



ソフトウェア イメージの管理

- [イメージリポジトリについて \(1 ページ\)](#)
- [ソフトウェア イメージの整合性検証 \(2 ページ\)](#)
- [ソフトウェア イメージの表示 \(2 ページ\)](#)
- [推奨されるソフトウェア イメージの使用 \(3 ページ\)](#)
- [ソフトウェア イメージのインポート \(3 ページ\)](#)
- [デバイスファミリへのソフトウェア イメージの割り当て \(4 ページ\)](#)
- [デバイスのソフトウェア イメージをインストール モードでアップロード \(5 ページ\)](#)
- [ゴールデン ソフトウェアのイメージについて \(6 ページ\)](#)
- [ゴールデン ソフトウェア イメージの指定 \(6 ページ\)](#)
- [ソフトウェア イメージのプロビジョニング \(7 ページ\)](#)

イメージ リポジトリについて

Cisco DNA Center は、ネットワークにあるデバイスのすべてのソフトウェアイメージとソフトウェア メンテナンス アップデート (SMU)、サブパッケージ、ROMMON イメージなどを保存します。イメージリポジトリには次の機能があります。

- **イメージリポジトリ**：Cisco DNA Center はイメージタイプとバージョンに応じて、固有のソフトウェアイメージをすべて保存します。ユーザはソフトウェアイメージの表示、インポート、および削除ができます。
- **プロビジョニング**：ソフトウェアイメージをネットワーク内のデバイスにプッシュできます。

イメージリポジトリ機能を使用する前に、Cisco Catalyst 3000、4000、および 6000 などの古いデバイスで Transport Layer Security (TLS) プロトコルを有効にする必要があります。システムアップグレード後は、TLS を再度有効にする必要があります。詳細については、『[Cisco DNA Center 管理者ガイド](#)』[英語]の「Cisco DNA Center のセキュリティの構成」を参照してください。

ソフトウェアイメージの整合性検証

整合性検証アプリケーションでは、デバイスの感染を示す予期しない変更や無効な値がないか、Cisco DNA Centerに格納されたソフトウェアイメージをモニタします。インポートプロセス中に、システムは、インポートしているイメージのソフトウェアおよびハードウェアプラットフォームのチェックサム値と、既知の適正な値（Known Good Values、KGV）ファイルのプラットフォームで識別されたチェックサム値を比較して、2つの値が一致するようにして、イメージの整合性を判断します。

整合性検証アプリケーションで現在のKGVファイルを使用して選択したソフトウェアイメージを検証できない場合は、[Image Repository] ウィンドウにメッセージが表示されます。整合性検証アプリケーションおよびKGVファイルのインポートの詳細については、[Cisco Digital Network Architecture Center 管理者ガイド \[英語\]](#) を参照してください。

ソフトウェアイメージの表示

ディスカバリを実行するか、手動でデバイスを追加した後、Cisco DNA Center は、デバイスのソフトウェアイメージ、SMU、およびサブパッケージに関する情報を自動的に保存します。

ステップ 1 Cisco DNA Center のホームページで、[Design] > [Image Repository] を選択します。 >

ソフトウェアイメージは、デバイスタイプに基づいて編成され、表示されます。デフォルトでは、物理デバイス用のソフトウェアイメージが表示されます。仮想デバイスのソフトウェアイメージを表示するには、[Virtual] タブに切り替えます。

ステップ 2 [Image Name] 列で、下向き矢印をクリックすると、指定されたデバイスタイプファミリーのすべてのソフトウェアイメージを表示できます。[イメージを使用 (Using Image)] 列は、[イメージ名 (Image Name)] フィールドで示された特定のイメージを使用しているデバイス数を示します。番号のリンクをクリックすると、イメージを使用しているデバイスを表示できます。

ステップ 3 [Version] 列で、[Add On] リンクをクリックすると、適用可能な [SMUs]、[Subpackages]、[ROMMON]、[APSP]、および基本イメージの [APDP] アップグレードが表示されます。

サブパッケージは、既存の基本イメージに追加できる追加の機能です。ここには、イメージファミリーと基本イメージのバージョンに一致するサブパッケージバージョンが表示されます。

AP サービスパック (APSP) と AP デバイスパック (APDP) は、ワイヤレスコントローラに関連付けられた AP をアップグレードするためのイメージです。

- 新しい AP ハードウェアモデルが導入されると、既存のワイヤレスネットワークへの接続に APDP が使用されます。
- 関連付けられた AP の場合、重要な AP バグ修正が APSP によって適用されます。

(注) いずれかの SMU をゴールデンとしてタグ付けすると、基本イメージがインストールされたときに、それが自動的に有効化されます。


サブパッケージはゴールデンとしてタグ付けすることはできません。

ROMMON のアップグレードでは、cisco.com の設定が必須です。デバイスが追加されると、該当するデバイスの最新の ROMMON の詳細が cisco.com から取得されます。また、基本イメージのインポートまたは基本イメージのタグ付けがある場合、ROMMON イメージが cisco.com から自動的にダウンロードされます。

ステップ 4 [Device Role] 列で、これが「ゴールデン」ソフトウェアイメージであることを示すデバイスロールを選択します。詳細については、[ゴールデンソフトウェアのイメージについて \(6 ページ\)](#) および [ゴールデンソフトウェアイメージの指定 \(6 ページ\)](#) を参照してください。

推奨されるソフトウェアイメージの使用

Cisco DNA Center は、管理しているデバイスの Cisco 推奨のソフトウェアイメージを表示します。ユーザーはそこから選択できます。

ステップ 1 Cisco DNA Center のホーム ページで、 > [システム設定 (System Settings)] > [設定 (Settings)] > [Cisco クレデンシャル (Cisco Credentials)] の順に選択し、Cisco.com へ接続するための正しいクレデンシャルが入力されていることを確認します。

ステップ 2 [Design] > [Image Repository] を選択します。

Cisco DNA Center は、デバイス タイプに従って Cisco 推奨のソフトウェアイメージを表示します。

ステップ 3 推奨のイメージをゴールデンとして指定します。詳細については、「[ゴールデンソフトウェアイメージの指定 \(6 ページ\)](#)」を参照してください。

Cisco 推奨のイメージをゴールデンとして指定すると、Cisco DNA Center はそのイメージを cisco.com から自動的にダウンロードします。

ステップ 4 推奨のソフトウェアイメージをネットワーク内のデバイスにプッシュします。詳細については、「[ソフトウェアイメージのプロビジョニング \(7 ページ\)](#)」を参照してください。

ソフトウェアイメージのインポート

ローカルコンピュータまたは URL から、ソフトウェアイメージおよびソフトウェアイメージ更新プログラムをインポートできます。

FTP を使用して FTP サーバからイメージをインポートする場合は、FTP 標準を使用します。

```
ftp://username:password@ip_or_hostname/path
```

-
- ステップ 1** Cisco DNA Center のホームページから、**[Design] > [Image Repository]**を選択します。
- ステップ 2** **[Import]** をクリックします。
- ステップ 3** **[Choose File]** をクリックして、ローカルに保存されているソフトウェアイメージまたはソフトウェアイメージの更新に移動します。または、ソフトウェアイメージのインポート元またはソフトウェアイメージの更新元となる HTTP または FTP を指定するイメージ URL を入力します。
- ステップ 4** インポートするイメージがサードパーティ（シスコ以外）ベンダー向けの場合、**[Source]** で **[Third Party]** を選択します。**[Application Type]** を選択し、デバイスの **[Family]** を示し、**[Vendor]** を特定します。
- ステップ 5** **[Import]** をクリックします。
- ウィンドウにインポートの進行が表示されます。
- ステップ 6** **[タスクの表示 (Show Tasks)]** をクリックして、イメージが正常にインポートされたことを確認します。
- SMU をインポートした場合、Cisco DNA Center は自動的に SMU を適切なソフトウェアイメージに適用し、対応するソフトウェアイメージの下に **[アドオン (Add-On)]** リンクが表示されます。
- ステップ 7** **[アドオン (Add-On)]** リンクをクリックすると、SMU が表示されます。
- ステップ 8** **[Device Role]** フィールドで、この SMU をゴールデンとしてマークするロールを選択します。[ゴールデンソフトウェアイメージの指定 \(6 ページ\)](#) を参照してください。
- SMU をゴールデンとしてマークするには、事前に対応するソフトウェアイメージをゴールデンとしてマークする必要があります。
-

デバイスファミリへのソフトウェアイメージの割り当て

ソフトウェアイメージをインポート後、使用可能なデバイスファミリに割り当てることができます。インポートしたイメージは、いつでも複数のデバイスに割り当てることができます。

インポートしたソフトウェアイメージをデバイスファミリに割り当てするには、次の手順を実行します。

-
- ステップ 1** Cisco DNA Center のホームページで、**[Design] > [Image Repository]** を選択します。
- ステップ 2** **[Imported Images]** をクリックします。
- ステップ 3** **[Assign]** リンクをクリックします。
- ステップ 4** **[Assign Device Family]** ウィンドウで、このイメージを割り当てるデバイスファミリを選択します。
- ステップ 5** **[Assign]** をクリックします。

ソフトウェアイメージがデバイスファミリに割り当てられ、そのイメージを使用しているデバイスの数が **[Using Image]** 列に表示されます。イメージを割り当てたら、そのイメージをゴールデンイメージとしてマークできます。「[ゴールデンソフトウェアイメージの指定](#)」を参照してください。

(注) PnP デバイスでは、デバイスが使用可能になる前に、ソフトウェアイメージをインポートしてデバイスファミリに割り当てることができます。また、イメージをゴールデンイメージとしてマークすることもできます。デバイスがインベントリで使用可能になると、そのデバイスファミリに割り当てられたイメージが、そのデバイスファミリの新しく追加されたデバイスに自動的に割り当てられます。

イメージがインポートされ、Cisco DNA Center に cisco.com ログイン情報が追加されると、Cisco DNA Center はイメージに適用可能なデバイスファミリのリストを提供します。リストから、必要なデバイスファミリを選択できます。

イメージが cisco.com で使用できない場合、またはログイン情報が Cisco DNA Center に追加されていない場合は、そのイメージに適したデバイスファミリを設計する必要があります。

デバイスのソフトウェアイメージをインストールモードでアップロード

[イメージリポジトリ (Image Repository)] ページでは、ソフトウェアイメージがインストールモードの状態として表示されることがあります。デバイスがインストールモードの場合、Cisco DNA Center は、ソフトウェアイメージをデバイスから直接アップロードできません。デバイスがインストールモードのときは、次の手順で示すように、最初に手動でソフトウェアイメージを Cisco DNA Center リポジトリへアップロードしてから、イメージをゴールデンとしてマーキングします。

-
- ステップ 1 Cisco DNA Center のホーム ページで、[設計 (Design)] > [イメージリポジトリ (Image Repository)] を選択します。
 - ステップ 2 [Image Name] カラムで、[Install Mode] で実行中のデバイスのソフトウェアイメージを検索します。
 - ステップ 3 [インポート (Import)] をクリックして、インストールモードであるイメージのバイナリソフトウェアイメージファイルをアップロードします。
 - ステップ 4 [ファイルの選択 (Choose File)] をクリックしてローカルに保存されているソフトウェアイメージへ移動するか、または [イメージの URL を入力 (Enter image URL)] でソフトウェアイメージのインポート元となる HTTP または FTP を指定します。
 - ステップ 5 [Import] をクリックします。
ウィンドウにインポートの進行が表示されます。
 - ステップ 6 [タスクの表示 (Show Tasks)] をクリックして、インポートしたソフトウェアイメージが、正常にインポートされ、Cisco DNA Center リポジトリに追加されたことを示す緑色であることを確認します。
 - ステップ 7 [Refresh] をクリックします。

[イメージリポジトリ (Image Repository)] ウィンドウを更新します。Cisco DNA Center にソフトウェアイメージが表示され、[ゴールデンイメージ (Golden Image)] および [デバイスロール (Device Role)] 列がグレー表示ではなくなります。

ゴールデンソフトウェアのイメージについて

Cisco DNA Center では、ソフトウェアイメージと SMU をゴールデンとして指定できます。ゴールデンソフトウェアイメージや SMU は、特定のデバイスタイプのコンプライアンス要件を満たす検証済みのイメージです。ソフトウェアイメージや SMU をゴールデンとして指定すると、反復的な設定変更の必要がなくなることで時間を節約でき、デバイス間の一貫性を確保できます。標準化されたイメージを作成するために、イメージと対応する SMU をゴールデンとして指定できます。特定のデバイスロールのゴールデンイメージを指定することもできます。たとえば、Cisco 4431 統合サービスルータ デバイス ファミリのイメージがある場合、アクセスロールだけを持つ Cisco 4431 デバイスに対するゴールデンイメージを追加で指定できます。

対応するイメージもゴールデンとしてマークされていない限り、SMU をゴールデンとしてマークすることはできません。

ゴールデンソフトウェアイメージの指定

デバイスファミリまたは特定のデバイスロールに対するゴールデンソフトウェアイメージを指定することができます。デバイスロールは、ネットワークにおける役目と配置に従って、デバイスを識別およびグループ分けするために使用されます。

ステップ 1 Cisco DNA Center のホーム ページで、[設計 (Design)] > [イメージリポジトリ (Image Repository)] を選択します。

デバイスタイプに従ってソフトウェアイメージが表示されます。

ステップ 2 [ファミリ (Family)] 列で、ゴールデンイメージを指定するデバイスファミリを選択します。

ステップ 3 [イメージ名 (Image Name)] 列で、ゴールデンイメージとして指定するソフトウェアイメージを選択します。

ステップ 4 [デバイスロール (Device Role)] 列で、ゴールデンイメージを指定するデバイスロールを選択します。同じデバイスファミリのデバイスを所有していたとしても、各デバイスロールに異なるゴールデンイメージを指定することができます。物理イメージのデバイスロールのみ選択できます。仮想イメージは選択できないことに注意してください。

ゴールデンイメージとして指定したソフトウェアイメージが Cisco DNA Center リポジトリにアップロードされていない場合は、このプロセスには多少時間がかかります。[イメージリポジトリ (Image Repository)] ページの [アクション (Action)] 列で、ゴミ箱アイコンがグレー表示されている場合、イメージはまだ Cisco DNA Center リポジトリにアップロードされていません。Cisco DNA Center では最初にソフトウェアイメー

ジをリポジトリにアップロードする必要があります。その後、イメージをゴールデンとしてマークすることができます。ソフトウェアイメージが **[アクション (Action)]** 列のアクティブなごみ箱アイコンで示された Cisco DNA Center リポジトリに既にアップロードされている場合、ゴールデンイメージを特定するプロセスはより速く完了します。

ソフトウェアイメージのプロビジョニング

ソフトウェアイメージをネットワーク内のデバイスにプッシュできます。ソフトウェアイメージをデバイスにプッシュする前に、Cisco DNA Center はデバイス管理ステータスの確認、ディスク容量の確認など、デバイスのアップグレード準備の事前チェックを実行します。事前チェックに失敗した場合は、ソフトウェアイメージの更新を実行できません。デバイスのソフトウェアイメージをアップグレード後、Cisco DNA Center は CPU 使用率、ルート サマリなどを確認し、イメージのアップグレード後にネットワークの状態が変更されていないことを保証します。



(注) 複数のデバイスに対して事前チェックを実行できます。

Cisco DNA Center は、各デバイスのソフトウェアイメージを、その固有のデバイス タイプに対してゴールデンと指定したイメージと比較します。デバイスのソフトウェアイメージとゴールデンイメージに違いがある場合、Cisco DNA Center はデバイスのソフトウェアイメージを無効とします。これらのデバイスに対するアップグレード準備の事前チェックがトリガーされます。すべての事前チェックをクリアしたら、新しいイメージをデバイスに配信 (コピー) し、有効化 (新しいイメージを実行中のイメージにすることが) できます。新しいイメージの有効化には、デバイスの再起動が必要です。再起動によって現在のネットワークアクティビティが中断される可能性があるため、後でプロセスをスケジュールすることができます。

そのデバイスタイプにゴールデンイメージを指定していない場合、そのデバイスのイメージは更新できません。 [ゴールデンソフトウェアイメージの指定 \(6 ページ\)](#) を参照してください。

ステップ 1 Cisco DNA Center ホームページで、**[Provision]** をクリックします。

ステップ 2 [Focus] ドロップダウンリストから **[Software Images]** を選択します。イメージをアップグレードするデバイスを選択します。

(注) デバイスの事前チェックに成功したら、**[OS Image]** カラムの **[Outdated]** リンクに緑色のチェックマークが付きます。デバイスのアップグレードを準備するための事前チェックでいずれかに失敗した場合、**[Outdated]** リンクのマークが赤色に変わり、そのデバイスの OS イメージを更新できなくなります。先に進む前に **[Outdated]** リンクをクリックし、エラーを修正します。

[デバイスのアップグレードの準備の事前チェック リスト \(8 ページ\)](#) を参照してください。

デバイスのアップグレードの準備の事前チェック リスト

ステップ 3 [Actions] ドロップダウンリストから [Software Image] > [Update Image] を選択し、以下を実行します。 >

- a) [Distribute] : [Now] をクリックしてすぐに配信を開始するか、[Later] をクリックして特定の時間に配信のスケジュールを設定します。

(注) 選択したデバイスに既にイメージが配信されている場合、配信プロセスはスキップされ、イメージの有効化のみ可能になります。

- b) [次へ (Next)] をクリックします。

- c) [Activate] : [Now] をクリックして直ちに有効化を開始するか、[Later] をクリックして特定の時間に有効化をスケジュールします。

(注) 今は配信プロセスのみを実行する場合、この手順をスキップすることができます。

- d) (オプション) [Schedule Activation after Distribution is completed] チェックボックスをオンにします。

- e) [確認 (Confirm)] : [確認 (Confirm)] をクリックして、更新を確認します。

更新のステータスは、[OS の更新ステータス (OS Update Status)] 列で確認できます。このカラムが表示されない場合は、 をクリックして、[OS Update Status] を選択します。

ステップ 4 (オプション) イメージのアップグレードの進行状況を表示するには、[アップグレードステータス (Upgrade Status)] をクリックします。

(注) Cisco DNA Center と別のファブリック デバイス間にエッジルータなどのデバイスがある場合、ソフトウェアイメージが他のデバイスにプロビジョニングされている間に、この間にあるデバイスがリロードすると、ソフトウェア更新プロセスが失敗する可能性があります。

デバイスのアップグレードの準備の事前チェック リスト

事前チェック	説明
ファイル転送のチェック	デバイスが SCP および HTTPS を介して到達可能かどうかチェックします。
NTP クロックのチェック	デバイスの時間と Cisco DNA Center の時間を比較して、Cisco DNA Center 証明書が正常にインストールされていることを確認します。
フラッシュのチェック	更新に十分なディスク容量があるかどうか確認します。十分なディスク容量がない場合、警告またはエラー メッセージが返されます。自動フラッシュクリーンアップでサポートされるデバイスとファイルの削除方法については、 Auto Flash Cleanup を参照してください。
設定レジスタのチェック	設定レジスタの値を確認します。
暗号化 RSA チェック	RSA 証明書がインストールされているかどうかチェックします。
暗号化 TLS のチェック	デバイスが TLS 1.2 をサポートしているかどうかチェックします。

事前チェック	説明
IP ドメイン名のチェック	ドメイン名が設定されているかどうかチェックします。
スタートアップ設定のチェック	このデバイス用のスタートアップ設定があるかどうかを確認します。
NFVIS Flash チェック	NFVIS デバイスでゴールデンイメージをアップグレードする準備ができているかどうかを確認します。
サービス契約のチェック	デバイスに有効なライセンスがあるかどうかを確認します。

Auto Flash Cleanup

デバイスのアップグレード準備の事前チェックの間、フラッシュのチェックにより、新しいイメージをコピーするための十分なスペースがデバイスにあるかどうかを確認されます。スペースが十分でない場合：

- **自動フラッシュクリーンアップをサポートしているデバイスの場合**：フラッシュのチェックが失敗し、警告メッセージが表示されます。このようなデバイスの場合、十分なスペースを作成するために、イメージの配信プロセス中に自動クリーンアッププロセスが試行されます。自動フラッシュクリーンアップの一環として、Cisco DNA Center は未使用の .bin、.pkg、および .conf ファイルを特定し、デバイスに十分な空き領域ができるまでそれらのファイルの削除を繰り返します。イメージの配信はフラッシュクリーンアップ後に試行されます。削除されたファイルは [システム (System)] > [監査ログ (Audit Logs)] で確認できます。



(注) 自動フラッシュクリーンアップは、Nexus スイッチとワイヤレスコントローラを除くすべてのデバイスでサポートされています。

- **自動フラッシュクリーンアップをサポートしていないデバイスの場合**：フラッシュのチェックが失敗し、エラーメッセージが表示されます。イメージのアップグレードを開始する前に、デバイスのフラッシュからファイルを削除して、必要なスペースを作成できます。

