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

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。ユーザー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 イメージをモニターします。システムは、インポートプロセス中に、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、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 つの値の一致を確認することで、イメージの整合性を決定します。

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 GUI で [Menu] アイコン（☰）をクリックして選択します**[Design]** > **[Image Repository]**。

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。

（注） cisco.com のログイン情報が設定されていない場合、警告アラートが表示されます。

ステップ 2 [Family] 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のすべてのソフトウェアイメージを表示できます。[Device(s)] 列には、[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が示されます。デバイスの番号をクリックすると、そのイメージを使用しているデバイスが表示されます。

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シスコ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。

（注） シスコが推奨する最新のソフトウェアイメージのみをダウンロードできます。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（≡）をクリックして選択します**[System]** > **[Settings]** > **[Cisco.com Credentials]** の順に選択します。

ステップ 2 cisco.com に接続するための正しいログイン情報が入力されていることを確認します。

ステップ 3 Cisco DNA Center GUI で [Menu] アイコン（≡）をクリックして選択します**[Design]** > **[Image Repository]**。

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 4 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。

ステップ 5 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 （9 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。

インポートされたイメージは、特定のデバイスファミリに存在するさまざまなスーパーバイザに基づいて分類されます。異なるスーパーバイザによる分類では、Cisco Catalyst 9400 シリーズ ファミリのみがサポートされます。

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 GUI で [Menu] アイコン（☰）をクリックして選択します**[Design]** > **[Image Repository]**。

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] を選択して、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 **[Add-On]** リンクが表示されます。

ステップ 7 **[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している必要があります。

（注） Cisco DNA Center では、FMC によって管理される FTD デバイスのソフトウェアイメージをインポートすることはできません。インベントリに追加した FMC が「Managed」状態になると、FMC に存在するソフトウェアイメージがイメージリポジトリに表示され、デバイスファミリに基づいて分類されます。

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した後、使用可能なデバイスファミリに割り当てたり割り当てを解除したりできます。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るには、次の手順を実行します。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Design]** > **[Image Repository]**。

ステップ 2 [Imported Images] をクリックします。

ステップ 3 対応するイメージ名の行の [Assign] をクリックします。

ステップ 4 [Assign Device Family] ウィンドウで、[Device Series from Cisco.com] または [All Device Series] を選択し、イメージのマッピング先の [Assign] リンクをクリックします。

注：Cisco.com ログイン情報が設定されていない場合は、**[System]** > **[Settings]** > **[Cisco.com Credentials]** の順に選択して、ログイン情報を指定します。

ステップ 5 グローバル階層から適切なサイトを選択して [Assign] をクリックし、[Save] をクリックします。

ステップ 6 イメージの割り当てを解除するには、グローバル階層からサイトを選択し、[Action] 列の [Unassign] リンクをクリックします。

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 [Devices(s)] 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。

デバイスファミリがゴールデンイメージとしてマークされている場合、そのイメージをデバイスファミリから削除することはできません。

（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 GUI で [Menu] アイコン（≡）をクリックして選択します**[Design]** > **[Image Repository]**。

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。

[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、[Golden Image] および [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 GUI で [Menu] アイコン（≡）をクリックして選択します**[Design]** > **[Image Repository]**。

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 **[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 **[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 ゴールデンとして指定したソフトウェアイメージが Cisco DNA Center リポジトリにすでにアップロードされている場合は、[Golden Image] 列のスターアイコンをクリックします。

ソフトウェアイメージがゴールデンとしてマークされます。

ステップ 5 ゴールデンとして指定したソフトウェアイメージが Cisco DNA Center リポジトリにまだアップロードされていない場合は、[Golden Image] 列のダウンロードアイコンをクリックします。

この処理には、しばらく時間がかかる場合があります。

（注） デバイスからソフトウェアイメージをインポートすることはできません。

ステップ 6 [Download Image] ダイアログボックスで、次のいずれかを実行します。

- [Mark the image as golden after download] チェックボックスはデフォルトのオンのままにし、[Download] をクリックします。ソフトウェアイメージがダウンロードされ、ゴールデンとしてマークされます。

  （注） Cisco.com のログイン情報が設定されていない場合は、ログイン情報を指定するよう求められます。

  進行中のソフトウェアイメージのダウンロードが [Device Role] 列に表示されます。

  ソフトウェアイメージがダウンロードされ、ゴールデンとして正常にマークされると、スターアイコンが金色に変わります。ソフトウェアイメージのダウンロードが失敗すると、スターアイコンが赤色に変わり、[Please Retry] ステータスが表示されます。

- [Mark the image as golden after download] チェックボックスをオフにし、[Download] をクリックします。ソフトウェアイメージがリポジトリにダウンロードされますが、ゴールデンとはマークされません。

ステップ 7 **[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。

イメージ配信サーバの設定

ソフトウェアイメージを配信するように外部イメージ配信サーバを設定できます。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[System]** > **[Settings]** > **[Device Settings]** > **[Image Distribution Servers]**。

ステップ 2 [Add] をクリックして新しいイメージ配信サーバを追加します。

ステップ 3 サーバ設定値の設定

- [Host]：イメージ配信サーバのホスト名または IP アドレス。
- [Root Location]：ファイル転送用の作業ルートディレクトリ。

  （注） Cisco AireOS コントローラの場合、設定されたパスが 16 文字を超えると、イメージの配信は失敗します。

- [Username]：イメージ配信サーバへのログインに使用される名前。ユーザには、サーバの作業ルートディレクトリに対する読み取り/書き込み権限が必要です。
- [パスワード]：イメージ配信サーバへのログインに使用されるパスワード。
- [ポート番号]：イメージ配信サーバが実行されているポート番号。

ステップ 4 [**Save**] をクリックします。

ステップ 5 イメージ配信サーバの設定を編集するには、次の手順を実行します。

a) 設定を変更するイメージ配信サーバの [Edit] アイコンをクリックします。
b) [Edit] ウィンドウで必要な変更を行います。
c) [Save] をクリックします。

サイトへのイメージ配信サーバの追加

地理的に異なる地域にある SFTP サーバを、サイト、ビルディング、およびフロアに関連付けることができます。ネットワーク階層内のすべてのデバイスは、ネットワークのアップグレードの際、関連付けられたイメージ配信サーバを使用します。

始める前に

イメージ配信サーバを設定する必要があります。『イメージ配信サーバの設定 （7ページ）』を参照してください。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Design]** > **[Network settings]**。

ステップ 2 左ペインで、イメージ配信サーバを関連付けるサイトを選択します。

ステップ 3 [サーバの追加（Add Servers）] をクリックします。

ステップ 4 [Add Servers] ウィンドウで、[Image Distribution] チェックボックスをオンにします。

ステップ 5 [OK] をクリックします。

ステップ 6 [Primary] ドロップダウンリストをクリックし、プライマリとして設定するイメージ配信サーバを選択します。

ステップ 7 [Secondary] ドロップダウンリストをクリックし、セカンダリとして設定するイメージ配信サーバを選択します。

ステップ 8 [Save] をクリックします。

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 GUI で [Menu] アイコン（☰）をクリックして選択します**[Provision]** > **[Devices]** > **[Inventory]**。

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が成功すると、[Software Image] 列の [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、そのデバイスのソフトウェア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」を参照してください。

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

[Image Upgrade] ウィンドウが表示されます。

ステップ 4 [Analyze Selection]：アップグレードするデバイスを選択し、[Next] をクリックします。

ステップ 5 [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。

現在のワークフローで実行する検証ツールを選択し、新しいカスタムチェックを追加するには、次の手順を実行します。

a) 情報アイコンにマウスポインタを合わせると、検証に使用される検証基準と CLI コマンドが表示されます。
b) オンとオフを切り替えるトグルボタンをクリックして、現在のワークフローで実行しない検証ツールをオフにします。
c) 新しいカスタム事前チェックと事後チェックをステージごとに追加するには、次の手順を実行します。

- [Add a New Check] リンクをクリックして、[Add a New Custom Check] ウィンドウを開きます。
- カスタムチェックの名前を [Name] に入力します。
- [When] ドロップダウン矢印をクリックし、必要に応じて事前か事後またはその両方を選択します。
- [Select a Test Device] ドロップダウン矢印をクリックし、カスタムチェックを実行するデバイスを選択します。
- [Open Command Runner] をクリックし、CLI コマンドを入力します。
- [Additional Criteria] 領域を展開します。
- [Operation] ドロップダウン矢印をクリックし、[Distribution] を選択します。
- [Device Series] ドロップダウン矢印をクリックし、カスタムチェックを実行するデバイスシリーズを選択します。
- **[Save]** をクリックします。
- カスタムチェックを編集する場合は、対応する [More] アイコンをクリックし、[Edit] を選択して、必要な変更を行い、[Save] をクリックします。
- カスタムチェックを削除する場合は、対応する [More] アイコンをクリックし、[Delete] を選択して、[Confirm Delete] メッセージで [Delete] をクリックします。

（注）
- 外部イメージ配信サーバをネットワーク階層に関連付けている場合、ネットワーク階層下のすべてのデバイスへのイメージ配信は、イメージ配信サーバから行われます。サイトへのイメージ配信サーバの追加 （8 ページ）を参照してください。
- 選択したデバイスにイメージがすでに配信されている場合は、[Next] をクリックします。
- [SWIM Events for ITSM (ServiceNow)] バンドルが有効になっている場合は、後でイメージを更新（配布およびアクティブ化）する必要があります。イメージを更新するために [Now] をクリックしないでください。ここでイメージを更新する必要がある場合は、まずバンドルとその統合ワークフロー（ServiceNowでのイメージ更新スケジュールの承認）を無効にする必要があります。バンドルにアクセスするには、[Platform] > [Manage] > [Bundles] > [SWIM Events for ITSM（ServiceNow）] の順に選択します。[SWIM Events for ITSM（ServiceNow）] ウィンドウの [Disable] ボタンをクリックします。バンドルとワークフローを無効にするプロセスには数秒かかるため、イメージの更新に進む前に数秒待ちます。

ステップ 6 **[Next]** をクリックします。

ステップ 7 [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。

現在のワークフローで実行する検証ツールを選択し、新しいカスタムチェックを追加するには、次の手順を実行します。

a) 情報アイコンにマウスポインタを合わせると、検証に使用される検証基準と CLI コマンドが表示されます。
b) オンとオフを切り替えるトグルボタンをクリックして、現在のワークフローで実行しない検証ツールをオフにします。
c) 新しいカスタム事前チェックと事後チェックをステージごとに追加するには、次の手順を実行します。

- [Add a New Check] リンクをクリックして、[Add a New Custom Check] ウィンドウを開きます。
- カスタムチェックの名前を [Name] に入力します。
- [When] ドロップダウン矢印をクリックし、必要に応じて事前か事後またはその両方を選択します。
- [Select a Test Device] ドロップダウン矢印をクリックし、カスタムチェックを実行するデバイスを選択します。
- [Open Command Runner] をクリックし、CLI コマンドを入力します。
- [Additional Criteria] 領域を展開します。
- [Operation] ドロップダウン矢印をクリックし、[Activation] を選択します。
- [Device Series] ドロップダウン矢印をクリックし、カスタムチェックを実行するデバイスシリーズを選択します。
- **[Save]** をクリックします。
- カスタムチェックを編集する場合は、対応する [More] アイコンをクリックし、[Edit] を選択して、必要な変更を行い、[Save] をクリックします。
- カスタムチェックを削除する場合は、対応する [More] アイコンをクリックし、[Delete] を選択して、[Confirm Delete] メッセージで [Delete] をクリックします。

ステップ 8 [Next] をクリックします。

ステップ 9 [Summary]：イメージのアップグレード設定を確認します。変更を加える場合は [Back] をクリックし、それ以外の場合は [Submit] をクリックします。

[Actions] ドロップダウンリストから、**[Software Images]** > **[Image Update Status]** の順に選択して、更新ステータスを確認します。

ISSU 互換性マトリクスのインポート

In-Service Software Upgrade（ISSU）は、再起動なしで、またはサービスの中断を最小限に抑えて、デバイス上のイメージをアップグレードするプロセスです。Catalyst スイッチの Cisco IOS XE ISSU 互換性マトリクスの例については、https://software.cisco.com/download/home/286315874/type/286326638/release/17.4.1 を参照してください。ISSU を使用してデバイスをアップグレードする際は、ISSU 互換性マトリクスを Cisco DNA Center にダウンロードしてインポートすることができます。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（≡）をクリックして選択します**[Design]** > **[Image Repository]**。

ステップ 2 [Import] をクリックします。

[Import Image/Add-On] ウィンドウが表示されます。

ステップ 3 ISSU 互換性マトリクスとソフトウェアイメージをインポートするには、次の手順を実行します。

a) [Choose File] をクリックしてソフトウェアイメージを選択するか、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 送信元の URL を入力します。

b) 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] を選択して、デバイスの [Family] を示し、[Vendor] を特定します。

c) [Select ISSU Compatibility Matrix] で [Choose File] をクリックして ISSU 互換性マトリクスファイルを選択します。

d) [インポート（Import）] をクリックします。

ステップ 4 （任意）すでにインポートされているソフトウェアイメージの ISSU 互換性マトリクスをインポートするには、次の手順を実行します。

a) [Select ISSU Compatibility Matrix] で [Choose File] をクリックして ISSU 互換性マトリクスファイルを選択します。

b) [インポート（Import）] をクリックします。

ステップ 5 [Show Tasks] をクリックして ISSU 互換性マトリクスファイルの**インポート**ステータスを表示します。

ISSU を使用したソフトウェアイメージのアップグレード

In-Service Software Upgrade（ISSU）を使用してデバイスをアップグレードすると、再起動する必要がなくなり、サービスの中断が減少します。

始める前に

ISSU を使用してデバイスをアップグレードする前に、ISSU 互換性マトリクスファイルをインポートする必要があります。ISSU 互換性マトリクスのインポート （11 ページ）を参照してください。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Provision]** > **[Devices]** > **[Inventory]**。

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。

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

[Image Upgrade] ウィンドウが表示されます。

ステップ 4 [Analyze Selection] ページで、ISSU アップグレードを有効にします。

a) ISSU でアップグレードするデバイスを選択します。

（注） [To Image] 列を参照して ISSU 検証ステータスを確認します。

- **オレンジ色で表示される ISSU**：選択したイメージに ISSU との互換性がないため、ISSU の検証に失敗しました。
- **灰色で表示される ISSU**：ISSU の検証が成功し、デバイスは ISSU をサポートしています。

b) [ISSU] ドロップダウンリストから [Enable ISSU Upgrade] を選択します。
c) [Next] をクリックします。

ステップ 5 [Distribute] ページから [Now] をクリックして即座にイメージ配信を開始するか、[Later] をクリックして特定の時間に配信をスケジュールします。

現在のワークフローで実行する検証ツールを選択し、新しいカスタムチェックを追加するには、次の手順を実行します。

a) 情報アイコンにカーソルを合わせると、検証に使用される検証基準と CLI コマンドが表示されます。
b) トグルボタンをクリックして、現在のワークフローで実行しない検証ツールをオフにします。
c) （任意）新しいカスタム事前チェックおよび事後チェックを追加するには、次の手順を実行します。
   - [Add a New Check] リンクをクリックして、[Add a New Custom Check] ウィンドウを開きます。
   - カスタムチェックの名前を [Name] に入力します。
   - [When] ドロップダウンリストをクリックし、必要に応じて事前か事後またはその両方を選択します。
   - [Select a Test Device] ドロップダウンリストをクリックし、カスタムチェックを実行するデバイスを選択します。
   - [Open Command Runner] をクリックし、CLI コマンドを入力します。
   - [Additional Criteria] 領域を展開します。
   - [Operation] ドロップダウン矢印をクリックし、[Distribution] を選択します。
   - [Device Series] ドロップダウン矢印をクリックし、カスタムチェックを実行するデバイスシリーズを選択します。
   - **[Save]** をクリックします。
   - カスタムチェックを編集する場合は、対応する [More] アイコンをクリックし、[Edit] を選択して、必要な変更を行い、[Save] をクリックします。
   - カスタムチェックを削除する場合は、対応する [More] アイコンをクリックし、[Delete] を選択して、[Confirm Delete] メッセージで [Delete] をクリックします。

（注）
- ネットワーク階層に関連付けられている外部イメージ配信サーバーは、ネットワーク階層内のすべてのデバイスにイメージを配信します。サイトへのイメージ配信サーバの追加（8 ページ）を参照してください。
- 選択したデバイスにイメージがすでに配信されている場合は、[Next] をクリックします。
- [SWIM Events for ITSM (ServiceNow)] バンドルが有効になっている場合は、後でイメージを更新（配布およびアクティブ化）する必要があります。イメージを更新するために [Now] をクリックしないでください。

  ここでイメージを更新する必要がある場合は、まずバンドルとその統合ワークフロー（ServiceNow でのイメージ更新スケジュールの承認）を無効にする必要があります。バンドルにアクセスするには、[Platform] > [Manage] > [Bundles] > [SWIM Events for ITSM（ServiceNow）] の順に選択します。[SWIM Events for ITSM（ServiceNow）] ウィンドウの [Disable] ボタンをクリックします。バンドルとワークフローを無効にするプロセスには数秒かかるため、イメージの更新に進む前に数秒待ちます。

ステップ 6 **[Next]** をクリックします。

ステップ 7 [Activate] ページから、[Now] をクリックして即座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。

現在のワークフローで実行する検証ツールを選択し、新しいカスタムチェックを追加するには、次の手順を実行します。

a) 情報アイコンにカーソルを合わせると、検証に使用される検証基準と CLI コマンドが表示されます。
b) トグルボタンをクリックして、現在のワークフローで実行しない検証ツールをオフにします。
c) （任意）新しいカスタム事前チェックおよび事後チェックを追加するには、次の手順を実行します。
   - [Add a New Check] リンクをクリックして、[Add a New Custom Check] ウィンドウを開きます。
   - カスタムチェックの名前を [Name] に入力します。
   - [When] ドロップダウンリストをクリックし、必要に応じて事前か事後またはその両方を選択します。
   - [Select a Test Device] ドロップダウンリストをクリックし、カスタムチェックを実行するデバイスを選択します。
   - [Open Command Runner] をクリックし、CLI コマンドを入力します。
   - [Additional Criteria] 領域を展開します。
   - [Operation] ドロップダウンリストをクリックし、[Activation] を選択します。
   - [Device Series] ドロップダウンリストをクリックし、カスタムチェックを実行するデバイスシリーズを選択します。
   - **[Save]** をクリックします。
   - カスタムチェックを編集する場合は、対応する [More] アイコンをクリックし、[Edit] を選択して、必要な変更を行い、[Save] をクリックします。

- カスタムチェックを削除する場合は、対応する [More] アイコンをクリックし、[Delete] を選択して、[Confirm Delete] メッセージで [Delete] をクリックします。

ステップ 8 [Next] をクリックします。

ステップ 9 [Summary] ページから、イメージのアップグレード設定を確認します。変更を加える場合は [Back] をクリックし、それ以外の場合は [Submit] をクリックします。

[Actions] ドロップダウンリストから、**[Software Images]** > **[Image Update Status]** の順に選択して、更新ステータスを確認します。

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

事前チェック	説明
ファイル転送のチェック	HTTPS と SCP を通じてデバイスに到達できるかどうかをチェックします。 プロトコルのデフォルトの順序は、HTTPSが先で、SCP はその後です。
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、自動フラッシュクリーンアップ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。
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 のチェック	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。

イメージ更新ステータスの表示

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Provision]** > **[Devices]** > **[Inventory]**。

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。

ステップ 3 [Actions] ドロップダウンリストから、**[Software Images]** > **[Image Update Status]** の順に選択します。

デフォルトでは、[Image Update Status] ウィンドウに最近のすべてのイメージ更新タスクが表示されます。下矢印をクリックし、[Failed]、[In-progress]、[Success] のいずれかのタスクを選択できます。

ステップ 4 各タスクに対応する下矢印をクリックし、次の手順を実行してタスクの詳細を表示します。

a) [Show Scripts] をクリックして、事前チェックと事後チェックのステータスを表示します。
b) [View] をクリックして、事前チェックと事後チェックの詳細を表示します。
c) [View Diff] をクリックして、事前チェックと事後チェックの差異を表示します。

自動フラッシュクリーンアップ

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が確認されます。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。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。