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

Catalyst 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：Catalyst 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「Catalyst Center のセキュリティの構成」を参照してください。

（注） リリース 2.3.3 以降、Catalyst Center では、IE3x00 シリーズおよび IE9x00 シリーズ スイッチのソフトウェアイメージ管理（SWIM）およびソフトウェア メンテナンス アップデート（SMU）のプライマリブートオプションとして内部ブートフラッシュのみをサポートします。

Catalyst Center の以前のリリース（リリース 2.3.3 より前）があり、ネットワーク内の IE3x00 または IE9x00 デバイスがセキュアデジタル（SD）フラッシュメモリモジュールですでに起動されている場合は、**boot flash-primary** コマンドを使用して、内部ブートフラッシュをデバイスのプライマリブートオプションとして設定してください。

実行コンフィギュレーションを SD フラッシュからブートフラッシュに保存して同期するには、**sync** コマンドを使用します。

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、Catalyst 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 DNA Center* の管理者ガイド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、Catalyst 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 左上隅にあるメニューアイコンをクリックして次を選択します：**[Design]** > **[Image Repository]**。

[Image Repository] ウィンドウには、デバイスファミリ、ソフトウェアイメージ、およびアドバイザリに関する詳細が要約されています。

- [SUMMARY]：デバイスファミリ、デバイス、およびゴールデンイメージがないデバイスファミリの数が表示されます。
- [TOTAL IMAGES]：実行中のイメージ、インポートされたイメージ、およびゴールデンイメージの数が表示されます。
- [ADVISORIES]：クリティカルおよび高のアドバイザリの数を表示します。

[Image Families] テーブルには、デバイスファミリごとに [Family Name]、[Devices]、[Images]、[Advisories]、および [Images Marked Golden] の詳細が表示されます。

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

ステップ 2 ウィンドウの上部にある [Routers]、[Switches]、[Wireless Controllers]、[Security and VPN]、[Sensors]、または [Virtual Devices] をクリックするか、[Image Families] テーブルの検索またはフィルタアイコンをクリックして、デバイスファミリをフィルタリングします。

デフォルトでは、[Image Repository] ウィンドウにすべてのデバイスファミリが表示されます。

（注） イメージのアクティブ化およびイメージの更新機能は、サードパーティのデバイスではサポートされていないため、サードパーティ（シスコ以外）のデバイスは、[Image Repository] ウィンドウに表示されません。

ステップ 3 [Sync Updates] をクリックし、後続の警告メッセージで [OK] をクリックして、Cisco DNA Center のすべての管理対象デバイスの cisco.com からのイメージ情報を同期します。

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。

[Show Tasks] でタスクの進捗状況を確認することができます。タスクが成功すると、すべてのデバイスファミリのイメージ情報が更新されます。

（注） イメージ情報を取得できるのは 1 時間に 1 回のみです。

ステップ 4 [Show Tasks] をクリックして、ソフトウェアイメージに関連するすべてのタスクのステータスを表示します。

[Recent Tasks] スライドインペインには、最近の 50 件のタスクのステータスが表示されます。[Task Status] ドロップダウンリストから、[All]、[Failed]、[In-Progress]、または [Successful] を選択して、ステータスに基づいてタスクをフィルタリングします。

ステップ 5 [Import Image] をクリックして、ソフトウェアイメージまたはソフトウェア イメージ アップデートをインポートします。詳細については、ソフトウェア イメージのインポート （6 ページ）を参照してください。

ステップ 6 [Update Devices] をクリックして、インベントリ内のデバイスを更新します。

[Inventory] ウィンドウでデバイスを選択し、**[Actions]** > **[Inventory]**に移動して、インベントリ内のデバイスを編集、再同期、再起動、または削除します。

ステップ 7 [Image Families] テーブルで、[Imported Images] をクリックして、インポートされたソフトウェアイメージの詳細を表示します。[Imported Images] 行は、常にテーブルの最初の行として表示されます。

[Imported Image Family] ウィンドウの [Images] テーブルには、インポートされたすべてのソフトウェアイメージの [Image Name]、[Version]、[Device Series Assigned]、および [Action] が表示されます。

[Action] 列で [Assign] をクリックして、ソフトウェアイメージをデバイスファミリに割り当てます。詳細については、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 （7 ページ）を参照してください。

ステップ 8 [Image Families] テーブルで、デバイスファミリの名前をクリックして、特定のデバイスファミリに関連付けられているすべてのソフトウェアイメージを表示します。

[Image Family] ウィンドウの [Images] テーブルには、すべてのソフトウェアイメージの [Image Name]、[Version]、[Devices]、[Advisories]、[Golden Image] および [Device Roles & Tags] が表示されます。

[Image Family] ウィンドウで、次の手順を実行します。

a) 左側のペインで、[Roles & Tags]、[Major Versions]、または [Golden Images] をクリックするか、[Images] テーブルの検索またはフィルタアイコンをクリックして、ソフトウェアイメージをフィルタリングします。

b) [Version] 列で、[Add On] リンクをクリックすると、基本イメージ用の適用可能な [SMUs]、[PSIRT SMU]、[Subpackages]、[ROMMON]、[APSP]、および [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。

c) [Device(s)] 列でデバイスの数をクリックすると、そのイメージを使用しているデバイスが表示されます。

d) [Advisory] 列で、[Critical] または [High] のアドバイザリの数をクリックして、特定のソフトウェアイメージのアドバイザリを表示します。

[Image Advisory] スライドインペインには、ソフトウェアイメージの**ファミリ名**、**バージョン**、および**アドバイザリ**が表示されます。アドバイザリは、[Critical]、[High]、[Medium]、[Low]、および [Informational] に分類されます。

[CRITICAL]、[HIGH]、または [MEDIUM] をクリックして、各カテゴリに固有のアドバイザリを表示します。

アドバイザリを修正するには、次の手順を実行します。

1. [Fix Advisories] をクリックします。

   [Image Update] ウィンドウが表示されます。

2. デバイスを更新する推奨ソフトウェアイメージを選択します。

推奨されるソフトウェアイメージがイメージリポジトリにない場合は、cisco.com からダウンロードできます。

3. [Download and Mark Golden] をクリックします。

   [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 gold after download] チェックボックスをオン（デフォルト）のままにします。その後、[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。
   - [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。

4. [OK] 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ます。[Show Tasks] で進捗状況を確認することができます。

e) [Golden Image] 列で、星のアイコンをクリックして、ソフトウェアイメージをゴールデンとして指定します。

   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、ダウンロードアイコンをクリックして、ソフトウェアイメージをインポートします。

   ゴールデンイメージの詳細については、ゴールデン ソフトウェアのイメージについて （9 ページ）およびゴールデン ソフトウェア イメージの指定 （9 ページ）を参照してください。

f) [Device Roles & Tags] 列で、次の手順を実行します。

1. 編集アイコンをクリックし、デバイスロールやデバイスタグを割り当てます。

   デバイスロール、デバイスタグ、またはその両方を割り当てるには、対応するソフトウェアイメージがインポートされている必要があります。

2. [Assign Device Roles & Tags] スライドインペインで、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とタグを選択します。

   （注）
   - ソフトウェアイメージに両方が選択されている場合、デバイスタグはデバイスロールよりも優先されます。
   - **[Provision]** > **[Network Devices]** > **[Inventory]** で新しいデバイスタグを作成して割り当てることができます。

3. [Save] をクリックします。

推奨されるソフトウェア イメージの使用

Catalyst 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 左上隅にあるメニューアイコンをクリックして次を選択します：**[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 左上隅にあるメニューアイコンをクリックして次を選択します：**[Design]** > **[Image Repository]**。

Catalyst 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 （9 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 （13 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 左上隅にあるメニューアイコンをクリックして次を選択します：**[Design]** > **[Image Repository]**。

ステップ 2 [Import Images] をクリックします。

ステップ 3 [Import Image/Add-on] slide-in paneスライドインペインで、[Select from computer] オプションボタンをクリックし、[Choose a 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そのアップデートを参照します。

または、[Enter URL] オプションボタンをクリックして、[Enter Image URL] フィールドに、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。

（注） ソフトウェアイメージは、連邦情報処理標準（FIPS）に準拠しています。Catalyst Center で FIPS モードが有効になっている場合、URL からイメージをインポートすることはできません。コンピュータまたは cisco.com からイメージをインポートします。

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。

（注） イメージのアクティブ化およびイメージの更新機能は、サードパーティ（シスコ以外）のデバイスではサポートされていません。

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、Catalyst 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 （9 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） Catalyst 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 左上隅にあるメニューアイコンをクリックして次を選択します：**[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、Catalyst Center に cisco.com ログイン情報が追加されると、Catalyst 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 Catalyst 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

[Image Repository] ウィンドウでは、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、Catalyst 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 Catalyst 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 左上隅にあるメニューアイコンをクリックして次を選択します：**[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、Catalyst 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。Catalyst 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

Catalyst 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 左上隅にあるメニューアイコンをクリックして次を選択します：**[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 Catalyst 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 Catalyst 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

イメージ配信サーバーは、ソフトウェアイメージの保管と配信に役立ちます。ソフトウェアイメージを配信するように最大3つの外部イメージ配信サーバーを設定できます。また、新しく追加されたイメージ配信サーバーに 1 つ以上のプロトコルを設定できます。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[System]** > **[Settings]** > **[Device Settings]** > **[Image Distribution Servers]**。

ステップ 2 [Image Distribution Servers] ウィンドウで、[Servers] をクリックします。

[Image Distribution Servers] テーブルには、イメージ配信サーバーのホスト、ユーザー名、SFTP、SCP、および接続に関する詳細が表示されます。

ステップ 3 [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。

[Add a New Image Distribution Server]slide-in pane が表示されます。

ステップ 4 イメージ配信サーバについて、次の項目を設定します。

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

  （注） Cisco AireOS ワイヤレスコントローラ 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ーへのログインに使用されるユーザー名を入力します。ユーザー名には、サーバー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。
- [Password]：イメージ配信サーバー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ーが実行されているポート番号を入力します。

ステップ 5 [Save] をクリックします。

ステップ 6 一部のワイヤレスコントローラの旧バージョンのソフトウェアでは、SFTP の暗号方式として弱い暗号方式（SHA1 ベースの暗号など）しかサポートされていないため、Catalyst Center でソフトウェアイメージの管理やワイヤレスアシュアランスの設定を行うには、ワイヤレスコントローラからの SFTP 接続に対して SFTP 互換モードを有効にする必要があります。Catalyst Center の SFTP サーバーでは、弱い暗号方式のサポートを最大 90 日間まで一時的に有効にすることができます。弱い暗号を許可するには、以下を実行します。

a) SFTP サーバーの IP アドレスの横にある [i] アイコンにカーソルを合わせ、[Click here] をクリックします。
b) [Compatibility Mode] slide-in paneで [Compatibility Mode] チェックボックスをオンにして期間（1 分～ 90 日）を入力します。
c) [Save] をクリックします。

ステップ 7 （任意） 設定を編集するには、対応するイメージ配信サーバーの横にある [Edit] アイコンをクリックし、必要な変更を行って [Save] をクリックします。

ステップ 8 （任意） イメージ配信サーバーを削除するには、イメージ配信サーバーの横にある [Delete] アイコンをクリックし、[Delete] をクリックします。

イメージ配信サーバーのプロトコル順序の変更

イメージ配信サーバーのプロトコル順序を変更できます。プロトコルの順序は、イメージ配信サーバーで検証チェックを実行するのに役立ちます。デフォルトでは、ソフトウェアイメージはプロトコル順序の最初のプロトコルを使用して配信されます。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[System]** > **[Settings]** > **[Device Settings]** > **[Image Distribution Servers]**。

ステップ 2 [Image Distribution Servers] ウィンドウで、[Preferences] タブをクリックします。

デフォルトのプロトコル順序が表示されます。

ステップ 3 [Protocol Order] エリアで、[On/Off] プロトコルトグルボタンをクリックしてプロトコルを有効または無効にします。

（注） イメージを配信するには HTTPS または SCP プロトコルを有効にする必要があります。すべてのプロトコル順序で SFTP プロトコルを有効にする必要があります。

HTTPS プロトコルが無効になっているか、HTTPS プロトコル使用時にイメージ配信に失敗した場合、ソフトウェアイメージは SCP プロトコルを使用して配信されます。

ステップ 4 プロトコルをドラッグアンドドロップしてプロトコルの順序を変更します。

ステップ 5 [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（10ページ）』を参照してください。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します： **[Design]** > **[Network Settings]** > **[Servers]** の順に選択します。

ステップ 2 [イメージ配信（Image Distribution）] エリアを展開して、イメージ配信サーバーとして機能する SFTP サーバーを選択します。

ステップ 3 [イメージ配信サーバーの追加（Add image distribution servers）] チェックボックスをオンにして、フィールドを表示します。

ステップ 4 [Primary] ドロップダウンリストから、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 5 + アイコンをクリックして、[Secondary] ドロップダウンリストから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 6 [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

Catalyst 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。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、Catalyst Center はデバイスのソフトウェアイメージを無効とします。この場合、古いソフトウェアイメージを更新できます。

ソフトウェアイメージをデバイスにプッシュする前に、Catalyst 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アップグレードを実行できません。デバイスのソフトウェアイメージをアップグレードする前に、問題を修正する必要があります。

すべての事前チェックに成功したら、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。

ソフトウェアイメージが正常にアップグレードされると、Catalyst Center は CPU 使用率、ルートサマリの確認などのアップグレードの事後チェックを実行し、ネットワークの状態が変更されていないことを確認します。

始める前に

- デバイスタイプに指定されたゴールデンイメージがあることを確認します。ゴールデン ソフトウェア イメージの指定 （9 ページ）を参照してください。
- Catalyst Center で ITSM を有効にすると、Catalyst Center ソフトウェアイメージの更新をより適切に制御するための ITSM 承認プロセスが適用されます。設定変更の拡張制御を有効にするには、**[System]** > **[Settings]** > **[Visibility and Control of Configurations]** ウィンドウで、[ITSM Approval] をクリックして、ITSM でイメージ更新承認のスケジュールを設定します。詳細については、*Cisco Catalyst Center Administrator Guide* の「Enable Visibility and Control of Configurations」を参照してください。

（注） 構成の可視性を有効にしている場合、システムはイメージアップグレードの構成プレビューを生成できません。これは、SWIM ワークフローで予想される動作です。

- ソフトウェアイメージをすぐにアップグレードする必要がある場合は、[Visibility and Control of Configurations] ウィンドウで [ITSM Approval] を無効化するか、[Automation Events for ITSM (ServiceNow)] バンドルを無効化できます。バンドルにアクセスするには、**[Platform]** > **[Manage]** > **[Bundles]** > **[Automation Events for ITSM (ServiceNow)]** の順に選択します。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

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] リンクのチェック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]** > **[Image Update]** を選択します。

[Image Update] ワークフローにリダイレクトされます。

ステップ 4 [Image Update] ウィンドウの [Task Name] フィールドに一意の名前を入力します。

ステップ 5 [Software Distribution Checks] ウィンドウで、トグルボタンをクリックして、ソフトウェア配布の事前チェックと事後チェックを有効または無効にします。

（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た場合、ネットワーク階層下のすべてのデバイスにイメージ配信サーバからイメージが配信されます。サイトへのイメージ配信サーバの追加 （12 ページ）を参照してください。

現在のワークフローで実行する検証ツールを選択する、または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) 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。

1. [Add a Custom Check] をクリックして、[New Custom Check] ウィンドウを開きます。
2. カスタムチェックの名前を [Name] に入力します。
3. [When] ドロップダウンリストで、[pre] か [post] またはその両方を選択します。
4. [Select a Test Device] ドロップダウンリストから、チェックを実行するデバイスを選択します。
5. [Open Command Runner] をクリックし、CLI コマンドを入力します。
6. [Add Known Command-Patterns to Ignore During Checks] を展開し、チェックで一致した出力を無視するために使用するコマンドパターンを追加します。

   コマンドパターンを追加するには、次の手順を実行します。

   - 新しいパターンを作成するには、目的の名前と文字列またはパターンを入力します。

- 既存のパターンを使用するには、[Most Commonly Used Patterns] をクリックし、目的のパターンを選択して、[Add Selected] をクリックします。
- [Test All Patterns] をクリックします。

7. [Additional Criteria] 領域を展開します。

[Operation] ドロップダウンリストから、[Distribution]、[Activation]、または両方を選択します。

8. [Device Series] ドロップダウンリストから、目的のデバイスシリーズを選択し、[Save] をクリックします。

d) （オプション）チェックの順序を変更するには、変更するチェックを目的の順序にドラッグアンドドロップします。

（注） ワークフローウィンドウの上部で、青い進行状況バーにカーソルを合わせると、現在の手順を特定したり、前の任意の手順に戻ったりできます。

ステップ 6 [Software Activation Checks] ウィンドウで、トグルボタンをクリックして、ソフトウェア アクティベーションの事前チェックと事後チェックを有効または無効にします。

（オプション）[Skip Activation] トグルボタンをクリックして、現在のイメージ更新のアクティベーションをスキップします。

新しいカスタムの事前チェックと事後チェックを追加するには、ステップ 5 のサブステップ c を実行します。

ステップ 7 [Device Activation Order] ウィンドウで、次の手順を実行します。

a) デバイスを連続した順序に移動するには、目的のデバイスを選択し、[Move to Sequential Update Order] をクリックします。

b) [Sequential] タブでデバイスを選択し、[Reorder List] をクリックします。

デバイスの順序を変更するには、デバイスを目的の順序にドラッグアンドドロップし、[Finish Reorder] をクリックします。

（注） デフォルトでは、デバイスの最初のアクティベーション順序は並列に設定されています。アクティベーションの順序を変更するには、[Edit] をクリックします。

c) 順序の最初にあるデバイスのアクティベーションが失敗した場合に、残りのデバイスのアクティベーションプロセスを中止するには、[Abort on Update Failure] トグルボタンをクリックします。

d) ISSU アップグレードを有効にするには、アップグレードするデバイスを選択します。[ISSU] ドロップダウンリストから [Enable ISSU Upgrade] を選択します。

ステップ 8 [Schedule Task and Clean Up] ウィンドウで、次の手順を実行します。

a) アクティベーションまたは配布をすぐに開始するには、[Now] オプションボタンをクリックします。

b) 後でアクティベーションまたは配布を実行するようにスケジュールするには、[Later] オプションボタンをクリックして、日付、時刻、およびタイムゾーンを定義します。

c) （オプション）ソフトウェア配布直後にソフトウェア アクティベーション プロセスをトリガーするには、[After Distribution] トグルボタンをクリックします。

d) （オプション）デバイスメモリのフラッシュクリーンアップを開始するには、[Initiate Flash Cleanup After Activation] チェックボックスをオンにします。

（注） Catalyst Center は実行中のソフトウェアイメージのみを保存し、デバイスに保存されている以前のソフトウェアイメージをすべて削除します。

ステップ 9 [Initiate Flash Cleanup after Activation] チェックボックスをオンにして、デバイスに保存されている以前のソフトウェアイメージをすべて削除します。

（注） Catalyst Center は実行中のソフトウェアイメージのみを保存し、デバイスに保存されている以前のソフトウェアイメージをすべて削除します。

ステップ 10 [Summary] ウィンドウで、設定を確認します。変更するには、[Edit] をクリックします。

ステップ 11 続行するには、[Submit] をクリックします。

ステップ 12 （任意） 更新ステータスを確認するには、[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。

ISSU 互換性マトリクスのインポート

In-Service Software Upgrade（ISSU）は、サービスの中断なしで、または最小限に抑えて、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。ISSU は、長期リリース内または長期リリース間（17.3.x から 17.3.y や、17.3.x から 17.6.y など）でのみサポートされます。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/17.6.2 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、Catalyst Center でターゲットリリースに対応する ISSU 互換性マトリクスをダウンロードしてインポートできます。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Design]** > **[Image Repository]**。

ステップ 2 [Import Images] をクリックします。

ステップ 3 [Import Image/Add-on] slide-in paneで、[Select ISSU Compatibility Matrix] オプションボタンをクリックし、[Choose a file] をクリックして、ローカルに保存されている ISSU 互換性マトリックスファイルに移動します。

ステップ 4 [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。

（注） Catalyst Center 2.3.7 以降では、互換性マトリックスファイルは、ISSU 対応デバイスの実行イメージと cisco.com で入手可能なゴールデンタグ付きイメージに対して自動的にダウンロードされます。

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 （16 ページ）を参照してください。
- Catalyst Center で ITSM を有効にすると、Catalyst Center ソフトウェアイメージの更新をより適切に制御するための ITSM 承認プロセスが適用されます。設定変更の拡張制御を有効にするには、**[System]** > **[Settings]** > **[Visibility and Control of Configurations]** ウィンドウで、[ITSM Approval] をクリックして、ITSM でイメージ更新承認のスケジュールを設定します。詳細については、*Cisco Catalyst Center Administrator Guide* の「Enable Visibility and Control of Configurations」を参照してください。

（注） [Visibility of Configurations] を有効にしている場合、イメージアップグレードの構成プレビューは生成されません。これは、SWIM ワークフローで予想される動作です。

- ソフトウェアイメージをすぐにアップグレードする必要がある場合は、[Visibility and Control of Configurations] ウィンドウで [ITSM Approval] を無効にするか、[Cisco DNA Center Automation Events for ITSM (ServiceNow)] バンドルを無効にすることができます。バンドルにアクセスするには、**[Platform]** > **[Manage]** > **[Bundles]** > **[Cisco DNA Center Automation Events for ITSM (ServiceNow)]** の順に選択します。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

ステップ 2 [Focus] ドロップダウンリストから [Software Images] を選択し、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] ウィンドウで、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] 列には ISSU 検証ステータスが表示されます。

- **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] ウィンドウから、イメージ配信を今すぐ開始する（[Now]）か、後で開始するようにスケジュールするかを選択します。

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。

1. [Add a New Check] をクリックして、[Add a New Custom Check] ウィンドウを開きます。
2. カスタムチェックの名前を [Name] に入力します。
3. [When] ドロップダウンリストをクリックし、事前か事後またはその両方を選択します。
4. [Select a Test Device] ドロップダウンリストから、カスタムチェックを実行するデバイスを選択します。
5. [Open Command Runner] をクリックし、CLI コマンドを入力します。
6. [Additional Criteria] 領域を展開します。
7. [Operation] ドロップダウン矢印をクリックし、[Distribution] を選択します。
8. [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。
9. **[Save]** をクリックします。
10. 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。
11. 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 （12 ページ）を参照してください。
- Catalyst Center で [ITSM Approval] が有効になっている場合は、承認を受け取った後にのみイメージを更新（配布およびアクティブ化）できます。

ステップ 6 [Next] をクリックします。

ステップ 7 [Activate] ウィンドウで、アクティブ化を今すぐ開始する（[Now]）か、後で開始するようにスケジュールするかを選択します。

ステップ 8 [Initiate Flash Cleanup after Activation] チェックボックスをオンにして、デバイスに保存されている以前のソフトウェアイメージをすべて削除します。

（注） Catalyst Center は実行中のソフトウェアイメージのみを保存し、デバイスに保存されている以前のソフトウェアイメージをすべて削除します。

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。

1. [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。
2. カスタムチェックの名前を [Name] に入力します。
3. [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。
4. [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。
5. [Open Command Runner] をクリックし、CLI コマンドを入力します。
6. [Additional Criteria] 領域を展開します。
7. [Operation] ドロップダウンリストをクリックし、[Activation] を選択します。
8. [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。
9. **[Save]** をクリックします。
10. 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。
11. 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 9 [Next] をクリックします。

ステップ 10 [Summary] ウィンドウで、設定を確認します。変更するには、[Edit] をクリックします。

ステップ 11 [Actions] ドロップダウンリストから、**[Software Images]** > **[Image Update Status]** の順に選択し、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 Catalyst Center の時間を比較して、Catalyst 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 左上隅にあるメニューアイコンをクリックして次を選択します：**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

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。

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] ウィンドウにすべてのイメージ更新タスクが表示されます。

ステップ 4 更新ステータスに基づいてタスクをフィルタ処理するには、[In Progress]、[Success]、または [Failure] をクリックします。

ステップ 5 左側のペインで、[Task Names] または [Image Versions] をクリックして、操作またはイメージバージョンに基づいてタスクをフィルタ処理します。

[Status] 列には、タスクの現在のステータスが表示されます。進行中のタスクの場合、進捗状況バーにイメージ更新の進捗状況が示されます。

ステップ 6 デバイス名をクリックすると、タスクの詳細情報が表示されます。詳細については、イメージ更新ワークフローの表示 （21 ページ）を参照してください。

ステップ 7 [Upcoming Tasks] をクリックして、後で実行するようにスケジュールされているタスクを確認します。

[Upcoming Tasks] スライドインペインが表示されます。

ステップ 8 [Devices Scheduled] 列のデバイスの数をクリックして、イメージ更新タスクがスケジュールされているデバイスを確認します。

ステップ 9 チェックボックスをオンにしてタスクが失敗したデバイスを選択し、[Retry] をクリックしてイメージの更新を再試行します。

[Image Upgrade] ウィンドウが表示されます。このウィンドウから、イメージ更新タスクを今すぐ実行するように、または後で実行するようにスケジュールできます。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 （13 ページ）を参照してください。

イメージ更新ワークフローの表示

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

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。

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。

ステップ 4 [Image Update Status] ウィンドウで、デバイスの名前をクリックして、イメージのアップグレードに関する詳細情報を表示します。

ステップ 5 [Operations] タブをクリックします。

slide-in pane には、[Distribution] および [Activation] 操作に関連付けられている各タスクのステータスと、各操作の完了にかかった時間が表示されます。

ステップ 6 [Distribution] を展開して、[Distribution] 操作に関連付けられている次のタスクのステータスと、各タスクの完了にかかった時間を表示します。

- [Verify Image Availability]（レガシーデバイスのみ）：イメージリポジトリ内のソフトウェアイメージを確認します。
- [Image Integrity Verification (KGV)]：ソフトウェアイメージのソフトウェアおよびハードウェア プラットフォームチェックサム値を、既知の正常値（KGV）でプラットフォームに対して識別されたチェックサム値と比較します。

- [Pre Distribution Operation]：ソフトウェアイメージ配布用に選択されたすべての事前チェックを実行します。
- [Distribution]：プライマリ外部イメージ配布サーバーを介してソフトウェアイメージを配布します。

  プライマリ外部イメージ配布サーバーを介したソフトウェアイメージの配布が失敗した場合、ソフトウェアイメージはセカンダリイメージ配布サーバーを介して配布されます。両方の外部サーバーを介した配布が失敗した場合、ソフトウェアイメージは内部 Catalyst Center サーバーを介して配布されます。
- [Post Distribution Operation]：ソフトウェアイメージ配布用に選択されたすべての事後チェックを実行します。
- [Image Checksum Verification On Device]：デバイス上のソフトウェアイメージのチェックサム値を検証します。
- [Unpack Image]（Polaris のみ）：CLI で **install-add** コマンドを実行します。イメージの解凍は、イメージがインストールモードの場合にのみ実行されます。
- [AP Pre-Image Download]（AP のみ）：デバイスに関連付けられたすべての AP の配布プロセスに関する詳細を表示します。

ステップ 7 [Activation] を展開して、[Activation] 操作に関連付けられている次のタスクのステータスと、各タスクの完了にかかった時間を表示します。

- [Pre Activation Operation]：ソフトウェア イメージ アクティベーション用に選択されたすべての事前チェックを実行します。
- [Image Activation]：CLI で **install-activate** コマンドを実行します。このステップにより、イメージのアクティベーションプロセスに関する詳細情報が表示されます。

  （注） Cisco Catalyst 9000 シリーズ スタックスイッチの場合、「スタックの検証」事前チェックにより、スイッチ内のすべてのスタックメンバーの状態が検証されます。スタックメンバーでゴールデンイメージが実行されていない場合、**auto-upgrade** コマンドが実行されます。
- [Staggered AP Upgrade]（AP のみ）：デバイスに関連付けられたすべての AP のアクティベーションプロセスに関する詳細を表示します。
- [Install Commit]（Polaris のみ）：CLI で **install-commit** コマンドを実行します。
- [Remove Inactive Images]：デバイスに保存されている以前のソフトウェアイメージをすべて削除し、実行中のイメージのみを保存します。
- [Collect Running Image Details]：実行中のイメージの詳細を収集します。
- [Verify Image Activation]：ソフトウェアイメージが適切にアップグレードされているかどうかを確認します。
- [Post Activation Operation]：ソフトウェア イメージ アクティベーション用に選択されたすべての事後チェックを実行します。

（注）
- IOS-XE ソフトウェアで実行されている Cisco Catalyst 9800 組み込みワイヤレス コントローラ デバイスおよびCisco Catalyst 9000 シリーズ スイッチの場合、ソフトウェアイメージは（次の 3 つのコマンドを実行することにより）、**install-add**（配布でのイメージの解凍ステップ）、**install-activate**（アクティベーションでのイメージのアクティベーションステップ）、および **install-commit**（アクティベーションでのインストール コミット ステップ）の 3 つのステップでアップグレードされます。
- デバイスが非アクティブ状態の場合、CLI で最初に **install-add** コマンドが実行されます。続いて、**install-activate** および **install-commit** コマンドが実行されます。デバイスが未コミット状態の場合、**install-commit** コマンドが直接実行されます。
- **install-activate** および **install-commit** コマンドは、アクティベーション中に別々のマイルストーンで順番に実行されるため、更新をキャンセル、ロールバック、またはコミットできます。

ステップ 8 [PSIRT SMU Activation] を展開して、PSIRT SMU のアクティベーション操作に関連付けられた次のタスクのステータスと、各タスクの完了にかかった時間を表示します。
- アクティベーション前のスクリプトの実行。
- アクティベーション。
- アクティベーション後のスクリプトの実行。

ステップ 9 [APSP Distribution] を展開して、[Distribution] 操作に関連付けられている次のタスクのステータスと、各タスクの完了にかかった時間を表示します。
- [Image Integrity Verification]：ソフトウェア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 チェックサム値を、既知の正常値（KGV）でプラットフォームに対して識別されたチェックサム値と比較します。
- [Pre Distribution Operation]：ソフトウェアイメージ配布用に選択されたすべての事前チェックを実行します。
- [Distribution]：プライマリ外部イメージ配布サーバーを介してソフトウェアイメージを配布します。
- [Post Distribution Operation]：ソフトウェアイメージ配布用に選択されたすべての事後チェックを実行します。
- [Image Checksum Verification On Device]：デバイス上のソフトウェアイメージのチェックサム値を検証します。
- [Unpack Image]（Polaris のみ）：CLI で install-add コマンドを実行します。イメージの解凍は、イメージがインストールモードの場合にのみ実行されます。
- [AP Pre-Image Download]（AP のみ）：デバイスに関連付けられたすべての AP に関する AP イメージ事前ダウンロードタスクに関する詳細を表示します。

ステップ 10 [Tasks] タブをクリックすると、タスクに関連付けられている事前チェックおよび事後チェックのステータスと詳細情報が表示されます。

ステップ 11 [Differences] 列で、相違の数、各スクリプトに対応する数をクリックして、事前チェックと事後チェックの相違を確認します。

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、十分な容量を確保するために、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、Catalyst 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容量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 **[Activities]** > **[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、容量を確保できます。

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。