

BPAユーザガイドOSアップグレードv5.1

- [はじめに](#)
 - [主な機能](#)
 - [エンドツーエンドフロー](#)
 - [価値提案](#)
 - [サポートされるコントローラとデバイスプラットフォーム](#)
 - [新しい機能](#)
- [前提条件](#)
- [OSアップグレードアプリケーションの操作](#)
 - [ソフトウェア イメージの管理](#)
 - [ソフトウェアイメージ](#)
 - [ソフトウェアイメージのメタデータの同期](#)
 - [ソフトウェアイメージメタデータの追加](#)
 - [ソフトウェアイメージメタデータの一括アップロード](#)
 - [既存のソフトウェアイメージメタデータの編集](#)
 - [ソフトウェアイメージメタデータの削除](#)
 - [イメージ配布サーバの管理](#)
 - [イメージ配布サーバ](#)
 - [イメージサーバの詳細の追加](#)
 - [イメージサーバの詳細の編集](#)
 - [イメージサーバの詳細の削除](#)
 - [ソフトウェアの分析](#)
 - [前提条件](#)
 - [BPAへのソフトウェアインサイトデータのフェッチ](#)
 - [セキュリティアドバイザリを表示と管理](#)
 - [優先度の高いバグを表示と管理](#)
 - [ソフトウェアインサイトの表示](#)
 - [ベンダーが推奨するソフトウェアバージョンの表示と選択](#)
 - [ソフトウェアアップグレードが必要なデバイスの特定](#)
 - [ソフトウェアの適合性](#)
 - [前提条件](#)
 - [参照データ管理アプリケーションでのEPLDモジュール・データの作成](#)
 - [ソフトウェア適合性の表示と管理](#)
 - [ソフトウェア準拠ポリシーの作成](#)
 - [オンデマンドでのソフトウェア適合性チェックの実行](#)
 - [ソフトウェア適合性チェックの実行のスケジューリング](#)
 - [ソフトウェア準拠ポリシーの更新](#)
 - [ソフトウェアパフォーマンスポリシーの削除](#)
 - [適合結果の表示およびダウンロード](#)
 - [アップグレードポリシー](#)
 - [前提条件](#)
 - [アップグレード・ポリシーの表示と管理](#)
 - [アップグレードポリシーの作成](#)

- [ブリッジSMU](#)
- [アップグレードポリシーの編集](#)
- [アップグレードポリシーの表示](#)
- [アップグレードポリシーの削除](#)
- [アップグレードポリシーへのアクセスの制御](#)
- [アップグレードジョブ](#)
 - [前提条件](#)
 - [アップグレード・ジョブの表示および管理](#)
 - [アップグレードジョブのスケジュール](#)
 - [ジョブでのバッチの編集](#)
 - [アップグレードジョブの実行と進行状況の監視](#)
 - [ソフトウェアアップグレードレポートのダウンロード](#)
 - [ジョブのアーカイブ](#)
 - [ジョブの削除](#)
 - [ジョブ内のバッチの削除](#)
 - [ジョブのキャンセル](#)
 - [完了したジョブまたはアップグレードのロールバック](#)
- [Settings](#)
 - [ソフトウェアの適合性](#)
 - [ロールバック](#)
- [導入の設定](#)
- [アクセス制御](#)
 - [ロールベースアクセスコントロール](#)
 - [リソースグループ](#)
 - [ゼロトラストフラグの設定](#)
- [OSのアップグレード問題のトラブルシューティング](#)
 - [準拠ポリシーの作成時にターゲットデバイスモデルが表示されない](#)
 - [ソフトウェアの適合性に非動作ステータスが示される](#)
 - [特定のデバイスのソフトウェア適合結果のステータスが不明です](#)
 - [アップグレードジョブ完了の進捗率](#)
 - [ジョブスケジュールに達し、デバイスが待機中の状態になる](#)

はじめに

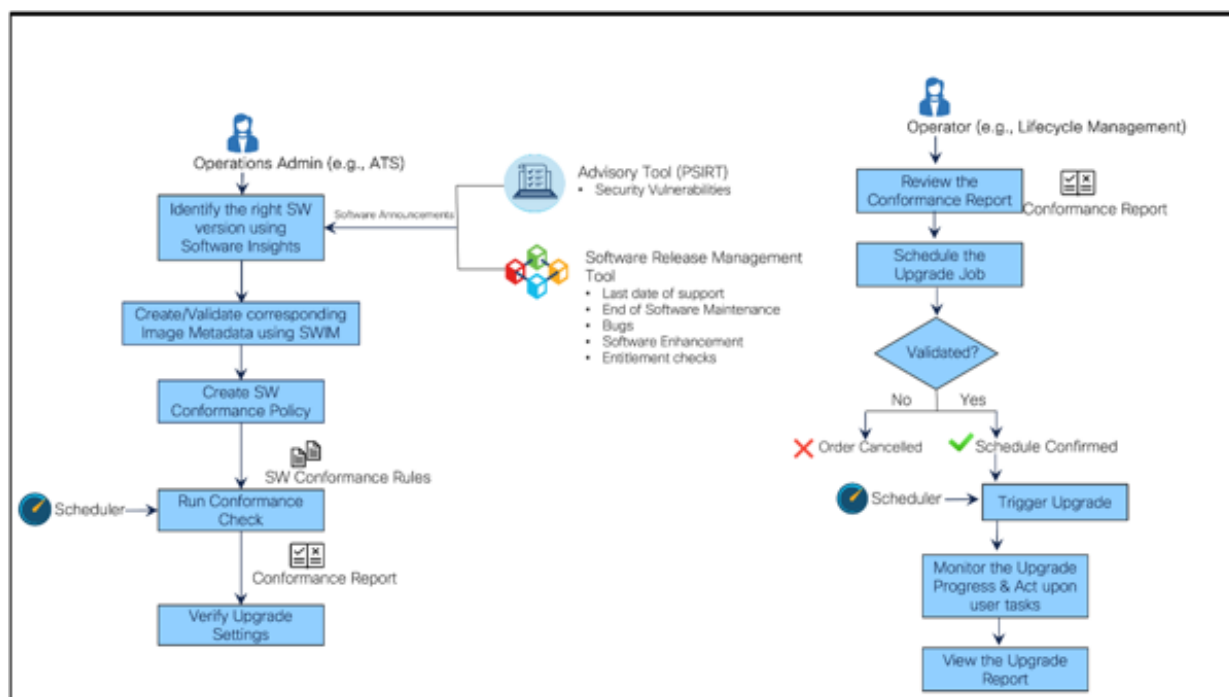
Business Process Automation(BPA)のOSアップグレードアプリケーションは、ソフトウェアの適合性を実行し、異なるドメイン間でネットワークデバイスのアップグレードを行う包括的な自動化ソリューションを提供します。複数のドメインコントローラをサポートし、統合されたユーザーエクスペリエンスを提供するオペレーティングシステム(OS)の基本アップグレードと、Software Maintenance Update(SMU)またはRPM Package Manager(RPM)パッチアップデートの両方をサポートします。

主な機能

OSアップグレードアプリケーションは、次の主要な自動化機能を提供します。

- ソフトウェアイメージ管理：使用するソフトウェアアップグレードプロセスのための（すべてのベンダーの）ソフトウェアイメージとそのバージョンの一元化されたリスト
- ソフトウェアに関する洞察：ネットワーク資産の影響を受けるソフトウェアリスクと脆弱性を特定し、ベンダーが推奨するソフトウェアバージョンに関する洞察を取得します。
- ソフトウェアコンFORMANCE：ネットワーク内で、ソフトウェアイメージのアップグレードが必要なすべてのアセットを識別します。
- アップグレード手順説明書(MOP)の定義：各ベンダーデバイスモデルまたはファミリの事前チェックおよび事後チェックとともに、アップグレードプロセスを事前定義します。
- アップグレードジョブ：メンテナンス期間中に非適合資産のアップグレードを地域をまたいでスケジュールし、アップグレードの進捗状況を監視して詳細なレポートを取得します

エンドツーエンドフロー



エンドツーエンドフロー

上の図は、Operations AdministratorとNetwork Operatorという2つの異なるユーザペルソナのOSアップグレードアプリケーションのコールフローを示しています。これらはアウトオブザボックス(OOB)で提供されます。OOBルールおよび対応する権限についての詳細は、『[アクセス制御](#)』を参照してください。

ペルソ	説明	Workspace
運用管理者	ネットワーク資産に影響を与えるソフトウェアの脆弱性（アドバイ	BPA:OSアップグレード/ソフトウェアイメージ管理/アドバイザリ

ペルソ	説明	Workspace
	ザリ、バグ、サポート終了速報など)を検出	
運用管理者	影響を受けるソフトウェアバージョンと影響を受ける資産を特定し、ベンダー提供の提案に基づいて適切なターゲットバージョンを決定します。	BPA:OSアップグレード/ソフトウェアイメージ管理/洞察
運用管理者	必要なソフトウェアイメージメタデータを作成します。	BPA:OSアップグレード/ソフトウェアイメージ管理/ソフトウェアイメージ
運用管理者	影響を受けるデバイスモデルのインテントを作成し、オンデマンドまたはスケジュールされたポリシー実行時にポリシーを実行します。	BPA:OSアップグレード/ソフトウェアコンフォーマンスポリシー
運用管理者	適合しない資産または影響を受ける資産を特定します。	BPA:OSのアップグレード/ソフトウェアへの準拠/結果の表示
運用管理者	アップグレードMOPに従って、アップグレードポリシーを作成または変更します。これには、事前および事後チェック、配布またはアクティベーションのワークフロー、トラフィックの転送または反転、およびシングルステップまたはマルチステップアップグレードのロールバックの事前定義が含まれます。	BPA:OSのアップグレード/アップグレードポリシー
ネットワークオペレータ	すべての適合しないデバイスをアップグレードするジョブをスケジュールします	BPA:OSのアップグレード/アップグレードジョブ
ネットワークオペレータ	アップグレードジョブの進行状況を監視します	BPA:OSのアップグレード/アップグレードジョブ/ジョブの詳細
ネットワークオペレータ	問題を分類するためのユーザタスク(存在する場合)に従い、プロセスを次のステップに進めることができます。	BPA:OSのアップグレード/アップグレードジョブ/ジョブの詳細

価値提案

OSアップグレードアプリケーションでは、次の付加価値が提供されます。

- Northbound Operations Support Systems(OSS)およびBusiness Support Systems(BSS)からのサービス消費を容易にするAPI初のアプローチ
- さまざまなドメインコントローラによって管理されるネットワーク全体で、ネットワークデバイスのソフトウェア適合性を迅速に検証
- オペレータは、バッチ処理、キューイング、およびスケジューリングのメカニズムを使用して、アップグレードジョブをより詳細に制御できます
- アップグレードジョブはレビュー用に早期に作成し、後で実行できます
- 最小からゼロの障害で、より高速で優れたスループットを実現するキューイングメカニズム
- アップグレード前の自動構成バックアップにより、障害発生時にシームレスな復元が可能
- チェック前およびチェック後の実行により、サービスを中断することなくアップグレードを確実に実行
- ポリシー駆動型のアプローチにより、アップグレードMOPを事前および事後検証チェック、配布またはアクティブ化、トラフィックの転送または反転、およびロールバックの各プロセスで柔軟に事前定義し、必要に応じてカスタマイズ可能

サポートされるコントローラとデバイスプラットフォーム

次のプラットフォームはBPAで検証済みで、OOBがサポートされています。ただし、フレームワークは汎用的で、新しいプラットフォームに拡張できます。追加のプラットフォームに対するOOBサポートは、優先順位に基づいて将来のリリリースで提供される予定です。

ドメインコントローラ	デバイスプラットフォーム
Cisco Catalyst Center v2.3.7.5-70434	- Cisco IOS、Cisco IOS-XE - Cisco IOS、Cisco IOS-XE
vManage v20.12.4	注：リモートサーバの配布が機能するには、デバイスがv17.9.x以降である必要があります
Nexusダッシュボードファブリックコントローラ(NDFC)v12.1.2eおよびv12.2.2	- Cisco-NXOS(N9k)
ファイアウォール管理センター(FMC)v7.4.1	- Firepower 3140 - Cisco-IOSXR(NCS540、NCS560、ASR9K)
ネットワークサービスオーケストレータ(NSO)v6.3	- Cisco-NXOS(N9K) 注:NX-OS NED v5.25.17以上が必要
クロスネットワークコントローラ(CNC)v6.0	- Cisco-IOSXR(NCS540、ASR9K)
ANSIBLE v2.9.18 (AWX - 17.1.0)	- Cisco-IOSXR(NCS540、ASR9K)
デバイスへの直接接続(Telnet)およびSecure Shell(SSH)経由)	- Cisco-IOSXR(NCS540、ASR9K)

新しい機能

このリリースのOSアップグレードユースケースで利用可能になった追加機能については、『[BPAリリースノート](#)』を参照してください。

前提条件

OSアップグレードアプリケーションを使用する前に、次の前提条件を満たす必要があります。

- OSのアップグレード、バックアップと復元、スケジューラサービス、および必要なすべてのプラットフォームサービスまたはコントローラエージェントサービスが稼働していること
- 必要なアーティファクト（ワークフロー、プロセステンプレート、デフォルトアップグレードポリシーなど）がロードされます。
- 必要なコントローラが追加され、デバイスが正常に同期されました。詳細は、『[サポートされているコントローラとデバイスプラットフォーム](#)』を参照してください

OSアップグレードアプリケーションの操作

OSアップグレードアプリケーションは、次のコンポーネントで構成されています。

- ソフトウェアイメージ管理(SWIM)
- イメージ配布サーバの管理
- ソフトウェアの分析
- ソフトウェアの適合性
- アップグレードポリシー
- アップグレードジョブ
- Settings

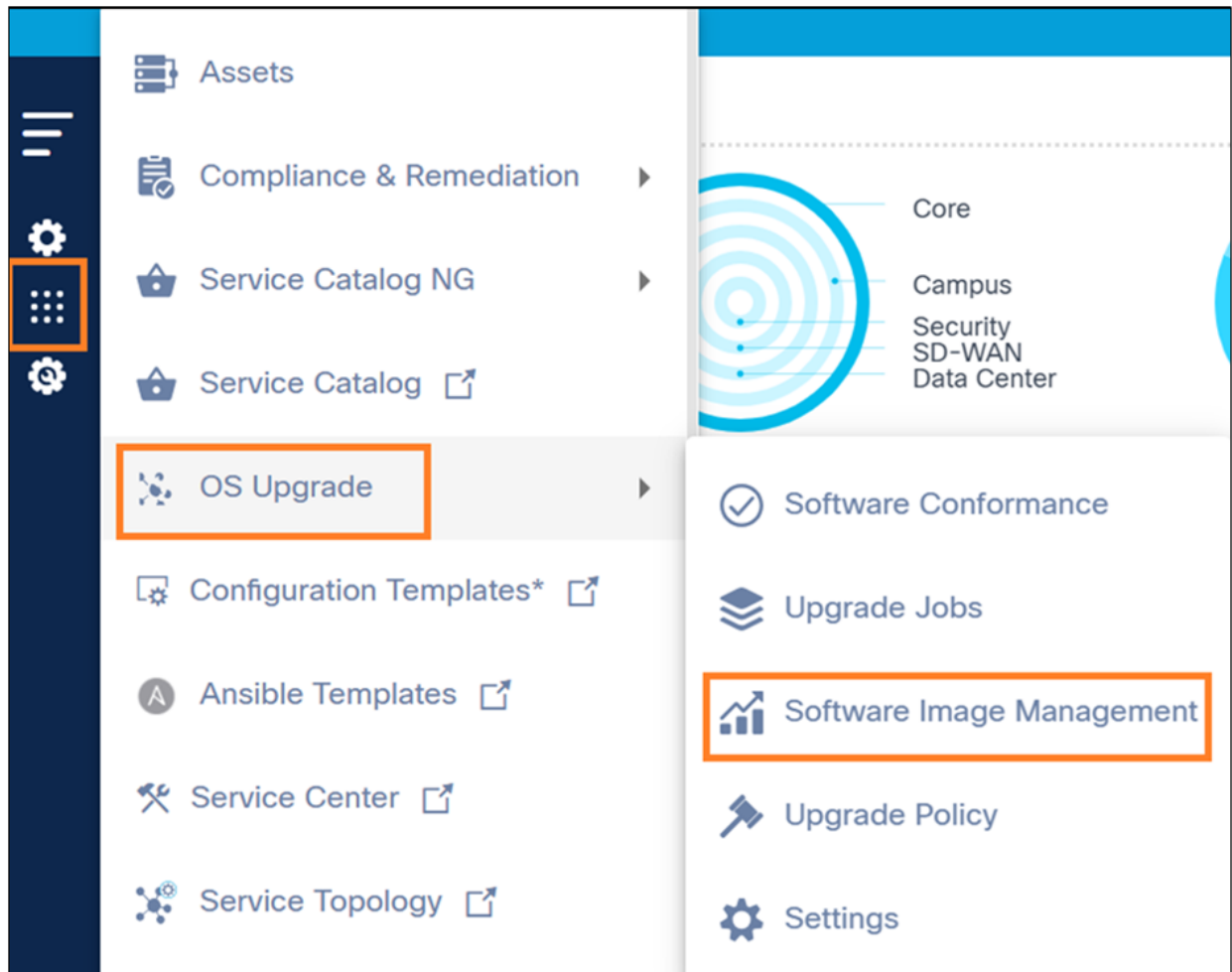
ソフトウェア イメージの管理

SWIMコンポーネントを使用すると、Operationsユーザは、NSO、ANSIBLE、CNC、FMC、Direct-to-Deviceなど、OOBイメージ管理をサポートしないコントローラのソフトウェアイメージの詳細を管理できます。また、vManage、NDFC、Cisco Catalyst Centerなどのコントローラによって維持されるソフトウェアイメージの詳細も一覧表示され、すべてのドメインコントローラにわたって維持されるソフトウェアの一元化されたリストが提供されます。ソフトウェアイメージとイメージ配布サーバは、SWIMモジュール内の2つの主要なサブコンポーネントです。

ソフトウェアイメージ

ソフトウェアイメージのページにアクセスするには、次の手順を実行します。

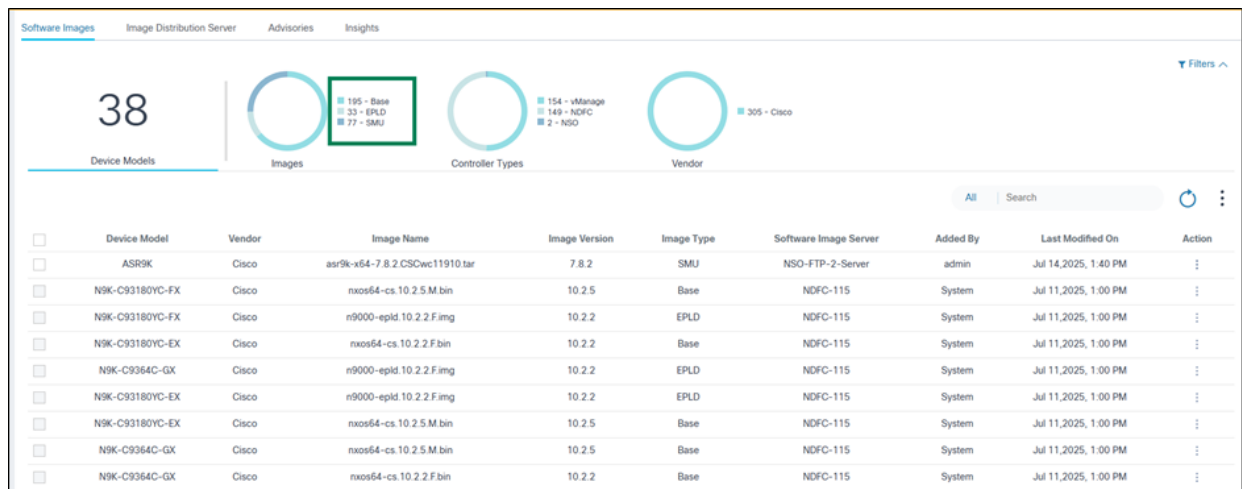
1. ソフトウェアイメージ管理にアクセスできるクレデンシャルを使用してBPAにログインします。



ソフトウェアイメージ管理のナビゲーション

2. OS Upgrade > Software Image Managementの順に選択します。

Image Managementページには、Software Images、Image Distribution Server、Advisories、およびInsightsの各タブが表示されます。



Software Imagesタブ

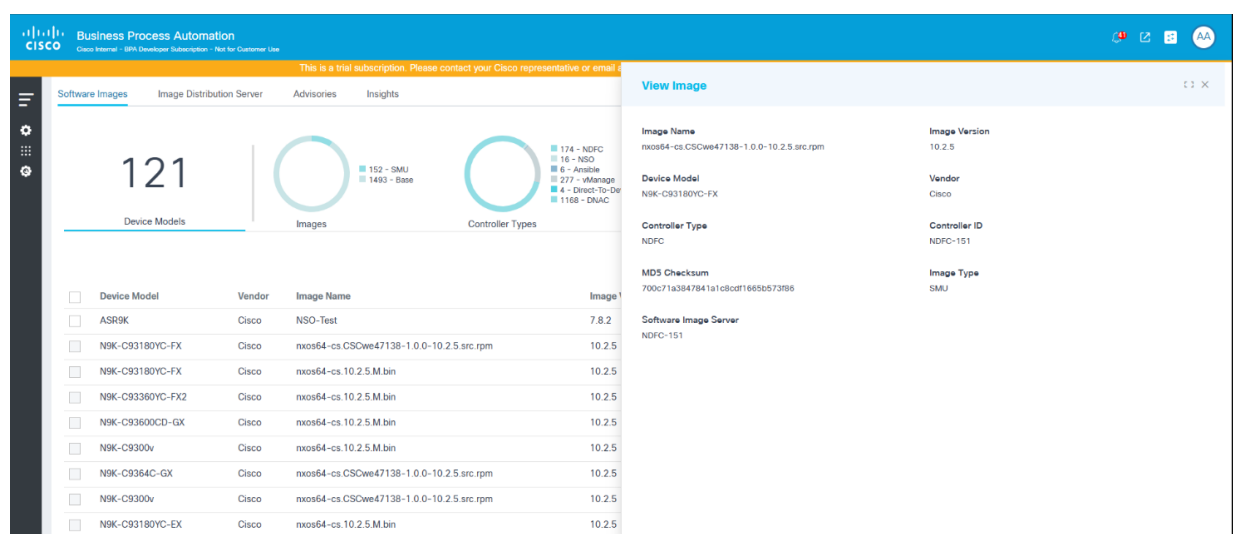
Software Imagesタブには、次の情報が含まれます。

- 上部に表示される分析セクションには、次の情報が含まれます。
 - デバイスモデルおよび関連するソフトウェアイメージの総数
 - タイプ（ベース、SMUなど）に基づいてイメージをフィルタリングできるイメージクイックフィルタ。この番号は、それぞれのイメージタイプに関連付けられているイメージの総数を示します。
 - コントローラタイプの簡易フィルタ。イメージがホストされているコントローラタイプ（Cisco Catalyst Center、vManage、NSOまたはNDFC、Direct-to-Device、CNC、ANSIBLE、FMCなど）に基づいてイメージをフィルタリングできます。この数値は、各コントローラタイプに関連付けられているイメージの総数を示します。
 - ソフトウェアを公開したベンダーに基づいてイメージをフィルタリングできるベンダーの簡易フィルタ
- その他のオプションアイコンには、次の機能があります。
 - イメージ詳細の追加：新しいイメージメタデータの追加
 - 一括アップロード：.csv形式のイメージメタデータの一括アップロード
 - Sync Images：コントローラからの同期イメージメタデータ（Cisco Catalyst Center、vManage、NDFC、FMCなど）
 - すべて削除：選択したイメージの一括削除

 注：イメージの詳細の追加、削除、および一括アップロードは、NSO、ANSIBLE、CNC、およびDirect-to-Deviceコントローラでのみ許可されます。

- Searchフィルタはイメージの検索に使用でき、次の排他的な検索フィルタが含まれています。
 - すべて：すべてのフィールドを検索します。
 - イメージ名：特定のイメージ名を持つイメージを検索します。
 - デバイスモデル：指定したモデルのイメージを検索します。

- ・ イメージバージョン：特定のソフトウェアバージョンを持つイメージを検索します。
- ・ Software Image Server：特定のイメージサーバに関連付けられているイメージを検索します。
- ・ Refreshアイコンをクリックすると、ページが更新され、選択したフィルタがクリアされます。
- ・ 既存のイメージは、次の列を持つグリッドテーブルに表示されます。
 - ・ デバイスモデル：イメージの詳細が適用されるデバイスモデル
 - ・ ベンダー：ソフトウェアイメージを発行するベンダー
 - ・ Image Name：イメージのファイル名
 - ・ イメージバージョン：イメージのソフトウェアバージョン
 - ・ イメージタイプ：イメージタイプを決定します(ベース、SMU、電子プログラマブルロジックデバイス(EPLD)など)。
 - ・ Software Image Server：現在のイメージが存在するイメージサーバ
 - ・ 追加者：画像メタデータを追加したユーザー
 - ・ 最終更新日：最後のイメージ詳細更新のタイムスタンプ
 - ・ Action：行固有のアクション（編集、削除など）を選択できるMore Optionsアイコンを提供します。
- ・ 対応する列ヘッダーをクリックして画像を並べ替える



イメージの表示

- ・ 行をクリックすると、View Imageウィンドウが開きます

ソフトウェアイメージのメタデータの同期

ソフトウェアイメージのオンデマンド同期を実行するには：



イメージの同期

1. More Optionsアイコン> Sync Imagesの順に選択します。vManage、Cisco Catalyst Center、NDFC、およびFMCからのイメージメタデータの詳細が検出され、BPAに保存されます。

注: FMCコントローラでは、同期が実行されるたびに既存のデータが保持されます。新しいイメージのみが追加されます。

2. FMCコントローラからのイメージ名に「FTD」または「Firepower Threat_Defense」という単語が含まれている場合、そのイメージのdeviceModelはFTDとしてマッピングされます。

または

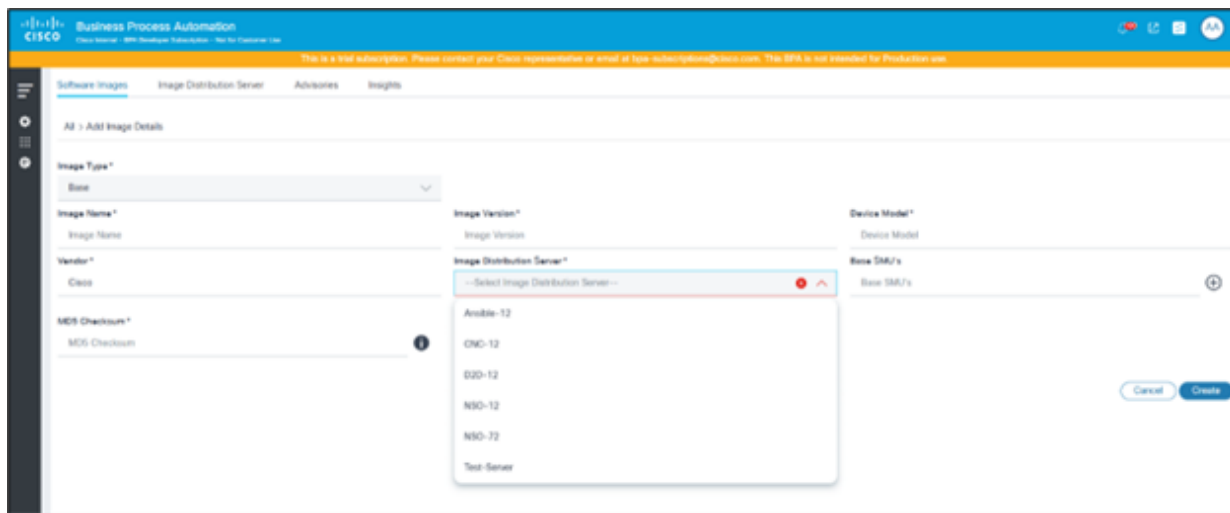
FMCコントローラからのイメージ名に「FMC」、「FW_Mgmt_Center」、または「Firewall_Management_Center」という単語が含まれている場合、そのイメージのdeviceModelはFMCとしてマッピングされます。

注: FMCでは、モデル情報をイメージメタデータに関連付けることはできません。同期が完了したら、それぞれのイメージメタデータを編集し、必要に応じてモデルを更新します。FMCのアップグレードプロセスは、モデルをアップデートしないと正常に機能しません。

3. vManageリモートサーバからのイメージは、最初は同期操作後にVersionカラムに Universally Unique Identifier(UUID)がマッピングされます。オペレータは、必要なりモートサーバのメタデータを手動で編集し、適切なイメージバージョンで更新する必要があります。このマッピングを行わないと、他のOSアップグレードコンポーネント(ソフトウェアの適合性、アップグレードポリシー、アップグレードジョブなど)が期待どおりに動作しません。
4. 自動SWIMメタデータ同期を一定間隔でスケジュールするには、『[展開設定](#)』を参照してください。

ソフトウェアイメージメタデータの追加

1. More Optionsアイコン> Add Image Detailsを選択します。Add Image Detailsページが表示されます。



イメージの詳細の追加

2. 次のフィールドに情報を入力します。

- Image Type : イメージタイプ (Base、SMU、EPLDなど)
- イメージ名 : イメージファイルの名前。ユーザは、イメージの相対パスまたは絶対パスを [名前]フィールドに入力できます。ユーザーが絶対パスを指定した場合、イメージはそのパスから直接取得されます。相対パスを指定した場合、配布時にリポジトリ・サーバーで定義されたベース・パスが追加され、フル・パスが解決されます
- イメージバージョン : イメージのソフトウェアバージョン
- デバイスモデル : イメージにタグが付けられるデバイスモデル

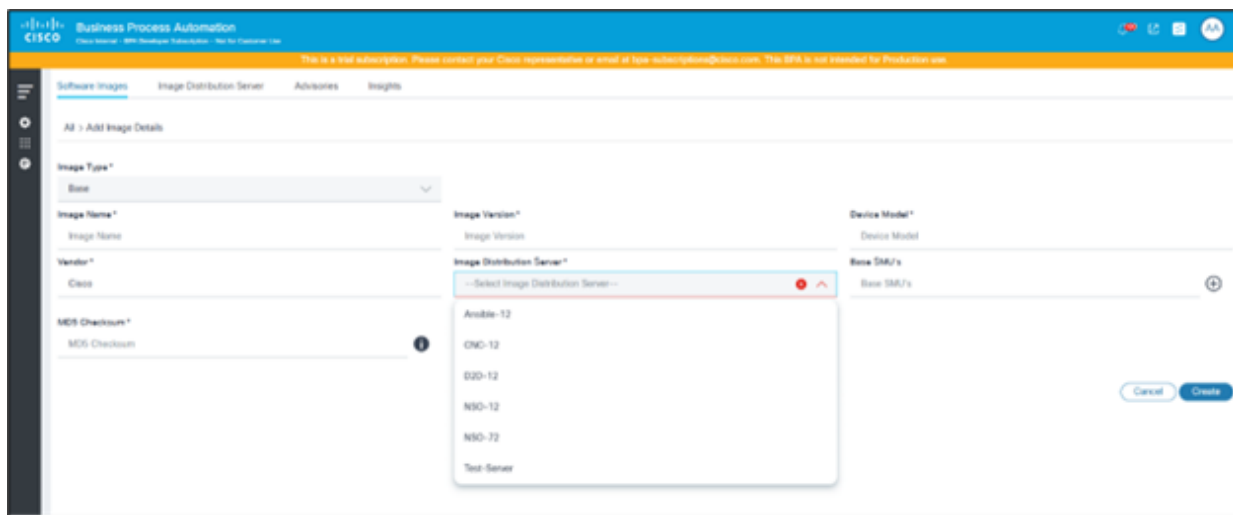
 注 : デバイスモデルは、CNC、NSO、Direct-To-Device、またはANSIBLEコントローラから提供される、該当するデバイスのモデル情報と一致している必要があります。

- Vendor : イメージを公開したベンダーまたはプロバイダー。デフォルトはCiscoですが、必要に応じて変更できます
- Image Distribution Server: Image Nameフィールドに示されたソフトウェアファイルをホストするイメージ配布サーバを選択します。イメージ配信サーバを選択すると、イメージ配信サーバ内で定義された指定コントローラタイプに関連付けられたすべてのコントローラIDに対してイメージが生成されます。ユーザがイメージ配布サーバの下でコントローラインスタンスを追加または削除すると、それらのコントローラインスタンスに対応するソフトウェアイメージが追加または削除されます。
- ベースSMU : ベースゴールデンイメージに存在するSMU。このオプションは、イメージタイプがベースの場合にのみ適用されます

- MD5チェックサム：検証用のイメージMD5チェックサム

3. [Create] をクリックします。Progress通知が表示され、確認メッセージが表示されます。

 注：ブリッジSMUのイメージメタデータは、アップグレードポリシーで使用する前に追加する必要があります。ブリッジSMUを追加するには、Image TypeドロップダウンリストからSMUを選択します。



ブリッジSMUイメージメタデータの追加

ソフトウェアイメージメタデータの一括アップロード

	A	B	C	D	E	F	G
1	Device Model	Vendor	Image Name	Version	Image Type	Image Distribution Server	MD5 Checksum
2	NCS-540	Cisco	test22	1.1.1	Base	Ansible server	680fcd5f9f3558d6fd581edc0835ce2a
3	NCS-540	Cisco	test23	2.2.2	Base	Ansible server	b4ecef95e419c63d8da124d214deaaf
4	NCS-540	Cisco	test33	2.2.2	Base	Ansible server	b4ecef95e419c63d8da124d214deaaf
5	NCS-540	Cisco	test421	2.2.2	Base	Ansible server1	b4ecef95e419c63d8da124d214deaaf

イメージ情報を含むサンプルCSVファイル

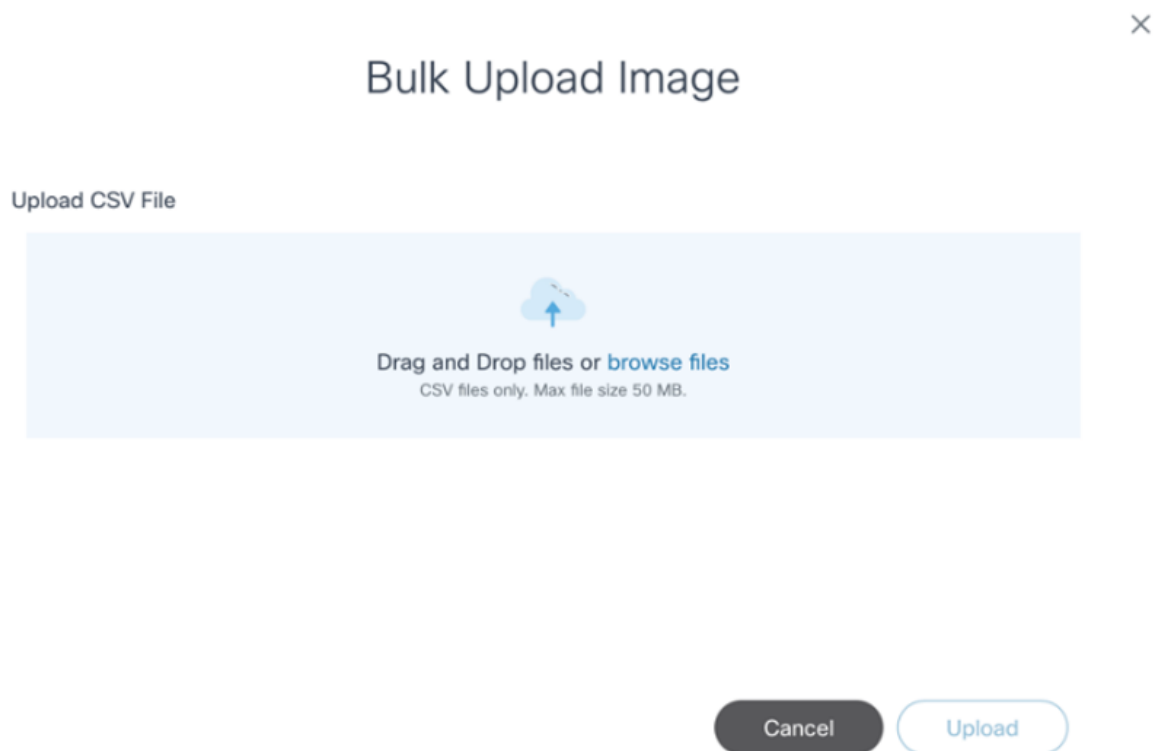
1. 必要なイメージの詳細と次の列名を含む.csvファイルを準備します。

- [Image Name]
- バージョン
- デバイスモデル
- ベンダー
- イメージのタイプ

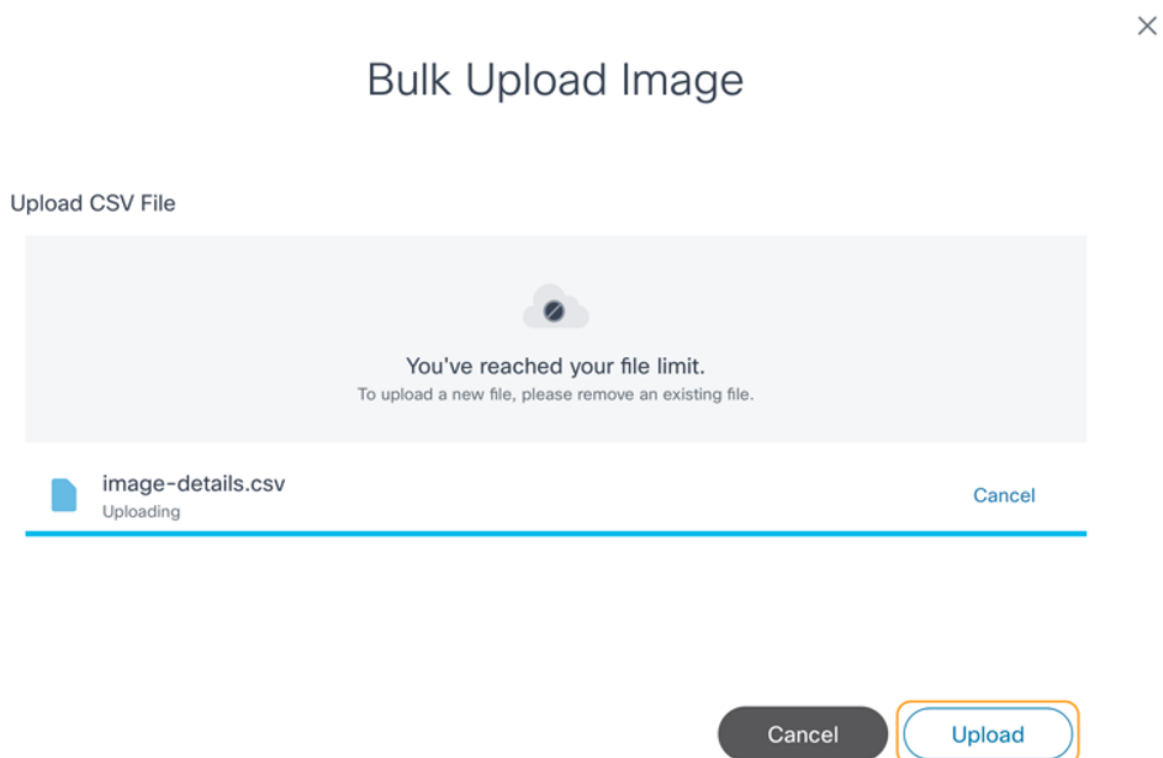
 注:Base、SMU、およびEPLDの値のみがサポートされます。

- イメージ配布サーバ
- MD5チェックサム

2. More Optionsアイコン> Bulk Uploadの順に選択します。Bulk Upload Imageウィンドウが開きます。

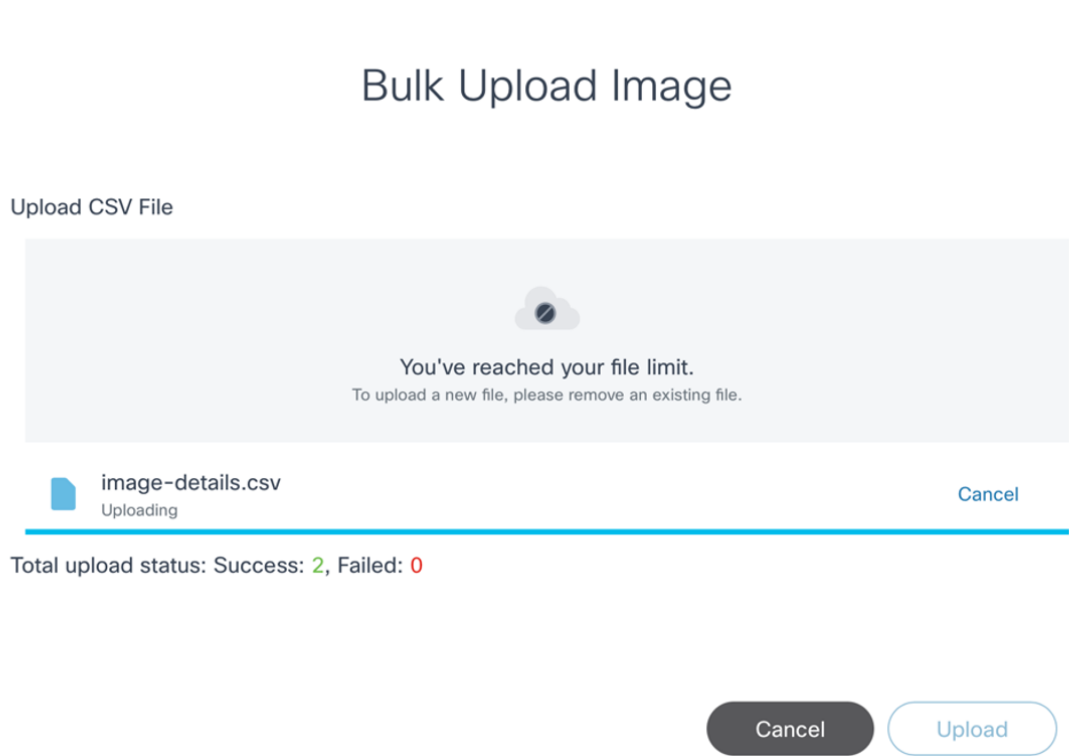


イメージの一括アップロード



イメージの一括アップロード - CSVアップロード

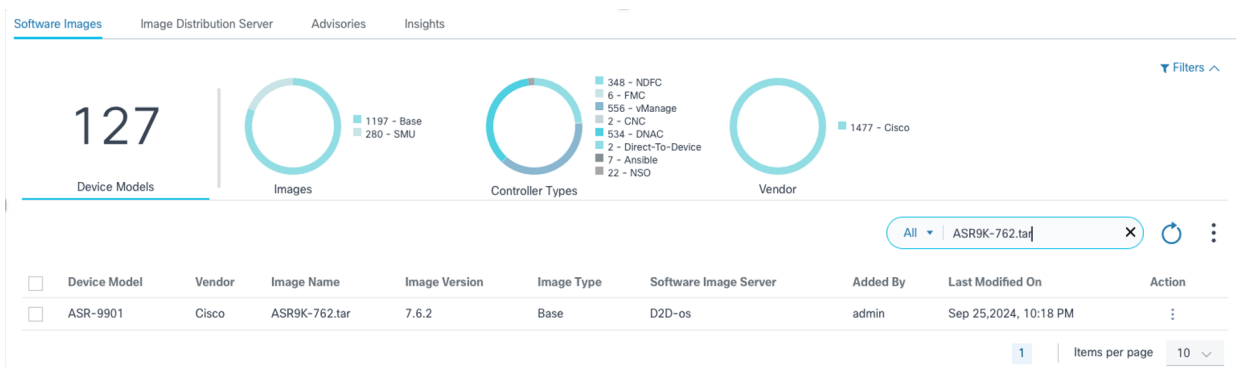
3. 準備した.csvファイルを選択して、Uploadをクリックします。.csvのイメージの詳細が検証され、処理されます。ファイルがアップロードされると、最終的な一括アップロードステータスが表示されます。



イメージの一括アップロードの成功ステータス

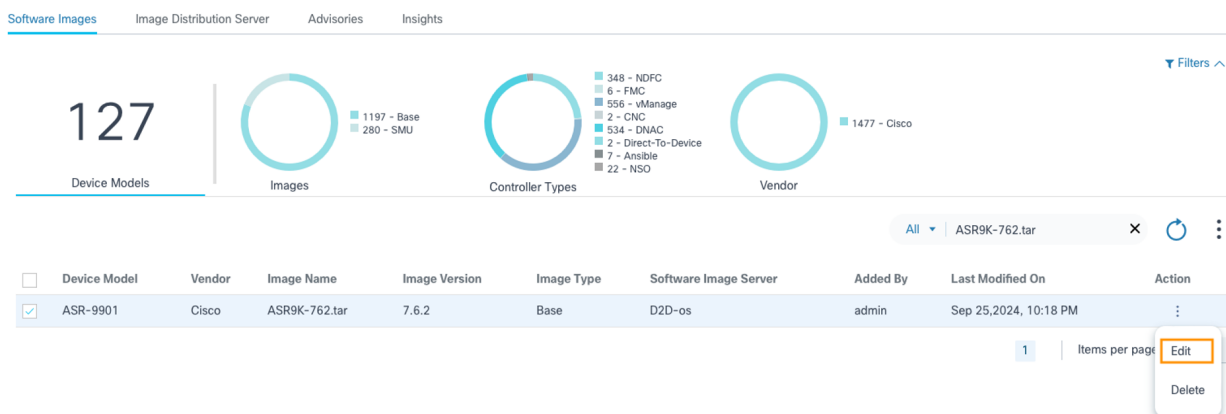
 注：データ検証エラー（レコードの重複や無効なパラメータなど）が発生した場合、エラーメッセージが一括アップロードイメージウィンドウにグリッドとして表示されます。ユーザは、.csvファイルの値を修正して再アップロードできます。

既存のソフトウェアイメージメタデータの編集



ソフトウェアイメージメタデータの検索

1. Searchフィルタを使用して、更新する必要があるイメージを探します。



編集

2. 目的のイメージのActionカラムから、More Optionsアイコン> Editを選択します。

Image Type*
SMU

Image Name*
asr9k-x64-7.7.2.CSCwe22538.tar

Image Version*
7.7.2

Device Model*
ASR-9901

Vendor*
Cisco

Image Distribution Server*
D2D-12

MD5 Checksum*
b70ace4d081339d11983b17f070d1e7

Cancel Save

ソフトウェアイメージの編集

3. 必要なパラメータを更新し、Saveをクリックして変更を保存するか、Cancelをクリックして変更を破棄します。進行状況の通知が表示され、その後、イメージの更新を確認するメッセージが表示されます。

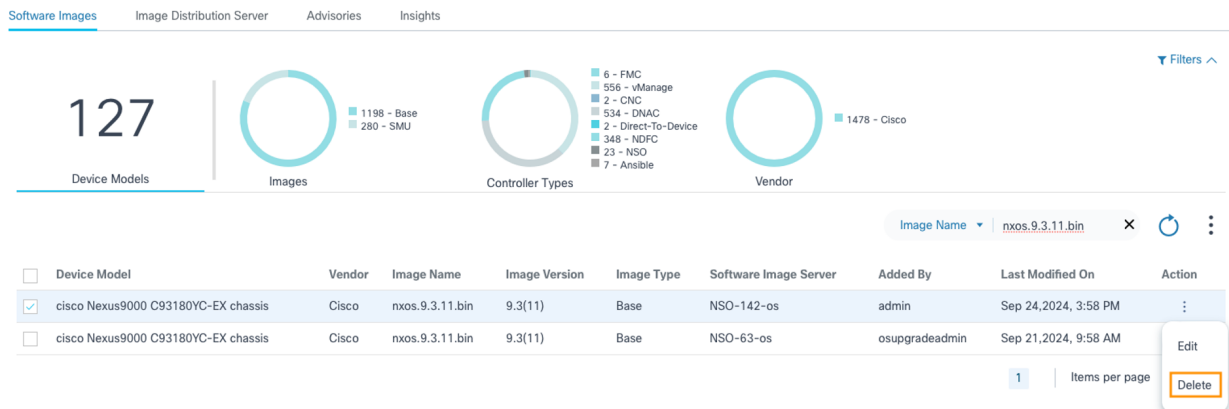
注：次のリストに注意してください。

- 編集は、CNC、NSO、D2D、ANSIBLE、FMC、およびvManageコントローラで可能（リモートサーバイメージメタデータにのみ適用可能）
- デバイスモデルの更新は、vManageリモートサーバイメージに対してのみサポートされています
- vManageリモートサーバイメージメタデータで更新できるのは、Software Versionフィールドだけです
- vManageイメージでは、ユーザはコントローラインスタンスの代わりにソフトウェアイメージサーバを表示できます

ソフトウェアイメージメタデータの削除

ソフトウェアイメージメタデータの検索

1. Searchフィールドを使用して、目的のイメージを見つけます。



[削除 (Delete)]

2. 目的のイメージのActionカラムから、More Optionsアイコン> Deleteを選択して、イメージを削除します。

または



すべて削除

複数のイメージを削除するには、目的のイメージを選択してMore Optionsアイコン> Delete Allの順に選択します。

確認が表示されます。



Delete Image

Are you sure you want to delete the selected images?

Cancel

Ok

確認

3. [OK] をクリックします。進行状況を示す通知が表示され、確認メッセージが表示されます。



注：次のリストに注意してください。

- ・イメージメタデータを追加できるのは、NSO、ANSIBLE、Direct-to-Device、およびCNCコントローラのみです。他のすべてのエンタープライズコントローラでは、組み込みのSWIM機能が利用され、それぞれのコントローラからイメージが検出されます
- ・イメージ検出機能は、NSO、ANSIBLE、Direct-to-Device、およびCNCコントローラのイメージサーバではサポートされていません。
- ・デフォルトでは、vManageリモートサーバイメージのメタデータには、同期後のバージョンパラメータのUUIDが含まれています。ユーザはメタデータを編集し、対応するバージョンでUUIDを更新する必要があります。対応するイメージバージョンは、vManageコントローラから、またはイメージが存在するデバイスにログインすることによって特定できます。

イメージ配布サーバの管理

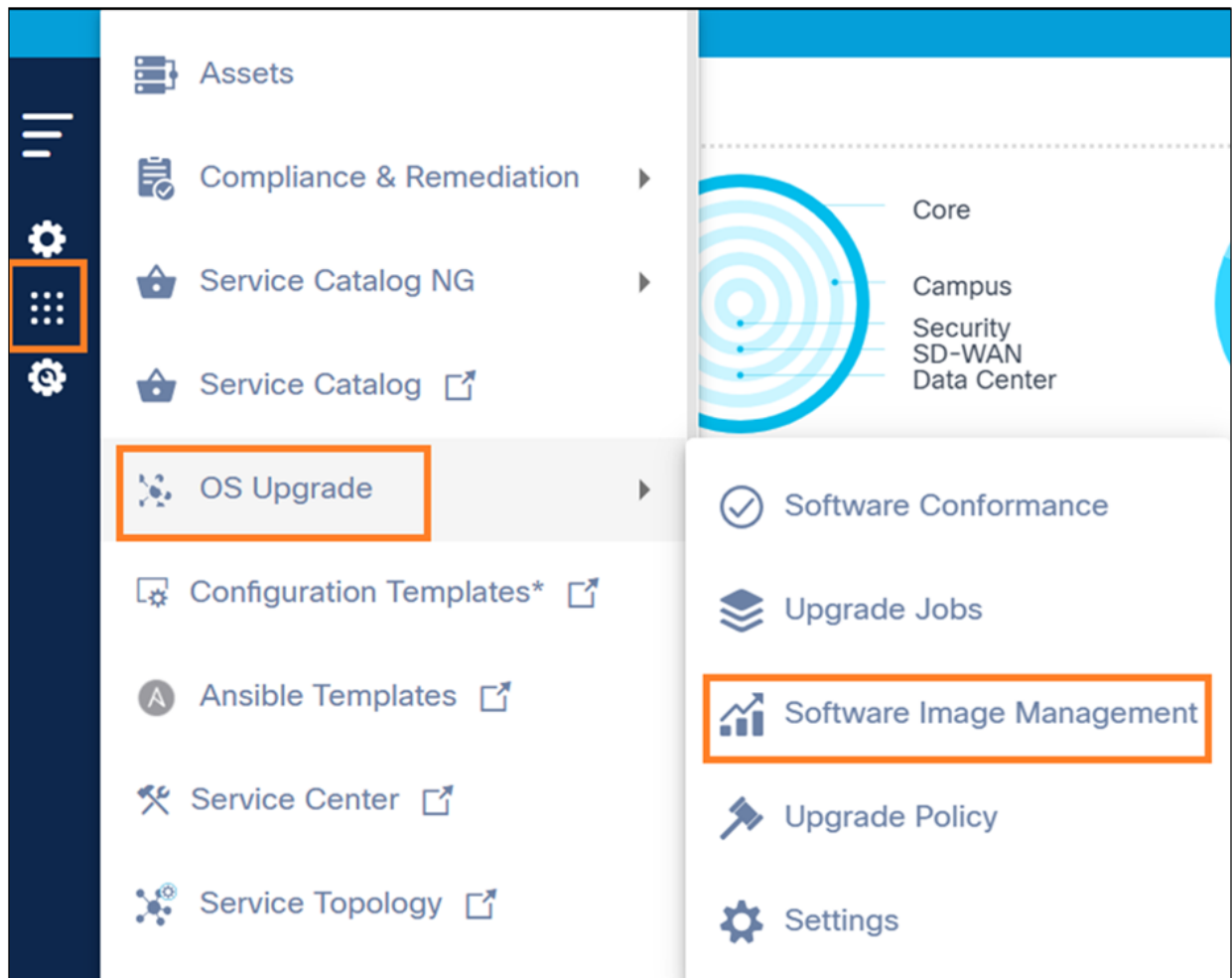
イメージ配布サーバ

このコンポーネントを使用すると、Operationsユーザーは、OOBイメージリポジトリ管理をサポートしていないCNC、NSO、ANSIBLE、FMC、およびDirect-To-Deviceコントローラのイメージリポジトリサーバーの詳細を管理できます。

Image Distribution Serverページにアクセスするには、次の手順を実行します。

1. Image Distribution Serverへの管理アクセス権を持つクレデンシャルを使用してBPAにログ

インします。



ソフトウェア イメージの管理

2. OS Upgrade > Software Image Managementの順に選択します。

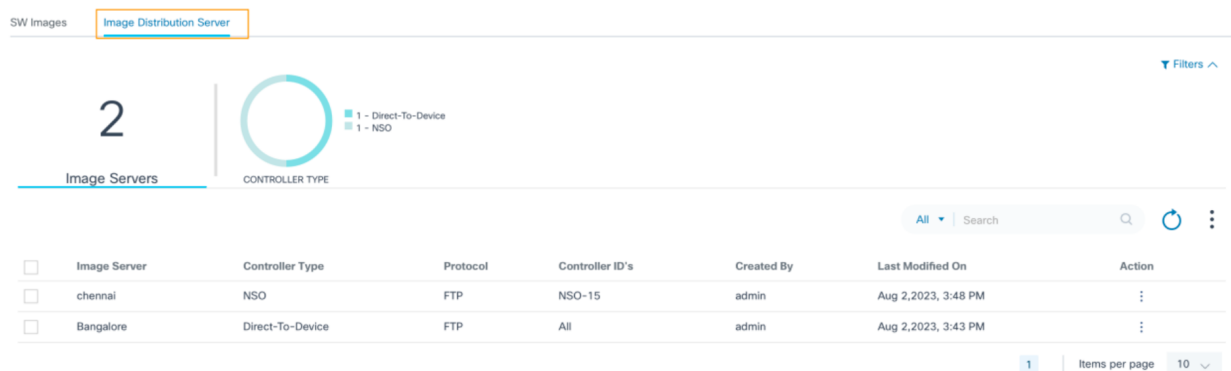


Image Distribution Serverタブ

3. Image Distribution Serverタブをクリックします。

Image Distribution Serverタブには次の項目があります。

- 上部に表示される分析セクションには、次の情報が含まれます。
 - このBPAインスタンスでオンボードされたイメージサーバーの合計数です
 - コントローラタイプの簡易フィルタ。コントローラのタイプ (NSO、Direct-to-Device、CNC、ANSIBLE、FMCなど) に基づいて、イメージサーバをフィルタリングできます。数値は、そのコントローラタイプに関連付けられているイメージ配信サーバの総数を示します。
- More Optionsアイコン。次の機能を提供します。
 - イメージサーバーの追加：新しいイメージ配布サーバーの追加
 - すべて削除：選択したディストリビューションサーバの一括削除
- 分散サーバの検索に使用できる検索フィルタ。次の排他的な検索フィルタが含まれます。
 - All：すべてのフィールドを検索します。
 - イメージサーバ：特定のサーバ名を持つサーバを検索します。
 - コントローラID：特定のコントローラIDに関連付けられているサーバを検索します。
- ページを更新し、選択したフィルタをクリアするために使用できる更新アイコン
- 既存のディストリビューションサーバは、次のカラムを持つグリッドテーブルに表示されます。
- イメージサーバ：リポジトリサーバの一意の名前
 - Controller Type：このイメージサーバが適用されるコントローラのタイプ
 - プロトコル：リポジトリサーバでサポートされているコピープロトコル

 注：サポートされているのは、FTP、SCP、およびSecure File Transfer Protocol(SFTP)だけです

- コントローラID：現在のリポジトリサーバが使用可能または適用可能なコントローラインスタンス。コントローラインスタンスとは、そのコントローラで管理されるデバイスのことです
- 作成者:リポジトリサーバにオンボーディングしたユーザ
- Last Modified On：サーバの詳細が最後に更新された日時のタイムスタンプ
- Action:EditやDeleteなど、行固有のアクションを提供します。

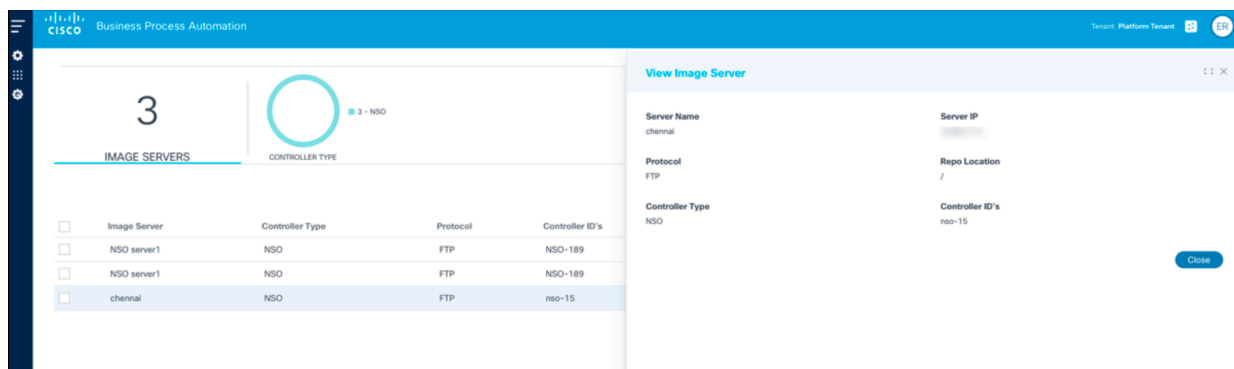
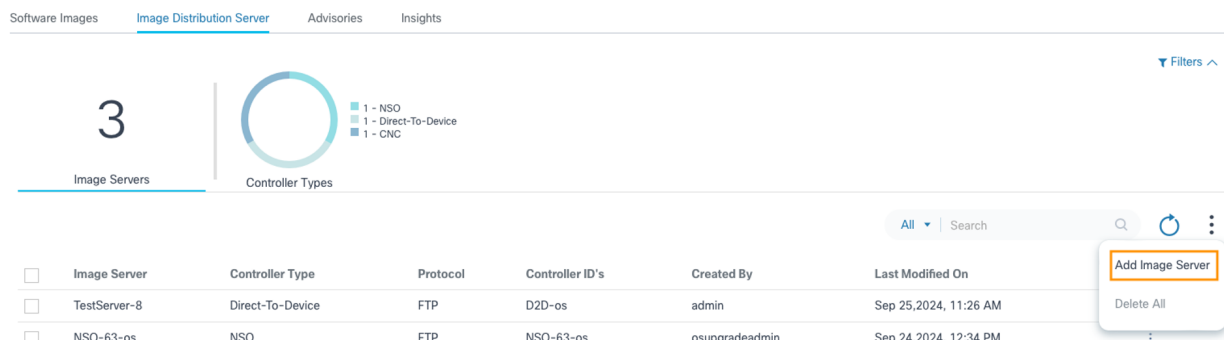


Image Server	Controller Type	Protocol	Controller ID's
☐ NSO server1	NSO	FTP	NSO-189
☐ NSO server1	NSO	FTP	NSO-189
☒ channel	NSO	FTP	nso-15

View Image Serverパネル

- ・ 行をクリックすると、View Image Serverウィンドウが開きます

イメージサーバーの詳細の追加



イメージサーバーの追加

4. More Optionsアイコン> Add Image Serverの順に選択します。Add Image Serverページが表示されます。

The screenshot shows the 'Add Image Server' form. It has a header 'All > Add Image Server'. The form contains several fields: 'Server Name*' (Server Name), 'Root Location*' (Root Location), 'User Name*' (Username), 'Server IP*' (Server IP), 'Controller Type*' (Select option), 'Password*', 'Protocol*' (Select option), and 'Controller Instances*'. There are 'Cancel' and 'Create' buttons at the bottom right.

イメージサーバーの詳細の追加

The screenshot shows the 'Add Image Server' form with sample data. The fields are filled with: 'Server Name*' (Demo-server), 'Root Location*' (/), 'User Name*' (calo), 'Server IP*' (1.2.3.4), 'Controller Type*' (NSO), 'Password*' (masked), 'Protocol*' (FTP), and 'Controller Instances*' (NSO-142-OS). There are green checkmarks next to the 'Server Name', 'Root Location', 'Controller Type', and 'Protocol' fields. There are 'Cancel' and 'Create' buttons at the bottom right.

サンプルの詳細を含むイメージサーバーの追加

5. 次のフィールドに情報を入力します。

- ・ サーバー名：イメージ・リポジトリ・サーバーの一意の名前
- ・ サーバIP：リポジトリサーバのIPv4アドレス

注：追加する前に、ネットワークデバイスからこのIPに到達できることを確認してください



- プロトコル：イメージコピー用のイメージリポジトリサーバによってサポートされます。



注:FTP、SCP、およびSFTPプロトコルのみがサポートされます。

- リポジトリの場所：リポジトリ・サーバー内のイメージ・ファイルのベース・パス



注：イメージファイルがイメージサーバリポジトリフォルダのルートにある場合、「/」は値として機能します。

- Controller Type：現在のイメージサーバが適用可能なコントローラのタイプ



注:NSO、Direct-To-Device、CNC、およびANSIBLEのみがサポートされます。

- コントローラインスタンス：管理対象のデバイスに基づいて適用可能な1つ以上のコントローラインスタンス。イメージのコピーには、特定のイメージリポジトリサーバを使用します。
- User：リポジトリからイメージファイルにアクセスするために使用するカスタムのクレデンシャル

6. [Create] をクリックします。進行状況を示す通知が表示され、確認メッセージが表示されます。

イメージサーバの詳細の編集

4

IMAGE SERVERS

4 - NSO

CONTROLLER TYPE

All | rtp

Filters

☐	Image Server	Controller Type	Protocol	Controller ID's	Created By	Last Modified On	Action
☐	RTP	NSO	FTP	NSO-161		May 30, 2023, 5:18 PM	

1Items per page10

イメージサーバの検索

7. Searchフィールドを使用して、更新する必要があるディストリビューションサーバを見つけます。

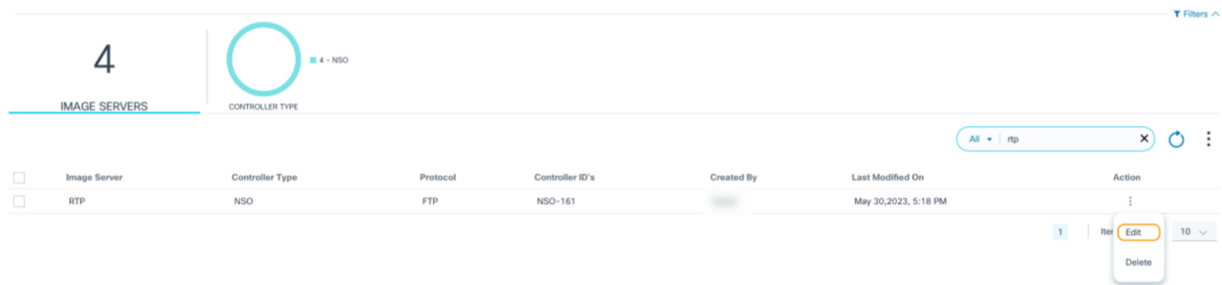


Image Server	Controller Type	Protocol	Controller ID's	Created By	Last Modified On	Action
RTP	NSO	FTP	NSO-161		May 30, 2023, 5:18 PM	Edit Delete

イメージサーバーの編集

8. Actionカラムから、More Optionsアイコン> Editを選択します。
9. 必要なパラメータを更新します。
10. [Save] をクリックします。進行状況の通知が表示され、確認メッセージが表示されます。

イメージサーバーの詳細の削除

1. Searchフィルタを使用して、目的のサーバを見つけます。

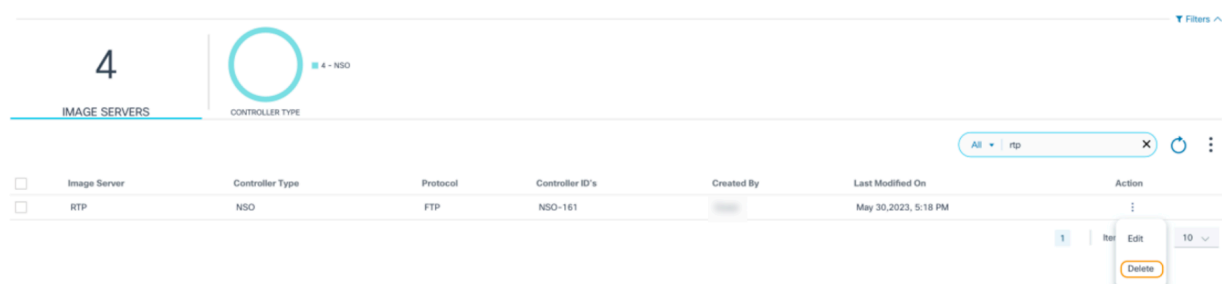


Image Server	Controller Type	Protocol	Controller ID's	Created By	Last Modified On	Action
RTP	NSO	FTP	NSO-161		May 30, 2023, 5:18 PM	Edit Delete

イメージサーバーの削除

2. ActionカラムでMore Optionsアイコン> Deleteの順に選択し、1つのディストリビューションサーバを削除します。

または

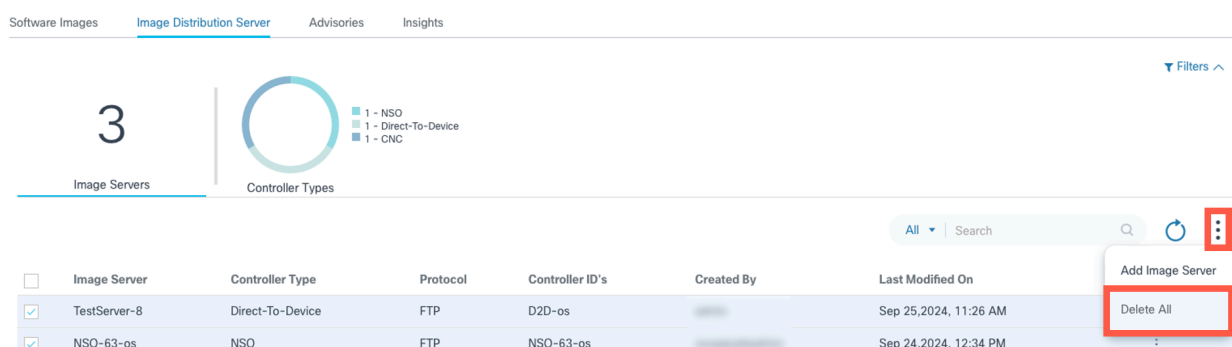
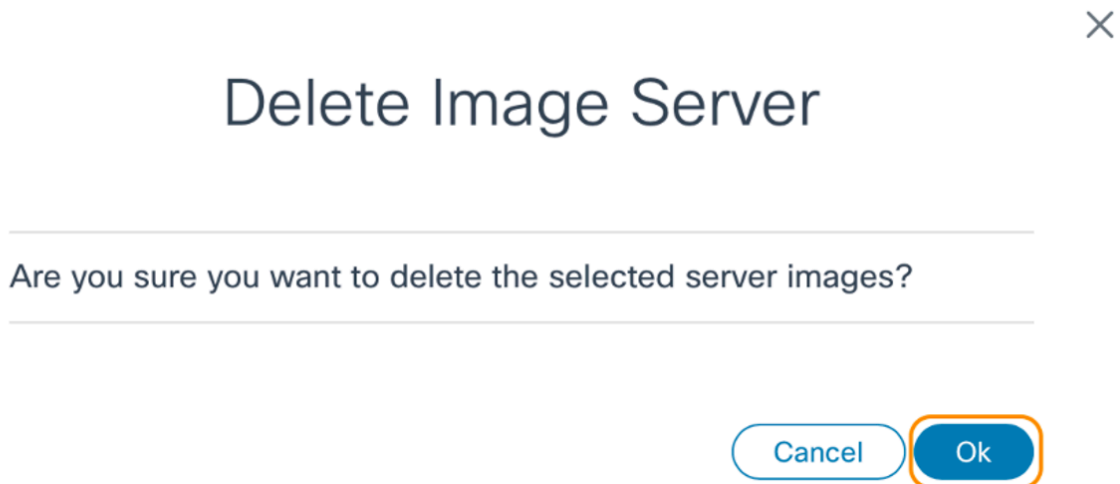


Image Server	Controller Type	Protocol	Controller ID's	Created By	Last Modified On	Action
☒ TestServer-8	Direct-To-Device	FTP	D2D-os		Sep 25, 2024, 11:26 AM	Add Image Server Delete All
☒ NSO-63-os	NSO	FTP	NSO-63-os		Sep 24, 2024, 12:34 PM	

複数のイメージサーバーの削除

必要なサーバを選択してMore Optionsアイコン> Delete Allの順に選択し、複数のディストリビューションサーバを削除します。

確認が表示されます。



削除の確認

3. [OK] をクリックします。進行状況の通知が表示され、確認メッセージが表示されます。

ソフトウェアの分析

Software Insightsは、セキュリティアドバイザリ、バグ、ネットワーク資産によってさらされるソフトウェアのサポート終了(End-of-Life)など、すべてのセキュリティ脆弱性を検出します。また、Cisco Catalyst CenterおよびNDFCコントローラで管理されるデバイスモデルに対するソフトウェアの提案も示します。管理者ユーザは、ネットワーク資産に対して推奨されるソフトウェアバージョンを選択し、その提案が使用可能な場合は、デバイスモデルの準拠ポリシーを作成できます。

前提条件

- 分析用アダプタを有効にします。「Cisco-Insights-Adapter」という名前のCisco Insights Server用のアダプタは、OOBで使用できます。一部の外部サードパーティのInsightsサーバと統合するには、対応するアダプタを構築する必要があります。詳細については、『BPA開発者ガイド』の「[Insightsアダプタの設定](#)」を参照してください。
- BPAシステムをシスコクラウドに接続するには、インターネット接続が必要です。
- 同期操作に進む前に、アダプタ設定にclient_idとclient_secretがあることを確認します。
- 必要に応じて、次の手順に従ってインターネットのプロキシを設定できます。
- IOS-XR OSタイプの場合、必要に応じて、参照データ管理(RefD)でカスタムデバイスシリーズとモデルのマッピングを実行できます。カスタムシリーズとモデルのマッピングの詳細

については、『[BPA Developer Guide](#)』を参照してください。

- BPA Kubernetesポッドでは、シスコからアドバイザリ、バグ、サポート終了情報を収集するためにインターネットアクセスが必要です。BPAネットワークが直接インターネットにアクセスしていないが、プロキシ経由で利用できる場合は、以下の手順に従ってKubernetesポッドにインターネット用のプロキシを使用させます。

1. <<http://proxy-domain.com:port>>の代わりに実際のプロキシアドレスを使用してスクリプトを更新します。
2. 導入YAMLまたはhelmチャートの各ポッドに対して環境パラメータを設定します。
3. NO_PROXYまたはno_proxy設定ですべてのデプロイ名を追加して、Kubernetesノードで次のスクリプトを実行します。

```
#!/bin/bash
# Define the environment variables
HTTP_PROXY=""<

>"
HTTPS_PROXY=""<< http://proxy-domain.com:port>>"
http_proxy=""<

>"
https_proxy=""<

>"

NO_PROXY="*.svc,localhost,127.0.0.1,192.168.0.0/16,10.0.0.0/8,172.16 .0.0/12,adaptor-builder,agent-mana
no_proxy="*.svc,localhost,127.0.0.1,192.168.0.0/16,10.0.0.0/8,172.16 .0.0/12,adaptor-builder,agent-mana
# Get the list of deployments
deployments=$(kubectl get deployments -n bpa-ns | grep -v NAME | awk '{print $1}')

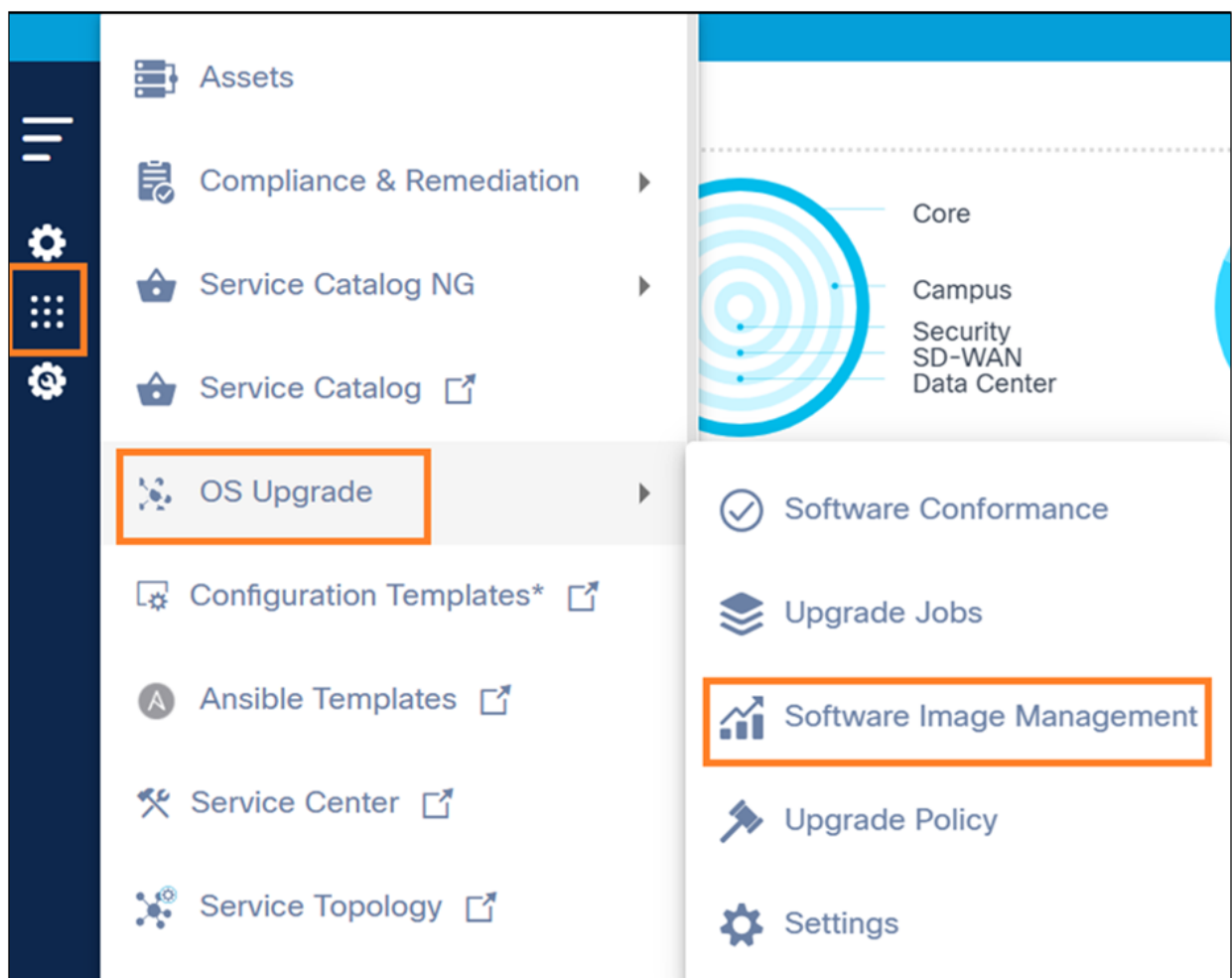
# Loop through each deployment and set the environment variables
for dp in $deployments;do
    kubectl set env deployment/$dp\
        HTTP_PROXY=$HTTP_PROXY \
        HTTPS_PROXY=$HTTPS_PROXY \
        http_proxy=$http_proxy \
        https_proxy=$https_proxy \
        NO_PROXY=$NO_PROXY \
        no_proxy=$no_proxy \
    -n bpa-ns
done
```

 注：上記のようにプロキシを設定すると、Insights Adapterはシスコネットワークに到達し、必要なSoftware InsightsデータをBPAにダウンロードできます。プロキシなしで他の外部Insightsサーバに直接接続する場合は、no_proxy変数に追加してください。

BPAへのソフトウェアインサイトデータのフェッチ

ソフトウェアの洞察データをBPAに同期するには：

1. 同期ソフトウェアの洞察データにアクセスできるクレデンシャルを使用してBPAにログインします。



ソフトウェアイメージ管理のナビゲーション

2. 側面パネルからOS Upgrade > Software Image Managementの順に選択します。



[アドバイザリ]タブ

3. Advisoriesタブをクリックします。

同期してBPAにソフトウェアの洞察を取得



同期してBPAにソフトウェアの洞察を取得

4. Syncをクリックします。

これにより、インベントリに存在する資産に関連するすべてのセキュリティアドバイザリ、優先度の高いバグ、サポート終了速報、およびソフトウェアの提案が検出されます。セキュリティアドバイザリとソフトウェアのサポート終了日は、OSのタイプとソフトウェアバージョンに基づいて決定されます。製品IDとソフトウェアのバージョンに基づいて、優先度の高いバグやソフトウェアの提案が決定されます。

Last Updatedにはインサイトデータが最後に同期された日時が表示され、Sync Statusフィールドには最後の同期ステータスが表示されます。



注：該当するアドバイザリ、バグ、リリースノート、および提案はすべて、「Cisco-Insights-Adapter」ファイルを通じてCiscoクラウドから取得されます。

セキュリティアドバイザリの表示と管理

アドバイザリページにアクセスするには：

1. アドバイザリへの管理アクセス権を持つクレデンシャルでBPAにログインします。

- Impactsでは、アドバイザリの重大度に基づいてフィルタリングが可能です。デフォルトではAllが選択されています。
- Last Updatedは、アドバイザリの最終更新日に基づいてフィルタリングします。デフォルトではAllが選択されています
- すべてクリア：選択したフィルタをリセットします。
- 検索フィルタはアドバイザリの検索に使用され、次の排他的な検索フィルタが含まれます。
 - All:Advisory、CVE、およびSoftware Versionsなどの列での検索
 - アドバイザリ：検索で指定された条件でアドバイザリを検索します。
 - CVE：特定のCommon Vulnerabilities and Exposures(CVE)のアドバイザリを検索
 - ソフトウェアバージョン：特定のOSタイプまたはソフトウェアバージョンに関連するアドバイザリを検索します。
- Refreshアイコンを使用すると、ページを更新して、選択したフィルタをクリアできます
- 既存のアドバイザリは、次の列で表示されます。
 - アドバイザリ：アドバイザリの要約
 - 影響：アドバイザリの重大度
 - CVE:割り当てられたCVE
 - ソフトウェアバージョン：影響を受けるOSタイプおよびソフトウェアバージョン
 - 最終更新：アドバイザリが最後に更新された日時
 - バージョン：アドバイザリバージョン
 - 影響を受ける可能性のある資産：このアドバイザリの影響を受ける可能性のある資産の数
- ヘッダーフィールドをクリックすると、アドバイザリがソートされます



注：並べ替えは、影響を受ける可能性のあるアセットのオプションではありません。

Filters

Impacts

☒ All

☐ Critical

☐ High

☐ Medium

☐ Low

Last Updated

☒ All

☐ <30 Days

☐ 31-60 Days

☐ 61-90 Days

☐ >90 Days

Clear All

Advisory	Impact	CVE
Cisco NX-OS Software TACACS+ or RADIUS Remote Aut	High	CVE-2023-20168
...		
Cisco NX-OS Software OSPFv3 Denial of Service Vul	High	CVE-2022-20823
...		
Cisco NX-OS Software NX-API Command Injection Vul	High	CVE-2022-20650
...		
Cisco NX-OS Software MPLS OAM Denial of Service V	High	CVE-2021-1588
...		
Cisco NX-OS Software Cisco Fabric Services Over I	High	CVE-2022-20624
...		
Cisco NX-OS Software CLI Command Injection Vulner	Medium	CVE-2023-20050
...		
Cisco IOx for IOS XE Software Privilege Escalatio	Critical	CVE-2020-3227
...		
Cisco IOx for IOS XE Software Command Injection V	Medium	CVE-2021-1384
...		
Cisco IOx Application Hosting Environment Vulnera	Medium	CVE-2022-20677,CVE-2022-20718,CVE-2022-207

High

Cisco NX-OS Software OSPFv3 Denial of Service Vulnerability

CVE CVE-2022-20823

Published Aug 24, 2022, 9:30 PM(1 year ago)

Last Updated Aug 24, 2022, 9:30 PM(1 year ago)

Version 1.0

View Security Advisory

Summary Affected Assets (2)

A vulnerability in the OSPF version 3 (OSPFv3) feature of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device.

This vulnerability is due to incomplete input validation of specific OSPFv3 packets. An attacker could exploit this vulnerability by sending a malicious OSPFv3 link-state advertisement (LSA) to an affected device. A successful exploit could allow the attacker to cause the OSPFv3 process to crash and restart multiple times, causing the affected device to reload and resulting in a DoS condition.

アドバイザリ詳細ビュー

- アドバイザリ行を選択すると、次のタブを含むアドバイザリの詳細ビューが開きます。
 - サマリー：選択したアドバイザリのサマリーを表示します。デフォルトで表示されます。
 - 影響を受ける資産：資産名、シリアル番号、モデル名、ソフトウェアバージョン、

IPアドレス、コントローラIDなど、影響を受ける可能性のある資産の詳細を表示します。このタブでは、資産の並べ替えや検索を実行できます

Filters

Impacts

All

Critical

High

Medium

Low

Last Updated

All

<30 Days

31-60 Days

61-90 Days

>90 Days

Clear All

Advisory	Impact	CVE
Cisco NX-OS Software TACACS+ or RADIUS Remote Aut	High	CVE-2023-20168
Cisco NX-OS Software OSPFv3 Denial of Service Vul	High	CVE-2022-20823
Cisco NX-OS Software NX-API Command Injection Vul	High	CVE-2022-20650
Cisco NX-OS Software MPLS OAM Denial of Service V	High	CVE-2021-1588
Cisco NX-OS Software Cisco Fabric Services Over I	High	CVE-2022-20624
Cisco NX-OS Software CLI Command Injection Vulner	Medium	CVE-2023-20050
Cisco Ix for IOS XE Software Privilege Escalatio	Critical	CVE-2020-3227
Cisco Ix for IOS XE Software Command Injection V	Medium	CVE-2021-1384
Cisco Ix Application Hosting Environment Vulnera	Medium	CVE-2022-20677,CVE-2021-20718,CVE-2022-207

High

Cisco NX-OS Software OSPFv3 Denial of Service Vulnerability

CVE

CVE-2022-20823

Published

Aug 24, 2022, 9:30 PM(1 year ago)

Last Updated

Aug 24, 2022, 9:30 PM(1 year ago)

Version

1.0

View Security Advisory

Summary

Affected Assets (2)

Below is the list of assets known to be affected by this security advisory. Expand to view the details.

2 Total Assets

All

Search

Asset Name	Serial Number	Model Name	Version	Role	IP Address	Controller ID
CNXS-N93180-2		N9K-C93180YC-FX	9.3(7)	super spine		NDFC
CNXS-N93600CD-2		N9K-C93600CD-GX	9.3(7)	border		NDFC

1Items per page10

セキュリティアドバイザリを表示

- セキュリティアドバイザリリンクの表示：公式のアドバイザリページに移動します。

優先度の高いバグの表示と管理

Software ImagesImage Distribution ServerAdvisoriesInsights

Security Advisories

Priority Bugs

Filters

Impacts

Security Advisories are determined by matching the OS Type and SW version of the devices

Last Updated : Dec 20, 2023, 1:17:06 PM Sync Status : Completed Sync

Security Advisories 214 Total

All

Search

Advisory	Impact	CVE	Softwares Versions	Last Updated	Version	Potentially Affected Assets
----------	--------	-----	--------------------	--------------	---------	-----------------------------

優先度の高いバグの選択

前のセクションで説明したアドバイザリページを開いたら、Priority Bugsタブをクリックします。Priority Bugsページが表示されます。

Software ImagesImage Distribution ServerAdvisoriesInsights

Security Advisories

Priority Bugs

Filters

Severity

Priority bugs are determined by matching the product Id and SW version of the devices

Last Updated : Dec 20, 2023, 1:17:06 PM Sync Status : Completed Sync

Priority Bugs 73 Total

All

Search

Bug ID	Severity	Summary	Product Versions	Potentially Affected Assets
CSCwh39932	6	N9300 fails to establish OSPF adjacency in non-vp	N9K-C93360YC-FX2:10.2(5)	2
CSCwd31302	2	CIAM: Vulnerabilities in rpm 4.14.2 CVE-2021-3593	N9K-C93360YC-FX2:10.2(5)	2
CSCwi43066	3	DOC: Update N9K SFlow documentation for tah sampl	N9K-C9364C-GX:9.3(10),N9K-C93180YC-FX:9.3(10)	2
CSCwi40943	3	/32 route is not getting installed in the RIB on	N9K-C9364C-GX:9.3(10),N9K-C93180YC-FX:9.3(10)	2
CSCwi52972	2	Multicast traffic forwarding issues for random fl	N9K-C9364C-GX:9.3(10),N9K-C93180YC-FX:9.3(10)	2
CSCwi15483	3	Interface UP without cable, only QSPF interted	N9K-C93180YC-FX:9.3(7)	1
CSCwi23447	2	Nexus 9504 unable to upgrade correctly from 9.3(7	N9K-C93180YC-FX:9.3(7)	1
CSCwi26553	6	Web UI on 17.9.4 performance/response is slow	C9300-24T:17.9.4,C9300-24UX:17.9.4	0
CSCwh99413	4	Console Logging for some XPATH isco-IOS-XE-instal	C9300-24T:17.9.4,C9300-24UX:17.9.4	0
CSCwi23471	2	Evaluation of all for HTTP/2 Rapid Reset Attack v	C9300-24T:17.9.4,C9300-24UX:17.9.4	0

123...8NextItems per page10

優先バグ

Priority Bugsページでは次のオプションが利用可能です。

- バグの重大度に基づいてフィルタリングできる重大度フィルタ。デフォルトではすべてが選択されています。
- Searchフィルタはバグの検索に使用でき、次の排他的な検索フィルタが含まれています。
 - [すべて]:すべてのフィールドを検索します。
 - バグID:指定されたバグIDを持つバグを検索します
 - 概要:概要に含まれる特定のキーワードを持つバグを検索します
 - 製品バージョン:特定の製品IDまたはソフトウェアバージョンに関連するバグを検索します
- Refreshアイコンを使用すると、ページを更新して、選択したフィルタをクリアできます
- 優先度の高いバグは、次の列とともに表に表示されます。
 - Bug ID
 - 重大度:バグの重大度
 - Summary:バグの要約詳細
 - 製品バージョン:影響を受ける製品IDとソフトウェアバージョン
 - 影響を受ける可能性のあるアセット:バグの影響を受ける可能性のあるアセットの数
- 並べ替えは、影響を受ける可能性のある資産を除く任意の列ヘッダーをクリックして実行できます。

The screenshot displays the 'Priority Bugs' section of a software management tool. On the left, a sidebar contains a 'Filters' section with a 'Severity' dropdown menu set to 'All'. Below the menu is a 'Clear All' button. The main area shows a table of bugs with columns for 'Bug ID', 'Severity', and 'Summary'. The table lists several bugs, including CSCwh39932 (Severity 6), CSCwd31302 (Severity 2), CSCwi43066 (Severity 3), CSCwi40943 (Severity 3), CSCwi52972 (Severity 2), CSCwi15483 (Severity 3), CSCwi23447 (Severity 2), CSCwi26553 (Severity 6), CSCwh99413 (Severity 4), and CSCwi23471 (Severity 2). On the right, a detailed view for bug CSCwh39932 is shown, including its severity (Sev 6), a description of the issue (N9300 fails to establish OSPF adjacency), affected assets (2), and a summary of the problem.

バグ詳細ビュー

- バグをクリックすると、次の内容を含むバグの詳細ビューが開きます。
 - Summaryタブ: Bug Severity、Description、およびApproverwayの詳細が表示されます。

Software Images Image Distribution Server **Advisories** Insights

Security Advisories

Priority Bugs

Filters

Severity

- All
- Sev 1
- Sev 2
- Sev 3
- Sev 4
- Sev 5
- Sev 6

Clear All

Priority Bugs 73 Total

Bug ID	Severity	Summary
CSCwh39932	6	N9300 fails to establish OSPF adjacency in
CSCwd31302	2	CIAM: Vulnerabilities in rpm 4.14.2 CVE-20
CSCwi43066	3	DOC: Update N9K SFlow documentation fo
CSCwi40943	3	/32 route is not getting installed in the RIB
CSCwi52972	2	Multicast traffic forwarding issues for rand
CSCwi15483	3	Interface UP without cable, only QSFP inter
CSCwi23447	2	Nexus 9504 unable to upgrade correctly fr
CSCwi26553	6	Web UI on 17.9.4 performance/response is
CSCwh99413	4	Console Logging for some XPATH Isco-IO
CSCwi23471	2	Evaluation of all for HTTP/2 Rapid Reset At

Sev 6

CSCwh39932 : N9300 fails to establish OSPF adjacency in non-vpc vlan with orphan port connected L3 device

Summary **Affected Assets (2)**

Below is the list of assets known to be affected by this security advisory. Expand to view the details.

2 Total Assets

Asset Name	Serial Number	Model Name	Version	Role	IP Address	Controller ID
CNXS-N93360YC-2		N9K-C93360YC-FX2	10.2(5)	border		NDFC-151
CNXS-N93360YC-1		N9K-C93360YC-FX2	10.2(5)	border		NDFC-151

1 Items per page 10

「影響を受ける資産」タブ

- 「影響を受ける資産」タブ：資産名、シリアル番号、モデル名、ソフトウェアバージョン、IP アドレス、コントローラIDなど、影響を受ける可能性のあるすべての資産の詳細を表示します。このタブでは、資産の並べ替えや検索を実行できます

Software Images Image Distribution Server **Advisories** Insights

Security Advisories

Priority Bugs

Filters

Severity

- All
- Sev 1
- Sev 2
- Sev 3
- Sev 4
- Sev 5
- Sev 6

Clear All

Priority Bugs 73 Total

Bug ID	Severity	Summary
CSCwh39932	6	N9300 fails to establish OSPF adjacency in
CSCwd31302	2	CIAM: Vulnerabilities in rpm 4.14.2 CVE-20
CSCwi43066	3	DOC: Update N9K SFlow documentation fo
CSCwi40943	3	/32 route is not getting installed in the RIB
CSCwi52972	2	Multicast traffic forwarding issues for rand
CSCwi15483	3	Interface UP without cable, only QSFP inter
CSCwi23447	2	Nexus 9504 unable to upgrade correctly fr
CSCwi26553	6	Web UI on 17.9.4 performance/response is
CSCwh99413	4	Console Logging for some XPATH Isco-IO
CSCwi23471	2	Evaluation of all for HTTP/2 Rapid Reset At

Sev 6

CSCwh39932 : N9300 fails to establish OSPF adjacency in non-vpc vlan with orphan port connected L3 device

Summary **Affected Assets (2)**

Below is the list of assets known to be affected by this security advisory. Expand to view the details.

2 Total Assets

Asset Name	Serial Number	Model Name	Version	Role	IP Address	Controller ID
CNXS-N93360YC-2		N9K-C93360YC-FX2	10.2(5)	border		NDFC-151
CNXS-N93360YC-1		N9K-C93360YC-FX2	10.2(5)	border		NDFC-151

1 Items per page 10

優先度の高いバグの表示

- 優先度の高いバグの表示リンク：公式のバグ検索ツールに移動します。

Assets

29 Total

Domain

Core

Campus

Data Center

Security

SD-WAN

Controller Type

Controller

ANSIBLE-156

NSO-183

ANSIBLE

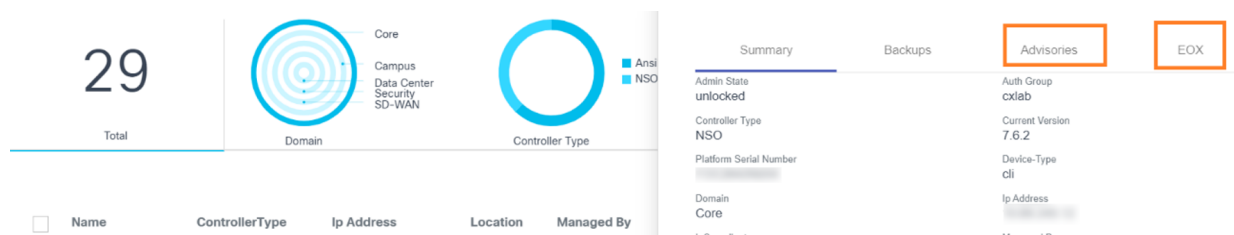
NSO

Filters

Name	ControllerType	Ip Address	Location	Managed By	Product Description	Product Family	Software Type	Software Version	Action
ASR9K-12	NSO			NSO-183		ASR9K	IOS-XR	7.6.2	
ASR9K-13	NSO			NSO-183	ASR9K-13	ASR9K	IOS-XR	7.6.2	
ASR9K-154	NSO			NSO-183		ASR9K	IOS-XR	7.6.2	
ASR9K-155	NSO			NSO-183		ASR9K	IOS-XR	7.7.2	
asr9k-154	NSO			NSO-183		ASR9K	IOS-XR	7.6.2	

資産

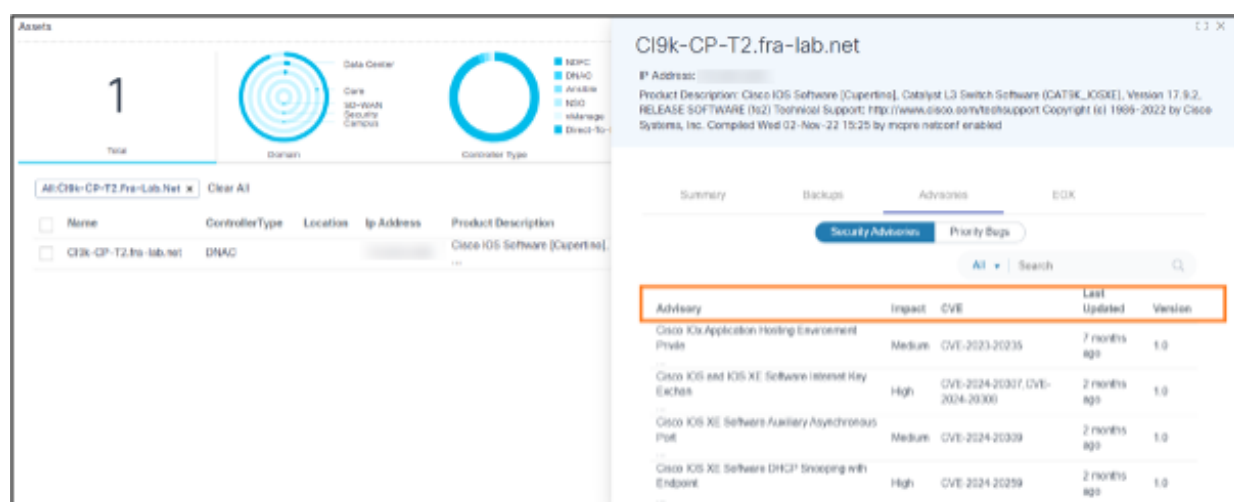
アセットマネージャでは、ユーザはすべてのアセットのリストを表示できます。アセットを選択すると、パネルにアセットレベルの情報が表示されます。この情報には、アドバイザリとEOXの2つのタブに分類されたアセットソフトウェアの脆弱性の詳細が含まれます。



アドバイザリとEOX

Advisoriesタブには、Security AdvisoriesとPriority Bugsの2つのサブタブがあります。これらのタブの詳細については、以下のセクションで説明します。

セキュリティ アドバイザリ



選択した資産のセキュリティアドバイザリ

Security Advisoriesサブタブで、ユーザは選択した資産に影響を与えるすべてのセキュリティアドバイザリを表示できます。セキュリティアドバイザリ表の列には、アドバイザリ、影響、CVE、最終更新日、およびバージョンが含まれます。



セキュリティアドバイザリ検索

Assets

1

Total

Domain

Controller Type

All:CI9k-CP-T2.fra-lab.net x Clear All

Name	ControllerType	Location	Ip Address	Product Description
CI9k-CP-T2.fra-lab.net	DNAC			Cisco IOS Software [Cupertino],

CI9k-CP-T2.fra-lab.net

IP Address:

Product Description: Cisco IOS Software [Cupertino], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 17.9.2, RELEASE SOFTWARE (fc2) Technical Support: <http://www.cisco.com/techsupport> Copyright (c) 1986-2022 by Cisco Systems, Inc. Compiled Wed 02-Nov-22 15:25 by mcpre netconf enabled

Summary Backups Advisories EOX

Security Advisories Priority Bugs

Impact Critical

Advisory	Impact	CVE	Last Updated	Version
Multiple Vulnerabilities in Cisco IOS XE Software	Critical	CVE-2023-20198,CVE-2023-20273	6 months ago	2.6

1 Items per page 10

セキュリティアドバイザリ検索 – 影響オプション

ユーザは、Advisories、Impact、CVE、Last Updated、およびVersion列の値に基づいてアドバイザリを検索できます。ページネーションを使用すると、ページ間を移動できます。

優先バグ

Assets

1

Total

Domain

Controller Type

All:CI9k-CP-T2.fra-lab.net x Clear All

Name	ControllerType	Location	Ip Address	Product Description
CI9k-CP-T2.fra-lab.net	DNAC			Cisco IOS Software [Cupertino],

CI9k-CP-T2.fra-lab.net

IP Address:

Product Description: Cisco IOS Software [Cupertino], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 17.9.2, RELEASE SOFTWARE (fc2) Technical Support: <http://www.cisco.com/techsupport> Copyright (c) 1986-2022 by Cisco Systems, Inc. Compiled Wed 02-Nov-22 15:25 by mcpre netconf enabled

Summary Backups Advisories EOX

Security Advisories Priority Bugs

All Search

Bug ID	Severity	Summary
CSCwd60753	4	CCO flow does not support forward slash in the pa

選択した資産に影響する優先度の高いバグ

Priority Bugsサブタブで、ユーザは特定の資産に影響を与える優先度のすべてのバグにアクセスできます。このタブのカラムには、Bug ID、Severity、Summaryがあります。

Assets

1

Total

Domain

Controller Type

All:CI9k-CP-T2.fra-lab.net x Clear All

Name	ControllerType	Location	Ip Address	Product Description
CI9k-CP-T2.fra-lab.net	DNAC			Cisco IOS Software [Cupertino],

CI9k-CP-T2.fra-lab.net

IP Address:

Product Description: Cisco IOS Software [Cupertino], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 17.9.2, RELEASE SOFTWARE (fc2) Technical Support: <http://www.cisco.com/techsupport> Copyright (c) 1986-2022 by Cisco Systems, Inc. Compiled Wed 02-Nov-22 15:25 by mcpre netconf enabled

Summary Backups Advisories EOX

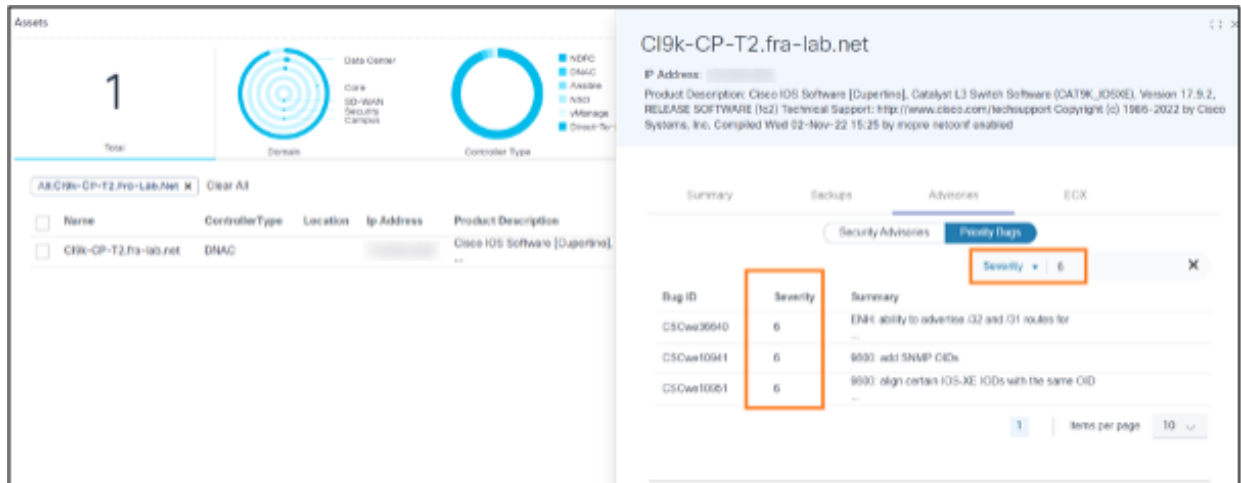
Security Advisories Priority Bugs

All 9800

Bug ID	Severity	Summary
CSCwe10941	6	9800: add SNMP OIDs
CSCwe10951	6	9800: align certain IOS-XE OIDs with the same OID

1 Items per page 10

サマリーによる優先度の高いバグ検索



重大度による優先度の高いバグ検索

ユーザは、Bug ID、Severity、およびSummary列の値に基づいて優先度の高いバグを検索できます。ページネーションを使用すると、ページ間を簡単に移動できます。

EOX



EOXタブ

EOXタブには、次の3つの重要な日付を含む、資産に固有のソフトウェアサポート終了データが表示されます。

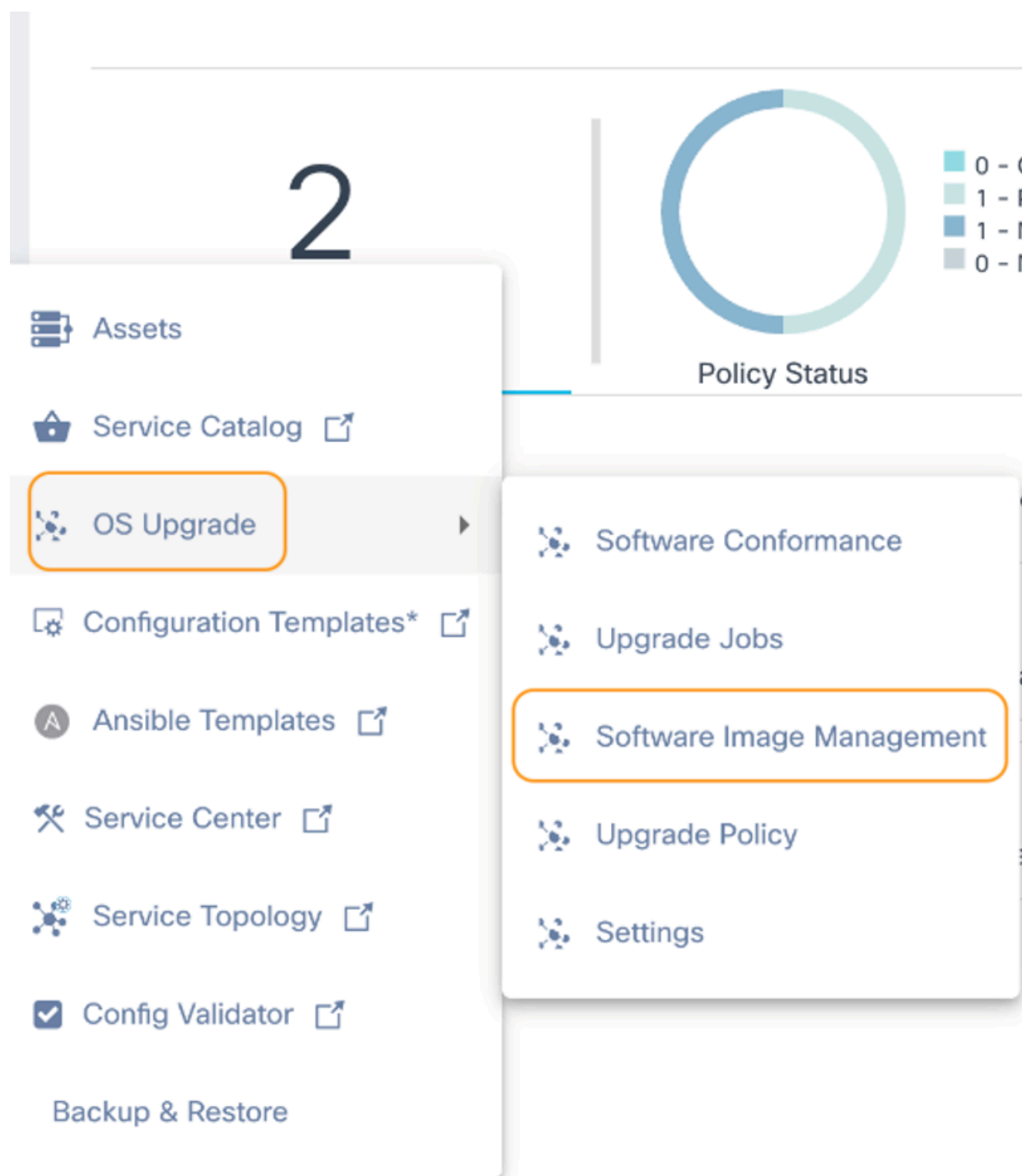
- ソフトウェアメンテナンスの終了
- セキュリティサポートの終了
- [サポート終了日 (Last Date of Support)]

ソフトウェアインサイトの表示

Software Insightsは、Cisco Catalyst CenterおよびNDFCコントローラによって管理されるデバイスモデルのソフトウェア候補を提供します。管理者ユーザは、候補が利用可能な場合に、デバイスモデルの準拠ポリシーを作成できます。

Software Insightsにアクセスするには：

1. Insightsへの管理アクセス権を持つクレデンシャルを使用してBPAにログインします。



ソフトウェア イメージの管理

2. 側面パネルからOS Upgrade > Software Image Managementの順に選択します。

Software Images

Image Distribution Server

Advisories

Insights

Filters

Suggestions

All

No

Yes

Clear All

24 Total Device Models

All

Search

Device Model	Product Family	Software Type	Current Releases	Selected Release	Assets	Suggestions	Action
WS-C3850-48P-E	Cisco Catalyst 3850 Series Ethernet Stackable Swi ...	IOS-XE	16.12.6		1	Yes	
N9K-C9300v	Data Center Switches	NX-OS	9.3(9)		7	No	
WS-C2960S-48FPD-L	Cisco Catalyst 2960-X/XR Series Switches	IOS	15.0(2)SE		1	Yes	
WS-C3750X-48PF-S	Cisco Catalyst 3750 Series Switches	IOS	15.2(4)E1		1	Yes	
C9300-24T	Cisco Catalyst 9300 Series Switches	IOS-XE	17.9.2		1	Yes	
C9800-CL-K9	Cisco Catalyst 9800 Wireless Controllers for Cloud	IOS-XE	17.9.2		1	Yes	
C9300-24UX	Cisco Catalyst 9300 Series Switches	IOS-XE	17.9.2		1	Yes	
N9K-C9364C-GX	Data Center Switches	NX-OS	9.3(10)		1	Yes	
C9500-24Y4C	Cisco Catalyst 9500 Series Switches	IOS-XE	17.9.2		1	Yes	
C9500-48Y4C	Cisco Catalyst 9500 Series Switches	IOS-XE	17.5.1		1	Yes	

1

2

3

Next

Items per page

10

「インサイト」タブ

3. Insightsタブをクリックします。

Insightsタブには次の情報が含まれます。

- ユーザが提案に基づいてデータをフィルタリングできるフィルタ。Allがデフォルトで選択されています。
 - Yesを指定すると、提案を含むデバイスモデルのデータがフィルタリングされます
 - Noは、提案のないデバイスモデルのデータをフィルタリングします

Software Images

Image Distribution Server

Advisories

Insights

Filters

Suggestions

☒ All

☐ No

☐ Yes

Clear All

29 Total Device Models

All

Search

Device Model

Product Family

Software Type

Current Releases

Selected Release

Assets

Suggest

Export to CSV

WS-C3850-48P-E

Cisco Catalyst 3850 Series Ethernet Stackable Swi

IOS-XE

16.12.6

1

No

C9500-48Y4C

Cisco Catalyst 9500 Series Switches

IOS-XE

17.5.1

1

No

N9K-C93180YC-EX

Data Center Switches

NX-OS

10.2(2)

2

No

N9K-C9500v

N9K

NX-OS

9.3(5)

1

No

WS-C4500X-32

Cisco Catalyst 4500-X Series Switches

IOS-XE

03.11.02.E

1

No

CSVにエクスポート

- More Optionsアイコンには、ページに表示されているデータをエクスポートするためのExport to CSVオプションがあります
 - Refreshアイコンをクリックすると、ページが更新され、選択したフィルタがクリアされます
 - 検索フィルタはデータの検索に使用され、次の排他的な検索フィルタが含まれます。
- All：すべての列を検索します(デバイスモデル、製品ファミリ、ソフトウェアタイプなど)。
- デバイスモデル：特定のデバイスモデル名のデータを検索します。
- 製品ファミリ：特定の製品ファミリ名でデータを検索します。
- ソフトウェア・タイプ：特定のソフトウェア・タイプ名のデータを検索します。
 - 既存のデバイスモデルは、次の列で表示されます。

- デバイスモデル：デバイスモデルの名前
- 製品ファミリ：デバイスモデルが属する製品ファミリの名前
- Software Type：デバイスモデルが属するソフトウェアタイプの名前
- Current Releases：デバイスモデルのインベントリに現在存在する一意のソフトウェアバージョンのリスト
- Selected Release：シスコが提供する提案の中からオプションバージョンとして選択された推奨リリースバージョン
- 資産：デバイスモデルの資産マネージャに存在する資産の数
- Suggestions：デバイスモデルで使用可能な候補について、YesまたはNoを表示します

Software Images Image Distribution Server Advisories **Insights**

Filters

Suggestions

☒ All
☐ No
☐ Yes

Clear All

24 Total Device Models

Device Model	Product Family	Software Type	Current Releases	Selected Release	Assets	Suggestions	Action
ASR1001-X	Cisco ASR 1000 Series Aggregation Services Routers	IOS-XE	17.9.2a,17.6.5		2	Yes	⋮
C9300-48U	Cisco Catalyst 9300 Series Switches	IOS-XE	17.9.2,17.6.4		4	Yes	⋮
N9K-C93600CD-GX	Data Center Switches	NX-OS	10.2(6)		1	Yes	⋮
C9500-40X	Cisco Catalyst 9500 Series Switches	IOS-XE	17.9.2		2	Yes	⋮
WS-C4500X-32	Cisco Catalyst 4500-X Series Switches	IOS-XE	03.11.02.E		1	No	⋮
C9300-48P	Cisco Catalyst 9300 Series Switches	IOS-XE	17.9.2,17.5.1		3	Yes	⋮
N9K-C93180YC-EX	Data Center Switches	NX-OS	9.3(10),10.2(2)	10.2(6)	4	Yes	⋮
N9K-C93180YC-FX	Data Center Switches	NX-OS	9.3(10),9.3(7)		2	Yes	⋮
WS-C3750X-48PF-L	Cisco Catalyst 3750 Series Switches	IOS	15.2(4)E10		1	Yes	⋮
ASR1002-X	Cisco ASR 1000 Series Aggregation Services Routers	IOS-XE	17.6.5,17.9.3a		2	Yes	⋮

Prev 1 2 3 Next Items per page 10

候補ナビゲーションの表示

- Action: More Optionsアイコンを使用して、行固有のアクションを指定します(例：View Suggestions、View Assets)。



注：デバイスモデルに提案がない場合、「View Suggestions」は無効になります。

ベンダーが推奨するソフトウェアバージョンの表示と選択

Software Images
Image Distribution Server
Advisories
Insights

Filters

Suggestions

- All
- No
- Yes

Clear All

24 Total Device Models

Device Model	Product Family
ASR1001-X	Cisco ASR 1000 Series Aggregation Services Routers
C9300-48U	Cisco Catalyst 9300 Series Switches
N9K-C93600CD-GX	Data Center Switches
C9500-40X	Cisco Catalyst 9500 Series Switches
WS-C4500X-32	Cisco Catalyst 4500-X Series Switches
C9300-48P	Cisco Catalyst 9300 Series Switches
N9K-C93180YC-EX	Data Center Switches
N9K-C93180YC-FX	Data Center Switches
WS-C3750X-48PF-L	Cisco Catalyst 3750 Series Switches
ASR1002-X	Cisco ASR 1000 Series Aggregation Services Routers

Device Model : N9K-C93600CD-GX
Product Family : Data Center Switches

Suggestions
Affected Assets (1)

? Select one of the Cisco suggested software releases as the standard or policy while taking into consideration known issues and any workaround
Last Suggestion Date :Dec 20, 2023

Release Version & Date	CURRENT	OPTIMAL - 1
	10.2(6) Sep 1, 2023 Release Notes	10.2(6) Sep 1, 2023 Release Notes
Conformance Policy		Create
Bugs	Current Exposure : 7 sev1 0 sev2 1 sev3 4 sev4 1 sev5 0 sev6 1	Future Exposure : 7 sev1 0 sev2 1 sev3 4 sev4 1 sev5 0 sev6 1
Security Advisories	Current Exposure : 0 Critical 0 High 0 Informational 0 Low 0 Medium 0	Future Exposure : 0 Critical 0 High 0 Informational 0 Low 0 Medium 0
EoX	End of SW Maintenance Nov 30, 2023 End of Security Support Feb 28, 2025 Last date of Support Aug 31, 2025	End of SW Maintenance Nov 30, 2023 End of Security Support Feb 28, 2025 Last date of Support Aug 31, 2025

[修正候補]タブ

Action列でMore Optionsアイコン> View Suggestionsを選択すると、サイドパネルが開いて洞察の詳細がすべて表示されます。Suggestionsタブには、選択したデバイスモデルの現在のリリース情報と推奨リリース情報が表示されます。1つのデバイスモデルに複数の推奨リリースがある場合があります。次のデータを使用できます。

- リリースバージョンと日付：シスコクラウドで利用可能な現在および推奨リリースのリリースバージョン、日付、およびメモの詳細が表示されます。インベントリのアセットが複数のバージョンに属する場合、適用可能なすべてのバージョンがカンマ区切り値として現在の列に表示されます
- Create Conformance Policy：管理者は、デバイスロールをAnyとして持つ特定のバージョンの準拠ポリシーを作成できます。

 注：準拠ポリシーの作成は、NDFCコントローラデバイスモデルでのみサポートされています

Device Model : N9K-C93180YC-EX
Product Family : Data Center Switches

Suggestions

Affected Assets (4)

Select one of the Cisco suggested software releases as the standard or policy while taking into consideration known issues and any workaround

Last Suggestion Date :Dec 20, 2023

Release Version & Date	CURRENT 9.3(10),10.2(2) Dec 16, 2021 Release Notes	OPTIMAL - 1 10.2(6) Sep 1, 2023 Release Notes
Conformance Policy		Insights-policy-for-N9K-C93180YC-EX Created On : Dec 20, 2023

ポリシーの削除オプション

注：デバイスモデルにポリシーがすでに存在する場合、エラーが表示されます。ポリシーが存在しない場合、ポリシーはEnabled状態で作成されます。Insightsからポリシーを作成した場合、ユーザーはポリシーを削除するオプションを選択できます。

- Bugs：各リリースの統合バグ数を表示
- セキュリティアドバイザリ：各リリースの統合アドバイザリ数を表示します
- EoX：各リリースのソフトウェアメンテナンス終了日、セキュリティサポート終了日、サポート終了日が表示されます。

Device Model : N9K-C93360YC-FX2
Product Family : Data Center Switches

Suggestions

Affected Assets (2)

2 Total Assets

All ▾ | Search

Asset Name	Serial Number	Model Name	Version	Role	IP Address	Controller ID
CNXS-N93360YC-2		N9K-C93360YC-FX2	10.2(5)	border		NDFC-151
CNXS-N93360YC-1		N9K-C93360YC-FX2	10.2(5)	border		NDFC-151

1 | Items per page 10 ▾

「影響を受ける資産」タブ

More Optionsアイコン> View AssetsをAction列から選択すると、サイドパネルが開いて、デフォルトでAffected Assetsタブが表示されます。「影響を受ける資産」タブでは、資産名、シリアル番号、モデル名、ソフトウェアバージョン、IPアドレス、コントローラIDなどの列に、影響を受ける可能性のある資産の詳細が表示されます。このタブでは、アセットの並べ替えと検索を実行できます。

ソフトウェアアップグレードが必要なデバイスの特定

詳細は、『[ソフトウェア準拠](#)』を参照してください。

ソフトウェアの適合性

ソフトウェアコンFORMANCEは、対象ソフトウェアバージョンに準拠していないネットワーク内のアセットを特定するのに役立ちます。検証は、ソフトウェアコンFORMANCEのインテントを定義するポリシーとルールに基づいて行われます。これらのポリシーは、スケジュールに基づいて、またはオンデマンドで実行できます。適合性ポリシーが正常に実行されると、適合結果が取得され、該当する資産のステータスが示されます。適合範囲は、デバイスの役割、コントローラインスタンスの管理などのさまざまな基準に依存します。

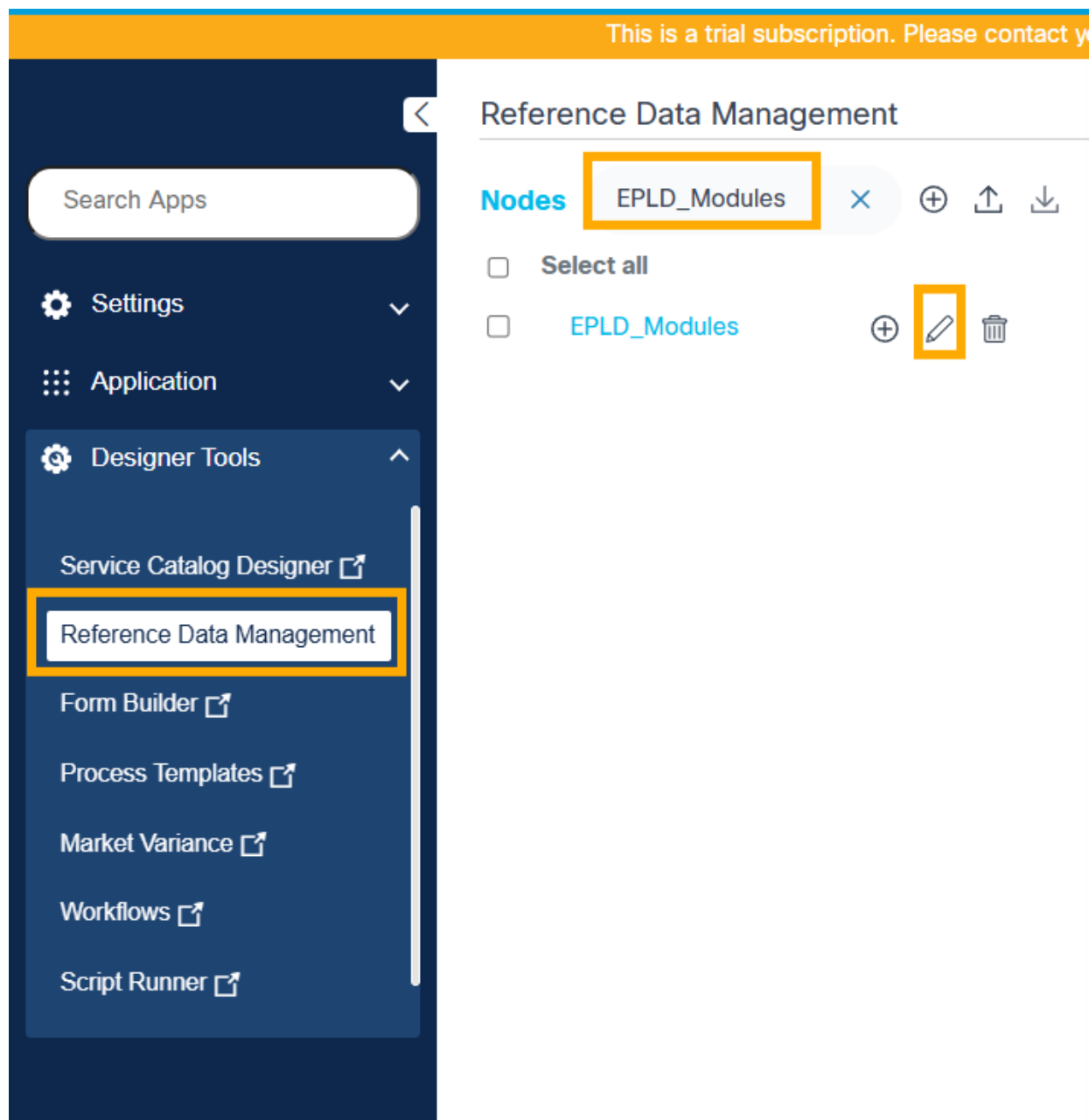
前提条件

- Cisco Catalyst Center、vManage、NDFC、FMCなどのコントローラのソフトウェアイメージは同期している必要があります。詳細については、『[ソフトウェアイメージのメタデータの同期](#)』を参照してください。
- NSO、CNC、Direct-to-Device、ANSIBLEなどのコントローラに必要なソフトウェアイメージメタデータを追加する必要があります。詳細は、『[ソフトウェアイメージメタデータの追加](#)』を参照してください。
- EPLDモジュール・データを管理するには、RefDアプリケーションへのアクセス権が必要です。
- 必須リリースのEPLDモジュール情報は、RefDアプリケーションにあらかじめ入力されている必要があります
- EPLDモジュール情報がOOBで使用できない場合、ユーザーはEPLDモジュール情報を手動でRefDアプリケーションに追加する必要があります

参照データ管理アプリケーションでのEPLDモジュール・データの作成

準拠ポリシーを作成する前に、RefDアプリケーションでEPLDモジュール参照データを作成します。RefDアプリケーションには、Nexusソフトウェアバージョンv10.2(8)およびv10.4(5)のEPLDモジュール情報がそれぞれ含まれています。その他のデバイスバージョンでは、EPLDモデル情報をRefDアプリケーションに手動で追加する必要があります。

EPLDモジュールのメタデータに他のリリースを追加するには、次の手順を実行します。



参照データ管理

1. Reference Data Managementアプリケーションに移動し、「EPLD_Modules」を検索します。
2. 「EPLD_Modules」ファイルを選択し、編集アイコンを選択します。

Edit Node

Name* EPLD_Modules

Data Source* Internal

Data Type* JSON

☐ Protected data

```
1 {
2   "N9K-C92348GC-X": {
3     "10.5(2)": [
4       {
5         "Module": "IOFPGA",
6         "Version": "0x15",
7       }
8     ],
9     "10.5(1)": [
10      {
11        "Module": "IOFPGA",
12        "Version": "0x15",
13      }
14    ],
15  },
16  "N9K-C93108TC-EX": {
17    "10.5(2)": [
18      {
19        "Module": "IOFPGA",
20        "Version": "0x15",
21      }
22    ],
23  },
24 }
```

EPLD_Modules.json

Cancel Save Upload Download

ノードの編集

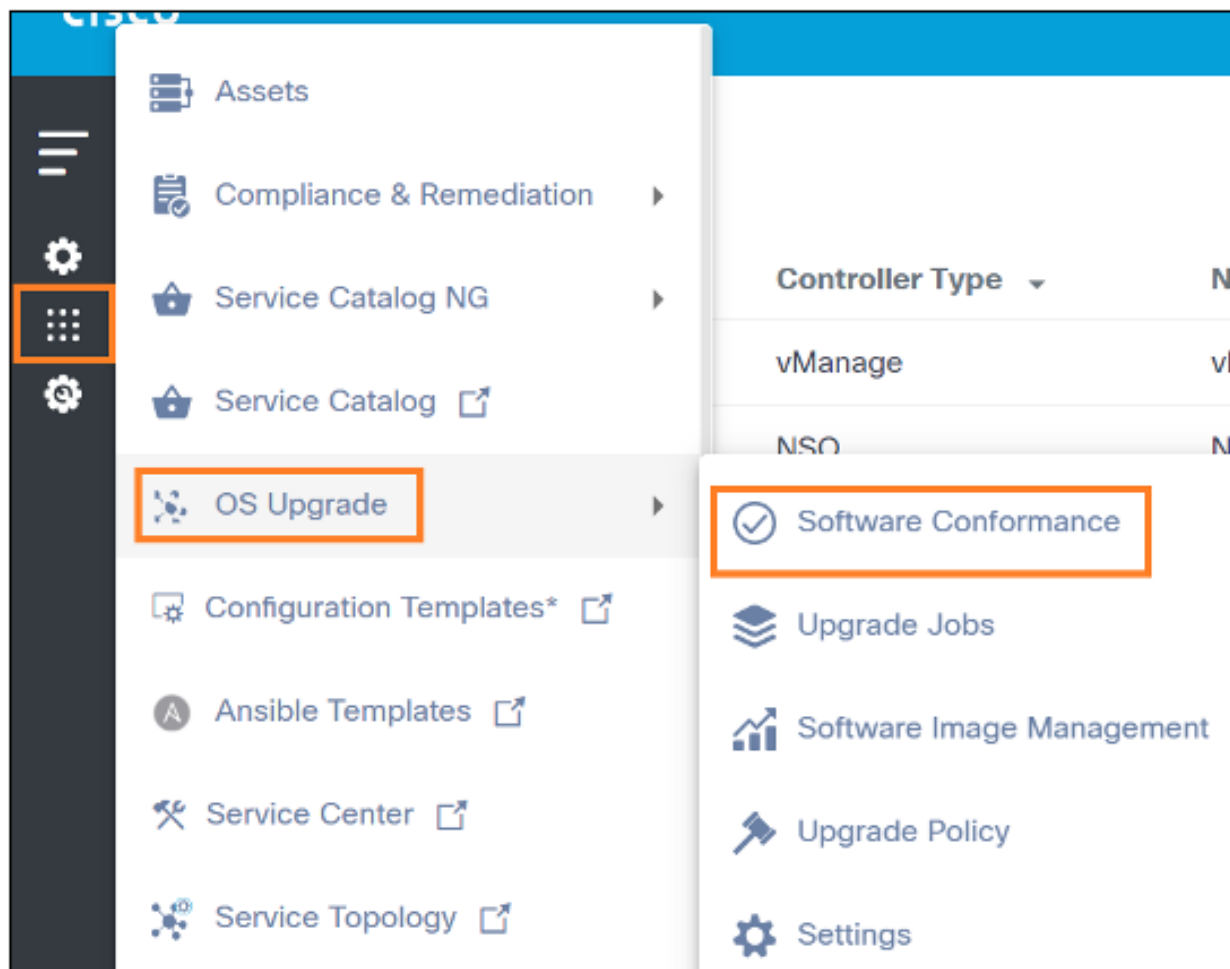
3. 次の構造を持つ新しいエントリを追加して、新しいリリースのEPLDモジュールメタデータを追加します。

```
structure:
  "N9K-C92348GC-X": {
    "10.5(2)": [
      {
        "Module": "IOFPGA",
        "Version": "0x15"
      }
    ]
  }
}
```

4. Saveをクリックし、準拠ポリシーで選択可能な新しいEPLDモジュールメタデータを検証します。サポートされているリリースのEPLDデータは事前に入力されています。

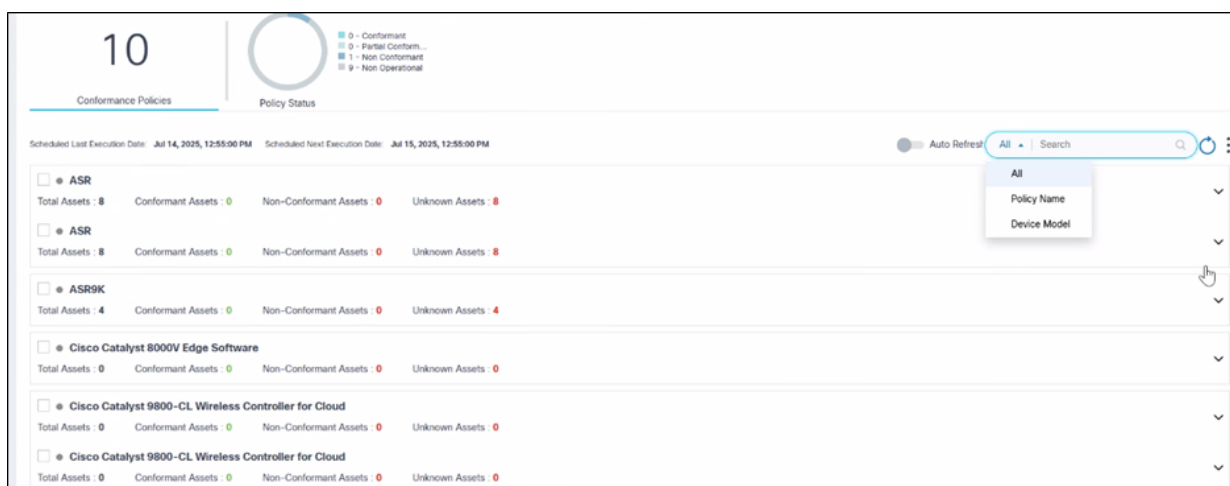
ソフトウェア適合性の表示と管理

1. ソフトウェアコンフォーマンスにアクセスできるクレデンシャルでBPAにログインします。



ソフトウェア適合性ナビゲーション

2. OS Upgrade > Software Conformanceの順に選択します。Software Conformanceページが表示されます。



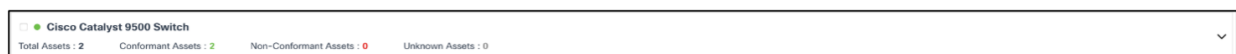
ソフトウェアの適合性

「ソフトウェア準拠」ページには次の情報が含まれます。

- 上部に表示される分析セクションには、次の情報が含まれます。

- 。システム内に存在する準拠ポリシーの合計数
- 。ポリシーステータスの簡易フィルタ：次の基準に基づいてフィルタリングします。
 - 。適合：指定されたモデルのBPA管理対象デバイスはすべて、定義されたソフトウェアバージョン上にあります
 - 。部分的な適合：モデルが指定された一部のBPA管理対象デバイスは、定義済みのソフトウェアバージョン上にあります。残りのデバイスは異なるソフトウェアバージョンにあります
 - 。非適合：指定されたモデルを持つすべてのBPA管理対象デバイスは、特定のソフトウェアバージョンと比較すると異なるソフトウェアバージョンにあります
 - 。Non-Operational：ポリシーで指定されたデバイスモデルに基づく該当デバイスが見つかりません
- 。計画最終実行日および計画次実行日。以前に実行された計画適合性チェックの日時、および次の計画適合性チェックがすべてのポリシーに対して実行される日時を示します
- 。検索フィールド。デバイスモデル、ポリシー名、またはすべてのパラメータに基づいてポリシーをフィルタリングするために使用します。ユーザはすべてを選択してすべてのパラメータを検索できます
- 。自動更新切り替えを有効にすると、ユーザー定義の間隔で進行中の準拠ポリシーを自動的に更新できます。切り替えを有効にするには：
 - 。OS Upgrade > Settingsの順に選択して、更新間隔を変更します
 - 。自動リフレッシュ間隔を必要な値に変更します
 - 。[Save] をクリックします。
- 。Auto Refresh切り替えが有効になっている場合、ソフトウェア適合性ポリシーダッシュボードは新しい間隔で更新されます
- 。Refreshアイコン：ページを更新し、選択したフィルタをクリアします。
- 。次のオプションを示すその他のオプションアイコン。
 - 。ポリシーの作成
 - 。すべてのポリシーを実行
 - 。選択した複数のポリシーの削除

ポリシーはデバイスモデルに基づいてグループ化され、展開可能なパネルとして表示されます。これにより、異なるコントローラで管理されているデバイスモデル全体を1つのビューで表示できます。



準拠ポリシーの折りたたみビュー

折りたたまれたビューでは、パネルにデバイスモデルと、Total Assets、Conformant Assets、Non-Conformant Assets、Unknown Assetsなどの簡単な統計が表示されます。

Cisco Catalyst 9500 Switch								
Total Assets : 2			Conformant Assets : 2		Non-Conformant Assets : 0		Unknown Assets : 0	
Name	Region	Device Role	Target Version	Created By	Created On	Executed On	State	Action
Cat 9500	Global	All	17.06.04	admin	May 8, 2023, 5:19 PM	May 8, 2023, 5:41 PM	enabled	⋮
							1	Items per page 10

準拠ポリシーの拡張ビュー

展開されたビューには、デバイスモデルに関連するすべてのポリシーが表示されます。各ポリシーに対して、実行、ポリシーの編集、結果の表示などの追加のアクションを実行するには、アクション列からその他のオプションアイコンを選択します。

ソフトウェア準拠ポリシーの作成

1. ソフトウェアコンFORMANCEへの管理アクセス権を持つクレデンシャルを使用してBPAにログインします。
2. OS Upgrade > Software Conformanceの順に選択します。Software Conformanceページが表示されます。

10

0 - Conformant

0 - Partial Conformant

1 - Non Conformant

9 - Non Operational

Conformance Policies

Policy Status

Scheduled Last Execution Date: Jul 14, 2025, 12:55:00 PM

Scheduled Next Execution Date: Jul 15, 2025, 12:55:00 PM

Auto Refresh

All

Search

ASR

Total Assets : 8

Conformant Assets : 0

Non-Conformant Assets : 0

Unknown Assets : 8

ASR

Total Assets : 8

Conformant Assets : 0

Non-Conformant Assets : 0

Unknown Assets : 8

ASR9K

Total Assets : 4

Conformant Assets : 0

Non-Conformant Assets : 0

Unknown Assets : 4

Cisco Catalyst 8000V Edge Software

Total Assets : 0

Conformant Assets : 0

Non-Conformant Assets : 0

Unknown Assets : 0

Cisco Catalyst 9800-CL Wireless Controller for Cloud

Total Assets : 0

Conformant Assets : 0

Non-Conformant Assets : 0

Unknown Assets : 0

Create Policy

Delete

Run All

ポリシーの作成

3. More Optionsアイコン> Create Policyを選択します。

ポリシーフォームの作成

4. Policy Name、Device Model(s)、Target Version、SMU、EPLD、Device Role、Asset Groups、およびAdditional Conformance Check Templateの各フィールドに情報を入力します。SMU(s)、Asset Group(s)、およびAdditional Conformance Check Templateはオプションのフィールドです。

注：ユーザはCreate Conformance Policyフォームで複数のデバイスモデルを選択できるようになりました。

注：ソフトウェア準拠フレームワークは、ベースOSバージョンで準拠チェックを実行し、デバイスを管理する特定のモデル、ロール、またはコントローラインスタンスのデバイスに対してSMUパッチを適用できます。その他のカスタムチェックが必要な場合は、必要なコマンドと検証ルールを含むプロセステンプレートを作成できます。これらのコマンドと検証ルールは、「Additional Conformance Check Template」フィールドにマッピングできます。

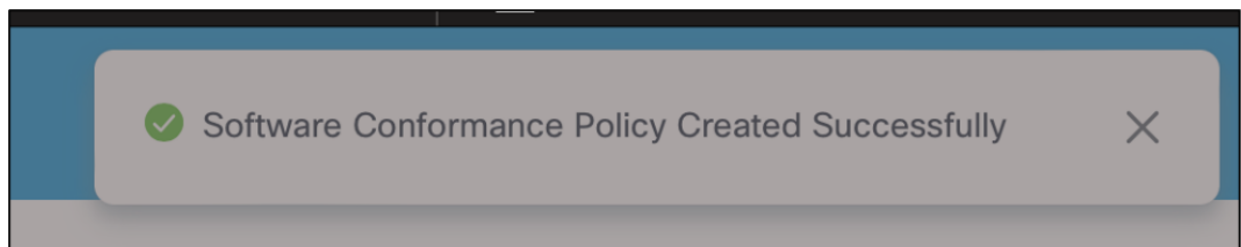
5. [Create] をクリックします。確認が表示されます。

注：次のリストに注意してください。

- ・ ユースケース管理者は、選択したデバイスモデルに対して、異なるデバイスロールを持つ複数のポリシーを柔軟に作成できます。1つのポリシーで複数のロールを選択できます。
- ・ Device Role(s)ドロップダウンリストからAnyを選択すると、その他すべてのデバイスロール (Access、Coreなど) が無効になります。他のデバイスロールが選択されている場合、Anyは無効になります。
- ・ CNC、NSO、ANSIBLE、Direct-to-Deviceなどのコントローラによって管理されるデバイスでは、デバイスにロール情報がないため、Anyロール(Device Role(s)ドロップダウンリストから選択)を使用してコンプライアンスチェックを実行できます。
- ・ FMCのDevice Role(s)ドロップダウンリストからAnyを選択すると、スタンドアロンデバイ

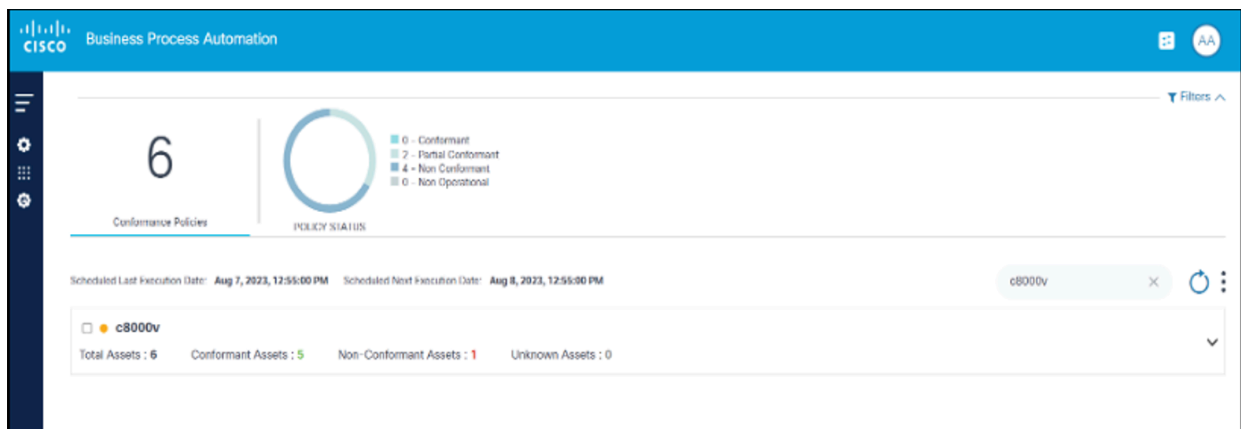
ス、コントロールデバイス、データデバイスを含むすべてのデバイスでソフトウェアへの準拠が実行されます。

- SMUの準拠とアップグレードは、CNC、NSO、ANSIBLE、FMC、Direct-to-Device、およびNDFCコントローラでのみサポートされます。
- このリリースでは、RegionドロップダウンリストのGlobalのみがサポートされています
- ユーザは、ドロップダウンリストから資産グループを選択できます。Allがデフォルトで選択されています。ユーザーは、1つ以上の資産グループを選択できます。特定の資産グループを選択すると、選択した資産グループのデバイスに対してのみポリシーが実行されます。
- Device Model、Target Version、およびSMU(s)フィールドに予期される値が表示されない場合、Discover Imagesをクリックして再試行します。
- Device Model、Asset Group(s)、およびRoleの各フィールドは連携して一意のポリシーを形成します。ポリシーが重複して設定されることはありません。
- EPLDフィールドに値が入力されるのは、選択されたデバイスモデルとターゲットバージョンでEPLDイメージメタデータが使用可能な場合だけです。
- ポリシー名は一意であり、重複するポリシー名は許可されません。



適合性ポリシーの作成の確認

- OS Upgrade Next Generation(Next-Gen)にタグ付けされたプロセステンプレートが、Additional Conformance Check Templateフィールドに表示されます。



準拠ポリシーの検索結果

6. Searchフィールドにデバイスモデルを入力して、作成したポリシーを検索します。

The screenshot displays the Cisco Business Process Automation interface. On the left, a list of policies is shown, including 'ASR9K', 'N9K-C93180YC-FX', and 'N9K-C93360YC-FX2'. The right pane shows the details for the 'Multi-Model-Policy-Demo' policy. The policy is named 'Multi-Model-Policy-Demo', is in the 'Global' region, and has a target version of '10.2.5'. The device model is 'N9K-C93180YC-FX', and the controller ID is 'NDFC-OS'. The policy is currently 'Enabled'. Below the policy details, there is a search bar and a 'No Record Found' message.

適合性ポリシーの表示

7. Policyをクリックして、ポリシーの詳細ビューを表示します。

オンデマンドでのソフトウェア適合性チェックの実行

1. 実行アクセス権を持つクレデンシャルでBPAにログインします。
2. OS Upgrade > Software Conformanceの順に選択します。Software Conformanceページが表示されます。

The screenshot shows the Cisco Business Process Automation interface with the 'Software Conformance' page selected. The page displays a 'Conformance Policies' section with a large number '9' and a 'POLICY STATUS' section with a donut chart showing the status of policies: 1 - Conformant, 1 - Partial Conformance, 5 - Non Conformance, and 2 - Non Operational. Below the status section, there is a search bar with the text 'N9K' and a list of policies. The policies listed are 'N9K-C93360YC-FX2' and 'N9K-C9336C-FX2'. The 'N9K-C93360YC-FX2' policy has 2 total assets, 0 conformant assets, 2 non-conformant assets, and 0 unknown assets. The 'N9K-C9336C-FX2' policy has 1 total asset, 1 conformant asset, 0 non-conformant assets, and 0 unknown assets.

ポリシー検索

3. Searchフィールドを使用して、オンデマンドで実行するポリシーを検索します。

1

Conformance Policies

Policy Status

0 - Conformant
1 - Partial Conformant
0 - Non Conformant
0 - Non Operational

Scheduled Last Execution Date: Apr 25, 2024, 12:55:00 PM Scheduled Next Execution Date: Apr 26, 2024, 12:55:00 PM

Search Device M...

Run

View Results

Edit

Delete

ASR9K

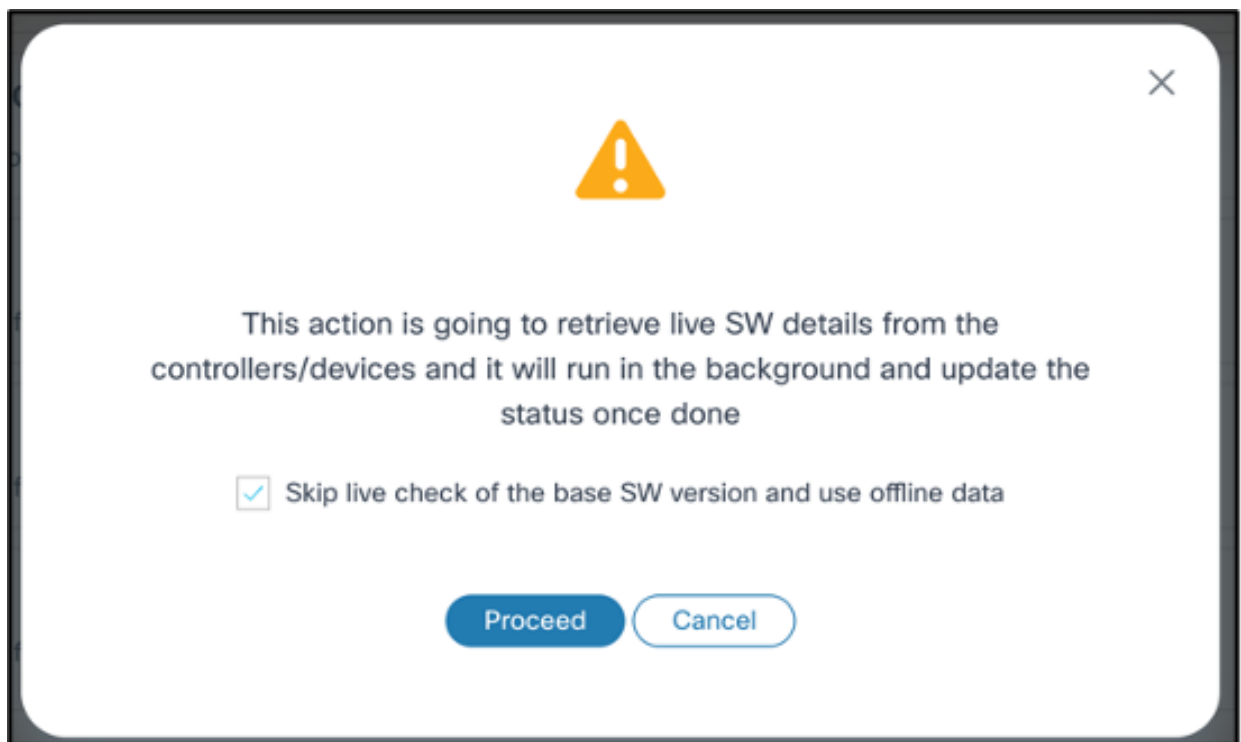
Total Assets : 13 Conformant Assets : 4 Non-Conformant Assets : 9 Unknown Assets : 0

Name	Region	Device Roles	Target Version	Created By	Created On	Executed On	Execution Status	Policy Status
ASR9k	Global	Any	7.7.2	admin	Apr 24, 2024, 7:57 PM	Apr 25, 2024, 12:55 PM	Completed	Partial Conformant

1 Items per page 10

RUN

- ポリシーのAction列から、More Options > Runの順に選択します。デバイスに対してライブインベントリチェックを実行する必要があるかどうかを検証するための確認が表示されます。



準拠ポリシーの実行の確認

- 準拠チェックを実行する前にライブインベントリの同期が必要な場合は、ベースソフトウェアバージョンのライブチェックをスキップしてオフラインデータを使用するチェックボックスをオフにして、続行をクリックします。この場合、適合性チェックは同期後にのみ実行されます。右上隅に通知が表示されます。



Software Conformance policy execution initiated



適合性ポリシー実行の通知



注：次のリストに注意してください。

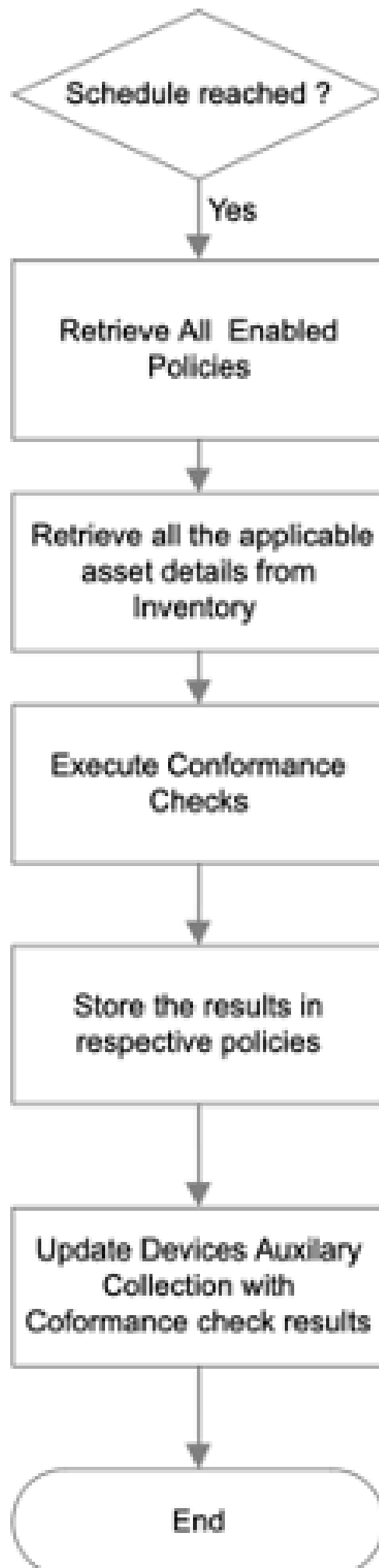
- 準拠チェックは、デフォルトで資産在庫データを使用して実行されます。
- このプロセス中にインベントリまたはデバイスの同期が失敗すると、それぞれのポリシーデバイスが不明としてマークされ、SMUチェックはスキップされます。
- SMUの場合、適合チェックを実行する前にデバイスからリアルタイムデータが取得され、「ベースソフトウェアバージョンのSkip Live Check」および「オフラインデータを使用」チェックボックスが選択されているかどうかチェックされます。
- ポリシーに複数のデバイスモデルが含まれている場合、デバイスモデルに対してポリシーを実行すると、関連付けられているすべてのポリシーの実行が開始されます。

ソフトウェア適合性チェックの実行のスケジューリング

ソフトウェア適合性チェックは、スケジューラサービスを使用して定期的に自動的に実行できます。スケジュール済み準拠チェックを実行するように設定できます。

- 日次
- 1日2回
- 毎週
- 1度

スケジュールに達すると、Enabled状態のすべてのポリシーが自動的に実行され、適合結果が各ポリシーに保存されます。

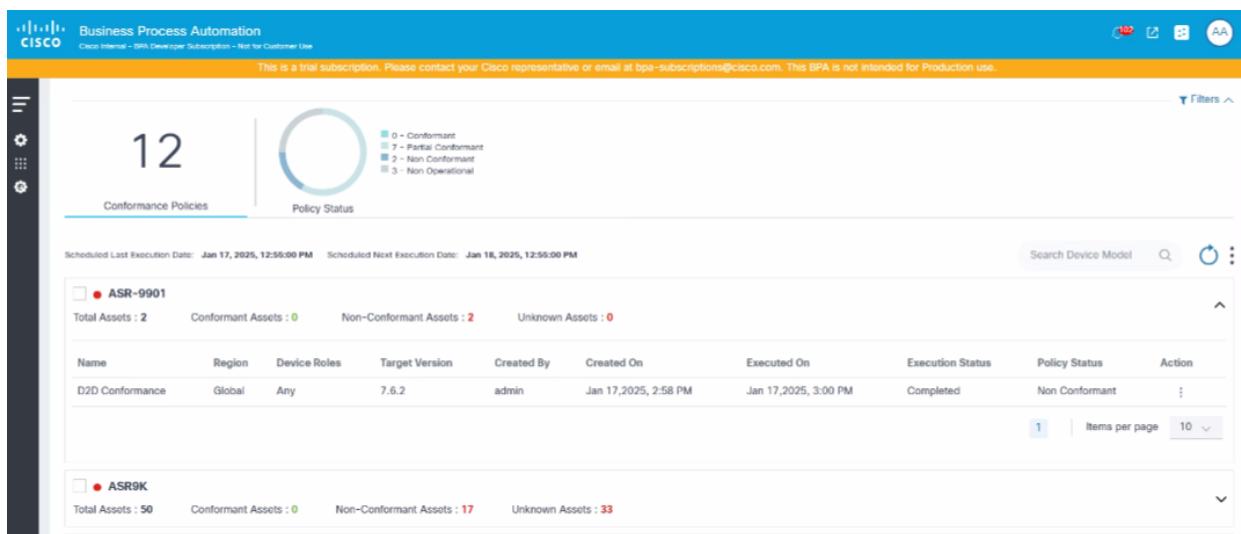


ソフトウェア適合性チェックのコールフローの実行スケジュール

詳細は、『[ソフトウェア準拠](#)』を参照してください。

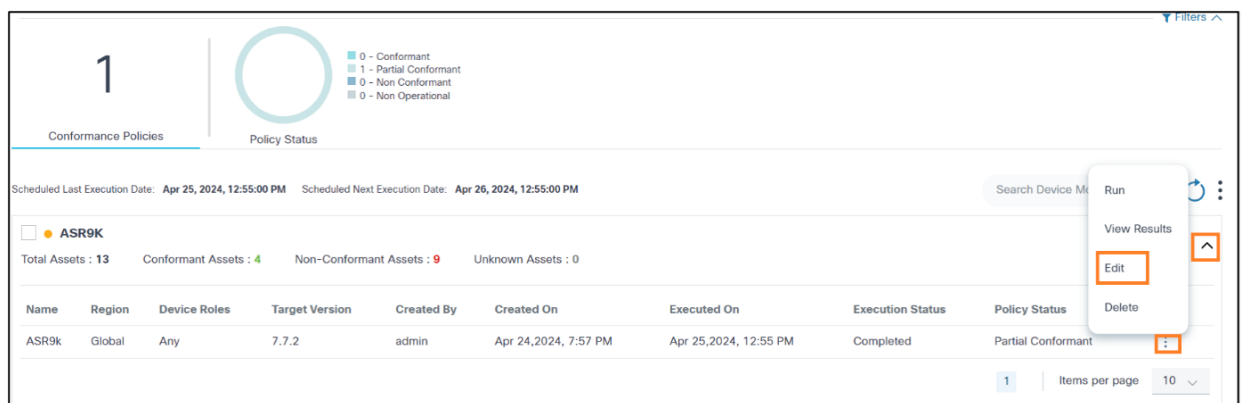
ソフトウェア準拠ポリシーの更新

1. ソフトウェアコンフォーマンスの管理アクセス権を持つクレデンシャルでBPAにログインします
2. OS Upgrade > Software Conformanceの順に選択します。Software Conformanceページが表示されます。



ソフトウェアの適合性

3. Searchフィールドを使用して、目的のポリシーを見つけます。



編集

4. ポリシーのAction列から、More Optionsアイコン> Editを選択します。

All > N9K-C93180YC-FX > Multi-Model-Policy-Demo Sync Images

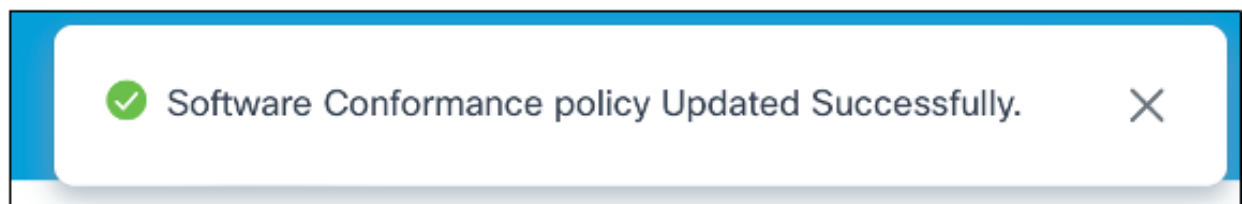
Policy Name*	Device Model*	Target Version*	SMU(s)
Multi-Model-Policy-Demo	N9K-C93180YC-FX, N9K-C93360YC-FX2 ✓	10.2.5	Select option(s)
Region*	Device Role(s)*	Controller ID(s)	Additional Conformance Check Template
Global	Any ✓	NDFC-OS	Select option

State
☒ Enable

Cancel Save

詳細が入力された準拠ポリシーの編集

- 必要に応じて、Target Version、SMU、Device Roles、Controller ID、Policy State、および Additional Conformance Check Template フィールドを編集します。
- [Save] をクリックします。確認が表示されます。

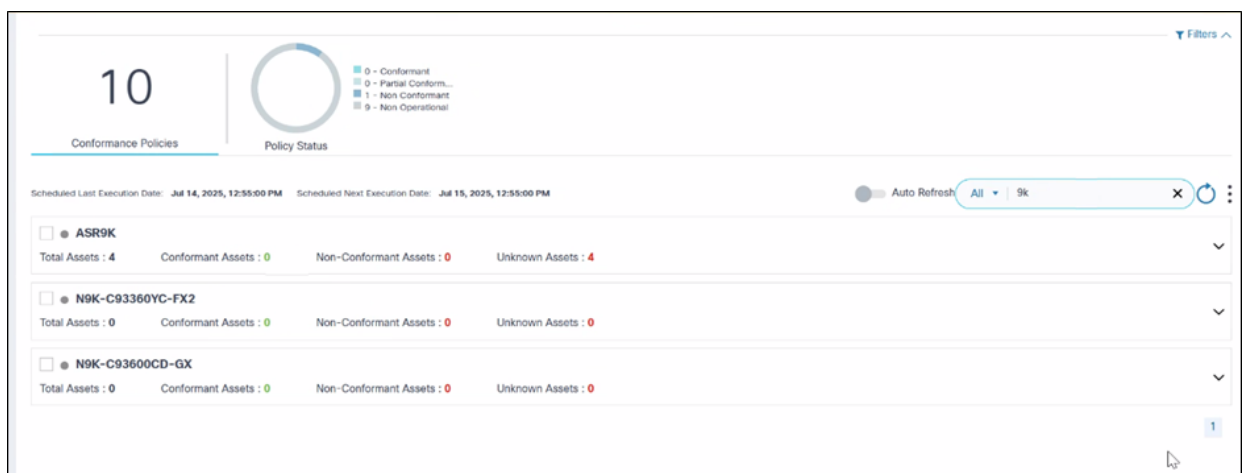


更新の成功の確認

 注：ソフトウェアコンFORMANCEポリシーが進行中のアップグレードジョブに使用される場合、ポリシーは編集できません。

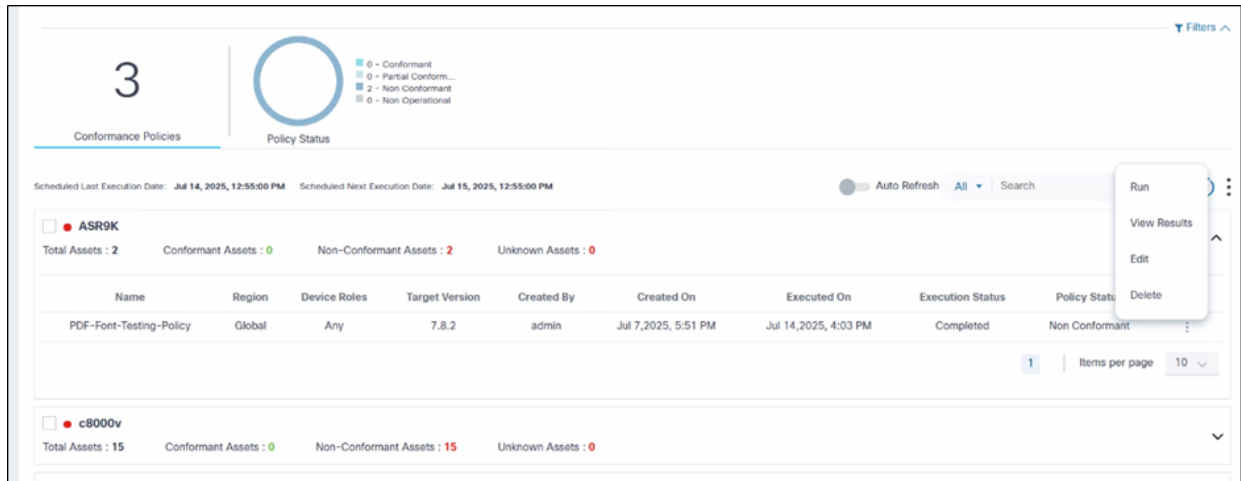
ソフトウェアコンFORMANCEポリシーの削除

- 管理アクセス権を持つクレデンシャルでBPAにログインします。
- OS Upgrade > Software Conformanceの順に選択します。Software Conformanceページが表示されます。



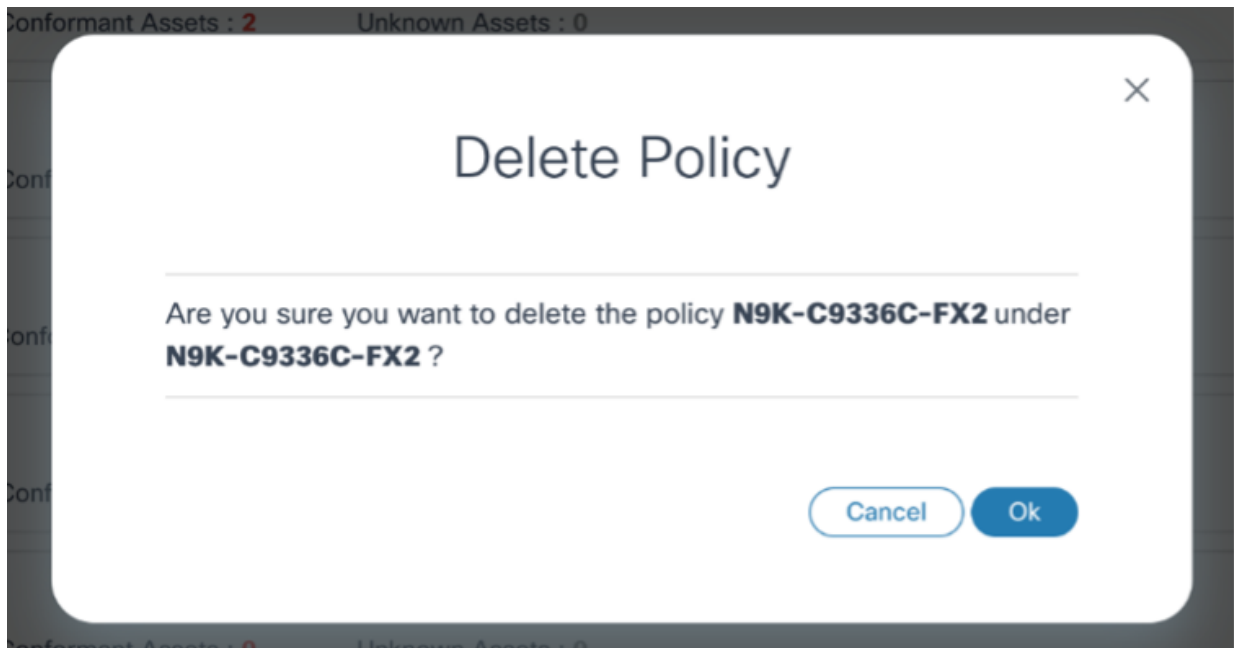
準拠ポリシーの検索結果

- Search フィールドを使用して、目的のポリシーを見つけます。

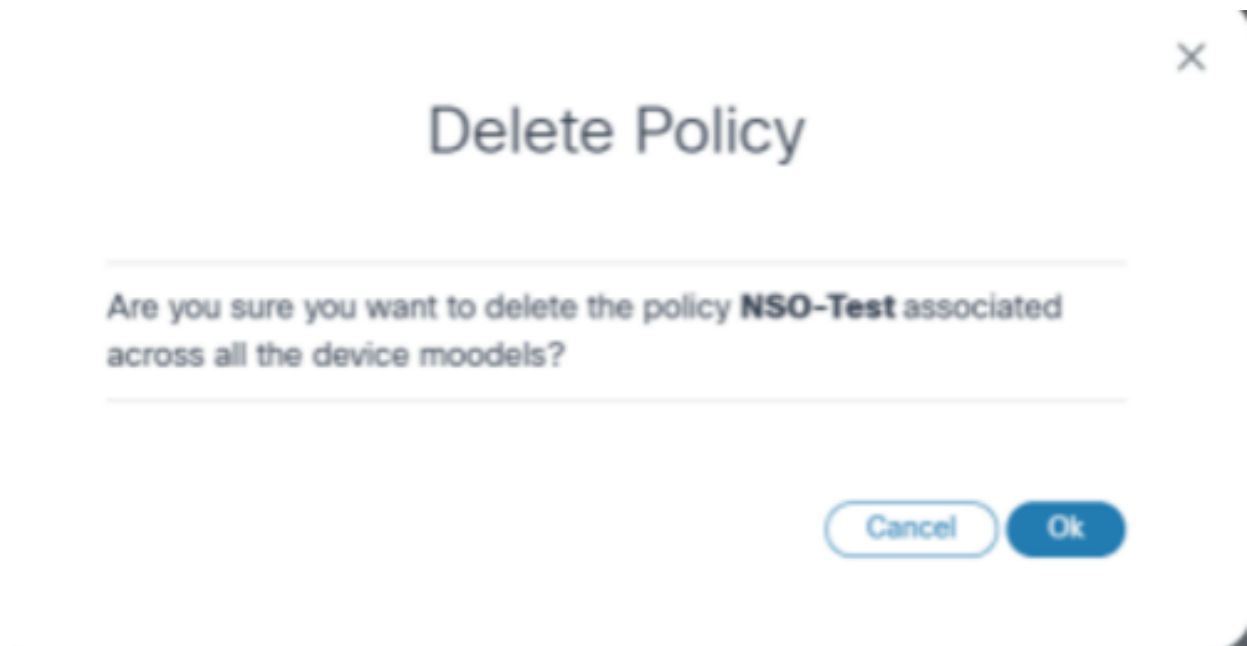


[削除 (Delete)]

4. ポリシーのAction列から、More Optionsアイコン> Deleteを選択します。確認ウィンドウが開きます。



ポリシーの削除の確認



ポリシーの削除の確認（ポリシーが複数のモデルに関連付けられている場合）

5. [OK] をクリックします。ポリシーが削除されます。

 注：次のリストに注意してください。

- ポリシーが複数のデバイスモデルに関連付けられている場合、ポリシーを削除すると、関連付けられている各モデルの関連ポリシーがすべて削除されます。
- ソフトウェアコンFORMANCEポリシーが進行中のアップグレードジョブに使用されている場合、ポリシーは削除できません。

適合結果の表示およびダウンロード

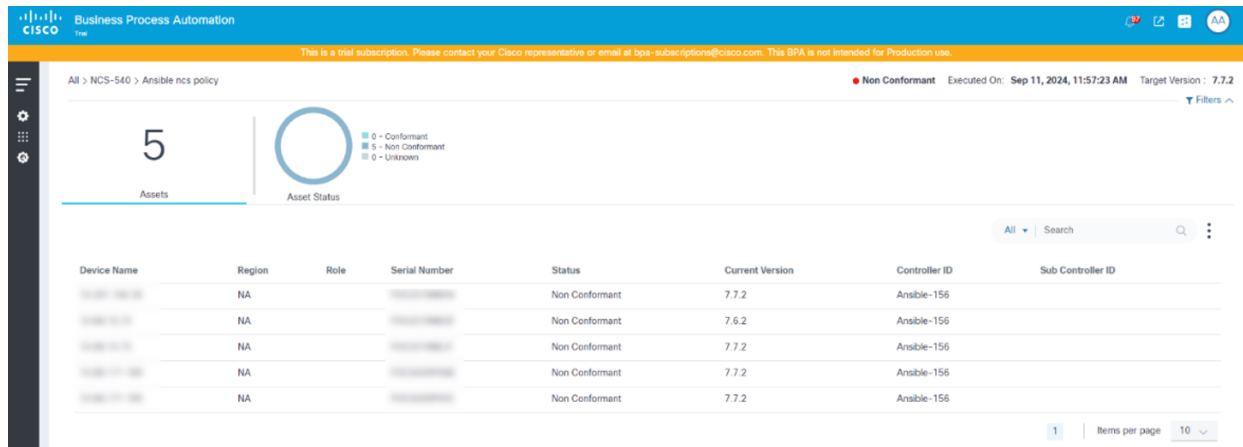
ポリシーが実行されると、次のようになります。

A screenshot of a web application interface for "Conformance Policies". At the top, there's a summary for "3" policies. Below that, a table lists policies. The first policy is "ASR9K" with 2 total assets (0 conformant, 2 non-conformant, 0 unknown). The second policy is "c8000v" with 15 total assets (0 conformant, 15 non-conformant, 0 unknown). A table below shows details for the "PDF-Font-Testing-Policy". A context menu is open over the "Policy Status" column, showing options: "Run", "View Results", "Edit", and "Delete".

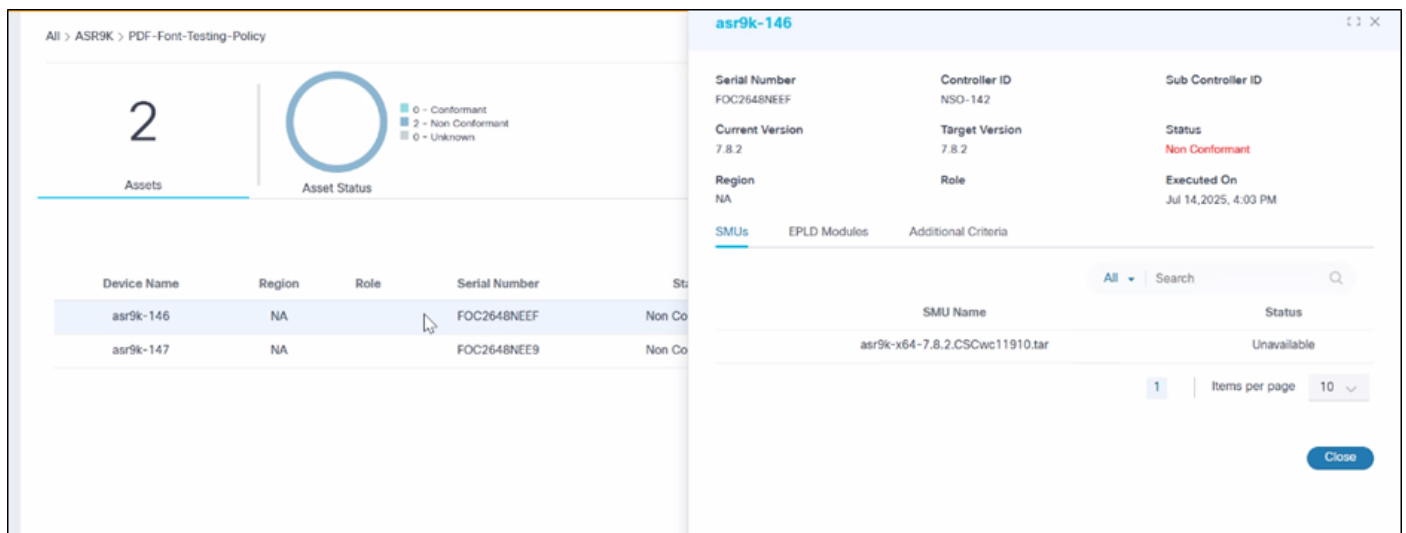
Name	Region	Device Roles	Target Version	Created By	Created On	Executed On	Execution Status	Policy Status
PDF-Font-Testing-Policy	Global	Any	7.8.2	admin	Jul 7, 2025, 5:51 PM	Jul 14, 2025, 4:03 PM	Completed	Non Conformant

結果の表示オプション

1. Software Conformanceページで、More Optionsアイコン> View Resultsを選択します。結果ページが表示され、ユーザはデバイスの適合性ステータスを確認できます。



結果の表示



Command Output:

Label : 7.7.2

Node 0/RP0/CPU0 [RP]

Boot Partition: xr_lv32

Active Packages: 11

```
ncs540-xr-7.7.2 version=7.7.2 [Boot image]
ncs540-lictrl-1.0.0.0-r772
ncs540-mpls-1.0.0.0-r772
ncs540-li-1.0.0.0-r772
ncs540-mgbl-1.0.0.0-r772
ncs540-isis-1.0.0.0-r772
ncs540-ospf-1.0.0.0-r772
ncs540-k9sec-1.0.0.0-r772
ncs540-mcast-1.0.0.0-r772
ncs540-mpls-te-rsvp-1.0.0.0-r772
ncs540-eigrp-1.0.0.0-r772
```

Node 0/0/CPU0 [LC]

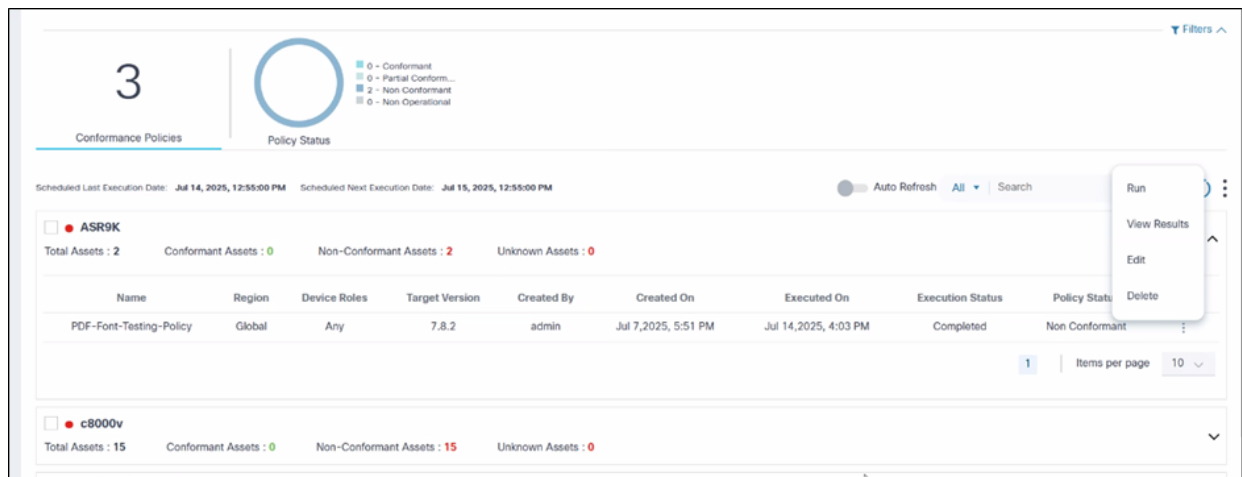
Boot Partition: xr_lcp_lv32

Active Packages: 11

```
ncs540-xr-7.7.2 version=7.7.2 [Boot image]
ncs540-lictrl-1.0.0.0-r772
ncs540-mpls-1.0.0.0-r772
ncs540-li-1.0.0.0-r772
ncs540-mgbl-1.0.0.0-r772
```

2. 行を選択すると、SMUステータスおよび追加条件とともに特定の資産詳細が表示されます。

 注:SMUの詳細は、NSO、CNC、ANSIBLE、Direct-to-Device、およびNDFCコントローラ資産についてのみ表示されます。EPLDモジュールは、NDFCコントローラでのみ表示されます。



結果の表示

3. デバイスのAction列から、More Optionsアイコン> View Resultsを選択します。

Assets

Asset Status: 13 (4 - Conformant, 9 - Non Conformant, 0 - Unknown)

Device Name	Region	Role	Serial Number	Status	Current Version	Controller ID	Sub Controller ID	Download
10.255.160.156	NA		10.255.160.156	Non Conformant	7.6.2	ANSIBLE-156		
10.255.160.156	NA		10.255.160.156	Conformant	7.7.2	ANSIBLE-156		
10.255.160.156	NA		10.255.160.156	Conformant	7.7.2	ANSIBLE-156		
10.255.160.156	NA		10.255.160.156	Non Conformant	7.6.2	ANSIBLE-156		
10.255.160.156	NA		10.255.160.156	Non Conformant	7.6.2	ANSIBLE-156		
10.255.160.156	NA		10.255.160.156	Non Conformant	7.6.2	NSO-183		

ダウンロード

4. More Optionsアイコン> Downloadの順に選択し、SMUのプレゼンスステータスを示す.csv形式で結果をダウンロードします。

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
1	Device Na	Serial Num	Controller	Sub Contr	Region	Device Rol	Current Ve	Target Ver	Device Sta	Execution	ncs540-7:	Compliance	Compliance	Remarks				
2	10.255.160.156	10.255.160.156	Ansible-156	NA		7.7.2	7.7.2	Non Confo	11 Sep 202	Unavailabl	show_inst:Success	Device conformance check completed along with Process Template						
3	10.255.160.156	10.255.160.156	Ansible-156	NA		7.6.2	7.7.2	Non Confo	11 Sep 202	Unavailabl	show_inst:NA	Device conformance check completed						
4	10.255.160.156	10.255.160.156	Ansible-156	NA		7.7.2	7.7.2	Non Confo	11 Sep 202	Unavailabl	show_inst:Success	Device conformance check completed along with Process Template						
5	10.255.160.156	10.255.160.156	Ansible-156	NA		7.7.2	7.7.2	Non Confo	11 Sep 202	Unavailabl	show_inst:Success	Device conformance check completed along with Process Template						
6	10.255.160.156	10.255.160.156	Ansible-156	NA		7.7.2	7.7.2	Non Confo	11 Sep 202	Unavailabl	show_inst:Success	Device conformance check completed along with Process Template						

Excelシートビュー

注意: 「結果の表示」には、最後に実行された準拠チェックの結果のみが表示されます。ユーザは、アクセス権を持つアセットのみを表示できます。動作しないポリシーの場合、[結果の表示]は無効になります。

考えられるデバイスステータス:

- Conformant : デバイスが定義済みのポリシーに準拠していることを示します。
- Non-Conformant : 次の条件に一致する場合に、デバイスが適合していないことを示します。

ターゲットバージョン	SMU	コンプライアンスチェック	ステータス
適合しない	適用外	適用外	適合しない
適合	使用不可	失敗した規則	適合しない
適合	Available	失敗した規則	適合しない
適合	使用不可	ルールの成功	適合しない

- Unknown : デバイ스에現在のソフトウェアバージョン情報がなく、デバイ스의ソフトウェア適合性チェックを実行できなかったことを示します。

Unknownステータスの基準は次のとおりです。

ターゲットバージョン	SMU	EPLD	コンプライアンスチェック	ステータス
適合しない	適用外	適用外	適用外	適合しない
適合	使用不可	適合しない	失敗した規則	適合しない
適合	使用不可	適合	失敗した規則	適合しない
適合	Available	適合	失敗した規則	適合しない
適合	Available	適合しない	失敗した規則	適合しない
適合	使用不可	適合	ルールの成功	適合しない
適合	使用不可	適合	ルールの成功	適合しない

可能なSMUステータス :

- Available:SMUがデバイスにあり、アクティブ状態であることを示します
- Unavailable:SMUが存在しない可能性があるか、または存在するにもかかわらず非アクティブ状態であることを示します

考えられるEPLDモジュールステータス :

- Conformant: EPLDモジュールが、予期されるターゲットバージョンでデバイスに存在することを示します。
- Non-Conformant: 予期されたバージョンと一致しないターゲットバージョンでEPLDモジュールがデバイスに存在することを示します。
- Missing Module: デバイスでEPLDモジュールが設定されていないか、サブスクライブされていないことを示します。

考えられるコンプライアンスチェックテンプレートの状態:

- 成功: デバイスが有効なコマンドとルールを使用してプロセステンプレートを正常に実行したことを示します
- Failed: デバイスがプロセステンプレートを実行できなかったことを示します (コマンドが正しくない場合など)。
- NA: デバイスがプロセステンプレートを実行する資格がないことを示します (デバイスが定義済みのターゲットバージョンに適合していない場合など)。

 注: 次のリストに注意してください。

- ソフトウェア適合性チェックは、デフォルトテナントに属するデバイスでのみ機能します
- ソフトウェア適合性チェックは、デバイスの現在のソフトウェアバージョンの正しいソースとして、資産インベントリに依存します。資産インベントリデータが古くなると、ソフトウェア適合性チェックの結果も古くなります。古いデータの問題を回避するには、準拠ポリシーの実行を開始するときにライブインベントリチェック機能を使用します
- デフォルトスケジュールは、OS Upgrade > Settings > Software Conformanceで変更できます
- BPA 5.1へのアップグレード後、既存のポリシーはすべて無効な状態に移行します。ユーザは各ポリシーを編集し、適切な値を選択して有効にし、今後の使用に備えて変更を保存する必要があります

アップグレードポリシー

アップグレードポリシーコンポーネントでは、次の2種類のポリシーがサポートされています。

- シングルステップポリシー:
 - Any-Any (任意)
 - <特定のソースバージョン(7.7.1)> - <特定のターゲットバージョン(7.7.2)>
- マルチステップポリシー:
 - v7.7.1 ~ 7.7.2
 - v7.7.2 - 7.7.8
- マルチステップアップグレードでは、次の例に示すように、ブリッジSMUを含めることができます。
 - v7.7.1 ~ v7.7.1[ブリッジSMU]

。 V7.7.1[ブリッジSMU] - 7.7.8

アップグレードポリシーコンポーネントでは、次のプラットフォーム固有のアーティファクトを事前に定義する柔軟性が提供されます。

- アップグレードパス
- 事前検証および事後検証テンプレートまたはワークフロー
- 配布ワークフロー
- アクティベーションワークフロー
- バックアップワークフロー
- タイムアウト値
- ロールバックワークフロー
- 有効な相違点の前後
- トラフィック転送ワークフローまたはトラフィック反転ワークフロー

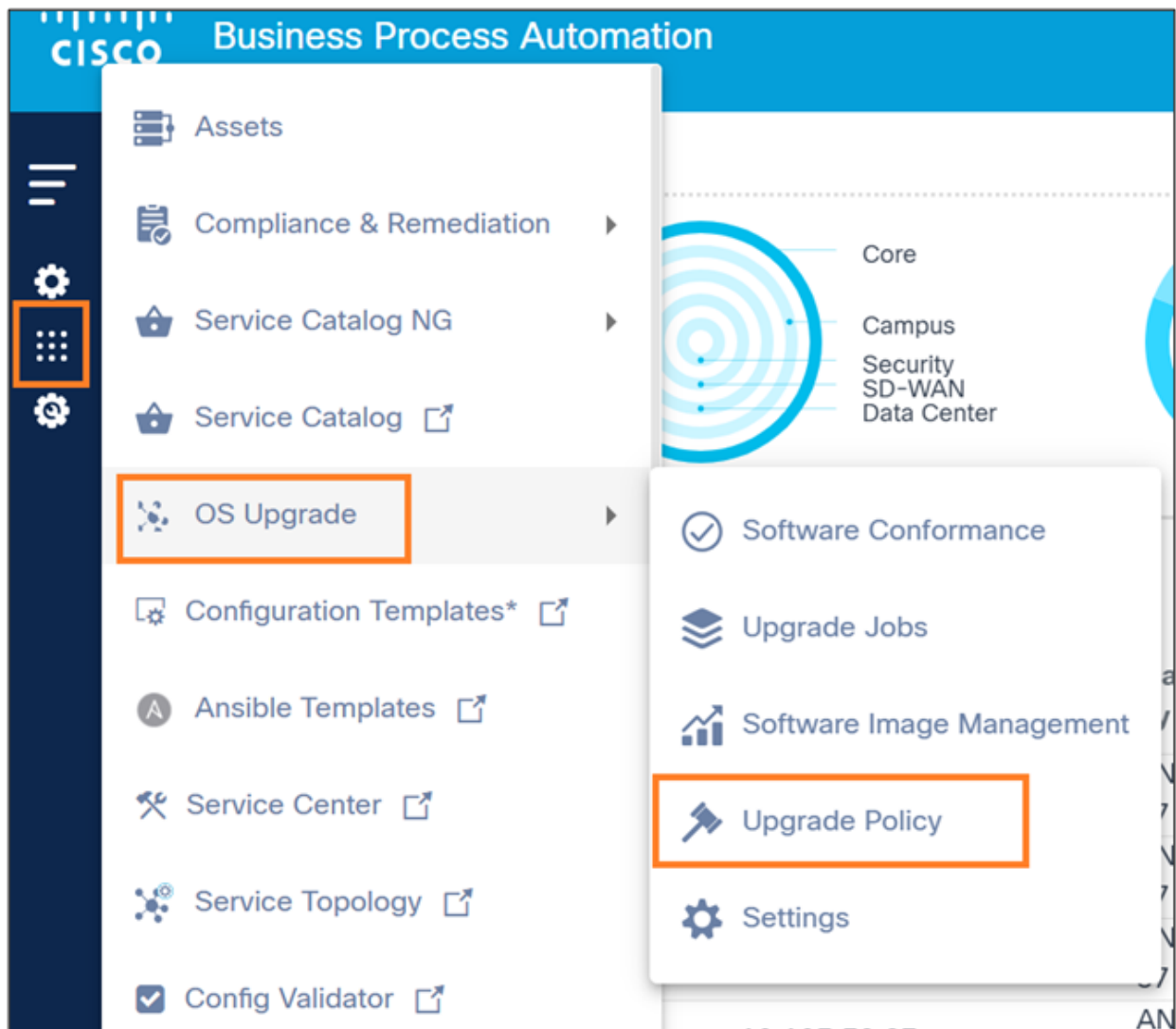
前提条件

- 必要な事前検証および事後検証プロセステンプレートまたはワークフロー
- 必要なバックアップ、配布、アクティブ化、およびロールバックのワークフロー
- 必要なイメージメタデータ

アップグレード・ポリシーの表示と管理

Upgrade Policyページにアクセスするには：

1. アップグレードポリシーに十分なアクセス権を持つクレデンシャルを使用してBPAにログインします。



アップグレードポリシーナビゲーション

2. OS Upgrade > Upgrade Policyの順に選択します。Upgrade Policyページが表示されます。

Device Model	Controller Type	Name	Created By	Last Modified On	Action
ASR-9901	Direct-To-Device	D2D-ASR-9901-Default	System	Mar 22, 2024, 11:14 AM	

アップグレードポリシー

Upgrade Policyページには次の項目が含まれています。

- 上部に表示される分析セクションには、次の情報が含まれます。

- 。システム内のアップグレードポリシーの合計数
- 。コントローラタイプの簡易フィルタ。コントローラのタイプでフィルタリングできます。
- More Optionsアイコン。このアイコンには、Create Policyや、Delete Allなどの一括処理アクションを作成するためのオプションがあります。
- Searchフィルタ：ポリシーを検索します。次のようにフィルタリングできます。
 - 。 All：すべてのフィールドを検索します。
 - 。 デバイスモデル：指定したモデルのポリシーを検索します。
 - 。 名前：指定したポリシー名を持つポリシーを検索します
 - 。 作成者：指定したユーザーのポリシーを検索します
- それぞれの列名またはテーブルフィールドをクリックして、ポリシーを並べ替えます

The screenshot displays the Cisco Business Process Automation (BPA) interface. On the left, a sidebar shows a menu with a gear icon. The main area is divided into two sections. The top section, titled 'Policies', shows a large number '61' and a donut chart representing 'Controller Types'. The chart is divided into segments for different controller types: 3 - NDFC, 25 - NSO, 5 - vltanage, 3 - CNC, 2 - Direct-To-Device, 4 - DNAC, 13 - Ansible, and 1 - FMC. Below the chart is a table with columns for 'Device Model', 'Controller Type', and 'Name'. The table lists several policies, including 'ASR-9901', 'ASR9K', and 'Ansible'. The right section shows a detailed view of the 'Ansible_TR_TD_workflow_check' policy. It includes a description, max batch count, default policy, and a list of workflows under 'Backup Details' and 'Traffic Diversion'.

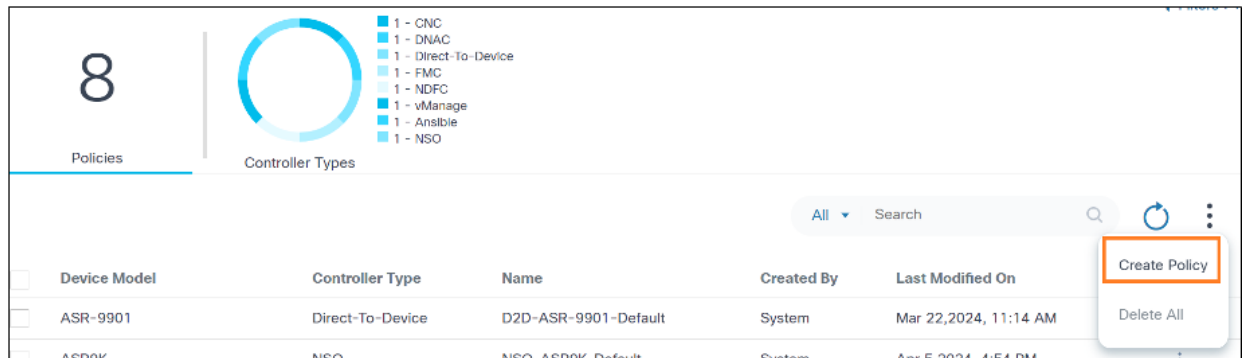
ポリシーの詳細ビュー

- 特定のポリシーまたはポリシーの詳細ビューの行をクリックする

 注：ポリシー名が一意的の場合、同じデバイスモデルおよびコントローラタイプに任意の数のポリシーを設定できます。

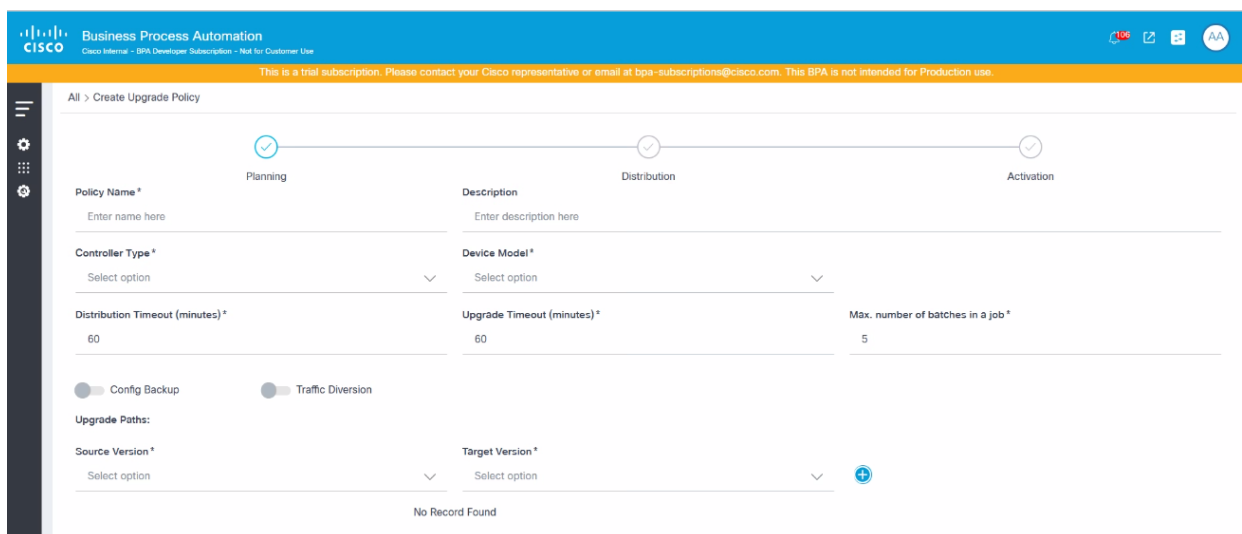
アップグレードポリシーの作成

1. アップグレードポリシーの管理アクセス権を持つクレデンシャルを使用してBPAにログインします。
2. OS Upgrade > Upgrade Policyの順に選択します。Upgrade Policyページが表示されます。



ポリシーの作成

3. More Options > Create Policyの順に選択します。Create Upgrade Policyページが表示されます。



アップグレードポリシーの作成

計画

1. 全体的なポリシーに関連するパラメータを設定します。次の表に、各フィールドの簡単な説明を示します。

フィールド	説明
ポリシー名	ポリシー名
説明	ポリシーの簡単な説明
コントローラのタイプ	OSアップグレードの実行に使用される適切なコントローラ
デバイスモデル	OSアップグレードの実行に使用されるデバイスモデル
配信タイムアウト (分)	イメージ配布アクティビティの最大待機時間 (分)
アップグレードのタイムアウト (分)	イメージのアクティブ化アクティビティの最大待機時間

フィールド

説明

間 (分)

ジョブ内のバッチの最大数

ジョブに追加できるバッチの数。許可される最大バッチ数は20です

バックアップが必要な場合にこの切り替えを有効にし、vManageおよびDirect-to-Deviceコントローラのウィンドウで次のフィールドに入力します。

- Workflow Name : 適用可能なバックアップ・ワークフロー

注 : ワークフローが見つからない場合は、ワークフローにOS Upgrade NextGenタグが正しくタグ付けされていることを確認してください

- 最新のワークフローを使用 : 選択すると、選択したワークフローの最新バージョンが使用されます

- ワークフローバージョン : カスタムワークフローバージョン。選択できるのは、[最新のワークフローを使用]が選択されていない場合のみです。

構成バックアップの切り替え

NDFC、NSO、CNC、およびCisco Catalyst Centerコントローラの場合、バックアップはバックアップおよび復元サービス経由で行われます。したがって、[バックアップの詳細]ウィンドウでバックアップと復元のポリシーを選択する必要があります。

注 : ユーザはコントローラタイプに適したポリシーを選択する必要があります。バックアップと復元のポリシーの詳細については、「[バックアップと復元](#)」セクションを参照してください。

Nexusデバイスのバックアップを有効にするには、scp-server機能の設定がターゲットデバイス上に存在している必要があります。

トラフィック転送が必要な場合にこの切り替えを有効にし、Traffic Diversionウィンドウで次のフィールドに入力します。

Traffic Diversion切り替え

- Traffic Diversion Workflow : 適用可能なTraffic Diversionワークフロー。

注：ワークフローが見つからない場合は、ワークフローにOS Upgrade NextGenタグが正しくタグ付けされていることを確認してください

- トラフィック反転ワークフロー：適用可能なトラフィック反転ワークフロー。

注：ワークフローが見つからない場合は、ワークフローにOS Upgrade NextGenタグが正しくタグ付けされていることを確認してください

- 最新のワークフローを使用：上記の選択したワークフローの最新バージョン

- ワークフローバージョン：カスタムワークフローバージョン。選択できるのは、[最新のワークフローを使用]が選択されていない場合のみです

アップグレードパスは、適用可能なステップアップグレードパスを定義します。さまざまな需要に対応するため、次のフィールドに複数のソースバージョンとターゲットバージョンを追加できます

- Source Version：アップグレードパスの開始バージョン

- Target Version：アップグレードパスの終了バージョン

- Source Version (Any) to Target Version (Any)：これは、すべてのデバイスモデルのデフォルト値であるSource VersionフィールドとTarget Versionフィールドの両方にAnyを選択することで使用可能になります。このシナリオでは、DistributionページとActivationページでアップグレードの統一プロセスを実行します

- Source Version (Specific Version) to Target Version (Specific Version)：デバイスモデルで使用可能な特定のイメージバージョンを選択することで使用可能になります。複数のソースバージョンとターゲットバージョンを追加できます。配布およびアクティベーションアップグレードプロセスの入力数は、追加されたソースバージョンとターゲットバージョンの数と一致し、それぞれに対応するソースバージョンとターゲットバージョンのラベルが付いた折りたたみセクションとして表示されます。アップグレードパスでは、必須の

アップグレードパス

フィールド

説明

SMUをソースバージョンに適用してから、それぞれのアップグレードパスにブリッジSMUとして追加してターゲットバージョンにアップグレードする必要があります。ブリッジSMUの詳細については、次の項を参照してください。

ブリッジSMU

ブリッジSMU（必須アップグレードまたはダウングレードSMUとも呼ばれる）は前提条件であり、同じプラットフォームまたはモデルの別のソフトウェアリリースにアップグレードまたはダウングレードする前にインストールする必要があります。

アップグレードパスでのブリッジSMUの追加

The screenshot displays the 'Planning' stage of a configuration process. It features several input fields and a table for defining upgrade paths. The 'Upgrade Paths' section includes a table with columns for Source Version, Bridge SMU(S), Target Version, and Action. A dropdown menu is open for the Action column, showing options to 'Delete Path' or 'Add Bridge SMUs'.

Source Version	Bridge SMU(S)	Target Version	Action
7.6.2		7.7.2	⋮

アップグレードパスのオプション

1. アップグレードパスを追加した後、More Optionsアイコンを選択します。Delete PathおよびAdd Bridge SMUsオプションが表示されます。

Policy Name*
Enter name here

Controller Type*
NSO

Distribution Timeout (minutes)*
60

Config Backup

Traffic Diversion

Upgrade Paths:

Source Version
Select option

Target Version
Select option

Source Version	Bridge SMU(S)	Target Version	Action
7.6.2		7.7.2	1 ⋮ Delete Path Add Bridge SMUs

Cancel Next

ブリッジSMUの追加

2. Add Bridge SMUsを選択します。Add Bridge SMUsウィンドウが開きます。指定したアップグレードパスで使用可能なすべてのブリッジSMUが表示されます。

Add Bridge SMUs

Select option(s)

- ☒ asr9k-x64-7.6.2.CSCwf77420.tar
- ☐ asr9k-x64-7.6.2.CSCwc41614.tar

ブリッジSMUの追加

3. Add Bridge SMUsウィンドウで、ブリッジSMUを追加するための適切なチェックボックスをオンにするか、削除するためのチェックボックスをオフにします。ブリッジSMUを追加すると、アップグレードパスが選択したブリッジSMUの詳細で更新されます。

Policy Name* ✓

Controller Type* ✓ ✓

Distribution Timeout (minutes)*

Device Model* ✓ ✓

Upgrade Timeout (minutes)*

Max. number of batches in a job*

☐ Config Backup ☐ Traffic Diversion

Upgrade Paths:

Source Version Target Version +

Source Version	Bridge SMU(S)	Target Version	Action
7.6.2	asr9k-x64-7.6.2.CSCw77420.tar	7.7.2	⋮

ブリッジSMUを使用するアップグレードパス

 注：ブリッジSMUを含む各アップグレードパスは、アップグレードの過程で2段階のアップグレードと見なされます。上の図に示すアップグレードパスでは、最終的なアップグレードパスは次のようになります。

- 7.6.2 ~ 7.6.2 [ブリッジSMU]

このパスは、ブリッジSMUを使用してv7.6.2で実行されているデバイスを更新することを表します。

- 7.6.2 [ブリッジSMU] - 7.7.2

このパスは、v7.6.2からv7.7.2へのデバイスのアップグレードを表します。この場合、デバイスのソースバージョンは7.6.2で、適用されるブリッジSMUも含まれます。

ブリッジSMUの編集

Source Version Target Version +

Source Version	Bridge SMU(S)	Target Version	Action
7.7.2	asr9k-x64-7.7.2.CSCwe22538.tar,asr9k-x64-7.7.2.CSCwd07897.tar	7.8.2	⋮

1 | Items per page

ブリッジSMUを使用するアップグレードパス

1. Upgrade Pathsセクションで、More Optionsアイコン> Edit Bridge SMUsの順に選択します。Edit Bridge SMUsウィンドウが開きます。

Edit Bridge SMUs

Select option(s)

☒ asr9k-x64-7.7.2.CSCwd07897.tar

☒ asr9k-x64-7.7.2.CSCwe22538.tar

ブリッジSMUの編集

- 適切なチェックボックスをオンまたはオフにして、ブリッジSMUを更新します。
- [OK] をクリックします。変更の概要が表示されます。

Policy Name *	Planning	Description	Distribution	Activation
ASR9K bridge 772		Enter description here		
Controller Type *	NSO	Device Model *	ASR9K	
Distribution Timeout (minutes) *	60	Upgrade Timeout (minutes) *	60	Max. number of batches in a job *
				5
☒ Config Backup ☒ Traffic Diversion				
Upgrade Paths:				
Source Version	Bridge SMU(S)		Target Version	
Select option	Select option		Select option	
7.7.2	asr9k-x64-7.7.2.CSCwd07897.tar,asr9k-x64-7.7.2.CSCwe22538.tar		7.8.2	
		1	Items per page	25

Cancel Next

変更の概要

- 変更の概要を確認し、Nextをクリックします。

ブリッジSMUの削除

Source Version	Bridge SMU(S)	Target Version	Action
7.7.2	asr9k-x64-7.7.2.CSCwe22538.tar,asr9k-x64-7.7.2.CSCwd07897.tar	7.8.2	
		1	Items per page

Delete Path

Edit Bridge SMUs

Cancel Next

ブリッジSMUの編集

- Upgrade Pathsセクションで、More Optionsアイコン> Edit Bridge SMUsの順に選択します。Edit Bridge SMUsウィンドウが開きます。

Edit Bridge SMUs

Select option(s)

☒ asr9k-x64-7.7.2.CSCwd07897.tar

☒ asr9k-x64-7.7.2.CSCwe22538.tar

ブリッジSMUの編集

- 適切なチェックボックスをオフにして、ブリッジSMUを削除します。
- [OK] をクリックします。変更の概要が表示されます。

Policy Name *	Planning	Description	Distribution	Activation
ASR9K bridge 772	Enter description here			
Controller Type *	NSO	Device Model *	ASR9K	
Distribution Timeout (minutes) *	60	Upgrade Timeout (minutes) *	60	Max. number of batches in a job *
				5
☒ Config Backup ☒ Traffic Diversion				
Upgrade Paths:				
Source Version	Select option		Target Version	Select option
7.7.2	asr9k-x64-7.7.2.CSCwd07897.tar, asr9k-x64-7.7.2.CSCwe22538.tar		7.8.2	:
1 Items per page 25				

Cancel Next

変更の概要

配信

Distributionは、Image Distributionに関連する入力パラメータ（つまり、イメージコピー）を取ります。次のイメージは、各アップグレードパスタイプに必要な入力パラメータです。

Workflow Name *

ASR9K_Device_SW_Distribution

Pre/Post Common Templates

Select option(s)

Pre Check Templates

asr9k_distribution_precheck

Post Check Templates

asr9k_distribution_postcheck

Pre/Post Workflow

Previous Next

イメージ配布セクション - シングルステップアップグレード

✓

Planning

✓

Distribution

✓

Activation

Workflow Name *

ASR9K_Device_SW_Distribution

✓

☒ Use latest workflow

Workflow Version *

Select option

▼

Pre/Post Common Templates

Select option(s)

▼

Pre Check Templates

Select option(s)

▼

Post Check Templates

Select option(s)

▼

☒ Pre/Post Workflow

Pre check Workflow *

OS_Upgrade_Precheck_PostCheckExample

✓

✓

☒ Use latest workflow

Workflow Version *

Select option

▼

Post check Workflow *

OS_Upgrade_Precheck_PostCheckExample

✓

✓

☒ Use latest workflow

Workflow Version *

Select option

▼

Previous

Next

イメージ配布セクション – ワークフローの前後を切り替えたシングルステップアップグレード

All > D2D_multi_step_policy > Edit Upgrade Policy

✓

Planning

✓

Distribution

✓

Activation

7.6.2 to 7.7.2

Workflow Name *

ASR9K_Device_SW_Distribution

▼

☒ Use latest workflow

Workflow Version *

Select option

▼

Pre/Post Common Templates

Select option(s)

▼

Pre Check Templates

asr9k_distribution_precheck

▼

✓

Post Check Templates

asr9k_distribution_postcheck

▼

✓

☒ Pre/Post Workflow

☐ Use the same properties for all the below upgrade paths

7.7.2 to 7.8.2

Workflow Name *

ASR9K_Device_SW_Distribution

▼

☒ Use latest workflow

Workflow Version *

Select option

▼

Pre/Post Common Templates

Select option(s)

▼

Pre Check Templates

asr9k_distribution_precheck

▼

✓

Post Check Templates

asr9k_distribution_postcheck

▼

✓

☒ Pre/Post Workflow

Previous

Next

ディストリビューションセクション：マルチステップアップグレード

✓

Planning

✓

Distribution

✓

Activation

7.6.2 to 7.7.2

Workflow Name *

ASR9K_Device_SW_Distribution

▼

☒ Use latest workflow

Workflow Version *

Select option

▼

Pre/Post Common Templates

Select option(s)

▼

Pre Check Templates

Select option(s)

▼

Post Check Templates

Select option(s)

▼

☒ Pre/Post Workflow

Pre check Workflow *

OS_Upgrade_Precheck_PostCheckExample

✓

✓

☒ Use latest workflow

Workflow Version *

Select option

▼

Post check Workflow *

Select option

▼

☐ Use latest workflow

Workflow Version *

Select option

▼

☐ Use the same properties for all the below upgrade paths

7.7.2 to 7.8.2

Workflow Name *

ASR9K_Device_SW_Distribution

▼

☒ Use latest workflow

Workflow Version *

Select option

▼

Pre/Post Common Templates

Select option(s)

▼

Pre Check Templates

Select option(s)

▼

Post Check Templates

Select option(s)

▼

☒ Pre/Post Workflow

Pre check Workflow *

OS_Upgrade_Precheck_PostCheckExample

✓

✓

☒ Use latest workflow

Workflow Version *

Select option

▼

ディストリビューションセクション：マルチステップアップグレード

Workflow configuration interface showing two sections for version ranges 7.6.2 to 7.7.2 and 7.7.2 to 7.7.2. Each section has fields for Workflow Name, Pre/Post Common Templates, Pre Check Templates, Post Check Templates, and Workflow Version. The 'Pre/Post Workflow' section is expanded, showing options for 'Use the same properties for all the below upgrade paths' and 'Pre/Post Workflow'.

ディストリビューションセクション：ブリッジSMUのアップグレード

1. イメージ配布に関連するパラメータを設定します。
2. 次の表に、各フィールドの簡単な説明を示します。

フィールド	説明
ワークフロー名	適用可能な配布ワークフロー
最新のワークフローを使用	選択したワークフローの最新バージョンを選択します
ワークフローバージョン	カスタムワークフローバージョン。これは、[最新のワークフローを使用]チェックボックスがオフの場合にのみ選択できます
導入前/導入後の共通テンプレート	両方の段階（事前確認と事後確認）で実行されるプロセステンプレート
ワークフローの前後の切り替え	注：チェックはディストリビューションマイルストーンにのみ適用されます。 詳細は、『 プロセステンプレート 』を参照してください ユーザは配布マイルストーン内でプレチェックまたはポストチェックのワークフローの実行を選択できます。この切り替えがオンの場合、チェック前またはチェック後のワークフローのみを設定できます。
ワークフローの事前確認	チェック前の段階でのみ実行されるコマンドが含まれます。
ポストチェックワークフロー	注：これらのチェックは、ディストリビューションマイルストーンに固有のものです。 ポストチェックワークフローは、ポストチェック段階で一意に実行されるコマンドで構成されます。

フィールド

説明

注：これらのチェックは、ディストリビューションマイルストーンに固有のものです。

排他的なプレチェックコマンドを含むプロセステンプレート。テンプレートはプレチェック段階でのみ実行されます。

プレチェックテンプレート

注：チェックはディストリビューションマイルストーンにのみ適用されます。

排他的なポストチェックコマンドを含むプロセステンプレート。テンプレートはポストチェック段階でのみ実行されます。

ポストチェックテンプレート

注：チェックはディストリビューションマイルストーンにのみ適用されます。

複数選択アップグレードでは、すべてのアップグレードパスに一貫したプロパティが適用されます。

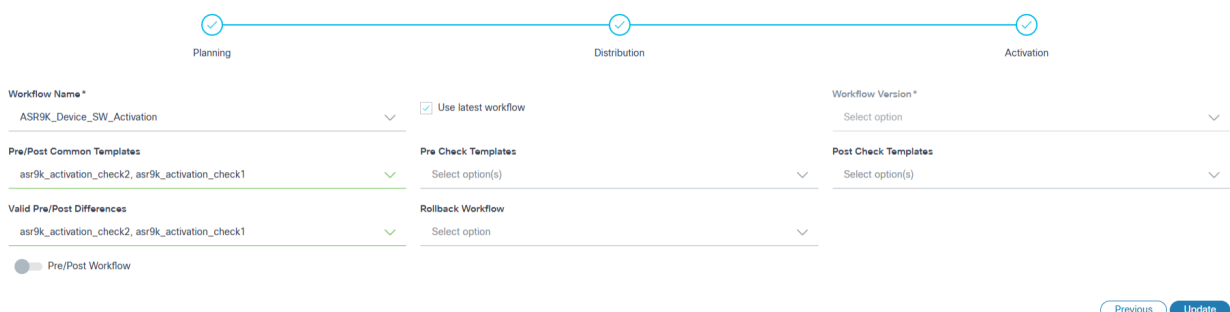
以下のアップグレードパスすべてに同じプロパティを使用する

注：選択すると、複数選択アップグレードのすべてのアップグレードパスに同じプロパティが適用されます。

 注：ワークフローまたはプロセステンプレートは、OS Upgrade Next-Genタグを使用して適切にタグ付けする必要があります。

3. Nextをクリックして、Activationセクションに進みます。

有効化



Workflow Name*
ASR9K_Device_SW_Activation

Pre/Post Common Templates
asr9k_activation_check2, asr9k_activation_check1

Valid Pre/Post Differences
asr9k_activation_check2, asr9k_activation_check1

Pre Check Templates
Select option(s)

Post Check Templates
Select option(s)

Rollback Workflow
Select option

Workflow Version*
Select option

Pre/Post Workflow

Previous Update

アクティベーションセクション：シングルステップアップグレード



Workflow Name *
ASR9K_Device_SW_Activation

Pre/Post Common Templates
asr9k_activation_check2, asr9k_activation_check1

Valid Pre/Post Differences
asr9k_activation_check1, asr9k_activation_check2

Pre/Post Workflow

Use the same properties for all the below upgrade paths

Workflow Version *
Select option

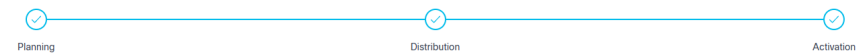
Pre Check Templates
Select option(s)

Post Check Templates
Select option(s)

Rollback Workflow
Select option

Previous Update

アクティベーションセクション：マルチステップアップグレード



Workflow Name *
ASR9K_Device_SW_Activation

Pre/Post Common Templates
asr9k_activation_check2, asr9k_activation_check1

Valid Pre/Post Differences
asr9k_activation_check1, asr9k_activation_check2

Pre/Post Workflow

Use the same properties for all the below upgrade paths

Workflow Version *
Select option

Pre Check Templates
Select option(s)

Post Check Templates
Select option(s)

Rollback Workflow
ASR9K_Device_SW_Rollback

Previous Update

アクティベーションセクション：ブリッジSMUのアップグレード

1. イメージのアクティブ化に関連するパラメータを設定します。
2. 次の表に、各フィールドの簡単な説明を示します。

フィールド	説明
ワークフロー名	該当するアクティベーションワークフロー
最新のワークフローを使用	選択したワークフローの最新バージョンを選択します
ワークフローバージョン	カスタムワークフローバージョン。選択できるのは、[最新のワークフローを使用]チェックボックスがオフの場合のみです
導入前/導入後の共通テンプレート	両方の段階で実行されるプロセステンプレート（事前確認と事後確認）。 注：チェックマークが付いているのは、アクティベーションマイルストーンだけです。

詳細は、『[プロセステンプレート](#)』を参照してください

排他的なプレチェックコマンドを含むプロセステンプレート。テンプレートはプレチェック段階でのみ実行されます。

プレチェックテンプレート

注：チェックマークが付いているのは、アクティベーションマイルストーンだけです。

排他的なポストチェックコマンドを含むプロセステンプレート。テンプレートはポストチェック段階でのみ実行されます。

小切手後テンプレート

注：チェックマークが付いているのは、アクティベーションマイルストーンだけです。

差分を無視するように選択されたプロセステンプレート。

有効な導入前/導入後の差異

注：チェックマークが付いているのは、アクティベーションマイルストーンだけです。

適用可能なロールバック・ワークフロー。

ロールバックワークフロー

注意：複数選択アップグレードで、ロールバック・ワークフローを使用するアップグレード・パスの1つが選択されている場合は、デフォルトで、他のすべてのアップグレード・ステップがロールバック・ワークフローを使用して選択されます。

このカスタムプレチェックワークフローは、実行結果を選択およびレビューできる特定のコマンドで構成されます。チェック前の段階でのみ実行されます。

ワークフローの事前確認

注：これらのチェックは、アクティベーションマイルストーンに固有のものです。

このカスタムポストチェックワークフローは、実行結果を選択およびレビューできる特定のコマンドで構成されます。チェック後の段階でのみ行われます。

ポストチェックワークフロー

注：これらのチェックは、アクティベーションマイルストーンに固有のものです。

以下のアップグレードパスすべてに同じプロパティを使用する

複数選択アップグレードでは、すべてのアップグレードパスに一貫したプロパティが適用されます。

注：選択すると、複数選択アップグレードのすべてのアップグレードパスに同じプロパティが適用されます。

- Nexusデバイスに必要な公開キーアルゴリズムは、NSOで設定する必要があります。
- Nexusデバイスでプレチェックテンプレートとポストチェックテンプレートを実行するように、bgp、bfd、およびhsrpの機能を設定します。

3. [Create] をクリックします。フィールドの要約が表示されます。

The screenshot shows a 'Summary' dialog box for a 'Single step upgrade' policy. The fields are as follows:

Field	Value
Name	Single step upgrade
Description	This upgrade policy for ansible
Max Batch Count	5
Default Policy	No
Ansible	NCS-540

The 'Planning' tab is selected, and the 'Backup Details' dropdown is visible. A 'Submit' button is at the bottom right.

概要 – 1ステップのアップグレードポリシー

The screenshot shows a 'Summary' dialog box for a 'Multi step upgrade' policy. The fields are as follows:

Field	Value
Name	Multi step upgrade
Description	This upgrade policy for ansible
Max Batch Count	5
Default Policy	No
Ansible	NCS-540

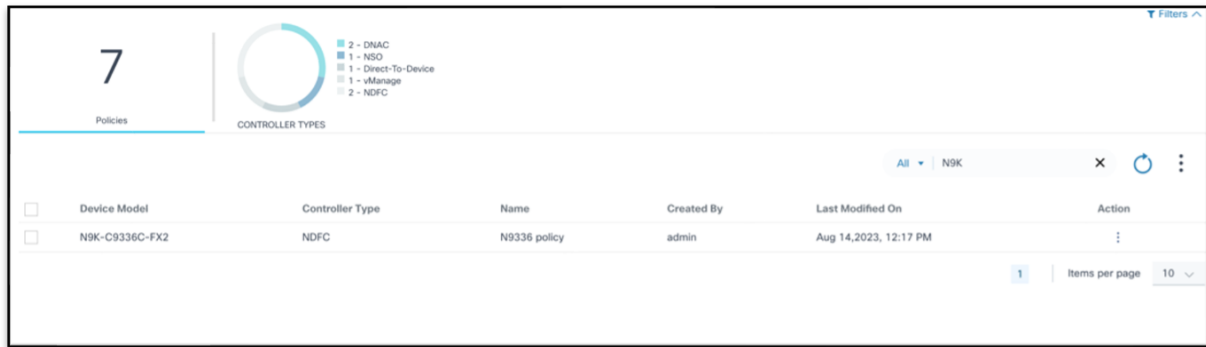
The 'Planning' tab is selected, and the 'Backup Details' and 'Upgrade Paths' dropdowns are visible. A 'Submit' button is at the bottom right.

概要 – 複数ステップのアップグレードポリシー

4. フィールドの要約を確認し、Submitをクリックします。進行状況を示す通知が表示され、確認メッセージが表示されます。ポリシーは、作成が成功するとページに表示されます。

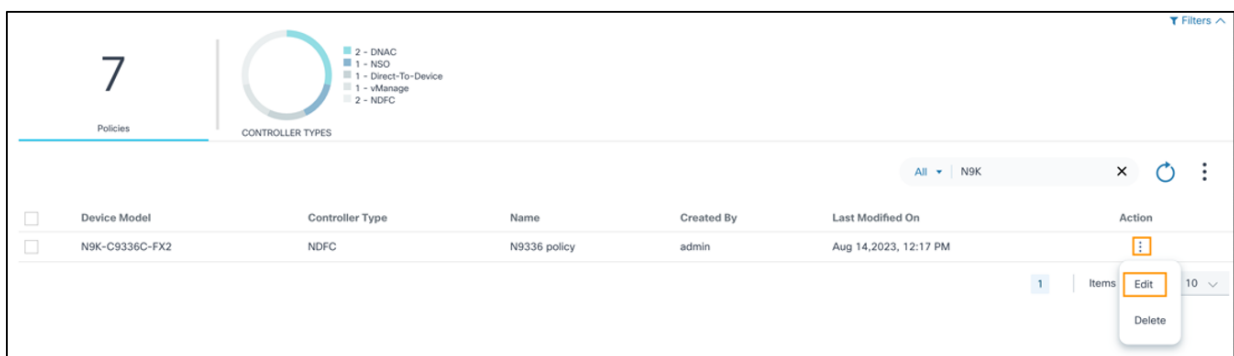
必要に応じて、他のデバイスモデル用の追加のアップグレードポリシーを作成できます。

アップグレードポリシーの編集



アップグレードポリシーの検索結果

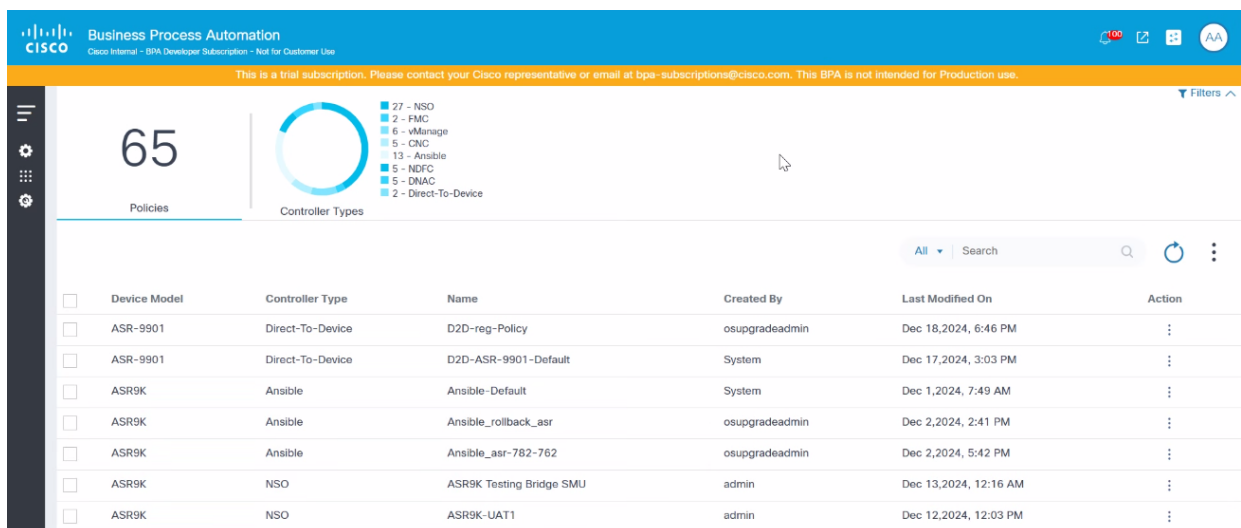
1. Upgrade Policyページで、Searchフィールドを使用して、目的のポリシーを見つけます。



アップグレードポリシーの編集

2. ポリシーのAction列から、More Optionsアイコン> Editを選択します。
3. 関連するフィールドを更新し、Updateをクリックします。変更の概要が表示されます。
4. 変更の概要を確認し、Submitをクリックします。進行状況の通知が表示され、確認メッセージが表示されます。

アップグレードポリシーの表示



アップグレードポリシー

1. Upgrade Policyページで、目的のアップグレードポリシーの行を選択します。ポリシーの詳細ビューが開きます。

The screenshot shows the Cisco Business Process Automation (BPA) interface. The main area displays a list of policies with columns for Device Model, Controller Type, and Name. A sidebar on the right shows details for the 'Ansible-Default' policy, including Max Batch Count, Default Policy, and Upgrade Paths.

Device Model	Controller Type	Name	
☐	ASR-9901	Direct-To-Device	D2D-reg-Policy
☐	ASR-9901	Direct-To-Device	D2D-ASR-9901-Default
☐	ASR9K	Ansible	Ansible-Default
☐	ASR9K	Ansible	Ansible_rollback_asr
☐	ASR9K	Ansible	Ansible_asr-782-762
☐	ASR9K	NSO	ASR9K Testing Bridge SMU
☐	ASR9K	NSO	ASR9K-UAT1

Controller Types: 27 - NSO, 2 - FMC, 6 - vManage, 5 - CNC, 13 - Ansible, 5 - NDFC, 5 - DNAC, 2 - Direct-To-Device

Ansible-Default

Max Batch Count: 5

Default Policy: Yes

Ansible

System

Dec 1, 2024, 7:49 AM

Planning Distribution Activation

Backup Details

Workflow: IOSXR_Ansible_Device_SW_Backup (Version : Latest)

Traffic Diversion

Traffic Diversion Workflow: OS_Upgrade_Device_SW_TrafficDiversion (Version: Latest)

Traffic Reversal Workflow: OS_Upgrade_Device_SW_TrafficReversal (Version: Latest)

Upgrade Paths

- 7.8.2 to 7.7.2
- 7.7.2 to 7.6.2

アップグレードポリシーの詳細ビュー

アップグレードポリシーの削除

 注：デフォルトポリシーは削除できませんが、ユーザはプロセステンプレートとワークフローを編集できます。

The screenshot shows the Cisco Business Process Automation (BPA) interface. The main area displays a list of policies with columns for Device Model, Controller Type, Name, Created By, Last Modified On, and Action. A sidebar on the right shows details for the 'N9K-C9336C-FX2' policy.

Device Model	Controller Type	Name	Created By	Last Modified On	Action	
☐	N9K-C9336C-FX2	NDFC	N9336 policy	admin	Aug 14, 2023, 12:17 PM	

CONTROLLER TYPES: 2 - DNAC, 1 - NSO, 1 - Direct-To-Device, 1 - vManage, 2 - NDFC

7

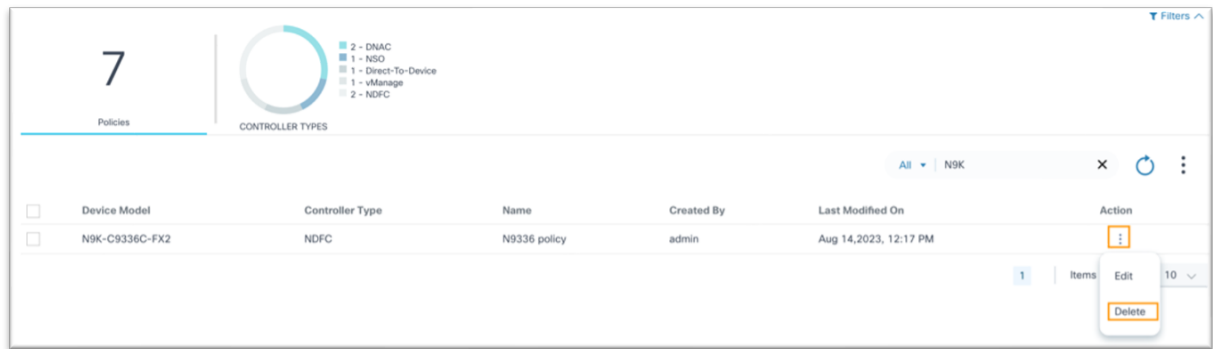
Policies

Filters: All N9K

Items per page: 10

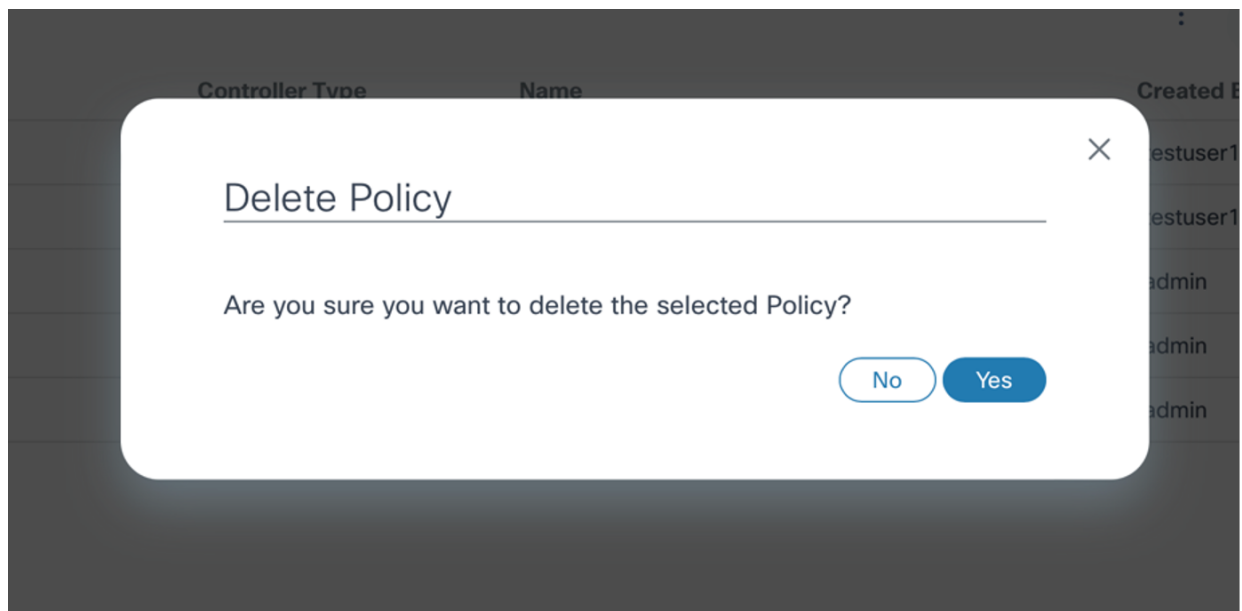
アップグレードポリシー

1. Upgrade Policiesページで、Searchフィールドを使用して、目的のポリシーを見つけ**す。



アップグレードポリシーの削除

2. ポリシーのAction列から、More Options > Deleteの順に選択します。確認ウィンドウが開きます



ポリシーの削除の確認

3. [Yes] をクリックします。

アップグレードポリシーへのアクセスの制御

この機能は、アップグレードポリシーのアクセスコントロールを提供し、権限のないユーザによるOSアップグレードアプリケーションで定義されたポリシーのアップデートを制限します。管理者は、アクセス可能なポリシーを使用してリソースグループを定義することで、アクセスを制限できます。

リソースグループを作成するには

1. Settings > Resource Groupsの順に移動します。

2. 管理者以外のユーザーがアクセスできるポリシーを持つリソースグループを作成します。このユーザグループに属する非管理者ユーザは、このリソースグループで使用可能なポリシーにのみアクセスできます。
3. アクセスポリシーを作成して、リソースグループをユーザグループに関連付けます。

詳細は、『[アクセスコントロール](#)』を参照してください。



注：次の点に注意してください。

- ・ ユーザが配布とアクティベーションのワークフローを誤って選択すると、意図しない動作が発生する可能性があります。ワークフローを正しくマッピングし、配布、アクティベーション、ロールバック、デバイスモデルなどのマイルストーンの適用性を確認するのはユーザの責任です。
- ・ ワークフローとプロセステンプレートをOS Upgrade Next-Genタグにマッピングして、ポリシーの作成または更新時に選択できるようにする必要があります。
- ・ システムユーザーによって作成された既定のOOBポリシーは削除できませんが、ユーザーはプロセステンプレートとワークフローを編集できます。

アップグレードジョブ

ソフトウェアのアップグレードは、アップグレード・ジョブ・アプリケーションを使用して管理します。このアプリケーションは、1つ以上のバッチで構成され、各バッチには1つ以上のネットワーク・デバイスがあります。ジョブはドラフトモードで作成でき、複数回保存できます。アップグレードはジョブがコミットされた後にのみ開始できるため、オペレータは事前に変更を計画できます。

前提条件

- ・ アップグレード用に予約されたメンテナンスウィンドウ
- ・ アップグレード変更要求の事前承認
- ・ 構成のバックアップと復元サービスが実行中である必要があります
- ・ スケジューラサービスが起動して実行中である必要があります
- ・ 外部システム（チケット発行システムなど）用のBPAアダプタがある場合は、オンボーディングする必要があります

アップグレード・ジョブの表示および管理

1. アップグレードジョブにアクセスできるクレデンシャルを使用してBPAにログインします。
2. OS Upgrade > Upgrade Jobsの順に選択します。Upgrade Jobページが表示されます。



アップグレードジョブ

アップグレードジョブページには次の情報が含まれます。

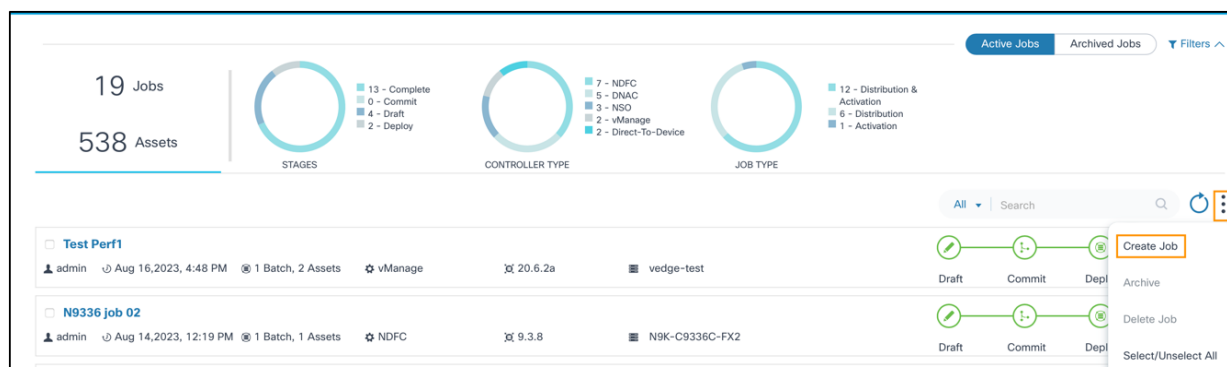
 注：デフォルトでは、10個のジョブが表示されます。ページ番号を使用して、他のジョブページに移動できます。

- アクティブなジョブとアーカイブされたジョブを切り替えるために使用できるアクティブなジョブとアーカイブされたジョブのトグル
- 上部に表示される分析セクションには、次の情報が含まれます。
 - ジョブとジョブに関連付けられた資産の合計
 - 次のフィルタを使用したステージ・チャート：
 - ドラフト：ジョブはドラフトフェーズにあり、まだコミットされていません
 - コミット：スケジュールに達するまで、必要なすべてのデバイス、バッチ、またはスケジュールでジョブがコミットされます
 - 配布：1つ以上のバッチに対してアップグレード処理が開始されました
 - 完了：すべてのバッチに属するすべてのデバイスのアップグレード処理が完了しました
 - コントローラタイプチャート：Cisco Catalyst Center、vManage、NSO、NDFC、Direct-to-Device、CNC、ANSIBLE、およびFMCコントローラタイプ別にジョブフィルタリングが可能
 - 次のフィルタを使用した[ジョブの種類]グラフ：
 - 配布：コントローラからデバイスにイメージのステージングまたはコピーを実行するジョブ
 - アクティベーション：デバイスのソフトウェアのアクティベーションまたはアップグレードを実行するジョブ
 - 配布およびアクティベーション：ステージングまたはコピーと、デバイスのソフトウェアのアクティベーションまたはアップグレードの両方を実行するジョブ
- Searchフィールド。このフィールドを使用して、すべてのメタデータ全体またはJob NameフィールドとCreated Byフィールドで汎用検索を実行できます。

- Refreshアイコン。ジョブサマリーを更新し、Searchフィールドのグラフフィルタまたはカスタム検索をクリアするために使用できます。
- More Optionsアイコン：新しいアップグレードジョブのCreateや、選択したジョブのArchiveまたはDeleteを行うためのオプションを提供。ユーザはAllを選択または選択解除できる
- ジョブはパネルとして表示され、次の情報をすばやく確認できます。
 - 使用可能なユーザタスクがある場合、ユーザタスクアイコンがユーザタスクの数とともに表示されます
 - ジョブを作成したユーザー
 - ジョブ作成日
 - バッチと資産の数
 - コントローラタイプ (Cisco Catalyst Center、vManage、NDFC、Direct-to-Device、CNC、ANSIBLE、FMCなど)
 - ターゲットバージョン
 - 該当するデバイスモデル
 - 各マイルストーンの色の凡例を含むジョブステージ (ドラフト、コミット、配置、完了) のマイルストーンビュー：
 - 灰色：マイルストーンが開始されていません
 - 青：マイルストーンは進行中です
 - 赤：マイルストーンの問題
 - 緑：マイルストーン完了
 - マイルストーンの最後に表示される色の凡例で、ジョブのステータスを示します。
 - 緑：ジョブが完了しました
 - 赤：ジョブに問題があります
 - 青：ジョブが進行中です

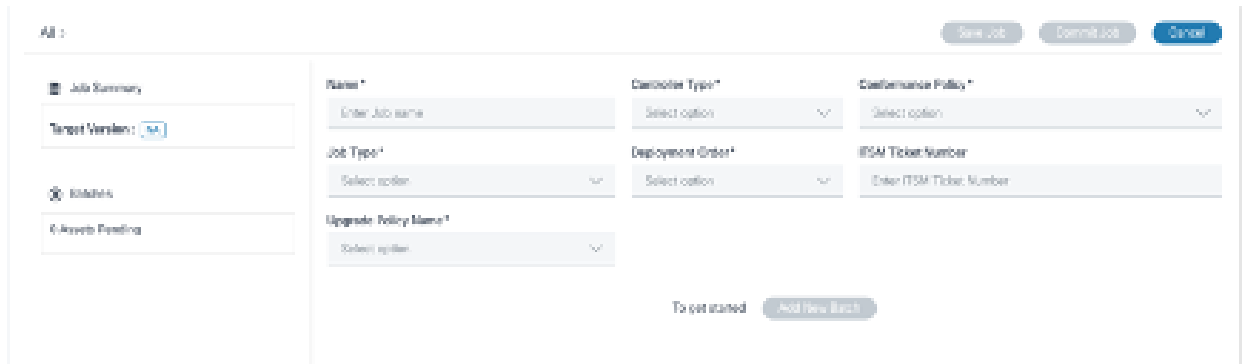
アップグレードジョブのスケジュール

ジョブを作成するには、次の手順に従います。



アップグレードジョブの作成オプション

1. Upgrade Jobページで、More Optionsアイコン> Create Jobを選択します。Create Upgrade Jobページが表示されます。



アップグレードジョブの作成

2. Nameフィールドにジョブ名を入力します。
3. コントローラタイプ (Cisco Catalyst Center、vManage、NDFC、Direct-to-Device、CNC、FMC、ANSIBLE、NSOなど) を選択します。
4. 適合しないデバイスを含む適合ポリシーを選択します。

 注：リストから使用できるのは、1回以上実行され、1つ以上の非適合デバイスを持つ適合ポリシーだけです。ポリシーを選択すると、使用する適用可能なアップグレードポリシーが自動的に識別されます。

Create Jobフォームの左側のJob Summaryの下に、次の詳細情報が表示されます。

- 影響を受けるデバイスモデル

 注：選択した準拠ポリシーに複数のデバイスモデルが関連付けられている場合、複数のデバイスモデルが表示されます。

- ターゲットバージョン
- 既存のリリースバージョンと対応する数の集計
- 許可されるバッチの最大数
- 適合しない資産の総数

 注意：選択した準拠ポリシーが複数のデバイスモデルに関連付けられている場合、すべての関連モデルの非適合資産の集計が表示されます。

- バッチを追加するオプション

5. 次のいずれかのアップグレードジョブの種類を選択します。

- 配布：配布のみのジョブは、実際のアクティベーションの前にソフトウェアイメージのステージングが行われる場合に役立ちます
- アクティベーション：アクティベーション専用ジョブは、すでに配布が完了しているデバイスのアップグレードを配布のみのジョブを使用して実行するのに役立ちます
- 配布とアクティブ化：イメージの配布とステージングとアクティブ化はどちらも同じジョブ内で行われるため、デバイスへのイメージのコピーとアップグレードの両方をカバーするメンテナンス期間を十分に確保できる場合に便利です

6. Upgrade Orderを選択します。パラレルモードでは複数のデバイスが同時に処理されますが、シーケンシャルモードではデバイスが1つずつ処理されます。

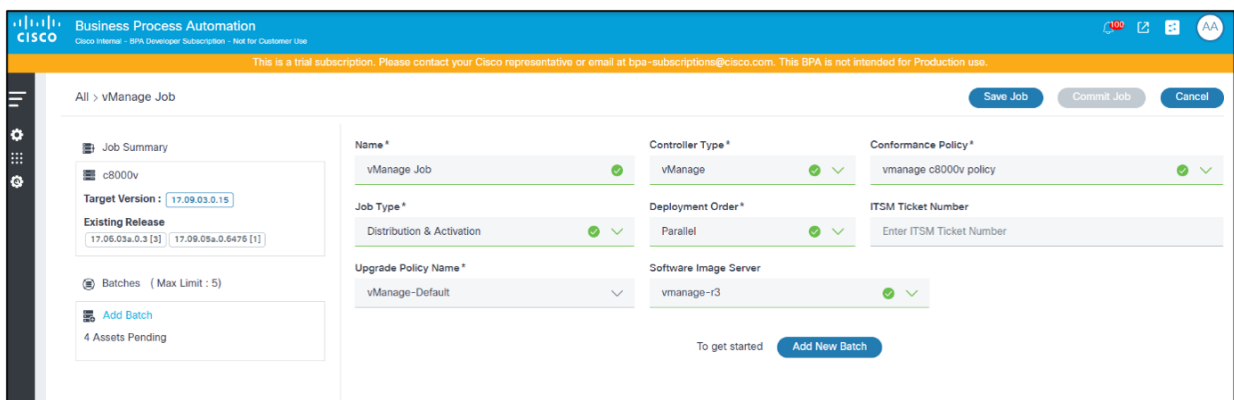
 注：パラレルモードで処理できるデバイスの最大数は、導入構成によって異なります。選択したアップグレード順序はジョブ全体に適用できますが、必要に応じて特定のバッチ内で上書きできます。

7. IT Service Management(ITSM)Ticket Numberフィールドに変更要求番号を追加します。

8. Upgrade Policy Nameを選択します。コントローラのタイプと適合ポリシーデバイスモデルに基づいて、適用可能なアップグレードポリシーのみが表示されます。ユーザはアップグレードポリシーの1つを選択できます。ソフトウェア準拠ポリシーに複数のモデルが関連付けられている場合、各モデルに関連付けられているすべての関連アップグレードポリシーが表示されます。すべてのモデルで有効なアップグレードポリシーを慎重に選択してください。

9. Software Image Serverを選択して、どのvManageイメージリポジトリ（ローカルまたはリモートなど）を使用するかを指定します。

 注：この入力は、vManageコントローラタイプにのみ適用されます。



詳細が入力されたアップグレードジョブの作成（準拠ポリシーに1つのモデルがある）

詳細が入力されたアップグレードジョブの作成 (準拠ポリシーに複数のモデルがあります)

- ジョブをコミットする準備ができるまで下書きを保存するには、Save Jobをクリックします。

バッチの追加と新しいバッチの追加

- バッチを追加するには、Add BatchリンクまたはAdd New Batchをクリックします。「バッチ作成」ウィンドウが開きます。

バッチの作成

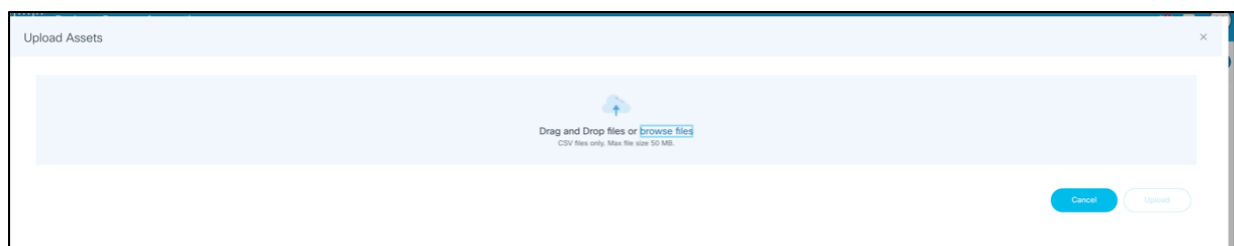
- 関連するバッチ名を入力し、展開オーダーを選択します。

 注：ここで選択したアップグレードタイプは、ジョブ作成ページで選択したアップグレードタイプより優先されます。

13. Software Image Serverを選択して、どのvManageリポジトリ（ローカルまたはリモートなど）を使用するかを指定します。

 注：このフィールドは、vManageコントローラタイプにのみ適用されます。ここで選択したSoftware Image Serverは、「Job Creation」ページで選択したサーバより優先されます

14. 資産をバッチに追加します。資産は、次の2つの方法でバッチに追加できます。



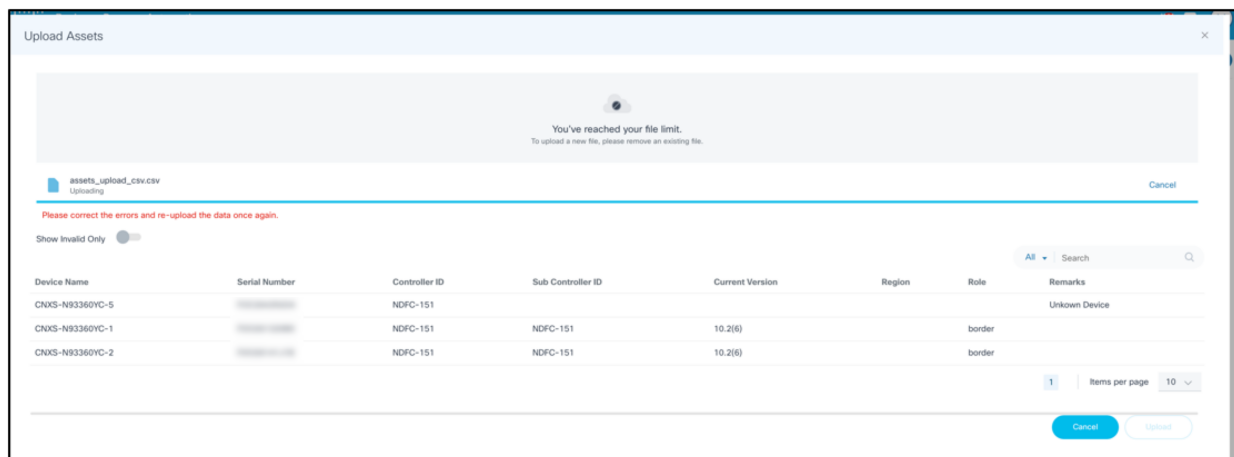
アセットのアップロード

オプション 1：

- a. Upload Assetsをクリックします。Upload Assetsウィンドウが開きます。
- b. アップロードする.csvファイルを選択します。

 注:.csvファイルには、次の詳細情報が含まれている必要があります。

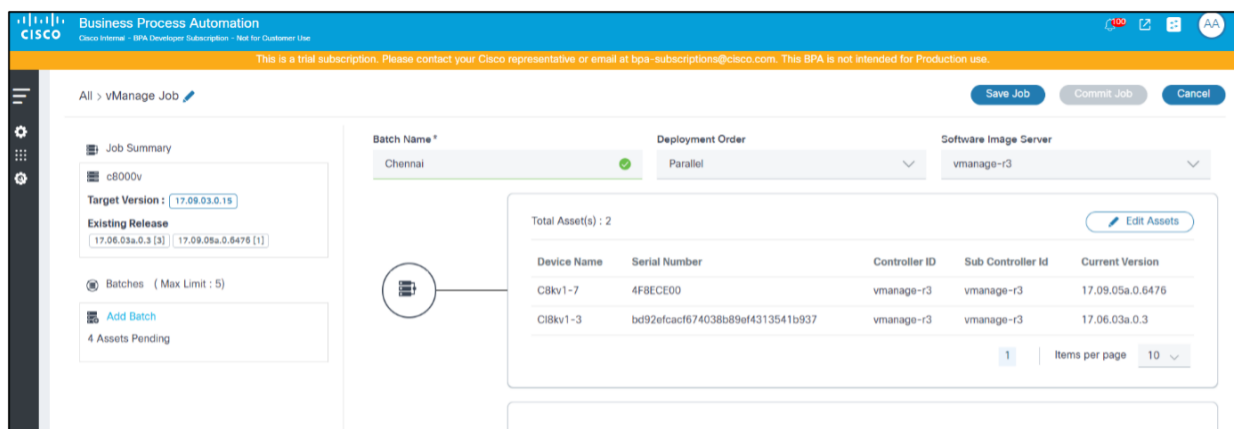
- デバイス名：デバイスまたはアセットの名前
 - シリアル番号：デバイスのシリアル番号
 - コントローラID:デバイスを管理するコントローラの名前
 - Sub Controller ID:デバイスを管理するサブコントローラIDの名前
- c. [Upload] をクリックします。.csvファイルのデータが検証され、有効なデータと無効なデータの両方が表示されます。Show Invalid Onlyトグルを使用すると、アップロードされたアセットの詳細から無効なデバイスをフィルタリングできます。



CSVファイルでアップロードされたサンプルアセット

- d. アップロードしたファイルにエラーがある場合は、エラーを修正してから再度アップロードします。

 注：アップロードされたすべてのデバイスが有効な場合のみ、ユーザは資産選択を続行できます。



バッチの追加 – 選択した資産

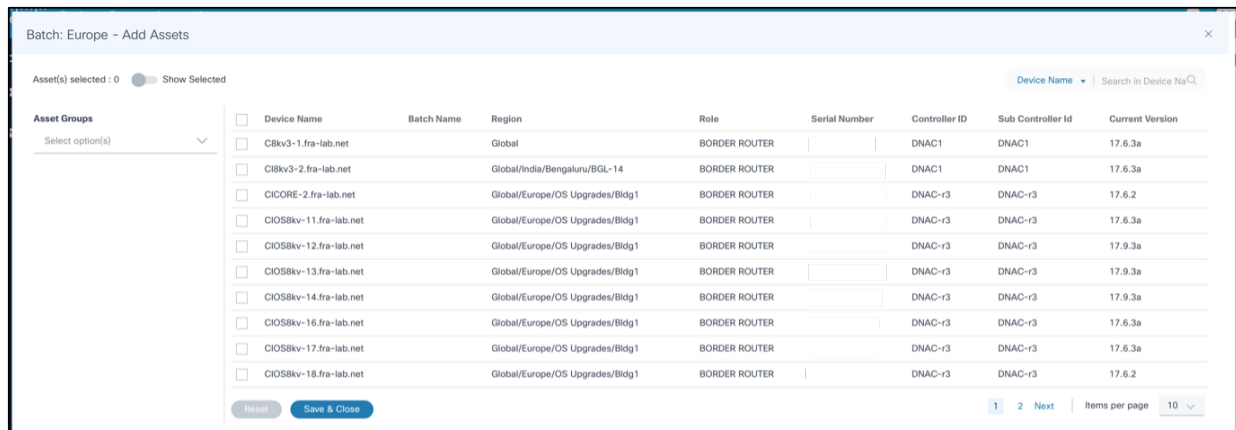
オプション 2：

- a. Add Assetsをクリックします。Asset Selectionウィンドウが開きます。

 注：資産のアップロード およびAdd Assetsは同時に使用できません。

- b. FMCコントローラタイプの場合は、アップグレードを実行するコントロールノードまたはスタンドアロンノードを選択します。

 注：データノードのアップグレードはコントロールノードで処理されるため、データデバイスはアップグレードジョブでは許可されません。



Device Name	Batch Name	Region	Role	Serial Number	Controller ID	Sub Controller Id	Current Version
☐ C8kv3-1.fra-lab.net		Global	BORDER ROUTER		DNAC1	DNAC1	17.6.3a
☐ C8kv3-2.fra-lab.net		Global/India/Bengaluru/BGL-14	BORDER ROUTER		DNAC1	DNAC1	17.6.3a
☐ CIOCORE-2.fra-lab.net		Global/Europe/OS Upgrades/Bldg1	BORDER ROUTER		DNAC-r3	DNAC-r3	17.6.2
☐ CIO8kv-11.fra-lab.net		Global/Europe/OS Upgrades/Bldg1	BORDER ROUTER		DNAC-r3	DNAC-r3	17.6.3a
☐ CIO8kv-12.fra-lab.net		Global/Europe/OS Upgrades/Bldg1	BORDER ROUTER		DNAC-r3	DNAC-r3	17.9.3a
☐ CIO8kv-13.fra-lab.net		Global/Europe/OS Upgrades/Bldg1	BORDER ROUTER		DNAC-r3	DNAC-r3	17.9.3a
☐ CIO8kv-14.fra-lab.net		Global/Europe/OS Upgrades/Bldg1	BORDER ROUTER		DNAC-r3	DNAC-r3	17.9.3a
☐ CIO8kv-16.fra-lab.net		Global/Europe/OS Upgrades/Bldg1	BORDER ROUTER		DNAC-r3	DNAC-r3	17.6.3a
☐ CIO8kv-17.fra-lab.net		Global/Europe/OS Upgrades/Bldg1	BORDER ROUTER		DNAC-r3	DNAC-r3	17.6.3a
☐ CIO8kv-18.fra-lab.net		Global/Europe/OS Upgrades/Bldg1	BORDER ROUTER		DNAC-r3	DNAC-r3	17.6.2

デバイスの選択

c. 現在のバッチに含める適切なデバイスを選択します。

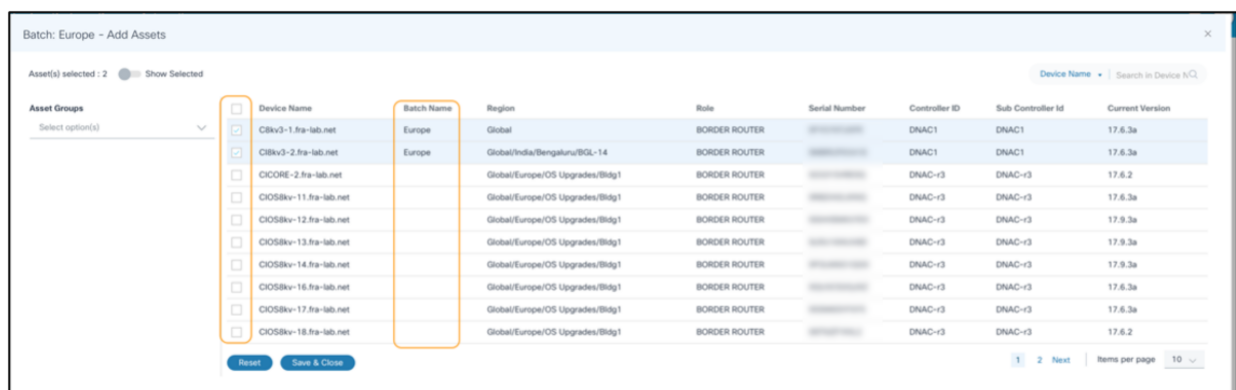
検索フィルタを使用して、異なる属性に基づいてデバイスをフィルタリングできます。フィルタリング条件に一致するすべてのデバイスは、デバイス名列ヘッダーのチェックボックスをオンにすることで、一括で選択できます。ユーザは、資産グループでフィルタリングするオプションもあります。

Show Selectedトグルを有効にすると、選択したアセットのみを表示できます。

 注：Show Selected切り替えが有効な場合、Asset Groupsフィルタは無効になります。

d. Save and Closeをクリックします。

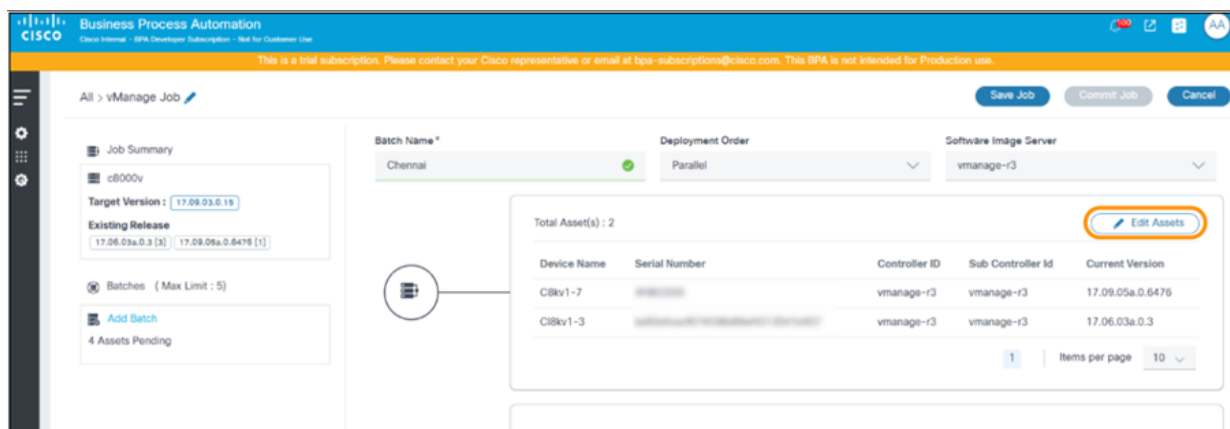
Resetをクリックすると、選択内容が破棄され、アセット選択の元の状態が保持されます。



Device Name	Batch Name	Region	Role	Serial Number	Controller ID	Sub Controller Id	Current Version
☒ C8kv3-1.fra-lab.net	Europe	Global	BORDER ROUTER		DNAC1	DNAC1	17.6.3a
☒ C8kv3-2.fra-lab.net	Europe	Global/India/Bengaluru/BGL-14	BORDER ROUTER		DNAC1	DNAC1	17.6.3a
☐ CIOCORE-2.fra-lab.net		Global/Europe/OS Upgrades/Bldg1	BORDER ROUTER		DNAC-r3	DNAC-r3	17.6.2
☐ CIO8kv-11.fra-lab.net		Global/Europe/OS Upgrades/Bldg1	BORDER ROUTER		DNAC-r3	DNAC-r3	17.6.3a
☐ CIO8kv-12.fra-lab.net		Global/Europe/OS Upgrades/Bldg1	BORDER ROUTER		DNAC-r3	DNAC-r3	17.9.3a
☐ CIO8kv-13.fra-lab.net		Global/Europe/OS Upgrades/Bldg1	BORDER ROUTER		DNAC-r3	DNAC-r3	17.9.3a
☐ CIO8kv-14.fra-lab.net		Global/Europe/OS Upgrades/Bldg1	BORDER ROUTER		DNAC-r3	DNAC-r3	17.9.3a
☐ CIO8kv-16.fra-lab.net		Global/Europe/OS Upgrades/Bldg1	BORDER ROUTER		DNAC-r3	DNAC-r3	17.6.3a
☐ CIO8kv-17.fra-lab.net		Global/Europe/OS Upgrades/Bldg1	BORDER ROUTER		DNAC-r3	DNAC-r3	17.6.3a
☐ CIO8kv-18.fra-lab.net		Global/Europe/OS Upgrades/Bldg1	BORDER ROUTER		DNAC-r3	DNAC-r3	17.6.2

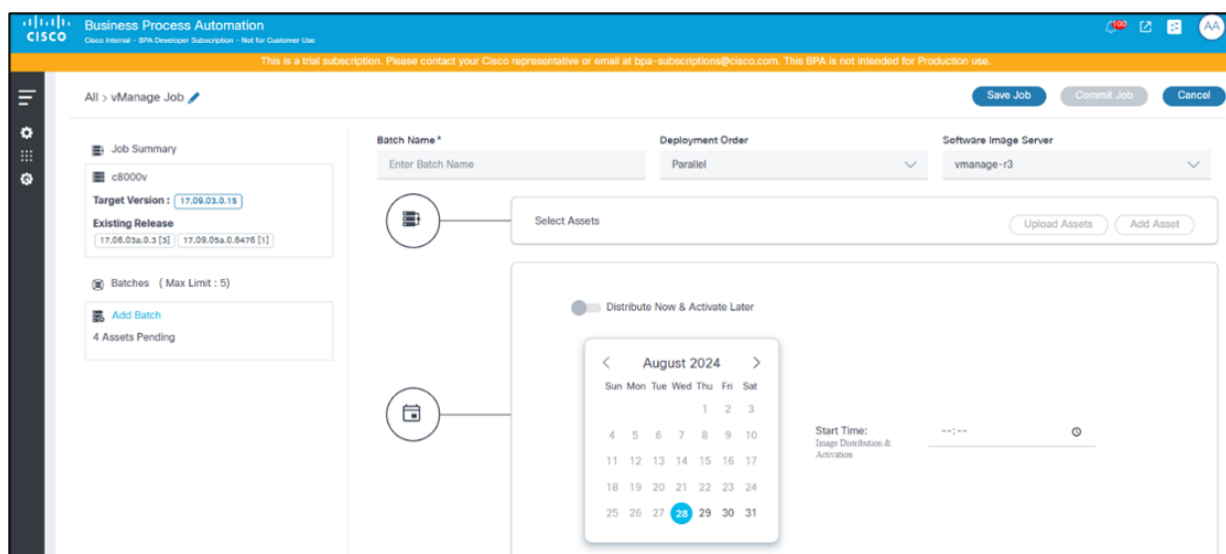
リセット

- e. アセットの選択で変更が必要な場合は、Edit Assetsをクリックします。



アセットのバッチ編集

- f. アセットを選択またはクリアして必要な変更を行い、Save and Closeをクリックします。バッチ資産の編集中に、別のジョブとバッチの一部である現在選択されている資産を識別するには、チェックマークと「バッチ名」列に表示されるバッチ名を使用します。



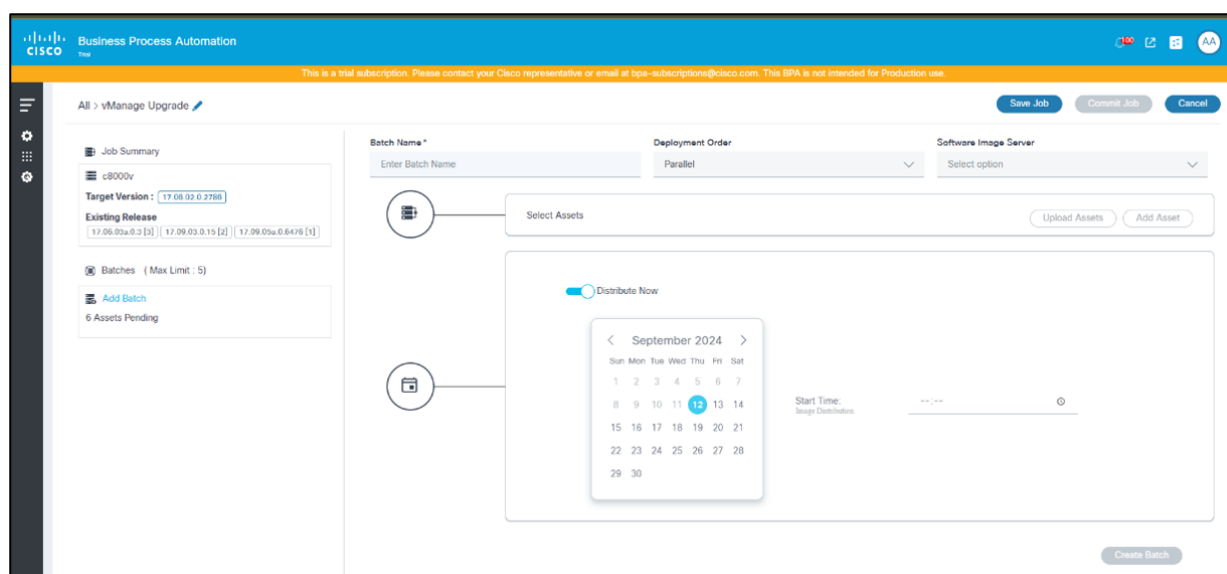
アップグレードジョブスケジューラ

15. 日付ピッカーから日付を選択し、時刻ピッカーから時刻を選択して、現在のバッチに対して選択したアップグレードタイプをトリガーする時刻をスケジュールします。

 注意：選択した製造オーダー・タイプによって、使用可能な計画のタイプが変更されます。

考えられるシナリオを次に示します。

ジョブの種類	今すぐ配布の切り替え	スケジュール日時	配布の詳細
配信	デフォルトで無効	アクティブ	配布は、指定されたスケジュールされた日時に実行されます
配信	Enabled	Disabled	ジョブのコミット後に配布が行われる
有効化	N/A	アクティブ	アクティブ化は指定された日時に行われます
配布とアクティベーション	デフォルトで無効	アクティブ	配布とアクティブ化は指定された日時に行われます
配布とアクティベーション	Enabled	アクティブ	ジョブのコミットおよびアクティブ化のトリガー後に、指定されたスケジュールされた日時に配布が実行されます



配布ジョブ・タイプ計画オプション

CISCO Business Process Automation
This is a trial subscription. Please contact your Cisco representative or email at bpa-subscriptions@cisco.com. This BPA is not intended for Production use.

Save Job Commit Job Cancel

All > vManage Upgrade

Job Summary

c8000v

Target Version: 17.06.02.0.2788

Existing Release: 17.06.03a.0.3 [2] 17.09.03.0.15 [2] 17.09.05a.0.6476 [1]

Batches (Max Limit: 5)

Add Batch

6 Assets Pending

Batch Name*
Enter Batch Name

Deployment Order
Parallel

Software Image Server
Select option

Select Assets

Upload Assets Add Asset

Start Time: Image Activation

Create Batch

有効化ジョブタイプスケジュールオプション

Distribute Now & Activate Later

Start Time: 13:10

Create Batch

配布およびアクティベーションのジョブタイプスケジュールオプション

CISCO Business Process Automation
This is a trial subscription. Please contact your Cisco representative or email at bpa-subscriptions@cisco.com. This BPA is not intended for Production use.

Save Job Commit Job Cancel

All > vManage Upgrade

Job Summary

c8000v

Target Version: 17.06.02.0.2788

Existing Release: 17.06.03a.0.3 [2] 17.09.03.0.15 [2] 17.09.05a.0.6476 [1]

Batches (Max Limit: 5)

Add Batch

6 Assets Pending

Batch Name*
Enter Batch Name

Deployment Order
Parallel

Software Image Server
Select option

Select Assets

Upload Assets Add Asset

Distribute Now & Activate Later

Start Time: Image Activation

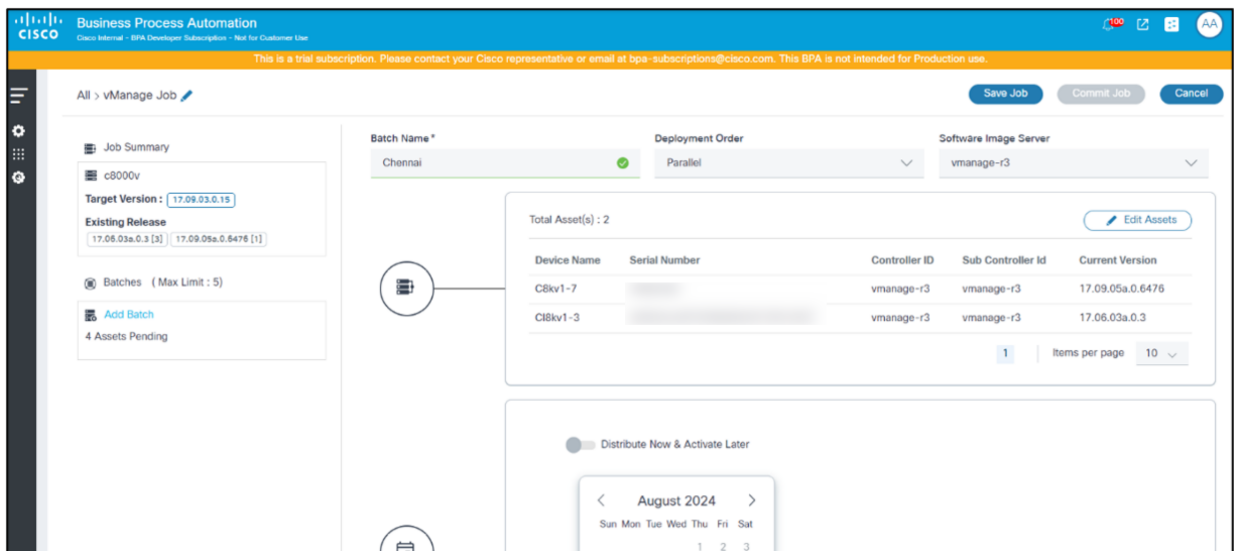
Create Batch

配布とアクティベーションのジョブタイプスケジュールオプション ([今すぐ配布して後でアクティブ化]切り替えが有効になっている場合)

 注：次のリストに注意してください。

- 複数のバッチをスケジュールする場合は、システムの過負荷を回避できるように、2つのバッチの間にタイムギャップを設けてください。複数のバッチが重複している場合は、それらを1つのバッチに追加することを検討してください。
- 今すぐ配布して後でアクティブ化切り替えが有効な場合は、ジョブコミット時間とアクティベーションスケジュールの時間の間隔を指定します。アクティブ化されていない場合、アクティブ化ワークフローは手動による介入を必要とするユーザタスクを作成する可能性があります (ユーザは配布が完了するまで待ってから再試行する必要があります) 。

16. Create Batchをクリックします。バッチは、ページの左側に表示できます。



ジョブの作成 – ジョブのコミット

必要な数のバッチを作成します。必要な情報がすべて使用可能になるまで、ジョブをドラフト状態にすることができます。

 注：Save Jobをクリックしてドラフトを保存することで、ジョブデータの損失を回避してください。

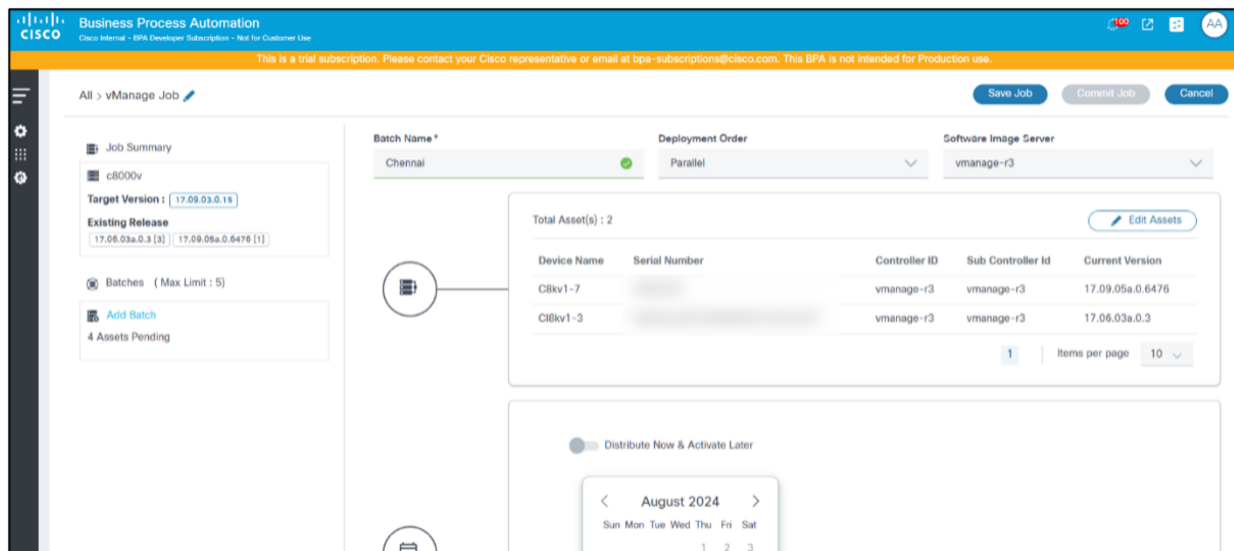
17. Commit Jobをクリックして、ジョブの作成を終了します。いずれかのバッチに対してスケジュールがトリガーされると、ジョブは「配布」状態に移行します。

 注：最大バッチ数のしきい値は、アップグレードポリシーページで拡張または更新できます。

ジョブでのバッチの編集

 注意：バッチを更新できるのは、ジョブがドラフト段階の場合のみです。

1. 左側のパネルから目的のバッチを選択します。



アセットの編集

2. Edit Assetsをクリックします。
3. 資産の追加または資産のアップロードで資産を選択または消去するか、日付または開始時刻を変更してバッチスケジュールを変更して、必要な変更を行います。
4. Update Batchをクリックします。

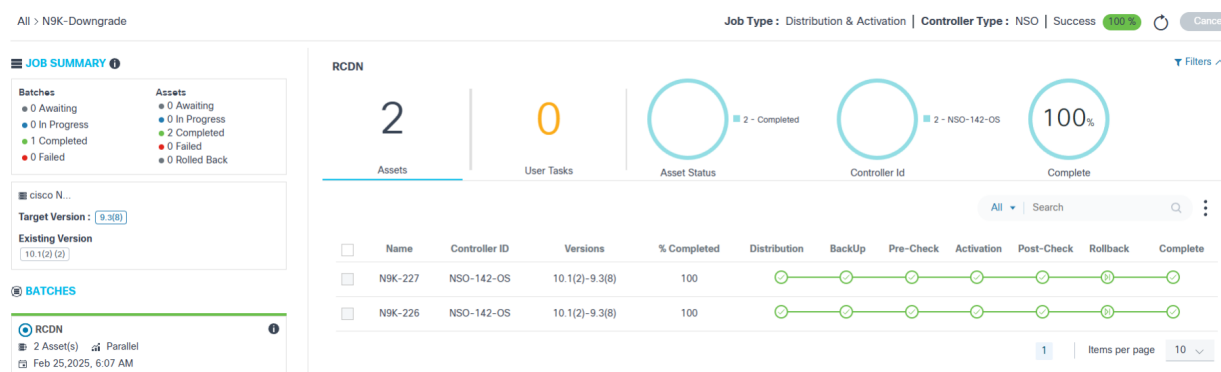
アップグレードジョブの実行と進行状況の監視

1. アップグレードジョブにアクセスできるクレデンシャルを使用してBPAにログインします。
2. OS Upgrade > Upgrade Jobsの順に選択します。Upgrade Jobページが表示されます。

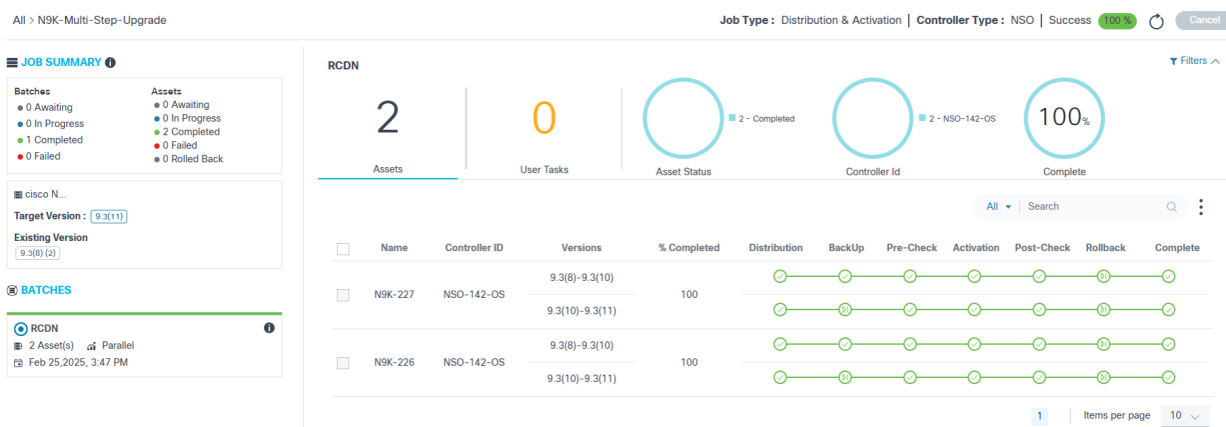


アップグレードジョブ

3. 検索フィルタと使用可能なグラフフィルタを組み合わせると、ジョブを迅速にフィルタリングできます。
4. 目的のジョブをクリックします。Job Summaryページが表示されます。



シングルステップアップグレード



複数ステップのアップグレード

左側のパネルには、次の情報が表示されます。

All > N9K-Multi-Step-Upgrade

☰ JOB SUMMARY ⓘ

Batches

- 0 Awaiting
- 0 In Progress
- 1 Completed
- 0 Failed

Assets

- 0 Awaiting
- 0 In Progress
- 2 Completed
- 0 Failed
- 0 Rolled Back

ジョブサマリー

- バッチとそれぞれの資産の概要

☰ c8000v

Target Version : 17.09.01a.0.240

Existing Version

17.09.03.0.15 (1)

準拠ポリシーの詳細 (ポリシーに1つのモデルがある場合)

 N9K-C93...,N9K-C93...

Target Version :

10.2.5

Existing Release

9.3(7) [4]

準拠ポリシーの詳細（ポリシーに複数のモデルがある場合）

- ジョブの影響を受けるデバイスのモデル、ターゲットソフトウェアのバージョン、および既存のリリースバージョン
- このジョブの一部であるバッチのリスト

 BATCHES

 chennai

 1 Asset(s)  Parallel

 Aug 14,2023, 12:20 PM

バッチ詳細

- バッチ詳細：
 - 灰色の上枠線は、バッチがスケジュールを待機していることを示します
 - 上の青い枠線は、バッチ配置が進行中であることを示します
 - 上の緑色の枠線は、バッチ配置が完了したことを示します

Job Summaryページの上部に、次の情報が表示されます。

All > vmanage_1_2_e2e

Job Type : Distribution & Activation | Controller Type : vManage | Success

100 %



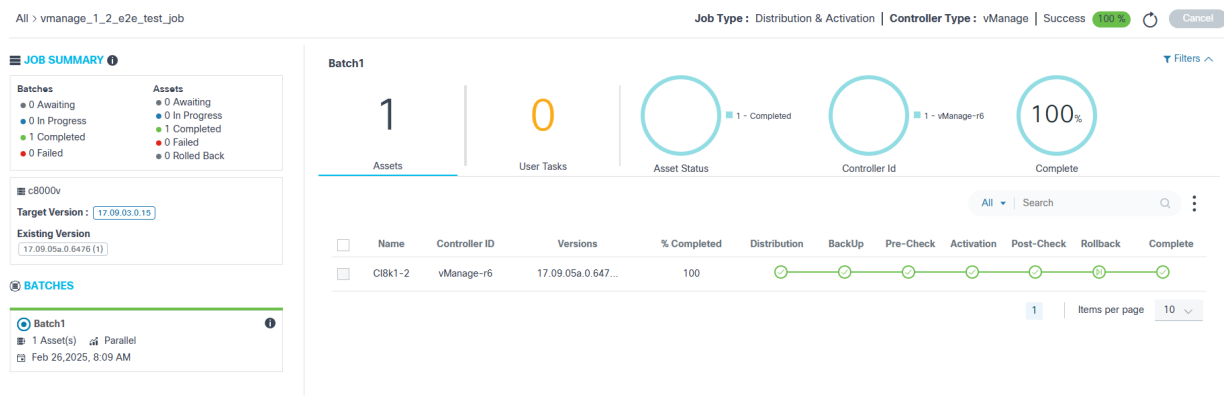
Cancel

ジョブの概要のトップ

- 現在のジョブのブレッドクラムナビゲーション（例：All > vmanage_1_2_e2e）。AllオプションはJobsダッシュボードに切り替わります
- ジョブの種類
- コントローラ タイプ
- 完了割合を含むジョブの状態：
 - 成功：アップグレードジョブが成功しました
 - Failed：アップグレードジョブが何らかの理由で失敗しました
 - In-Progress：アップグレードジョブが進行中です

 **注意:** 1つのバッチのスケジュールに達した場合でも、製造オーダー・ステータスは「進行中」に移動されます

- 待機中：ジョブはコミットされていますが、1つ以上のバッチスケジュールに達するのを待機中です



ジョブサマリー

Job Summaryページでは、次のオプションを使用できます。

- Refreshアイコンを使用すると、更新をオンデマンドで取得できます
- Cancelは、いずれかのバッチのスケジュールに達していない限り、ドラフトステージおよびコミットステージのジョブをキャンセルするために使用します
- 有効化：以前に完了したジョブに含まれていたものと同じバッチと資産を使用して、新しい有効化ジョブを「草案」状態で作成します
 - Activateは、ジョブタイプがDistributionで、正常に完了した場合にのみ使用できます
 - 有効化ジョブがすでに作成され、「有効化」をクリックすると、メッセージが以前に作成されたジョブのステータスとともに表示され、作成済みのジョブをリダイレクトするオプションが提供されます。新しく作成されたジョブでは、ユーザはバッチまたはアセットを編集または削除できますが、ジョブタイプ、コントローラタイプ、および適合ポリシーは編集できません。
- アセットのページ化されたリストが分析セクションの下に表示されます
- Searchフィールドでは、次のようなカラムを全般的に、またフィールド固有に検索できま

す。

- Device Name
- コントローラID
- シリアル番号

Name	Controller ID	Sub Controller ID	Serial Number	Distribution	BackUp	Pre-Check	Activation	Post-Check	Download
NCS540-75	CNC-211			✓	✓	✓	✓	✓	
NCS540-36	CNC-211			✓	✓	✓	✓	✓	

バッチレポートのダウンロード

- More Optionsアイコン> Downloadの順に選択して、バッチレベルのレポートをダウンロードするオプション。レポートは、バッチレベルの詳細とデバイスの詳細で構成されます

Name	Controller ID	Versions	% Completed	Distribution	BackUp	Pre-Check	Activation	Post-Check	Rollback	Complete
CNXS-N93360YC-1...	NDFC	10.2(5)-10.3.5	100	✓	✓	✓	✓	✓	✓	✓

並べ替え – シングルステップアップグレード

Name	Controller ID	Versions	% Completed	Distribution	BackUp	Pre-Check	Activation	Post-Check	Rollback	Complete
N9K-227	NSO-142-OS	9.3(8)-9.3(10)	100	✓	✓	✓	✓	✓	✓	✓
		9.3(10)-9.3(11)		✓	✓	✓	✓	✓	✓	✓

並べ替え – マルチステップアップグレード

JOB SUMMARY

Batches

- 0 Awaiting
- 0 In Progress
- 1 Completed
- 0 Failed

Assets

- 0 Awaiting
- 0 In Progress
- 1 Completed
- 0 Failed
- 0 Rolled Back

ASR9K

Target Version : 7.7.2

Existing Version : 7.6.2 (1)

BATCHES

chennai

1 Asset(s) Parallel

Feb 19, 2025, 4:48 PM

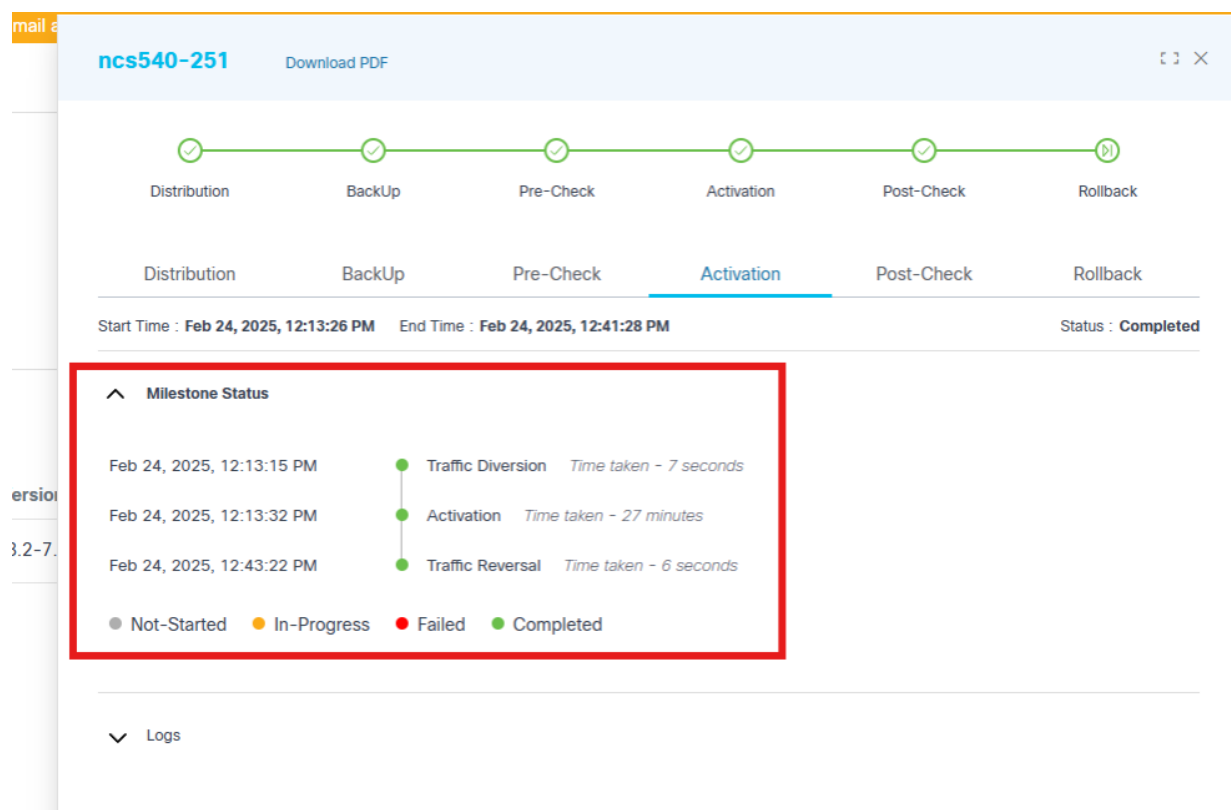
Name	Controller ID	Versions	% Completed	Distribution	BackUp	Pre-Check	Activation	Post-Check	Rollback	Complete
ASR9K-79	NSO-142	7.6.2-7.6.2[Bri...]	100	✓	✓	✓	✓	✓	✓	✓
		7.6.2[Bridge SM...]		✓	✓	✓	✓	✓	✓	✓

並べ替え : ブリッジSMUアップグレード

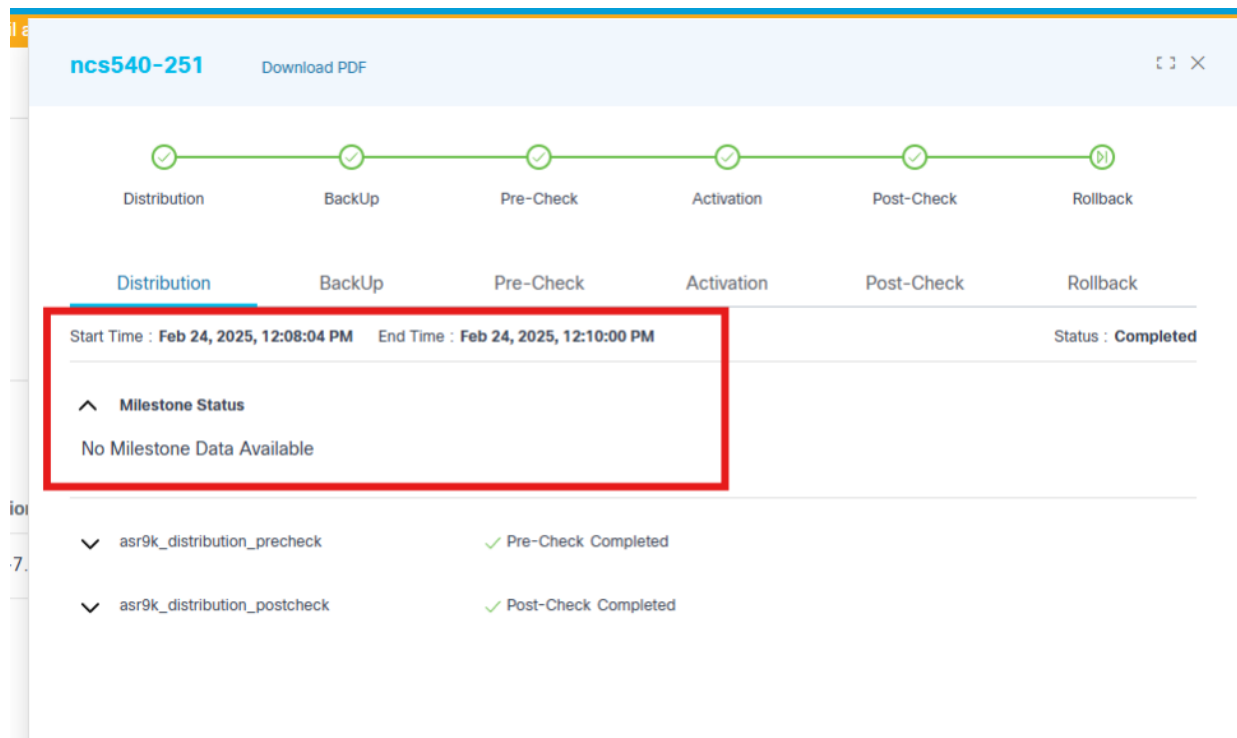
- 並べ替えは、列名をクリックして実行できます
- 各デバイスについて、名前、コントローラID、バージョン、および%完了とともに、次のアップグレードマイルストーンが表示されます。
 - 配信
 - バックアップ
 - 事前チェック
 - トラフィック転送
 - 有効化
 - チェック後
 - トラフィックリバーサル
 - ロールバック
 - 完了

 注: 「%完了」には、デバイスのマイルストーンの完了数に基づいて進行状況が表示されます。バッチ内のすべてのデバイスレベルの完了率が集計され、バッチ完了率が計算されます。次に、すべてのバッチ完了率が集計され、ジョブ・レベルの完了率が計算されます。

カスタムマイルストーンとも呼ばれるサブマイルストーンは、追加されたときに標準マイルストーンの下で実行され、表示される中間の重要なステップです。カスタムマイルストーンの追加の詳細については、『[BPA Developer Guide](#)』を参照してください。



サブマイルストーンビュー (標準マイルストーン名にサブマイルストーンが追加されている場合)



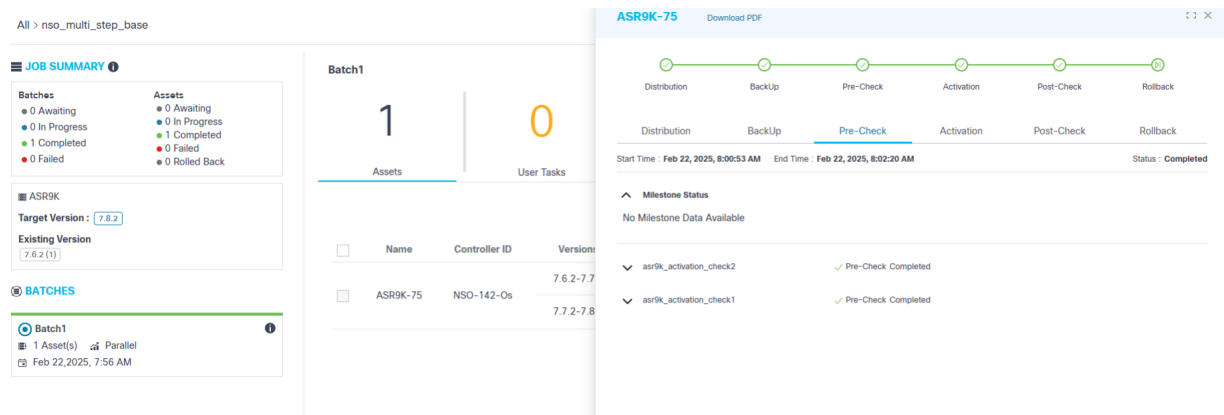
サブマイルストーンビュー（標準マイルストーン名にサブマイルストーンが追加されていない場合）

 注：マイルストーンは、選択した職種によって異なります。TrafficReversalマイルストーンは配布ジョブでは使用できません。

トラフィック転送とトラフィック反転は、アクティベーションマイルストーンの下に移動します。

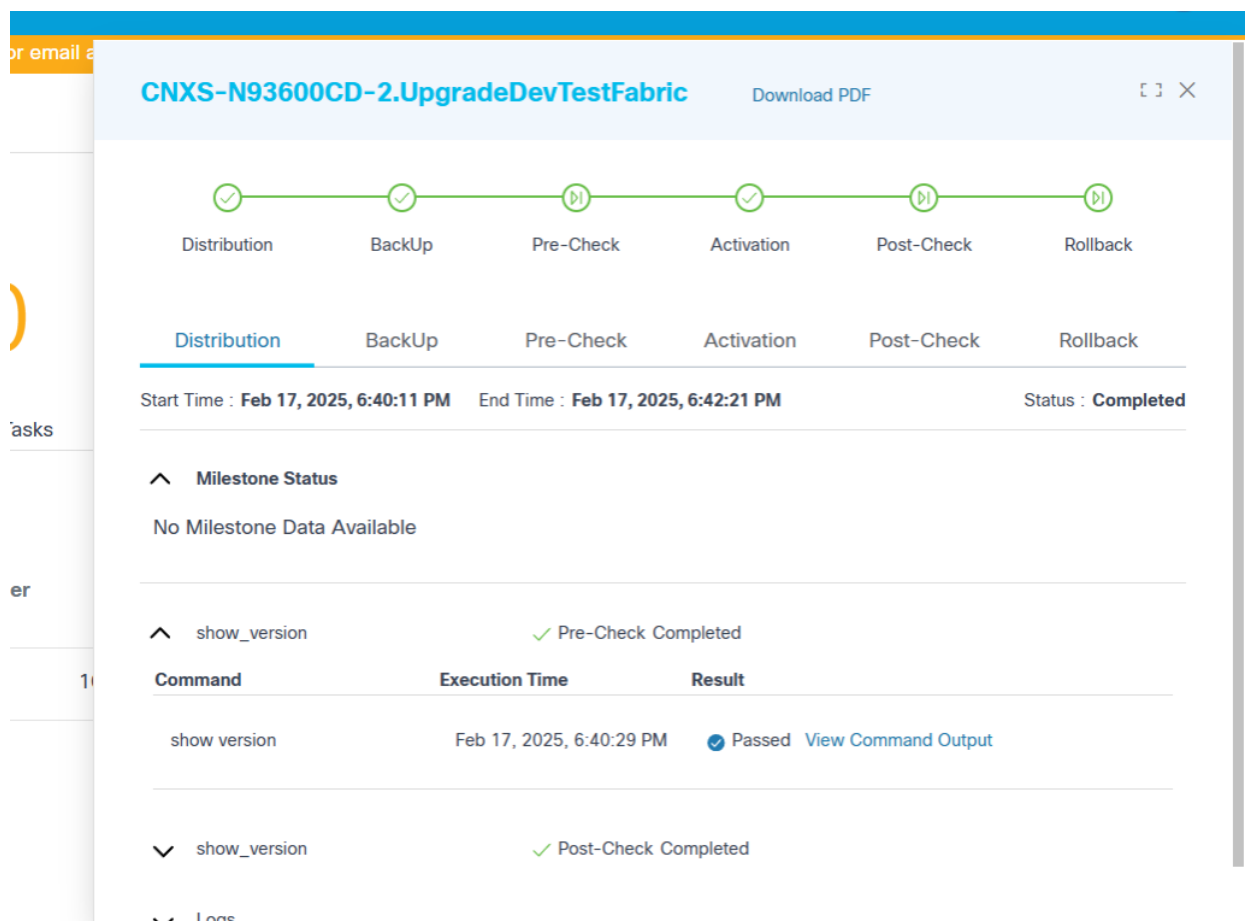
・マイルストーンの色の凡例で、次の要素で構成されます。

- 。灰色のチェック：保留中
- 。ブルーチェック：進行中
- 。緑のフラグ：スキップ
- 。緑色のチェック：完了
- 。オレンジ色のチェック：ユーザタスク
- 。レッドチェック：失敗



事前および事後のマイルストーン表示

チェック前またはチェック後の実行を伴うマイルストーンの場合、ユーザーは完全なコマンド出力と、それぞれのプロセステンプレートで設定されたすべてのコマンドの検証ルールおよびステータスを表示できます。



事前確認コマンド出力を含む配信マイルストーンビュー

1. コマンドの出力と、チェック前およびチェック後のコマンドに関連付けられているルールを表示するには、View Command Outputリンクをクリックします。

Rules:

View Rules

Operation

Result

#Rule1

!Contains

✓

▼

Command Output:

Tue Nov 26 06:14:52.404 UTC
23099260 kbytes total (14885100 kbytes free)

事前および事後のコマンド出力と関連ルール

2. 展開アイコンを選択すると、各ルールの詳細が表示されます。

Rules:

View Rules

Operation

Result

#Rule1

!Contains

✓

^

Rule:

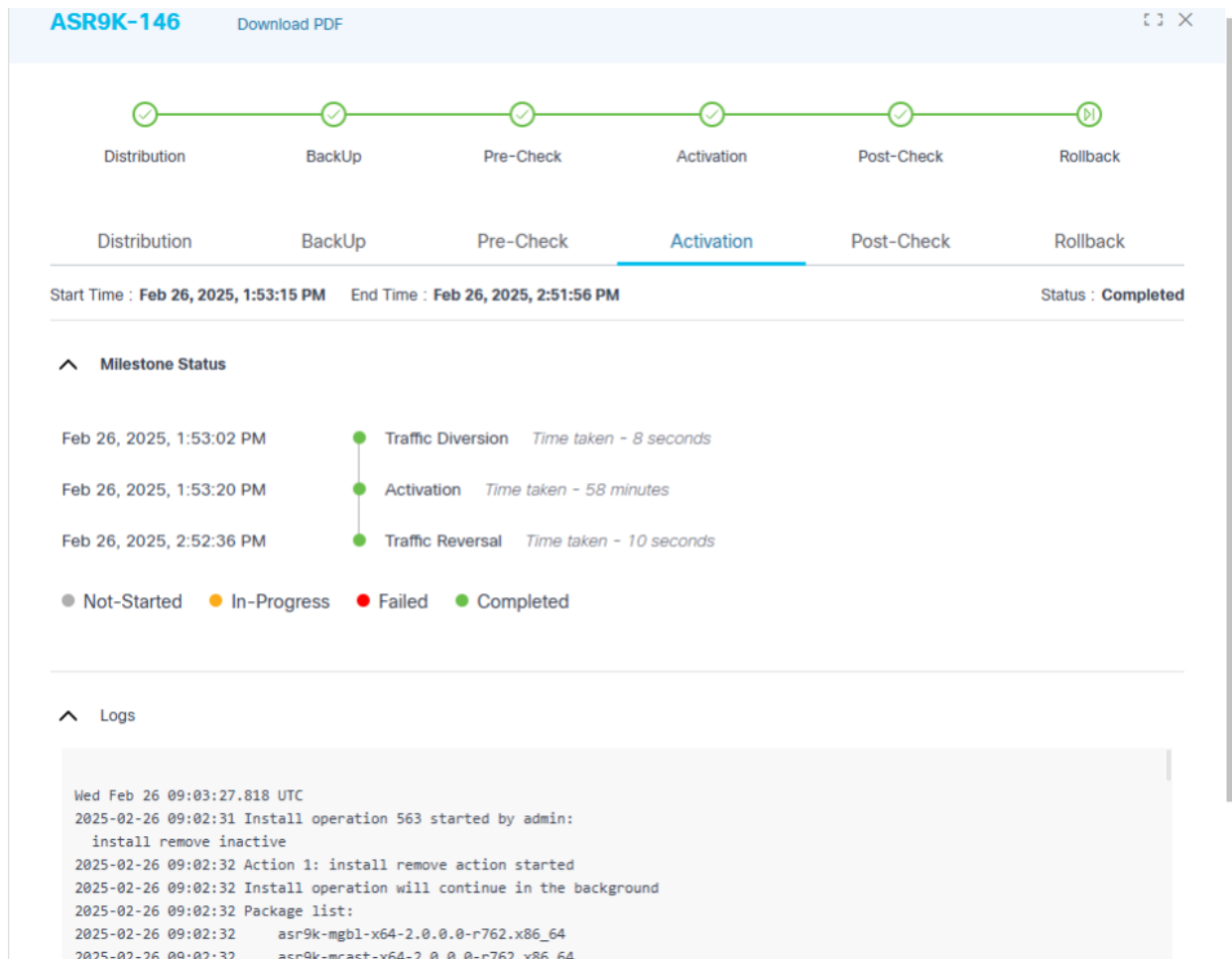
Invalid input detected

Command Output:

Tue Dec 3 20:19:26.594 UTC
disk_status_config minor 80
disk_status_config severe 90
disk_status_config critical 95
aaa admin-accounting enable false
aaa authentication users user admin
uid 9000
gid 100
password

ssh_keydir /var/confd/homes/admin/.ssh
homedir /var/confd/homes/admin
!
aaa authentication groups group aaa-r
gid 100
users %%__system_user__%%
!

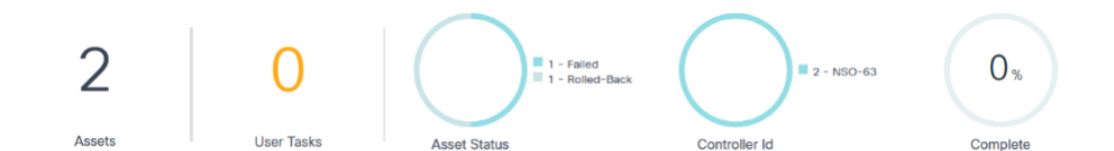
検証ルールを含む事前および事後のコマンド出力



ライブログを含むアクティベーションマイルストーンビュー

上の図は、アクティベーションのマイルストーンの詳細を示しています。これには、特定のデバイスのソフトウェアアクティベーションの進捗状況を監視するのに役立つライブログが含まれます。

マイルストーンが開始または完了したときに、そのマイルストーンをクリックすると、詳細情報が表示されます。



分析セクション

Job Summaryページの上部に表示される分析セクションには、現在選択されているジョブに関連する次の情報が表示されます。

- バッチ名 (アジアなど)
- フィルタ^は分析セクションを折りたたんで展開します
- 次のバッチの詳細が順番に表示されます。

- ユーザタスクを処理するには、ユーザタスクの数をクリックします。「ユーザタスク詳細」ウィンドウが開き、以下の情報が表示されます。



- The screenshot shows the 'User Task' dialog in Camunda. The 'Message' section displays the error: 'Error while executing task Device_DeviceID001_ServiceTask'. The 'Details' section lists the following error messages:

 - Following template(s) associated command(s) having invalid differences: ["varName_activation_check?"]
 - ["show route authority"] > [response] ["show route (all summary)"] > [response] ["show health (path)"]
 - [response] ["show status (no)"] > [response] ["varName_activation_check?"] > [response] ["show route"]

At the bottom right, there are buttons for 'Rollback', 'Retry All', 'Retry', 'Continue', 'Cancel', and 'Close'.

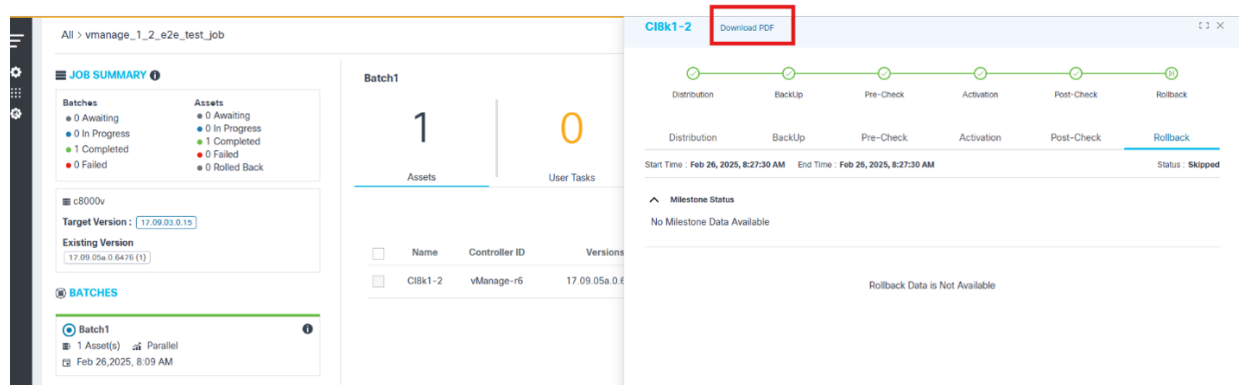
ユーザタスク

ユーザタスクの表示オプション

- タスクのコンテキストに基づいて、次のオプションが表示されます。
 - 再試行：タスクを再実行します。
 - Retry All：事前および事後のすべてのチェックを再実行します。
 - 続行：次のタスクに進みます
 - Rollback：以前のバージョンにロールバックします。このオプションは、アクティブ化またはポストチェックが失敗した場合、またはチェック前後で無効な違いが見つかった場合に使用できます
 - キャンセル：現在のジョブをキャンセルします。
 - 閉じる：「ユーザー・タスク」ウィンドウを閉じます。
- ユーザータスクがある場合はそれを実行し、Refreshアイコンを選択してユーザータスクの合計数を更新します
- バッチ完了率の合計
- コントローラIDでフィルタリングするクリック可能なグラフ

 注：コントローラIDの前の数字は、各コントローラで管理されているデバイスの合計数を示します。

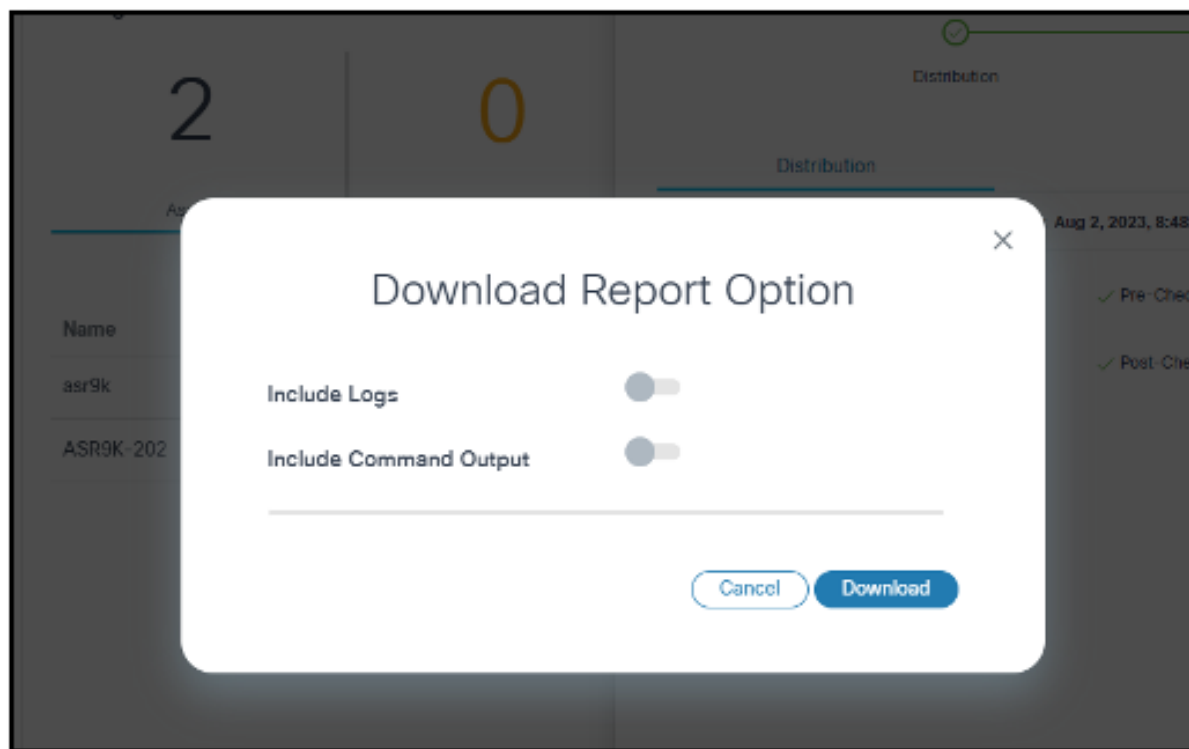
ソフトウェアアップグレードレポートのダウンロード



PDF のダウンロード

詳細表示のヘッダーに、デバイス名が表示され、続いてPDFのダウンロードが表示されます。ユーザは、現在選択されているデバイスのアップグレードレポートをPDF形式で生成およびダウンロードできます。PDF形式のアップグレードレポートをダウンロードするには、次の手順を実行します。

1. Download PDFをクリックします。Download Report Optionウィンドウが開きます。



レポートのダウンロードオプション

2. Include LogsとInclude Command Outputsのトグルを有効にします。

- Include Logs : レポートにライブログ (存在する場合) を含めます
- Include Command Output : レポートにプレチェックとポストチェックのコマンド出力を含めます。この場合、コマンド出力の後にルールが続きます

3. [Download] をクリックします。レポートの生成が開始されます。

 注: Include LogsとInclude Command Outputの両方のトグルを有効にすると、レポート生成の処理時間とレポートサイズが増加します。詳細なレポートが必要な場合にのみ、この切り替えを使用します。コマンド出力切り替えのオン/オフに関係なく、レポートにはコマンドルールが含まれます。

Device Report

Device Name	asr-147
Controller ID	D2D-OSUpgrade
Serial Number	
Current Version	7.8.2
Target Version	7.7.2

Software Upgrade Version: 7.8.2 - 7.7.2

Milestone: Distribution

Milestone	Distribution
Execution Start Time	Fri, 29 Nov 2024 05:45:45 GMT
Execution End Time	Fri, 29 Nov 2024 06:24:53 GMT
Overall Status	Completed

Pre-Check

Process Template precheck_passfailrules

Command	Execution Time	Result
admin show running-config	Wed, 21 Jan 1970 01:20:59 GMT	Failed
Rules :		
Rule	View Rules	Operation Result
#Rule1	Invalid input detected	!Contains Passed
#Rule2	asdf	Contains Failed
#Rule3	qwerty	!Contains Passed

デバイスレポート

ジョブのアーカイブ

- アップグレードジョブに十分なアクセス権を持つクレデンシャルを使用してBPAにログインします。
- OS Upgrade > Upgrade Jobsの順に選択します。Upgrade Jobページが表示されます。
- 検索フィルタを使用可能なグラフフィルタと組み合わせて使用し、ジョブをフィルタリングします。
- 1つ以上のジョブを選択します。



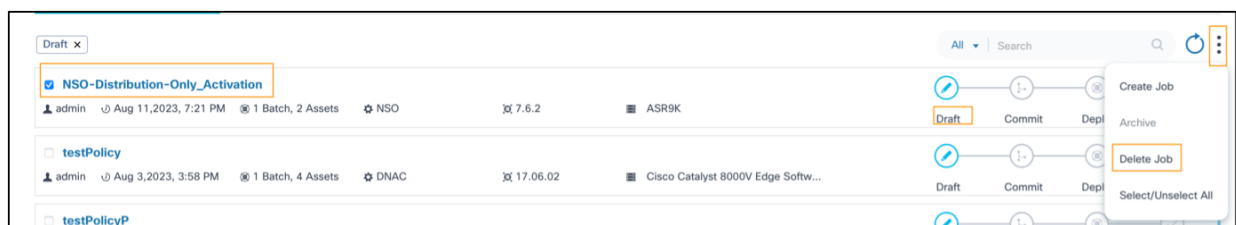
ジョブのアーカイブ

5. More Optionsアイコン> Archiveの順に選択します。

注意：アーカイブできるのは、完了した製造オーダーのみです。

ジョブの削除

1. アップグレードジョブに十分なアクセス権を持つクレデンシャルを使用してBPAにログインします。
2. OS Upgrade > Upgrade Jobsの順に選択します。Upgrade Jobページが表示されます。
3. 検索フィルタを使用可能なグラフフィルタと組み合わせて使用し、ジョブをフィルタリングします。
4. 1つ以上のジョブを選択します。



ジョブの削除

5. More Optionsアイコン> Delete Jobを選択します。

注：ジョブを削除できるのは、ジョブがドラフト段階にある場合だけです。

ジョブ内のバッチの削除

 Job Summary

 Cisco Catalyst 8000V Edge Software

Target Version : 17.06.03a

Existing Release

17.7.2 (2) 17.9.2a (11)

 Batches (Max Limit : 5)

☒ Europe 

 2 Asset(s)  Parallel

 May 20, 2023, 2:03 PM

☐ India 

 1 Asset(s)  Parallel

 May 27, 2023, 2:03 PM

 [Add Batch](#)

10 Assets Pending

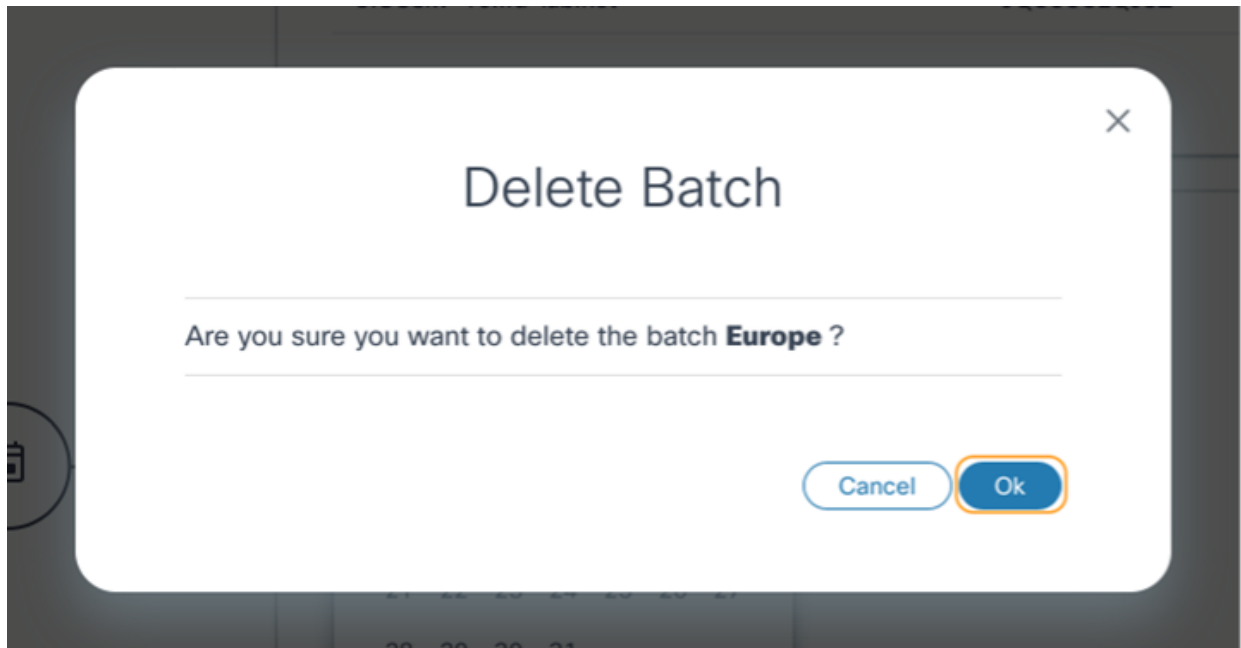
Batch Name *

Europe



ジョブ内のバッチの削除

1. サイドパネルで目的のバッチの削除アイコンを選択します。確認ウィンドウが開きます。



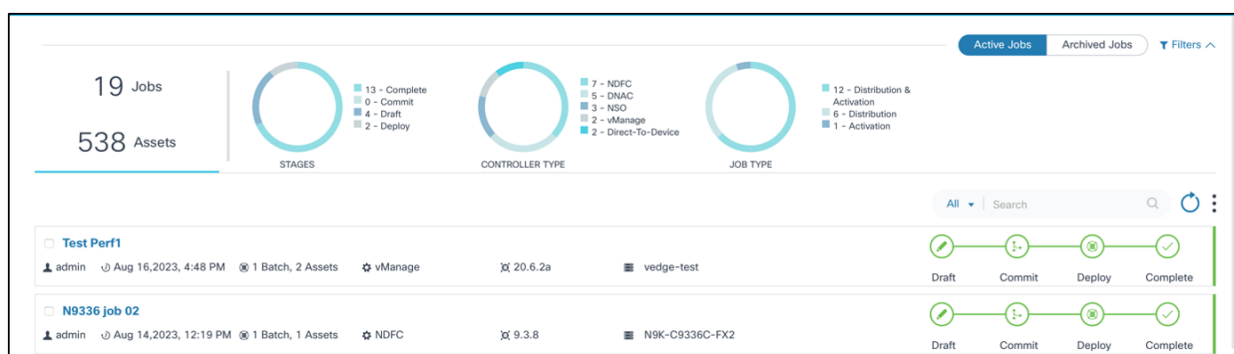
バッチの削除の確認

2. [OK] をクリックします。

削除されたバッチに関連付けられた資産は、保留中の資産プールに戻り、新規または既存のバッチで選択できるようになります。

ジョブのキャンセル

1. アップグレードジョブに十分なアクセス権を持つクレデンシャルを使用してBPAにログインします。
2. OS Upgrade > Upgrade Jobsの順に選択します。Upgrade Jobページが表示されます。



アップグレードジョブ

3. 検索フィルタと使用可能なグラフフィルタを組み合わせ使用し、目的のジョブをフィルタ

リングします。

4. 目的のジョブをクリックします。Job Summaryページが表示されます。

Last Saved On : May 11,2023, 6:11 PM

Save Job

Commit Job

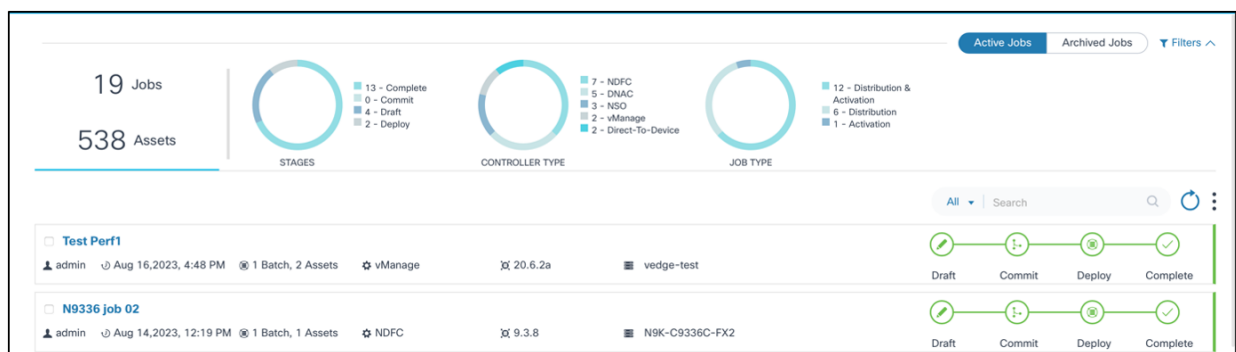
Cancel

Cancel

5. [Cancel] をクリックします。

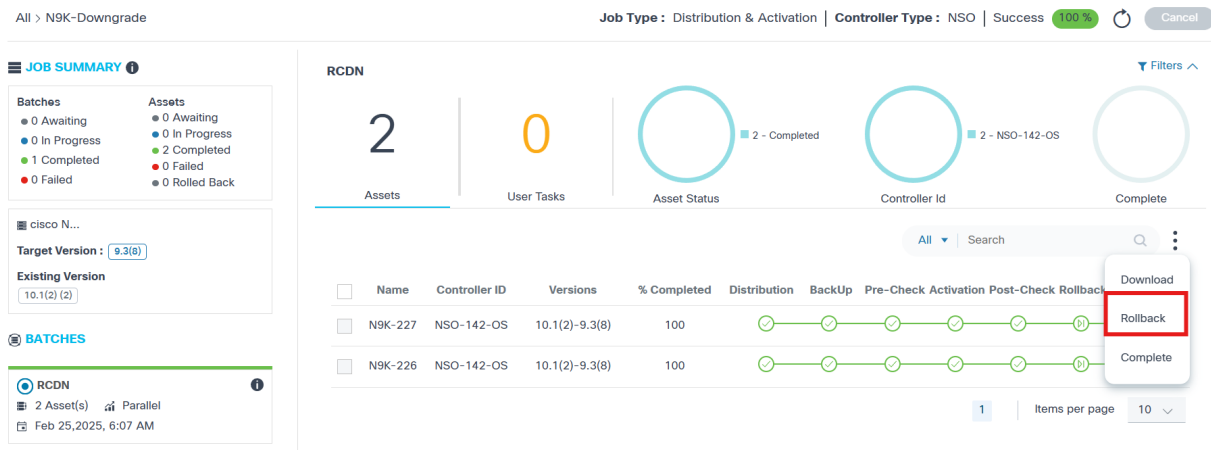
完了したジョブまたはアップグレードのロールバック

1. アップグレードジョブに十分なアクセス権を持つクレデンシャルを使用してBPAにログインします。
2. OS Upgrade > Upgrade Jobsの順に選択します。Upgrade Jobページが表示されます。



アップグレードジョブ

3. 検索フィルタと使用可能なグラフフィルタを組み合わせ使用し、目的のジョブをフィルタリングします。
4. 目的のジョブをクリックします。Job Summaryページが表示されます。左側のペインで必要なバッチを選択し、右側のパネルで完了確認/ロールバックが必要なデバイスを選択します
5. More Optionsアイコンを選択し、要件に応じてRollbackまたはCompleteのいずれかのメニューアクションをクリックします。



ロールバック

注：デバイスは、次の前提条件が満たされている場合にのみ選択できます。

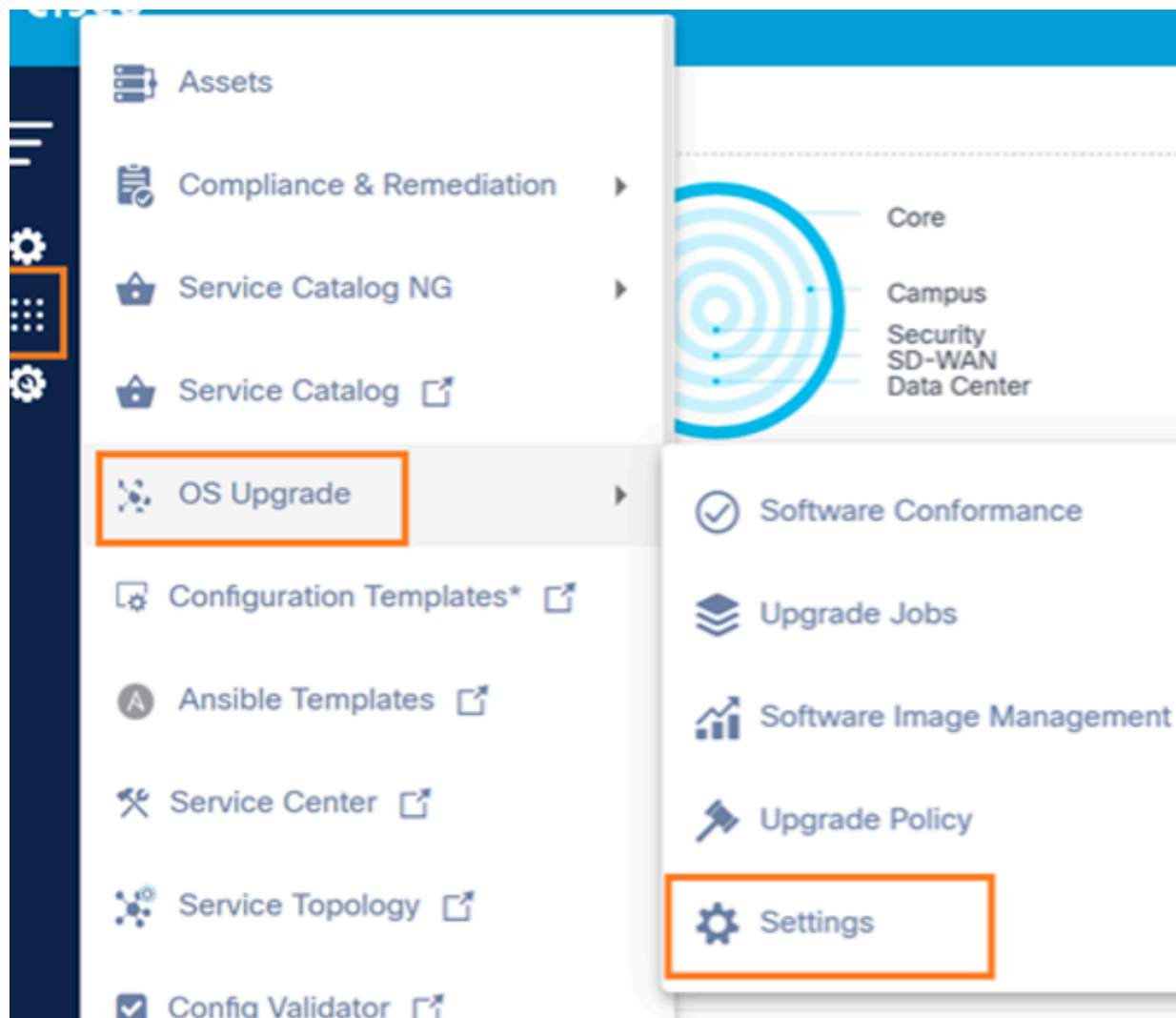
- 完了したアップグレード済みジョブのロールバックオプションを有効にするには、設定が必要です。詳細については、「[設定](#)」を参照してください。
- 時間内にアクションが実行されなければ、デバイスは自動的にComplete状態に移行します
- ロールバックがすでに完了している場合、またはロールバックマイルストーンが[待機中]状態の場合、デバイスはオンデマンドロールバックアクションに使用できます

Settings

OSアップグレード設定は、OSアップグレードアプリケーションの他のコンポーネントで 사용되는共通の設定を保持するプレースホルダを提供します。

Settingsページにアクセスするには、次の手順を実行します。

- 設定への管理アクセス権を持つクレデンシャルでBPAにログインします。



Settings

2. OS Upgrade > Settingsの順に選択します。Settingsページが開きます。

Settingsページには、次の2つのタブがあります。

- ソフトウェア準拠：自動適合実行スケジュールを許可する構成は、このタブで更新できます
- ロールバック：デバイス全体のアップグレードをロールバックできる設定は、このタブで更新できます

ソフトウェアの適合性

Software Conformance Rollback

Scheduled Conformance Check ☒ Enable

Start Date
07/04/2025

Cron Pattern

Minutes (0 - 59)	Hour (0 - 23)	Day (Month) (1 - 31)	Month (1 - 12)	Day (Week) (1 - 7)
25	7	*	*	*

Please click on save to check updated next execution date & time.

Auto Refresh Interval (seconds)
30

Reset Save

「ソフトウェア適合性」タブ

Software Conformanceタブには次の情報が表示されます。

- 計画適合チェック：計画を有効または無効にします。
- 開始日：MM/DD/YYYYを選択します。

 注：開始日は将来の日付にする必要があります。

- Cron Pattern:次の詳細情報を指定します。
 - 分(0 ~ 59)
 - 時間(0 ~ 23)
 - 日 (月) (1-31)
 - 月(1 ~ 12)
 - 日 (週) (1-7)
- Add Auto Refresh Interval：デフォルト値は30秒です
- 保存：変更の保存

ロールバック

Software Conformance Rollback

User Verification ☒ Enable

Confirmation Threshold Time (hrs)*
5

Reset Save

「ロールバック」タブ

Rollbackタブには次の情報が表示されます。

- ユーザ検証の切り替え：ユーザ検証を有効または無効にします。
 - enabled状態：アップグレードジョブ内のデバイスは、Configuration Threshold Time(hrs)で設定されたしきい値に達するまで、ユーザ確認によるロールバックまたはアップグレードの完了を待機します。しきい値に達すると、デバイスは自動的に Completed状態に移行します
 - 無効状態：アップグレードジョブ内のデバイスは、ユーザの確認を待たずに、自動的にアップグレードを完了します
- Confirmation Threshold Time:待機時間のしきい値を時間単位で追加します。
- 保存：変更の保存

導入の設定

- 準拠ポリシーチェックとSWIMメタデータの両方のデフォルトスケジュールは、現地時間の午前7:25に毎日設定されます。
- SWIMイメージメタデータ同期のデフォルトスケジュールを変更するには、BPAがインストールされているディレクトリ「<BPA install directory>/conf/@cisco-bpa-platform/mw-osupgrade-nxtgen/config.json」に移動し、Cron式を使用してschedule.swimScheduleプロパティを更新します。スケジュールは導入後に更新できます。詳細は、『[ソフトウェア準拠](#)』を参照してください。
- 異なるコントローラタイプに対してパラレルモードで処理されるデバイスの最大数を増減するには、次の手順を実行します。

1. 次のファイルを更新します。

- Cisco Catalyst Centerファイル: 「<BPA_INSTALL_DIRECTORY>/conf/@cisco-bpa-platform/mw-dnac-agent/config.json」
- vManageファイル: 「<BPA_INSTALL_DIRECTORY>/conf/@cisco-bpa-platform/mw-vmanage-agent/config.json」
- NDFCファイル: "<BPA_INSTALL_DIRECTORY>/conf/@cisco-bpa-platform/mw-ndfc-agent/config.json"
- FMCファイル: 「<BPA_INSTALL_DIRECTORY>/conf/@cisco-bpa-platform/mw-fmc-agent/config.json」

2. Update throttling > capabilities > image-activation, image-distributeの順に移動し、同時アクティブ化または配布制限を増やします。

 注：これらの制限を更新する前に、『[サポート対象のコントローラとデバイスプラットフォーム](#)』を参照してください。

アクセス制御

ロールベースアクセスコントロール

BPAはロールベースアクセスコントロール(RBAC)をサポートします。RBACモデルでは、ロールはユーザが実行できる一連の権限 (アクションなど) をカプセル化します。アクセス制御では、管理者は事前に定義されたロールまたは新しく作成されたロールをユーザグループに権限とともに割り当てることができます。ユーザは1つ以上のユーザグループに属することができ、各ユーザグループは1つ以上のロールに割り当てられて、そのグループ内のユーザに特定のアクセス権限を付与することができます。

次の表に、OOB OSアップグレードのロールと関連する権限の概要を示します。

サービス	Group	意図	スーパー 管理者	ユースケ ース管理 者	読み取り 専用ユー ザ (OSア ップグレ ードユー ススペース 読み取り 専用ユー ザ)	Operator
OSUpgradeサービ ス	ui_app	アップグレードジ ョブアプリケーション の表示/非表示 を切り替えます	Yes	Yes	Yes	Yes
OSUpgradeサービ ス	ui_app	ソフトウェアコン フォーマンスアプ リケーションの表 示と非表示を切り 替えます	Yes	Yes	Yes	Yes
OSUpgradeサービ ス	ui_app	SWIMアプリケー ションの表示と非 表示を切り替える	Yes	Yes	Yes	Yes
OSUpgradeサービ ス	ui_app	ソフトウェアアッ プグレードポリシ ーアプリケーション の表示と非表示 を切り替えます	Yes	Yes	Yes	Yes
OSUpgradeサービ ス	ui_app	ソフトウェアアッ プグレードの設定 の表示/非表示を切 り替えます	Yes	Yes	Yes	Yes

サービス	Group	意図	スーパー 管理者	ユースケ ース管理 者	読み取り 専用ユー ザ (OSア ップグレ ードユー スケース 読み取り 専用ユー ザ)	Operator
OSUpgradeサービ ス	アップグレードジ ョブ	アップグレードジ ョブの管理 (作成 、更新、削除、コ ミットなど)	Yes	Yes	いいえ	Yes
OSUpgradeサービ ス	アップグレードジ ョブ	アップグレードジ ョブのキャンセル	Yes	Yes	いいえ	Yes
OSUpgradeサービ ス	アップグレードジ ョブ	ジョブのオンデマ ンドアーカイブ	Yes	Yes	いいえ	Yes
OSUpgradeサービ ス	アップグレードジ ョブ	手動承認	Yes	Yes	いいえ	Yes
OSUpgradeサービ ス	Software- conformance- policy (ソフトウ ェアコンプライア ンスポリシー)	ソフトウェア準拠 ポリシーと実行結 果の表示	Yes	Yes	Yes	Yes
OSUpgradeサービ ス	Software- conformance- policy (ソフトウ ェアコンプライア ンスポリシー)	ソフトウェア適合 性ポリシーの作成 、更新、および削 除	Yes	Yes	いいえ	いいえ
OSUpgradeサービ ス	Software- conformance- policy (ソフトウ ェアコンプライア ンスポリシー)	ソフトウェア適合 性ポリシーのオン デマンド実行	Yes	Yes	いいえ	Yes
OSUpgradeサービ ス	アップグレードポ リシー	OSアップグレー ドポリシーの表示	Yes	Yes	Yes	Yes
OSUpgradeサービ ス	アップグレードポ リシー	OSアップグレー ドポリシーの管理	Yes	Yes	いいえ	いいえ
OSUpgradeサービ ス	SWIMイメージ管 理	ソフトウェアイメ ージの作成、更新 、および削除	Yes	Yes	いいえ	Yes
OSUpgradeサービ ス	SWIMイメージ管 理	SWIMの表示	Yes	Yes	Yes	Yes
OSUpgradeサービ ス	SWIMイメージ管	ソフトウェアイメ	Yes	Yes	いいえ	Yes

サービス	Group	意図	スーパー 管理者	ユースケ ース管理 者	読み取り 専用ユー ザ (OSア ップグレ ードユー スケー ス読み 取り 専用ユー ザ)	Operator
ス	理	ージの同期				
OSUpgradeサービ ス	ソフトウェアの推 奨事項	ソフトウェア推奨 メタデータの同期	Yes	Yes	いいえ	いいえ
OSUpgradeサービ ス	ソフトウェアの推 奨事項	アドバイザリまた はインサイトの表 示	Yes	Yes	Yes	Yes
OSUpgradeサービ ス	ソフトウェアの推 奨事項	準拠ポリシーの管 理	Yes	Yes	いいえ	いいえ
OSUpgradeサービ ス	ソフトウェア適合 性設定	ソフトウェア準拠 設定の表示	Yes	Yes	Yes	Yes
OSUpgradeサービ ス	ソフトウェア適合 性設定	ソフトウェア準拠 設定の管理	Yes	Yes	いいえ	いいえ

 注：カスタムロールと権限マッピングは、要件に従って実行できます。「[リソースグループ](#)」を参照してください。

リソースグループ

この機能は、アップグレードポリシーなどのBPAリソースに対する細かいアクセスコントロールを提供し、権限のないユーザによるOSアップグレードアプリケーションで定義されたポリシーのアップデートを制限します。管理者は、アクセス可能なポリシーを使用してリソースグループを定義することで、アクセスを制限できます。

リソースグループを作成するには

1. Settings > Resource Groupsの順に移動します。

Add Resource Group

Resource Group name *
osupgrade-res-grp

Resource Type:
os-upgrade-policy

Description:
Enter resource group description

Resources:

☐	Name	ASRSK	NSO
☐	Nso-qa1	ASRSK	NSO
☐	NSO-asr9k-policy-2	ASRSK	NSO
☒	NSO-any-to-any-policy	ASRSK	NSO

1 Items per page 10

Cancel Submit

リソースグループの追加

2. 管理者以外のユーザーがアクセスできるポリシーを持つリソースグループを作成します。
3. Resource Typeとしてos-upgrade-policyを選択します。対応するリソースが表示されます。
4. 必要なアップグレードポリシーを選択します。
5. [Submit] をクリックします。このユーザグループに属する非管理者ユーザは、選択したリソースグループでのみ使用可能なポリシーにアクセスできます。

リソースグループをユーザグループに関連付けるには、アクセスポリシーを作成します。

Add Policy

Policy name *
osupgrade-access-policy

Description:
Enter policy description

Resource Groups:

All osupg X

☐	Resource Groups
☒	osupgrade-res-grp

1 Items per page 10

Asset Groups:

All Search

☐	Asset Groups	Group Type
☐	ALL-ACCESS	static
☐	ReadOnly	static
☐	replacement-nodes	static

1 Items per page 10

User Groups:

All osupgrade X

☐	User Groups
☒	osupgrade-user-grp

1 Items per page 10

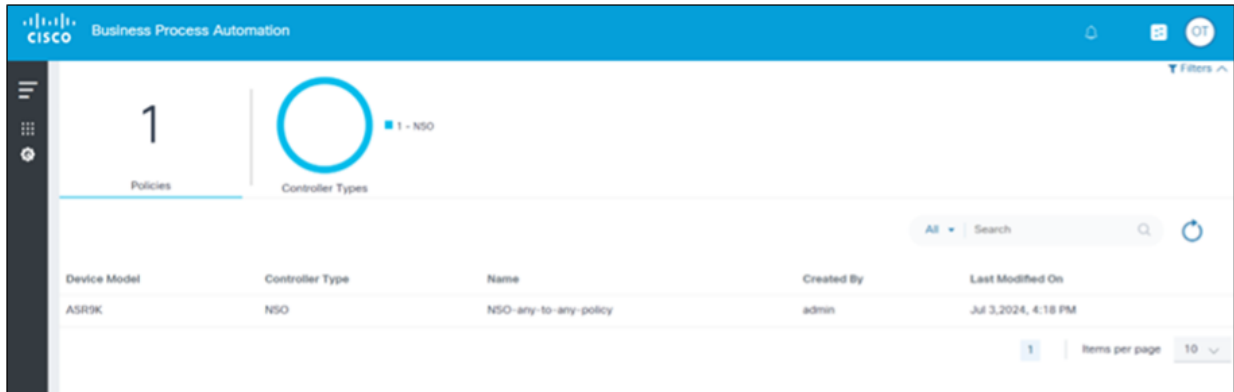
アクセスポリシーの追加

 注：リソースグループは、作成後、アクセスポリシーを使用してユーザグループに関連付ける必要があります。次の詳細については、『[アクセスコントロール](#)』を参照してください。

- ユーザ
- ロール
- ユーザーグループ
- アクセスポリシー

- ・ リソースグループ
- ・ 資産グループ

次に、制限されたリソースへのアクセス権を持つ非管理者ユーザの例を示します。



リソース制限を持つ非管理者ユーザー

ゼロトラストフラグの設定

ユーザがアクセスできるリソースは、ゼロ信頼フラグの設定によって異なります。ゼロ信頼フラグは、trueまたはfalseに設定できます。次の表は、ゼロトラストフラグの設定に基づくリソースアクセスの可能性をまとめたものです。

User	ユーザグループ	アクセスポリシー	リソースグループ	リソース	ゼロトラスト	Enabled
ユーザ1	UG1	AP1	RG1	2リソース	2リソース	2リソース
ユーザ1	UG1	AP2	RG2	リソースなし	リソースなし	リソースなし
ユーザ1	UG1	アクセスポイント3	ニル		リソースなし	すべてのリソース
ユーザ1	UG1	ニル	ニル		リソースなし	すべてのリソース

ゼロトラストフラグを有効または無効にするには、次の手順を実行します。

1. 次の設定パスに移動します。

```
cd /opt/bpa/bpa-helm-chart-
```

```
/charts/cisco-bpa-platform-mw-auth/public_conf/config.json
```

2. zeroTrustPoliciesの値を変更します。
3. 次のコアバンドルに移動します。

```
cd /opt/bpa/bpa-helm-chart-
```

4. 次のコマンドを実行して、コアルームを削除します。

```
helm delete bpa-rel -n bpa-ns
```

5. 次のコマンドを実行して、ポッドのステータスを確認します

```
kubect1 get pods -n bpa-ns
```

6. 次のコマンドを実行して、すべてのポッドの終了後にコアヘルムをインストールします。

```
helm install bpa-rel --create-namespace --namespace bpa-ns
```

7. 次のコマンドを実行して、起動するポッドのステータスを確認します。

```
kubect1 get pods -n bpa-ns
```

OSのアップグレード問題のトラブルシューティング

このセクションでは、BPAのOSアップグレードアプリケーションで確認された問題に関連するトラブルシューティングのヒントを示します。

準拠ポリシーの作成時にターゲットデバイスモデルが表示されない

SWIMのSoftware Imagesで、対応するイメージメタデータが使用できることを確認してください。見つからない場合は、次のいずれかのオプションを実行します。

- Cisco Catalyst Center、NDFC、vManage、FMCなどのコントローラからイメージメタデータを取得するためのイメージの同期
- NSO、CNC、Direct-to-Device、ANSIBLEなどのコントローラに必要なイメージメタデータの作成

ソフトウェアの適合性に非動作ステータスが示される

これは、次の理由が考えられます。

- ソフトウェア準拠ポリシーの作成時に、選択したモデルのアセットが見つかりませんでした
- SWIMでのモデルの名前が、すべてのデバイスのデバイスインベントリにある適合デバイスモデルと一致しません
- ソフトウェア適合性作成の一部としてSMUが選択され、すべてのデバイスのSMU検出が失敗した場合
- コンプライアンスチェックテンプレートの実行のために選択されたプロセステンプレートが失敗したか、見つかりませんでした
- ソフトウェアコンフォーマンスの作成時に、選択したモデルの下にあるすべてのデバイスでシリアル番号または現在のバージョンを使用できません

特定のデバイスのソフトウェア適合結果のステータスが不明です

これは、次の理由が考えられます。

- SWIMでのモデル名がデバイスインベントリの適合デバイスモデルと一致しません
- ソフトウェア適合性作成の一部としてSMUが選択され、デバイスのSMU検出が失敗した場合
- コンプライアンスチェックテンプレートの実行のために選択されたプロセステンプレートが失敗したか、見つかりませんでした
- デバイスのシリアル番号または現在のバージョンが使用できない

アップグレードジョブ完了の進捗率

アップグレードが完了しても、アップグレードジョブ完了の進行状況のパーセンテージが100未満である場合は、OS Upgrade > Settings > Rollbackの順に選択してWait for Rollback設定が有効

になっていることを確認し、User Verificationトグルがオンになっていることを確認します。全体の完了割合が100を下回ったままの場合は、RollbackまたはCompleteを選択します。

ジョブスケジュールに達し、デバイスが待機中の状態になる

スケジュールされたジョブが開始された後、デバイスがAwaiting状態のままになっている場合は、Kafka、Camunda、Scheduler、およびOS Upgradeのマイクロサービスを再起動してみてください。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。