SCCMhpi.local\SMS_H01\OSD\Lib\BootImages\HP\Client Browse...

Save settings

Create Close

HP Client Boot Image

ベースイメージのアーキテクチャとWindowsプレインストール環境ブートイメージでサポートされているアーキテクチャに応じて、x86および/またはx64イメージが作成されます。

Windows 10用のHP WinPEドライバーパックには、64ビットのブートイメージ用のドライバが含まれています。

以前のバージョン用のWinPEドライバーパックには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、新しいブートイメージが[ブート イメージ]→[HP Client Boot Images]に作成されます。

WinPEでデバッグ目的でコマンドプロンプトを使用するため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]を選択します。
2. [カスタマイズ]タブを選択し、[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展開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、または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を変更した場合は、ブートイメージを選択して、[コンテンツの配布]を選択します。

HP Client Task Sequence

デプロイメント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]を選択します。
2. リボンメニューのHP Client PCsセクションの[Create Deployment Task Sequence]を選択します。
3. Task Sequence Template 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。次のテンプレートが選択可能です。
 - Default template for Windows 10 : Windows 10用のテンプレート
 - Default template for Windows 7 or Windows 8 : Windows 7/8用のテンプレート
 - Configure RAID example : RAID構成用のテンプレート
4. Task sequence nameとNetwork account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]のチェックを外します。

Configuration ManagerのBDEタスクシーケンスステップの情報は以下を参照してください。
<https://technet.microsoft.com/enus/library/hh846237.aspx>
6. [Create]をクリックします。
7. Successのダイアログで[OK]をクリックします。

HP Client Task Sequence

Create HP Client Bare Metal Deployment Task Sequence

Task sequence template: Default template for Windows 10

A default task sequence example for Windows 10 that shows you how to change HP BIOS settings in a task sequence using HP BIOS Configuration Utility. Please read the user guide on how to configure the HP BIOS using the Set BIOS Configuration step.

Task sequence name: HP Client Task Sequence

Network (Administrator) account:
Enter administrator-level credentials to access shares and WMI on the site server.

Account name: Domain#UserName

Password:

Confirm password:

Operating system installation:

Use an OS WIM
 Scripted OS

Operating system package to use

Include BitLocker Drive Encryption steps

Required HP client packages:

HP Client BIOS Configuration Utility
HP Client Support Tools

Create Cancel

重要

選択したテンプレートに応じて、以下のステップはデータの削除を伴います。

- Remove Disk Partitions(diskpart clean)
- Format and Partition Disk
- Call Intel RSTCli Utility – Delete All Metadata
- Call Intel RSTCli Utility – Configure RAID Volume

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責任を負いかねます。

HP Client Task Sequence

タスクシーケンスの設定

タスクシーケンスのリストを更新して、作成したタスクシーケンスを表示します。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設定する必要があります。

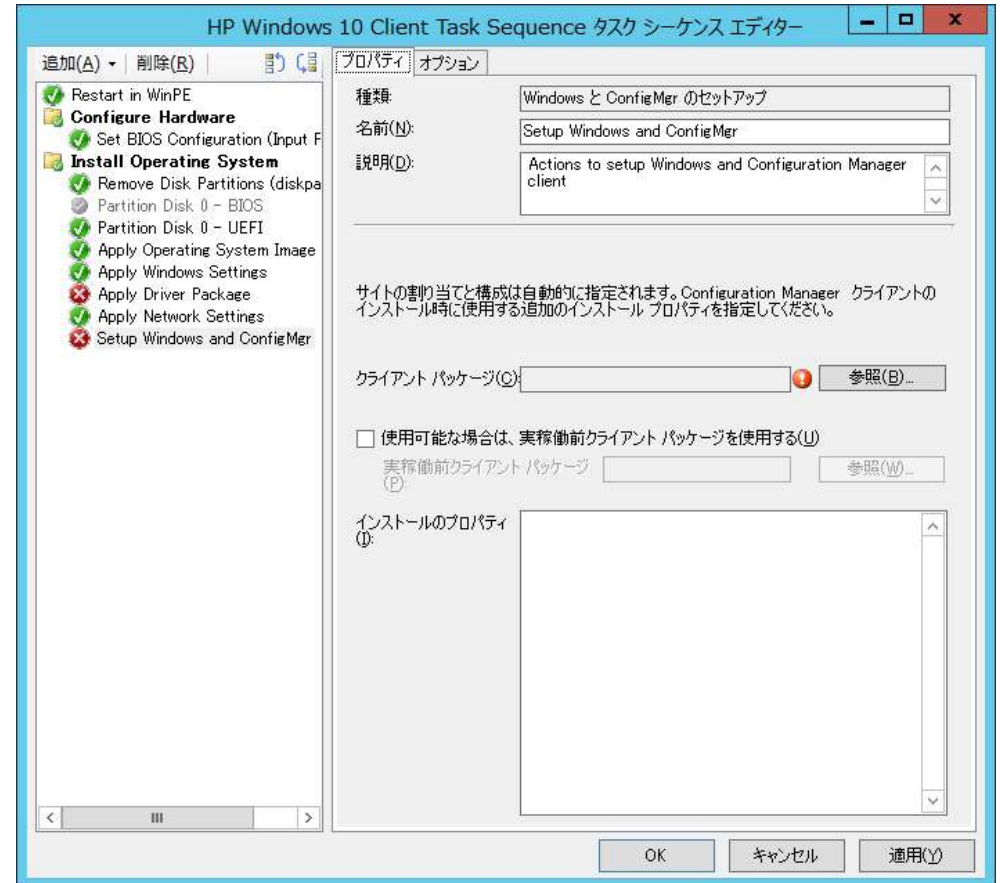
Configure RAID Exampleテンプレートに含まれている特定のステップは「Configure RAID Exampleテンプレートの使用」で説明します。

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 Client Driver Pack」の章を参照してください。
2. 対象のタスクシーケンスを右クリックして[編集]を選択します。
3. タスクシーケンスで参照されているオブジェクトが見つからない事のダイアログが表示されますので[OK]をクリックします。

以下の画像はDefault Template for Windows 10テンプレートを使用して作成したタスクテンプレートのもので、

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。デフォルトのパーティションはディスク容量の1%となっています。必要に応じてこの値をWindowsリカバリイメージのサイズ（通常500 MB以上）に変更します。

HP Client Task Sequence

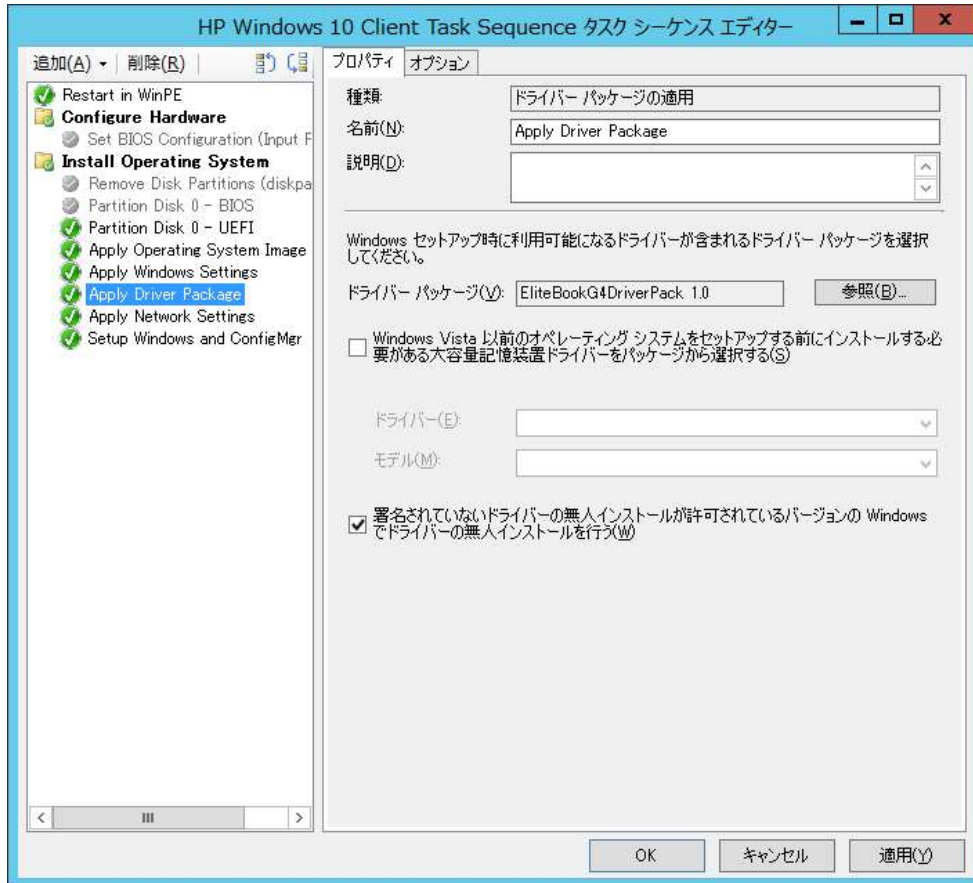


HP Client Task Sequence

4. デプロイメントの対象OSに応じて以下のステップを設定します。
 - Set BIOS Configuration (Input file)—BIOS Config Utilityを使用してBIOS設定を変更できます。TPMを使用する場合はこのステップでTPMを有効にして初期化する必要があります。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。
 - Remove Disk Partitions(diskpart clean)—このステップの設定は不要です。タスクシーケンスが適切に実行されるにはネットワーク上のコンテンツディレクトリにアクセスできるように設定されている必要があります。詳細は「Allowing access to deployment content」を参照してください。このステップが不要な場合はステップを無効にしてください。
 - Format and Partition Disk—ディスクを必要に応じてフォーマットおよびパーティション化するための適切な手順を有効にします。たとえば、UEFIまたはUEFI Hybrid (CSMを使用) 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を無効にします。
 - Apply Driver Packages—デプロイメント対象のOSイメージに追加するHPドライバーパックを選択します。
 - Apply Network Settings—デプロイメント対象をワークグループにするかドメインに参加するかを選択し、必要に応じてActive Directoryドメインのアカウント情報を入力します。

追加のタスクシーケンスステップを参照し、必要に応じて追加およびパラメータを設定します。
5. すべてのタスクシーケンスステップの設定が完了したら[OK]または[適用]をクリックして変更を保存します。

HP Client Task Sequence



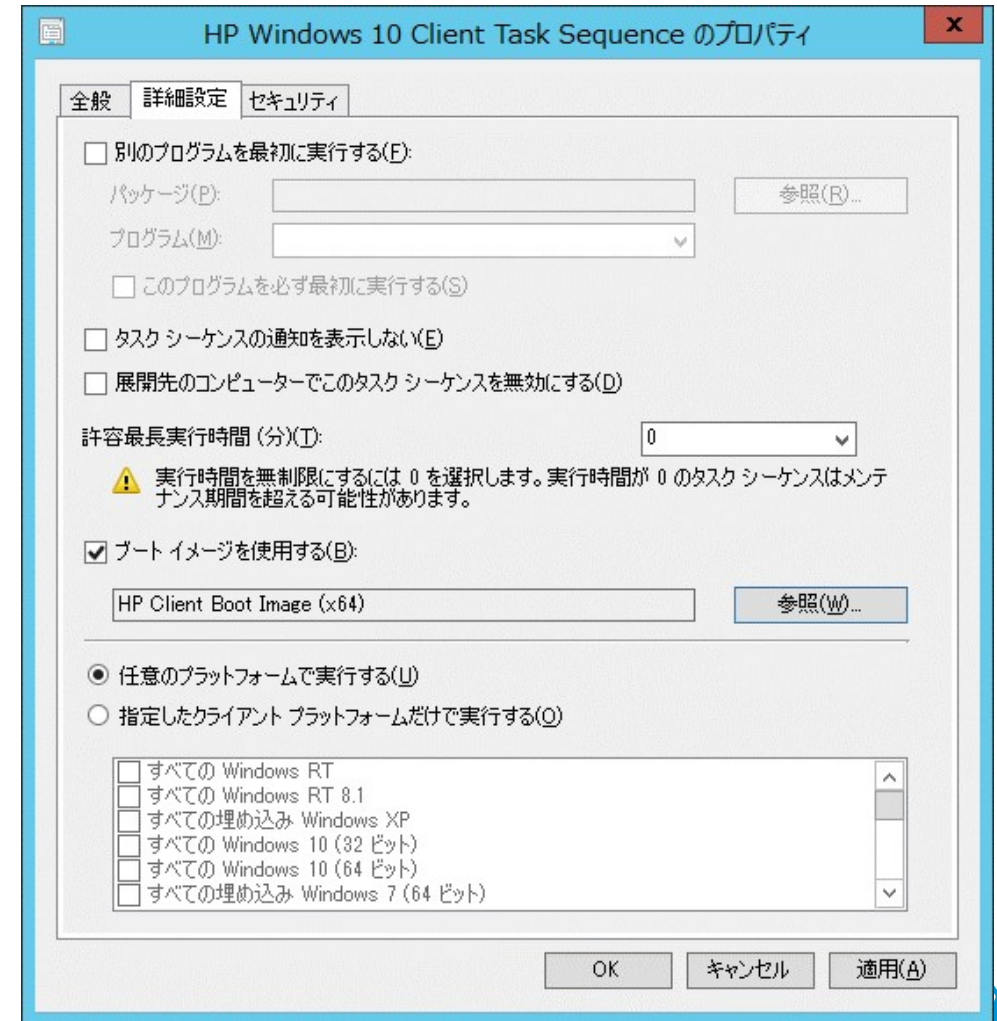
HP Client Task Sequence

ブートイメージの割り当て

1. 対象の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。
4. [OK]をクリックします。

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。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。



HP Client Task Sequence

デプロイメントコンテンツへのアクセス許可設定

HP MIKタスクシーケンスのRemove Disk Partitions(diskpart clean)ステップはネットワークから直接実行する必要があります。そのためには、ブートイメージを含むタスクシーケンスのすべてのパッケージとコンテンツが以下のように設定されている必要があります。

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。

HP Client Task Sequence

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BIOS設定を行う事ができます。このコマンドラインの実行タスクではBIOS Config Utility(BCU)を使用します。

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>

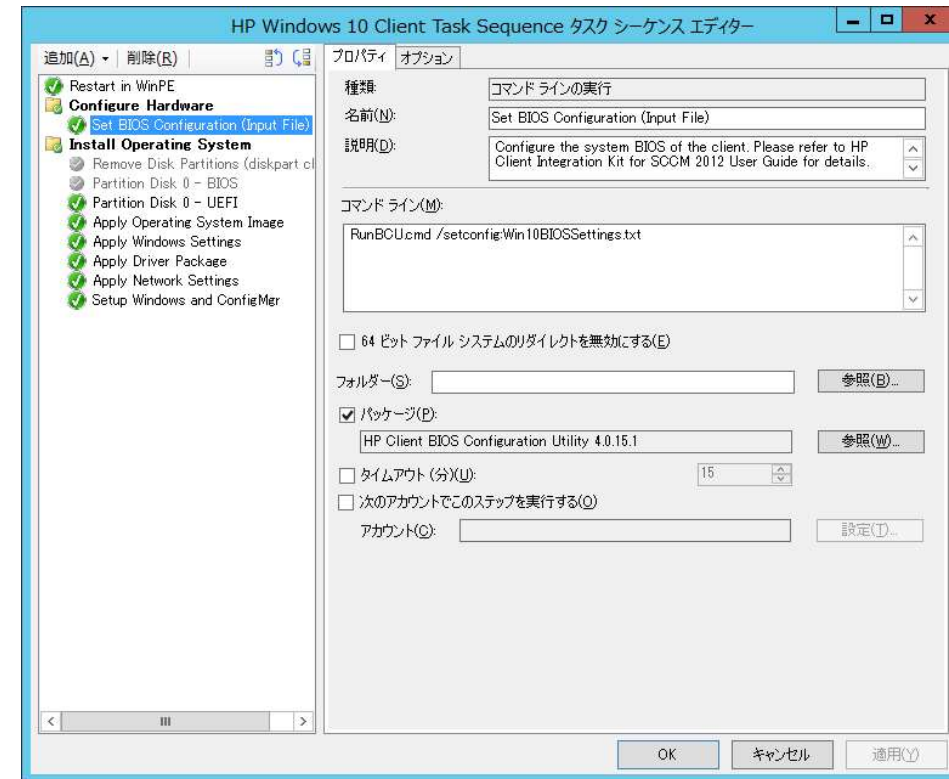
パラメータやオプションの一覧はHP BIOS Configuration Utility User Guideを参照してください。

サンプルのBIOS設定 (REPSET) ファイル

(BCUSettingExampleOnly.REPSET) がBCUのソースフォルダ内のConfigフォルダにあります。この設定ファイルを使用する場合のコマンドラインは以下のようになります。

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

REPSETファイルはコマンドラインを簡単にするためにBCUソースフォルダまたはそのサブフォルダに置くことを推奨します。



HP Client Task Sequence

BIOS設定ファイルの追加および編集

注記

このタスクシーケンスステップを使用する際には以下を注意してください。

- パッケージフォルダのBIOS設定ファイルの追加や編集した時には、新しいBIOS設定ファイルがこのタスクシーケンスステップで使用できるようにHP BIOS Configuration Utilityパッケージを配布ポイントにアップデートしてください。
- いくつかのBIOS設定変更はターゲットコンピュータが再起動するまで反映されません。全ての設定が適用されるには再起動が必要な場合があります。
- 特定のBIOS設定を変更するとタスクシーケンスが失敗する場合があります。タスクシーケンスを広く展開する前に必要な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、正しく動作するために特別なエスケープが必要な場合があります。詳細については、*HP BIOS Configuration Utility User Guide*を参照してください。

HP Client Task Sequence

1. 対象のコンピュータからBIOS設定ファイルを抽出します。BIOS設定ファイルの設定を変更したい箇所を編集して残りの部分は削除します。
2. BCUのパッケージソースフォルダを確認します。Configuration Managerで[ソフトウェアライブラリ]→[概要]→[パッケージ]→[HP Client Support Tools]を右クリックして[プロパティ]を選択します。データソースタブのソースフォルダを確認します。
3. BIOS設定（REPSET）ファイルをBCUソースフォルダにコピーします。
4. 配布ポイントを更新して新しいREPSETファイルがタスクシーケンスで利用できるようにします。

HP Client Task Sequence

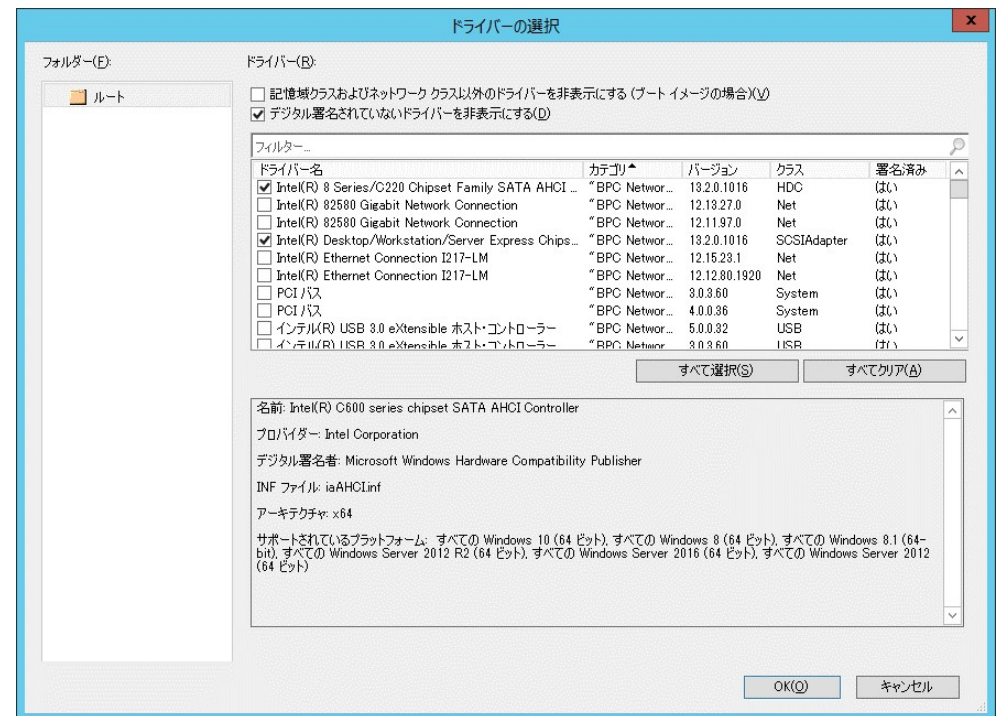
Configure RAID Exampleテンプレートの使用方法

タスクシーケンスで使用するブートイメージの準備

1. ブートイメージに必要なドライバーが含まれている事を確認します。
2. この後のステップで追加するドライバーとの競合を避けるためにIntel Rapid Storage Technology (Intel RST) RAIDドライバーを削除します。
3. 対象のクライアントコンピュータをサポートするバージョンのIntel Rapid Storage Technology RAIDドライバーをブートイメージに追加します。

注記

Windows 7およびWindows 8.1でのみ利用可能です。



HP Client Task Sequence

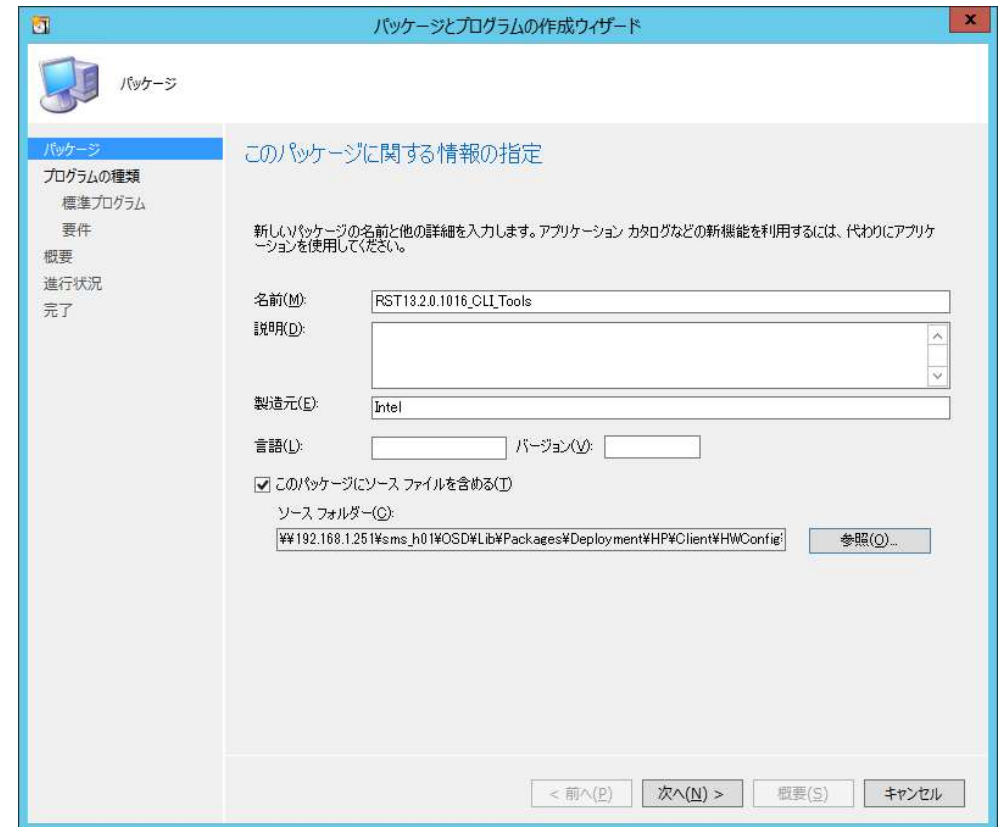
タスクシーケンスで使用するパッケージの準備

1. 対象のクライアントコンピュータのドライバerpパッケージがインポートされている事を確認します。
2. <https://downloadcenter.intel.com> にアクセスして、[RST Cli]を検索します。ドライバerpのバージョンに対応したツールのバージョンを選択してダウンロードします。

注記：

ドライバerpとツールのメジャーバージョンとマイナーバージョンを合わせる必要があります。バージョン12.8.Xのツールはドライバerpバージョン12.8.Xで動作します。

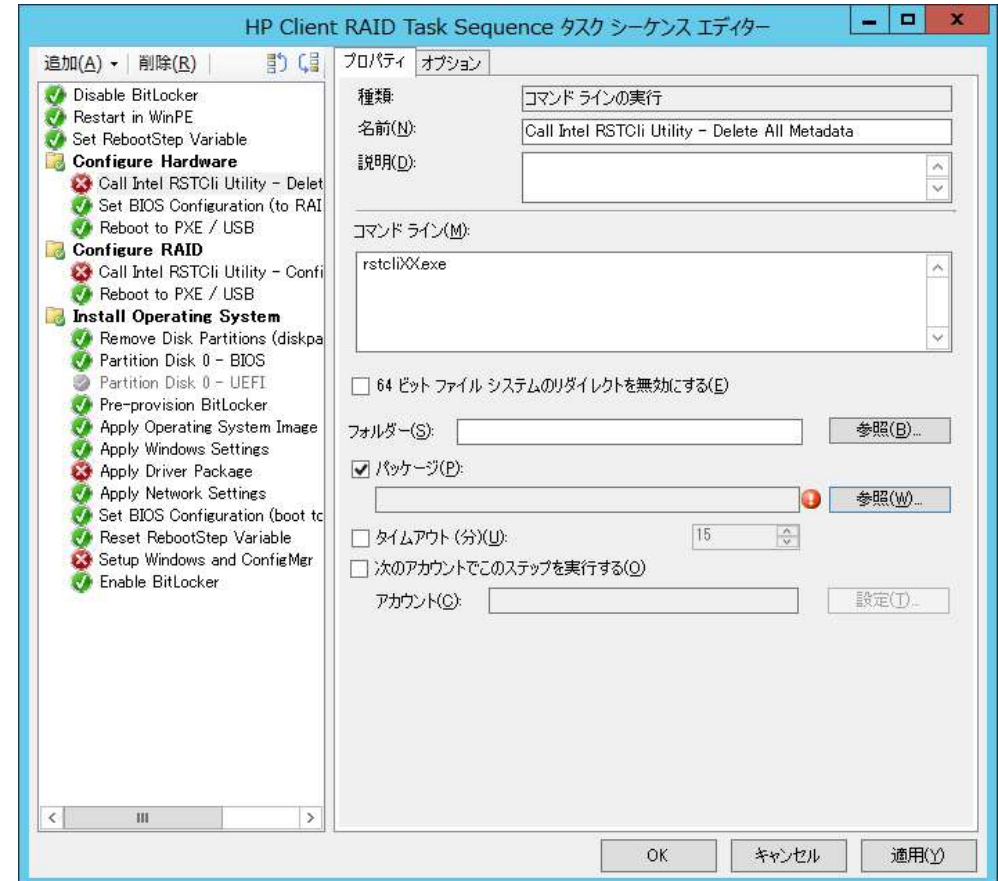
3. ダウンロードしたファイルを解凍します。解凍したフォルダの中にあるX64とx86のZIPファイルをさらに解凍します。
4. 解凍したファイルとフォルダをソフトウェアパッケージのソースフォルダにコピーします。
5. ソースフォルダを参照するソフトウェアパッケージを作成します。



HP Client Task Sequence

タスクシーケンスステップの設定

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. [Call Intel RSTCli Command Line Utility – Delete All Metadata]のステップを選択します。このステップではIntel RSTコマンドラインツールを使用して既存のディスクのメタデータを削除します。



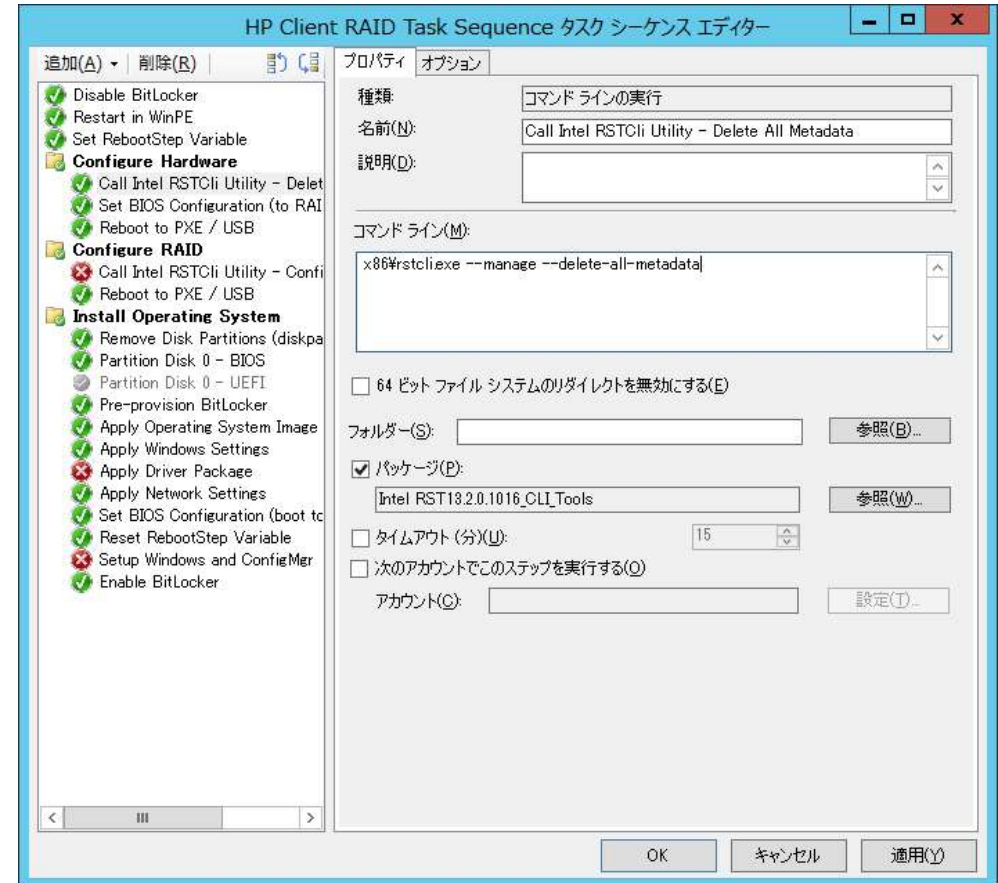
HP Client Task Sequence

3. パッケージの[参照]ボタンをクリックして、前の手順で作成したIntel RSTコマンドラインツールのパッケージを選択します。
4. コマンドラインを実際の環境に合わせて書き換えます。コマンドラインツールのドキュメントを参照してください。

コマンドラインの例

x86¥rstcli.exe -manage -delete-all-metadata

このコマンドライン例の、x86¥rstcli.exeはパッケージのソースフォルダーからの相対パスです。
X64のブートイメージを使用する場合、この例ではx64¥rstcli64.exeになります。



HP Client Task Sequence

3. [Set BIOS Configuration (to RAID mode)]のステップを選択します。このステップではBIOS設定でRAIDモードを有効にします。

以下の内容を含むBIOS設定 (REPSET) ファイルを使用してBIOS Config Utility(BCU)を実行します。

Configure Storage Controller for RAID

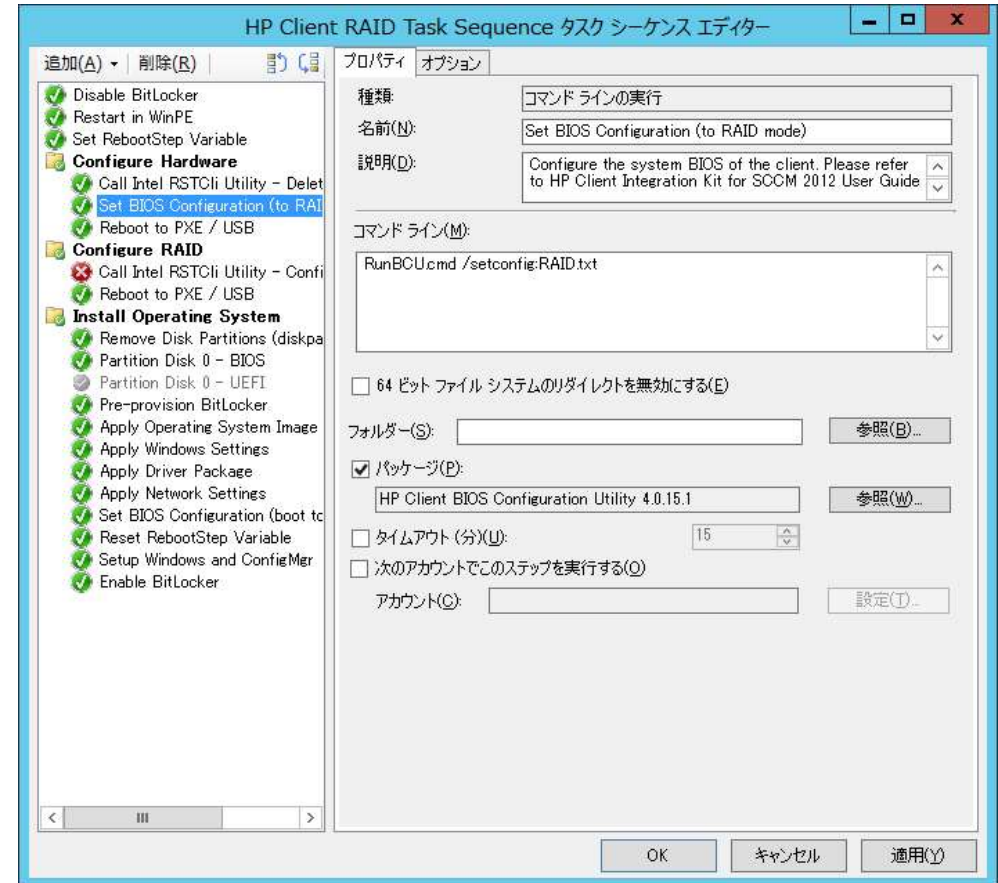
Disable

*Enable

以下はBIOS設定ファイル名をRAID.txtとしてBCUのソースフォルダに置いてある場合のコマンドラインです。

RunBCU.cmd /setconfig:"RAID.txt

詳細はBIOS設定ファイルの追加および編集をご参照ください。



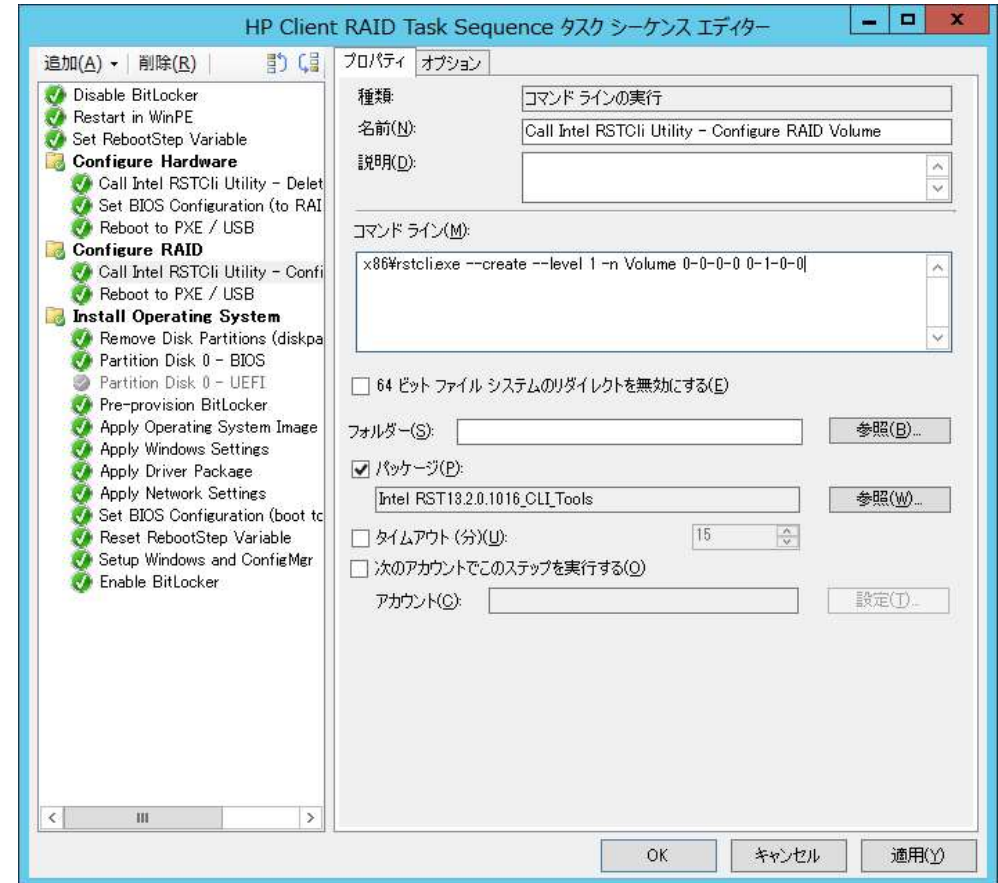
HP Client Task Sequence

- [Call Intel RSTcli Command Line Utility – Configure RAID Volume]のステップを選択します。このステップではIntel RSTコマンドラインツールを使用してRAIDボリュームを作成します。
- パッケージの[参照]ボタンをクリックして、前の手順で作成したIntel RSTコマンドラインツールのパッケージを選択します。
- コマンドラインを実際の環境に合わせて書き換えます。コマンドラインツールのドキュメントを参照してください。

コマンドラインの例

```
x86¥rstcli.exe --create --level 1 --n Volume 0-0-0-0 0-1-0-0
```

このコマンドライン例の、x86¥rstcli.exeはパッケージのソースフォルダーからの相対パスです。X64のブートイメージを使用する場合、この例ではx64¥rstcli64.exeになります。



HP Client Task Sequence

7. デプロイメントの対象OSに応じて以下のステップを設定します。

- Remove Disk Partitions(diskpart clean)ーこのステップの設定は不要です。タスクシーケンスが適切に実行されるにはネットワーク上のコンテンツディレクトリにアクセスできるように設定されている必要があります。詳細は「Allowing access to deployment content」を参照してください。このステップが不要な場合はステップを無効にしてください。
- Format and Partition Diskーディスクを必要に応じてフォーマットおよびパーティション化するための適切な手順を有効にします。たとえば、UEFIまたはUEFI Hybrid（CSMを使用）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を無効にします。
- Apply Driver Packagesーデプロイメント対象のOSイメージに追加するHPドライバーパックを選択します。
- Apply Network Settingsーデプロイメント対象をワークグループにするかドメインに参加するかを選択し、必要に応じてActive Directoryドメインのアカウント情報を入力します。

追加のタスクシーケンスステップを参照し、必要に応じて追加およびパラメータを設定します。

8. すべてのタスクシーケンスステップの設定が完了したら[OK]または[適用]をクリックして変更を保存します。

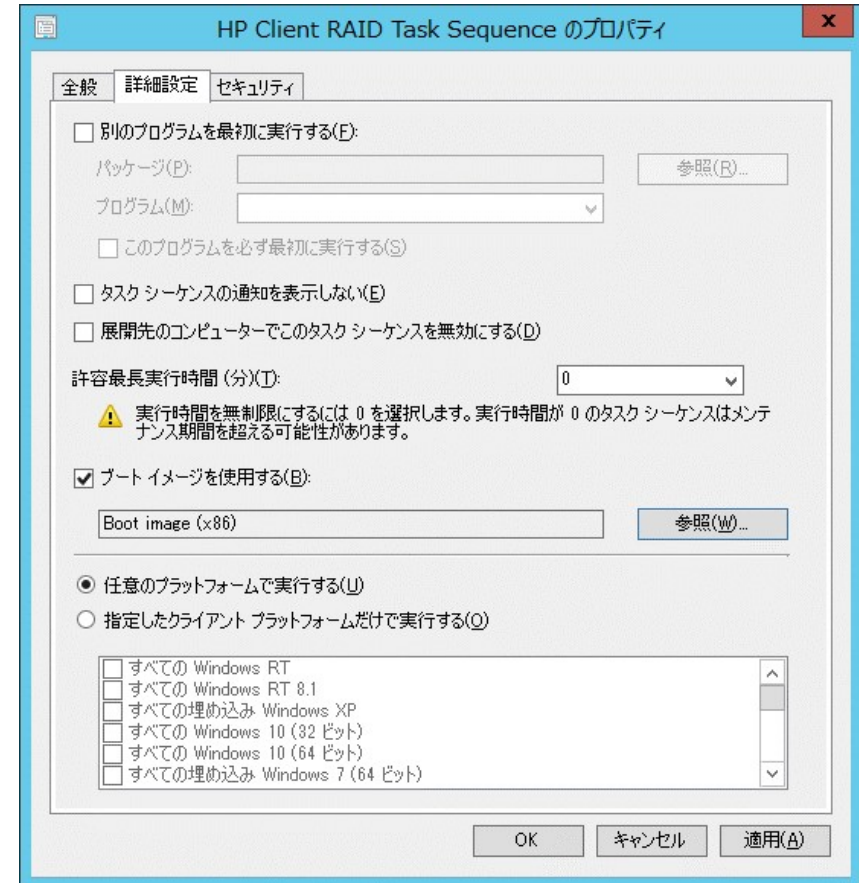
HP Client Task Sequence

ブートイメージの割り当て

1. 対象の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。
4. [OK]をクリックします。

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。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。



HP Client Task Sequence

デプロイメントコンテンツへのアクセス許可設定

HP MIKタスクシーケンスのRemove Disk Partitions(diskpart clean)ステップはネットワークから直接実行する必要があります。そのためには、ブートイメージを含むタスクシーケンスのすべてのパッケージとコンテンツが以下のように設定されている必要があります。

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。

HP Client Task Sequence

タスクシーケンスの実行のフロー

タスクシーケンスは次の3つのタスク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変数を使用して、PXE / USB経由で複数回再起動したときの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、RebootStep変数の設定タスクは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りますので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の値が3であることを確認します。この条件が満たされると、3番目のステップ群が実行されます。

タスクシーケンスの終了時に、Reset RebootStep VariableタスクはRebootStepを0にリセットします。

HP Client Task Sequence

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で再起動してタスクシーケンスを展開するときは、配布ポイント画面で、実行中のタスクシーケンスによって必要になったときに配布ポイントから配布コンテンツから直接コンテンツにアクセスするように展開オプションを設定します。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[利用可能]としてデプロイされ、[必須]としてデプロイされていない場合は、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。
- このステップが正常に動作するには、ターゲット・クライアント・システムにリブート用の適切なブート順序が設定されている必要があります。（つまり、PXE経由でブートする場合、PXE NICはブート順序内の他のブートデバイスの前にある必要があります）。ターゲット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アドバタイズメントを消去します
 - 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。

HP Client Task Sequence

- 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RebootStep変数の値をクリアまたはリセットが必要になる場合があります。
 - A) ターゲット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、削除ボタンを選択します。

本書の取り扱いについて

- 本書は、株式会社日本HPが販売する製品を検討されているお客様が実際のご利用方法に合わせた設定を行う際に役立つ手順の一例を示すものです。いかなる場合においても本書の通りになる事を保証するものではありません。
- 本書の内容は、将来予告なしに変更されることがあります。HP製品およびサービスに対する保証については、該当製品およびサービス保証規定書に記載されています。本書のいかなる内容も、新たな保証を追加するものではありません。本書の内容につきましては万全を期しておりますが、本書中の技術的あるいは校正上の誤り、省略に対して責任を負いかねますのでご了承ください。
- この文書の著作権は株式会社日本HPに帰属します。株式会社日本HPの許可なく一部または全体の複製・転載・編集等を行うことや、許可されていない第三者への開示等の行為全てを禁止します。
- 本文中使用される企業名、製品名、商標などはそれを保持する企業・団体に帰属します。





keep reinventing