

BPA-Benutzerhandbuch Betriebssystem-Upgrade v5.1

- [Einleitung](#)
 - [Wichtigste Funktionen](#)
 - [End-to-End-Fluss](#)
 - [Wertangebot](#)
 - [Unterstützte Controller und Geräteplattformen](#)
 - [Neue Funktionen](#)
- [Voraussetzungen](#)
- [Arbeiten mit der Betriebssystem-Aktualisierungsanwendung](#)
 - [Management von Software-Images](#)
 - [Software-Images](#)
 - [Software-Images werden synchronisiert](#)
 - [Hinzufügen von Software-Image-Metadaten](#)
 - [Massenhochladen von Metadaten zu Softwareabbildern](#)
 - [Bearbeiten vorhandener Metadaten von Software-Images](#)
 - [Löschen von Metadaten für Software-Images](#)
 - [Image Distribution Server-Management](#)
 - [Image Distribution Server](#)
 - [Hinzufügen von Image Server-Details](#)
 - [Bearbeiten der Image Server-Details](#)
 - [Image Server-Details werden gelöscht](#)
 - [Software-Informationen](#)
 - [Voraussetzungen](#)
 - [Abrufen von Software-Erkennungsdaten in BPA](#)
 - [Anzeigen und Verwalten von Sicherheitsempfehlungen](#)
 - [Anzeigen und Verwalten von Prioritätsfehlern](#)
 - [Anzeigen von Software-Einblicken](#)
 - [Anzeigen und Auswählen der vom Anbieter vorgeschlagenen Softwareversionen](#)
 - [Identifizierung von Geräten, die ein Software-Upgrade benötigen](#)
 - [Softwarekonformität](#)
 - [Voraussetzungen](#)
 - [Erstellen von EPLD-Moduldaten in einer Referenzdatenverwaltungsanwendung](#)
 - [Anzeigen und Verwalten der Softwarekonformität](#)
 - [Erstellen von Software-Konformitätsrichtlinien](#)
 - [Durchführung von Software-Konformitätsprüfungen bei Bedarf](#)
 - [Planen der Durchführung von Software-Konformitätsprüfungen](#)
 - [Aktualisieren von Software-Konformitätsrichtlinien](#)
 - [Software-Konformitätsrichtlinien werden gelöscht](#)
 - [Konformitätsergebnisse anzeigen und herunterladen](#)
 - [Upgrade-Richtlinie](#)
 - [Voraussetzungen](#)

- [Anzeigen und Verwalten von Aktualisierungsrichtlinien](#)
- [Erstellen von Aktualisierungsrichtlinien](#)
- [Bridge-SMUs](#)
- [Aktualisierungsrichtlinien bearbeiten](#)
- [Anzeigen von Aktualisierungsrichtlinien](#)
- [Aktualisierungsrichtlinien werden gelöscht](#)
- [Kontrolle des Zugriffs auf Aktualisierungsrichtlinien](#)
- [Aufträge aktualisieren](#)
 - [Voraussetzungen](#)
 - [Anzeigen und Verwalten von Aktualisierungsaufträgen](#)
 - [Planen von Aktualisierungsaufträgen](#)
 - [Bearbeiten eines Stapels in einem Auftrag](#)
 - [Ausführung von Upgrade-Aufträgen und Überwachung des Fortschritts](#)
 - [Bericht zum Software-Upgrade herunterladen](#)
 - [Jobs archivieren](#)
 - [Löschen von Jobs](#)
 - [Löschen von Stapeln in Jobs](#)
 - [Jobs abbrechen](#)
 - [Rollback abgeschlossener Jobs oder Upgrades](#)
- [Einstellungen](#)
 - [Softwarekonformität](#)
 - [Rollback](#)
- [Bereitstellungskonfiguration](#)
- [Zugriffskontrolle](#)
 - [Rollenbasierte Zugriffskontrolle](#)
 - [Ressourcengruppen](#)
 - [Einstellung des Kennzeichens "Keine Vertrauenswürdigkeit"](#)
- [Fehlerbehebung bei Betriebssystem-Upgrades](#)
 - [Zielgerätemodell kann beim Erstellen einer Konformitätsrichtlinie nicht angezeigt werden](#)
 - [Softwarekonformität zeigt Betriebsausfall an](#)
 - [Der Status des Ergebnisses der Softwarekonformität bestimmter Geräte ist unbekannt](#)
 - [Prozentsatz des Abschlusses des Aktualisierungsauftrags](#)
 - [Zeitplan erreicht, Geräte im Wartezustand](#)

Einleitung

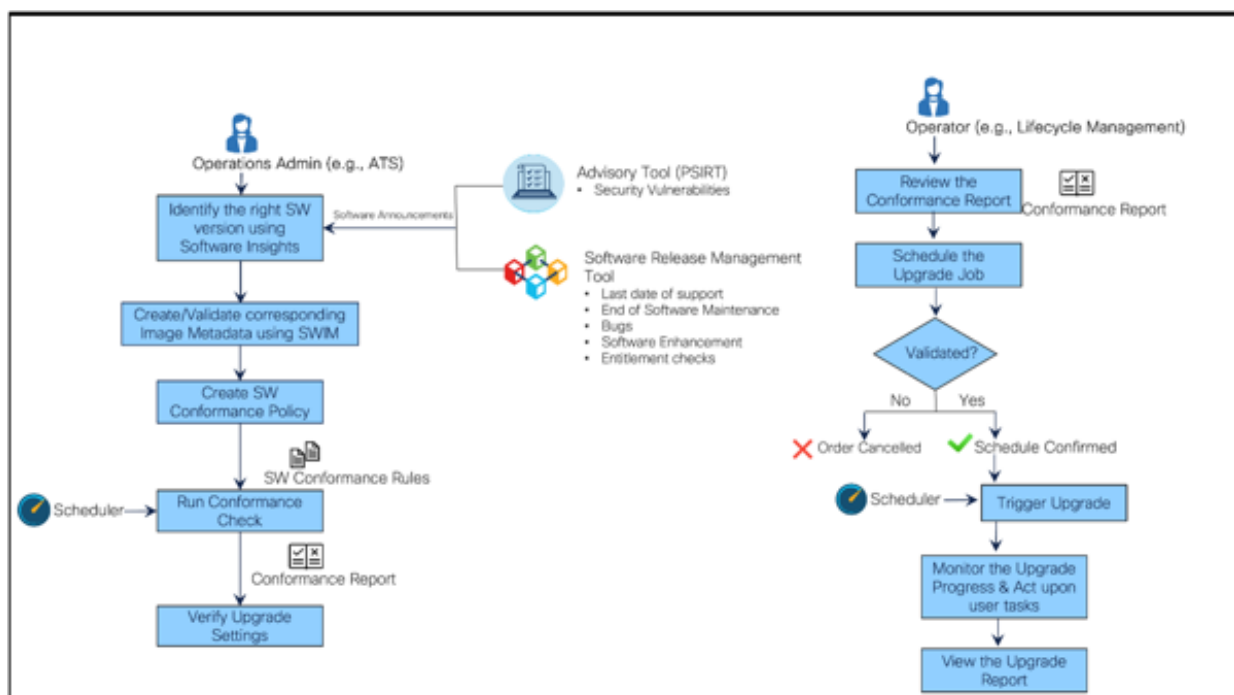
Die BPA-Anwendung (Business Process Automation) für Betriebssystem-Upgrades bietet eine umfassende Automatisierungslösung zur Durchführung von Software-Konformität und Upgrades von Netzwerkgeräten über verschiedene Domänen hinweg. Es unterstützt mehrere Domain Controller und bietet eine einheitliche Benutzererfahrung. Es unterstützt sowohl Betriebssystem-Upgrades als auch SMU- (Software Maintenance Update) und RPM Package Manager-Patch-Updates.

Wichtigste Funktionen

Die Anwendung "Betriebssystem-Upgrade" bietet die folgenden wichtigen Automatisierungsfunktionen:

- Management von Software-Images: Eine zentrale Liste der Software-Images und ihrer Versionen (von allen Anbietern) für den Software-Upgrade-Prozess
- Software-Einblicke: Identifiziert Risiken und Schwachstellen von Software in Bezug auf Netzwerkressourcen und erhält Einblicke in die vom Anbieter empfohlenen Softwareversionen
- Softwarekonformität: Identifiziert alle Ressourcen im Netzwerk, deren Software-Images aktualisiert werden müssen.
- Upgrade Method Of Procedure (MOPP) Definition: Vordefinierung des Upgrade-Prozesses sowie Vor- und Nachprüfungen für jedes Gerätemodell oder jede Gerätereihe des Anbieters
- Aktualisierungsaufträge: Zeitplanung von Upgrades für nicht konforme Ressourcen während Wartungsfenstern für alle geografischen Regionen, Überwachung des Upgrade-Fortschritts und Bereitstellung detaillierter Berichte

End-to-End-Fluss



End-to-End-Fluss

Die obige Abbildung zeigt die Anruflüsse der Anwendung "Betriebssystem-Upgrade" für zwei verschiedene Benutzerpersonas: Operations Administrator und Network Operator, sofort einsatzbereit. Weitere Informationen zu OOB-Rollen und den entsprechenden Berechtigungen finden Sie unter [Zugriffskontrolle](#).

Person	Beschreibung	Arbeitsplatz
Betriebsadministrator	Erkennung von Softwareschwachstellen (z. B. Advisories, Bugs, End-of-Life Bulletins), die sich auf Netzwerkressourcen auswirken	BPA: Betriebssystem-Upgrade/Software-Image-Management/Empfehlungen
Betriebsadministrator	Identifiziert die betroffene Softwareversion und die betroffenen Ressourcen und bestimmt die richtige Zielversion auf Basis der vom Anbieter unterbreiteten Vorschläge	BPA: Betriebssystem-Upgrade/Management von Software-Images/Einblicke
Betriebsadministrator	Erstellt die erforderlichen Software-Image-Metadaten	BPA: Betriebssystem-Upgrade/Management von Software-Images/Software-Images
Betriebsadministrator	Erstellt die Absicht für betroffene Gerätemodelle und führt die Richtlinie bei Bedarf oder bei der geplanten Richtlinienausführung aus	BPA: Richtlinie für Betriebssystem-Upgrade/Software-Konformität
Betriebsadministrator	Identifiziert die nicht konformen oder betroffenen Ressourcen	BPA: Betriebssystem-Upgrade/Softwarekonformität/Ergebnisse anzeigen
Betriebsadministrator	Erstellt oder ändert die Upgrade-Richtlinie gemäß dem Upgrade-MOPP. Dazu gehören die Vorab- und Nachprüfung, Workflows für die Verteilung oder Aktivierung, die Umleitung oder Umkehrung des Datenverkehrs und das Rollback für ein- oder mehrstufige Upgrades.	BPA: Richtlinie für Betriebssystem-Upgrade
Netzbetreiber	Plant ein Upgrade aller nicht konformen Geräte	BPA: Jobs für Betriebssystem-Upgrade
Netzbetreiber	Überwacht den Fortschritt des Aktualisierungsauftrags	BPA: Betriebssystem-Upgrade-/Upgrade-Aufträge/Auftragsdetails
Netzbetreiber	Reagiert ggf. auf Benutzeraufgaben, um Probleme zu beheben, und ermöglicht dem Prozess, mit dem nächsten Schritt	BPA: Upgrade-/Upgrade-Aufträge/Auftragsdetails

Wertangebot

Die folgenden Vorteile werden durch die Anwendung für Betriebssystem-Upgrades erzielt:

- API-basierter Ansatz zur Vereinfachung der Servicenutzung über das Northbound Operations Support System (OSS) und das Business Support System (BSS)
- Schnelle Überprüfung der Softwarekonformität von Netzwerkgeräten in Netzwerken, die von verschiedenen Domänencontrollern verwaltet werden
- Operatoren haben mehr Kontrolle über Upgrade-Jobs durch Batch-, Warteschlangen- und Planungsmechanismen
- Upgrade-Jobs können frühzeitig für Überprüfungen erstellt und später ausgeführt werden.
- Ein Warteschlangenmechanismus, der einen schnelleren und besseren Durchsatz bei minimalen bis null Ausfällen ermöglicht
- Automatische Backups vor dem Upgrade für eine nahtlose Wiederherstellung bei Ausfällen
- Ausführung vor und nach der Überprüfung, um sicherzustellen, dass Upgrades ohne Serviceunterbrechungen erfolgreich sind
- Ein richtlinienbasierter Ansatz, der die Flexibilität bietet, den Upgrade-MOPP mit Prüfungen vor und nach der Validierung, Verteilung oder Aktivierung, Datenverkehrsumleitung oder -umleitung und Rollback-Prozessen vorab zu definieren, sodass sie bei Bedarf angepasst werden können

Unterstützte Controller und Geräteplattformen

Die folgenden Plattformen wurden für BPA validiert und werden für OOB unterstützt. Der Rahmen ist jedoch allgemein gehalten und kann auf neue Plattformen ausgedehnt werden. OOB-Unterstützung für zusätzliche Plattformen wird in künftigen Versionen nach Priorität bereitgestellt.

Domänencontroller	Geräteplattformen
Cisco Catalyst Center 2.3.7.5-70434	- Cisco IOS, Cisco IOS-XE - Cisco IOS, Cisco IOS-XE
vManage v20.12.4	Anmerkung: Die Geräte müssen v17.9.x oder höher sein, damit die Remote-Serververteilung funktioniert.
Nexus Dashboard Fabric Controller (NDFC) v12.1.2e und v12.2.2	- Cisco-NX-OS (N9k)
Firewall Management Center (FMC)	- FirePOWER 3140

v7.4.1

Network Services Orchestrator (NSO)
v6.3

- Cisco IOS XR (NCS540, NCS560, ASR9K)
- Cisco-NX-OS (N9K)

Anmerkung: NX-OS NED v5.25.17 oder höher ist erforderlich

Cross Network Controller (CNC) v6.0
ANSIBLE v2.9.18 (AWX - 17.1.0)

- Cisco IOS XR (NCS 540, ASR9K)
- Cisco IOS XR (NCS 540, ASR9K)

Direct-to-Device (über Teletype-
Netzwerk (Telnet) und Secure Shell
(SSH))

- Cisco IOS XR (NCS 540, ASR9K)

Neue Funktionen

Informationen zu inkrementellen Funktionen, die für den Anwendungsfall "Betriebssystem-Upgrade" dieser Version verfügbar gemacht wurden, finden Sie in den [BPA-Versionshinweisen](#).

Voraussetzungen

Die folgenden Voraussetzungen müssen erfüllt sein, bevor die Anwendung für das Betriebssystem-Upgrade verwendet werden kann:

- Betriebssystem-Upgrade, Backup und Wiederherstellung, Scheduler-Services und alle erforderlichen Plattform-Services oder Controller-Agent-Services sind verfügbar und laufen.
- Erforderliche Artefakte (z. B. Workflows, Prozessvorlagen, Standard-Upgrade-Richtlinien usw.) werden geladen
- Erforderliche Controller werden hinzugefügt, und die Geräte werden erfolgreich synchronisiert. Weitere Informationen finden Sie unter [Unterstützte Controller und Geräteplattformen](#)

Arbeiten mit der Betriebssystem-Aktualisierungsanwendung

Die Anwendung für das Betriebssystem-Upgrade besteht aus den folgenden Komponenten:

- Software-Image-Management (SWIM)
- Image Distribution Server-Management
- Software-Informationen

- Softwarekonformität
- Upgrade-Richtlinie
- Aufträge aktualisieren
- Einstellungen

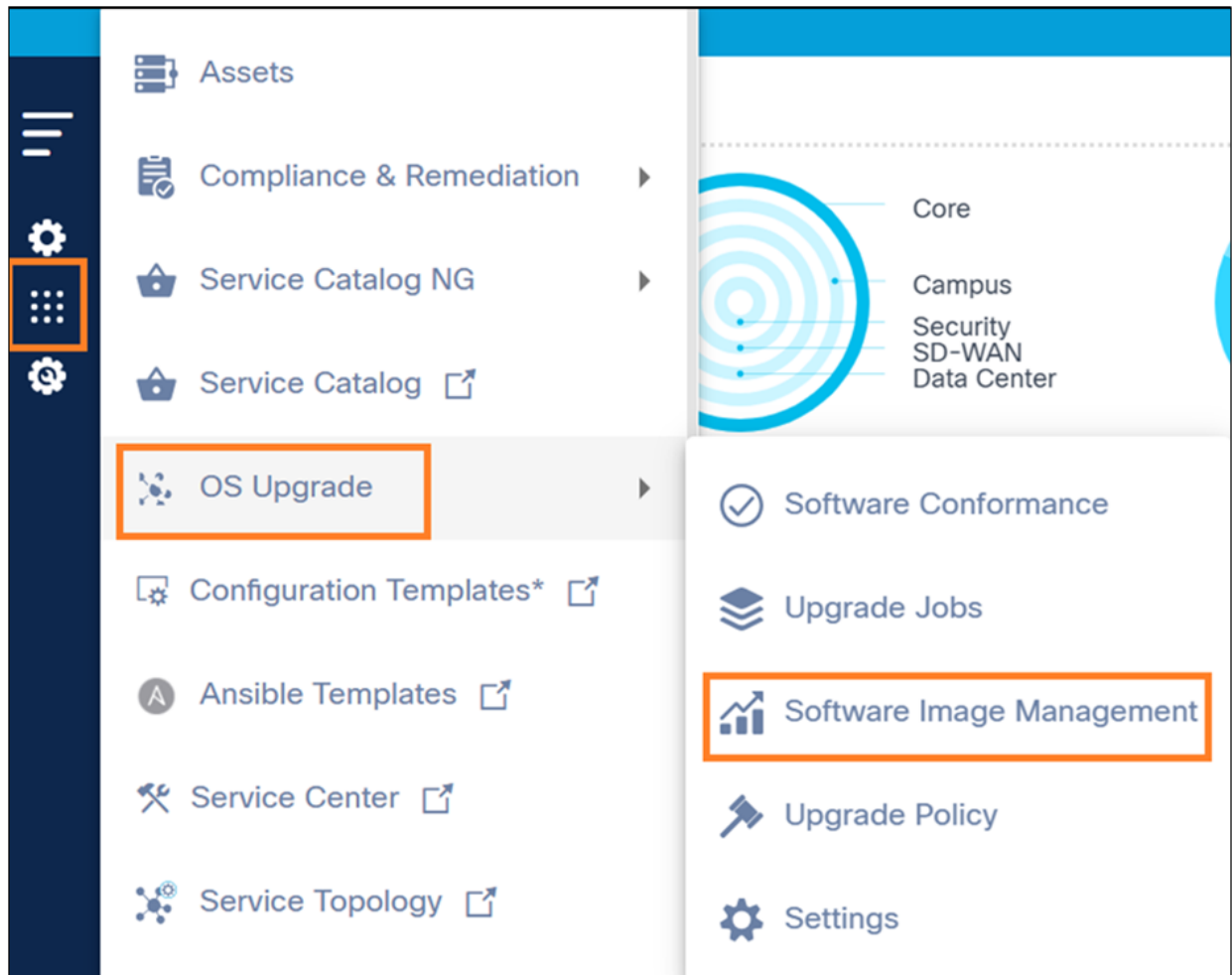
Management von Software-Images

Mit der SWIM-Komponente können Operations-Benutzer Software-Image-Details für Controller wie NSO, ANSIBLE, CNC, FMC und Direct-to-Device verwalten, die keine Unterstützung für OOB-Image-Management bieten. Außerdem werden die Software-Image-Details aufgeführt, die von Controllern wie vManage, NDFC und Cisco Catalyst Center verwaltet werden. So wird eine zentrale Liste der Software bereitgestellt, die auf allen Domänencontrollern gewartet wird. Software-Images und der Image Distribution Server sind die beiden Hauptunterkomponenten des SWIM-Moduls.

Software-Images

So rufen Sie die Seite Software-Images auf:

1. Melden Sie sich bei BPA mit Anmeldeinformationen an, die Zugriff auf das Software-Image-Management haben.



Navigation im Software-Image-Management

2. Wählen Sie Betriebssystem-Upgrade > Software-Image-Management aus.

Auf der Seite Image Management (Image-Verwaltung) werden folgende Registerkarten angezeigt: Software-Images, Image Distribution Server, Advisories und Insights.

Software Images									
38 Device Models Images 195 - Base 33 - EPLD 77 - SMU Controller Types 154 - vManage 149 - NDFC 2 - NSO Vendor 305 - Cisco									
All Search Filters									
☐	Device Model	Vendor	Image Name	Image Version	Image Type	Software Image Server	Added By	Last Modified On	Action
☐	ASR9K	Cisco	asr9k-x64-7.8.2.CSCwc11910.tar	7.8.2	SMU	NSO-FTP-2-Server	admin	Jul 14, 2025, 1:40 PM	⋮
☐	N9K-C93180YC-FX	Cisco	nxos64-cs.10.2.5.M.bin	10.2.5	Base	NDFC-115	System	Jul 11, 2025, 1:00 PM	⋮
☐	N9K-C93180YC-FX	Cisco	n9000-epld.10.2.2.F.img	10.2.2	EPLD	NDFC-115	System	Jul 11, 2025, 1:00 PM	⋮
☐	N9K-C93180YC-EX	Cisco	nxos64-cs.10.2.2.F.bin	10.2.2	Base	NDFC-115	System	Jul 11, 2025, 1:00 PM	⋮
☐	N9K-C9364C-GX	Cisco	n9000-epld.10.2.2.F.img	10.2.2	EPLD	NDFC-115	System	Jul 11, 2025, 1:00 PM	⋮
☐	N9K-C93180YC-EX	Cisco	n9000-epld.10.2.2.F.img	10.2.2	EPLD	NDFC-115	System	Jul 11, 2025, 1:00 PM	⋮
☐	N9K-C93180YC-EX	Cisco	nxos64-cs.10.2.5.M.bin	10.2.5	Base	NDFC-115	System	Jul 11, 2025, 1:00 PM	⋮
☐	N9K-C9364C-GX	Cisco	nxos64-cs.10.2.5.M.bin	10.2.5	Base	NDFC-115	System	Jul 11, 2025, 1:00 PM	⋮
☐	N9K-C9364C-GX	Cisco	nxos64-cs.10.2.2.F.bin	10.2.2	Base	NDFC-115	System	Jul 11, 2025, 1:00 PM	⋮

Registerkarte Software-Images

Die Registerkarte Software-Images enthält Folgendes:

- Ein oben angezeigter Abschnitt zu Analysen bietet folgende Informationen:
 - Die Gesamtzahl der Gerätemodelle und der zugehörigen Software-Images
 - Ein Schnellfilter für Bilder, der das Filtern von Bildern nach Typ ermöglicht (z. B. base, SMU); Die Zahl gibt die Gesamtzahl der Bilder an, die einem jeweiligen Bildtyp zugeordnet sind.
 - Ein Schnellfilter für Controller-Typen, der das Filtern von Images auf Basis des Controller-Typs ermöglicht (z. B. Cisco Catalyst Center, vManage, NSO oder NDFC, Direct-to-Device, CNC, ANSIBLE, FMC), für den die Images gehostet werden; Die Zahl gibt die Gesamtzahl der Bilder an, die einem jeweiligen Controllertyp zugeordnet sind.
 - Ein Schnellfilter für den Anbieter, der das Filtern von Bildern anhand des Anbieters ermöglicht, der die Software veröffentlicht hat
- Das Symbol Weitere Optionen bietet folgende Funktionen:
 - Bilddetails hinzufügen: Neue Bildmetadaten hinzufügen
 - Massen-Upload: Massen-Upload von Bildmetadaten im CSV-Format
 - Bilder synchronisieren: Synchronisieren von Image-Metadaten von Controllern (z. B. Cisco Catalyst Center, vManage, NDFC und FMC)
 - Alle löschen: Massenlöschung ausgewählter Bilder

 Anmerkung: Das Hinzufügen, Löschen und Hochladen von Image-Details ist nur für NSO-, ANSIBLE-, CNC- und Direct-to-Device-Controller zulässig.

- Der Suchfilter kann für die Suche von Bildern verwendet werden und enthält die folgenden exklusiven Suchfilter:
 - Alle: In allen Feldern suchen
 - Bildname: Suche nach Bildern mit einem bestimmten Bildnamen
 - Gerätemodell: Nach Bildern mit einem angegebenen Modell suchen
 - Bildversion: Suche nach Images mit einer bestimmten Softwareversion
 - Software-Image-Server: Suche nach Bildern, die einem bestimmten Image-Server zugeordnet sind
- Das Symbol Aktualisieren aktualisiert die Seite und löscht ausgewählte Filter.
- Vorhandene Bilder werden in einer Rastertabelle mit den folgenden Spalten angezeigt:
 - Gerätemodell: Gerätemodell, für das die Bilddetails gelten
 - Anbieter: Anbieter, der die Software-Images veröffentlicht
 - Bildname: Dateiname des Bilds
 - Bildversion: Softwareversion des Images
 - Bildtyp: Bestimmt den Bildtyp (z. B. Base, SMU, Electronic Programmable Logic Device (EPLD))
 - Software-Image-Server: Image-Server, auf dem das aktuelle Image vorhanden ist
 - Hinzugefügt von: Benutzer, der die Bildmetadaten hinzugefügt hat

- Zuletzt geändert am: Zeitstempel der letzten Bilddetails-Aktualisierung
- Aktion: Stellt ein Symbol Weitere Optionen bereit, über das zeilenspezifische Aktionen (z. B. Bearbeiten, Löschen) ausgewählt werden können
- Bilder sortieren, indem Sie auf eine entsprechende Spaltenüberschrift klicken

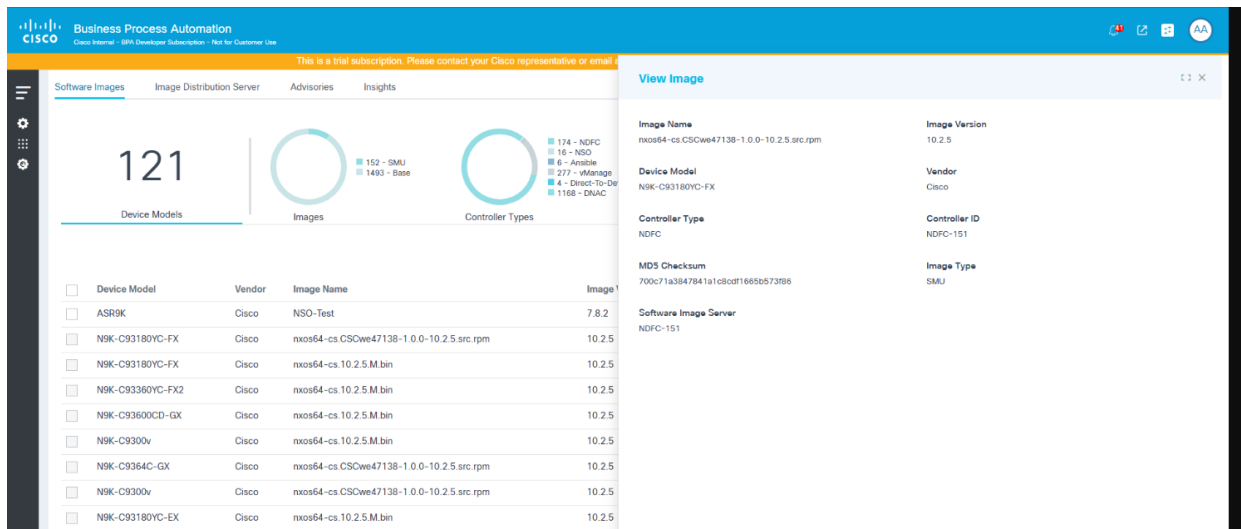


Bild anzeigen

- Durch Klicken auf eine Zeile wird das Fenster Bild anzeigen geöffnet.

Software-Images werden synchronisiert

So führen Sie eine bedarfsgesteuerte Synchronisierung von Software-Images durch:



Bilder synchronisieren

1. Wählen Sie das Symbol Weitere Optionen > Bilder synchronisieren aus. Die Details der Image-Metadaten von vManage, Cisco Catalyst Center, NDFC und FMC werden erkannt und in BPA beibehalten.



Anmerkung: Bei FMC-Controllern werden bei jeder Synchronisierung vorhandene Daten beibehalten. Nur neue Bilder werden angehängt.

2. Wenn der Image-Name vom FMC-Controller das Wort "FTD" oder "Firepower Threat_Defense" enthält, wird das DeviceModel für dieses Image als FTD abgebildet.

ODER

Wenn der Image-Name vom FMC-Controller die Wörter "FMC", "FW_Mgmt_Center" oder "Firewall_Management_Center" enthält, wird das DeviceModel für dieses Image als FMC zugeordnet.

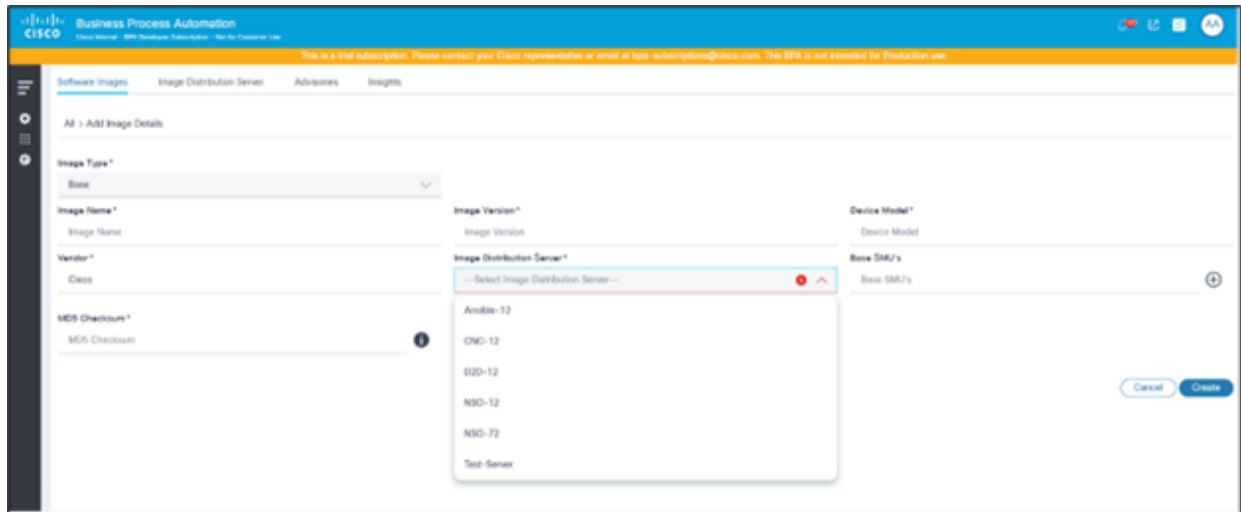


Anmerkung: FMC ordnet den Bildmetadaten keine Modellinformationen zu. Nachdem die Synchronisierung abgeschlossen ist, bearbeiten Sie die entsprechenden Bildmetadaten und aktualisieren Sie das Modell nach Bedarf. Der FMC-Upgrade-Prozess funktioniert ohne die Modellaktualisierung nicht wie erwartet.

3. Images von vManage-Remote-Servern weisen nach dem Synchronisierungsvorgang zunächst die Universally Unique Identifier (UUID) in der Spalte Version auf. Operatoren müssen die erforderlichen Metadaten für den Remote-Server manuell bearbeiten und mit der entsprechenden Image-Version aktualisieren. Wenn diese Zuordnung nicht vorgenommen wird, funktionieren andere Betriebssystem-Upgrade-Komponenten (z. B. Softwarekonformität, Upgrade-Richtlinien, Upgrade-Jobs usw.) nicht wie erwartet.
4. Informationen zur Planung einer regelmäßigen automatischen SWIM-Metadaten-Synchronisierung finden Sie unter [Bereitstellungskonfiguration](#).

Hinzufügen von Software-Image-Metadaten

1. Wählen Sie das Symbol Weitere Optionen > Bilddetails hinzufügen aus. Die Seite Bilddetails hinzufügen wird angezeigt.



Bilddetails hinzufügen

2. Geben Sie Informationen in die folgenden Felder ein:

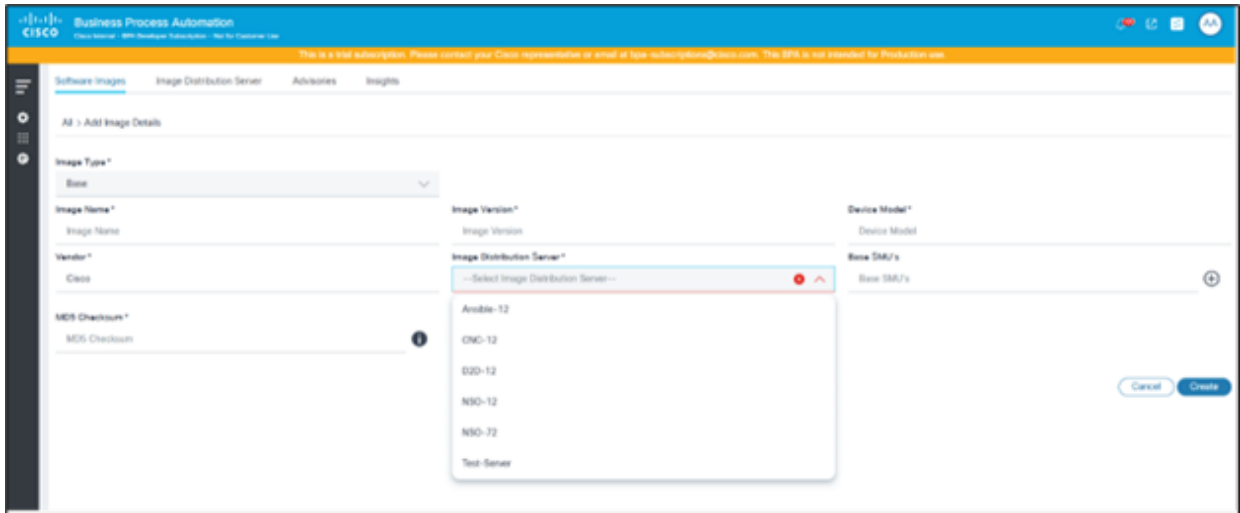
- Bildtyp: Bildtyp (z. B. Base, SMU, EPLD)
- Bildname: Name der Bilddatei; Benutzer können entweder einen relativen oder absoluten Pfad des Bilds in das Feld Name eingeben. Wenn Benutzer einen absoluten Pfad angeben, wird das Bild direkt von diesem Pfad abgerufen. Wenn Benutzer einen relativen Pfad angeben, löst das System den vollständigen Pfad auf, indem es den im Repository-Server während der Verteilung definierten Basispfad hinzufügt
- Bildversion: Softwareversion des Images
- Gerätemodell: Das Gerätemodell, für das das Bild markiert wird

 Anmerkung: Das Gerätemodell muss mit den Modellinformationen übereinstimmen, die vom CNC-, NSO-, Direct-To-Device- oder ANSIBLE-Controller für die entsprechenden Geräte bereitgestellt werden.

- Anbieter: Der Anbieter oder Anbieter, der das Bild veröffentlicht hat; Der Standardwert ist "Cisco", kann jedoch nach Bedarf geändert werden.
- Image Distribution Server: Wählen Sie den Image Distribution Server aus, der die im Feld Image Name (Image-Name) angegebene Software hostet. Bei der Auswahl eines Bildverteilungsservers werden Bilder für alle Controller-IDs generiert, die dem angegebenen, im Bildverteilungsserver definierten Controller-Typ zugeordnet sind. Wenn ein Benutzer Controller-Instanzen unter dem Image Distribution Server hinzufügt oder entfernt, werden die entsprechenden Software-Images für diese Controller-Instanzen hinzugefügt oder entfernt.
- Basis-SMUs: SMUs, die im goldenen Grundbild vorhanden sind; Diese Option ist nur verfügbar, wenn der Bildtyp Base ist.
- MD5-Prüfsumme: MD5-Prüfsumme für die Überprüfung

3. Klicken Sie auf Erstellen. Die Benachrichtigung Progress (Fortschritt) wird angezeigt, gefolgt von einer Bestätigungsmeldung.

 Anmerkung: Die Image-Metadaten für Bridge-SMUs müssen hinzugefügt werden, bevor sie in einer Aktualisierungsrichtlinie verwendet werden können. Um Bridge-SMUs hinzuzufügen, wählen Sie SMU aus der Dropdown-Liste Image Type (Image-Typ) aus.



Bridge-SMU-Image-Metadaten hinzufügen

Massenhochladen von Metadaten zu Softwareabbildern

	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

Beispiel-CSV-Datei mit Bildinformationen

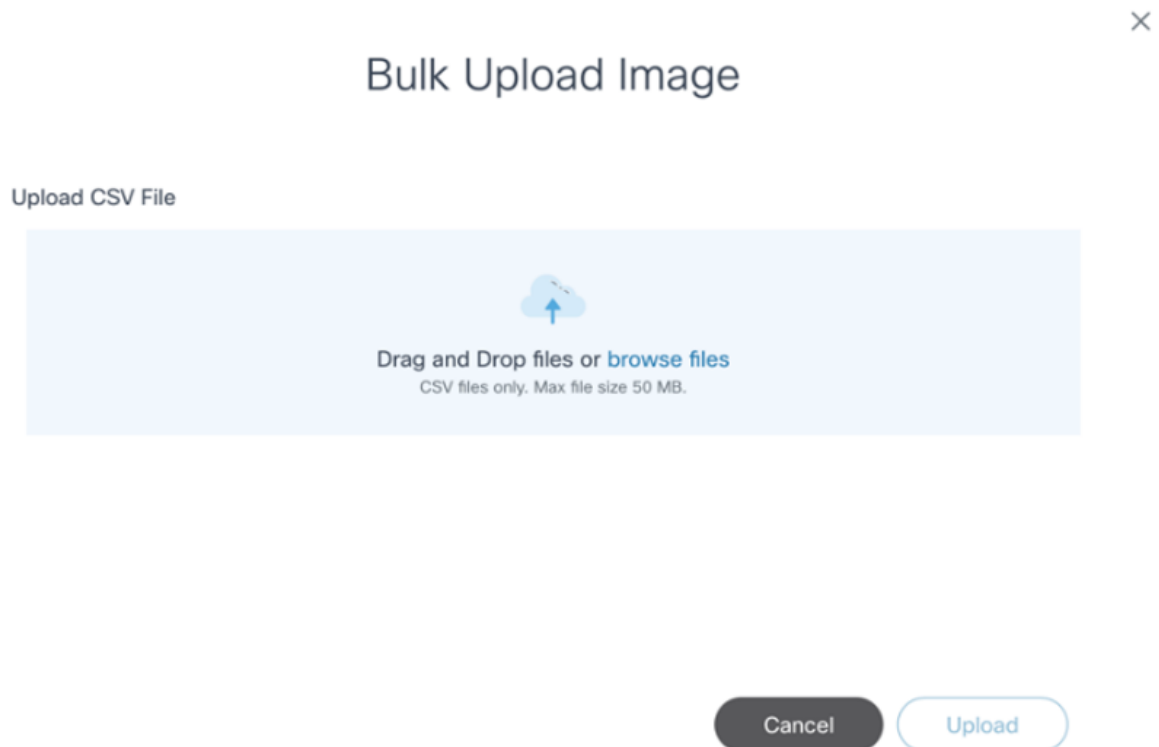
1. Bereiten Sie eine CSV-Datei mit den erforderlichen Bilddetails und den folgenden Spaltennamen vor:

- Bildname
- Version
- Gerätemodell
- Anbieter
- Bildtyp

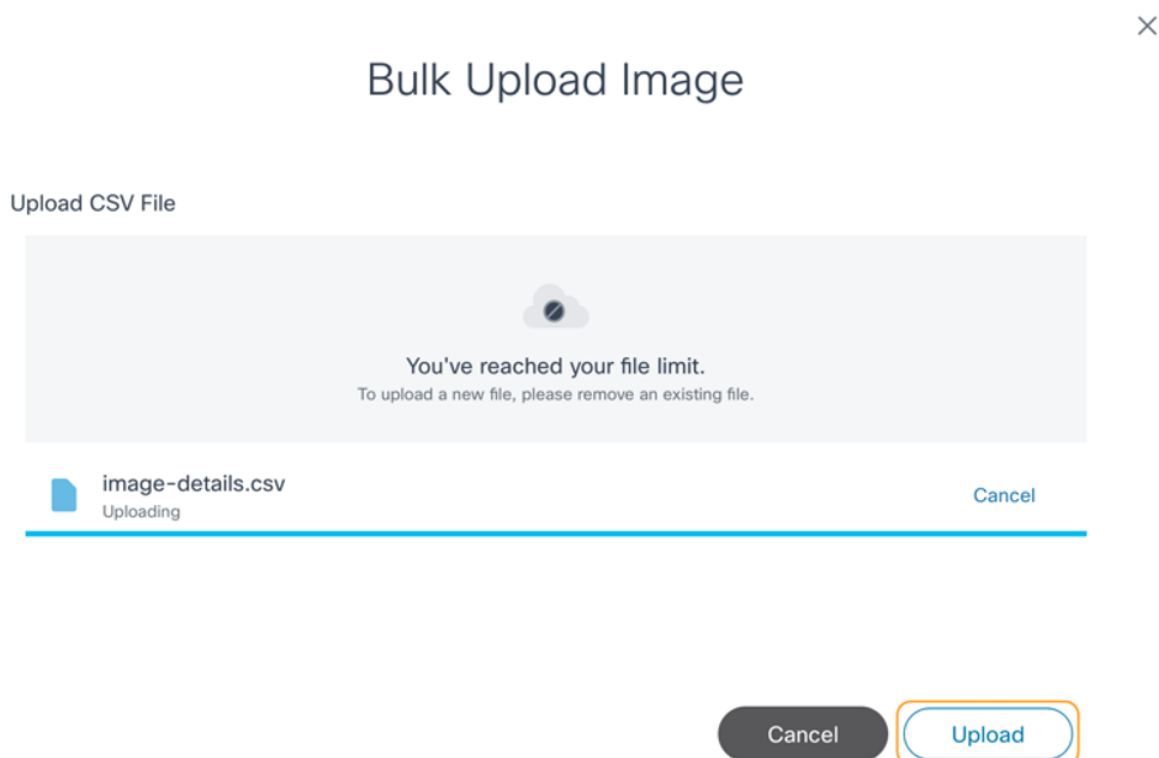
 Anmerkung: Es werden nur Base-, SMU- und EPLD-Werte unterstützt.

- Image Distribution Server
- MD5-Prüfsumme

2. Wählen Sie das Symbol More Options (Weitere Optionen) > Bulk Upload (Massenhochladen). Das Fenster Massen-Upload-Bild wird geöffnet.



Massen-Upload-Image



Massen-Upload-Image - CSV-Upload

3. Wählen Sie eine vorbereitete CSV-Datei aus, und klicken Sie auf Hochladen. Bilddetails aus

der CSV-Datei werden validiert und anschließend verarbeitet. Sobald die Datei hochgeladen wurde, wird der endgültige Status für den Massen-Upload angezeigt.

×

Bulk Upload Image

Upload CSV File

You've reached your file limit.
To upload a new file, please remove an existing file.

image-details.csv

Uploading

Cancel

Total upload status: Success: 2, Failed: 0

Cancel

Upload

Upload-Status des Großabbilds erfolgreich

 Anmerkung: Bei Datenvalidierungsfehlern (z. B. doppelte Datensätze oder ungültige Parameter) werden Fehlermeldungen im Fenster Massen-Upload-Bild als Raster angezeigt. Benutzer können die Werte in der CSV-Datei korrigieren und sie erneut hochladen.

Bearbeiten vorhandener Metadaten von Software-Images

Software Images

Image Distribution Server

Advisories

Insights

127

Device Models

1197 - Base

280 - SMUJ

Images

348 - NDFC

6 - FMC

556 - vManage

2 - CNC

534 - DNAC

2 - Direct-To-Device

7 - Ansible

22 - NSO

Controller Types

1477 - Cisco

Vendor

Filters

All

ASR9K-762.tar

×

↻

⋮

☐	Device Model	Vendor	Image Name	Image Version	Image Type	Software Image Server	Added By	Last Modified On	Action
☐	ASR-9901	Cisco	ASR9K-762.tar	7.6.2	Base	D2D-os	admin	Sep 25,2024, 10:18 PM	⋮

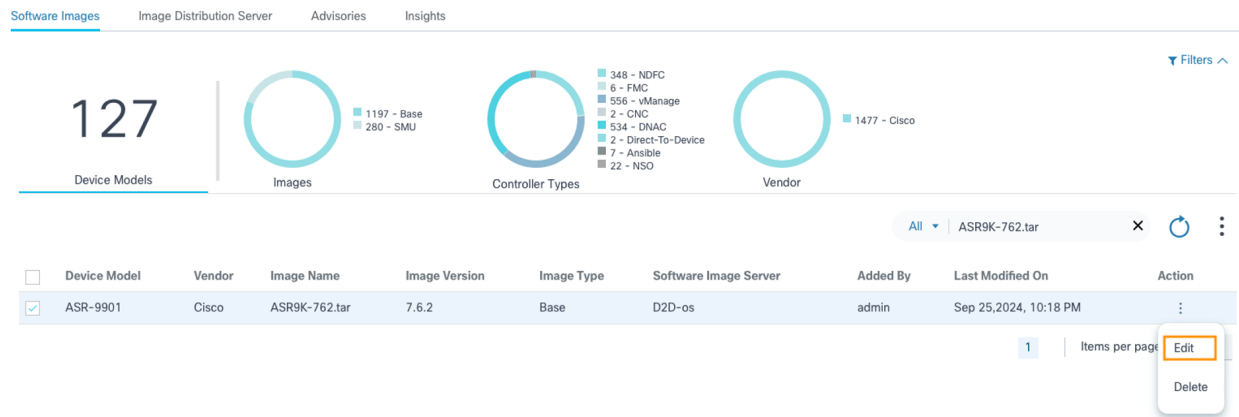
1

Items per page

10

Suchen in Metadaten von Software-Images

1. Suchen Sie mithilfe des Filters Suchen nach dem zu aktualisierenden Bild.



Bearbeiten

- Wählen Sie in der Spalte Aktion des gewünschten Bilds das Symbol Weitere Optionen > Bearbeiten aus.

Software Images | Image Distribution Server | Advisories | Insights

All > asr9k-x64-7.7.2.CSCwe22538.tar

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

MDS Checksum*
b70ace4d0813399d11983b17f070d1e7

Cancel Save

Software-Images bearbeiten

- Aktualisieren Sie die erforderlichen Parameter, und klicken Sie auf Speichern, um die Änderungen zu speichern, oder auf Abbrechen, um die Änderungen zu verwerfen. Eine Statusbenachrichtigung und eine Bestätigungsmeldung für die Image-Aktualisierung werden angezeigt.

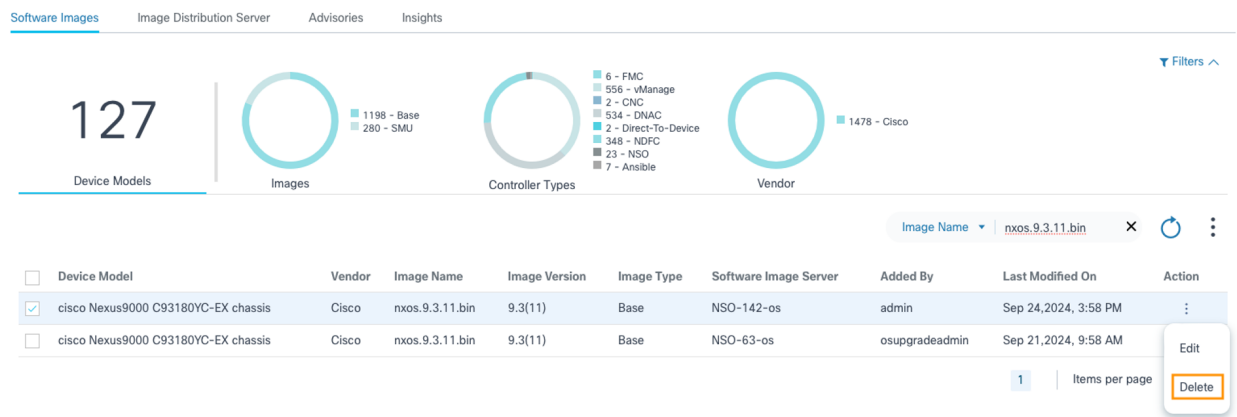
 Anmerkung: Die folgende Liste ist zu beachten.

- Die Bearbeitung ist für CNC-, NSO-, D2D-, ANSIBLE-, FMC- und vManage-Controller verfügbar (nur für Remote-Server-Image-Metadaten).
- Die Aktualisierung des Gerätemodells wird nur für vManage-Remote-Server-Images unterstützt.
- Nur das Feld Softwareversion kann für die Metadaten des Remote-Server-Images von vManage aktualisiert werden.
- Bei vManage-Images können Benutzer den Software-Image-Server anstelle von Controller-Instanzen anzeigen.

Löschen von Metadaten für Software-Images

Suchen in Metadaten von Software-Images

1. Verwenden Sie das Feld Suchen, um ein gewünschtes Bild zu suchen.



Löschen

2. Wählen Sie in der Spalte Aktion des gewünschten Bilds das Symbol Weitere Optionen > Löschen aus, um ein Bild zu löschen.

ODER



Alle löschen

Wählen Sie die gewünschten Bilder aus, und wählen Sie das Symbol Weitere Optionen > Alle löschen aus, um mehrere Bilder zu löschen.

Es wird eine Bestätigung angezeigt.



Delete Image

Are you sure you want to delete the selected images?

Cancel

Ok

Bestätigung

3. Klicken Sie auf OK. Daraufhin wird eine Statusbenachrichtigung und eine Bestätigungsmeldung angezeigt.



Anmerkung: Die folgende Liste ist zu beachten.

- Image-Metadaten können nur für die Controller NSO, ANSIBLE, Direct-to-Device und CNC hinzugefügt werden. Für alle anderen Enterprise-Controller wird die integrierte SWIM-Funktion genutzt, und Images werden von den jeweiligen Controllern erkannt
- Image-Erkennungsfunktionen werden für NSO-, ANSIBLE-, Direct-to-Device- und CNC-Controller-Image-Server nicht unterstützt.
- Standardmäßig enthalten die Metadaten des Remote-Server-Images von vManage die UUID für den Versionsparameter nach der Synchronisierung. Benutzer müssen die Metadaten bearbeiten und die UUID mit der entsprechenden Version aktualisieren. Die entsprechende Image-Version kann entweder vom vManage-Controller oder durch Anmeldung beim Gerät, auf dem das Image vorhanden ist, identifiziert werden.

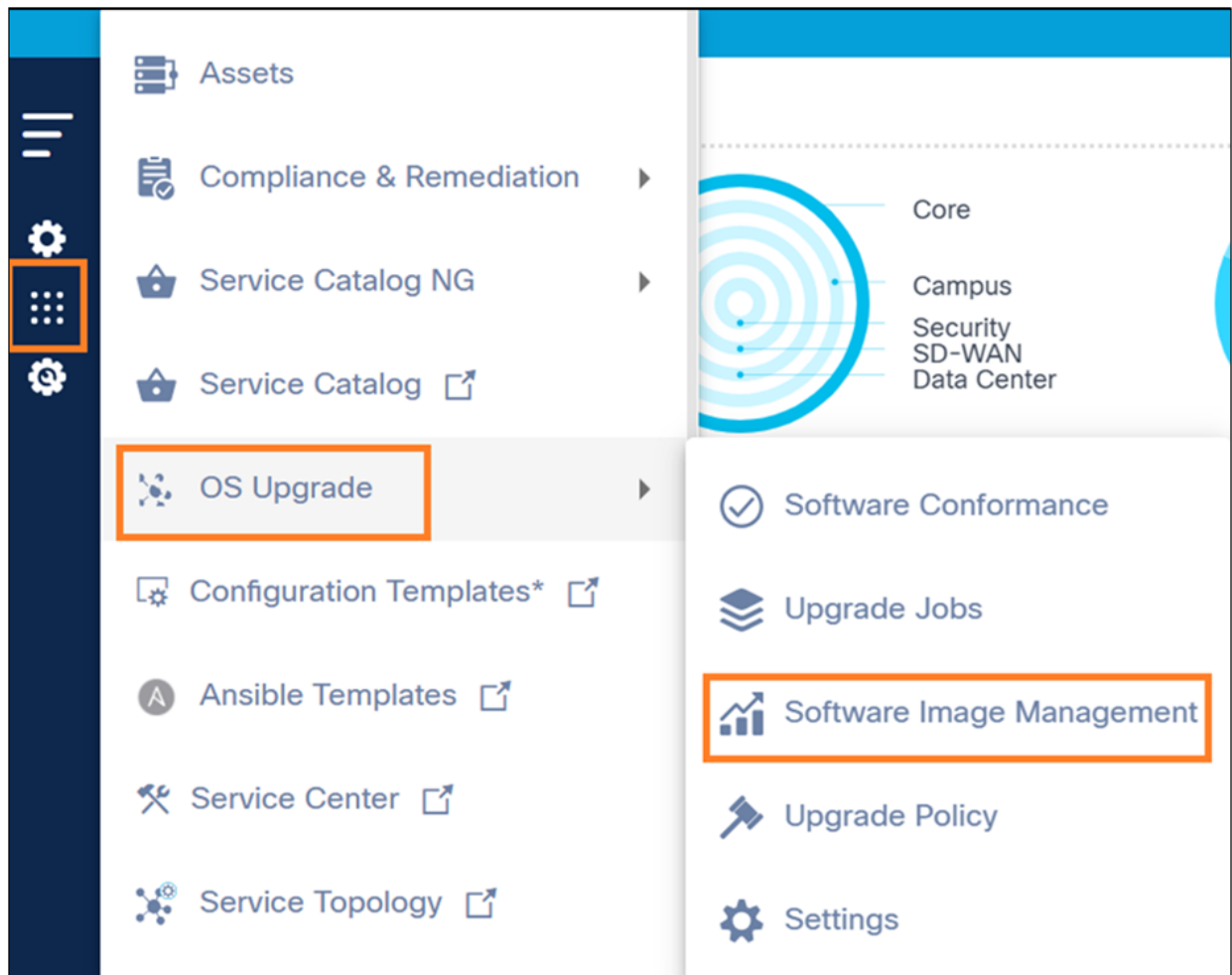
Image Distribution Server-Management

Image Distribution Server

Mit dieser Komponente können Operations-Benutzer Serverdetails für das Image-Repository für CNC-, NSO-, ANSIBLE-, FMC- und Direct-To-Device-Controller verwalten, die keine Unterstützung für das OOB-Image-Repository-Management bieten.

So greifen Sie auf die Seite Image Distribution Server zu:

1. Melden Sie sich bei BPA mit Anmeldeinformationen an, die den Verwaltungszugriff auf den Image Distribution Server verwalten.



Management von Software-Images

2. Wählen Sie Betriebssystem-Upgrade > Software-Image-Management aus.

SW Images Image Distribution Server

2 1 - Direct-To-Device 1 - NSO

Image Servers CONTROLLER TYPE

Image Server	Controller Type	Protocol	Controller ID's	Created By	Last Modified On	Action
☐ chennai	NSO	FTP	NSO-15	admin	Aug 2, 2023, 3:48 PM	⋮
☐ Bangalore	Direct-To-Device	FTP	All	admin	Aug 2, 2023, 3:43 PM	⋮

1 | Items per page 10

Registerkarte "Image Distribution Server"

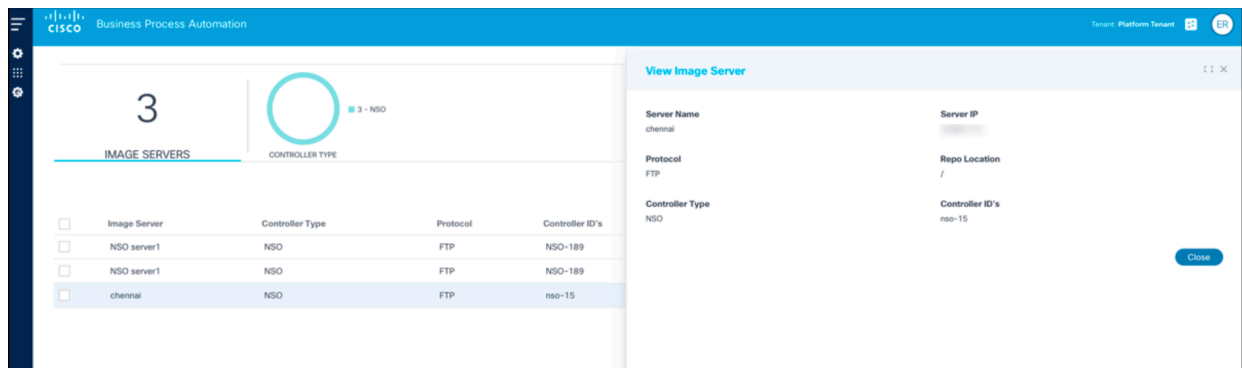
3. Klicken Sie auf die Registerkarte Image Distribution Server.

Die Registerkarte Image Distribution Server enthält Folgendes:

- Ein oben angezeigter Abschnitt zu Analysen bietet folgende Informationen:
 - Die Gesamtzahl der in dieser BPA-Instanz integrierten Image-Server
 - Ein Schnellfilter für den Controller-Typ, mit dem Image-Server basierend auf dem Controller-Typ gefiltert werden können (z. B. NSO, Direct-to-Device, CNC, ANSIBLE, FMC); Die Zahl gibt die Gesamtzahl der Image Distribution Server an, die diesem Controllertyp zugeordnet sind.
- Ein Symbol für weitere Optionen, das die folgenden Funktionen bietet:
 - Image-Server hinzufügen: Neuen Image Distribution Server hinzufügen
 - Alle löschen: Massenlöschung ausgewählter Verteilungsserver
- Ein Suchfilter, der zum Durchsuchen der Verteilungsserver verwendet werden kann und die folgenden exklusiven Suchfilter enthält:
 - Alle: Sucht in allen Feldern
 - Image-Server: Sucht nach Servern mit einem bestimmten Servernamen
 - Controller-ID: Sucht nach Servern, die einer bestimmten Controller-ID zugeordnet sind
- Ein Symbol Aktualisieren, mit dem die Seite aktualisiert und ausgewählte Filter gelöscht werden können.
- Vorhandene Verteilungsserver werden in einer Rastertabelle mit den folgenden Spalten angezeigt:
- Image-Server: Eindeutiger Name des Repository-Servers
 - Controller-Typ: Controller-Typ, auf den dieser Image-Server anwendbar ist
 - Protokolle: Vom Repository-Server unterstütztes Protokoll kopieren

 Anmerkung: Nur FTP, SCP und Secure File Transfer Protocol (SFTP) werden unterstützt.

- Controller-IDs: Controller-Instanzen, für die der aktuelle Repository-Server verwendbar oder anwendbar ist; Controller-Instanz bezieht sich auf Geräte, die von diesem Controller verwaltet werden.
- Erstellt von: Der Benutzer, der den Repository-Server integriert hat
- Zuletzt geändert am: Zeitstempel der letzten Aktualisierung der Serverdetails
- Aktion: Stellt zeilenspezifische Aktionen wie Bearbeiten und Löschen bereit



Bereich "Bildserver anzeigen"

- Durch Klicken auf eine Zeile wird das Fenster View Image Server geöffnet.

Hinzufügen von Image Server-Details

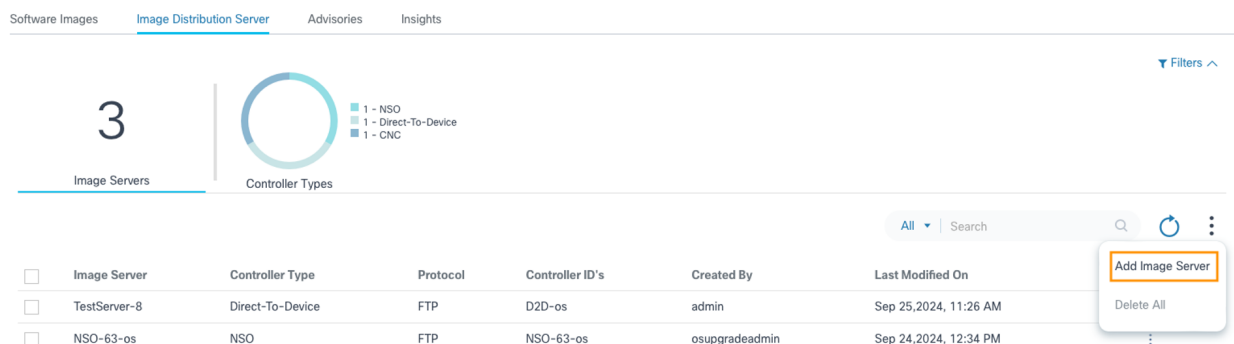


Image-Server hinzufügen

4. Wählen Sie das Symbol Weitere Optionen > Image Server hinzufügen aus. Die Seite Image-Server hinzufügen wird angezeigt.

Software Images **Image Distribution Server** Advisories Insights

All > Add Image Server

Server Name * 	Server IP * 	Protocol *
Root Location * 	Controller Type * 	Controller Instances *
User Name * 	Password * 	

Details zum Image-Server hinzufügen

Software Images **Image Distribution Server** Advisories Insights

All > Add Image Server

Server Name *	Server IP *	Protocol *
Demo-server	1.2.3.4	FTP
Root Location *	Controller Type *	Controller Instances *
/	NSO	NSO-142-OS
User Name *	Password *	
calo	*****	

Cancel Create

Image-Server mit Beispieldetails hinzufügen

5. Geben Sie Informationen in die folgenden Felder ein:

- Servername: Eindeutiger Name für den Image Repository Server
- Server-IP: IPv4-Adresse des Repository-Servers

 Anmerkung: Stellen Sie sicher, dass diese IP von Netzwerkgeräten erreichbar ist, bevor Sie sie hinzufügen.

- Protokolle: Unterstützt vom Image-Repository-Server für die Image-Kopie

 Anmerkung: Nur FTP-, SCP- und SFTP-Protokolle werden unterstützt.

- Repo-Standort: Basispfad der Image-Dateien im Repository-Server

 Anmerkung: Wenn Bilddateien im Stamm des Image Server-Repositoryordners vorhanden sind, funktioniert "/" als Wert.

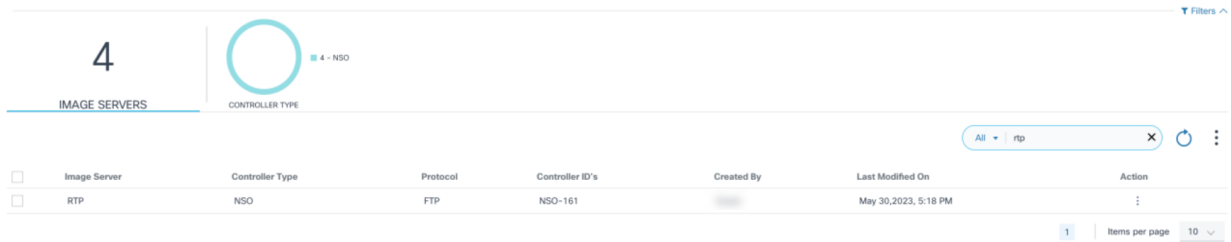
- Controller-Typ: Controller-Typ, für den der aktuelle Image-Server gilt

 Anmerkung: Nur NSO, Direct-To-Device, CNC und ANSIBLE werden unterstützt.

- Controller-Instanzen: Eine oder mehrere anwendbare Controller-Instanzen, basierend auf den verwalteten Geräten, für die der angegebene Image-Repository-Server zum Kopieren des Images verwendet werden soll
- Benutzer: Benutzerdefinierte Anmeldeinformationen für den Zugriff auf die Bilddateien aus dem Repository

6. Klicken Sie auf Erstellen. Die Statusbenachrichtigung wird angezeigt, gefolgt von einer Bestätigungsmeldung.

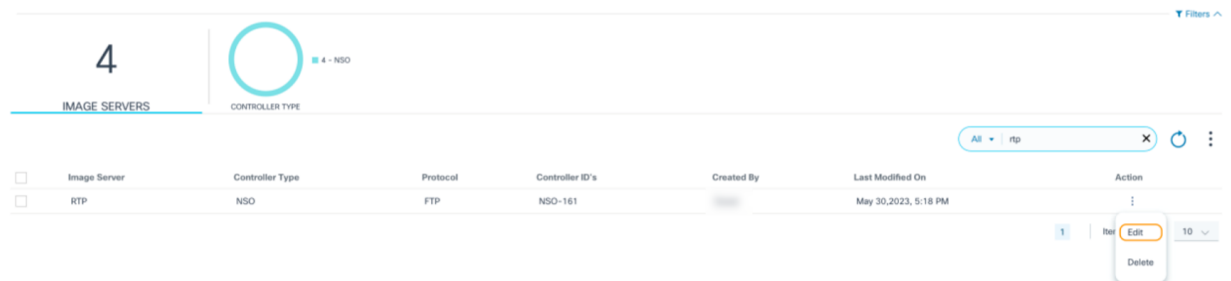
Bearbeiten der Image Server-Details



☐	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	⋮

Image Server-Suche

- Suchen Sie mithilfe des Felds Search (Suchen) den Verteilungsserver, der aktualisiert werden muss.



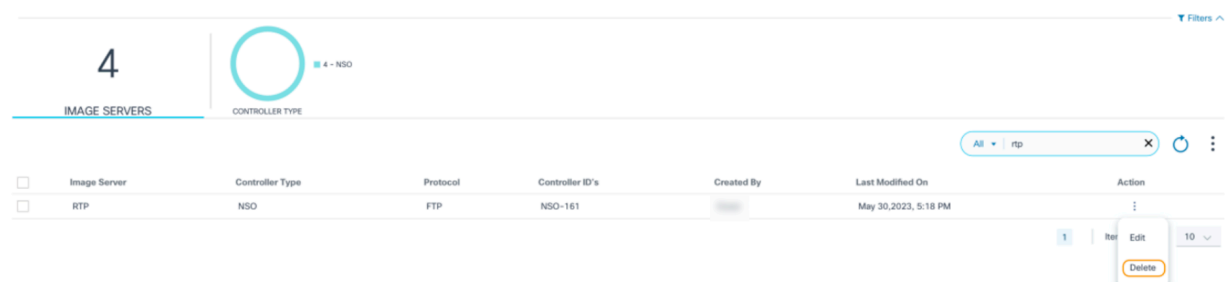
☐	Image Server	Controller Type	Protocol	Controller ID's	Created By	Last Modified On	Action
☐	RTP	NSO	FTP	NSO-161		May 30, 2023, 5:18 PM	⋮ Edit Delete

Abbildserver bearbeiten

- Wählen Sie in der Spalte Aktion das Symbol Weitere Optionen > Bearbeiten aus.
- Aktualisieren der erforderlichen Parameter
- Klicken Sie auf Speichern. Es wird eine Statusbenachrichtigung und eine Bestätigungsmeldung angezeigt.

Image Server-Details werden gelöscht

- Suchen Sie mithilfe des Filters Search (Suchen) den bzw. die gewünschten Server.



☐	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	⋮ Delete

Image-Server löschen

- Wählen Sie in der Spalte Aktion das Symbol Weitere Optionen > Löschen aus, um einen

einzelnen Verteilungsserver zu löschen.

ODER

Software Images | **Image Distribution Server** | Advisories | Insights

3 Image Servers

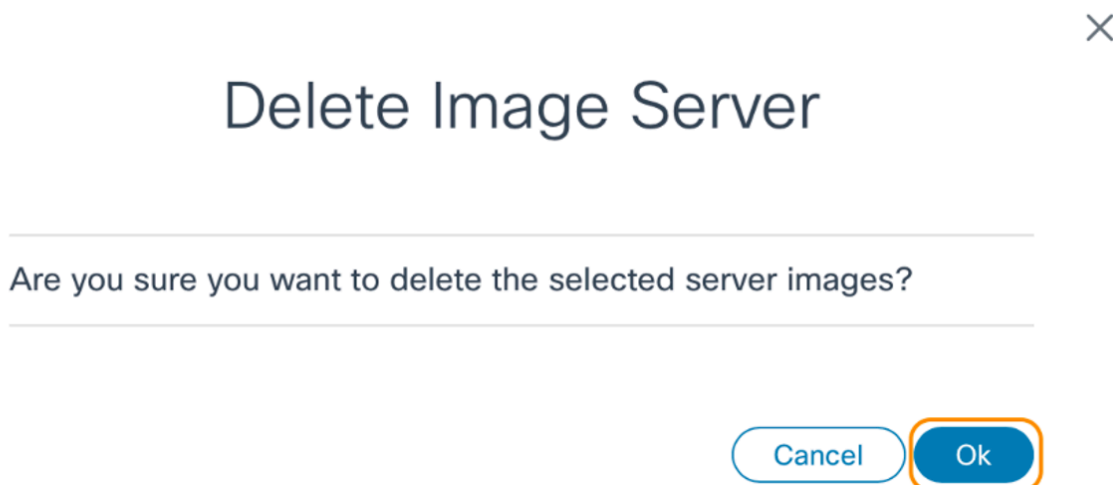
Controller Types: 1 - NSO, 1 - Direct-To-Device, 1 - CNC

☐	Image Server	Controller Type	Protocol	Controller ID's	Created By	Last Modified On	
☒	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	

Mehrere Image-Server löschen

Wählen Sie die gewünschten Server aus, und wählen Sie das Symbol Weitere Optionen > Alle löschen aus, um mehrere Verteilungsserver zu löschen.

Es wird eine Bestätigung angezeigt.



Löschbestätigung

3. Klicken Sie auf OK. Statusbenachrichtigungen werden angezeigt, gefolgt von einer Bestätigungsmeldung.

Software-Informationen

Software Insights erkennt alle Sicherheitslücken, z. B. Sicherheitsankündigungen, Bugs und End-of-Life-Bedrohungen, die durch die Netzwerkressourcen entstehen. Es enthält auch Softwarevorschläge für die von Cisco Catalyst Center- und NDFC-Controllern verwalteten

Gerätemodelle. Administrator-Benutzer können die empfohlene Softwareversion für Netzwerkressourcen auswählen und eine Konformitätsrichtlinie für die Gerätemodelle erstellen, wenn der Vorschlag verfügbar ist.

Voraussetzungen

- Aktivieren Sie den Adapter, um Einblicke zu erhalten. Der Adapter für den Cisco Insights-Server mit dem Namen "Cisco-Insights-Adapter" ist im OOB erhältlich. Für die Integration in einige externe Insights-Server von Drittanbietern müssen entsprechende Adapter erstellt werden. Weitere Informationen finden Sie unter Configuring Insights Adapter im [BPA Developer Guide](#).
 - Für die Verbindung des BPA-Systems mit der Cisco Cloud ist eine Internetverbindung erforderlich.
 - Vergewissern Sie sich, dass sich `client_id` und `client_secret` in der Adapterkonfiguration befinden, bevor Sie mit der Synchronisierung fortfahren.
 - Bei Bedarf kann ein Proxy für das Internet wie folgt konfiguriert werden:
 - Für den IOS-XR-Betriebssystemtyp kann die benutzerdefinierte Serien-Modell-Zuordnung im Referenzdaten-Management (Reference Data Management, RefD) nach Bedarf durchgeführt werden. Weitere Informationen zur benutzerdefinierten Serien-zu-Modell-Zuordnung finden Sie im [BPA-Entwicklerhandbuch](#).
 - BPA Kubernetes Pods benötigen einen Internetzugang, um Ratschläge, Fehler und Details zum Ende des Lebenszyklus von Cisco zu erfassen. Wenn das BPA-Netzwerk keinen direkten Internetzugang hat, aber über einen Proxy verfügbar ist, gehen Sie wie unten beschrieben vor, damit Kubernetes Pods den Proxy für das Internet verwendet.
1. Aktualisieren Sie das Skript mit der tatsächlichen Proxy-Adresse anstelle von `<<http://proxy-domain.com:port>>`.
 2. Konfigurieren Sie die Umgebungsparameter für jeden POD in den YAML- oder Helmdiagrammen der Bereitstellung.
 3. Führen Sie das folgende Skript im Kubernetes-Knoten aus, indem Sie alle Bereitstellungsnamen in der Konfiguration `NO_PROXY` oder `no_proxy` hinzufügen.

```
#!/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
```

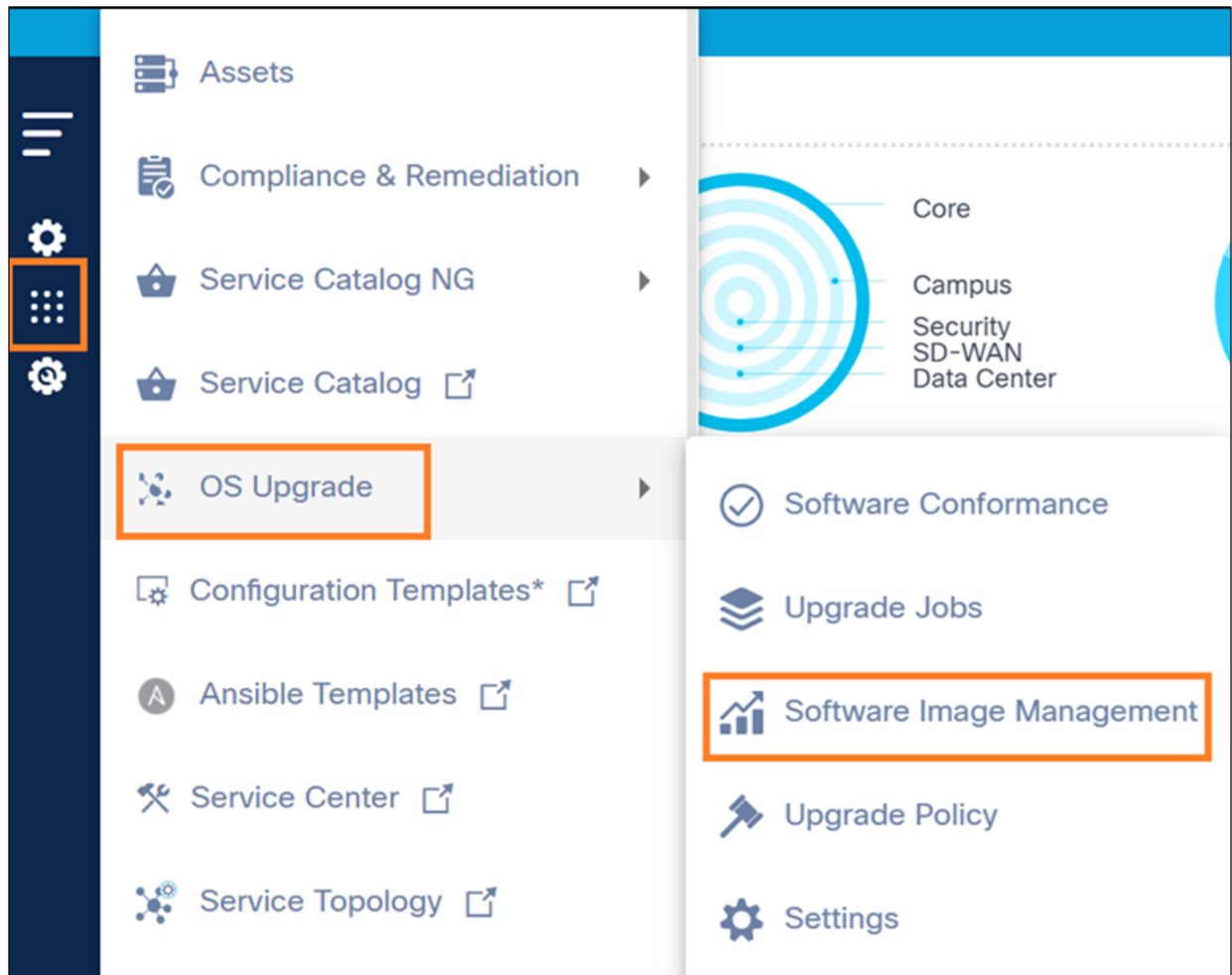
```
done
```

 Anmerkung: Durch die oben beschriebene Einrichtung des Proxys kann der Insights-Adapter auf das Cisco Netzwerk zugreifen und erforderliche Software Insights-Daten in BPA herunterladen. Wenn Sie sich direkt ohne Proxy mit einem beliebigen externen Insights-Server verbinden möchten, müssen Sie diese der Variablen no_proxy hinzufügen.

Abrufen von Software-Erkennungsdaten in BPA

So synchronisieren Sie Software-Einblicke in BPA:

1. Melden Sie sich bei BPA mit Anmeldeinformationen an, die Zugriff auf Software-Einblicke bieten.



Navigation im Software-Image-Management

2. Wählen Sie auf der Seitenleiste OS Upgrade > Software Image Management (Betriebssystem-Upgrade > Software-Image-Verwaltung) aus.



Registerkarte Ratgeber

3. Klicken Sie auf die Registerkarte Ratgeber.

Synchronisierung zum Abrufen von Software-Insights in BPA



Synchronisierung zum Abrufen von Software-Insights in BPA

4. Klicken Sie auf Synchronisieren.

Dabei werden alle Sicherheitsankündigungen, Fehler bei der Priorität, End-of-Life-Meldungen und Softwarevorschläge im Zusammenhang mit den im Bestand vorhandenen Ressourcen erkannt. Sicherheitsempfehlungen und Daten für das Ende des Lebenszyklus der Software werden basierend auf dem Betriebssystemtyp und der Softwareversion bestimmt. Prioritätsfehler und Software-Vorschläge werden basierend auf der Produkt-ID und der Software-Version bestimmt.

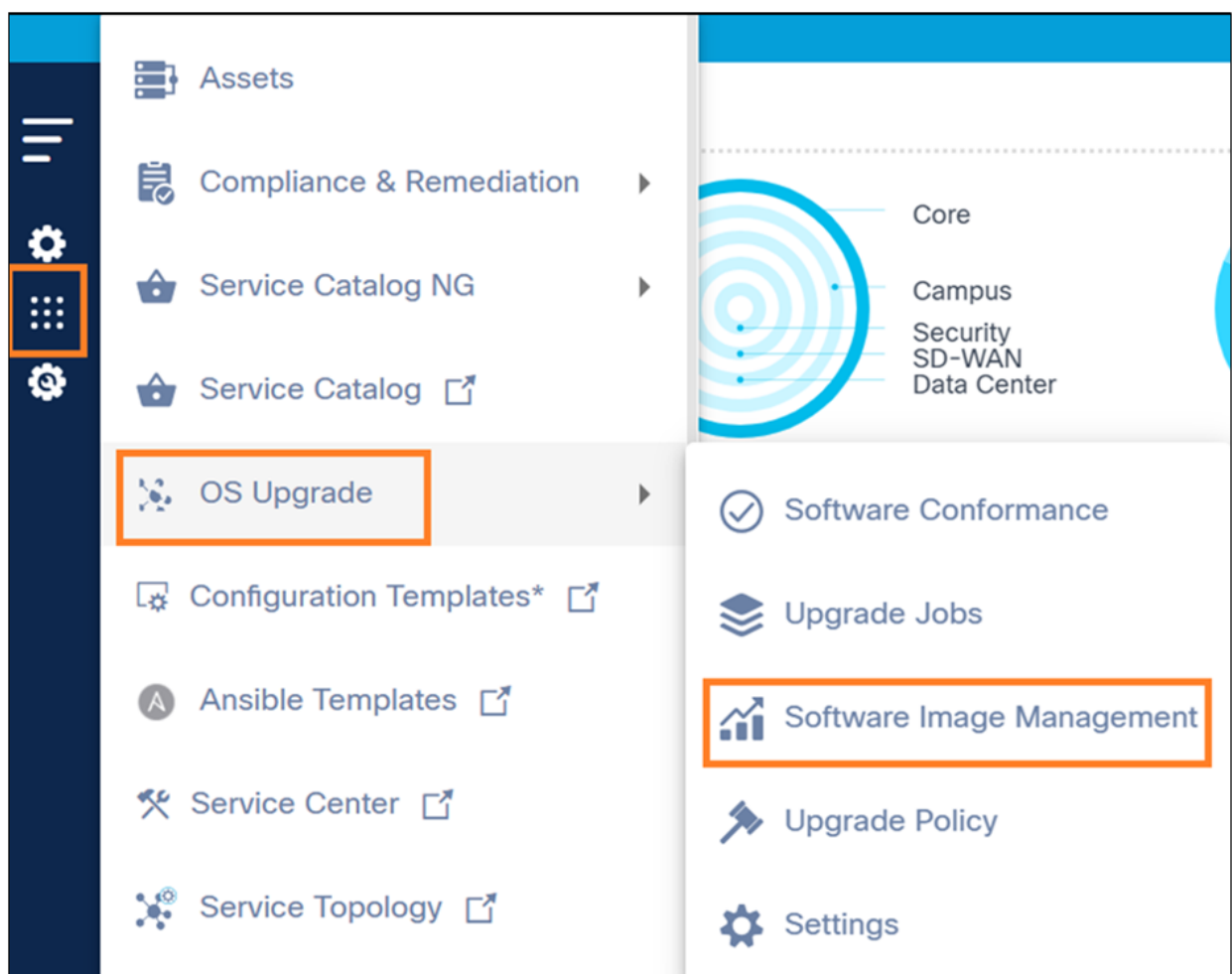
Letzte Aktualisierung zeigt das Datum und die Uhrzeit der letzten Synchronisierung der Einblicke an, und im Feld Synchronisierungsstatus wird der letzte Synchronisierungsstatus angezeigt.

 Anmerkung: Alle zutreffenden Hinweise, Fehler, Versionshinweise und Vorschläge werden über die Cisco-Cloud mithilfe der Datei "Cisco-Insights-Adapter" abgerufen.

Anzeigen und Verwalten von Sicherheitsempfehlungen

So rufen Sie die Seite "Ratgeber" auf:

1. Melden Sie sich bei BPA mit Anmeldeinformationen an, die den Zugriff auf Advisories verwalten.



Navigation im Software-Image-Management

2. Wählen Sie Betriebssystem-Upgrade > Software-Image-Management aus.

Software Images Image Distribution Server **Advisories** Insights

Security Advisories 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**

Priority Bugs

Filters

Impacts

- ☒ All
- ☐ Critical
- ☐ High
- ☐ Medium
- ☐ Low

Last Updated

- ☒ All
- ☐ <30 Days
- ☐ 31-60 Days
- ☐ 61-90 Days
- ☐ >90 Days

Clear All

Security Advisories 214 Total

Advisory	Impact	CVE	Softwares Versions	Last Updated	Version	Potentially Affected Assets
Vulnerability in NVIDIA Data Plane Development Kit	High	CVE-2022-28199	IOS-XE:17.6.2,IOS-XE:17.6.3a	1 year ago	1.0	4
Telnet Vulnerability Affecting Cisco Products: Ju	High	CVE-2020-10188	IOS-XE:16.9.2s	3 years ago	1.1	1
SNMP Remote Code Execution Vulnerabilities in CIs	High	CVE-2017-6736,CVE-2017-6737,CVE-2017-6738,CVE-201	IOS:15.2(4)E1,IOS:15.0(2)SE	8 months ago	1.10	2
OpenSSL RSA Temporary Key Cryptographic Downgrade	Medium	CVE-2015-0204	IOS:15.0(2)SE	8 years ago	14.0	1
OSPF LSA Manipulation Vulnerability in Multiple C	Medium	CVE-2013-0149	IOS:15.0(2)SE	6 years ago	1.4	1
Multiple Vulnerabilities in ntpd (April 2015) Aff	Medium	CVE-2015-1798,CVE-2015-1799	IOS:15.0(2)SE	8 years ago	1.11	1
Multiple Vulnerabilities in OpenSSL		CVE-2010-5298,CVE-2014-0076,CVE-				

Sicherheitsempfehlungen

3. Klicken Sie auf die Registerkarte Ratgeber. Die Seite Sicherheitsempfehlungen wird standardmäßig geöffnet.

Die folgenden Optionen werden zum Filtern von Advisordaten angezeigt:

- Die Auswirkungen ermöglichen eine Filterung nach dem empfohlenen Schweregrad. Alle sind standardmäßig ausgewählt.
- Last Updated (Zuletzt aktualisiert) ermöglicht die Filterung nach dem letzten Aktualisierungsdatum der Benachrichtigung. Alle sind standardmäßig ausgewählt.
- Alle löschen setzt die ausgewählten Filter zurück
- Der Suchfilter wird für die Suche nach Ratgebern verwendet und enthält die folgenden exklusiven Suchfilter:
 - Alle: Durchsucht Spalten wie Advisory, CVE und Software Versions
 - Beratung: Sucht nach Ratgebern mit den in der Suche angegebenen Begriffen
 - ZVE: Suche nach Advisors mit spezifischen Common Vulnerabilities and Exposures (CVE)
 - Software-Versionen: Sucht nach Ratschlägen zu bestimmten Betriebssystemtypen oder Softwareversionen
- Das Symbol Aktualisieren wird verwendet, um die Seite zu aktualisieren und die ausgewählten Filter zu löschen.
- Vorhandene Advisories werden mit den folgenden Spalten angezeigt:
 - Beratung: Zusammenfassung des Gutachtens
 - Auswirkungen: Beratender Schweregrad
 - Höchst.: CVEs zugewiesen
 - Softwareversionen: Betroffener Betriebssystemtyp und betroffene Softwareversionen
 - Letzte Aktualisierung: Datum und Uhrzeit der letzten Aktualisierung der Benachrichtigung

- Version: Ankündigung
- Potenziell betroffene Ressourcen: Anzahl der Vermögenswerte, die von der Beratung betroffen sein könnten
- Durch Klicken auf das Kopfzeilenfeld werden die Ratgeber sortiert.



Anmerkung: Die Sortierung ist für potenziell betroffene Ressourcen nicht möglich.

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-2018,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.

Ansicht mit beratungsbezogenen Details

- Wenn Sie eine Beratungszeile auswählen, wird die Detailansicht einer Beratung geöffnet, die die folgenden Registerkarten enthält:
 - Zusammenfassung: Zeigt eine Zusammenfassung des ausgewählten Hinweises an; wird standardmäßig angezeigt
 - Betroffene Ressourcen: Zeigt potenziell betroffene Ressourcendetails an, z. B. Gerätenamen, Seriennummern, Modellnamen, Softwareversionen, IP-Adressen und Controller-ID; Sortieren und Durchsuchen der Ressourcen können auf dieser Registerkarte durchgeführt werden.

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-2018,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

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

1 Items per page 10

Sicherheitsberatung anzeigen

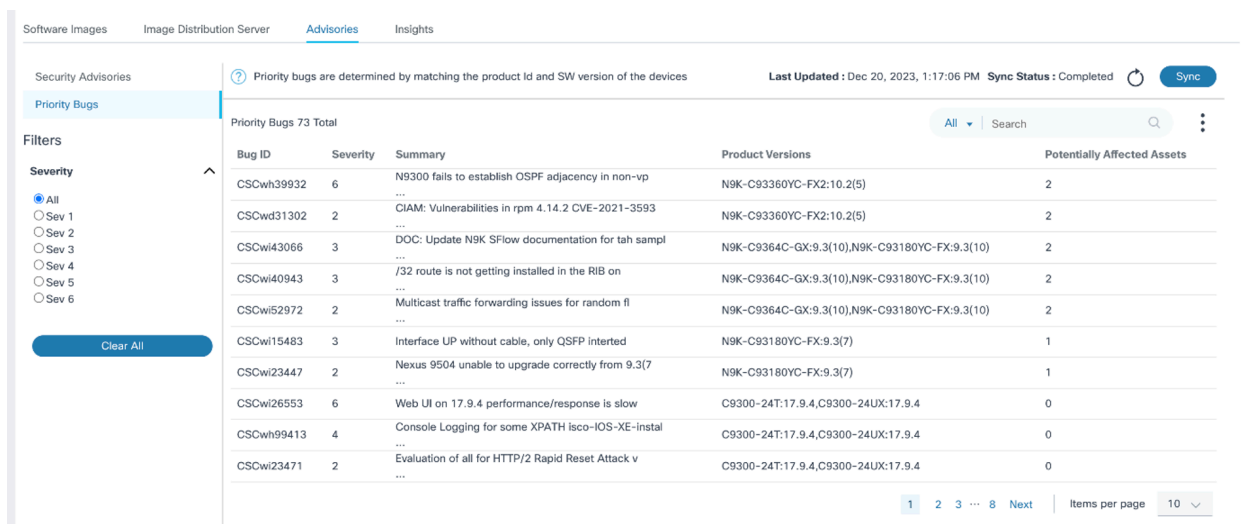
- Link "Sicherheitsempfehlung anzeigen": Navigiert zur offiziellen Advisory-Seite

Anzeigen und Verwalten von Prioritätsfehlern



Prioritätsfehler auswählen

Nachdem Sie die Seite Advisories wie im vorherigen Abschnitt beschrieben geöffnet haben, klicken Sie auf die Registerkarte Priority Bugs. Die Seite "Priority Bugs" wird angezeigt.



Prioritäre Fehler

Die folgenden Optionen sind auf der Seite Priority Bugs (Prioritätsfehler) verfügbar:

- Ein Schweregrad-Filter, der eine Filterung nach Schweregrad des Fehlers ermöglicht. Alle sind standardmäßig ausgewählt.
- Der Suchfilter kann zum Durchsuchen der Bugs verwendet werden und enthält die folgenden exklusiven Suchfilter:
 - Alle: Sucht in allen Feldern
 - Bug-ID: Sucht nach Bugs mit einer angegebenen Bug-ID
 - Zusammenfassung: Sucht nach Bugs mit spezifischen Schlüsselwörtern in der Zusammenfassung
 - Produktversionen: Sucht nach Bugs, die einer bestimmten Produkt-ID oder Softwareversion zugeordnet sind
- Über das Symbol Aktualisieren können Sie die Seite aktualisieren und die ausgewählten Filter löschen.

- Prioritätsfehler werden in der Tabelle mit den folgenden Spalten angezeigt:
 - Bug-ID
 - Schweregrad: Schweregrad des Bugs
 - Zusammenfassung: Zusammenfassung des Bugs
 - Produktversionen: Betroffene Produkt-ID und Softwareversionen
 - Potenziell betroffene Ressourcen: Anzahl der Ressourcen, die von dem Fehler betroffen sein könnten
- Die Sortierung kann durch Klicken auf eine beliebige Spaltenüberschrift erfolgen, mit Ausnahme von Potenziell betroffenen Ressourcen

The screenshot shows the Cisco Security Advisories interface. On the left, there's a sidebar with 'Security Advisories' and 'Priority Bugs' tabs. Below them are filters for severity (All, Sev 1, Sev 2, Sev 3, Sev 4, Sev 5, Sev 6) and a 'Clear All' button. The main area displays a table of priority bugs with columns: Bug ID, Severity, and Summary. The table lists 73 total bugs. On the right, a detailed view for bug CSCwh39932 (Severity 6) is shown, including a description, symptom, conditions, and a workaround.

Bug ID	Severity	Summary
CSCwh39932	6	N9300 fails to establish OSPF adjacency in non-vpc vlan with orphan port connected L3 device
CSCwd31302	2	CIAM: Vulnerabilities in rpm 4.14.2 CVE-2020-15150
CSCwi43066	3	DOC: Update N9K SFlow documentation for N9K 9504
CSCwi40943	3	/32 route is not getting installed in the RIB
CSCwi52972	2	Multicast traffic forwarding issues for random
CSCwi15483	3	Interface UP without cable, only QSPF interface
CSCwi23447	2	Nexus 9504 unable to upgrade correctly from
CSCwi26553	6	Web UI on 17.9.4 performance/response issues
CSCwh99413	4	Console Logging for some XPATH isco-IO
CSCwi23471	2	Evaluation of all for HTTP/2 Rapid Reset At

Bug Details for CSCwh39932 (Severity 6):
 Description: N9300 fails to establish OSPF adjacency in non-vpc vlan with orphan port connected L3 device.
 Symptom: OSPF stuck in exstart state.
 Conditions: VPC Orphan port connected L3 device establishing OSPF adjacency in non-vpc vlan carried on L2 trunk between vpc peers.
 Workaround: N/A

Bug-Detailansicht

- Wenn Sie auf einen Fehler klicken, öffnet sich die Detailansicht des Fehlers, die Folgendes beinhaltet:
 - Registerkarte "Übersicht": Zeigt Details zu Bug Severity, Description (Fehlerschweregrad) und Workaround an

The screenshot shows the same Cisco Security Advisories interface, but with the 'Affected Assets' tab selected for bug CSCwh39932. The tab shows a list of assets affected by the security advisory. The table has columns: Asset Name, Serial Number, Model Name, Version, Role, IP Address, and Controller ID. There are 2 total assets listed.

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

Registerkarte "Betroffene Ressourcen"

- Registerkarte "Betroffene Ressourcen": Zeigt alle potenziell betroffenen Ressourcendetails

an, wie z. B. den Asset-Namen, die Seriennummer, den Modellnamen, die Software-Version, die IP-Adresse und die Controller-ID; Sortieren und Durchsuchen der Ressourcen können auf dieser Registerkarte durchgeführt werden.

Software ImagesImage Distribution ServerAdvisoriesInsights

Security AdvisoriesPriority Bugs

FiltersSeverity

- 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 QSPF 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 6CSCwh39932 : N9300 fails to establish OSPF adjacency in non-vpc vlan with orphan port connected L3 device

View Priority Bugs

SummaryAffected 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

Prioritätsfehler anzeigen

- Link "Priority Bugs" anzeigen: Navigiert zum offiziellen Bug Search Tool

Assets

29Total

Core

Campus Data Center Security SD-WAN

Domain

Controller Type

Controller

Controller

ANSIBLE-156

NSO-183

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

Ressourcen

In Asset Manager können Benutzer eine Liste aller Ressourcen anzeigen. Bei der Auswahl einer Ressource werden Informationen auf Ressourcenebene angezeigt. Dazu gehören Details zu Sicherheitslücken in der Ressourcen-Software, die in zwei Registerkarten unterteilt sind: Ratgeber und EOX.

29Total

Core

Campus Data Center Security SD-WAN

Domain

Controller Type

Controller

Controller

ANSI

NSO

Name	ControllerType	Ip Address	Location	Managed By
------	----------------	------------	----------	------------

SummaryBackups

Admin Stateunlocked

Controller TypensNSO

Platform Serial Number

DomainCore

IsCompliant

AdvisoriesEOX

Auth Groupcxlab

Current Version7.6.2

Device-Typecli

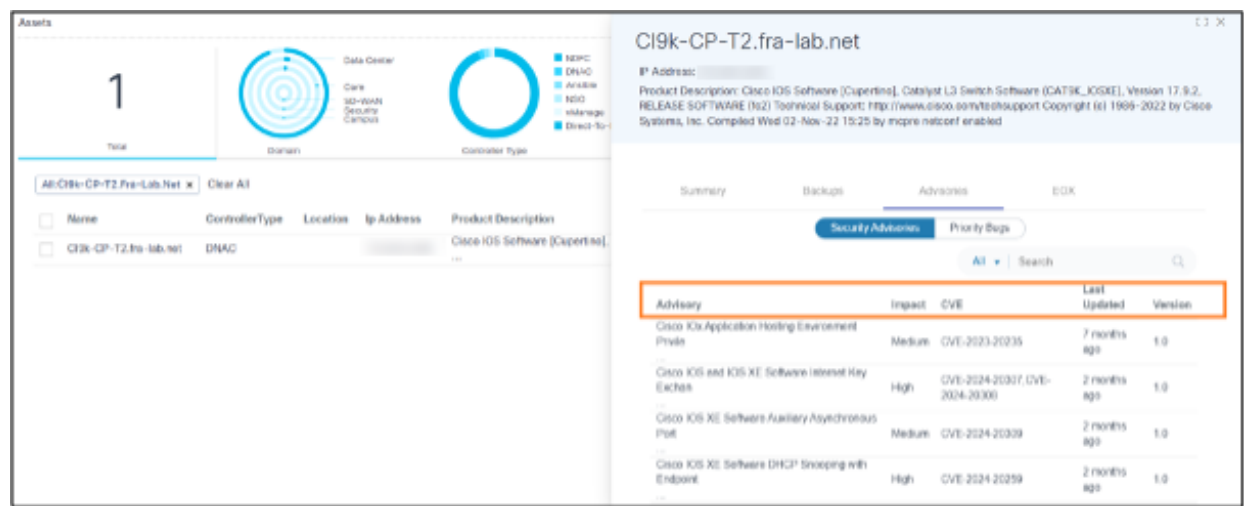
Ip Address

Managed By

Beratung und EoX

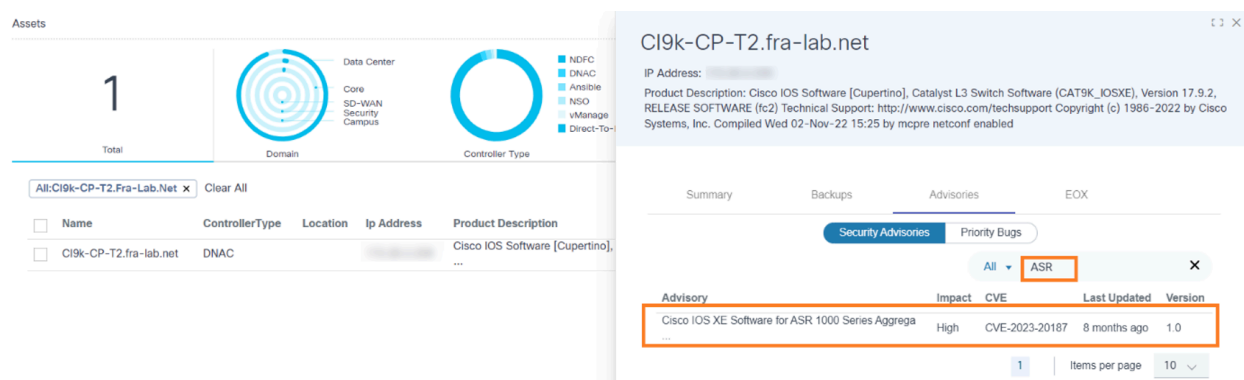
Die Registerkarte Advisories enthält zwei Unterregisterkarten: Security Advisories (Sicherheitsempfehlungen) und Priority Bugs (Prioritätsfehler). Weitere Einzelheiten zu diesen Registerkarten finden Sie in den nachstehenden Abschnitten.

Sicherheitsempfehlungen



Sicherheitsempfehlungen für ausgewählte Ressourcen

Auf der Unterregisterkarte "Security Advisories" (Sicherheitsempfehlungen) können Benutzer alle Sicherheitsempfehlungen anzeigen, die sich auf eine ausgewählte Ressource auswirken. Die Spalten in der Tabelle mit den Sicherheitsankündigungen umfassen Empfehlungen, Auswirkungen, CVE, Letzte Aktualisierung und Version.



Suche nach Sicherheitsempfehlungen

Assets

1 Total

Domain: Data Center, Core, SD-WAN, Security Campus

Controller Type: NDPC, DNAC, Ansible, NSO, vManage, Direct-To

Search: 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: [REDACTED]

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

Suche nach Sicherheitsempfehlungen - Auswirkungsoption

Benutzer können Advisories basierend auf Werten in den Spalten Advisories, Impact, CVE, Last Updated und Version durchsuchen. Paginierung ermöglicht es Benutzern, zwischen Seiten zu navigieren.

Prioritäre Fehler

Assets

1 Total

Domain: Data Center, Core, SD-WAN, Security Campus

Controller Type: NDPC, DNAC, Ansible, NSO, vManage, Direct-To

Search: 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: [REDACTED]

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

Prioritäre Bugs mit Auswirkungen auf ausgewählte Ressourcen

Auf der Unterregisterkarte "Priority Bugs" (Prioritätsfehler) können Benutzer auf alle Prioritätsfehler zugreifen, die eine bestimmte Ressource betreffen. Die Spalten auf dieser Registerkarte umfassen die Bug-ID, den Schweregrad und die Zusammenfassung.

Assets

1 Total

Domain: Data Center, Core, SD-WAN, Security Campus

Controller Type: NDPC, DNAC, Ansible, NSO, vManage, Direct-To

Search: 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: [REDACTED]

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

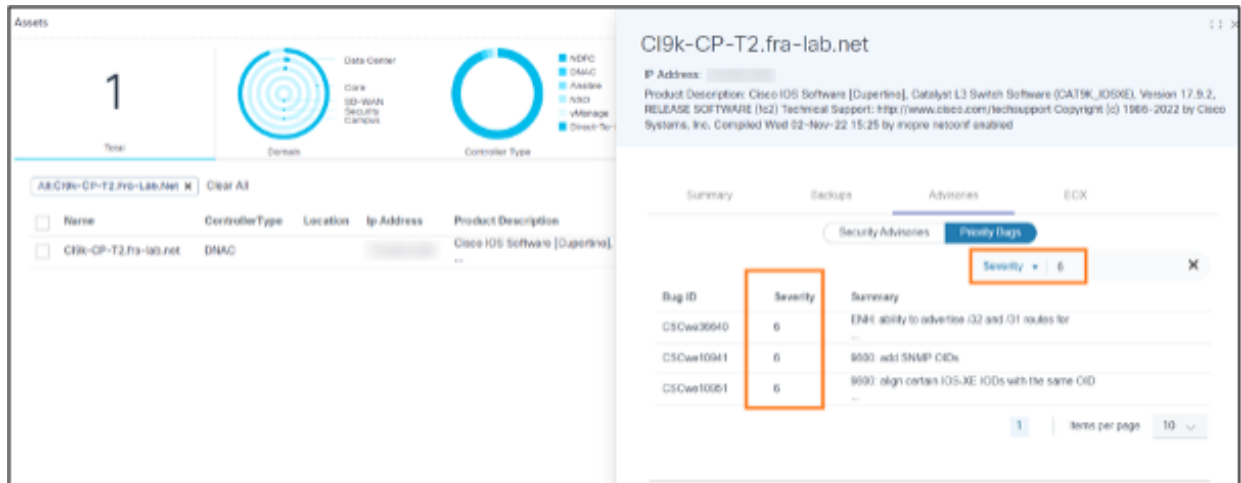
Security Advisories Priority Bugs

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

Suche nach Prioritätsfehlern nach Übersicht



Suche nach Priorität nach Schweregrad

Benutzer können anhand der Werte in den Spalten Bug ID, Severity und Summary nach Prioritätsfehlern suchen. Paginierung erleichtert das Navigieren zwischen Seiten.

EoX



Registerkarte EoX

Auf der Registerkarte EoX werden Daten zum Ende des Lebenszyklus einer Software für eine Ressource angezeigt. Diese Daten umfassen drei wichtige Daten:

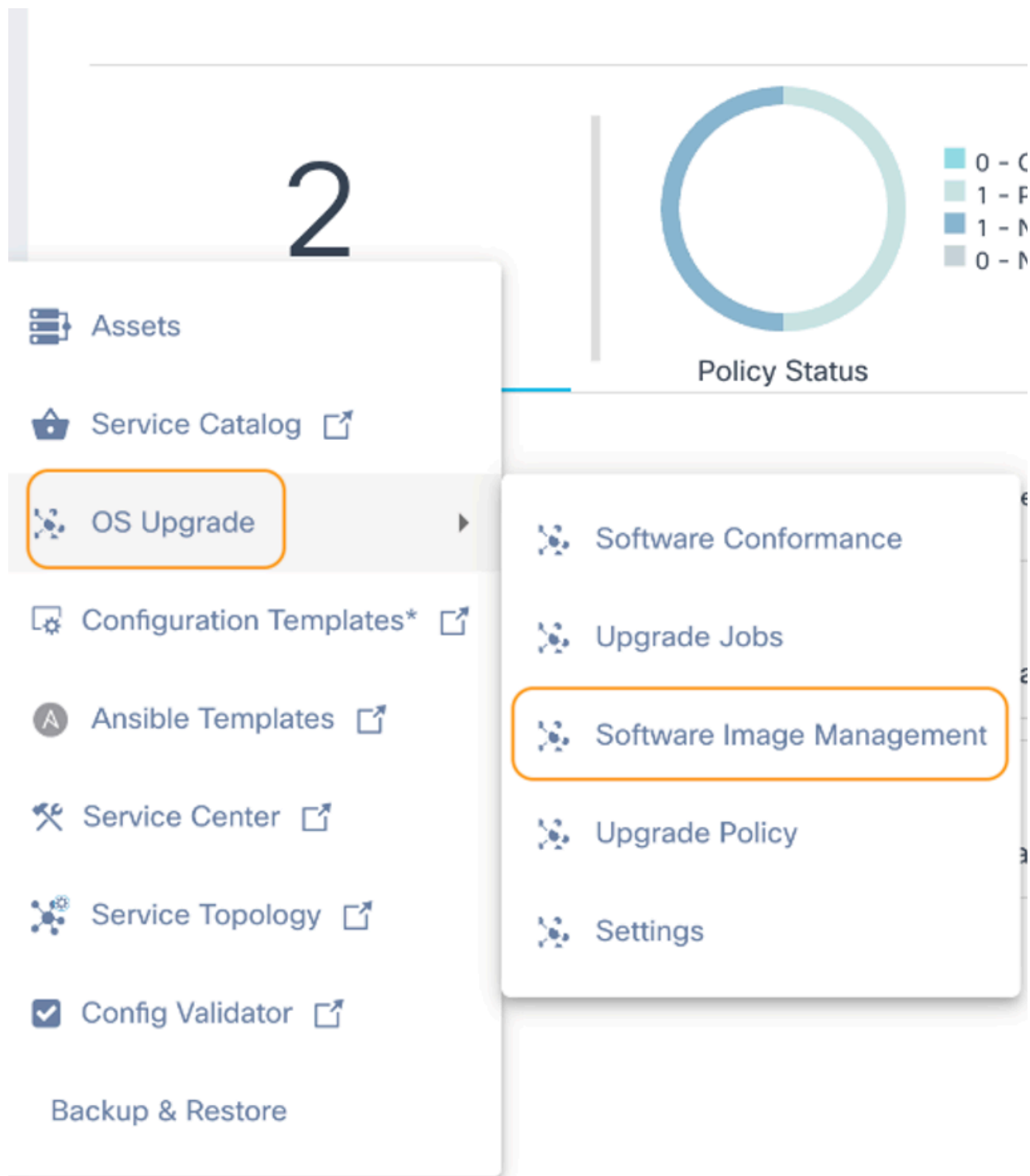
- Ende der Softwarewartung
- End-of-Security-Support
- Letztes Datum für den Support

Anzeigen von Software-Einblicken

Software Insights bietet Softwarevorschläge für die von Cisco Catalyst Center und NDFC-Controllern verwalteten Gerätemodelle. Administratoren können damit eine Konformitätsrichtlinie für die Gerätemodelle erstellen, wenn der Vorschlag verfügbar ist.

Zugriff auf Software Insights:

1. Melden Sie sich bei BPA mit Anmeldeinformationen an, die den Zugriff auf Insights verwalten.



Management von Software-Images

2. Wählen Sie auf der Seitenleiste OS Upgrade > Software Image Management (Betriebssystem-Upgrade > Software-Image-Verwaltung) aus.

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	⋮

Registerkarte "Einblicke"

3. Klicken Sie auf die Registerkarte Einblicke.

Die Registerkarte Einblicke enthält Folgendes:

- Ein Filter, mit dem Benutzer Daten auf der Grundlage von Vorschlägen filtern können. Alle sind standardmäßig ausgewählt.
 - Ja filtert Daten nach Gerätemodellen mit Vorschlägen
 - Filtert die Daten für Gerätemodelle nicht ohne Vorschläge

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	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	⋮

In CSV exportieren

- Das Symbol More Options (Weitere Optionen) bietet eine Option Export to CSV (In CSV exportieren) zum Exportieren der auf der Seite angezeigten Daten.
 - Das Symbol "Aktualisieren" aktualisiert die Seite und löscht die ausgewählten Filter.
 - Der Filter Suchen dient zum Durchsuchen der Daten und enthält die folgenden exklusiven Suchfilter:
- Alle: Sucht in allen Spalten (z. B. Gerätemodell, Produktfamilie und Softwaretyp)
- Gerätemodell: Sucht nach Daten mit einem bestimmten Gerätemodellnamen

- Produktfamilie Sucht nach Daten mit dem spezifischen Produktnamen
- Softwaretyp: Sucht nach Daten mit einem bestimmten Softwaretypnamen
 - Vorhandene Gerätemodelle werden in den folgenden Spalten angezeigt:
 - Gerätemodell: Name des Gerätemodells
 - Produktfamilie: Name der Produktfamilie, zu der das Gerätemodell gehört
 - Softwaretyp: Name des Softwaretyps, zu dem das Gerätemodell gehört
 - Aktuelle Versionen: Liste der eindeutigen Softwareversionen, die derzeit im Inventar für das Gerätemodell vorhanden sind
 - Ausgewählte Version: Vorgeschlagene Release-Version. Diese wurde als optionale Version aus den Vorschlägen von Cisco ausgewählt.
 - Ressourcen: Anzahl der im Asset Manager für das Gerätemodell vorhandenen Ressourcen
 - Vorschläge: Zeigt Ja oder Nein für alle Vorschläge an, die für das Gerätemodell verfügbar sind.

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

Vorgeschlagene Navigation anzeigen

- Aktion: Ermöglicht zeilenspezifische Aktionen über das Symbol Weitere Optionen (z. B. Vorschläge anzeigen und Ressourcen anzeigen)

 Anmerkung: Die Option Vorschläge anzeigen ist deaktiviert, wenn das Gerätemodell keine Vorschläge enthält.

Anzeigen und Auswählen der vom Anbieter vorgeschlagenen Softwareversionen

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

Registerkarte Vorschläge

Wenn Sie in der Spalte Aktion auf das Symbol Weitere Optionen > Vorschläge anzeigen klicken, wird ein Seitenfenster mit allen Details zum Einblick angezeigt. Die Registerkarte Vorschläge enthält die aktuellen und vorgeschlagenen Versionsinformationen für das ausgewählte Gerätemodell. Es ist möglich, dass ein Gerätemodell mehr als einen Vorschlag enthält. Folgende Daten sind verfügbar:

- Version und Datum der Veröffentlichung: Wenn die Cisco Cloud verfügbar ist, werden die Versionsinformationen, das Datum und die Notizen für aktuelle und vorgeschlagene Versionen angezeigt. Wenn die Anlagen im Bestand zu mehr als einer Version gehören, werden alle zutreffenden Versionen in der Spalte Aktuell als durch Kommas getrennte Werte angezeigt
- Konformitätsrichtlinie erstellen: Ermöglicht Administratoren die Erstellung einer Konformitätsrichtlinie für eine bestimmte Version, wobei die Geräterolle "Any" (Beliebig) lautet

Anmerkung: Die Erstellung von Konformitätsrichtlinien wird nur für NDFC-Controller-Gerätemodelle unterstützt.

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

Policy-Option löschen

 Anmerkung: Wenn bereits eine Richtlinie für das Gerätemodell vorhanden ist, wird ein Fehler angezeigt. Wenn keine Richtlinie vorhanden ist, wird eine Richtlinie im Status Aktiviert erstellt. Wenn eine Richtlinie aus Insights erstellt wird, können Benutzer die Richtlinie löschen.

- Bugs: Zeigt eine konsolidierte Fehleranzahl für jede Version an.
- Sicherheitsempfehlungen: Zeigt für jede Version eine konsolidierte Anzahl an Hinweisen an.
- EoX: Zeigt das Ende der Softwarewartung, das Ende des Sicherheits-Supports und das Datum des letzten Supports für jede Version an

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 ▾

Registerkarte "Betroffene Ressourcen"

Wenn Sie in der Spalte Aktion das Symbol Weitere Optionen > Anlagen anzeigen auswählen, wird ein seitliches Fenster geöffnet, in dem standardmäßig die Registerkarte Betroffene Anlagen angezeigt wird. Die Registerkarte "Betroffene Ressourcen" zeigt Details zu potenziell betroffenen Ressourcen in Spalten wie Asset-Name, Seriennummer, Modellname, Softwareversion, IP-Adresse und Controller-ID. Auf dieser Registerkarte können Sie die Ressourcen sortieren und durchsuchen.

Identifizierung von Geräten, die ein Software-Upgrade benötigen

Weitere Informationen finden Sie unter [Softwarekonformität](#).

Softwarekonformität

Softwarekonformität hilft bei der Identifizierung von Ressourcen in einem Netzwerk, die nicht mit der beabsichtigten Ziel-Softwareversion konform sind. Die Validierung basiert auf Richtlinien und Regeln, anhand derer die Software-Konformität definiert wird. Diese Richtlinien können geplant oder nach Bedarf ausgeführt werden. Bei erfolgreicher Umsetzung der Konformitätspolitik erhält man das Konformitätsergebnis, das den Status der geltenden Vermögenswerte angibt. Der Konformitätsbereich hängt von verschiedenen Kriterien ab, z. B. Geräterolle, Verwaltung der Controller-Instanz usw.

Voraussetzungen

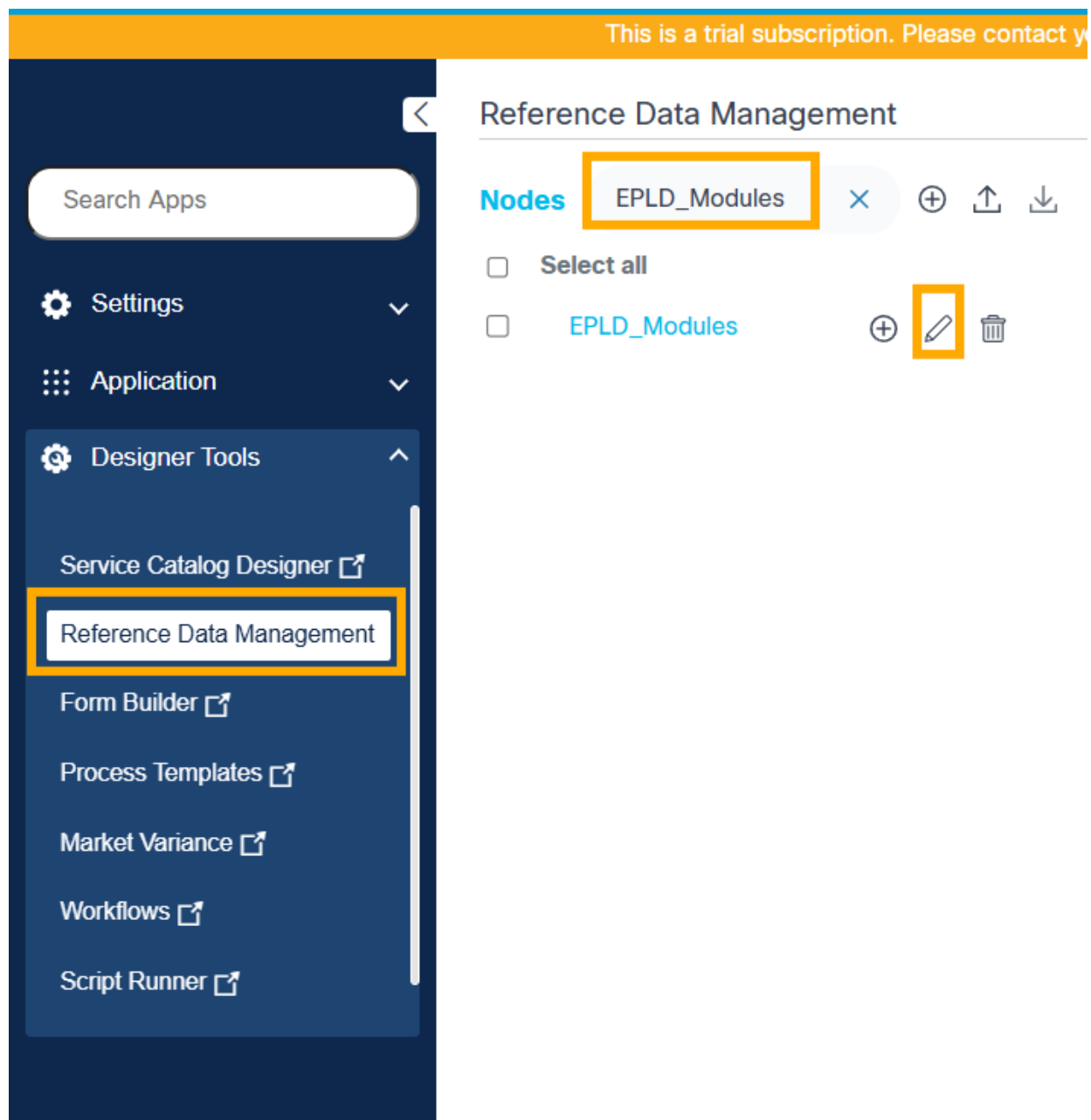
- Software-Images von Controllern wie Cisco Catalyst Center, vManage, NDFC und FMC müssen synchronisiert sein. Weitere Informationen finden Sie unter [Synchronisieren von Software-Images-Metadaten](#).
- Notwendige Software-Image-Metadaten für Controller wie NSO, CNC, Direct-to-Device und ANSIBLE müssen hinzugefügt werden. Weitere Informationen finden Sie unter [Hinzufügen von Software-Image-Metadaten](#).
- Benutzer benötigen Zugriff auf die RefD-Anwendung, um EPLD-Moduldaten zu verwalten.
- Informationen zum EPLD-Modul für erforderliche Releases sollten in der RefD-Anwendung vorab ausgefüllt werden.
- Benutzer müssen die EPLD-Modulinformationen in der RefD-Anwendung manuell hinzufügen, wenn sie nicht im OOB verfügbar sind.

Erstellen von EPLD-Moduldaten in einer Referenzdatenverwaltungsanwendung

Erstellen Sie vor dem Erstellen einer Konformitätsrichtlinie Referenzdaten für das EPLD-Modul in der RefD-Anwendung. Die RefD-Anwendung enthält EPLD-Modulinformationen für die Nexus Softwareversionen v10.2(8) bzw. v10.4(5). Bei anderen Geräteversionen müssen die EPLD-

Modellinformationen in der RefD-Anwendung manuell hinzugefügt werden.

Gehen Sie wie folgt vor, um weitere Releases zu den Metadaten des EPLD-Moduls hinzuzufügen:



Referenzdaten-Management

1. Navigieren Sie zur Anwendung Referenzdatenverwaltung und suchen Sie nach "EPLD_Modules".
2. Wählen Sie die Datei "EPLD_Modules" und wählen Sie das Symbol Bearbeiten.

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 x Cancel Save Upload Download

Knoten bearbeiten

3. Fügen Sie die Metadaten des EPLD-Moduls der neuen Version hinzu, indem Sie einen neuen Eintrag mit der folgenden Struktur anhängen:

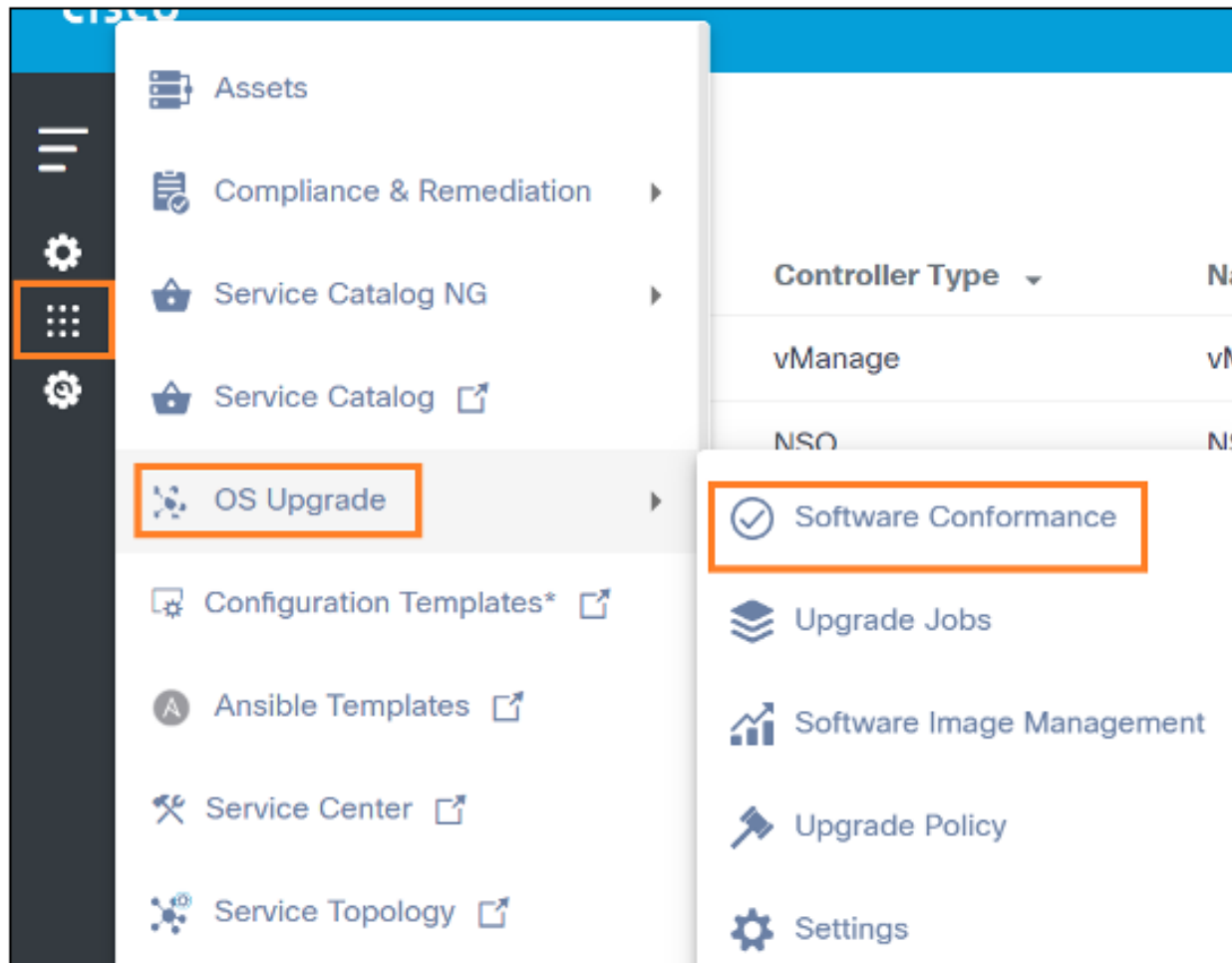
structure:

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

4. Klicken Sie auf Speichern, und validieren Sie die neuen Metadaten des EPLD-Moduls, die in der Konformitätsrichtlinie ausgewählt werden können. Die EPLD-Daten für die unterstützten Versionen werden vorab ausgefüllt.

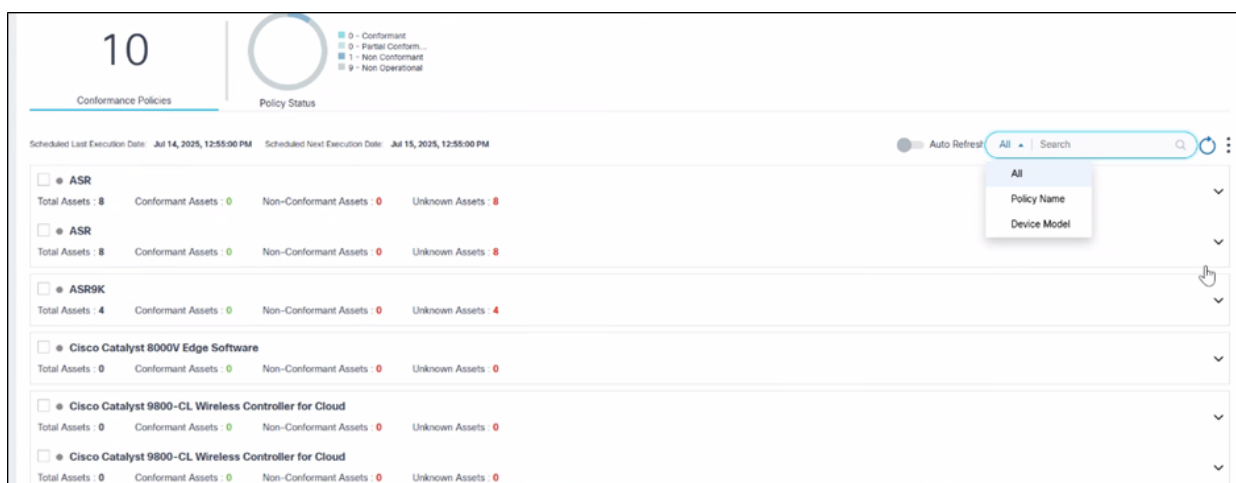
Anzeigen und Verwalten der Softwarekonformität

1. Melden Sie sich bei BPA mit Anmeldeinformationen an, die Zugriff auf die Softwarekonformität haben.



Navigation zur Softwarekonformität

2. Wählen Sie Betriebssystem-Upgrade > Softwarekonformität aus. Die Seite Softwarekonformität wird angezeigt.



Softwarekonformität

Die Seite Softwarekonformität enthält Folgendes:

- Ein oben angezeigter Abschnitt zu Analysen bietet folgende Informationen:

- Die Gesamtzahl der im System vorhandenen Konformitätsrichtlinien
- Ein Schnellfilter für den Richtlinienstatus, der anhand der folgenden Kriterien filtert:
 - Konformität: Alle von BPA verwalteten Geräte mit einem bestimmten Modell befinden sich in der definierten Softwareversion.
 - Teilkonform: Einige von BPA verwaltete Geräte mit einem bestimmten Modell befinden sich in der definierten Softwareversion. die übrigen Geräte sind in unterschiedlichen Softwareversionen
 - Nicht konform: Alle von BPA verwalteten Geräte mit einem bestimmten Modell verwenden im Vergleich zu einer bestimmten Softwareversion unterschiedliche Softwareversionen.
 - Nicht betriebsbereit: Auf Grundlage des in der Richtlinie angegebenen Gerätemodells wurden keine anwendbaren Geräte gefunden.
- Geplantes letztes Ausführungsdatum und Geplantes nächstes Ausführungsdatum, das Datum und Uhrzeit der zuvor durchgeführten geplanten Konformitätsprüfungen angibt und wann die nächste geplante Konformitätsprüfung für alle Richtlinien gilt
- Ein Suchfeld, das zum Filtern von Richtlinien basierend auf dem Gerätemodell, dem Richtliniennamen oder allen verwendet wird. Benutzer können Alle auswählen, um alle Parameter zu durchsuchen.
- Ein Umschalter für automatische Aktualisierung ermöglicht die automatische Aktualisierung der In-Progress-Konformitätsrichtlinie in benutzerdefinierten Intervallen, wenn diese Option aktiviert ist. So aktivieren Sie den Umschalter:
 - Wechseln Sie zu Betriebssystem-Upgrade > Einstellungen, um das Aktualisierungsintervall zu ändern.
 - Ändern des Intervalls für die automatische Aktualisierung mit einem gewünschten Wert
 - Klicken Sie auf Save (Speichern).
- Das Dashboard der Softwarekonformitätsrichtlinie wird im neuen Intervall aktualisiert, wenn der Umschalter für die automatische Aktualisierung aktiviert ist.
- Ein Symbol Aktualisieren, um die Seite zu aktualisieren und die ausgewählten Filter zu löschen
- Ein Symbol More Options (Weitere Optionen) mit den folgenden Optionen:
 - Erstellen einer Richtlinie
 - Alle Richtlinien ausführen
 - Mehrere ausgewählte Richtlinien löschen

Die Richtlinien werden basierend auf den Gerätemodellen gruppiert und als erweiterbare Symbolleisten angezeigt, um eine zentrale Ansicht der von verschiedenen Controllern verwalteten Gerätemodelle zu ermöglichen.



Zusammengefasste Ansicht der Konformitätsrichtlinie

In der zusammengefassten Ansicht werden das Gerätemodell und schnelle Statistiken angezeigt, z. B. Gesamterträge (Total Assets), konforme Bestände (Conformant Assets), nicht konforme Bestände (Non-Conformant Assets) und Unbekannte Bestände (Unknown Assets).

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

Erweiterte Ansicht der Konformitätspolitik

In der erweiterten Ansicht werden alle Richtlinien im Zusammenhang mit dem Gerätemodell angezeigt. Für jede Richtlinie können zusätzliche Aktionen, z. B. Ausführen, Richtlinie bearbeiten, Ergebnisse anzeigen usw., ausgeführt werden, indem das Symbol Weitere Optionen in der Spalte Aktion ausgewählt wird.

Erstellen von Software-Konformitätsrichtlinien

- Melden Sie sich mit Anmeldeinformationen, die den Zugriff auf die Softwarekonformität verwalten, beim BPA an.
- Wählen Sie Betriebssystem-Upgrade > Softwarekonformität aus. Die Seite Softwarekonformität wird angezeigt.

10

0 - Conformant

0 - Partial Conform...

1 - Non Conformant

9 - Non Operational

Policy Status

Conformance Policies

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	Create Policy Delete Run All
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	

Policy erstellen

- Wählen Sie das Symbol Weitere Optionen > Richtlinie erstellen aus.

Richtlinienformular erstellen

- Geben Sie Informationen in die Felder Policy Name (Richtlinienname), Device Model(s), Target Version (Zielversion), SMU's (SMUs), EPLD, Device Role (Geräterolle), Asset Groups (Ressourcengruppen) und Additional Conformance Check Template (Zusätzliche Konformitätsüberprüfungsvorlage) ein. SMU(s), Anlagengruppe(n) und Vorlage für zusätzliche Konformitätsprüfung sind optionale Felder.

Anmerkung: Benutzer können jetzt mehr als ein Gerätemodell im Formular "Create Conformance Policy" (Konformitätsrichtlinie erstellen) auswählen.

Anmerkung: Das Softwarekonformitäts-Framework kann Konformitätsprüfungen der Betriebssystem-Basisversion und SMU-Patches für die Geräte eines bestimmten Modells, einer bestimmten Rolle oder einer Controller-Instanz ausführen, die das Gerät verwaltet. Wenn zusätzliche benutzerdefinierte Prüfungen erforderlich sind, kann eine Prozessvorlage mit den erforderlichen Befehlen und Validierungsregeln erstellt werden, die dem Feld Zusätzliche Konformitätsüberprüfungsvorlage zugeordnet werden können.

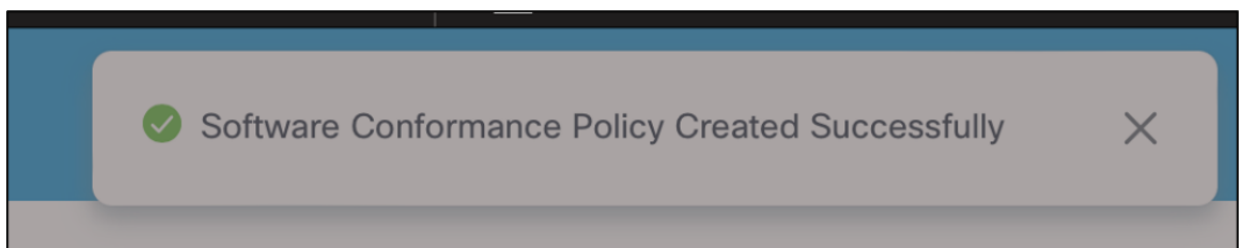
- Klicken Sie auf Erstellen. Es wird eine Bestätigung angezeigt.

Anmerkung: Die folgende Liste ist zu beachten.

- Anwendungsfall-Administratoren können flexibel mehrere Richtlinien mit unterschiedlichen Geräterollen für ein ausgewähltes Gerätemodell erstellen. In einer Richtlinie können mehrere Rollen ausgewählt werden.
- Wenn Any (Beliebig) aus der Dropdown-Liste Device Role(s) (Geräterolle(n)) ausgewählt ist, werden alle anderen Geräterollen (z. B. Access, Core usw.) deaktiviert. Wenn eine andere Geräterolle ausgewählt ist, ist Any (Beliebig) deaktiviert.
- Für Geräte, die von Controllern wie CNC, NSO, ANSIBLE oder Direct-to-Device verwaltet werden, kann die Compliance-Prüfung mit der Rolle "Any" (Beliebig) durchgeführt werden

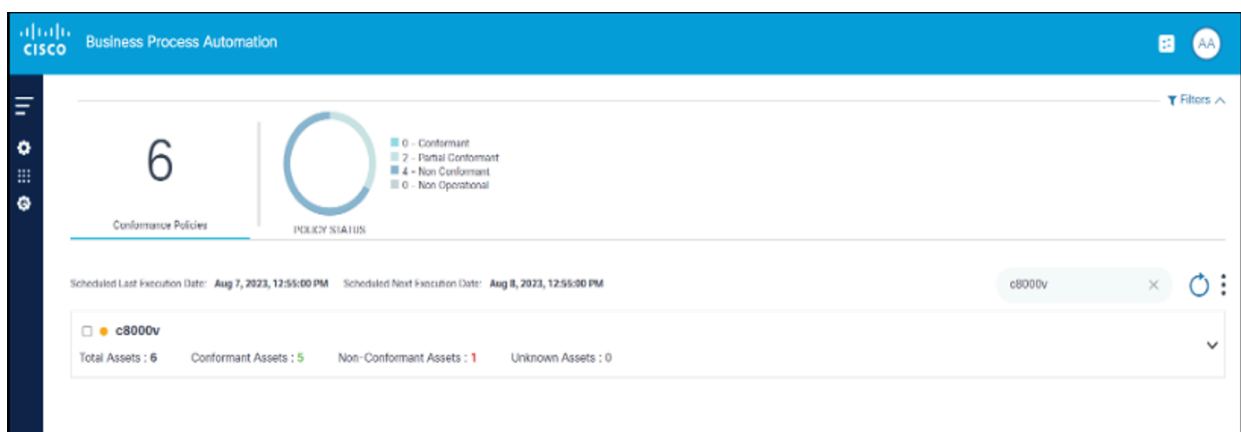
(ausgewählt aus der Dropdown-Liste "Device Role(s)" (Geräterolle(n)), da die Geräte keine Rolleninformationen haben.

- Wenn Any (Beliebig) aus der Dropdown-Liste Device Role(s) für FMC ausgewählt ist, wird die Softwarekonformität auf allen Geräten ausgeführt, einschließlich eigenständiger Geräte, Steuerungs- und Datengeräte.
- SMU(s)-Konformität und Upgrades werden nur für CNC-, NSO-, ANSIBLE-, FMC-, Direct-to-Device- und NDFC-Controller unterstützt.
- In dieser Version werden nur globale aus der Dropdown-Liste "Region" unterstützt.
- Benutzer können Asset Group(s) aus der Dropdown-Liste auswählen. Alle sind standardmäßig ausgewählt. Benutzer können eine oder mehrere Asset-Gruppen auswählen. Wenn eine bestimmte Asset-Gruppe ausgewählt ist, wird die Richtlinie nur für die Geräte der ausgewählten Asset-Gruppe ausgeführt.
- Wenn die erwarteten Werte für die Felder Gerätemodell, Zielversion und SMU(s) nicht angezeigt werden, klicken Sie auf Bilder erkennen, und versuchen Sie es erneut.
- Die Felder Gerätemodell, Ressourcengruppe(n) und Rolle bilden zusammen eine eindeutige Richtlinie. doppelte Richtlinien sind nicht zulässig.
- Das EPLD-Feld füllt Werte nur dann aus, wenn EPLD-Bildmetadaten für ausgewählte Gerätemodelle und Zielversionen verfügbar sind.
- Der Richtlinienname ist eindeutig, und doppelte Richtliniennamen sind nicht zulässig.



Bestätigung der Erstellung der Konformitätsrichtlinie

- Prozessvorlagen, die mit OS Upgrade Next Generation (Next-Gen) gekennzeichnet sind, werden im Feld Additional Conformance Check Template (Vorlage für zusätzliche Konformitätsprüfung) angezeigt.



Suchergebnis der Konformitätsrichtlinie

- Suchen Sie die erstellte Richtlinie, indem Sie das Gerätemodell in das Feld Suchen eingeben.

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 'N9K-C93180YC-FX' policy is selected, showing details such as 'Total Assets: 2', 'Conformant Assets: 0', 'Non-Conformant Assets: 2', and 'Unknown Assets: 0'. On the right, a detailed view of the 'Multi-Model-Policy-Demo' policy is shown, including fields for 'Policy Name', 'Region', 'Target Version', 'Device Model(s)', 'Device Role(s)', 'Controller Id(s)', and 'Additional Conformance Check Template'. The 'Device Model(s)' field is highlighted with a red box.

Konformitätsrichtlinie anzeigen

- Klicken Sie auf Policy (Richtlinie), um die Detailansicht der Richtlinie anzuzeigen.

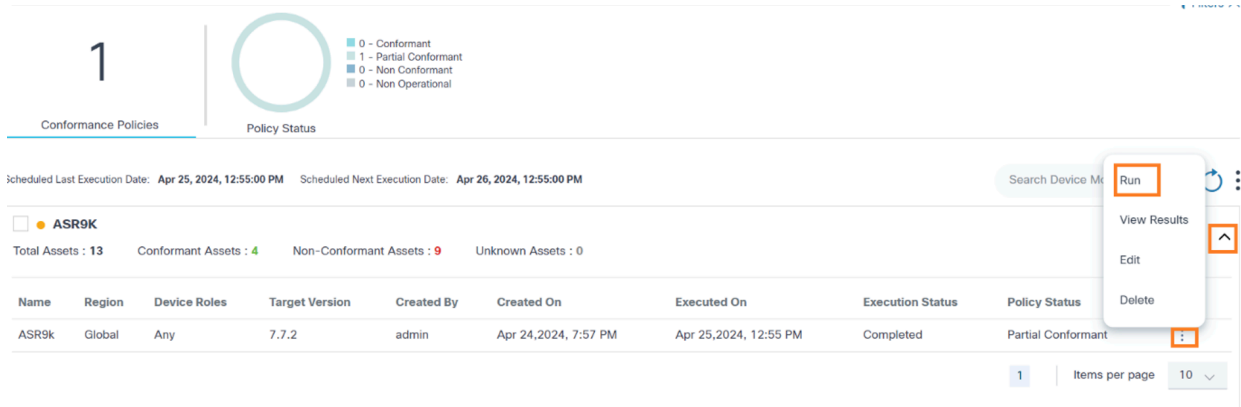
Durchführung von Software-Konformitätsprüfungen bei Bedarf

- Melden Sie sich bei BPA mit Anmeldeinformationen an, die über Ausführungszugriff verfügen.
- Wählen Sie Betriebssystem-Upgrade > Softwarekonformität aus. Die Seite Softwarekonformität wird angezeigt.

The screenshot displays the Cisco Business Process Automation interface, specifically the 'Software Compliance' page. The page shows a summary of compliance status with a large number '9' and a circular progress indicator. Below this, a table lists policies, including 'N9K-C93360YC-FX2' and 'N9K-C9336C-FX2'. The 'N9K-C93360YC-FX2' policy is highlighted, showing details such as 'Total Assets: 2', 'Conformant Assets: 0', 'Non-Conformant Assets: 2', and 'Unknown Assets: 0'. A search bar at the top right contains the text 'N9K'.

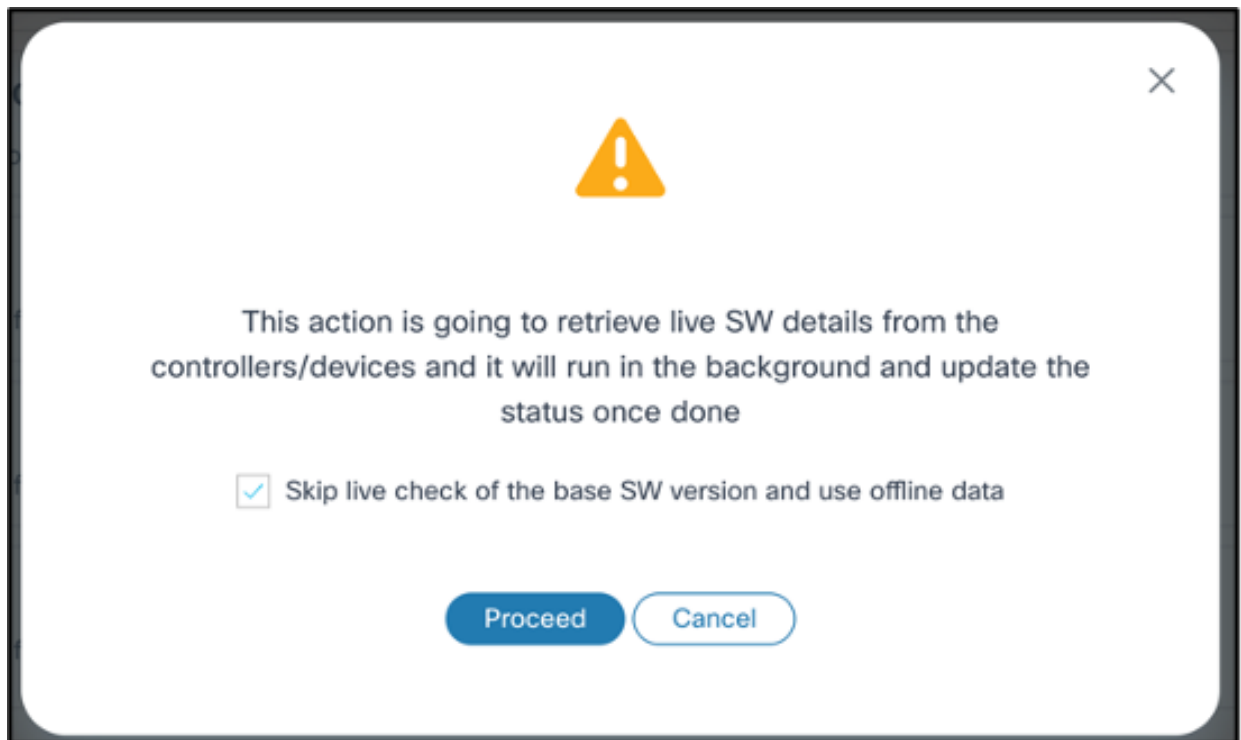
Richtliniensuche

- Suchen Sie im Feld Suchen nach der Richtlinie, die bei Bedarf ausgeführt werden soll.



Ausgeführt

- Wählen Sie in der Spalte "Aktion" der Richtlinie die Option Weitere Optionen > Ausführen aus. Es wird eine Bestätigung angezeigt, ob eine Live-Bestandsüberprüfung für die Geräte durchgeführt werden soll.



Bestätigung der Ausführung der Konformitätsrichtlinie

- Wenn eine Live-Bestandssynchronisierung erforderlich ist, bevor Konformitätsprüfungen ausgeführt werden, deaktivieren Sie das Kontrollkästchen Live Check der SW-Basisversion überspringen und Offlinedaten verwenden, und klicken Sie auf Weiter. In diesem Fall wird die Konformitätsprüfung erst nach der Synchronisierung durchgeführt. Oben rechts wird eine Benachrichtigung angezeigt.



Software Conformance policy execution initiated



Ausführungsbenachrichtigung zur Konformitätsrichtlinie



Anmerkung: Die folgende Liste ist zu beachten.

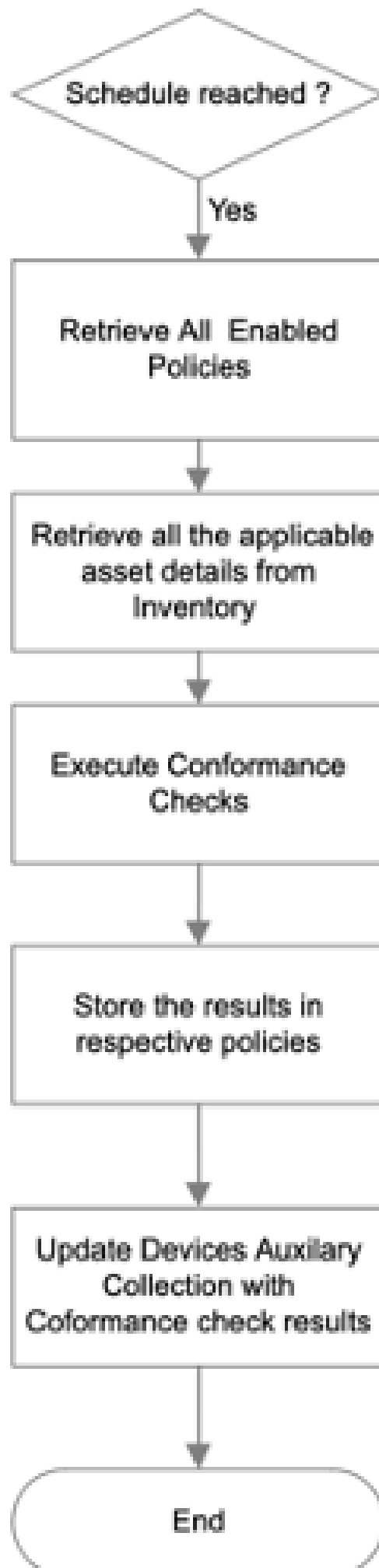
- Eine Konformitätsprüfung wird standardmäßig anhand der Bestandsdaten durchgeführt.
- Schlägt bei diesem Vorgang die Bestands- oder Gerätesynchronisierung fehl, wird das entsprechende Richtliniengerät als Unbekannt markiert, und die SMU-Prüfung wird übersprungen.
- Bei SMUs werden Echtzeitdaten vom Gerät abgerufen, bevor Konformitätsprüfungen durchgeführt werden, ob das Kontrollkästchen Live Check der SW-Basisversion überspringen und Offlinedaten verwenden aktiviert ist.
- Wenn eine Richtlinie mehrere Gerätemodelle umfasst, wird durch das Ausführen dieser Richtlinie für ein Gerätemodell die Ausführung aller zugeordneten Richtlinien initiiert.

Planen der Durchführung von Software-Konformitätsprüfungen

Softwarekonformitätsprüfungen können automatisch in regelmäßigen Abständen über den Scheduler-Service durchgeführt werden. Zeitgesteuerte Konformitätsprüfungen können wie folgt konfiguriert werden:

- Täglich
- Zweimal am Tag
- Wöchentlich
- Einmal

Sobald der Zeitplan erreicht ist, werden alle Richtlinien mit dem Status "Aktiviert" automatisch ausgeführt, und die Konformitätsergebnisse werden in den entsprechenden Richtlinien gespeichert.

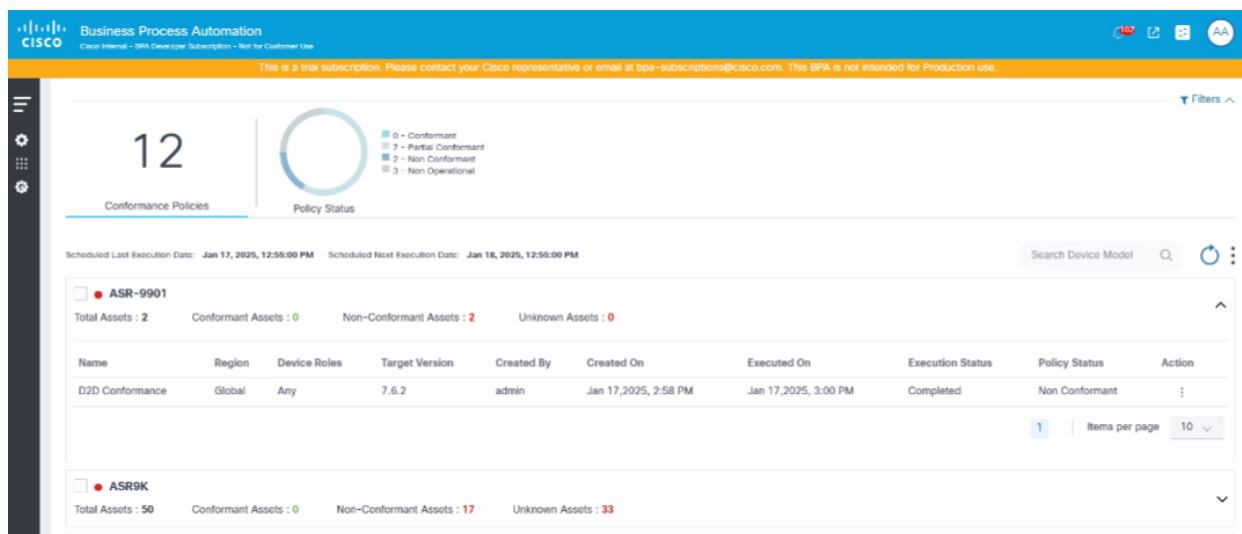


Geplante Ausführung von Softwarekonformitätsprüfungen - Anrufablauf

Weitere Informationen finden Sie unter [Softwarekonformität](#).

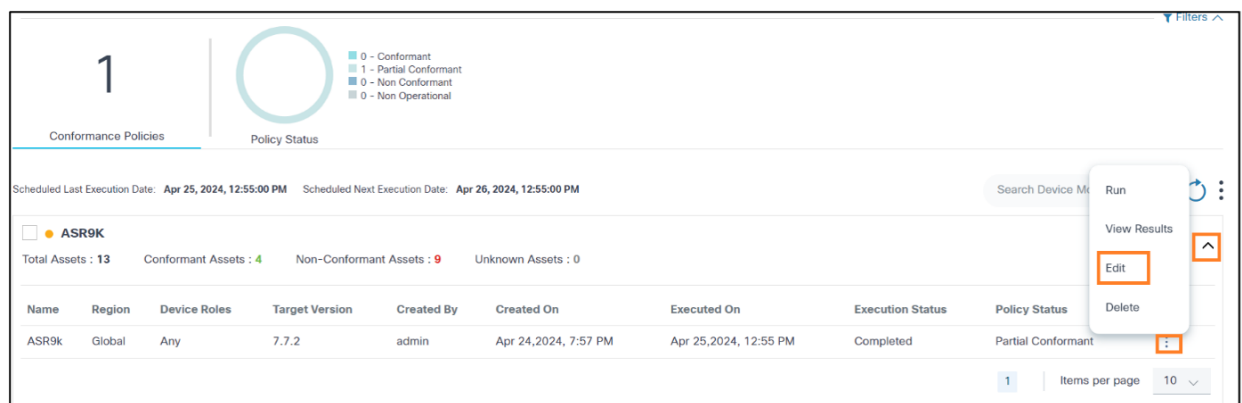
Aktualisieren von Software-Konformitätsrichtlinien

1. Melden Sie sich mit Anmeldeinformationen, die über Managementzugriff für Softwarekonformität verfügen, beim BPA an.
2. Wählen Sie Betriebssystem-Upgrade > Softwarekonformität aus. Die Seite Softwarekonformität wird angezeigt.



Softwarekonformität

3. Verwenden Sie das Feld Suchen, um die gewünschte Richtlinie zu finden.



Bearbeiten

4. Wählen Sie in der Spalte "Aktion" der Richtlinie das Symbol Weitere Optionen > Bearbeiten aus.

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

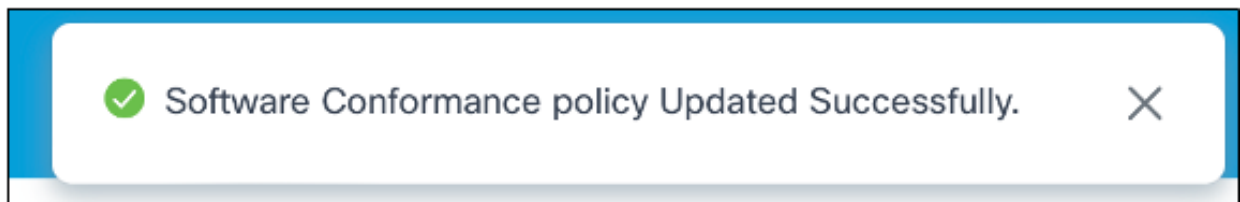
Policy Name*	Device Model*	Target Version*	SMU(s)
Multi-Model-Policy-Demo	N9K-C93180YC-FX, N9K-C93360YC-FX2 ✓	10.2.5 ✓	Select option(s) ✓
Region*	Device Role(s)*	Controller ID(s)	Additional Conformance Check Template
Global ✓	Any ✓	NDFC-OS ✓	Select option ✓

State
☒ Enable

Cancel Save

Konformitätsrichtlinie mit ausgefüllten Details bearbeiten

- Bearbeiten Sie die Felder Zielversion, SMUs, Geräte Rollen, Controller-ID(s), Richtlinienstatus und zusätzliche Vorlage für die Konformitätsprüfung nach Bedarf.
- Klicken Sie auf Speichern. Es wird eine Bestätigung angezeigt.

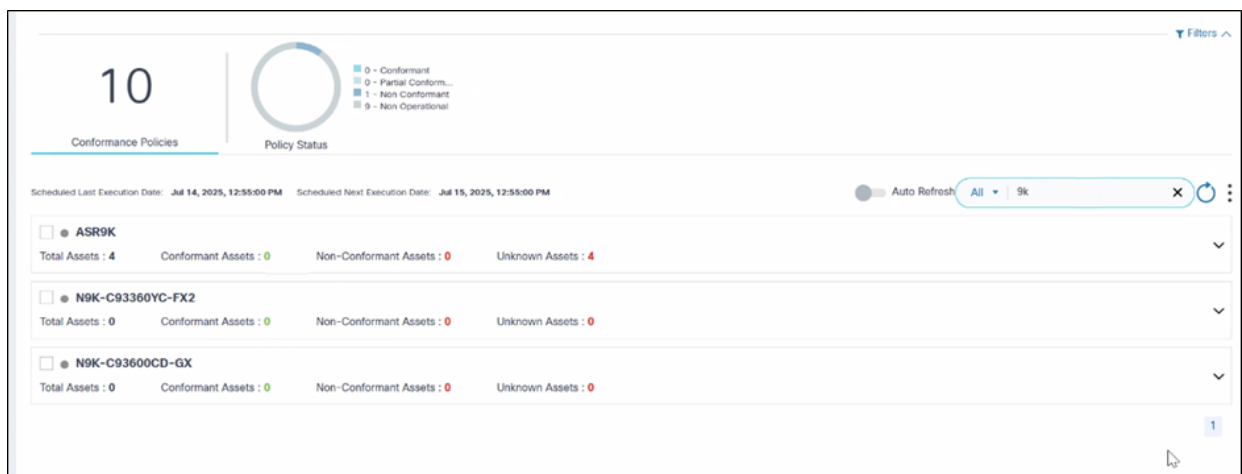


Bestätigung der erfolgreichen Aktualisierung

 Anmerkung: Wenn die Softwarekonformitätsrichtlinie für einen laufenden Upgrade-Auftrag verwendet wird, kann die Richtlinie nicht bearbeitet werden.

Software-Konformitätsrichtlinien werden gelöscht

- Melden Sie sich bei BPA mit Anmeldeinformationen an, die über Managementzugriff verfügen.
- Wählen Sie Betriebssystem-Upgrade > Softwarekonformität aus. Die Seite Softwarekonformität wird angezeigt.



Suchergebnis der Konformitätsrichtlinie

3. Verwenden Sie das Feld Suchen, um die gewünschte Richtlinie zu finden.

The screenshot shows the 'Conformance Policies' interface. At the top, there's a summary section with a large number '3' and a 'Policy Status' donut chart. Below this, a table lists policies. The first policy is 'PDF-Font-Testing-Policy' with a status of 'Non Conformant'. A dropdown menu is open next to it, showing options: 'Run', 'View Results', 'Edit', and 'Delete'. The table has columns: Name, Region, Device Roles, Target Version, Created By, Created On, Executed On, Execution Status, and Policy Status.

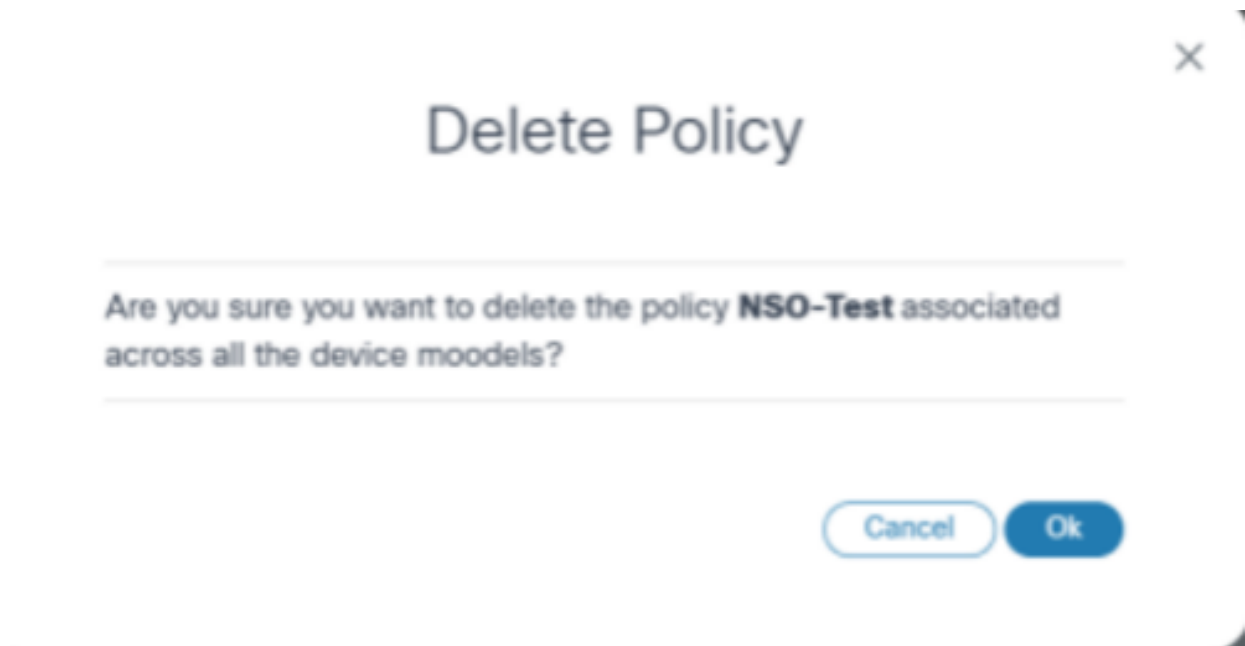
Name	Region	Device Roles	Target Version	Created By	Created On	Executed On	Execution Status	Policy Status
PDF-Font-Testing-Policy	Global	Any	7.8.2	admin	Jul 7, 2025, 5:51 PM	Jul 14, 2025, 4:03 PM	Completed	Non Conformant

Löschen

4. Wählen Sie in der Spalte "Aktion" der Richtlinie das Symbol Weitere Optionen > Löschen aus. Ein Bestätigungsfenster wird geöffnet.

The screenshot shows a 'Delete Policy' confirmation dialog box. The title is 'Delete Policy'. The main text asks: 'Are you sure you want to delete the policy **N9K-C9336C-FX2** under **N9K-C9336C-FX2** ?'. At the bottom, there are two buttons: 'Cancel' and 'Ok'.

Löschen der Richtlinie bestätigen



Bestätigung der Löschrichtlinie (wenn die Richtlinie mehreren Modellen zugeordnet ist)

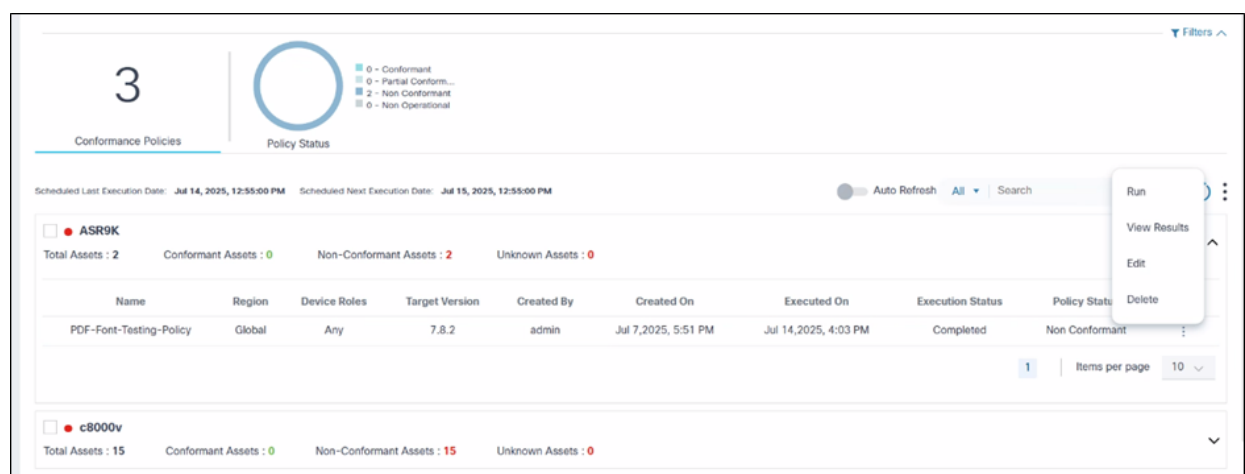
5. Klicken Sie auf OK. Die Richtlinie wird gelöscht.

 Anmerkung: Die folgende Liste ist zu beachten.

- Wenn eine Richtlinie mit mehreren Gerätemodellen verknüpft ist, werden beim Löschen einer Richtlinie alle zugehörigen Richtlinien für jedes verknüpfte Modell entfernt.
- Wenn die Softwarekonformitätsrichtlinie für einen laufenden Upgrade-Auftrag verwendet wird, kann die Richtlinie nicht gelöscht werden.

Konformitätsergebnisse anzeigen und herunterladen

Sobald eine Richtlinie ausgeführt wird:



3 Conformance Policies

Policy Status

- 0 - Conformant
- 0 - Partial Conform...
- 2 - Non Conformant
- 0 - Non Operational

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

☐ **ASR9K**

Total Assets : 2 Conformant Assets : 0 Non-Conformant Assets : 2 Unknown Assets : 0

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

1 Items per page 10

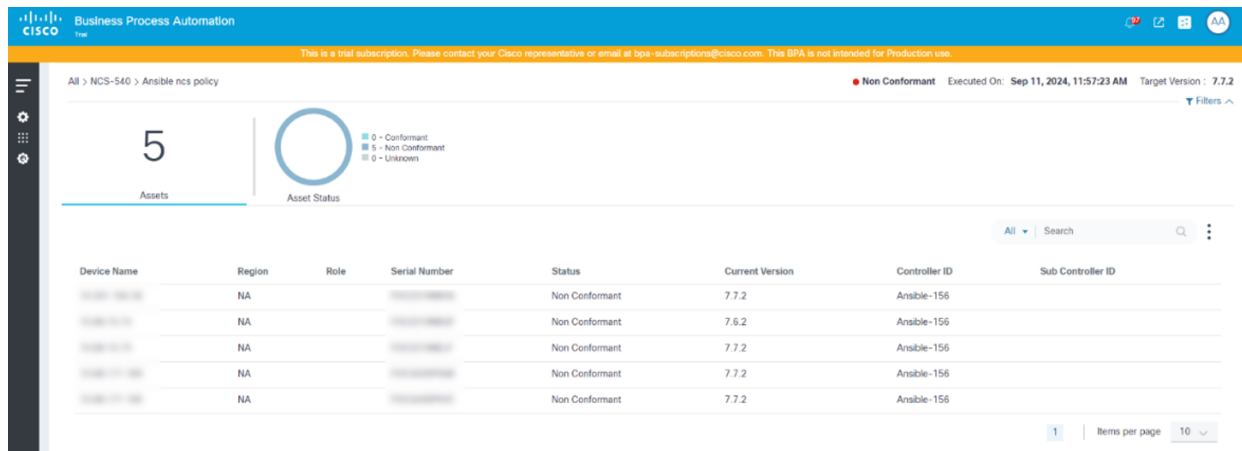
☐ **c8000v**

Total Assets : 15 Conformant Assets : 0 Non-Conformant Assets : 15 Unknown Assets : 0

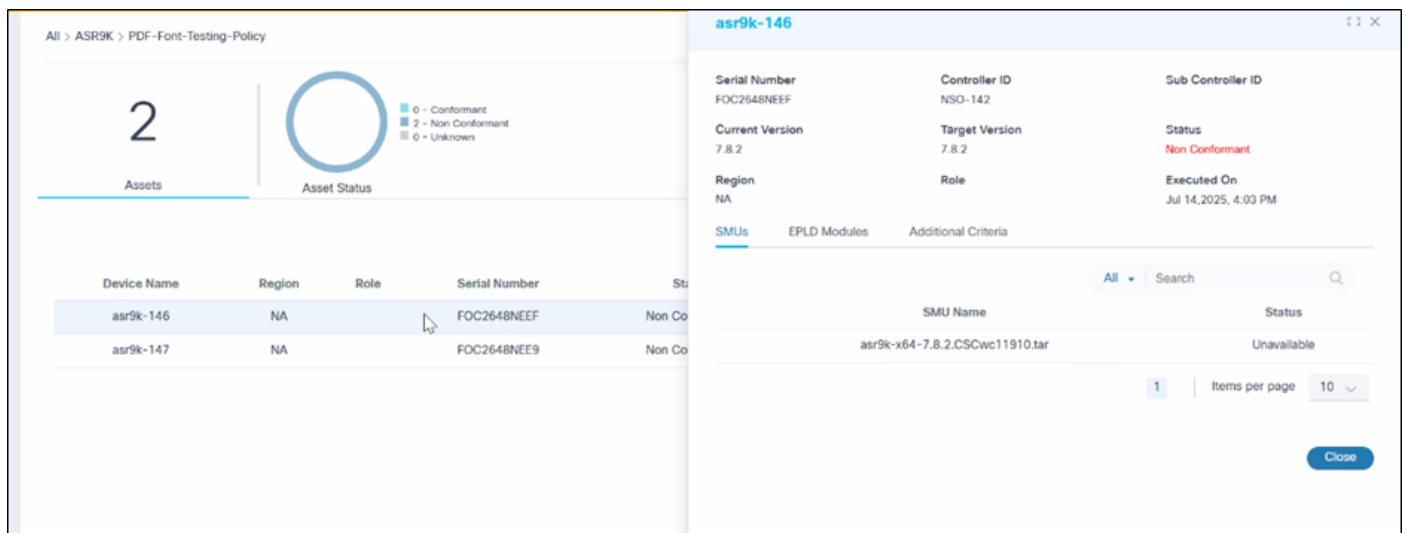
Run View Results Edit Delete

Ergebnisoption anzeigen

1. Wählen Sie auf der Seite Softwarekonformität das Symbol Weitere Optionen > Ergebnisse anzeigen aus. Die Seite Ergebnisse wird angezeigt, auf der Benutzer den Konformitätsstatus der Geräte anzeigen können.



Ergebnisse anzeigen



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]

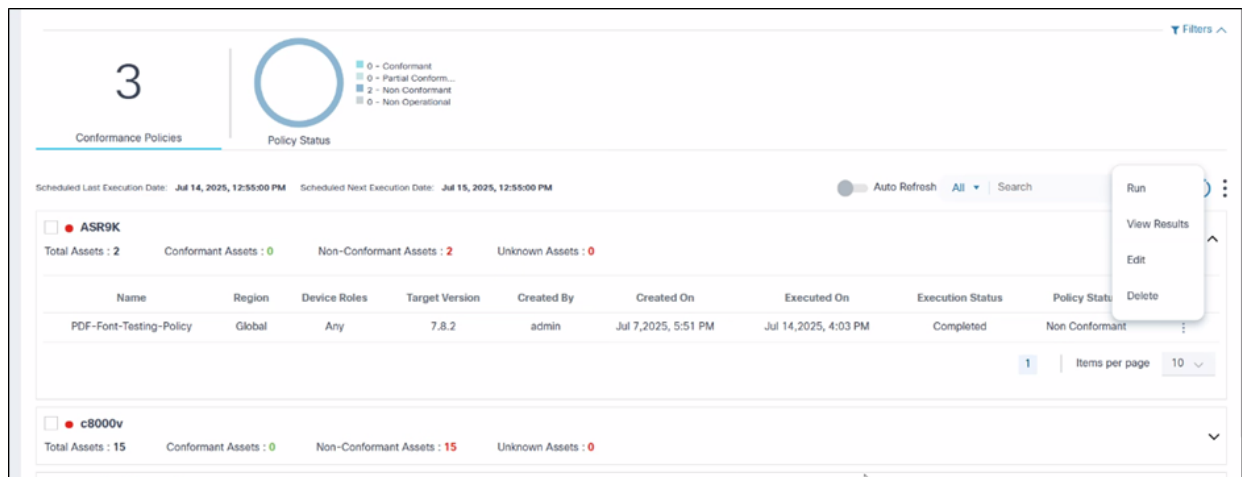
Boot Partition: xr_lcp_lv32

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. Wählen Sie eine Zeile aus, um bestimmte Anlagendetails zusammen mit dem SMU-Status und zusätzlichen Kriterien anzuzeigen.

 Anmerkung: Die SMU-Details werden nur für NSO-, CNC-, ANSIBLE-, Direct-to-Device- und NDFC-Controller-Ressourcen angezeigt. EPLD-Module werden nur für NDFC-Controller angezeigt.



Ergebnisse anzeigen

- Wählen Sie in der Spalte "Aktion" des Geräts das Symbol Weitere Optionen > Ergebnisse anzeigen aus.

Assets

Asset Status

4 - Conformant | 9 - Non Conformant | 0 - Unknown

All | Search

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

Download

Herunterladen

- Klicken Sie auf das Symbol More Options (Weitere Optionen) > Download (Herunterladen), um die Ergebnisse im CSV-Format mit dem SMU-Verfügbarkeitsstatus herunterzuladen.

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	Complianc	Complianc	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-Tabellenansicht

Anmerkung: "Ergebnisse anzeigen" zeigt nur die Ergebnisse der zuletzt durchgeführten Konformitätsprüfung an. Benutzer können nur die Ressourcen anzeigen, auf die sie Zugriff haben. Bei nicht betriebsbereiten Richtlinien ist Ergebnisanzeige deaktiviert.

Mögliche Gerätestatus:

- Konformität: Zeigt an, dass das Gerät der definierten Richtlinie entspricht.
- Nicht konform: zeigt an, dass das Gerät nicht konform ist, wenn folgende Bedingungen erfüllt sind:

Zielversion	SMU	Konformitätsprüfung	Status
Nicht konform	NA	NA	Nicht konform
Konformität	Nicht verfügbar	Regeln fehlgeschlagen	Nicht konform
Konformität	Verfügbar	Regeln fehlgeschlagen	Nicht konform
Konformität	Nicht verfügbar	Erfolgreiche Regeln	Nicht konform

- Unbekannt: Zeigt an, dass die Konformitätsprüfung der Gerätesoftware nicht durchgeführt werden konnte, da das Gerät nicht über aktuelle Softwareversionsinformationen verfügt.

Kriterien für den Status "Unbekannt":

Zielversion	SMU	EPLD	Konformitätsprüfung	Status
Nicht konform	NA	NA	NA	Nicht konform
Konformität	Nicht verfügbar	Nicht konform	Regeln fehlgeschlagen	Nicht konform
Konformität	Nicht verfügbar	Konformität	Regeln fehlgeschlagen	Nicht konform
Konformität	Verfügbar	Konformität	Regeln fehlgeschlagen	Nicht konform
Konformität	Verfügbar	Nicht konform	Regeln fehlgeschlagen	Nicht konform
Konformität	Nicht verfügbar	Konformität	Erfolgreiche Regeln	Nicht konform
Konformität	Nicht verfügbar	Konformität	Erfolgreiche Regeln	Nicht konform

Mögliche SMU-Status:

- Verfügbar: Zeigt an, dass SMU im Gerät vorhanden ist und sich im aktiven Zustand befindet.
- Nicht verfügbar: Zeigt an, dass SMU möglicherweise nicht vorhanden ist oder vorhanden ist, sich aber in einem inaktiven Zustand befindet.

Mögliche EPLD-Modulstatus:

- Konformität: Zeigt an, dass das EPLD-Modul im Gerät mit der erwarteten Zielversion vorhanden ist.
- Nicht konform: Zeigt an, dass das EPLD-Modul im Gerät vorhanden ist und eine unübertroffene erwartete Zielversion vorhanden ist.
- Fehlendes Modul: Zeigt an, dass die EPLD-Module auf dem Gerät nicht konfiguriert oder abonniert sind.

Mögliche Kompatibilitätsprüfungs-Vorlagenstatus:

- Erfolg: Zeigt an, dass das Gerät die Prozessvorlage mit gültigen Befehlen und Regeln erfolgreich ausgeführt hat.
- Fehlgeschlagen: Zeigt an, dass das Gerät die Prozessvorlage nicht ausführen konnte (z. B. wenn Befehle falsch sind).
- NA: Zeigt an, dass das Gerät nicht zur Ausführung der Prozessvorlage berechtigt ist (wenn das Gerät z. B. nicht mit der definierten Zielversion übereinstimmt).



Anmerkung: Die folgende Liste ist zu beachten.

- Die Überprüfung der Softwarekonformität funktioniert nur mit Geräten, die zum Standard-Tenant gehören.
- Die Überprüfung der Softwarekonformität stützt sich auf den Bestand an Ressourcen als Quelle der Wahrheit für die aktuellen Softwareversionen der Geräte. Wenn Inventardaten veraltet sind, sind die Ergebnisse der Softwarekonformitätsprüfungen veraltet. Um veraltete Daten zu vermeiden, verwenden Sie die Funktion zur Live-Bestandsüberprüfung, wenn Sie mit der Ausführung der Konformitätsrichtlinie beginnen.
- Der Standardzeitplan kann geändert werden unter Betriebssystem-Upgrade > Einstellungen > Softwarekonformität
- Nach dem Upgrade auf BPA 5.1 werden alle bereits vorhandenen Richtlinien in den deaktivierten Zustand versetzt. Die Benutzer müssen jede Richtlinie bearbeiten, die entsprechenden Werte auswählen, aktivieren und die Änderungen zur weiteren Verwendung speichern.

Upgrade-Richtlinie

Die Upgrade-Richtlinienkomponente unterstützt zwei Richtlinientypen:

- Richtlinie in einem Schritt:
 - Beliebig
 - <spezifische Quellversion (7.7.1)> - <spezifische Zielversion (7.7.2)>

- Mehrstufige Richtlinie:
 - v7.7.1 - 7.7.2
 - v7.7.2 - 7.7.8
- Ein mehrstufiges Upgrade kann Bridge-SMUs umfassen, wie im folgenden Beispiel gezeigt:
 - v7.7.1 - v7.7.1[Bridge-SMUs]
 - V7.7.1[Bridge-SMUs] - 7.7.8

Die Upgrade-Richtlinienkomponente bietet die Flexibilität, die folgenden plattformspezifischen Artefakte im Voraus zu definieren:

- Aktualisierungspfad
- Vorlagen oder Workflows vor und nach der Validierung
- Verteilungs-Workflow
- Aktivierungs-Workflow
- Backup-Workflow
- Timeoutwerte
- Rollback-Workflow
- Gültige Unterschiede vor und nach der Änderung
- Workflow für die Datenverkehrsumleitung oder für die Datenverkehrsumkehr

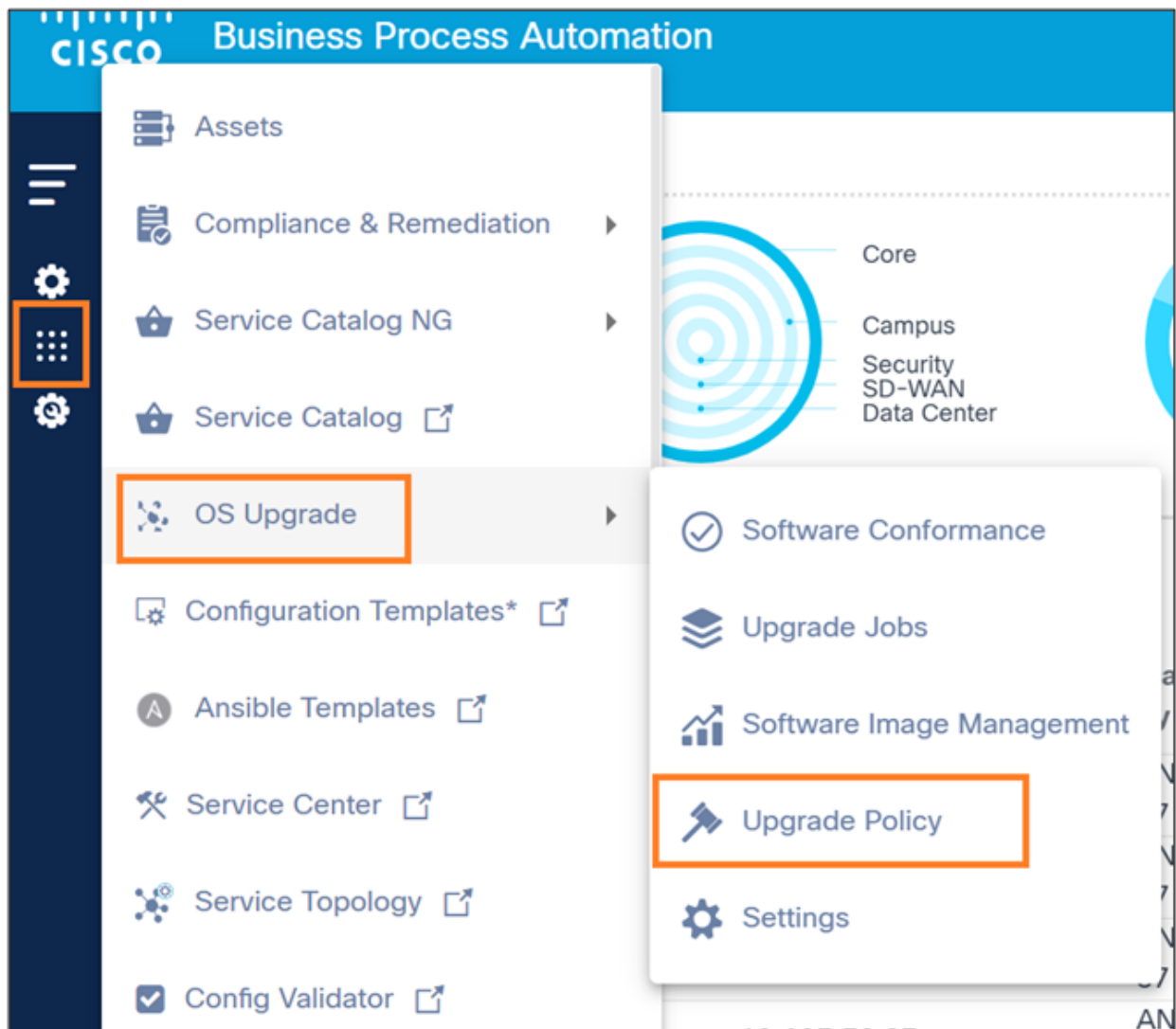
Voraussetzungen

- Erforderliche Prozessvorlagen oder Workflows vor und nach der Validierung
- Erforderliche Backup-, Distributions-, Aktivierungs- und Rollback-Workflows
- Erforderliche Bildmetadaten

Anzeigen und Verwalten von Aktualisierungsrichtlinien

So greifen Sie auf die Seite Upgrade Policy (Upgrade-Richtlinie) zu:

1. Melden Sie sich bei BPA mit Anmeldeinformationen an, die über ausreichenden Zugriff auf die Upgrade-Richtlinie verfügen.



Navigation zur Aktualisierungsrichtlinie

2. Wählen Sie Betriebssystem-Upgrade > Upgrade-Richtlinie aus. Die Seite "Upgrade Policy" wird angezeigt.

The screenshot shows the 'Upgrade Policy' page. At the top, there is a 'Policies' section with a large number '8' and a 'Controller Types' section with a donut chart. The donut chart is divided into segments representing different controller types: CNC, DNAC, Direct-To-Device, FMC, NDFC, vManage, Ansible, and NSO. Below these sections is a table with columns for Device Model, Controller Type, Name, Created By, Last Modified On, and Action. The table contains one row for the ASR-9901 device model.

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	

Upgrade-Richtlinie

Die Seite Upgrade Policy (Upgrade-Richtlinie) enthält Folgendes:

- Ein oben angezeigter Abschnitt zu Analysen bietet folgende Informationen:

- Die Gesamtzahl der Upgrade-Richtlinien im System
- Ein Schnellfilter für Controllertypen, mit dem nach Controller-Typ gefiltert werden kann.
- Ein Symbol für weitere Optionen mit der Option zum Erstellen von Richtlinien und Massenverarbeitungsaktionen wie Alle ausgewählten Richtlinien löschen
- Ein Suchfilter für Suchrichtlinien, die wie folgt gefiltert werden können:
 - Alle: In allen Feldern suchen
 - Gerätemodell: Suche nach Richtlinien mit einem angegebenen Modell
 - Name: Suche nach Richtlinien mit einem angegebenen Richtliniennamen
 - Erstellt von: Nach Richtlinien mit einem angegebenen Benutzer suchen
- Sortieren von Richtlinien durch Klicken auf die entsprechenden Spaltennamen oder Tabellenfelder

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 shows a summary with a large number '61' under 'Policies' and a donut chart under 'Controller Types' with a legend: 3 - NDFC, 25 - NSD, 5 - vltanage, 3 - CNC, 2 - Direct-To-Device, 4 - DNAC, 13 - Ansible, and 1 - FMC. Below this is a table of policies with columns for checkboxes, Device Model, Controller Type, and Name. The table lists several policies, including 'ASR-9901' and 'ASR9K'. On the right, a detailed view of the 'Ansible_TR_TD_workflow_check' policy is shown. It includes a description, max batch count, default policy, and a list of workflows under 'Backup Details' and 'Traffic Diversion'.

Richtliniendetail-Ansicht

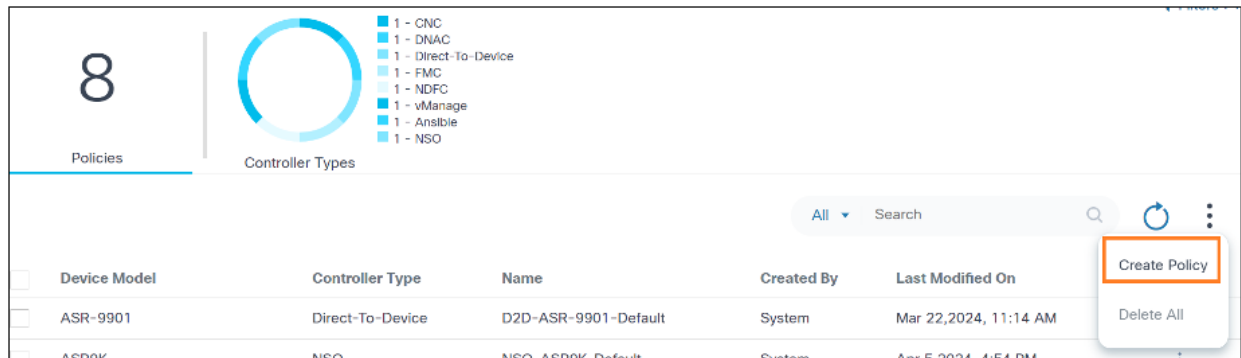
- Klicken auf eine bestimmte Richtlinie oder Zeilen in der Detailansicht einer Richtlinie



Anmerkung: Dieselben Gerätemodelle und Controller-Typen können beliebig viele Richtlinien haben, wenn die Richtlinienennamen eindeutig sind.

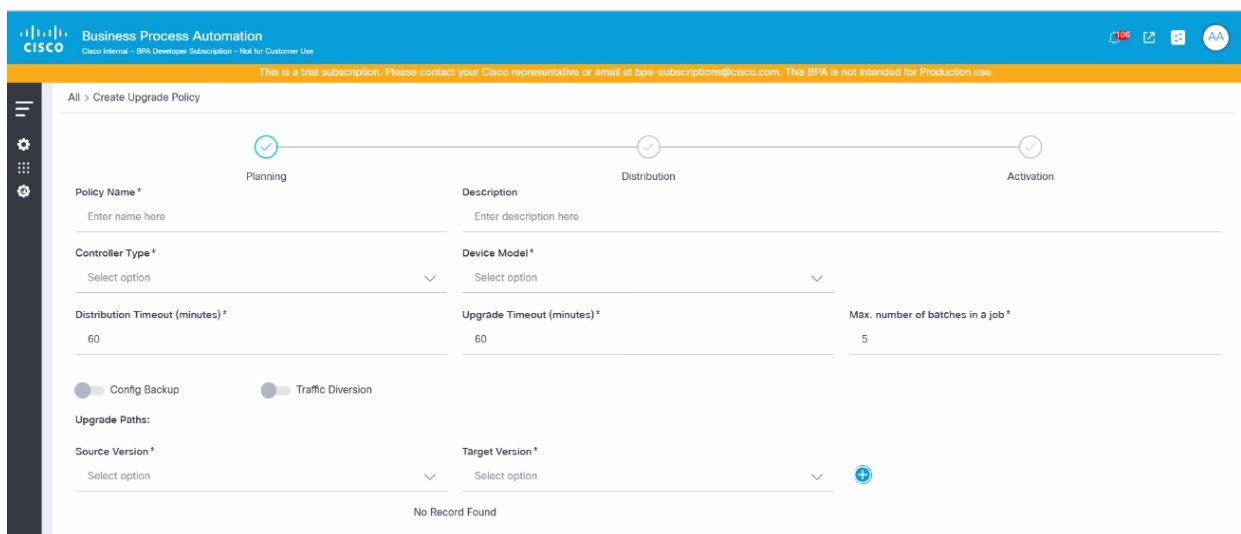
Erstellen von Aktualisierungsrichtlinien

1. Melden Sie sich bei BPA mit Anmeldeinformationen an, die über Managementzugriff für Upgrade-Richtlinien verfügen.
2. Wählen Sie Betriebssystem-Upgrade > Upgrade-Richtlinie aus. Die Seite "Upgrade Policy" wird angezeigt.



Policy erstellen

3. Wählen Sie Weitere Optionen > Richtlinie erstellen aus. Die Seite "Upgrade-Richtlinie erstellen" wird angezeigt.



Aktualisierungsrichtlinie erstellen

Planung

1. Konfigurieren Sie die Parameter für die allgemeine Richtlinie. Die folgende Tabelle enthält eine kurze Beschreibung der einzelnen Felder.

Feld	Beschreibung
Richtlinienname	Name der Richtlinie
Beschreibung	Kurze Beschreibung der Richtlinie
Controller-Typ	Geeigneter Controller, der zum Durchführen des Betriebssystem-Upgrades verwendet wird
Gerätemodell	Gerätemodell, das zum Durchführen des Betriebssystem-Upgrades verwendet wird
Verteilungs-Timeout (Minuten)	Maximale Wartezeit in Minuten für die Image-

Feld	Beschreibung
Upgrade-Timeout (Minuten)	Verteilungsaktivität Maximale Wartezeit in Minuten für die Image-Aktivierungsaktivität
Maximale Anzahl von Stapeln in einem Auftrag	Anzahl der Stapel, die einem Auftrag hinzugefügt werden können; Die maximal zulässige Anzahl von Stapeln ist 20. Aktivieren Sie diesen Umschalter, wenn ein Backup erforderlich ist, und füllen Sie die folgenden Felder im Fenster für vManage und Direct-to-Device-Controller aus: - Workflow-Name: Der entsprechende Backup-Workflow Anmerkung: Wenn die Workflows nicht gefunden werden können, stellen Sie sicher, dass die Workflows ordnungsgemäß mit dem Tag "Betriebssystem-Upgrade NextGen" gekennzeichnet sind. - Neuesten Workflow verwenden: Bei Auswahl dieser Option wird die neueste Version des ausgewählten Workflows verwendet.
Umschalter für Konfigurationssicherung	- Workflowversion: Die benutzerdefinierte Workflowversion. kann nur ausgewählt werden, wenn Letzten Workflow verwenden nicht ausgewählt ist. Bei NDFC-, NSO-, CNC- und Cisco Catalyst Center-Controllern erfolgt die Sicherung über den Backup- und Wiederherstellungsservice. Aus diesem Grund muss im Fenster Backup details (Backup-Details) eine Richtlinie für Backup und Wiederherstellung ausgewählt werden. Anmerkung: Benutzer müssen die entsprechende Richtlinie für den Controller-Typ auswählen. Im Abschnitt Sichern und Wiederherstellen finden Sie weitere Informationen zu Sicherungs- und Wiederherstellungsrichtlinien. Um das Backup für Nexus-Geräte zu aktivieren, muss die SCP-Server-Konfiguration auf den Zielgeräten

Feld

Beschreibung

vorhanden sein.

Aktivieren Sie diesen Umschalter, wenn eine Umleitung des Datenverkehrs erforderlich ist, und füllen Sie die folgenden Felder im Fenster Datenverkehrsumleitung aus:

- Workflow für die Datenverkehrsumleitung: Der entsprechende Workflow für die Datenverkehrsumleitung.

Anmerkung: Wenn die Workflows nicht gefunden werden können, stellen Sie sicher, dass die Workflows korrekt mit dem Tag "Betriebssystem-Upgrade NextGen" gekennzeichnet sind.

Umleitungs-Umschalter

- Workflow zur Datenverkehrsumkehr: Der entsprechende Workflow für die Datenverkehrsumkehr.

Anmerkung: Wenn die Workflows nicht gefunden werden können, stellen Sie sicher, dass die Workflows korrekt mit dem Tag "Betriebssystem-Upgrade NextGen" gekennzeichnet sind.

- Neuesten Workflow verwenden: Die neueste Version des oben ausgewählten Workflows

- Workflowversion: Die benutzerdefinierte Workflowversion. kann nur ausgewählt werden, wenn Letzten Workflow verwenden nicht ausgewählt ist.

Die Upgrade-Pfade definieren die entsprechenden Upgrade-Pfade für die einzelnen Schritte. Mehrere Quell- und Zielversionen können in den folgenden Feldern hinzugefügt werden, um unterschiedlichen Anforderungen gerecht zu werden

- Quellversion: Die Startversion des Upgrade-Pfads

Upgrade-Pfade

- Zielversion: Die Endversion des Upgrade-Pfads

- Quell-Version (Any) bis Ziel-Version (Any): Dies wird durch Auswahl von Any (Beliebig) für die Felder Source Version (Quellversion) und Target Version (Zielversion) verfügbar gemacht. Dies ist der Standardwert für alle Gerätemodelle. In diesem Szenario stellen die Seiten Distribution und Activation einen einheitlichen Prozess für das Upgrade bereit.

Feld

Beschreibung

- Quellversion (spezifische Version) in Zielversion (spezifische Version): Dies wird durch die Auswahl bestimmter Bildversionen für das Gerätemodell ermöglicht. mehrere Quell- und Zielversionen hinzugefügt werden können; Die Anzahl der Eingaben für den Verteilungs- und Aktivierungs-Upgrade-Prozess stimmt mit der Anzahl der hinzugefügten Quell- und Zielversionen überein. Jede dieser Versionen wird als reduzierbarer Abschnitt dargestellt, der mit den entsprechenden Quell- und Zielversionen gekennzeichnet ist. Für einen Upgrade-Pfad müssen SMUs auf die Quellversion angewendet werden, bevor ein Upgrade auf die Zielversion durchgeführt wird. Dazu müssen sie dem entsprechenden Upgrade-Pfad als Bridge-SMUs hinzugefügt werden. Weitere Informationen zu Bridge-SMUs finden Sie im nächsten Abschnitt.

Bridge-SMUs

Bridge-SMUs, die auch als obligatorische Upgrade- oder Downgrade-SMUs bezeichnet werden, sind eine Voraussetzung und müssen installiert werden, bevor ein Upgrade oder Downgrade auf eine andere Softwareversion derselben Plattform oder desselben Modells durchgeführt wird.

Hinzufügen von Bridge-SMUs in einem Upgrade-Pfad

Policy Name*
Enter name here

Description
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

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

1 | Delete Path | Add Bridge SMUs

Cancel Next

Upgrade-Pfadoptionen

1. Nachdem Sie einen Upgrade-Pfad hinzugefügt haben, wählen Sie das Symbol Weitere Optionen aus. Die Optionen Pfad löschen und Bridge-SMUs hinzufügen werden angezeigt.

Policy Name*
Enter name here

Description
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

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

Cancel Next

Bridge-SMUs hinzufügen

2. Wählen Sie Bridge-SMUs hinzufügen aus. Das Fenster Bridge-SMUs hinzufügen wird geöffnet. Alle verfügbaren Bridge-SMUs werden für den angegebenen Upgrade-Pfad angezeigt.

Add Bridge SMUs

Select option(s)

☒ asr9k-x64-7.6.2.CSCwf77420.tar

☐ asr9k-x64-7.6.2.CSCwc41614.tar

Bridge-SMUs hinzufügen

3. Aktivieren Sie im Fenster Bridge-SMUs hinzufügen das bzw. die entsprechenden Kontrollkästchen, um Bridge-SMUs hinzuzufügen, oder deaktivieren Sie die Kontrollkästchen, um sie zu entfernen. Nach dem Hinzufügen der Bridge-SMUs wird der Upgrade-Pfad mit den ausgewählten Bridge-SMU-Details aktualisiert.

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	⋮

Upgrade-Pfad mit Bridge-SMUs



Anmerkung: Jeder Upgrade-Pfad, der Bridge-SMU(s) enthält, gilt als Upgrade in zwei Schritten. Für den in der Abbildung oben gezeigten Upgrade-Pfad lautet der endgültige Upgrade-Pfad:

- 7.6.2 - 7.6.2 [Bridge-SMUs]

Dieser Pfad stellt die Aktualisierung des Geräts dar, das unter v7.6.2 ausgeführt wird, mit den Bridge-SMUs.

- 7.6.2 [Bridge-SMUs] - 7.7.2

Dieser Pfad stellt ein Upgrade des Geräts von v7.6.2 auf v7.7.2 dar. In diesem Fall ist die Quellversion des Geräts 7.6.2, einschließlich der darauf angewendeten Bridge-SMUs.

Bearbeiten von Bridge-SMUs

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

[Delete Path](#)

[Edit Bridge SMUs](#)

[Cancel](#) [Next](#)

Upgrade-Pfad mit Bridge-SMUs

1. Wählen Sie im Abschnitt "Upgrade Paths" das Symbol More Options (Weitere Optionen) > Edit Bridge SMUs (Bridge-SMUs bearbeiten). Das Fenster Edit Bridge SMUs wird geöffnet.

Edit Bridge SMUs

Select option(s)

- ☒ asr9k-x64-7.7.2.CSCwd07897.tar
- ☒ asr9k-x64-7.7.2.CSCwe22538.tar

Bridge-SMUs bearbeiten

2. Aktivieren oder deaktivieren Sie die entsprechenden Kontrollkästchen, um die Bridge-SMUs zu aktualisieren.
3. Klicken Sie auf OK. Es wird eine Zusammenfassung der Änderungen angezeigt.

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	Target Version			
Select option	Select option			
Source Version	Bridge SMU(S)	Target Version	Action	
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

Zusammenfassung der Änderungen

4. Überprüfen Sie die Zusammenfassung der Änderungen, und klicken Sie auf Weiter.

Bridge-SMUs löschen

Source Version	Target Version	
Select option	Select option	
Source Version	Bridge SMU(S)	Target Version
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

Bridge-SMUs bearbeiten

1. Wählen Sie im Abschnitt "Upgrade Paths" das Symbol More Options (Weitere Optionen) > Edit Bridge SMUs (Bridge-SMUs bearbeiten). Das Fenster Edit Bridge SMUs wird geöffnet.

✕

Edit Bridge SMUs

Select option(s) ^

☒
asr9k-x64-7.7.2.CSCwd07897.tar

☒
asr9k-x64-7.7.2.CSCwe22538.tar

Bridge-SMUs bearbeiten

2. Deaktivieren Sie die entsprechenden Kontrollkästchen, um Bridge-SMUs zu entfernen.
3. Klicken Sie auf OK. Es wird eine Zusammenfassung der Änderungen angezeigt.

Planning	Distribution	Activation								
Policy Name * ASR9K bridge 772	Description 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									
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Source Version</th> <th>Bridge SMU(S)</th> <th>Target Version</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td>7.7.2</td> <td>asr9k-x64-7.7.2.CSCwd07897.tar, asr9k-x64-7.7.2.CSCwe22538.tar</td> <td>7.8.2</td> <td>⋮</td> </tr> </tbody> </table> 1 Items per page 25			Source Version	Bridge SMU(S)	Target Version	Action	7.7.2	asr9k-x64-7.7.2.CSCwd07897.tar, asr9k-x64-7.7.2.CSCwe22538.tar	7.8.2	⋮
Source Version	Bridge SMU(S)	Target Version	Action							
7.7.2	asr9k-x64-7.7.2.CSCwd07897.tar, asr9k-x64-7.7.2.CSCwe22538.tar	7.8.2	⋮							

Cancel Next

Zusammenfassung der Änderungen

Vertrieb

Die Verteilung nimmt Eingabeparameter in Bezug auf die Bildverteilung (d. h. die Bildkopie) an. Die folgenden Images sind die erforderlichen Eingabeparameter für jeden Upgrade-Pfadtyp.

☒ 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 asr9k_distribution_precheck	Post Check Templates asr9k_distribution_postcheck
☐ Pre/Post Workflow		

Previous Next

Abschnitt "Image-Verteilung" - Upgrade in einem Schritt

✓

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

Abschnitt "Image Distribution": Upgrade in einem Schritt mit Aktivierung vor und nach dem Workflow

All > D2D_multistep_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

Abschnitt "Distribution" - Upgrade in mehreren Schritten

^ 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

Abschnitt "Distribution" - Upgrade in mehreren Schritten

Abschnitt "Distribution" - Bridge-SMU-Upgrade

1. Konfigurieren Sie die Parameter für die Bildverteilung.
2. Die folgende Tabelle enthält eine kurze Beschreibung der einzelnen Felder.

Feld	Beschreibung
Workflow-Name	Der entsprechende Verteilungs-Workflow
Neuesten Workflow verwenden	Aktuelle Version des ausgewählten Workflows auswählen
Workflowversion	Die benutzerdefinierte Workflowversion. Diese Option kann nur aktiviert werden, wenn das Kontrollkästchen Neuesten Workflow verwenden nicht aktiviert ist. Die Prozessvorlagen, die in beiden Phasen ausgeführt werden (d. h. Vor- und Nachprüfung)
Allgemeine Vorlagen vor/nach dem Einsatz	Anmerkung: Die Prüfungen beziehen sich nur auf den Meilenstein der Distribution. Weitere Informationen finden Sie unter Prozessvorlagen
Workflow-Wechsel vor/nach	Ermöglicht es Benutzern, die Ausführung von Workflows vor oder nach der Überprüfung im Distribution-Meilenstein auszuwählen. Wenn der Umschalter eingeschaltet ist, können nur Vor- oder Nachprüfungs-Workflows konfiguriert werden. Beinhaltet die Befehle, die nur während der Phase vor der Prüfung ausgeführt werden.
Workflow vor der Prüfung	Anmerkung: Diese Prüfungen sind spezifisch für den Meilenstein der Distribution.
Workflow nach der Überprüfung	Der Nachprüfungs-Workflow umfasst die Befehle, die

Feld

Beschreibung

während der Nachprüfungsphase eindeutig ausgeführt werden.

Anmerkung: Diese Prüfungen sind spezifisch für den Meilenstein der Distribution.

die Prozessvorlagen, die exklusive Befehle zur Vorabprüfung enthalten; Templates werden nur während der Pre-Check Phase ausgeführt.

Vorlagen vor dem Überprüfen

Anmerkung: Die Prüfungen beziehen sich nur auf den Meilenstein der Distribution.

die Prozessvorlagen, die exklusive Befehle nach der Überprüfung enthalten; -Templates werden nur im Nachprüfungsstadium ausgeführt.

Vorlagen nach der Prüfung

Anmerkung: Die Prüfungen beziehen sich nur auf den Meilenstein der Distribution.

Bei Multi-Select-Upgrades werden über alle Upgrade-Pfade hinweg konsistente Eigenschaften angewendet.

Verwenden Sie die gleichen Eigenschaften für alle unten aufgeführten Upgrade-Pfade.

Anmerkung: Wenn diese Option ausgewählt ist, werden die gleichen Eigenschaften auf alle Upgrade-Pfade bei der Aktualisierung mit Mehrfachauswahl angewendet.



Anmerkung: Workflows oder Prozessvorlagen müssen ordnungsgemäß mit dem Tag "Betriebssystem-Upgrade der nächsten Generation" gekennzeichnet werden.

3. Klicken Sie auf Weiter, um mit dem Abschnitt Aktivierung fortzufahren.

Aktivierung

Planning Distribution Activation

Workflow Name*
ASR9K_Device_SW_Activation

Use latest workflow

Workflow Version*
Select option

Pre/Post Common Templates
asr9k_activation_check2, asr9k_activation_check1

Pre Check Templates
Select option(s)

Post Check Templates
Select option(s)

Valid Pre/Post Differences
asr9k_activation_check2, asr9k_activation_check1

Rollback Workflow
Select option

Pre/Post Workflow

Previous Update

Aktivierungsabschnitt - Upgrade in einem Schritt

Feld	Beschreibung
	Anmerkung: Die Prüfungen beziehen sich nur auf den Meilenstein der Aktivierung.
Vorlagen vor dem Überprüfen	Weitere Informationen finden Sie unter Prozessvorlagen die Prozessvorlagen, die exklusive Befehle zur Vorabprüfung enthalten; Templates werden nur während der Pre-Check Phase ausgeführt.
Vorlagen für Nachprüfung	Anmerkung: Die Prüfungen beziehen sich nur auf den Meilenstein der Aktivierung. die Prozessvorlagen, die exklusive Befehle nach der Überprüfung enthalten; - Templates werden nur im Nachprüfungsstadium ausgeführt.
Gültiger Vor-/Nachunterschied	Anmerkung: Die Prüfungen beziehen sich nur auf den Meilenstein der Aktivierung. Die Prozessvorlagen, die zum Ignorieren der Unterschiede ausgewählt wurden. Anmerkung: Die Prüfungen beziehen sich nur auf den Meilenstein der Aktivierung. Der entsprechende Rollback-Workflow.
Rollback-Workflow	Anmerkung: Wenn einer der Upgrade-Pfade mit dem Rollback-Workflow bei der Aktualisierung mit mehreren Auswahl ausgewählt ist, werden alle anderen Upgrade-Schritte standardmäßig mit dem Rollback-Workflow ausgewählt.
Workflow vor der Prüfung	Dieser benutzerdefinierte Workflow zur Vorabprüfung besteht aus spezifischen Befehlen, deren Ausführungsergebnisse ausgewählt und überprüft werden können. Sie wird nur während der Vorprüfung durchgeführt.
Workflow nach der Überprüfung	Anmerkung: Diese Prüfungen beziehen sich auf den Aktivierungsmeilenstein. Dieser benutzerdefinierte Workflow nach der Überprüfung besteht aus bestimmten Befehlen, deren Ausführungsergebnisse ausgewählt und überprüft werden können. Sie erfolgt nur während der Nachkontrolle.
Verwenden Sie die gleichen Eigenschaften für alle unten aufgeführten Upgrade-Pfade.	Anmerkung: Diese Prüfungen beziehen sich auf den Aktivierungsmeilenstein. Bei Multi-Select-Upgrades werden über alle Upgrade-Pfade hinweg konsistente Eigenschaften angewendet. Anmerkung: Wenn diese Option ausgewählt ist, werden die gleichen Eigenschaften auf alle Upgrade-Pfade bei der Aktualisierung mit Mehrfachauswahl angewendet.



Anmerkung: Folgendes ist zu beachten:

- Der erforderliche Algorithmus für öffentliche Schlüssel für Nexus-Geräte muss im NSO konfiguriert werden.
- Konfigurieren Sie die Funktionen von BGP, BFD und HSRP, um Vorlagen vor und nach der Überprüfung auf den Nexus-Geräten auszuführen.

3. Klicken Sie auf Erstellen. Es wird eine Zusammenfassung der Felder angezeigt.

The screenshot shows a 'Summary' window in the NSO GUI. The title bar says 'Summary'. The content area has a light blue header with the title. Below the header, there are several fields: 'Name: Single step upgrade', 'Description: This upgrade policy for ansible', 'Max Batch Count: 5', and 'Default Policy: No'. There is also a 'Max Batch Count: 5' field. Below these fields, there are tabs for 'Planning', 'Distribution', and 'Activation'. The 'Planning' tab is selected. Under the 'Planning' tab, there is a 'Backup Details' section with a dropdown menu. A 'Submit' button is located at the bottom right of the window.

Zusammenfassung - Richtlinie für ein Upgrade in einem Schritt

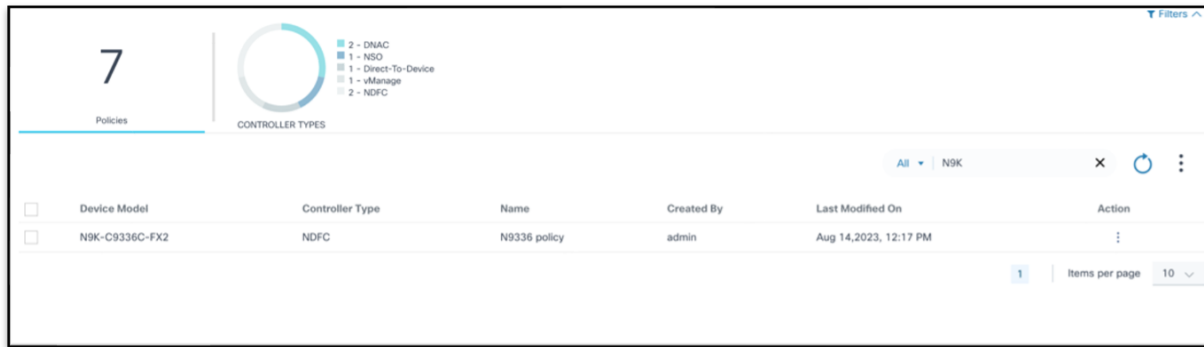
The screenshot shows a 'Summary' window in the NSO GUI. The title bar says 'Summary'. The content area has a light blue header with the title. Below the header, there are several fields: 'Name: Multi step upgrade', 'Description: This upgrade policy for ansible', 'Max Batch Count: 5', and 'Default Policy: No'. There is also a 'Max Batch Count: 5' field. Below these fields, there are tabs for 'Planning', 'Distribution', and 'Activation'. The 'Planning' tab is selected. Under the 'Planning' tab, there are two sections: 'Backup Details' and 'Upgrade Paths', each with a dropdown menu. A 'Submit' button is located at the bottom right of the window.

Zusammenfassung - Richtlinie für mehrstufige Upgrades

4. Überprüfen Sie die Feldübersicht, und klicken Sie auf Senden. Daraufhin wird eine Statusbenachrichtigung und eine Bestätigungsmeldung angezeigt. Die Richtlinien werden bei erfolgreicher Erstellung auf der Seite angezeigt.

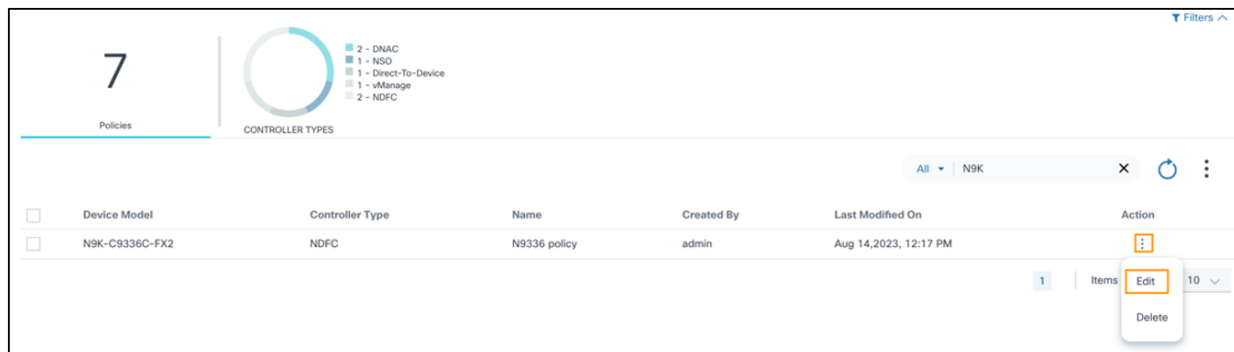
Zusätzliche Upgrade-Richtlinien für andere Gerätemodelle können nach Bedarf erstellt werden.

Aktualisierungsrichtlinien bearbeiten



Suchergebnis der Upgrade-Richtlinie

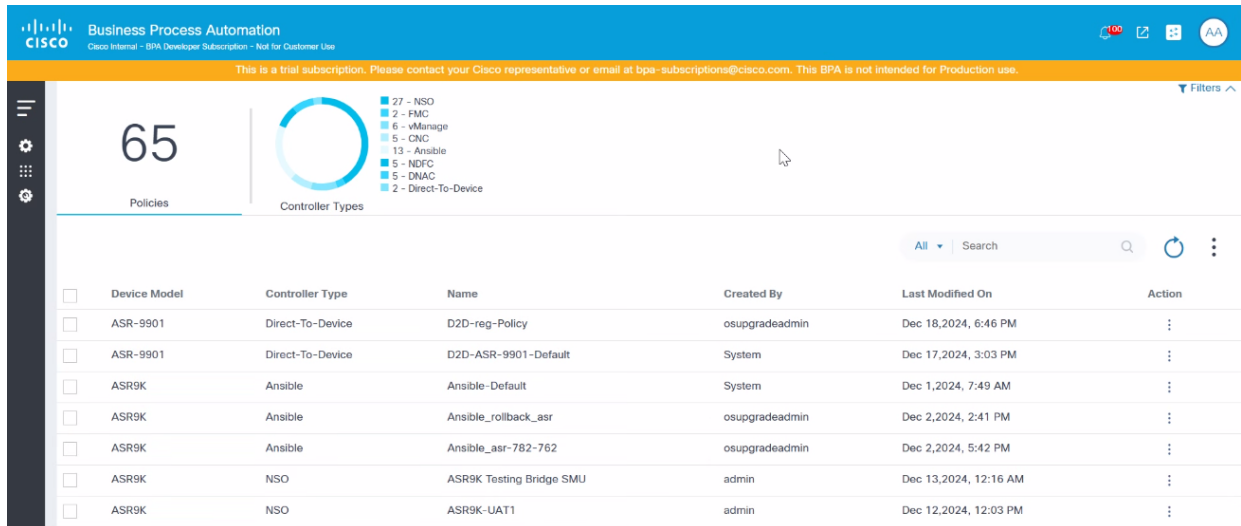
1. Suchen Sie auf der Seite "Upgrade Policy" (Aktualisierungsrichtlinie) mithilfe des Felds Search (Suchen) die gewünschte Richtlinie.



Aktualisierungsrichtlinie bearbeiten

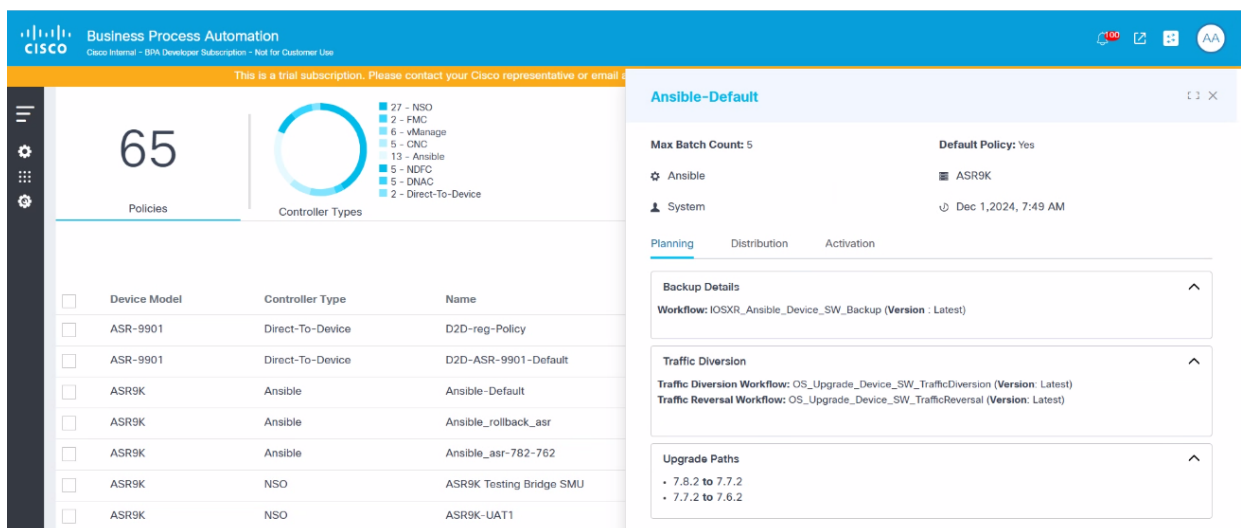
2. Wählen Sie in der Spalte "Aktion" der Richtlinie das Symbol Weitere Optionen > Bearbeiten aus.
3. Aktualisieren Sie die entsprechenden Felder, und klicken Sie auf Aktualisieren. Es wird eine Zusammenfassung der Änderungen angezeigt.
4. Überprüfen Sie die Zusammenfassung der Änderungen, und klicken Sie auf Senden. Statusbenachrichtigungen werden angezeigt, gefolgt von einer Bestätigungsmeldung.

Anzeigen von Aktualisierungsrichtlinien



Upgrade-Richtlinie

1. Wählen Sie auf der Seite Upgrade Policy (Upgrade-Richtlinie) die Zeile der gewünschten Upgrade-Richtlinie aus. Die Detailsansicht der Richtlinie wird geöffnet.



Detailsansicht der Upgraderichtlinie

Aktualisierungsrichtlinien werden gelöscht

 Anmerkung: Standardrichtlinien können nicht gelöscht werden, aber Benutzer können die Prozessvorlagen und Workflows bearbeiten.

7 Policies

CONTROLLER TYPES

- 2 - DNAC
- 1 - NSO
- 1 - Direct-To-Device
- 1 - vManage
- 2 - NDFC

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

1 Items per page 10

Upgrade-Richtlinie

1. Suchen Sie auf der Seite Upgrade Policies (Upgrade-Richtlinien) mithilfe des Felds Search (Suchen)** die gewünschte Richtlinie.

7 Policies

CONTROLLER TYPES

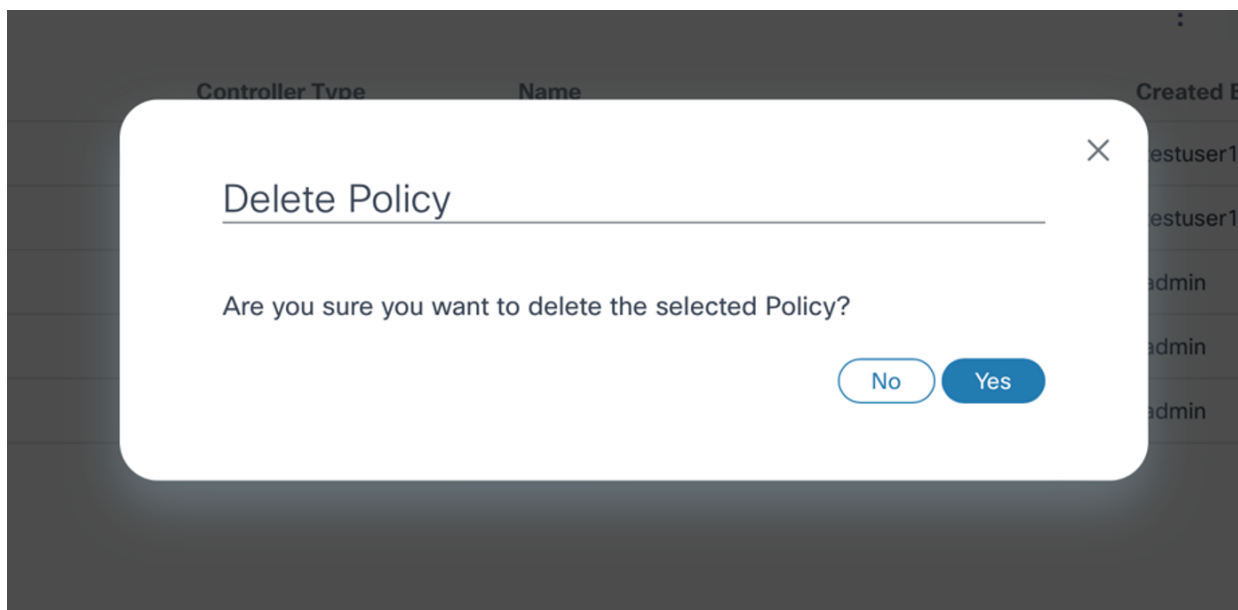
- 2 - DNAC
- 1 - NSO
- 1 - Direct-To-Device
- 1 - vManage
- 2 - NDFC

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

1 Items per page 10

Aktualisierungsrichtlinie löschen

2. Wählen Sie in der Spalte "Aktion" der Richtlinie die Option Weitere Optionen > Löschen aus. Ein Bestätigungsfenster wird geöffnet



Löschen der Richtlinie bestätigen

3. Klicken Sie auf Ja.

Kontrolle des Zugriffs auf Aktualisierungsrichtlinien

Diese Funktion bietet eine Zugriffskontrolle für Upgrade-Richtlinien und verhindert, dass nicht autorisierte Benutzer die in der Anwendung für Betriebssystem-Upgrades definierten Richtlinien aktualisieren. Administratoren können den Zugriff einschränken, indem sie eine Ressourcengruppe mit zugänglichen Richtlinien definieren.

So erstellen Sie eine Ressourcengruppe:

1. Navigieren Sie zu Einstellungen > Ressourcengruppen.
2. Erstellen Sie eine Ressourcengruppe mit Richtlinien, auf die Benutzer ohne Administratorrechte zugreifen können. Nicht-Administrator-Benutzer, die zu dieser Benutzergruppe gehören, haben jetzt nur Zugriff auf die Richtlinien, die in dieser Ressourcengruppe verfügbar sind.
3. Erstellen Sie eine Zugriffsrichtlinie, um die Ressourcengruppe einer Benutzergruppe zuzuordnen.

Weitere Informationen finden Sie unter [Zugriffskontrolle](#).



Anmerkung: Folgendes sollte beachtet werden.

- Benutzer können die falschen Workflows für die Verteilung und Aktivierung auswählen, was zu unbeabsichtigtem Verhalten führt. Der Benutzer ist dafür verantwortlich, den Workflow korrekt zuzuordnen und die Anwendbarkeit von Meilensteinen wie Verteilungs-, Aktivierungs-, Rollback- und Gerätemodellen zu überprüfen.
- Workflows und Prozessvorlagen müssen mit dem Tag "Betriebssystem-Upgrade der nächsten Generation" verknüpft werden, damit sie beim Erstellen oder Aktualisieren von Richtlinien ausgewählt werden können.
- Vom Systembenutzer erstellte Standard-OOB-Richtlinien können nicht gelöscht werden. Benutzer können jedoch die Prozessvorlagen und Workflows bearbeiten.

Aufträge aktualisieren

Software-Upgrades werden mit der Anwendung "Upgrade-Job" verwaltet, die aus einem oder mehreren Stapeln besteht, wobei jeder Stapel ein oder mehrere Netzwerkgeräte enthält. Ein Job kann im Entwurfsmodus erstellt und mehrmals gespeichert werden. Upgrades können erst nach der Ausführung des Auftrags erfolgen, sodass die Betreiber Änderungen im Voraus planen können.

Voraussetzungen

- Reserviertes Wartungsfenster für Upgrades
- Vorabgenehmigungen für Upgrade-Änderungsanforderungen
- Der Service für die Konfigurationssicherung und -wiederherstellung muss eingerichtet und ausgeführt werden.
- Der Scheduler Service muss in Betrieb sein
- BPA-Adapter für externe Systeme (z. B. ein Ticketsystem) müssen, falls vorhanden, integriert werden

Anzeigen und Verwalten von Aktualisierungsaufträgen

1. Melden Sie sich bei BPA mit Anmeldeinformationen an, die Zugriff auf Upgrade-Jobs haben.
2. Wählen Sie Betriebssystem-Upgrade > Upgrade-Jobs aus. Die Seite Upgrade-Auftrag wird angezeigt.



Auftrag aktualisieren

Die Seite Upgrade-Auftrag enthält Folgendes:

 Anmerkung: Standardmäßig werden zehn Jobs angezeigt. Seitenzahlen können verwendet werden, um zu anderen Job-Seiten zu navigieren.

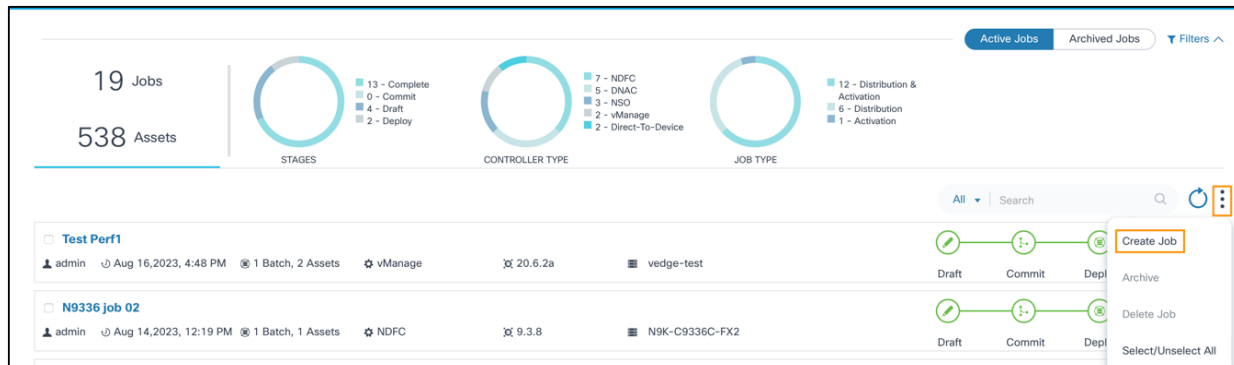
- Ein Umschalter für aktive und archivierte Jobs, mit dem zwischen aktiven und archivierten Jobs gewechselt werden kann.
- Ein oben angezeigter Abschnitt zu Analysen bietet folgende Informationen:
 - Mit den Jobs verknüpfte Jobs und Assets gesamt
 - Stufendiagramm mit folgenden Filtern:

- Entwurf: Job befindet sich im Entwurfsstadium und ist noch nicht festgelegt.
- Zusichern: Job wird mit allen erforderlichen Geräten, Batches oder Zeitplänen übernommen, bis der Zeitplan erreicht ist
- Bereitstellen: Die Aktualisierungsaktivität für einen oder mehrere Stapel wurde gestartet
- Vollständig: Die Aktualisierungsaktivität für alle Geräte, die zu allen Batches gehören, ist abgeschlossen
- Diagramm Controller-Typ: Ermöglicht Job-Filterung nach Cisco Catalyst Center-, vManage-, NSO-, NDFC-, Direct-to-Device-, CNC-, ANSIBLE- und FMC-Controllertypen
- Diagramm der Auftragstypen mit den folgenden Filtern:
 - Vertrieb: Aufträge, die das Staging oder Kopieren von Bildern vom Controller auf Geräte ausführen
 - Aktivierung: Aufträge, die die Aktivierung oder Aktualisierung der Software eines Geräts durchführen
 - Verteilung und Aktivierung: Aufträge, die Staging, Kopieren und Aktivierung oder Upgrade der Software eines Geräts ausführen
- Das Feld Suchen, mit dem eine generische Suche in allen Metadaten oder in den Feldern Jobname und Erstellt von durchgeführt werden kann.
- Das Symbol Aktualisieren, mit dem Sie die Jobübersicht aktualisieren und die Diagrammfilter oder eine benutzerdefinierte Suche im Feld Suchen löschen können.
- Das Symbol More Options (Weitere Optionen) mit Optionen zum Erstellen eines neuen Upgrade-Jobs und zum Archivieren oder Löschen ausgewählter Jobs Benutzer können Alle auswählen oder deaktivieren.
- Jobs werden als Bereiche angezeigt und bieten eine kurze Ansicht der folgenden Informationen:
 - Das Symbol User Task (Benutzeraufgabe) wird mit der Anzahl der verfügbaren Benutzeraufgaben angezeigt
 - Der Benutzer, der den Auftrag erstellt hat
 - Datum der Joberstellung
 - Die Anzahl der Stapel und Ressourcen
 - Controller-Typ (z. B. Cisco Catalyst Center, vManage, NDFC, Direct-to-Device, CNC, ANSIBLE oder FMC)
 - Die Zielversion
 - Das entsprechende Gerätemodell
 - Eine Meilensteinansicht der Jobphasen (d. h. Entwurf, Übernehmen, Bereitstellen und Abschließen) mit einer Farblegende für jeden Meilenstein:
 - Grau: Meilenstein wurde nicht gestartet
 - Blau: Meilenstein wird gerade umgesetzt
 - Rot: Meilenstein-Ausgabe
 - Grün: Meilenstein abgeschlossen
 - Eine farbige Legende am Ende der Meilensteine, die den Status des Jobs anzeigt:
 - Grün: Auftrag ist abgeschlossen

- Rot: Job hat Probleme
- Blau: Auftrag wird ausgeführt

Planen von Aktualisierungsaufträgen

So erstellen Sie einen Job:



Option für Aktualisierungsauftrag erstellen

1. Wählen Sie auf der Seite "Upgrade-Job" das Symbol Weitere Optionen > Job erstellen aus. Die Seite Upgrade-Auftrag erstellen wird angezeigt.

The 'Upgrade-Job' form contains the following fields and options:

- Name ***: Enter Job name
- Controller Type ***: Select option
- Confirmation Policy ***: Select option
- Job Type ***: Select option
- Deployment Order ***: Select option
- ITSM Ticket Number**: Enter ITSM Ticket Number
- Upgrade Policy Name ***: Select option

Buttons: Save Job, Commit Job, Cancel, Add New Batch.

Aktualisierungsauftrag erstellen

2. Geben Sie im Feld Name einen Jobnamen ein.
3. Wählen Sie den Controller-Typ aus (z. B. Cisco Catalyst Center, vManage, NDFC, Direct-to-Device, CNC, FMC, ANSIBLE oder NSO).
4. Wählen Sie eine Konformitätsrichtlinie mit nicht konformen Geräten aus.

Anmerkung: Nur die Konformitätsrichtlinien, die mindestens einmal ausgeführt werden und über mindestens ein nicht konformes Gerät verfügen, sind in der Liste verfügbar. Die entsprechende Upgrade-Richtlinie wird automatisch identifiziert, wenn eine Richtlinie ausgewählt wurde.

Die folgenden Details werden auf der linken Seite des Formulars Job erstellen unter Jobübersicht angezeigt:

- Betroffene Gerätemodelle



Anmerkung: Wenn der ausgewählten Konformitätsrichtlinie mehr als ein zugeordnetes Gerätemodell zugeordnet ist, werden mehrere Gerätemodelle angezeigt.

- Zielversion
- Aggregation der vorhandenen Releaseversionen und entsprechende Zählung
- Maximal zulässige Anzahl von Stapeln
- Gesamtzahl der nicht konformen Aktiva



Anmerkung: Wenn die ausgewählte Konformitätsrichtlinie mehreren Gerätemodellen zugeordnet ist, wird die Summe der nicht konformen Ressourcen für alle verknüpften Modelle angezeigt.

- Option zum Hinzufügen eines Stapels

5. Wählen Sie einen der folgenden Upgrade-Auftragstypen aus:

- Vertrieb: Aufträge, die nur über eine Distribution ausgeführt werden, sind nützlich, wenn das Staging des Software-Images vor der eigentlichen Aktivierung stattfindet.
- Aktivierung: Nur-Aktivierungs-Jobs sind hilfreich, um Upgrades von Geräten durchzuführen, deren Verteilung bereits über einen Nur-Verteilungs-Job abgeschlossen ist.
- Verteilung und Aktivierung: Sowohl die Image-Verteilung als auch das Staging und die Aktivierung erfolgen innerhalb desselben Jobs. Dies ist hilfreich in Szenarien, in denen ein reichliches Wartungsfenster zur Verfügung steht, um sowohl das Kopieren von Images auf ein Gerät als auch das Aktualisieren abzudecken.

6. Wählen Sie die Upgrade-Bestellung aus. Mehrere Geräte werden gleichzeitig im parallelen Modus verarbeitet, während Geräte einzeln im sequenziellen Modus verarbeitet werden.



Anmerkung: Die maximale Anzahl von Geräten, die im parallelen Modus verarbeitet werden können, hängt von der Bereitstellungskonfiguration ab. Die ausgewählte Aktualisierungsreihenfolge gilt für den gesamten Auftrag, kann jedoch je nach Bedarf innerhalb eines bestimmten Stapels überschrieben werden.

7. Fügen Sie die Nummer des Änderungsantrags im Feld "Ticketnummer für das IT-Servicemanagement (ITSM)" hinzu.

8. Wählen Sie den Namen der Aktualisierungsrichtlinie aus. Je nach Controller-Typ und Gerätemodell für die Konformitätsrichtlinie werden nur anwendbare Upgrade-Richtlinien angezeigt. Benutzer können eine der Upgrade-Richtlinien auswählen. Wenn der Softwarekonformitätsrichtlinie mehr als ein Modell zugeordnet ist, werden alle relevanten Aktualisierungsrichtlinien angezeigt, die den einzelnen Modellen zugeordnet sind. Benutzer sollten sorgfältig die Upgrade-Richtlinie auswählen, die für alle Modelle funktioniert.
9. Wählen Sie den Software-Image-Server aus, um anzugeben, welches vManage-Image-Repository (z. B. lokal oder remote) verwendet wird.



Anmerkung: Diese Eingabe gilt nur für den vManage-Controller-Typ.

Job Summary

Job: c8000v

Target Version: 17.09.03.0.15

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

Batches (Max Limit: 5)

Add Batch

4 Assets Pending

Form Fields:

- Name *: vManage Job ✓
- Controller Type *: vManage ✓
- Conformance Policy *: vmanage c8000v policy ✓
- Job Type *: Distribution & Activation ✓
- Deployment Order *: Parallel ✓
- ITSM Ticket Number: Enter ITSM Ticket Number
- Upgrade Policy Name *: vManage-Default ✓
- Software Image Server: vmanage-r3 ✓

To get started [Add New Batch](#)

Upgrade-Auftrag mit ausgefüllten Details erstellen (Konformitätsrichtlinie besteht aus einem Modell)

Job Summary

Job: N9K-C93...,N9K-C93...

Target Version: 10.2.5

Existing Release: 9.3(7) [4]

Batches (Max Limit: 5)

Add Batch

2 Assets Pending

Form Fields:

- Name *: test ✓
- Controller Type *: NDFC ✓
- Conformance Policy *: policy-demo ✓
- Job Type *: Distribution & Activation ✓
- Deployment Order *: Parallel ✓
- ITSM Ticket Number: Enter ITSM Ticket Number
- Upgrade Policy Name *: NDFC-Default ✓

To get started [Add New Batch](#)

Upgrade-Auftrag mit ausgefüllten Details erstellen (Konformitätsrichtlinie hat mehrere Modelle)

10. Klicken Sie auf Auftrag speichern, um den Entwurf zu speichern, bis der Auftrag übernommen werden kann.

All > vManage Job Save Job Commit Job

Job Summary

c8000v

Target Version: 17.09.03.0.15

Existing Release: 17.06.03a.0.3 [6]

Batches (Max Limit: 5)

Add Batch

6 Assets Pending

Name* vManage Job ✓

Controller Type* vManage ✓ ✓

Conformance Policy* vmanage sw conformance

Job Type* Distribution & Activation ✓ ✓

Deployment Order* Parallel ✓ ✓

ITSM Ticket Number Enter ITSM Ticket Number

Upgrade Policy Name* vManage-Default ✓

Software Image Server vManage-r3 ✓ ✓

To get started Add New Batch

Stapel hinzufügen und neuen Stapel hinzufügen

- Zum Hinzufügen eines Stapels klicken Sie auf den Link Stapel hinzufügen oder auf Neuen Stapel hinzufügen. Das Fenster Stapelerstellung wird geöffnet.

CISCO Business Process Automation
Cisco Internal - BPA Developer Subscription - Not for Customer Use
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.

All > vManage Job Save Job Commit Job Cancel

Job Summary

c8000v

Target Version: 17.09.03.0.15

Existing Release: 17.06.03a.0.3 [3] | 17.09.03a.0.6476 [1]

Batches (Max Limit: 5)

Add Batch

4 Assets Pending

Batch Name* Enter Batch Name

Deployment Order Parallel

Software Image Server vmanage-r3

Select Assets Upload Assets Add Asset

☐ Distribute Now & Activate Later

August 2024

Sun Mon Tue Wed Thu Fri Sat

1 2 3

4 5 6 7 8 9 10

11 12 13 14 15 16 17

18 19 20 21 22 23 24

25 26 27 28 29 30 31

Start Time: Image Distribution & Activation

Batch-Erstellung

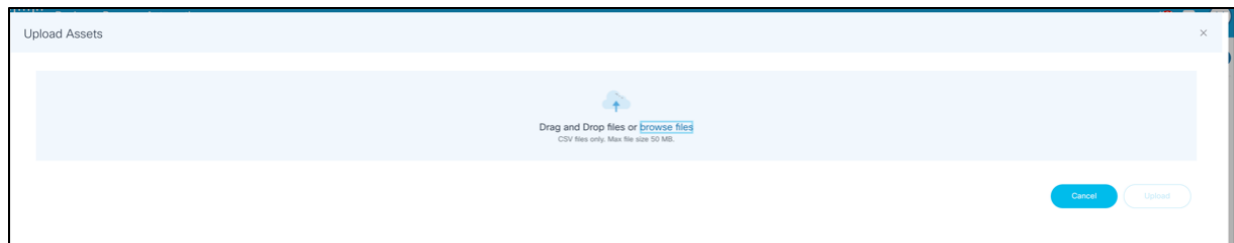
- Geben Sie einen relevanten Stapelnamen ein, und wählen Sie den Bereitstellungsauftrag aus.

 Anmerkung: Der hier ausgewählte Aktualisierungstyp hat Vorrang vor dem auf der Seite Auftragserstellung ausgewählten.

- Wählen Sie den Software-Image-Server aus, um anzugeben, welches vManage-Repository (z. B. lokal oder remote) verwendet wird.

 Anmerkung: Dieses Feld gilt nur für den vManage-Controller-Typ. Der hier ausgewählte Software-Image-Server hat Vorrang vor dem auf der Seite Job Creation (Auftragserstellung) ausgewählten Server.

14. Fügen Sie den Stapeln Ressourcen hinzu. Ressourcen können Chargen auf zwei Arten hinzugefügt werden:



Ressourcen hochladen

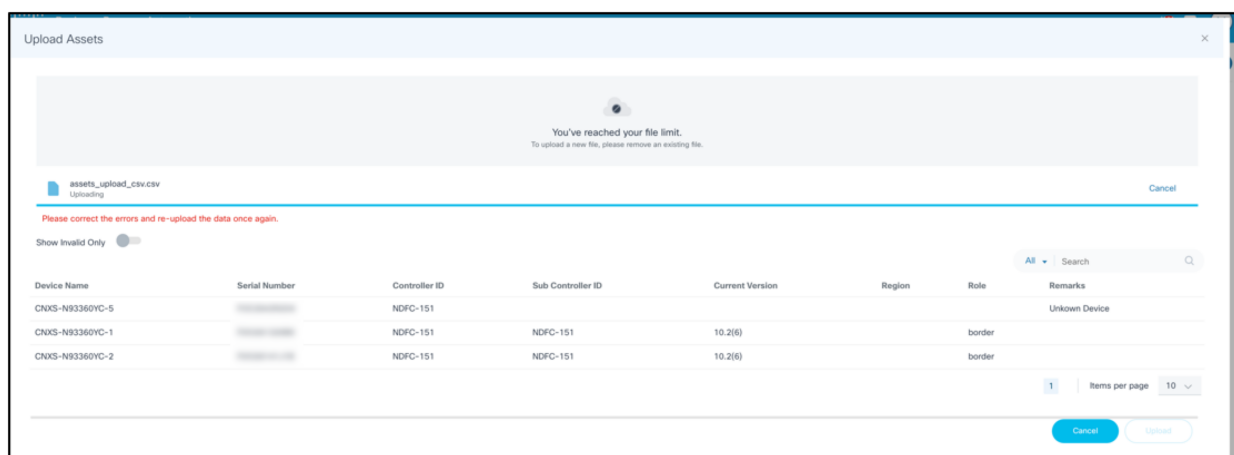
Option 1:

- Klicken Sie auf Ressourcen hochladen. Das Fenster Ressourcen hochladen wird geöffnet.
- Wählen Sie eine CSV-Datei zum Hochladen aus.



Anmerkung: Die CSV-Datei muss folgende Angaben enthalten:

- Gerätename: Name des Geräts oder der Ressource
 - Seriennummer: Seriennummer des Geräts
 - Controller-ID: Name des Controllers, der das Gerät verwaltet
 - Sub-Controller-ID: Name der Untercontroller-ID, die das Gerät verwaltet
- c. Klicken Sie auf Hochladen. Die CSV-Dateidaten werden validiert, und sowohl gültige als auch ungültige Daten werden angezeigt. Der Umschalter Show Invalid Only (Nur ungültige anzeigen) kann verwendet werden, um ungültige Geräte aus den hochgeladenen Ressourcendetails zu filtern.



Beispiel-Ressourcen, die über eine CSV-Datei hochgeladen wurden

- Wenn die hochgeladene Datei Fehler enthält, korrigieren Sie diese, und laden Sie sie erneut

hoch.



Anmerkung: Benutzer können die Auswahl der Ressourcen nur fortsetzen, wenn alle hochgeladenen Geräte gültig sind.

Device Name	Serial Number	Controller ID	Sub Controller ID	Current Version
C8kv1-7	4FBCE00	vmanage-r3	vmanage-r3	17.09.05a.0.6476
C8kv1-3	bd92efcac674038b89ef4313541b937	vmanage-r3	vmanage-r3	17.06.03a.0.3

Stapel hinzufügen - Ausgewählte Ressourcen

Option 2:

a. Klicken Sie auf Ressourcen hinzufügen. Das Fenster Anlagenauswahl wird geöffnet.



Anmerkung: Ressourcen hochladen und Ressourcen hinzufügen nicht gleichzeitig verwendet werden können.

b. Wählen Sie nur für den FMC-Controller-Typ den Steuerungsknoten oder den eigenständigen Knoten aus, um das Upgrade durchzuführen.



Anmerkung: Datengeräte sind im Aktualisierungsauftrag nicht zulässig, da das Upgrade der Datenknoten vom zugehörigen Kontrollknoten ausgeführt wird.

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
☐ C10RE-2-fra-lab.net		Global/Europe/OS Upgrades/Bldg1	BORDER ROUTER		DNAC-r3	DNAC-r3	17.6.2
☐ C10S8kv-11-fra-lab.net		Global/Europe/OS Upgrades/Bldg1	BORDER ROUTER		DNAC-r3	DNAC-r3	17.6.3a
☐ C10S8kv-12-fra-lab.net		Global/Europe/OS Upgrades/Bldg1	BORDER ROUTER		DNAC-r3	DNAC-r3	17.9.3a
☐ C10S8kv-13-fra-lab.net		Global/Europe/OS Upgrades/Bldg1	BORDER ROUTER		DNAC-r3	DNAC-r3	17.9.3a
☐ C10S8kv-14-fra-lab.net		Global/Europe/OS Upgrades/Bldg1	BORDER ROUTER		DNAC-r3	DNAC-r3	17.9.3a
☐ C10S8kv-16-fra-lab.net		Global/Europe/OS Upgrades/Bldg1	BORDER ROUTER		DNAC-r3	DNAC-r3	17.6.3a
☐ C10S8kv-17-fra-lab.net		Global/Europe/OS Upgrades/Bldg1	BORDER ROUTER		DNAC-r3	DNAC-r3	17.6.3a
☐ C10S8kv-18-fra-lab.net		Global/Europe/OS Upgrades/Bldg1	BORDER ROUTER		DNAC-r3	DNAC-r3	17.6.2

Geräteauswahl

- c. Wählen Sie die Geräte aus, die dem aktuellen Stapel hinzugefügt werden sollen.

Der Suchfilter kann zum Filtern von Geräten anhand verschiedener Attribute verwendet werden. Alle Geräte, die den Filterkriterien entsprechen, können in großen Mengen ausgewählt werden, indem das Kontrollkästchen in der Spaltenüberschrift GeräteName aktiviert wird. Benutzer haben auch die Möglichkeit, nach Asset-Gruppen zu filtern.

Der Umschalter Auswahl anzeigen kann aktiviert werden, um nur die ausgewählten Ressourcen anzuzeigen.



Anmerkung: Wenn der Umschalter Auswahl anzeigen aktiviert ist, wird der Filter Asset-Gruppen deaktiviert.

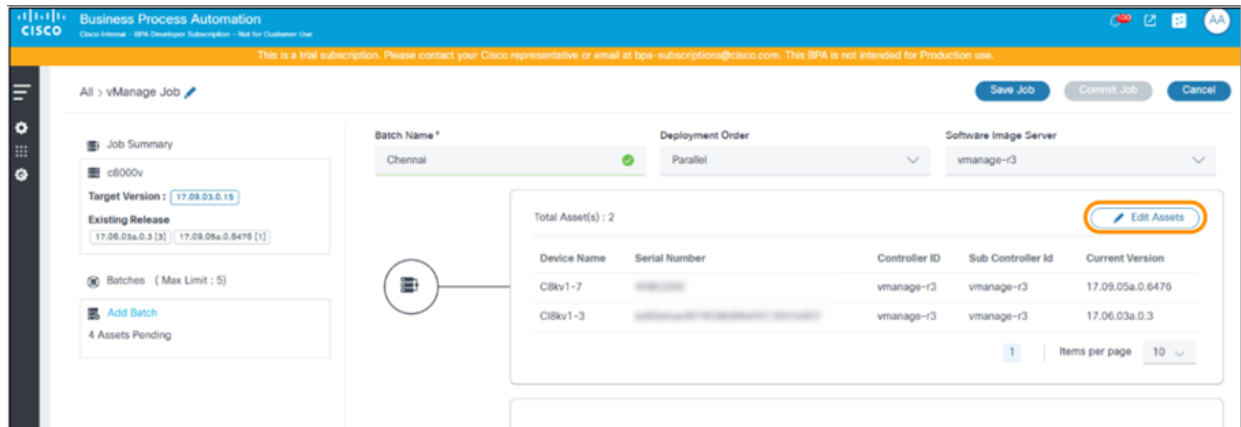
- d. Klicken Sie auf Speichern und schließen.

Durch Klicken auf Zurücksetzen werden die ausgewählten Elemente verworfen und der ursprüngliche Status der Ressourcenauswahl beibehalten.

Device Name	Batch Name	Region	Role	Serial Number	Controller ID	Sub Controller ID	Current Version
☒ CIBKv3-1.fra-lab.net	Europe	Global	BORDER ROUTER		DNAC1	DNAC1	17.6.3a
☒ CIBKv3-2.fra-lab.net	Europe	Global/India/Bengaluru/SQL-14	BORDER ROUTER		DNAC1	DNAC1	17.6.3a
☒ OICORE-2.fra-lab.net		Global/Europe/OS Upgrades/8btg1	BORDER ROUTER		DNAC-v3	DNAC-v3	17.6.2
☒ OIOSBkr-11.fra-lab.net		Global/Europe/OS Upgrades/8btg1	BORDER ROUTER		DNAC-v3	DNAC-v3	17.6.3a
☒ OIOSBkr-12.fra-lab.net		Global/Europe/OS Upgrades/8btg1	BORDER ROUTER		DNAC-v3	DNAC-v3	17.9.3a
☒ OIOSBkr-13.fra-lab.net		Global/Europe/OS Upgrades/8btg1	BORDER ROUTER		DNAC-v3	DNAC-v3	17.9.3a
☒ OIOSBkr-14.fra-lab.net		Global/Europe/OS Upgrades/8btg1	BORDER ROUTER		DNAC-v3	DNAC-v3	17.9.3a
☒ OIOSBkr-16.fra-lab.net		Global/Europe/OS Upgrades/8btg1	BORDER ROUTER		DNAC-v3	DNAC-v3	17.6.3a
☒ OIOSBkr-17.fra-lab.net		Global/Europe/OS Upgrades/8btg1	BORDER ROUTER		DNAC-v3	DNAC-v3	17.6.3a
☒ OIOSBkr-18.fra-lab.net		Global/Europe/OS Upgrades/8btg1	BORDER ROUTER		DNAC-v3	DNAC-v3	17.6.2

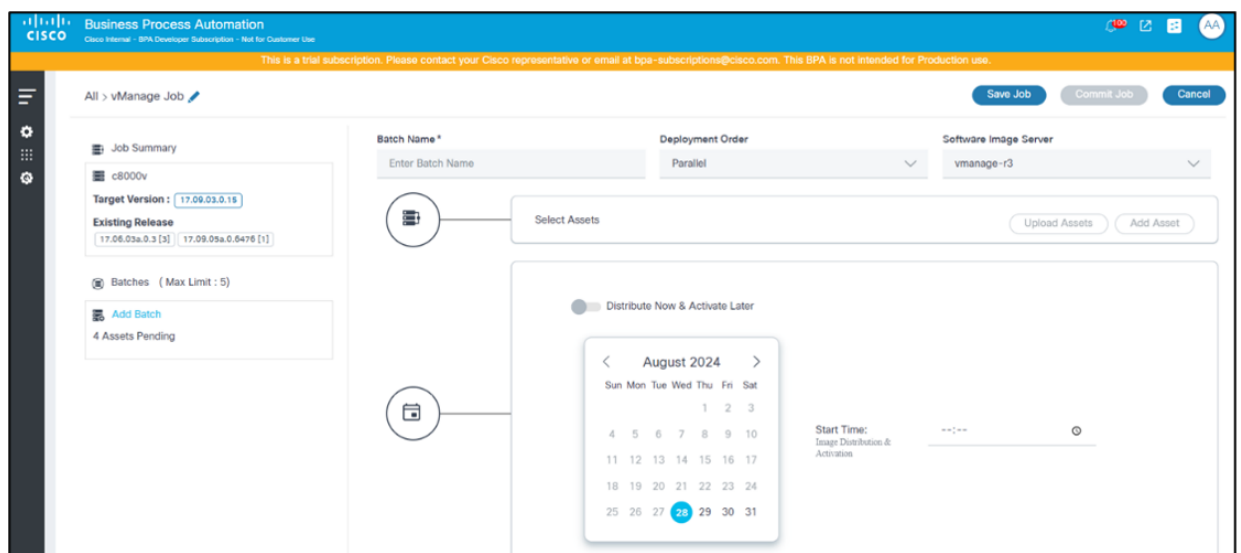
Zurücksetzen

- e. Wenn die Ressourcenauswahl geändert werden muss, klicken Sie auf Ressourcen bearbeiten.



Ressourcen zur Stapelbearbeitung

- f. Wählen oder löschen Sie die Ressourcen, um die erforderlichen Änderungen vorzunehmen, und klicken Sie auf Speichern und schließen. Beim Bearbeiten der Stapelressourcen können derzeit ausgewählte Ressourcen, die Teil eines anderen Auftrags oder Stapels sind, mit Häkchen und dem Stapelnamen in der Spalte Stapelname identifiziert werden.



Job Scheduler Upgrade

15. Wählen Sie ein Datum aus der Datumsauswahl und eine Uhrzeit aus der Zeitauswahl, um eine Zeit zum Auslösen des für den aktuellen Stapel ausgewählten Aktualisierungstyps zu planen.



Anmerkung: Der ausgewählte Auftragstyp ändert den Typ der verfügbaren Zeitpläne.

Folgende Szenarien sind möglich:

Auftragstyp	Jetzt verteilen, umschalten	Datum und Uhrzeit des Zeitplans	Distributordetails
Vertrieb	Standardmäßig deaktiviert	Aktiv	Die Verteilung erfolgt am angegebenen geplanten Datum und zur angegebenen geplanten Uhrzeit.
Vertrieb	Aktiviert	Deaktiviert	Verteilung erfolgt nach der Auftragsbestätigung Die Aktivierung erfolgt am angegebenen Datum und zur angegebenen Uhrzeit.
Aktivierung	–	Aktiv	Verteilung und Aktivierung erfolgen zum angegebenen Datum und Zeitpunkt. Die Verteilung erfolgt nach dem Commit des Jobs und Aktivierungs- Triggern am angegebenen geplanten Datum und zur angegebenen geplanten Uhrzeit.
Verteilung und Aktivierung	Standardmäßig deaktiviert	Aktiv	
Verteilung und Aktivierung	Aktiviert	Aktiv	

The screenshot displays the Cisco Business Process Automation (BPA) interface for vManage Upgrade. The interface includes a sidebar with navigation icons and a main content area. The main content area has a top bar with 'Save Job', 'Commit Job', and 'Cancel' buttons. Below this, there are sections for 'Batch Name' (with a text input field), 'Deployment Order' (set to 'Parallel'), and 'Software Image Server' (set to 'Select option'). A 'Distribute Now' button is prominently displayed. A calendar for September 2024 is shown, with the 12th selected. The 'Start Time' is set to 'Design Distribution'. The 'Create Batch' button is at the bottom right.

Planungsoptionen für Distributionsauftragstyp

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.

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

September 2024

Create Batch

Planungsoptionen für Aktivierungsauftragstyp

Distribute Now & Activate Later

August 2023

Start Time: 13:10

Image Distribution & Activation

Create Batch

Zeitplanoptionen für Vertriebs- und Aktivierungsauftragstyp

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.

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

September 2024

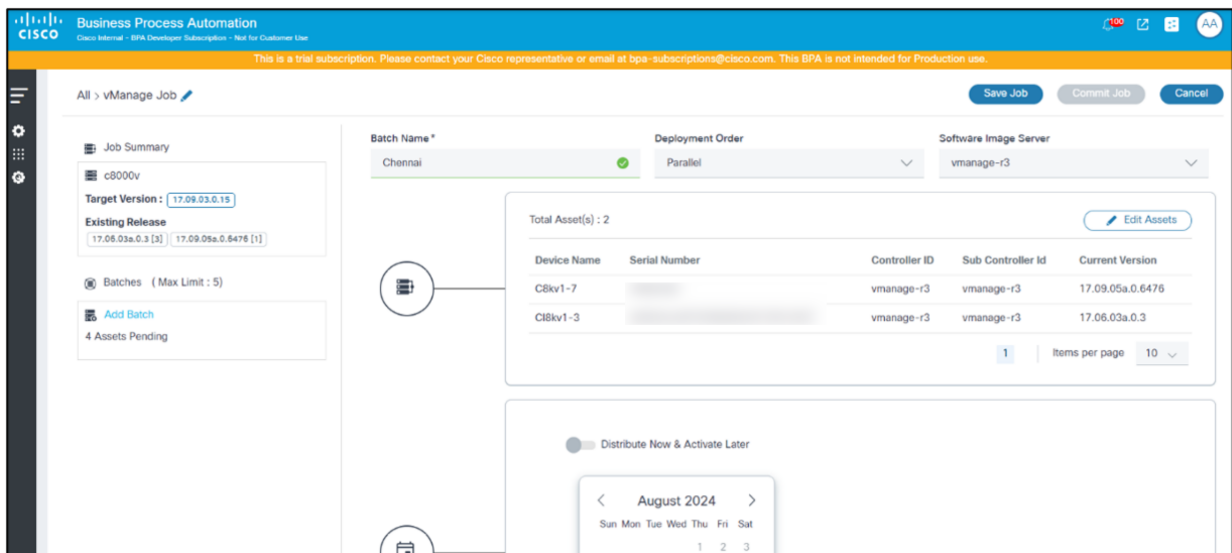
Create Batch

Zeitplanoptionen für Verteilungs- und Aktivierungsauftrag mit Jetzt verteilen und Später aktivieren Umschalten aktiviert

 Anmerkung: Die folgende Liste ist zu beachten.

- Wenn Sie mehrere Stapel planen, stellen Sie eine Zeitlücke zwischen den beiden Stapeln bereit, sodass eine Überlastung des Systems vermieden werden kann. Wenn sich mehrere Stapel überlappen, sollten Sie sie einem Stapel hinzufügen.
- Wenn der Umschalter "Jetzt verteilen" und "Später aktivieren" aktiviert ist, stellen Sie eine Zeitlücke zwischen der Auftragsbestätigungszeit und dem Aktivierungszeitplan ein. Andernfalls können Aktivierungs-Workflows Benutzeraufgaben erstellen, die einen manuellen Eingriff erfordern (d. h. Benutzer müssen warten, bis die Verteilung abgeschlossen ist, und dann einen erneuten Versuch starten).

16. Klicken Sie auf Stapel erstellen. Der Stapel kann auf der linken Seite angezeigt werden.



Auftrag erstellen - Auftrag bestätigen

Erstellen Sie so viele Stapel wie erforderlich. Ein Job kann den Status Entwurf haben, bis alle erforderlichen Informationen verfügbar sind.

 Anmerkung: Vermeiden Sie den Verlust von Auftragsdaten, indem Sie auf Auftrag speichern klicken, um den Entwurf zu speichern.

17. Klicken Sie auf Auftrag bestätigen, um die Auftragserstellung abzuschließen. Der Job wechselt in den Bereitstellungsstatus, wenn der Zeitplan für einen der Stapel ausgelöst wird.

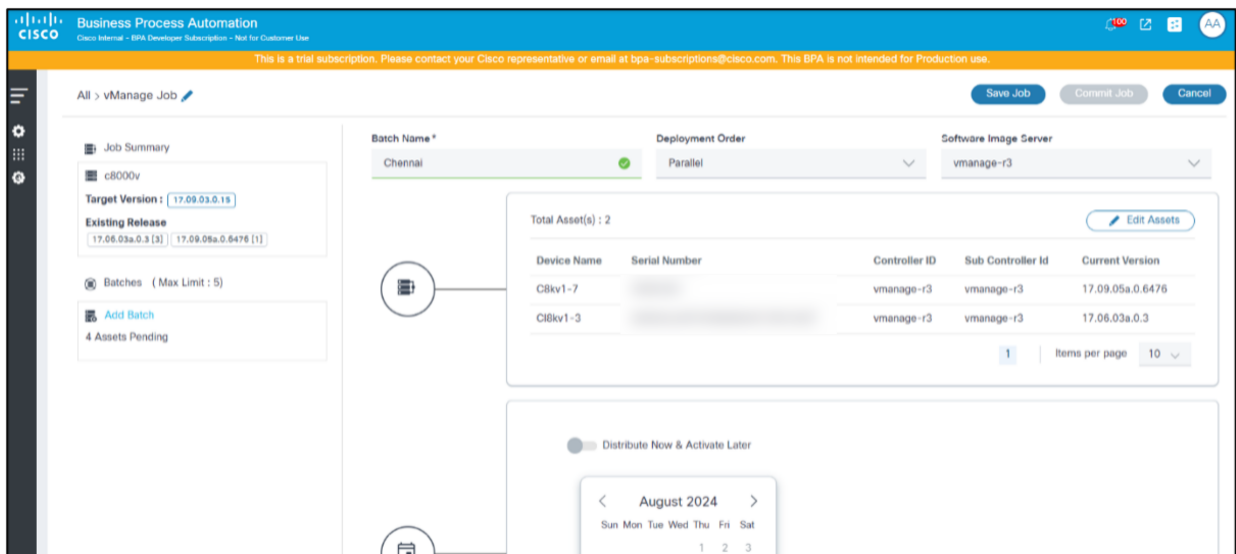
 Anmerkung: Der Schwellenwert für die maximale Anzahl von Batches kann auf der Seite

 Upgrade Policy (Aktualisierungsrichtlinie) erweitert oder aktualisiert werden.

Bearbeiten eines Stapels in einem Auftrag

 Anmerkung: Stapel können nur aktualisiert werden, wenn sich der Job in der Entwurfsphase befindet.

1. Wählen Sie den gewünschten Stapel im linken Bereich aus.



The screenshot shows the Cisco Business Process Automation (BPA) interface. The top header includes the Cisco logo and the text 'Business Process Automation'. Below the header, there is a warning message: 'This is a trial subscription. Please contact your Cisco representative or email at bpa-subscriptions@cisico.com. This BPA is not intended for Production use.' The main interface is divided into a left sidebar and a main content area. The sidebar contains a 'Job Summary' section with a 'c8000v' job, a 'Target Version' of '17.09.03.0.19', and an 'Existing Release' of '17.06.03a.0.3 [3]'. The main content area has a 'Batch Name' field set to 'Chennai', a 'Deployment Order' dropdown set to 'Parallel', and a 'Software Image Server' dropdown set to 'vmanage-r3'. Below these fields is a table of assets. The table has columns for 'Device Name', 'Serial Number', 'Controller ID', 'Sub Controller ID', and 'Current Version'. It lists two assets: 'CBkv1-7' and 'CBkv1-3', both with 'vmanage-r3' as the controller and sub-controller, and '17.09.05a.0.6476' as the current version. The 'Total Asset(s)' is 2. At the bottom of the main content area, there is a 'Distribute Now & Activate Later' toggle set to 'Distribute Now & Activate Later' and a calendar widget showing 'August 2024'.

Ressourcen bearbeiten

2. Klicken Sie auf Ressourcen bearbeiten.
3. Nehmen Sie die erforderlichen Änderungen vor, indem Sie Ressourcen unter Anlagen hinzufügen oder Anlagen hochladen auswählen oder löschen oder indem Sie den Stapelzeitplan ändern, indem Sie Änderungen am Datum oder an der Startzeit vornehmen.
4. Klicken Sie auf Stapel aktualisieren.

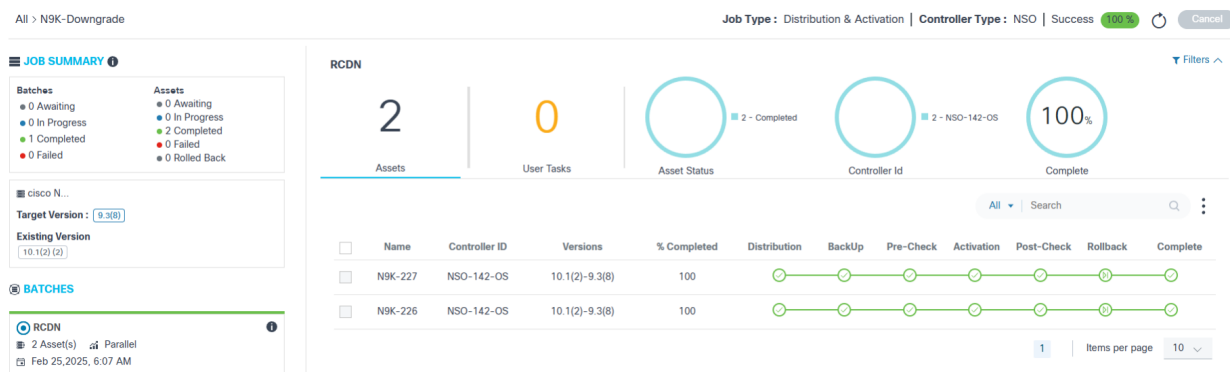
Ausführung von Upgrade-Aufträgen und Überwachung des Fortschritts

1. Melden Sie sich bei BPA mit Anmeldeinformationen an, die Zugriff auf Upgrade-Jobs haben.
2. Wählen Sie Betriebssystem-Upgrade > Upgrade-Jobs aus. Die Seite Upgrade-Auftrag wird angezeigt.

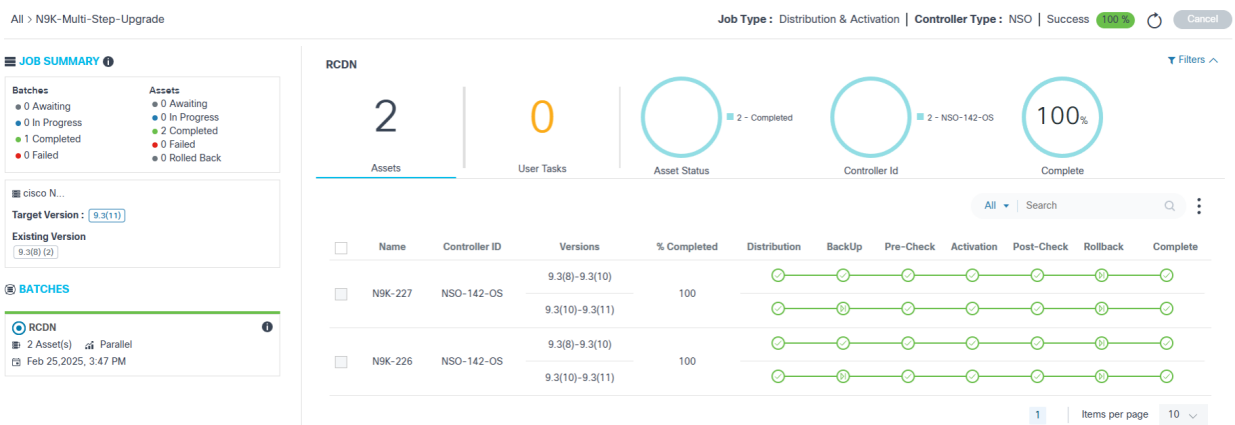


Auftrag aktualisieren

3. Verwenden Sie den Suchfilter in Kombination mit verfügbaren Diagrammfiltern, um den Job schnell zu filtern.
4. Klicken Sie auf den gewünschten Auftrag. Die Seite "Auftragsübersicht" wird angezeigt.



Upgrade in nur einem Schritt



Upgrade in mehreren Schritten

Im linken Bereich finden Sie folgende Informationen:

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

Job-Zusammenfassung

- Kurze Zusammenfassung der Stapel und zugehörigen Ressourcen

 c8000v

Target Version : 17.09.01a.0.240

Existing Version
17.09.03.0.15 (1)

Details zur Konformitätsrichtlinie (falls die Richtlinie nur ein Modell umfasst)

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

Target Version :

10.2.5

Existing Release

9.3(7) [4]

Details zur Konformitätsrichtlinie (falls die Richtlinie mehrere Modelle umfasst)

- Betroffenes Gerätemodell des Auftrags, Zielsoftwareversion und vorhandene Release-Version
- Eine Liste der Stapel, die zu diesem Auftrag gehören

BATCHES

chennai

1 Asset(s)

Parallel

Aug 14,2023, 12:20 PM

Batch-Details

- Chargendetails:
 - Der graue obere Rand zeigt an, dass der Stapel auf den Zeitplan wartet.
 - Blauer oberer Rand zeigt an, dass die Batch-Bereitstellung in Bearbeitung ist.
 - Der grüne obere Rand zeigt an, dass die Batch-Bereitstellung abgeschlossen ist.

Die folgenden Informationen werden oben auf der Seite "Job Summary" angezeigt:

All > vmanage_1_2_e2e

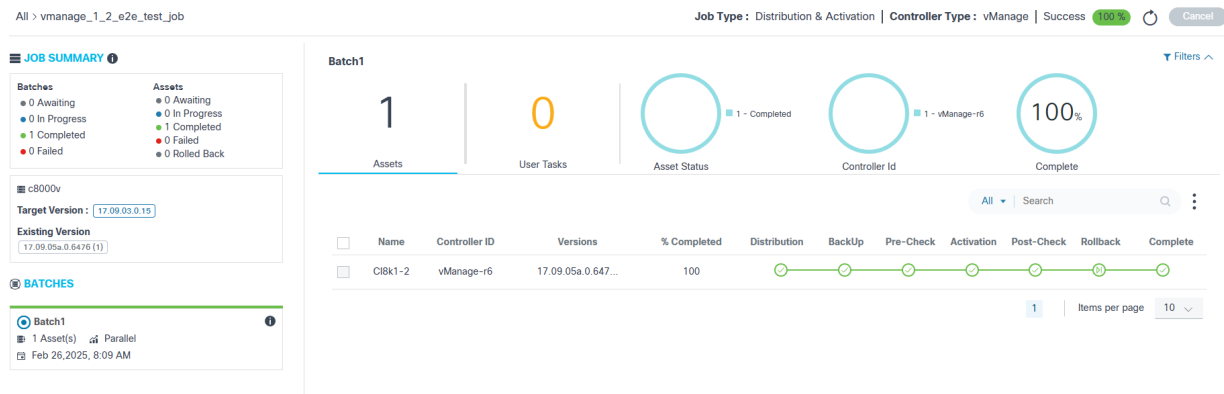
Job Type : Distribution & Activation | Controller Type : vManage | Success 100 % Cancel

Wichtigste Jobübersicht

- Die Breadcrumb-Navigation des aktuellen Jobs (z.B. All > vmanage_1_2_e2e). Die Option Alle wechselt zum Jobs Dashboard
- Der Auftragstyp
- Der Controller-Typ
- Auftragsstatus mit Abschlussprozentsatz:
 - Erfolg: Upgrade-Auftrag erfolgreich
 - Fehlgeschlagen: Fehler beim Upgrade-Auftrag.
 - In Bearbeitung: Upgrade-Job wird ausgeführt

 Anmerkung: Der Auftragsstatus wird in den Status "In Bearbeitung" verschoben, auch wenn der Zeitplan eines Stapels erreicht ist.

- Wartend: Job ist übernommen, wartet aber darauf, dass einer oder mehrere Batch-Zeitpläne erreicht werden



Job-Zusammenfassung

Die folgenden Optionen sind auf der Seite Job Summary (Auftragsübersicht) verfügbar:

- Über das Symbol Aktualisieren können Benutzer Aktualisierungen bei Bedarf abrufen.
- "Abbrechen" wird verwendet, um die Jobs in der Entwurfsstufe und der Commit-Stufe abzubrechen, es sei denn, der Zeitplan für einen Stapel ist erreicht.
- "Aktivieren" erstellt einen neuen Aktivierungsauftrag im Entwurfsstatus mit den gleichen Stapeln und Ressourcen, die Teil des zuvor abgeschlossenen Auftrags waren
 - Activate ist nur verfügbar, wenn der Auftragstyp Distribution lautet und erfolgreich abgeschlossen wurde.
 - Wenn der Aktivierungsauftrag bereits erstellt wurde und auf Aktivieren geklickt wird, wird eine Meldung mit dem Status des zuvor erstellten Auftrags angezeigt, in der die Option zur Umleitung des bereits erstellten Auftrags angegeben ist. Beim neu erstellten Auftrag können Benutzer Stapel oder Ressourcen bearbeiten oder löschen, aber Auftragstyp, Kontrollertyp und Konformitätsrichtlinie können nicht bearbeitet werden.
- Eine seitenweise Liste der Ressourcen wird unterhalb des Abschnitts "Analysen" angezeigt.

- Das Feld Suchen ermöglicht die allgemeine und feldspezifische Suche nach Spalten, z. B.:
 - Device Name (Gerätename)
 - Controller-ID
 - Seriennummer

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

1 | Items per page 10

Batch-Bericht herunterladen

- Die Option zum Herunterladen des Reports auf Stapelbasis durch Auswahl des Symbols Weitere Optionen > Herunterladen; Der Bericht enthält die Details auf Stapelbasis mit Gerätedetails.

☐	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	✓	✓	✓	✓	✓	✓	✓

1 | Items per page 10

Sortieren - Upgrade in einem Schritt

☐	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)		✓	✓	✓	✓	✓	✓	✓

Sortieren - Upgrade in mehreren Schritten

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

- chennal
 - 1 Asset(s) Parallel
 - Feb 19, 2025, 4:48 PM

chennal

1 Assets
 0 User Tasks
 1 - Completed Asset Status
 1 - NSO-142 Controller Id
 Complete

☐	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...]		✓	✓	✓	✓	✓	✓	✓

7.6.2[Bridge SMUs] - 7.7.2

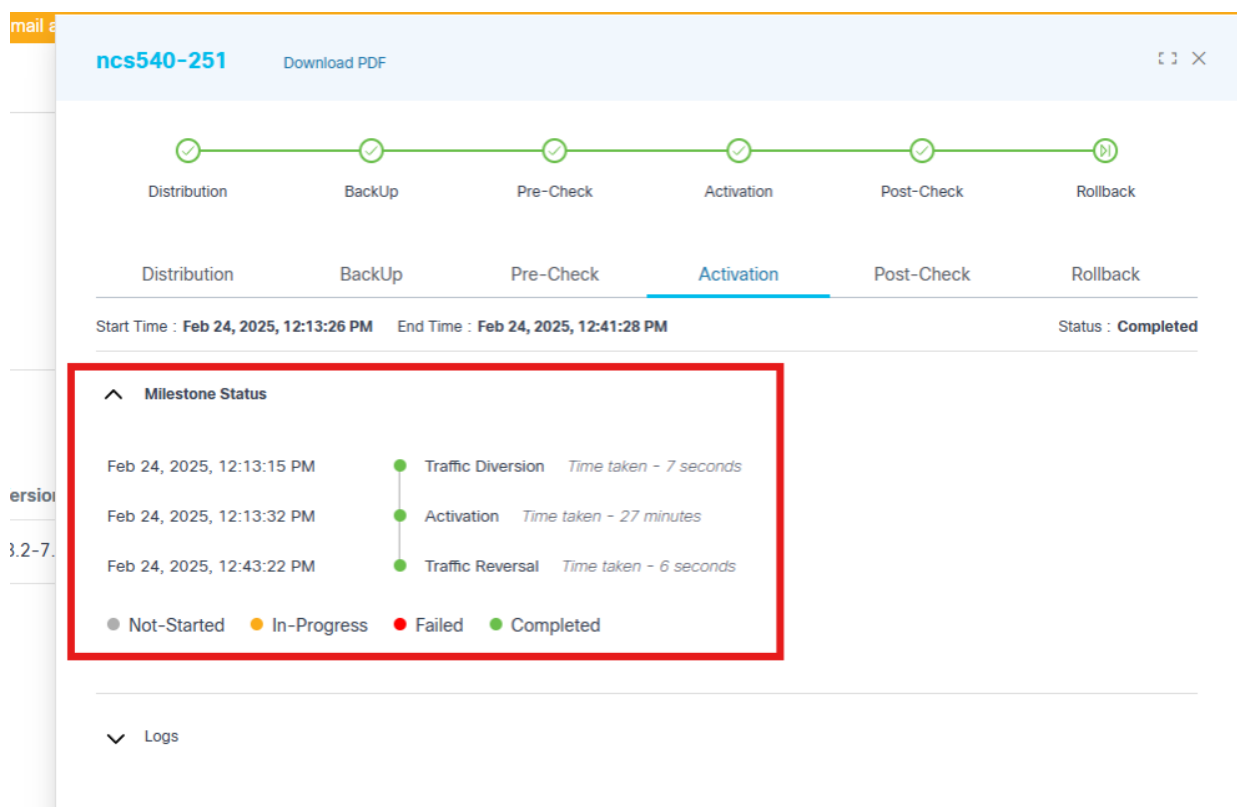
1 | Items per page 10

Sortieren - Bridge-SMU-Upgrade

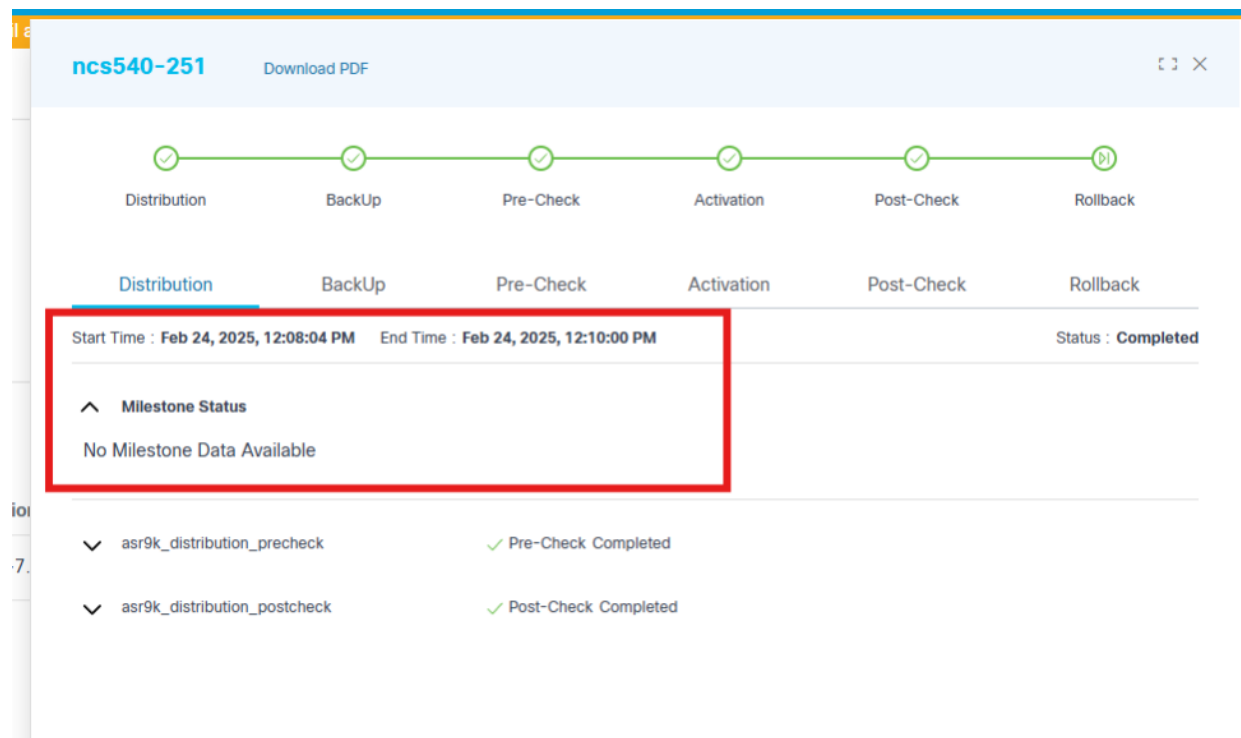
- Die Sortierung kann durch Klicken auf die Spaltennamen erfolgen
- Die folgenden Upgrade-Meilensteine werden für jedes Gerät zusammen mit Name, Controller-ID, Versionen und % Abgeschlossen angezeigt:
 - Vertrieb
 - Backup
 - Vorabprüfung
 - Verkehrsumleitung
 - Aktivierung
 - Nachprüfung
 - Verkehrsumkehr
 - Rollback
 - Abschließen

 Anmerkung: % abgeschlossen zeigt den Fortschritt basierend auf der Anzahl der abgeschlossenen Meilensteine für ein Gerät an. Alle Fertigstellungsprozentsätze auf Geräteebe in einem Stapel werden zusammengefasst, um den Fertigstellungsprozentsatz zu berechnen. Im Gegenzug werden alle Prozentsätze für die Fertigstellung des Stapels zusammengefasst, um den Prozentsatz für die Fertigstellung auf Jobebene zu berechnen.

Unter Sub-Meilensteinen werden auch benutzerdefinierte Meilensteine bezeichnet. Hierbei handelt es sich um die wichtigen Zwischenschritte, die ausgeführt werden und beim Hinzufügen unter dem Standard-Meilenstein angezeigt werden. Weitere Informationen zum Hinzufügen benutzerdefinierter Meilensteine finden Sie im [BPA-Entwicklerhandbuch](#).



Sub-Meilensteinansicht (Wenn Sub-Meilensteine unter dem Standard-Meilensteinnamen hinzugefügt werden)



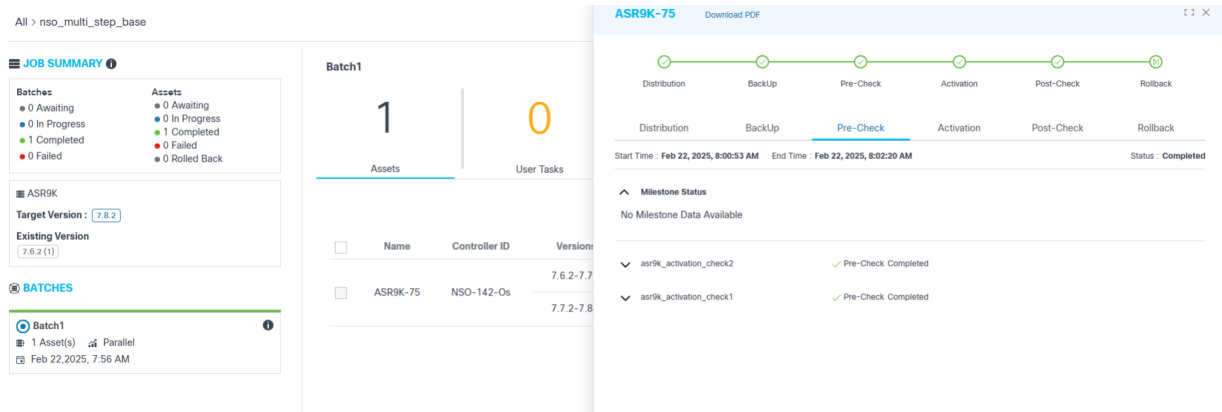
Ansicht der untergeordneten Meilensteine (wenn die untergeordneten Meilensteine nicht unter dem Standardnamen des Meilensteins hinzugefügt werden)



Anmerkung: Die Meilensteine variieren je nach ausgewähltem Auftragstyp. Der TrafficReversal-Meilenstein ist für Vertriebsjobs nicht verfügbar.

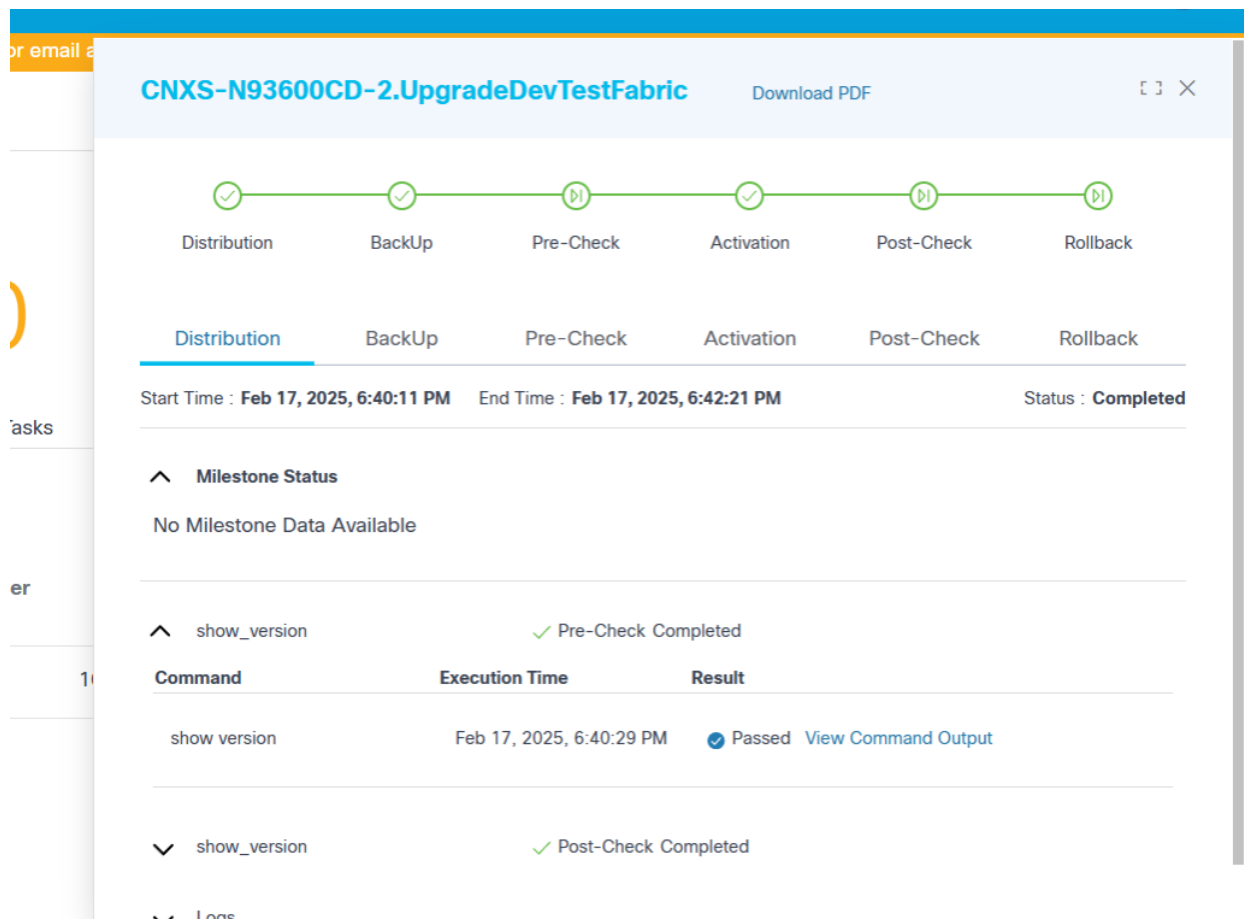
Verkehrsumleitung und Verkehrsumkehr werden im Rahmen des Aktivierungsmeilensteins bewegt.

- Eine Meilenstein-Farblegende, die aus folgenden Elementen besteht:
 - Grauer Scheck: Ausstehend
 - Blauer Scheck: In Bearbeitung
 - Grüne Markierung: Übersprungen
 - Grüner Scheck: Completed
 - Orange Check: Benutzeraufgabe
 - Roter Scheck: Fehler



Meilensteinansicht vor und nach der Überprüfung

Bei Meilensteinen mit Pre- oder Post-Check-Ausführung können Anwender die vollständige Befehlsausgabe zusammen mit den Validierungsregeln und deren Status für alle in der jeweiligen Prozessvorlage konfigurierten Befehle einsehen.



Meilensteinansicht der Distribution mit Befehlsausgabe vor der Überprüfung

1. Klicken Sie auf den Link Befehlsausgabe anzeigen, um die Befehlsausgabe und die Regeln anzuzeigen, die mit den Befehlen vor und nach der Überprüfung verknüpft sind.

Rules:

View Rules

Operation

Result

#Rule1

!Contains

✓

▼

Command Output:

Tue Nov 26 06:14:52.404 UTC

23099260 kbytes total (14885100 kbytes free)

Befehlsausgabe vor und nach der Überprüfung und zugehörige Regeln

- Klicken Sie auf das Symbol "Erweitern", um vollständige Details zu jeder Regel anzuzeigen.

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

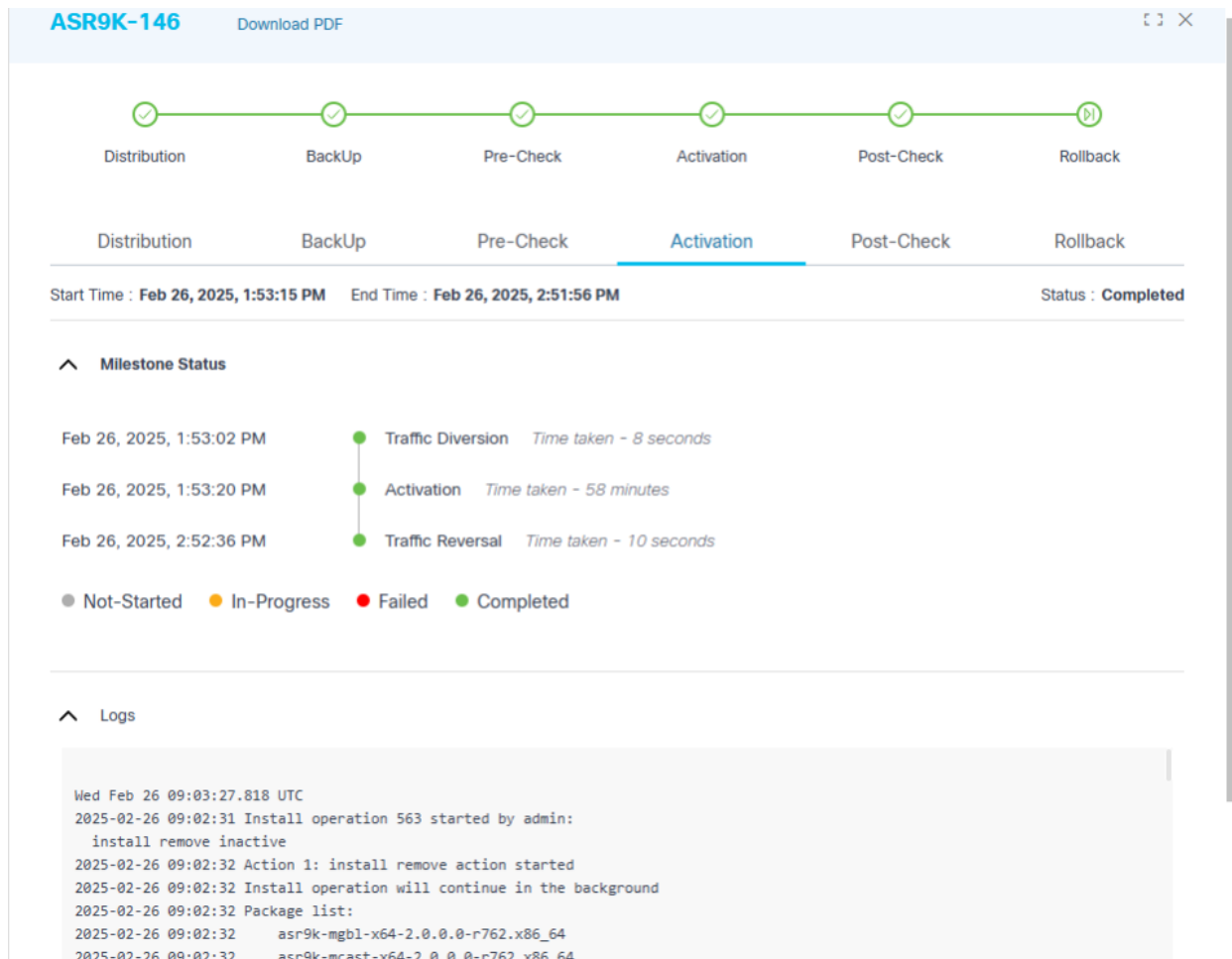
!

aaa authentication groups group aaa-r

gid 100

users %__system_user__%

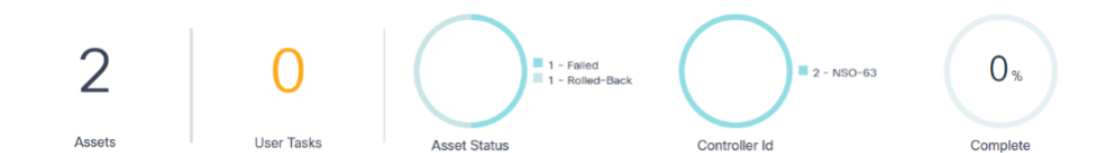
Befehlsausgabe vor und nach der Überprüfung mit Validierungsregeln



Meilenstein-Ansicht der Aktivierung mit Live-Protokollen

Die obige Abbildung enthält Details zum Aktivierungsmeilenstein. Dieser umfasst Live-Protokolle, die den Fortschritt der Softwareaktivierung eines bestimmten Geräts überwachen.

Wenn ein Meilenstein beginnt oder abgeschlossen wird, werden durch Klicken auf den Meilenstein weitere Informationen angezeigt.



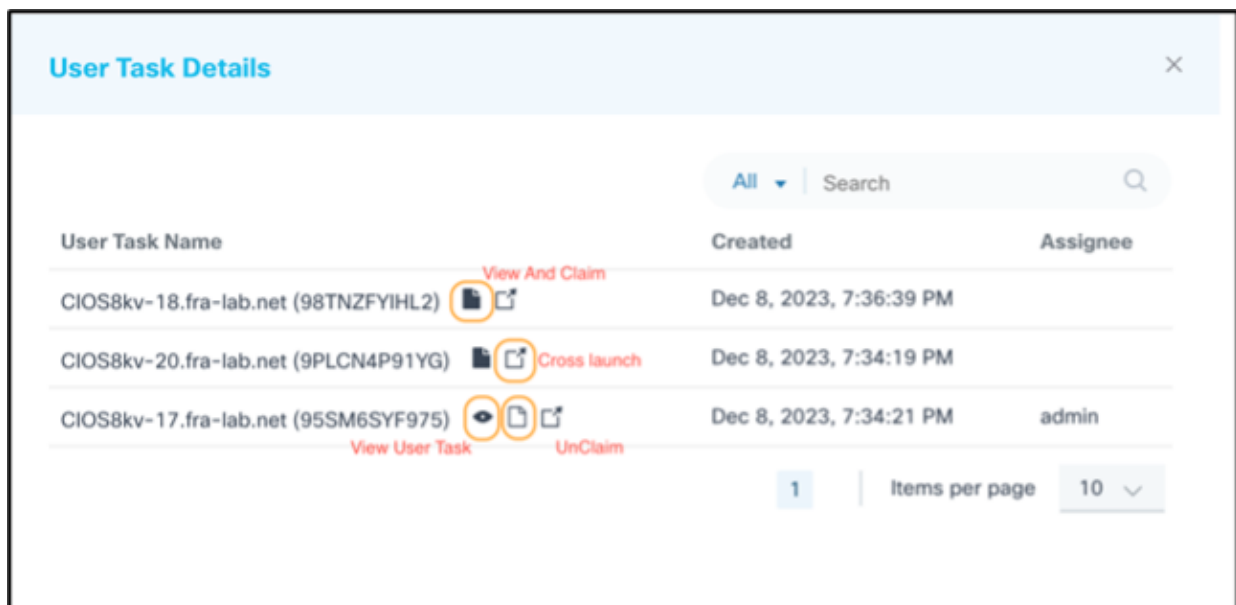
Bereich Analytik

Im Abschnitt "Analysen", der oben auf der Seite "Jobübersicht" angezeigt wird, werden die folgenden Informationen zum aktuell ausgewählten Job angezeigt:

- Der Stapelname (z. B. Asien)
- Filter ^ verkleinert und erweitert den Analysebereich
- Die folgenden Stapeldetails werden der Reihe nach angezeigt:

- Ressourcen: Gesamtzahl der Aktiva
- Benutzeraufgaben: Gesamtanzahl der Benutzeraufgaben, die auf Eingaben des Operations-Benutzers oder des Administrators warten
- Bestandsstatus: Filtert die Stapelgeräte nach ihrem Status. Der Rollback-Filter wurde hinzugefügt, um Geräte zu identifizieren, für die ein Rollback erfolgreich durchgeführt wurde.
- Controller-ID: Filtert die zu der ausgewählten Controller-ID gehörenden Batch-Geräte
- Vollständig: Gesamter Prozentsatz der Chargenabwicklung

Um auf Benutzeraufgaben zu reagieren, klicken Sie auf die Anzahl der Benutzeraufgaben. Das Fenster Benutzeraufgabendetails wird mit folgendem Inhalt geöffnet:

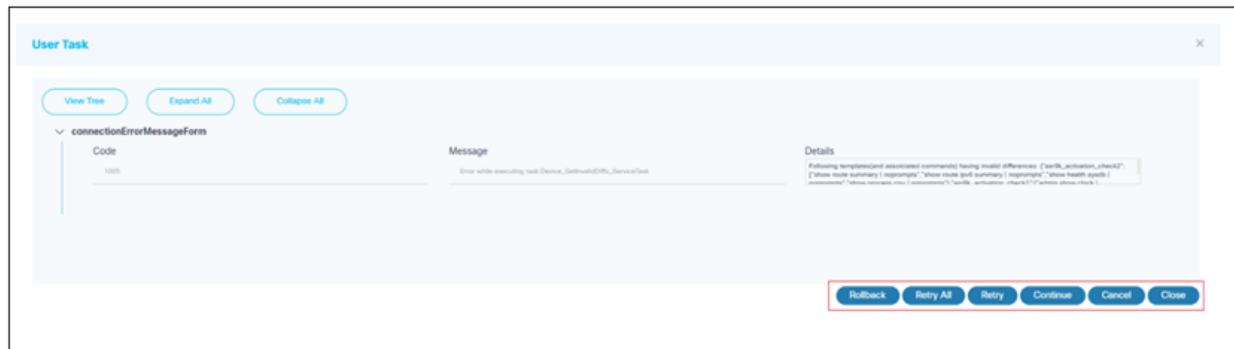


The screenshot shows a window titled "User Task Details" with a close button (X) in the top right corner. Below the title bar is a search bar with a dropdown menu set to "All" and a search icon. The main content is a table with three columns: "User Task Name", "Created", and "Assignee". There are three rows of data. Each row has a set of icons to its left. The first row has a "View And Claim" icon. The second row has a "Cross launch" icon. The third row has "View User Task" and "UnClaim" icons. The table is paginated, showing 1 item per page out of 10 items.

User Task Name	Created	Assignee
CIO8kv-18.fra-lab.net (98TNZFYIHL2)	Dec 8, 2023, 7:36:39 PM	
CIO8kv-20.fra-lab.net (9PLCN4P91YG)	Dec 8, 2023, 7:34:19 PM	
CIO8kv-17.fra-lab.net (95SM6SYF975)	Dec 8, 2023, 7:34:21 PM	admin

Details der Benutzeraufgabe

- Eine Liste der Benutzeraufgaben, die den jeweiligen Geräten entsprechen, die Aufmerksamkeit erfordern.
- Die folgenden Symbole für Optionen für Benutzeraufgaben:
 - Ansicht und Forderung: Details zu Benutzeraufgaben anzeigen
 - Cross-Launch: Anzeigen der BPA-Workflow-Aufgaben in der klassischen Benutzeroberfläche
 - Nicht beanspruchen: Benutzeraufgabenzuweisung entfernen
 - Benutzeraufgabe anzeigen: Details zu Benutzeraufgaben anzeigen



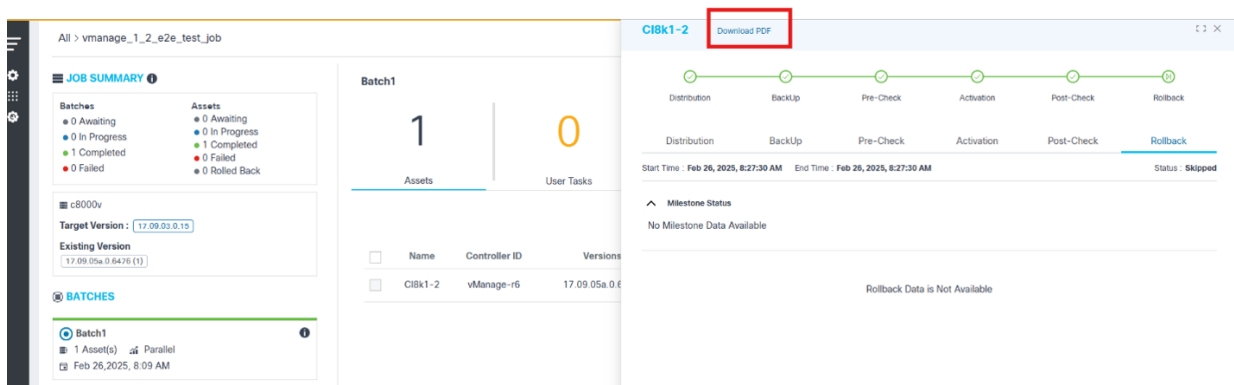
Benutzeraufgabe

Option "Benutzeraufgabe anzeigen"

- Je nach Aufgabenkontext werden die folgenden Optionen angezeigt:
 - Wiederholen: Führt die Aufgabe erneut aus
 - Alle wiederholen: Führt alle Vor- und Nachprüfungen erneut aus
 - Fortfahren: Fahren Sie mit der nächsten Aufgabe fort.
 - Rollback: Wechselt zurück zur vorherigen Version; Diese Option ist verfügbar, wenn die Aktivierung oder Nachprüfung fehlgeschlagen ist oder ungültige Unterschiede zwischen den Vor- und Nachprüfungen festgestellt wurden.
 - Abbrechen: Bricht den aktuellen Job ab
 - Schließen: Schließt das Fenster Benutzeraufgabe.
- Reagieren Sie ggf. auf die Benutzeraufgaben, und wählen Sie das Symbol Aktualisieren, um die Gesamtanzahl der Benutzeraufgaben zu aktualisieren.
- Gesamter Batch-Fertigstellungsprozentsatz
- Klickbares Diagramm zum Filtern nach Controller-IDs

 Anmerkung: Die Zahl vor der Controller-ID gibt die Gesamtzahl der vom jeweiligen Controller verwalteten Geräte an.

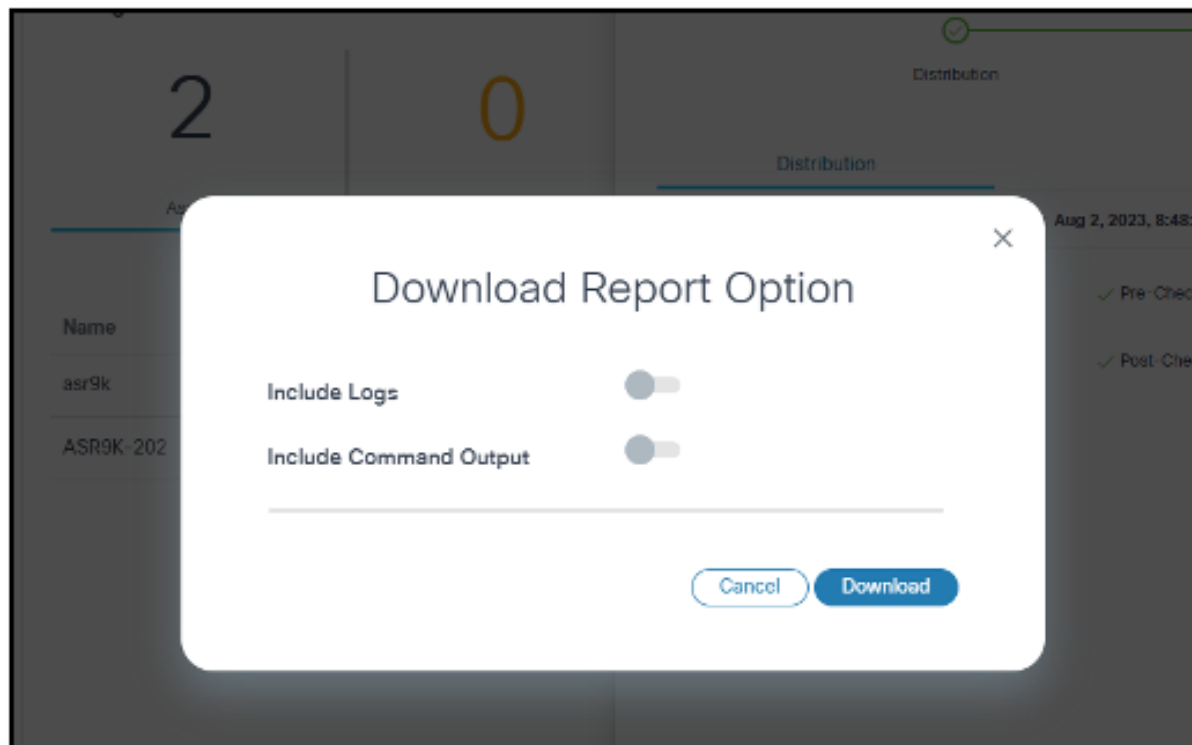
Bericht zum Software-Upgrade herunterladen



PDF herunterladen

Der Gerätenamen wird angezeigt, gefolgt von Download PDF in der Kopfzeile der Detailansicht. Benutzer können den Upgrade-Bericht für das aktuell ausgewählte Gerät im PDF-Format erstellen und herunterladen. So laden Sie den Upgrade-Bericht im PDF-Format herunter:

1. Klicken Sie auf PDF herunterladen. Das Fenster Download Report Option wird geöffnet.



Berichtsoption herunterladen

2. Aktivieren Sie die Umschalter Protokolle einschließen und Befehlsausgabe einschließen.
 - Protokolle einschließen: Umfasst Live-Protokolle (falls vorhanden) im Bericht
 - Befehlsausgabe einschließen: Schließt die Befehlsausgabe der Vor- und Nachprüfungen in den Bericht ein; In diesem Fall folgt der Befehl den Regeln.
3. Klicken Sie auf Download (Herunterladen). Die Berichterstellung wird gestartet.



Anmerkung: Wenn Sie sowohl Include-Protokolle als auch Include Command Output aktivieren, verlängert sich die Verarbeitungszeit für die Berichterstellung und die Berichtsgröße. Verwenden Sie diese Umschalter nur, wenn ein detaillierter Bericht erforderlich ist. Befehlsregeln sind im Bericht enthalten, unabhängig davon, ob die Befehlsausgabe aktiviert oder deaktiviert ist.

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
<pre>Rules : Rule View Rules Operation Result #Rule1 Invalid input detected !Contains Passed #Rule2 asdf Contains Failed #Rule3 qwerty !Contains Passed</pre>		

Gerätebericht

Jobs archivieren

1. Melden Sie sich bei BPA mit Anmeldeinformationen an, die über ausreichenden Zugriff auf Upgrade-Jobs verfügen.
2. Wählen Sie Betriebssystem-Upgrade > Upgrade-Jobs aus. Die Seite Upgrade-Auftrag wird angezeigt.
3. Verwenden Sie den Suchfilter in Kombination mit verfügbaren Diagrammfiltern, um die Jobs zu filtern.
4. Wählen Sie einen oder mehrere Jobs aus.



Auftrag archivieren

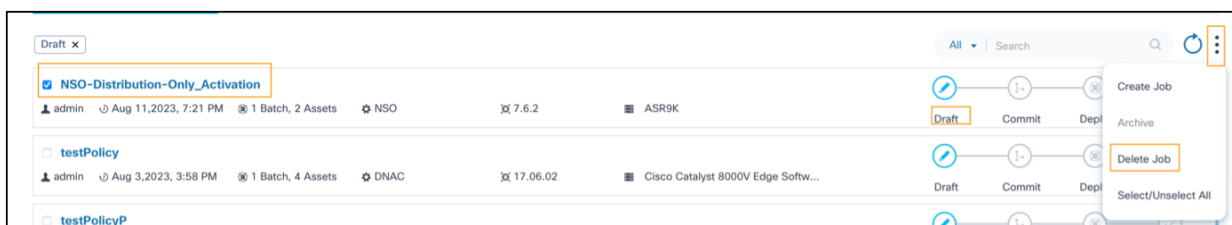
5. Wählen Sie das Symbol Weitere Optionen > Archivieren aus.



Anmerkung: Nur abgeschlossene Jobs können archiviert werden.

Löschen von Jobs

1. Melden Sie sich bei BPA mit Anmeldeinformationen an, die über ausreichenden Zugriff auf Upgrade-Jobs verfügen.
2. Wählen Sie Betriebssystem-Upgrade > Upgrade-Jobs aus. Die Seite Upgrade-Auftrag wird angezeigt.
3. Verwenden Sie den Suchfilter in Kombination mit verfügbaren Diagrammfiltern, um die Jobs zu filtern.
4. Wählen Sie einen oder mehrere Jobs aus.



Auftrag löschen

5. Wählen Sie das Symbol Weitere Optionen > Job löschen aus.



Anmerkung: Jobs können nur gelöscht werden, wenn sie sich im Entwurfsstadium befinden.

Löschen von Stapeln in Jobs

 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](#)

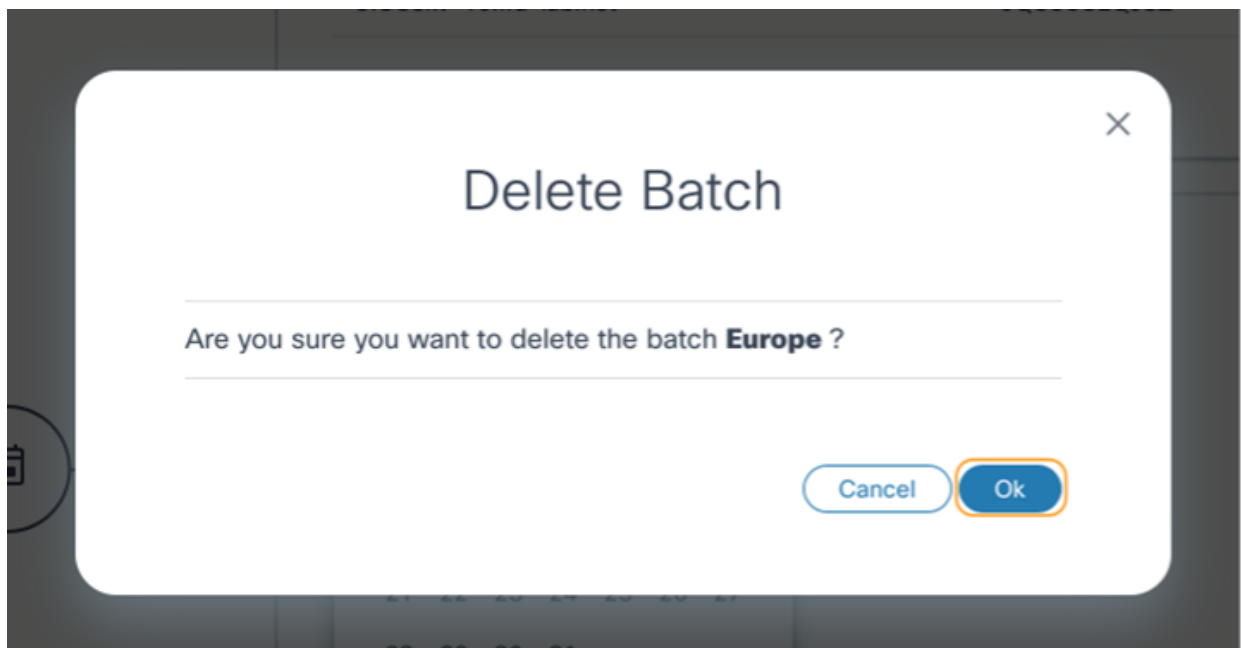
10 Assets Pending

Batch Name *

Europe



1. Klicken Sie im Seitenbereich auf das Symbol Löschen des gewünschten Stapels. Ein Bestätigungsfenster wird geöffnet.



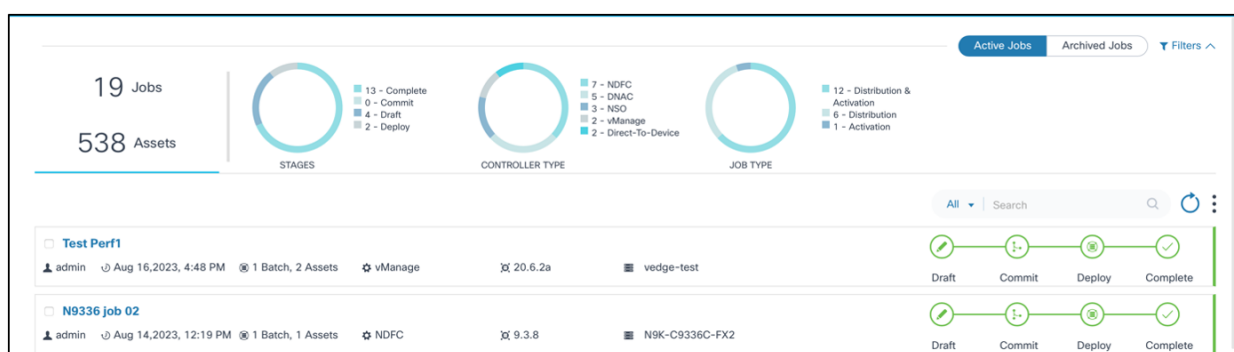
Löschen des Stapels bestätigen

2. Klicken Sie auf OK.

Mit dem gelöschten Stapel verknüpfte Ressourcen werden in den Pool ausstehender Ressourcen zurückgeführt und können in neuen oder vorhandenen Stapeln ausgewählt werden.

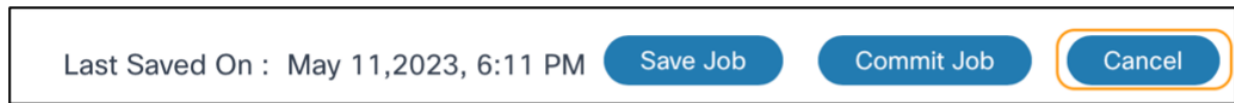
Jobs abbrechen

1. Melden Sie sich bei BPA mit Anmeldeinformationen an, die über ausreichenden Zugriff auf Upgrade-Jobs verfügen.
2. Wählen Sie Betriebssystem-Upgrade > Upgrade-Jobs aus. Die Seite Upgrade-Auftrag wird angezeigt.



Auftrag aktualisieren

3. Verwenden Sie den Suchfilter in Kombination mit verfügbaren Diagrammfiltern, um den gewünschten Job zu filtern.
4. Klicken Sie auf den gewünschten Auftrag. Die Seite "Auftragsübersicht" wird angezeigt.

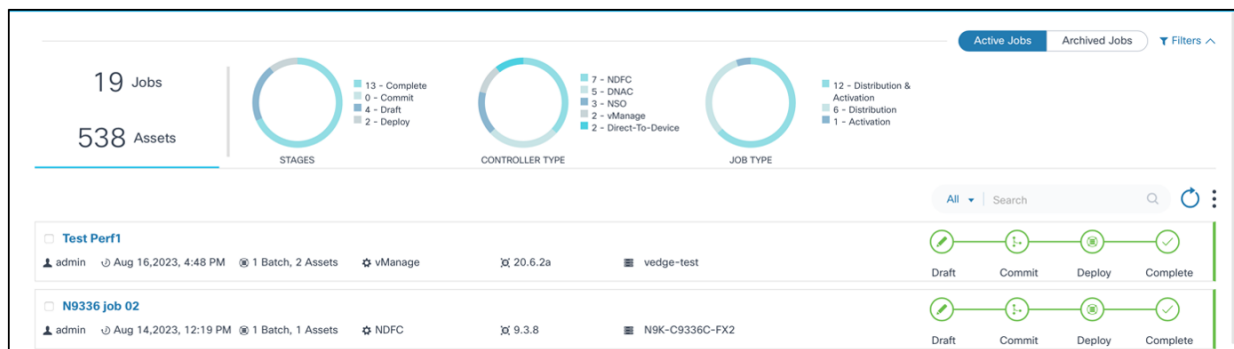


Abbrechen

5. Klicken Sie auf Abbrechen.

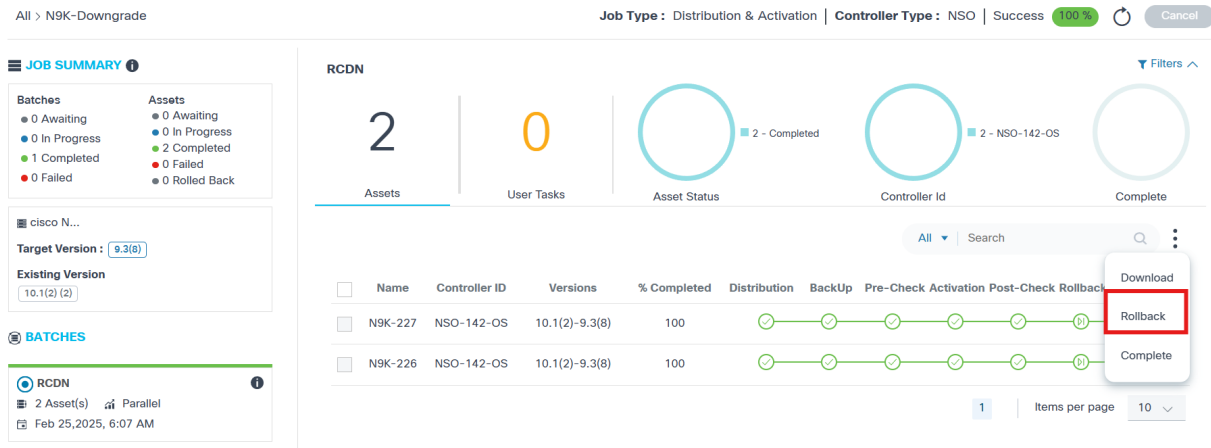
Rollback abgeschlossener Jobs oder Upgrades

1. Melden Sie sich bei BPA mit Anmeldeinformationen an, die über ausreichenden Zugriff auf Upgrade-Jobs verfügen.
2. Wählen Sie Betriebssystem-Upgrade > Upgrade-Jobs aus. Die Seite Upgrade-Auftrag wird angezeigt.



Auftrag aktualisieren

3. Verwenden Sie den Suchfilter in Kombination mit verfügbaren Diagrammfiltern, um den gewünschten Job zu filtern.
4. Klicken Sie auf den gewünschten Auftrag. Die Seite "Auftragsübersicht" wird angezeigt. Wählen Sie den gewünschten Stapel im linken Fensterbereich aus, und wählen Sie die gewünschten Geräte aus, für die im rechten Fensterbereich eine vollständige Bestätigung bzw. ein Rollback erforderlich ist.
5. Wählen Sie das Symbol More Options (Weitere Optionen) aus, und klicken Sie je nach Anforderung entweder auf Rollback (Rollback) oder auf Complete (Abschließen).



Rollback

 Anmerkung: Geräte können nur ausgewählt werden, wenn die folgenden Voraussetzungen erfüllt sind:

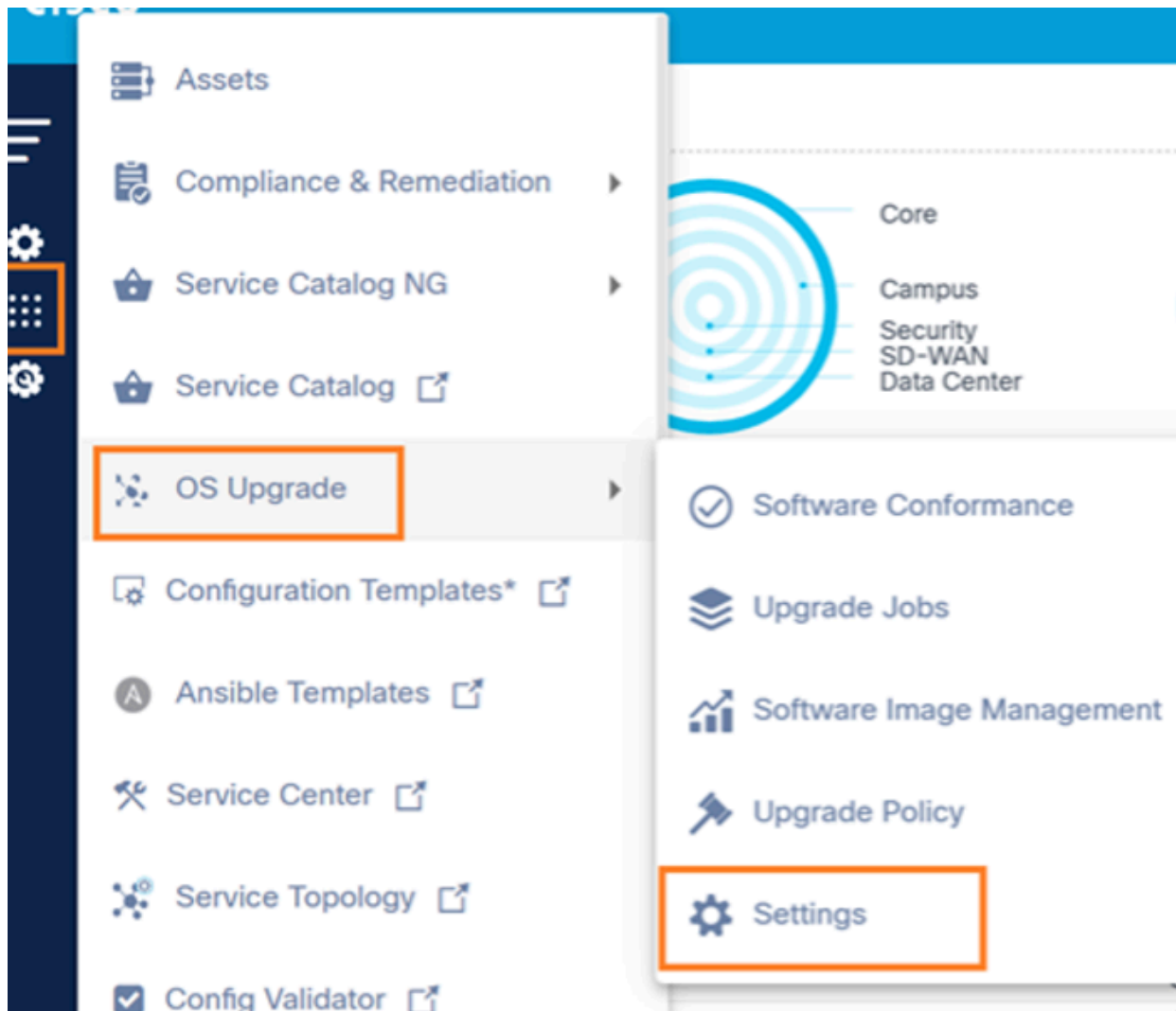
- Die Einstellungen müssen so konfiguriert werden, dass die Rollback-Option eines abgeschlossenen aktualisierten Jobs aktiviert wird. Weitere Informationen finden Sie unter [Einstellungen](#).
- Wenn innerhalb der vorgegebenen Zeit keine Maßnahmen ergriffen werden, werden die Geräte automatisch in den Status "Abgeschlossen" versetzt
- Für die Aktion "Rollback bei Bedarf" sind Geräte verfügbar, wenn das Rollback zuvor abgeschlossen wurde oder der Meilenstein für das Rollback den Status "Wartend" aufweist.

Einstellungen

Die Einstellungen für die Betriebssystemaktualisierung stellen einen Platzhalter für allgemeine Einstellungen bereit, die für andere Komponenten der Anwendung für die Betriebssystemaktualisierung verwendet werden.

So greifen Sie auf die Seite Einstellungen zu:

- Melden Sie sich bei BPA mit Anmeldeinformationen an, die den Zugriff auf die Einstellungen verwalten.



Einstellungen

2. Wählen Sie Betriebssystem-Upgrade > Einstellungen aus. Die Seite Einstellungen wird geöffnet.

Die Seite Einstellungen hat die beiden folgenden Register:

- Softwarekonformität: Auf dieser Registerkarte können Konfigurationen aktualisiert werden, die automatische Zeitpläne für die Konformitätsausführung zulassen.
- Rollback: Auf dieser Registerkarte können Konfigurationen aktualisiert werden, die ein Rollback für ein vollständiges Geräte-Upgrade ermöglichen.

Softwarekonformität

Registerkarte "Softwarekonformität"

Die Registerkarte "Softwarekonformität" enthält folgende Informationen:

- Geplante Konformitätsprüfung: Aktivieren oder Deaktivieren des Zeitplans
- Startdatum: Wählen Sie MM/TT/JJJJ



Anmerkung: Das Startdatum muss ein zukünftiges Datum sein.

- Cron-Muster: Machen Sie folgende Angaben:
 - Minuten (0-59)
 - Stunde (0-23)
 - Tag (Monat) (1-31)
 - Monat (1-12)
 - Tag (Woche) (1-7)
- Intervall für automatische Aktualisierung hinzufügen: Der Standardwert ist 30 Sekunden.
- Speichern: Änderungen speichern

Rollback

Registerkarte Rollback

Die Registerkarte Rollback bietet folgende Informationen:

- Umschalter für Benutzerüberprüfung: Benutzerüberprüfung aktivieren oder deaktivieren
 - Aktivierungsstatus: Die Geräte im Upgrade-Job warten auf die Bestätigung des Benutzers, den Rollback durchzuführen, oder das Upgrade abzuschließen, bis die unter "Configuration Threshold Time" (Konfigurationsschwellenwert-Zeit) konfigurierte Schwellenzeit erreicht ist. Wenn sie erreicht sind, wechseln die Geräte automatisch in den Status "Abgeschlossen".
 - Deaktivierter Status: Geräte im Upgrade-Job schließen das Upgrade automatisch ab, ohne auf die Bestätigung durch den Benutzer zu warten.
- Zeit für Bestätigungsschwellenwert: Hinzufügen einer bestimmten Wartezeit in Stunden
- Speichern: Änderungen speichern

Bereitstellungskonfiguration

- Standardzeitpläne für die Konformitätsprüfung und die SWIM-Metadaten werden täglich um 7:25 Uhr Ortszeit konfiguriert.
- Um die Standardzeitpläne für die Synchronisierung der SWIM-Bildmetadaten zu ändern, navigieren Sie zum installierten BPA-Verzeichnis "<BPA-Installationsverzeichnis>/conf/@cisco-bpa-platform/mw-osupgrade-nxtgen/config.json" und aktualisieren Sie die Eigenschaft "schedule.swimSchedule" mit dem Cron-Ausdruck. Zeitpläne können nach der Bereitstellung aktualisiert werden. Weitere Informationen finden Sie unter [Softwarekonformität](#).
- So erhöhen oder verringern Sie die maximale Anzahl von Geräten, die für verschiedene Controllertypen im Parallelmodus verarbeitet werden:

1. Aktualisieren Sie die folgenden Dateien:

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

2. Navigieren Sie zu Update Throttle > Capabilities > Image-Activation, Image-distribute, um die gleichzeitige Aktivierungs- oder Verteilungsgrenze zu erhöhen.

 Anmerkung: Bevor Sie diese Einschränkungen aktualisieren, sollten Sie die [unterstützten Controller und Geräteplattformen](#) lesen.

Zugriffskontrolle

Rollenbasierte Zugriffskontrolle

BPA unterstützt die rollenbasierte Zugriffskontrolle (RBAC). Im RBAC-Modell kapselt eine Rolle einen Satz von Berechtigungen (d. h. Aktionen), die ein Benutzer ausführen kann. Für die Zugriffskontrolle können Administratoren Benutzergruppen entweder vordefinierte Rollen oder neu erstellte Rollen mit Berechtigungen zuweisen. Ein Benutzer kann einer oder mehreren Benutzergruppen angehören, und jede Benutzergruppe kann einer oder mehreren Rollen zugewiesen werden, die den Benutzern in dieser Gruppe bestimmte Zugriffsberechtigungen zuweisen.

In der folgenden Tabelle sind die OOB-Betriebssystem-Upgrade-Rollen und die zugehörigen Berechtigungen aufgeführt.

Service	Gruppe	Absicht	Super-Administrator	Ticket-Administrator verwenden	
OSUpgradeService	ui_app	Anwendung für Aktualisierungsaufträge anzeigen oder ausblenden	Ja	Ja	J
OSUpgradeService	ui_app	Softwarekonformitätsanwendung anzeigen oder ausblenden	Ja	Ja	J
OSUpgradeService	ui_app	SWIM-Anwendung ein- oder ausblenden	Ja	Ja	J
OSUpgradeService	ui_app	Software-Upgraderichtlinien anzeigen oder ausblenden	Ja	Ja	J
OSUpgradeService	ui_app	Software-Upgrade-Einstellungen anzeigen oder ausblenden	Ja	Ja	J
OSUpgradeService	Aufträge aktualisieren	Verwaltung von Upgrade-Jobs (z. B. Erstellen, Aktualisieren, Löschen und Übertragen)	Ja	Ja	M
OSUpgradeService	Aufträge aktualisieren	Upgrade-Jobs abbrechen	Ja	Ja	M
OSUpgradeService	Aufträge aktualisieren	On-Demand-Archivierung der Jobs	Ja	Ja	M
OSUpgradeService	Aufträge aktualisieren	Manuelle Genehmigung	Ja	Ja	M

Service	Gruppe	Absicht	Super-Administrator	Ticket-Administrator verwenden	
OSUpgradeService	Software-Konformitätsrichtlinie	Software-Konformitätsrichtlinien und Ausführungsergebnisse anzeigen	Ja	Ja	J
OSUpgradeService	Software-Konformitätsrichtlinie	Erstellen, Aktualisieren und Löschen von Software-Konformitätsrichtlinien	Ja	Ja	M
OSUpgradeService	Software-Konformitätsrichtlinie	On-Demand-Ausführung von Software-Konformitätsrichtlinien	Ja	Ja	M
OSUpgradeService	Upgrade-Richtlinie	Betriebssystem-Upgrade-Richtlinien anzeigen	Ja	Ja	J
OSUpgradeService	Upgrade-Richtlinie	Richtlinien für Betriebssystem-Upgrades verwalten	Ja	Ja	M
OSUpgradeService	Swim-Image-Management	Software-Images erstellen, aktualisieren und löschen	Ja	Ja	M
OSUpgradeService	Swim-Image-Management	SWIM anzeigen	Ja	Ja	J
OSUpgradeService	Swim-Image-Management	Synchronisierung von Software-Images	Ja	Ja	M
OSUpgradeService	Software-Empfehlungen	Metadaten für Softwareempfehlungen synchronisieren	Ja	Ja	M
OSUpgradeService	Software-Empfehlungen	Anzeigen von Ratgebern oder Einblicken	Ja	Ja	J
OSUpgradeService	Software-Empfehlungen	Verwaltung der Konformitätsrichtlinie	Ja	Ja	M
OSUpgradeService	Softwarekonformität	Software-Konformitätseinstellungen anzeigen	Ja	Ja	J
OSUpgradeService	Softwarekonformität	Verwalten von Softwarekonformitätseinstellungen	Ja	Ja	M



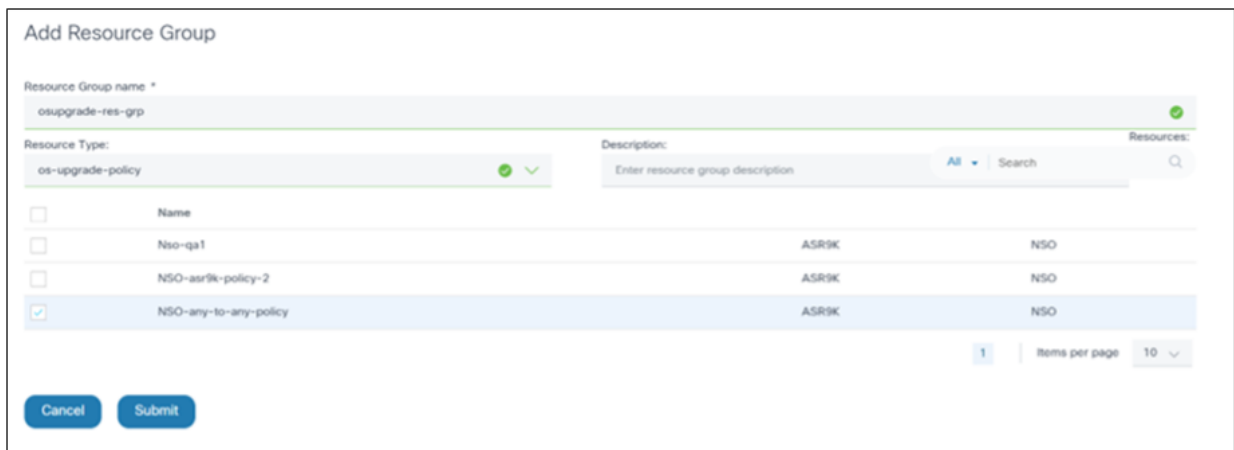
Anmerkung: Benutzerdefinierte Rollen und Berechtigungszuordnungen können je nach Anforderungen durchgeführt werden. Weitere Informationen finden Sie unter

Ressourcengruppen

Diese Funktion bietet eine präzise Zugriffskontrolle für BPA-Ressourcen, z. B. für Upgrade-Richtlinien, sodass nicht autorisierte Benutzer die in der Anwendung für Betriebssystem-Upgrades definierten Richtlinien nicht aktualisieren können. Administratoren können den Zugriff einschränken, indem sie eine Ressourcengruppe mit zugänglichen Richtlinien definieren.

So erstellen Sie eine Ressourcengruppe:

1. Navigieren Sie zu Einstellungen > Ressourcengruppen.



Add Resource Group

Resource Group name *
osupgrade-res-grp

Resource Type:
os-upgrade-policy

Description:
Enter resource group description

Resources:

Name	ASR9K	NSO
Nso-qa1	ASR9K	NSO
NSO-asr9k-policy-2	ASR9K	NSO
☒ NSO-any-to-any-policy	ASR9K	NSO

1 | Items per page: 10

Cancel Submit

Ressourcengruppe hinzufügen

2. Erstellen Sie eine Ressourcengruppe mit Richtlinien, auf die Benutzer ohne Administratorrechte zugreifen können.
3. Wählen Sie os-upgrade-policy als Ressourcentyp aus. Die entsprechenden Ressourcen werden angezeigt.
4. Wählen Sie die erforderlichen Upgrade-Richtlinien aus.
5. Klicken Sie auf Senden. Nicht-Administrator-Benutzer, die zu dieser Benutzergruppe gehören, haben jetzt nur Zugriff auf die Richtlinien, die in der ausgewählten Ressourcengruppe verfügbar sind.

Um die Ressourcengruppe einer Benutzergruppe zuzuordnen, erstellen Sie eine Zugriffsrichtlinie.

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

Zugriffsrichtlinie hinzufügen

Anmerkung: Nachdem die Ressourcengruppe erstellt wurde, sollte sie über Zugriffsrichtlinien einer Benutzergruppe zugeordnet werden. Weitere Informationen zu den folgenden Aspekten finden Sie unter [Zugriffskontrolle](#):

- Benutzer
- Rollen
- Benutzergruppen
- Zugriffsrichtlinien
- Ressourcengruppen
- Ressourcengruppen

Das nachfolgende Beispiel zeigt einen Benutzer ohne Administratorrechte, der Zugriff auf beschränkte Ressourcen hat:

CISCO Business Process Automation

1 Policies | 1 - NSO Controller Types

Device Model	Controller Type	Name	Created By	Last Modified On
ASR9K	NSO	NSO-any-to-any-policy	admin	Jul 3, 2024, 4:18 PM

1 | Items per page 10

Nicht-Administrator-Benutzer mit Ressourcenbeschränkungen

Einstellung des Kennzeichens "Keine Vertrauenswürdigkeit"

Der Zugriff auf Ressourcen durch einen Benutzer kann je nach Einstellung des "Zero-Trust"-Flags variieren. Das Null-Trust-Flag kann auf true oder false festgelegt werden. In der folgenden Tabelle sind die Ressourcenzugriffsmöglichkeiten auf Basis der Einstellung für das Flag "Zero-Trust" zusammengefasst.

Benutzer	Benutzergruppe	Zugriffsrichtlinie	Ressourcengruppe	Ressourcen	Ohne Vertrauen	Aktiviert
Benutzer 1	UG1	AP1	RG1	2 Ressourcen	2 Ressourcen	2 Ressourcen
Benutzer 1	UG1	AP2	RG2	0 Ressourcen	0 Ressourcen	0 Ressourcen
Benutzer 1	UG1	AP3	Nil		0 Ressourcen	Alle Ressourcen
Benutzer 1	UG1	Nil	Nil		0 Ressourcen	Alle Ressourcen

So aktivieren oder deaktivieren Sie das Flag "Zero Trust":

1. Navigieren Sie zum folgenden Konfigurationspfad:

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

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

2. Ändern Sie den Wert zeroTrustPolicies.
3. Navigieren Sie zum folgenden Core-Paket:

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

4. Führen Sie den folgenden Befehl aus, um den Core Helm zu löschen:

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


5. Führen Sie den folgenden Befehl aus, um den Status der PODs zu überprüfen.

```
kubectl get pods -n bpa-ns
```

6. Führen Sie den folgenden Befehl aus, um den Core Helm zu installieren, nachdem alle PODs beendet wurden:

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

7. Führen Sie den folgenden Befehl aus, um den Status der PODs zu überprüfen:

```
kubectl get pods -n bpa-ns
```

Fehlerbehebung bei Betriebssystem-Upgrades

Dieser Abschnitt enthält Tipps zur Fehlerbehebung bei Problemen mit der Anwendung "Betriebssystem-Upgrade" in BPA.

Zielgerätemodell kann beim Erstellen einer Konformitätsrichtlinie nicht angezeigt werden

Stellen Sie sicher, dass die entsprechenden Image-Metadaten in den Software-Images unter SWIM verfügbar sind. Wenn sie nicht gefunden werden, führen Sie eine der folgenden Optionen aus:

- Synchronisieren von Bildern, um Bildmetadaten von Controllern wie Cisco Catalyst Center, NDFC, vManage und FMC abzurufen
- Erstellen der erforderlichen Image-Metadaten für Controller wie NSO, CNC, Direct-to-Device und ANSIBLE

Softwarekonformität zeigt Betriebsausfall an

Dies kann aus folgenden Gründen der Fall sein:

- Bei der Erstellung der Software-Konformitätsrichtlinie wurden keine Ressourcen mit dem ausgewählten Modell gefunden.
- Der Name des Modells in SWIM stimmt nicht mit dem Modell des Konformitätsgeräts im Gerätebestand für alle Geräte überein.
- Wenn die SMU als Teil der Softwarekonformitätserstellung ausgewählt wurde und die SMU-Erkennung für alle Geräte fehlgeschlagen ist
- Die für die Ausführung der Compliance-Prüfvorlage ausgewählte Prozessvorlage ist fehlgeschlagen oder wurde nicht gefunden.
- Die Seriennummer oder die aktuelle Version ist beim Erstellen der Softwarekonformität nicht für alle Geräte im ausgewählten Modell verfügbar

Der Status des Ergebnisses der Softwarekonformität bestimmter Geräte ist unbekannt

Dies kann aus folgenden Gründen der Fall sein:

- Der Name des Modells in SWIM stimmt nicht mit dem Modell des Konformitätsgeräts im Gerätebestand überein.
- Wenn die SMU als Teil der Softwarekonformitätserstellung ausgewählt wurde und die SMU-Erkennung für ein Gerät fehlschlug
- Die für die Ausführung der Compliance-Prüfvorlage ausgewählte Prozessvorlage ist fehlgeschlagen oder wurde nicht gefunden.
- Die Seriennummer oder die aktuelle Version ist für die Geräte nicht verfügbar.

Prozentsatz des Abschlusses des Aktualisierungsauftrags

Wenn der Fortschritt des Aktualisierungsauftrags trotz abgeschlossener Aktualisierung unter 100 % liegt, stellen Sie sicher, dass die Einstellungen "Auf Rollback warten" (Wait for Rollback) unter Betriebssystem-Upgrade > Einstellungen > Rollback aktiviert sind und dass die Option "Benutzerverifizierung" aktiviert ist. Wenn der Gesamtprozentsatz der Fertigstellung unter 100 bleibt, wählen Sie Rollback oder Complete (Abschließen).

Zeitplan erreicht, Geräte im Wartezustand

Wenn sich die Geräte nach der Initiierung des geplanten Auftrags im Wartezustand befinden, versuchen Sie, die Mikrodienste Kafka, Camunda, Scheduler und Betriebssystem-Upgrade neu zu starten.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.